Security Framework for Software Defined Wireless Networks

by

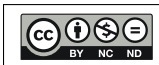
Christian MIRANDA

THESIS PRESENTED TO ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
IN PARTIAL FULFILLMENT FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
Ph.D.

MONTREAL, APRIL 15, 2023

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

 Christian MIRANDA, 2023



This Creative Commons license allows readers to download this work and share it with others as long as the author is credited. The content of this work cannot be modified in any way or used commercially.

BOARD OF EXAMINERS

THIS THESIS HAS BEEN EVALUATED

BY THE FOLLOWING BOARD OF EXAMINERS

M. Georges Kaddoum, Thesis supervisor
Department of Electrical Engineering, École de Technologie Supérieure

M. Segla Kpodjedo, President of the board of examiners
Génie logiciel et des TI, École de Technologie Supérieure

M. Khoa Nguyen Kim, Member of the jury
Department of Electrical Engineering, École de Technologie Supérieure

M. Khalil El-Khatib , External independent examiner
Faculty of Business and Information Technology, OntarioTech

THIS THESIS WAS PRESENTED AND DEFENDED

IN THE PRESENCE OF A BOARD OF EXAMINERS AND THE PUBLIC

ON FEBRUARY 15,2023

AT ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

ACKNOWLEDGEMENTS

First, I sincerely thank my supervisor, Professor Georges Kaddoum, for his unconditional support during my doctoral studies. His contribution to my academic success has been essential to this achievement.

One can only survive in the Ph.D. with peers who understand what it is to be a Ph.D. student. For this, I thank my lab-mates for their help and continuous encouragement. Precisely, I especially thank my colleagues who, with their expertise and empathy, collaborated with me to create my manuscripts, such as Kuljeet Kaur, Sahil Garg, Poulmanogo Illy, Jung-Yeon Baek and Bassant Selim. Thanks also to Dr. Elias Bou-Harb for his wise advice and support.

Moreover, I would like to thank MITACS and the companies that trusted me, such as Kontron and Ericsson, who contributed financially and scientifically to realizing my research projects. In particular, I sincerely thank Drs. Amine Boukhtouta, Taos Madi and Hyame Alameddine for the long hours of teaching and exchanging ideas, which they cultivated and contributed significantly to complete this critical stage of my life.

Finally, I would like to thank my mother, brother, and aunts and uncles for their unending support. Despite time and distance, they are always by my side.

Schéma de sécurité pour le réseaux sans fil définis par logiciel

Christian MIRANDA

RÉSUMÉ

Les réseaux 5G deviennent des infrastructures très complexes en raison des nouveaux services qu'ils sont censés fournir ainsi que de l'accessibilité accrue des appareils à l'internet. L'organisme de normalisation 3GPP ne cesse de promouvoir les meilleures pratiques et les processus de contrôle et de traitement des données au sein de ces infrastructures. Une pléthore de modèles commerciaux a également encouragé la prolifération et l'expansion de la connectivité des appareils et la densification du réseau par le biais de la solution 5G de base. La complexité du réseau et sa capacité à évoluer constamment ont modifié la manière dont il est sécurisé. Les mécanismes de sécurité traditionnels mettant en œuvre le contrôle d'accès (par exemple, les pare-feu IP/TCP ou de niveau application), bien que nécessaires, devraient devenir insuffisants pour répondre aux exigences de sécurité de la 5G. Les deux principaux outi,ls pour les réseaux 5G sont les réseaux définis par logiciel (SDN) et la virtualisation des fonctions réseau. Si ces technologies offrent certains avantages en matière de gestion et de programmabilité des réseaux, elles ouvrent la porte à de nouveaux problèmes de sécurité. Par exemple, l'exploitation de réseaux radio en nuage (C-RAN) dans le contexte d'un environnement virtualisé partagé entre différents locataires peut constituer un risque potentiel menant à d'innombrables attaques; cet environnement tend donc à être indigne de confiance. Dans cette ligne de référence, cette thèse vise à déployer de nouvelles approches pour prévenir, détecter et atténuer les menaces de sécurité sur les réseaux sans fil définis par logiciel 5G.

À cette fin, le deuxième chapitre de cette thèse conçoit et évalue une approche multicouche qui amalgame les informations de la couche physique (non cryptographique) en conjonction avec des procédures cryptographiques pour fournir simultanément une haute sécurité et une faible latence. En outre, un algorithme AES (Advanced Encryption Standard) est utilisé conjointement avec l'ensemble de données RSS (Radio Signal Strength) pour créer le protocole d'authentification.

Dans le troisième chapitre, un réseau IoT à faible puissance défini par logiciel pour prévenir les attaques de Rank est présenté. L'application d'un agent de renforcement et d'apprentissage utilisant la méthode SARSA (State Action Reward State Action) est utilisée pour aider et compléter un contrôleur SDN afin de réaliser une optimisation de route rentable et un routage de paquets avec provisionnement de la QoS pour prévenir les attaques de Rank.

Le quatrième chapitre présente une évaluation des performances dans laquelle des algorithmes de renforcement et d'apprentissage sans modèle sont utilisés pour aider le contrôleur SDN à obtenir une solution rentable pour prévenir les effets néfastes de l'attaque du Rank. Résultats expérimentaux démontrent que SARSA est plus efficace que l'algorithme d'apprentissage Q-learning, facilitant la mise en œuvre de systèmes de prévention des intrusions dans 6LowPAN défini par logiciel.

Le cinquième chapitre donne un aperçu des problèmes de sécurité dans le SD6LoWPAN, en tenant compte de ses ressources, de sa topologie et de son trafic. En outre, une étude est présentée sur les solutions de sécurité basées sur le SDN et l'intelligence artificielle qui sont suggérées dans la littérature. Les défis et les tendances de la recherche en matière de sécurité sont également mis en avant. En conclusion, une analyse des performances d'une solution de l'intelligence artificielle basée sur le SDN est présentée.

Le sixième chapitre traite des problèmes de sécurité qui prévalent dans le plan de données SDN. Dans ce sens, le travail se concentre sur l'authentification de haute précision et la détection d'anomalies dans le plan de données SDN non fiable et limité en ressources. À cette fin, un cadre de sécurité hiérarchique est proposé. Ce travail fusionne l'authentification légère avec un système collaboratif de détection des anomalies.

Mots-clés: 5G, SDN, NFV, C-RAN, Wireless Networks

Security Framework for Software Defined Wireless Networks

Christian MIRANDA

ABSTRACT

The fifth generation (5G) of wireless networks are very complex infrastructures due to their new services and the augmentation of the density of connected devices. The 3rd Generation Partnership Project (3GPP) standardization body continuously promotes best practices, control, and data handling processes within such infrastructures. Many business models have also encouraged the proliferation and expansion of device connectivity and network densification through the 5G core solution. The complexity of the network and its ability to evolve constantly influence the security approaches considered. Although necessary, traditional security mechanisms implementing access control (e.g., IP/TCP or application-level firewalls) cannot solely fulfill the security requirements of 5G. Two major enablers in 5G networks are Software Defined Networks (SDNs) and Network Function Virtualization (NFV). Although these technologies offer some advantages concerning network management and programmability, they open the door to new security issues. As such, running Cloud Radio Access Networks (C-RANs) in the context of a virtualized environment shared among different tenants can be a potential risk leading to numerous attacks; therefore, this environment tends to be untrusted. In this line of reference, this thesis targets deploying novel security solutions for the authentication, prevention, detection, and mitigation for 5G software-defined wireless networks.

Keywords: 5G, SDN, NFV, C-RAN, Wireless Networks

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF ABBREVIATIONS

1G	First Generation
2G	Second Generation
3DES	Triple Data Encryption Standard
3G	Third Generation
3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
AAA	Authentication, authorization, and accounting
AKA	Authentication and key agreement
AES	Advanced Encryption Standard
BBU	Baseband Unit
DES	Data Encryption Standard
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
HetNet	Heterogeneous Network
IoT	Internet of Things
IP	Internet Protocol
LLDP	Link Layer Discovery Protocol
LTE	Long-Term Evolution

MIMO	Multiple-Input Multiple-Output
MME	Mobility Management Entity
mmWave	Millimeter Wave
SIM	Subscriber Identity Module
SSL	Secure Socket layer
TLS	Transport Layer Security
TSP	Telecommunications service provider
VoIP	Voice over Internet Protocol
VoLTE	Voice over Long Term Evolution

LIST OF SYMBOLS AND UNITS OF MEASUREMENTS

c_{s_j}	The CPU capacity rate of the fog slice s_j
W_j	The total bandwidth of the RRH j
L_{s_j}	The average value of the load of the fog slice s_j
$r_j(\chi)$	The capacity of the IoT device (data rate)
$\Omega_j(\chi)$	average traffic load density of the location χ
ρ_j	The average traffic load of RRH j
$\nu_j(\chi)$	The average delivery time of the IoT workload from location χ
$\varrho(\chi)$	The ECT for each data flow from location χ
$\mu_j(\chi)$	The latency delay defined in RRH j
$\Omega_{s_j}{}'(\chi)$	The average computing load density of the BBU task from location χ in fog slice s_j
$\rho_{s_j}{}'$	The computation load of the fog slice s_j
$\varrho'(\chi)$	The ECT of the BBU task from location χ in fog slice s_j
$L_{s_j}(\chi)$	The average waiting time of the BBU task from location χ in fog slice s_j
$\mu_{s_j}{}'$	The computing delay of fog slice s_j
$P^k_{B_x,s_j}$(t)	The transition probability value at time t
h_{B_x,s_j}	The heuristic function
F_{B_x,s_j}	The pheromone indicator
α	The information heuristic factor
β	The expected heuristic factor

$\vec{\mathbf{S}}$	Represents the vector of cluster heads' identification
$\vec{\mathbf{C}}^u$	Represents the vector of cluster members' identification
$\vec{\mathbf{Z}}^u$	Is the vector of cluster members' identification whose snapshot is not collected by the sink at timeout
$\vec{\mathbf{R}}^u$	Is the watermarked data
M_{red}	Is a request message from the sink node to the i^{th} cluster members
$M^u_{white,i}$	Is a response message from the i^{th} cluster members to the sink
t_w	Illustrates the timeout for generating a new snapshot message at the sink node
W^u	Is a random position used to select the most significant bits (MSB) at the u^{th} cluster head
v^u	Is a value used to control the proportion of the marked data at the u^{th} cluster head
α^u	Is a value used to calculate the embedded location of the marked data at the u^{th} cluster head

INTRODUCTION

According to (Cisco), mobile data traffic is expected to expand at a compound annual rate of 57% until 2020. Hence, the available capacities provided by the fourth generation (4G) infrastructure will be exhausted (Rost, Banchs, Berberana, Breitbach, Doll, Droste, Mannweiler, Puente, Samdanis & Sayadi, 2016). To address this challenge, a new generation of mobile networks has emerged.

Since their conception, mobile communications systems have been vulnerable to security threats. In the first generation (1G), mobile networks had several limitations, such as the lack of support for encryption. They induced security threats to mobile terminals and channels, such as cloning and masquerading attacks. Later, in the second generation of mobile networks (2G), weaknesses in cryptographic algorithms led to an increase in both common attacks and the injection of fake data or the dissemination of unwanted traffic. Then, the third generation of mobile networks (3G) brought with it many vulnerabilities, such as unauthorized access to sensitive data. For example, in 3G, the International Mobile Subscriber Identity (IMSI) is sent in clear text when the user assigns the Temporary Mobile Subscriber Identity (TMSI). With the increased need for IP-based communication, the fourth generation of mobile networks (4G) enabled the proliferation of mobile terminals and channels, such as prominent cloning and masquerading attacks, which brought common IP-based attacks (Miki, Ohya, Yoshino & Umeda, 2005).

The fifth generation of mobile communications (5G) poses specific requirements such as ultra-low latency, network densification, ultra-low power consumption, and network virtualization, as shown in Fig. (0.1). Therefore, to address these requirements, introducing intelligence and quality of services can provide cost-effective solutions. Also, the deployment of emerging technologies, such as cloud computing, Software-Defined Wireless Networks (SDWNs), and network functions virtualization (NFV), have been proposed as promising solutions.

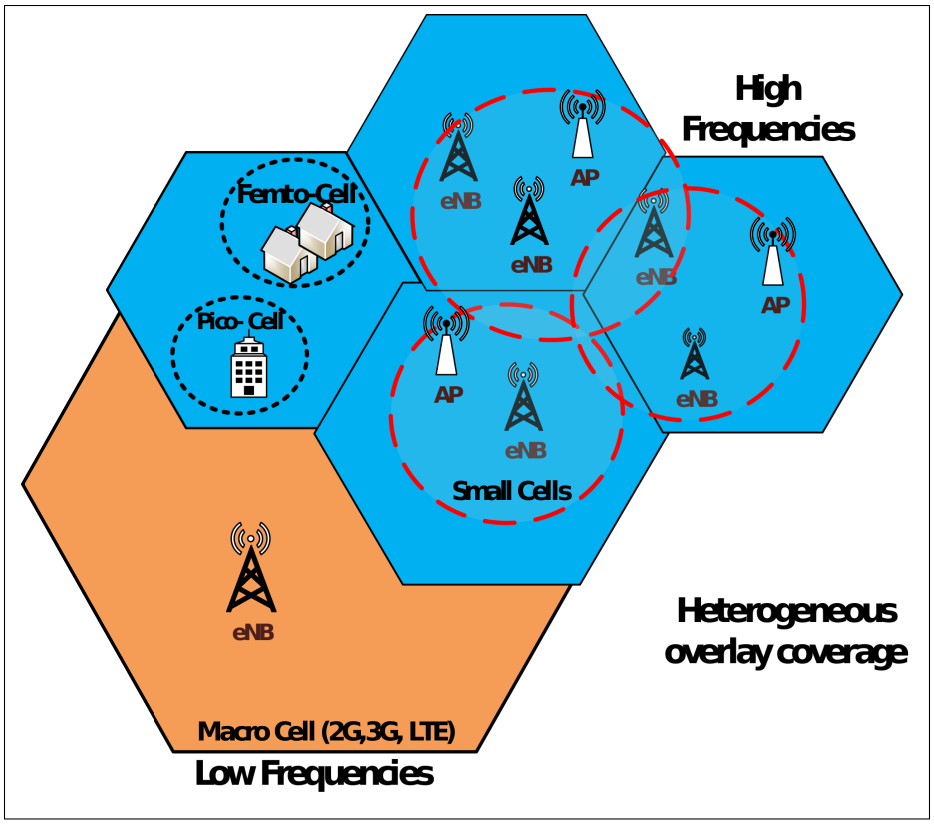


Figure 0.1 5G HetNet structure with densified small cells and overlay coverage

In particular, cloud computing provides efficient communication where service providers can handle large volumes of data, applications and services without significant investments in physical infrastructure. Consequently, mobile clouds will bring together technologically different systems into a single domain where multiple services can be deployed to achieve a higher degree of flexibility and availability with a significant decrease in Capital Expenditure (CapEx) and Operating Expenditure (OpEx) (Ahmad, Kumar, Liyanage, Okwuibe, Ylianttila & Gurtov, 2017).

The introduction of intelligence in 5G Heterogeneous Network (HetNet) deployments and Cloud Radio Access Networks (C-RANs) has been investigated in (Peng, Li, Zhao & Wang, 2015a). Moreover, Software-Defined Networks (SDNs) enable network function virtualization

by separating the network administration from the hardware plane. Also, SDNs facilitate the network configuration through abstraction (Akyildiz, Wang & Lin, 2015b). Further, NFV offers many advantages, such as independent vendor platforms, scalability and flexibility, performance improvement, and shorter development cycles (Hawilo, Shami, Mirahmadi & Asal, 2014).

Additionally, the multi-tenancy model and virtualized resources in these promising enablers have introduced new security threats that require novel techniques to guarantee data integrity and protection in the presence of malicious actors (Sabahi, 2011).

Some preliminary work has been proposed in state-of-the-art to address these challenges. For instance, a cross-layer architecture combining C-RAN with SDN characteristics is presented in (Martini, Paganelli, Cappanera, Turchi & Castoldi, 2015) to formulate the problem of composing and computing virtual networking functions to select nodes at the edge to minimize the overall latency (i.e., network and processing latency) in heterogeneous 5G infrastructure. In (Akyildiz, Wang & Lin, 2015a), the integration of SDN in a 5G network by considering cloudification and virtualization of networks is proposed. In addition, to consider SDN as a deployment medium within radio networks, the research community proposed to use SDN for security frameworks, specifically for ubiquitous IoT and sensor applications at the edge of radio networks. In (Sahoo, Sahoo & Panda, 2015), the authors proposed an architecture for IoT networks based on SDN. The architecture implements an SDN controller, who plays the role of blocking unauthenticated devices.

Moreover, in (Gonzalez, Charfadine, Flauzac & Nolot, 2016), a dynamic firewall, namely Distributed Smart Firewall (DISFIRE), is implemented within a grid network, where multiple SDN controllers are deployed in a hierarchical architecture. In the context of smart cities, in (Chakrabarty & Engels, 2016), the authors propose a secure architecture that relies on SDN controllers taking the Trusted Third Party (TTP) role. Furthermore, a software-defined wireless network (SDWN)-enabled fast cross-authentication scheme that combines non-cryptographic

and cryptographic algorithms to address the challenges of latency and weak security (Moreira, Kaddoum & Bou-Harb, 2018a; Kaur, Garg, Kaddoum & Guizani, 2020). The novelty of this work lies in devising and evaluating a multi-layer approach that amalgamates physical layer information (i.e., non-cryptographic) in conjunction with cryptographic procedures. This thesis proposal uses SDNs to corroborate security properties within 5G wireless networks.

This research focuses on novel approaches to prevent, detect, and mitigate security threats on software-defined 5G wireless networks. In this context, we will elaborate security framework stacks using machine learning algorithms to identify anomalies and prevent potential security threats. We employ supervised, and reinforcement learning approaches to build prevention and detection mechanisms. Moreover, we design and integrate virtual security functions to mitigate security threats and anomalies in 5G wireless networks. The virtual security functions are hooked to create on-the-fly security enforcement for 5G wireless networks. Security threat mitigation tactics are part of a security policy that is proven free of anomalies and redundant objectives. In this context, the purposes of this research are presented as follows.

1. Identification of security weaknesses in 5G wireless networks, a literature review will be analyzed, including the study of analytics within 5G wireless networks.
2. Deployment of machine learning algorithms to detect security threats and anomalies.
3. Comparison of machine learning algorithms regarding the accuracy, processing, and data collection method.
4. Introduction of a security framework to prevent, detect, and mitigate attacks.

These objectives aim to derive a consistent methodology from building prevention, detection, and mitigation systems to secure 5G wireless network deployments. Hence, the methodology used for this thesis is presented as follows

- Survey of state of the art: Relevant attacks and security threat models for 5G wireless network deployments will be surveyed to define the scope of the security study to propose a security framework stack for intrusion detection and mitigation systems.
- Security threat model in 5G wireless networks based on SDN architecture: Mitigation techniques will be analyzed to address security threats. In this context, using virtual security functions based on SDN architecture is vital in improving security and performance in 5G wireless network deployments.
- Proof of concepts and integration to showcase the feasibility of the proposed security mechanisms and academic results dissemination through scientific articles.

In addition, this research work will use data from 5G wireless networks to create intelligent algorithms to detect malicious attacks. We will use network traces generated from simulations and traces collected from 5G testbeds. We will also consider using machine learning prediction techniques to identify malicious attacks and big data analytics to frame the analysis of the significant number of logs observed in virtual radio deployments. The research roadmap is presented as follows:

1. The definition of a cross-layer authentication scheme combines non-cryptographic and cryptographic algorithms to address the challenges of latency and weak security.
2. The deployment of an intrusion prevention scheme using State Action Reward State Action (SARSA) to assist and complement an SDN controller in achieving cost-efficient route optimization and quality of service provisioning packet forwarding to prevent rank attacks in Software-Defined Low Power IoT Networks.
3. The introduction of a performance evaluation where model-free Reinforcement-Learning [RL] algorithms are leveraged to help the SDN controller achieve a cost-efficient solution to prevent rank attack harmful effects.
4. The introduction of an overview of security issues in SD6LoWPAN, considering its resource, topology, and traffic. In addition, a study of the SDN- and ML-based security solutions

that are suggested in the literature is presented. Security research challenges and trends are also put forward. In conclusion, a performance analysis of an SDN-based ML solution is presented.

5. The implementation of an SDN-based collaborative security framework hierarchically that combines three security layers. At the bottom of this approach (Layer L1), an IPS-based authentication process is designed to provide a lightweight security scheme in the data plane. In the middle of the framework (Layer L2), an IDS-enabled energy prediction model within the edge is designed to supply a cost-effective intrusion detection solution near the data plane. Finally, at the top of this framework (Layer L3), in the control plane, a Smart Monitoring System (SMS)-based SVM algorithm is introduced to achieve isolation, high performance, enhanced anomaly detection, and efficient mitigation by segregating malicious nodes over the Software-defined Wireless Sensor Networks (SDWSNs).

The dissertation is structured as shown in Fig. 0.2, and detailed as follows.

Chapter 1 presents a comprehensive literature review of 5G. It highlights the enabling technologies of 5G, such as Software Defined Networks and Network Function Virtualization, and briefly describes recent related works. Moreover, this chapter presents the most frequent security methods and approaches cited in the literature. It also analyzes the most commonly used prevention, detection, and mitigation methods, detailing their advantages and disadvantages.

Chapter 2 presents a software-defined wireless network (SDWN)-enabled fast cross-layer authentication scheme that combines non-cryptographic and cryptographic algorithms to address the challenges of high latency and robust security. Initially, the received radio signal strength vectors at the mobile terminal (MT) are used as a fingerprinting source to generate an unpredictable secret key. Subsequently, a cryptographic mechanism based on the authentication and key agreement protocols is executed to improve the confidentiality and integrity of the authentication handover. Further, with the help of the supervised KNN algorithm, a radio-trusted

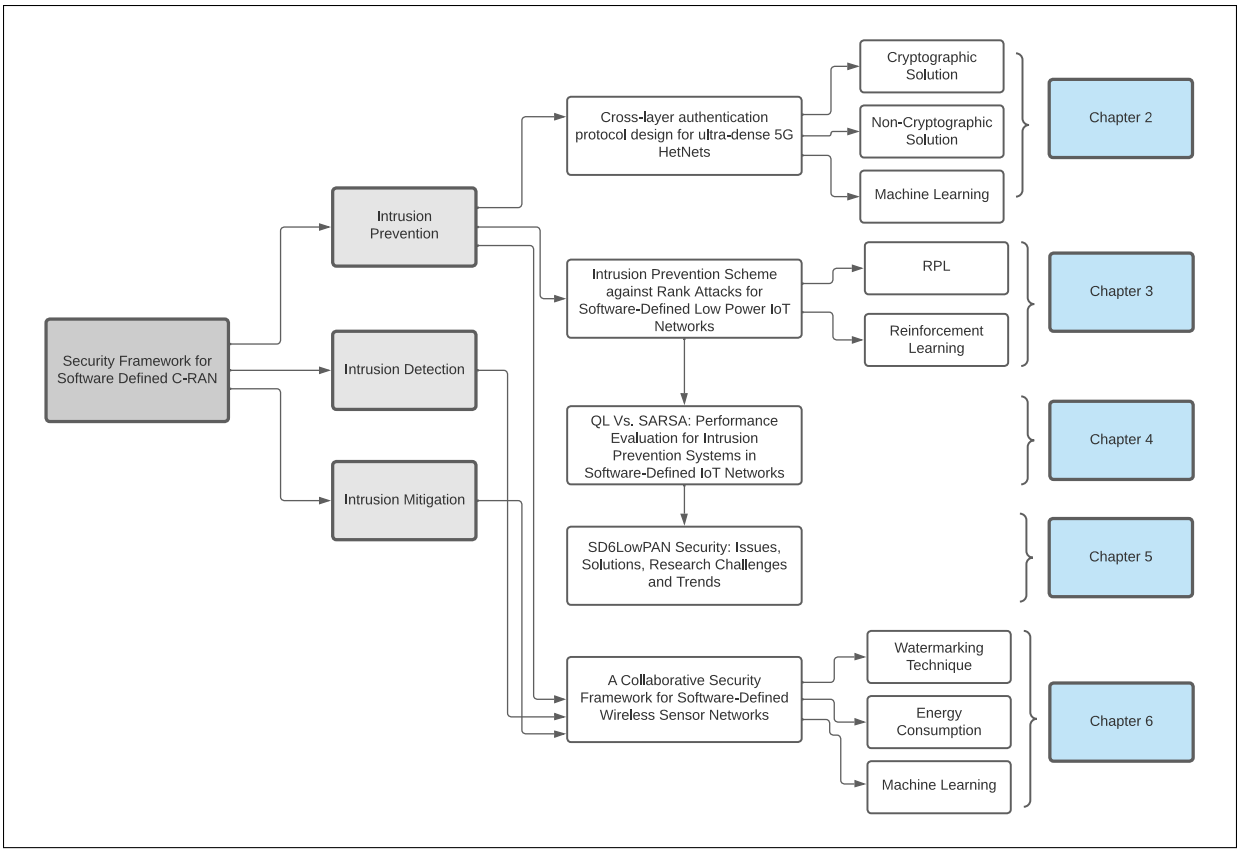


Figure 0.2 Thesis contributions

zone database is created to decrease the frequent authentication of radio devices in the network. The proposed scheme is analyzed under different scenarios.

Chapter 3 presents a Reinforcement-Learning agent to assist and complement the SDN controller in achieving cost-efficient route optimization and quality of service provisioning packet forwarding to prevent rank attacks. Experimental results confirm that this approach effectively prevents rank attacks while providing an adequate delay and radio duty cycle. Meanwhile, it maximizes the packet delivery ratio, facilitating practical implementations in software-defined Low Power Internet of Things (IoT) Networks.

Chapter 4 proposes a performance evaluation where model-free Reinforcement-Learning algorithms are leveraged to help the SDN controller achieve a cost-efficient solution to prevent

RA harmful effects. Experimental results demonstrate that the SARSA algorithm is more efficient than the Q-learning (QL) algorithm, facilitating the implementation of intrusion prevention systems (IPS) in software-defined Internet Protocol Version 6 Low Power Network (6LowPAN).

Chapter 5 provides an overview of security issues in SD6LoWPAN, considering its resource, topology, and traffic. In addition, a study of the SDN- and ML-based security solutions that are suggested in the literature is presented. Security research challenges and trends are also put forward. In conclusion, a performance analysis of an SDN-based ML solution is presented.

Chapter 6 presents an SDN-based collaborative security framework that combines Intrusion Prevention, Detection, and Smart Monitoring systems, taking advantage of energy snapshot readings, which are proposed and evaluated. Initially, a distributed snapshot algorithm and a watermarking technique are introduced to decrease latency and enhance the recurrent authentication in wireless sensor nodes. Subsequently, the security features of the proposed multilayer authentication approach are analyzed by executing automated protocol analysis using the AVISPA tool. Consequently, an IDS-enabled energy prediction model is designed at the network edge. Finally, to correlate the detection rate and reduce the false alarms that could be generated at the network edge, an SMS-based SVM algorithm is executed and tested in the control plane.

CHAPTER 1

BACKGROUND AND LITERATURE REVIEW

1.1 5G security requirements

5G HetNets are no longer restrained to offering faster mobile services for converged communication. Instead, they offer virtual services, which provide a portfolio of new features. The emerging network technologies such as software-defined networks and network functions virtualization (NFV) additionally improve the ability of 5G to support new business models to prosper. Meanwhile, these advances require complex security prerequisites. In (SIMalliance, b), 3GPP depicts the 5G security requirements that have to be addressed in different layers within the 5G HetNet architecture as follows:

- Clearer identity of the device, user, network, application, and service platform;
- Faster handling for low-latency security procedures;
- Lower complexity for authentication, confidentiality, and integrity procedures ;
- Enhanced privacy protection to protect the user identity and location;
- Seamless authentication across heterogeneous infrastructures, avoiding cryptographic services at intermediate nodes;
- Data verifiability.

Indeed, the security requirements of 5G will vary greatly depending on the application since the underlying technologies for simple sensors requiring daily probes are different from those of remote surgery that require real-time communications. According to (Ericsson), These requirements can be met by the following countermeasures:

- Novel identity management and credentials;
- Optimization of low-latency mobile security;
- Efficiency of cloud security;
- Design of flexible and scalable security architectures;
- Implementation of energy-efficient security.

1.1.1 Novel identity management and credentials

In legacy wireless networks, identity and key management depend on SIM cards. In 5G, compatible hardware, such as sensors and IoT devices, will be too small or cheap to host a SIM card. Therefore, it is essential to establish a novel method to produce, allocate and enforce lifecycle management over device identities. The authors in (Ericsson) propose two identity management mechanisms as follows:

- Combination of device identity and service identity: The novel identity management framework separates the service identity from the device identity. The physical device identity is unique and can be assigned during manufacturing. Hence, service identities are assigned by network service providers, where one or more service identities may correspond to one physical identity.
- From device-based management to user-based management: This allows the user to choose which device has allowed access to the network and what services may run on it. For example, devices of the same user may share bandwidth quotas online or offline.

1.1.2 Optimization of low-latency mobile security

The emergence of critical applications, such as vehicular ad hoc networks (VANETs) and sensor networks, has led to communication scenarios characterized by low latency and high-security requirements. In such systems, the 5G wireless network needs to maintain high reliability and quality of services to satisfy extremely low delays in traffic transmission, which is essential to prevent potential accidents such as vehicle collisions or surgical errors (Illy, Kaddoum, Moreira, Kaur & Garg, 2019; Illy, Kaddoum, de Araujo-Filho, Kaur & Garg, 2022b; De Araujo-Filho, Pinheiro, Kaddoum, Campelo & Soares, 2021; de Araujo-Filho, Kaddoum, Naili, Fapi & Zhu, 2022).

In addition, with ultra-dense technologies deployed in 5G, mobility management procedures may frequently occur when mobile terminals are moving. Considering the low latency requirement,

optimizing mobility management functional entities and processes has become a critical factor in 5G.

To address these challenges, wireless security must be redesigned and optimized to build an agile and simplified mobility management mechanism that supports the stringent low-latency requirements of emerging technologies. Similarly, networks must be transformed to deliver faster speeds, lower latency, and more capacity to facilitate the network traffic of billions of connected nodes and the next wave of new compute-intensive 5G applications. Cloud computing is poised to deliver 10x lower latency, 100x faster speeds, and 1000x more capacity than 5G, providing the foundation for breakthrough customer experiences, business efficiencies and revolutionary products and services.

1.1.3 Efficiency of cloud security

Cloud computing is a set of services provided to users over a dynamic network. Typically, cloud computing services are provided by an external provider that usually owns the infrastructure. In addition, a cloud provider can offer certain features, such as scalability, resiliency, flexibility, reliability, efficiency and outsourcing of non-core activities. Despite the potential improvements achieved by cloud computing to provide scalability to 5G wireless networks, cloud security must address its associated security requirements, such as:

- Design hypervisors and virtual network functions with high assertiveness on isolation;
- Build desirable ecosystems and architectures from existing trusted infrastructures and concepts for remote certification;
- Deploy more efficient cryptography solutions for the cloud-friendly environment;
- Create intuitive and trusted management for cloud systems.

To meet these requirements, wireless security must be redesigned and optimized to build an optimized mobility management mechanism that is flexible, simplified and compatible with the strict requirement of low latency.

1.1.4 Design of flexible and scalable security architecture

The emerging virtualization of network functions brings dynamic configurations to 5G. Therefore, it is crucial and essential to consider a more flexible and scalable security architecture for this. For example, synchronization in a telecom environment, such as radio signaling, could be designed at the network edge. These enhancements can achieve more effective security management while limiting threats to sensitive user data.

1.1.5 Improvement of energy-efficient security

Although security services, such as cryptographic solutions and essential management procedures, come with a high energy cost, the expense is no longer an issue for mobile services and devices (Asif & Muneer, 2007). The energy cost of encrypting one bit is two times lower than the cost of transmitting it. However, battery lifetime plays a fundamental role in performance for resource-constrained devices like sensors. Hence, there is a necessity to consider even more energy-efficient solutions.

The 5G wireless network architecture depends on the SDN architecture, as shown in Figure 1.1, which minimizes the technological gap between legacy IP and telecommunications networks. Accordingly, SDWNs are vulnerable to most attacks in general SDN networks. Nonetheless, this chapter includes an overview of the SDN architecture, expected security challenges, and related security attacks and solutions.

1.2 SDWN architecture

SDWN is an emerging technology resulting from separating the control plane from the data plane. It is composed of the following layers:

- Application layer: The application layer consists of end-user and business applications. In this context, legacy wireless network control devices, such as the Home Subscriber Server (HSS), the Policy and Charging Rules Function (PCRF), the Mobility Management Entity

(MME), and the Authentication Authorization and Accounting (AAA) are applications run on the highest layer of the SDN infrastructure (Yoon, Lee, Kang, Park, Shin, Yegneswaran, Porras & Gu, 2017). The northbound interface traverses the borderline between the application and control layers.

- Control layer: The control layer comprises centralized management controllers. The open application interface (API) empowers open switch information forwarding functions that are aware of the state collection and centralized control of the data layer (Liyanage, Ylianttila & Gurtov, 2014a). The control channel manages the communication between the controller and the data layer. This channel is implemented using control protocols, such as the OpenFlow (OF) protocol, the standard used control protocol in the SDN domain.

- Data layer: The data layer, also known as the infrastructure layer, primarily consists of a data forwarding process, which includes physical and virtual hardware and mobile terminals for exchanging and forwarding data packets (Liyanage *et al.*, 2014a). The user's data traffic is transported through the data plane. This communication channel is called the data channel.

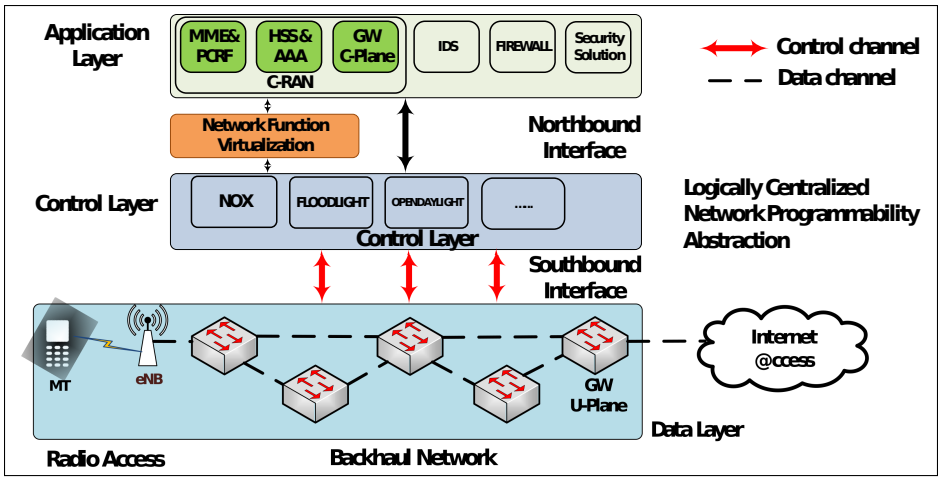


Figure 1.1 SDN functional Architecture

In addition, SDN integrates new paradigms such as NFV and OF protocol described as follows:

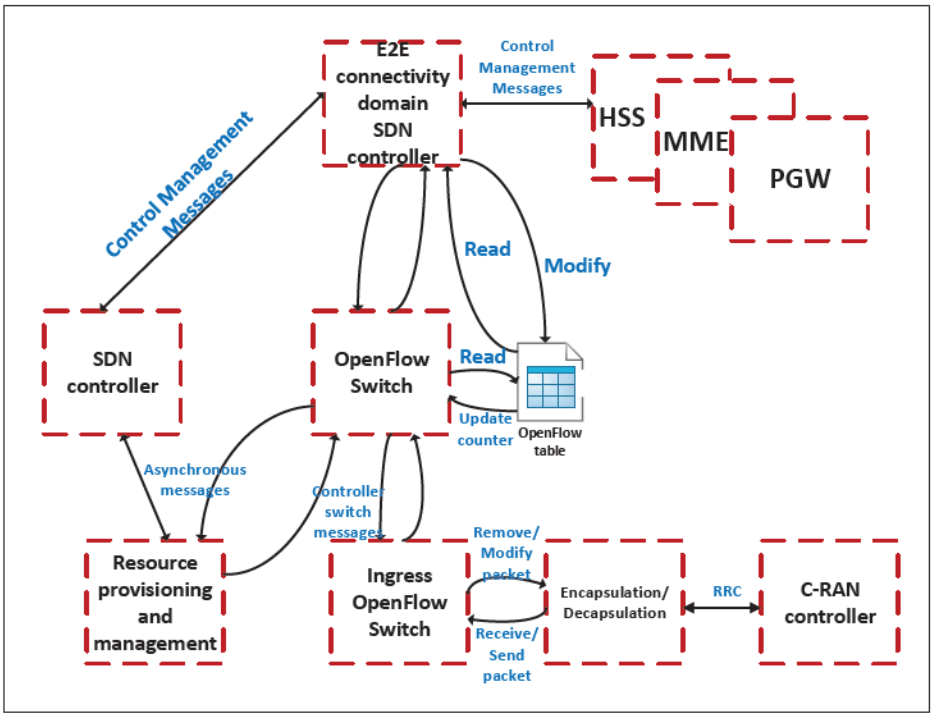


Figure 1.2 OpenFlow architecture

- OpenFlow: This is an open protocol used for communication between the network switch, commonly called the data plane, and the control plane. According to (Kloti, Kotronis & Smith, 2013b), the switch performs packet forwarding using one or more OpenFlow tables. These tables contain rules, header patterns, actions, and counters.

  The control plane installs the flow rules on the network switch. The controller can choose to install them proactively on its own accord or reactively in response to a notification sent by the switch regarding a packet failing to match existing rules.

  Given the novel features of SDWN, particularly OpenFlow, to transmute how networks are communicated, it is essential to consider the security implications of the OpenFlow protocol. Following the OpenFlow threat model described in (Kloti, Kotronis & Smith, 2013a), Fig. 1.2 shows the OpenFlow process and simplified data flow diagrams in the SDWN architecture.

- NFV: According to (Mijumbi, Serrat, Gorricho, Bouten, De Turck & Boutaba, 2016), the most important principle of NFV is decoupling the physical network devices from the functions that run on them. Accordingly, there is no need for new hardware to install new

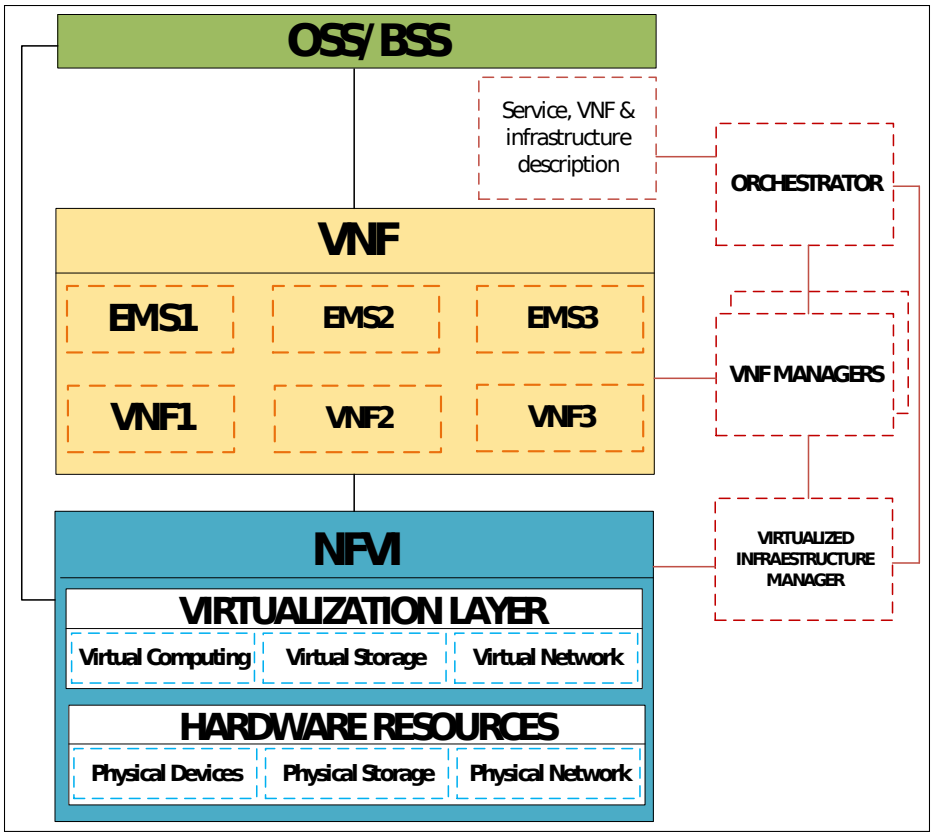


Figure 1.3 Diagram of the NFV architecture

network functions or business applications. For instance, a mobile service provider can execute software-based network functions in a specific format of virtual resources such as virtual machines or containers.

This network paradigm certainly allows the deployment of network functions, considering the consolidation of various network devices situated in reliable data centers, distributed network nodes, and end-user infrastructures. In this context, a given network service can be decomposed into a set of virtual network functions (VNFs), which could then be implemented in software running on one or more classical physical devices .

In (ETSI), the NFV-based LTE architecture with a reduced graph of NFV members is presented. The authors define an NFV as a promising approach enabling easy and fast

network function deployment in figure 1.3. In contrast to traditional network infrastructures, it delivers the following promises:

- Cost reduction of ownership by moving network functions from physical devices in virtual machines;
- Agile and cost-efficient deployment of network functions;
- Reduced energy consumption.

In contrast to common presumptions, NFV does not rely on software-defined networking (SDN). It can be implemented independently. SDN and NFV are complementary and bring significant advantages when used together. The key architectural components of NFV are the virtual infrastructure manager (VIM) and the hypervisor, which is the main element of the VIM. The flexible and scalable nature of NFV decreases the incident time response, provides better resiliency against distributed denial of service (DDoS) attacks, and enables on-demand security services, such as firewalls and intrusion detection and prevention systems (IDS/IPS), to block or reroute malicious traffic (Illy, Kaddoum, Kaur & Garg, 2022c; Rathee, Garg, Kaddoum, Choi, Hassan & AlQahtani, 2022; Babbar, Rani, Garg, Kaddoum, Piran & Hossain, 2021). In addition, security in NFV brings up important issues related to its adaptability in the underlying telecommunication infrastructure. Consequently, the hypervisor is susceptible to various security attacks, such as manipulating VM operative systems and data destruction. Moreover, other vulnerabilities can emerge when the hypervisor is hijacked. NFV dispatch software allows automated provisioning of network functions; however, this feature could be an open door for security weaknesses, such as malicious configuration, automatic network configuration, orchestration, and SDN controller vulnerabilities (Garg, Kaur, Kaddoum, Garigipati & Aujla, 2021; Rathee, Garg, Kaddoum & Choi, 2020; Illy, Kaddoum, de Araujo-Filho, Kaur & Garg, 2022a).

In (Hong, Xu, Wang & Gu, 2015), the authors discussed the probability of a topological poisoning attack, in which the visibility of the network, the OpenFlow controller, and network functions can be breached, leading to serious hijacking, denial-of-service, and man-in-the-middle attacks.

Furthermore, in (Hong *et al.*, 2015), the authors mention that decoy attacks can target the IP protocol address of the SDN controller, where the attacker intercepts OpenFlow traffic to prevent it from adequately reaching the network switch. As a result, the spoofed SDN controller can cause the spoofed traffic to bypass the policy charging rules function (PCRF), causing resource exhaustion and generating a distributed denial of service (DDoS) attack that leads to network performance degradation. In addition, the infected OpenFlow node can manipulate the counter and insert fake traffic into users, bypassing the charging system and adopting incorrect traffic costs.

According to (Shin & Gu, 2013), another information disclosure attack exists in which the network fingerprint and data controller may be disclosed due to an external XML mechanism attack. One of the most dangerous threats is the Distributed Denial of Service (DDoS) attack, resulting in the exhaustion of resources, SDN controller overload, and OpenFlow switches disconnection, as shown in (Kloti *et al.*, 2013a; Hong *et al.*, 2015; Shin & Gu, 2013; Shin, Song, Lee, Lee, Chung, Porras, Yegneswaran, Noh & Kang, 2014). In general, some research works indicate that the main security concerns in 5G are related to the SDWN. (Schehlmann, Abt & Baier, 2014).

1.3 SDWN security challenges

The prevailing security challenges are inherited from the SDN architecture due to the following:

- Centralized management: Since the network configuration, network service access control, and network service deployment are integrated into the centralized management at the control layer, an attacker can compromise the SDWN successfully, which might cause the interruption of network services and thus affect the whole network.
- Network programmability: SDWN network programmability has brought up new security concerns such as:
    - Additional interactions to handle various service level agreements and privacy issues arising from device and traffic isolation.

- Programmability could bring the convenience of automation, flexibility, and the exposition of various security threats. Consequently, it is necessary to strengthen the authentication algorithms in communication channels and virtual applications, to prevent the controller from exposure.
- Protection of the application-controller plane interface (A-CPI) and intermediate-controller plane interface (I-CPI). These SDN interfaces must support robust security components, especially when they cross domain boundaries.

- The deployment of SDN requires an infrastructure connected with different domains. Hence, it involves establishing authentication procedures to guarantee a secure channel configuration.
- The integration with the existing protocols must be ensured to SDNs. Meanwhile, in the construction of the SDN architecture, the ability to increase or decrease performance and cost in response to changes in application and system processing demands must be considered.

1.3.1 SDWN security attacks

The software-defined wireless network concept was proposed by (Kreutz, Ramos & Verissimo, 2013) as an extension of the SDN paradigm to integrate specific wireless network functionalities; Revoltingly, SDWN is vulnerable to security attacks that can arise at different sections of the wireless network. Security threats can be divided into Software-Defined Fronthaul (SDF) and Backhaul (SDB) networks.

As for wireless SDF applications, SDWN threats are inherited from physical layer threats surface attacks (Marinho, Granjal & Monteiro, 2015; Yoon *et al.*, 2017). On the other hand, security threats in SDB can be divided into four vectors, as follows:

- Application layer security;
- Control layer security;
- Data layer security;
- Communication channel security.

The security threats in communication channels are divided into security attacks over control channels and security attacks over the data layer. The scope of this research is limited to the security attacks in the data layer and the communication channel, as detailed in the following section.

1.3.1.1 Security attacks over control channels

The network controller is the critical component of the SDWN architecture due to its centralized intelligence and management capabilities; consequently, it is the target of the most common IP attacks. The absence of IP-level security is the main threat to control channel security. Current SDN control channels are based on higher-layer security mechanisms like TLS and the SSL (secure socket layer) communication protocol.

However, SSL and TSL are vulnerable to several IP-based attacks, such as Rivest Cipher 4 (RC4), Browser Exploit Against SSL/TLS (BEAST), Compression Ratio Info-leak Made Easy (CRIME), and Padding Oracle On Downgraded Legacy Encryption (POODLE) attacks (Liyanage *et al.*, 2014a). Consequentially, protection protocols from higher layers must be stronger to dispense a proper level of security and resiliency for the control channel.

In addition, in the control layer, the security level depends on various factors such as self-signed certificates (SSC), certificate authority (CA), and security protocols. Therefore, strong authentication between the control and data planes is necessary.

Further, the TLS/SSL protocols are insufficient to perform a robust authentication procedure between the control plane and the data plane; an attacker can inject fake flow requests to inundate the controller's resources and overload the flow tables in switches, performing DoS attacks.

Consequently, some researchers mention in (Meyer & Schwenk, 2013) that TLS/SSL authentication mechanisms are vulnerable to IP spoofing and CRIME attacks.

Table 1.1 Known attacks on control channel

Attack Type	Description	Impact
RC4 attack	The synchronization process enables this attack when it is continuously encrypting since the attacker can obtain the data in clear text.	Important information is extracted to perform future attacks and reveal the identity of network devices.
BEAST attack	The attacker mounts a plain-text attack with vectors available in the network using cipher block chaining.	Important information is extracted to perform future attacks and reveal the identity of network devices.
CRIME attack	During the authentication process, an attacker can catch session tokens to perform session hijacking.	Overload controller resources by adding or manipulating fake flow requests.
POODLE attack	The attacker downgrades TLS sessions to SSL3.0 sessions and uses design flaws in SSL 3.0 that allow changing padding data at the end of a block cipher. As a result, the encryption cipher becomes less secure each time it is passed.	Abnormal termination of the communication between the control and data layers.
DDoS	A set of attackers sends a succession of TCP Synchronization (SYN) requests to consume server resources and make the controller and DPSs unresponsive to legitimate traffic.	Overload of ternary content addressable memory (TCAM) of the data layer.
TCP reset attack	The attacker injects a sequence of TCP reset requests to reset the communication session prematurely.	Abnormal termination and service quality collapse of communication channels.
LUCKY 13 attack	The attacker performs a man-in-the-middle attack to recover the plain text from a CBC (Cipher-block chaining) encrypted TLS session.	Important information is extracted, which can be used to perform future attacks and reveal the identity of network devices.

1.3.1.2 Security attacks over the data channel

In IP-based telecommunications networks such as SDWN, the radio network layer (RNL) encryption terminates at the base station. Therefore, the data layer traffic is not encrypted. Thus, the data channel is vulnerable to eavesdropping, reestablishment, denial of service, and man-in-the-middle attacks. During an eavesdropping attack, the attacker can sniff the switch network to collect flow table information to observe traffic patterns. Consequently, the information gathered can be used to perform DoS attacks.

Nevertheless, the data channel in SDWN does not have defense mechanisms against data alteration attacks. For instance, a man-in-the-middle attacker can modify or destroy data without

Table 1.2 Known attacks on data channel

Attack Type	Description	Impact
Spoofing attacks	DoS attack is performed because an attacker may impersonate a legitimate Deposit Protection Security (DPS).	The traffic flows are transferred to the wrong destination.
Eavesdropping attacks	IP parameters and flow data are stolen by an attacker.	DoS, reset, spoofing, and flow modification attacks are performed.
DoS/DDoS attacks	The attacker exhausts the Ternary Content-Addressable Memory (TCAM) of switches.	Decreases or eliminates the availability of the DPS.
Message modification attacks	The attacker modifies flow tables with fake rules.	Exhausts memory in DPS and reduces QoS of user services
Replay attacks	An attacker intercepts legitimate signaling traffic and overloads the network by retransmitting it continuously.	Jeopardizes the data plane by destroying the in-flight flow rules.
Reset attacks	The attacker inserts a sequence of TCP reset requests to reset the communication session prematurely	Terminates the ongoing communication sessions between DPS devices

knowing the network provider. Accordingly, excessive flow entries may be stored in data layer switches; thus, overloading the controller due to the unreasonable flow requests forwarded to it; hence, decreasing the quality of service (QoS) of communication sessions. Moreover, the data plane also needs robust mutual authentication mechanisms in the control plane. Intruders can impersonate a legitimate switch without such authentication mechanisms and inject fake traffic flows to the data plane (Scott-Hayward, O'Callaghan & Sezer, 2013). In this vein, the attacker can deplete the flow tables of the data plane switch and downgrade the available bandwidth for data traffic. Moreover, the controller may also be affected by forwarding unnecessary flow requests. Common attacks on data channels, as summarized below (Liyanage, Braeken, Jurcut, Ylianttila & Gurtov, 2017; Yoon *et al.*, 2017).

Table 1.3 SDWN features and mitigation mechanisms

SDN feature	SDWN mitigation mechanism
Centralized control mode	Different security mechanisms have centralized security policy management and coordination. Authentication procedures and all security mechanisms are managed by the centralized controller.
Dynamic and flexible adjustment	Dynamically adjust the security mechanisms to satisfy varying traffic demands.
Scalability and flexibility	Common security mechanisms can be applied to any section of the network. Security mechanisms are decoupled from infrastructure devices and implemented in cloud-based resources. Security mechanisms use and share cloud-based resources.
Virtualized environment	Common security mechanisms are implemented over multiple access technologies and operators. Eliminates vendor-specific security mechanisms.
Decision-making procedures	Common monitoring tools and machine learning procedures can be used to monitor every section of the network. Network-monitoring resources are scaled to match traffic demand without changing the physical infrastructure.
Abstraction	Security mechanisms are not coupled to a specific section of the network. Security mechanisms are independent of the infrastructure. Complex network access technologies and protocols to security applications are hidden.
Granular policy management	Security policies are applied at more granular levels, such as user, application, or session.
Network programmability	Software applications allow rapid and efficient changes in the security mechanisms. Security mechanisms are modified quickly according to traffic demands.
Dynamic attack mitigation	Fast deployment of new security mechanisms to prevent and identify new attacks. Efficient forensics with holistic network informatics prevent future attacks.
Flow paradigm	Flow labels isolation.
Energy efficiency	It will be possible to make better use of sleep mode and achieve more power savings while avoiding DoS attacks.

1.3.1.3 Security solutions over communication channels

To prevent security threats from compromising the SDWN, real-time monitoring and decision-making features are imprescriptible for a suitable security scheme for 5G communication channels.

To secure the communication channels in current telecommunication networks, IPsec is the most commonly used security protocol (Bikos & Sklavos, 2013). Correspondingly it is possible to use IPsec with slight modifications to secure communication channels towards 5G as is presented in (Meyer & Schwenk, 2013), wherein the authors propose a Host Identity Protocol (HIP)-based secure control channel for SDWN. The authors suggest the following additional features to the existing SDWN architecture.

1. Distributed Security Gateways (SecGWs) are utilized to secure the controller from external intruders and provide high availability;
2. A SEC (Security) entity is attached as a control entity to control the SecGWs;
3. A Local Security Agent (LSA) application is installed in each data layer device to handle security policies;
4. The IPsec BEET (Bounded-End-to-End-Tunnel) is used to secure the control channel.

Also, (Liyanage, Abro, Ylianttila & Gurtov, 2016) propose virtualized middleboxes that can be especially useful for implementing dynamic, flexible and manageable security mechanisms in 5G wireless networks. Table 1.3 lists possible use cases of new SDWN functions to overcome existing wireless network security challenges. On the other hand, high-level security for critical communication can be achieved by using new security mechanisms, such as authentication procedures, integrity and encryption algorithms, as mentioned in (Zhang, Janakiraman, Sim & Kumar, 2006; Xiao, 2004a; Koreman, Morris, Wu, Jassim, Sellahewa, Ehlers, Chollet, Aversano, Bredin, Garcia-Salicetti et al., 2006), and biometric-based continuous authentication as addressed in (Altinok & Turk, 2003). Furthermore, in citepB-25, the authors propose an intrusion detection solution combining IP-trace back with Enhanced Adaptive Acknowledgment (EAACK). Meanwhile, in citepB-32, intrusion detection with neural networks

and watermarking techniques is proposed. Moreover, in citepB-33, intrusion detection based on a soft margin support vector machine (SVM) is proposed. In (Liu, Yu, Lung & Tang, 2009; Bu, Yu, Liu, Mason & Tang, 2011), intrusion detection and continuous authentication for SDWN are combined. Hence, the main challenges of these security schemes are high resource consumption, high overhead and lack of coordination. Thus, the solutions discussed in this section may not be viable to address the critical requirements of 5G. Therefore, preliminary results are presented in the following chapters to address these security challenges and provide a robust framework to minimize the possibility of attacks in SDWN.

CHAPTER 2

CROSS-LAYER AUTHENTICATION PROTOCOL DESIGN FOR ULTRA-DENSE 5G HETNETS

Christian Miranda[1] , Georges Kaddoum[2] , Elias Bou-Harb[3]

[1,2,3] Département de Génie Électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Article published in IEEE International Conference on Communications, May 2018.

2.1 Abstract

Creating a secure communication environment is becoming a significantly challenging task in 5G Heterogeneous Networks (HetNets), given the stringent latency and high capacity requirements of 5G networks. This is particularly factual, knowing that the infrastructure tends to be highly diversified, especially with the continuous deployment of small cells. In fact, frequent handovers in these cells introduce unnecessarily recurring authentications leading to increased latency. In this paper, we propose a software-defined wireless network (SDWN)-enabled fast cross-authentication scheme that combines non-cryptographic and cryptographic algorithms to address the challenges of latency and weak security challenges. Initially, the received radio signal strength vectors at the mobile terminal (MT) is used as a fingerprinting source to generate an unpredictable secret key. Subsequently, a cryptographic mechanism based upon the authentication and key agreement protocol by employing the generated secret key is performed to improve the confidentiality and integrity of the authentication handover. Further, we propose a radio-trusted zone database aiming to enhance the frequent authentication of radio devices that are present in the network. To reduce recurring authentications, a given covered area is divided into trusted zones where each zone contains more than one small cell, thus permitting the MT to initiate a single authentication request per zone, even if it keeps roaming between different cells. Accordingly, once the RSS vectors and the encrypted mobile identification are received by the authentication slice (AS), this latter builds the authentication vector using the

k-nearest neighborhood technique to estimate the k^{dh} fingerprint distribution which is compared to the radio trusted zones database to prove the legitimacy of the MT and the network slice (NS). A cross-layer authentication protocol is consequently executed. The proposed scheme is analyzed under different attack scenarios and its complexity is compared with cryptographic and non-cryptographic approaches to demonstrate its security resilience and computational efficiency.

2.2 Introduction

Wireless connectivity has progressively secured its place in the last decade to be an indispensable part of our communication means that has undoubtedly increased mobile traffic load. According to (Index), mobile data traffic is expected to expand at a compound annual rate of 57% until 2019 and is predicted, by year 2020, to exhaust the available capacities provided by the fourth generation (4G) and the long term evolution (LTE) infrastructures (Wang, Haider, Gao, You, Yang, Yuan, Aggoune, Haas, Fletcher & Hepsaydir, 2014a).

In addition, network densification using low-power small cells is considered to be a core solution for 5G. This new architecture indeed demands new requirements such as flexibility in management and configuration, adaptability and vendor-independence. To meet these requirements, software defined wireless networks (SDWN) have been proposed as a cost-effective solution (Akyildiz, Wang & Lin, 2015c). Hence, the hetnet nature of 5G with the separation of data and control planes and the virtualization of major network functions increase the need for authentication improvement, integrity, and privacy protection in the presence of malicious actors (Chen, Yang, Trappe & Martin, 2010).

The traditional authentication handover mechanism is based on a cryptographic key and on multiple handshakes. The authentication and key agreement (AKA) protocol which is standardized by the third generation partnership project (3GPP) in (Deng, Fu, Xie, Zhou, Zhang & Shi, 2009b) is widely used in current wireless networks. In brief, the AKA protocol

involves three entities which are (*i*) the mobile terminal (MT) which represents the user, (*ii*) the home environment (HE) and (*iii*) the serving network (SN).

AKA allows the SN to authenticate and exchange keys with the user, without ever being given the user's key. Instead, one-time authentication vector (AV) are issued to SN by the HE. All communication and computations in AKA are very efficient thanks to the use of symmetric-key cryptography. To this end, the client authenticates the network by computing the response (RES) using its k secret key and the network authenticates back to the client across-AV by associating its response with the expected response (XRES). Using symmetric cryptography, AKA shares a k secret key with the MT and the HE in order to maintain the privacy and security of the information.

By exploring and investigating the security analysis of current authentication protocols, we pinpoint several of their vulnerabilities against different attacks including resistance attacks, black hole attacks, replay attacks, man-in-the-middle attacks, impersonation attacks, and denial of service attacks (Chen *et al.*, 2010). We also note that considerable research has been made to improve such protocol. For instance, in (Li & Wang, 2011), the authors propose a security enhanced authentication and key agreement (SE-EPS AKA) method based on wireless public key infrastructure by using the ellipse curve cipher (ECC) encryption. Additionally, the research work in (Hamandi, Sarji, Chehab, Elhajj & Kayssi, 2013) points out a scheme which resolves the privacy problem and prevents mobility management entity (MME) masquerading. Moreover, the devised scheme takes into consideration the fact that the MT is energy-limited and for that reason, public key cryptography is not used at the MT. The mechanism in (Purkhiabani & Salahi, 2011) suggests an enhanced AKA protocol using a methodology which provides zero-knowledge proof using a pre-shared key that is never sent over the transmission medium. A new key exchange procedure is proposed in (Deng *et al.*, 2009b) where the user identity information and authentication vector in the network domain are encrypted using the public key cryptosystem. The public parent key adopted in local authentication is generated by means of random data. In (Abdo, Chaouchi & Aoude, 2012), the authors show that their proposed approach eliminates the synchronization between mobile station and its home network in the key exchange process.

Besides the discussed vulnerabilities, the conventional AKA authentication protocol may not fulfill the requirements of future dense small 5G network cells in terms of security, resistance to spoofing, low latency, infrequent handover and low computational costs (Andrews, Buzzi, Choi, Hanly, Lozano, Soong & Zhang, 2014).

Alternatively, it has been shown that exploiting the environment-dependent radiometric features of a specific transceiver pair, such as the channel state information (CSI) (Duan & Wang, 2016) and the received signal strength indicator (RSS) (Moghtadaiee & Dempster, 2014), can improve the authentication procedure. In fact, these channel characteristics can be used to differentiate signals arriving from authorized transmitters and those originating from spoofed transmitters (Hao, Wang & Behnad, 2014), (Yu, Baras & Sadler, 2008). Moreover, (Honkavirta, Perala, Ali-Loytty & Piche, 2009) presents a comparative survey of wireless local area network location fingerprinting schemes. The foundation behind these schemes is that RSS is location-specific, due to path loss and channel fading, where most works in this category usually assume that the users are static; thus generating an excessive false positive rate in mobile scenarios. Accordingly, an attacker who is at a different location from the genuine user might be placed in different RSS profiles and whereby can infer the RSS of the user by using a wireless sniffer tool.

To tackle these challenges, a promising cross-layer authentication method is proposed in this paper. The novelty of our work lies in devising and evaluating a multi-layer approach which amalgamates physical layer information (i.e., non-cryptographic) (Hou, Wang & Chouinard, 2012) in conjunction with cryptographic procedures. In this context, we define two security level agreements (SLAs) which are devised for decentralized and centralized networks, respectively. These agreements are established at the beginning between the network slice (NS) and the authentication slice (AS).

Moreover, we proposed the use of a radio trusted zones data base at the AS side. In fact, a given covered area is divided into trusted zones where each zone contains more than one small cell, thus permitting the MT to initiate a single authentication request per zone, even if it keeps roaming between different cells. On the other hand, the data base of each zone contains the

different RSS profiles and their corresponding localizations. Thanks to the widely used radio mapping technique, this database is filled. Hence, this approach aims to add another security level to the system and reduce the recurring authentications in the network.

At the MI side and for non-cryptographic procedures, the gathered RSS measurements at the MT are used to generate the k^{th} fingerprint aiming to randomize the secret key used by the AKA protocol. After this step, a cryptographic approach employing an enhanced AKA protocol is performed in order to improve the confidentiality and integrity of the authentication handover. Furthermore, sending the mobile identity (IM) on the fly in a clear form (without encryption) is still another weaknesses of the AKA protocol. We address this problem by generating a radio signal fingerprint that prevents such transmission patterns, thus obscuring IM. Subsequently, the obscured IM is encrypted and then transmitted with the RSS parameter to the AS to corroborate the MT identity within the NS.

Once received, the AS, in response, sends an AV built with the aid of the k^{th} fingerprint, to approve the NS identity into the MT. In addition, before AS sends AV to MT across NS, AS applies the k-nearest neighborhood (k-NN) technique on the revived RSS with the existing data base to estimate the k^{dh} fingerprint distribution. The nearest output of this algorithm is used to identify the corresponding legitimate location stored in the database. It should be mentioned that the inaccuracy of the estimation technique does not affect the reliability of the proposed protocol because the identification of legitimate location is already takes into consideration the localization error range to define the trusted radio zones. Finally, the AKA authentication protocol is performed as operated in conventional cryptographic protocols. To have better insights into this work, we frame the set of contributions of this paper as follows:

1. Defining two SLA for decentralized and centralized 5G networks and proposing a cross-layer authentication approach based on SLA specifications.
2. Exploiting the random and unique RSS *measurements* in order to compute a secret k^{th} fingerprint.
3. Enhancing the security level of 5G networks by introducing a novel approach rendered by the creation of a radio trusted Zones database.

4. Executing security protocol analysis and validating the sensitivity of the proposed cross-layer protocol against different threats by leveraging the AVISPA tool. Additionally, comparisons of the computational complexity of the proposed scheme against traditional cryptographic and non-cryptographic approaches are also conducted.

To the best of author's knowledge, the cross-authentication approach along with radio trusted zones have not yet been devised and evaluated in the literature. The remainder of this paper is organized as follows. Section II introduces the proposed system model and the protocol design. In Section III, the security and performance analysis are evaluated. Finally, this paper is summarized in Section IV, where a number of future endeavors are also put forward.

2.3 System Model and Protocol Design

In order to tackle the important security challenge in SDWN-based 5G HetNets which results from the separation of the radio control plane from the data plane, we propose an AS as a third party security agent to provide isolation and efficient security authentication management over the integral network. Therefore, a cross-layer authentication procedure is proposed. This procedure is mainly based on increasing the security level of the AKA protocol by using physical layer information and machine learning algorithms at the server side in order to estimate the authenticity of the radio devices. The following subsections will detail the various steps related to the proposed protocol, namely, fingerprint generation, estimation and distribution, the cross-layer authentication and protocol design.

2.3.1 Generation of the k^{th} fingerprint

In our approach, we employ a channel-based fingerprinting mechanism to enhance the authentication procedure. Towards this end, we first define two SLAs which address decentralized and centralized networks, respectively. For decentralized networks, the authentication procedure is comprised of two steps. For centralized networks, a complete three steps approach is applied. These agreements are established at the beginning between the NS and the AS.

After defining the agreement, the non-cryptographic procedure is performed. As shown in Figure 2.1, the RSS measurements from different base stations are gathered and then averaged. In fact, to make this RSS parameter unique and random to suit the generation of the k^{th} fingerprint key, different RSS values from various radio devices are required to compute the average. Otherwise, considering a single RSS measurement from one radio device and due to the multi-path propagation environment, two different users on different locations may have the same value, which hinders the security of the protocol. Hence, the received radio signal strength from different radio devices, when collected at the u^{th} MT side, can be represented as

$$\mathbf{RSS}_u = [R_{1,t_1}, R_{2,t_2} \ldots, R_{N,t_n}], \tag{2.1}$$

where t_i is the *time of arrival* of the signal received from the i^{th} access point R_{i,t_i} to the u^{th} MT at a given location. This time of arrival significantly reduces the possibility to impersonate the RSS vectors by an intruder.

The MT then averages the RSS vectors to generate the k^{th} fingerprint such that

$$k = \mathrm{E}[\mathbf{RSS}_{\mathrm{u}}], \tag{2.2}$$

where E[.] is the mean operator.

The generated k^{th} fingerprint aids in randomizing the secret key that is used by the AKA protocol. After this step, the AKA protocol is performed at the MT. As a first step in this protocol, the IM is masqueraded by the k^{th} fingerprint. The output of the masquerading, dubbed as temporary identification mobile (TIM) aims to hide the device IM. After masquerading, in order to protect TIM from catching attack, this latter is encrypted with the AES ecryption algorithm. Finally, MT sends TIM with the RSS vectors to the AS to corroborate the MT identity within the NS.

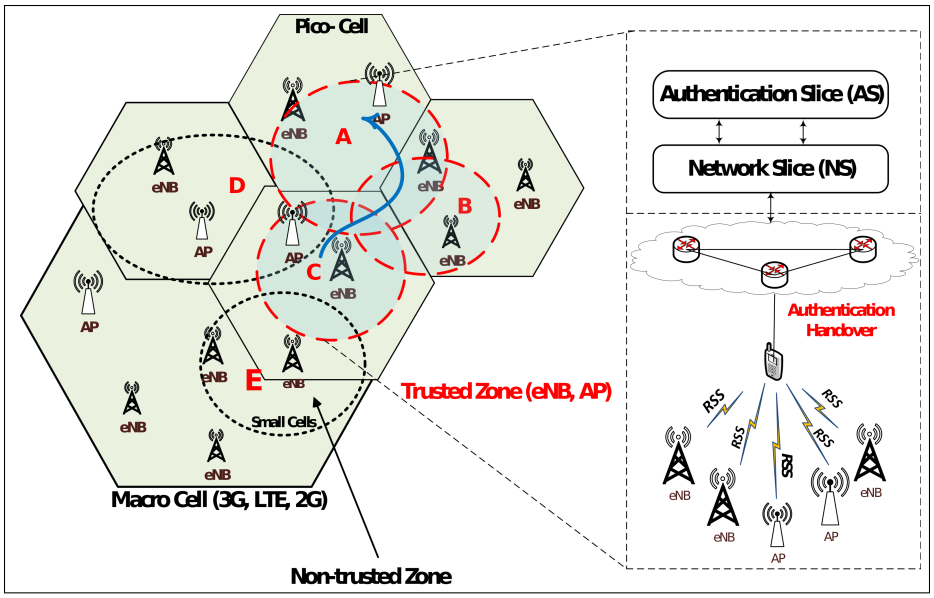


Figure 2.1 RSS vectors transfer between 5G radio devices through the MT in SDWN Architecture

2.3.2 Estimation of the k^{dh} fingerprint distribution

In this section, we will first introduce the proposed radio trusted zone concept that we consider in our system design to recognize the legitimacy of different radio device identities in the network. To this end, each zone is set to form a cluster of neighboring small cells. The database of this latter is built thanks to radio map database using the localization fingerprinting method in (Honkavirta *et al.*, 2009).

Since building the radio trusted zone database is out of the scope of this paper, in the remaining of this work, we assume the existence of this database at the AS side. Once the radio signal is received (i.e., TIM and RSS vectors), the AS analysis the RSS vectors and computes the k^{th} fingerprint as given in Eq. (6.2). The resultant key is used to unmask TIM in order to corroborate the IM authenticity within the NS. After this step, the deterministic k-NN method is used to estimate the k^{dh} fingerprint distribution. In fact, the k-NN method is one of the simplest ways to determine the fingerprinting process of wireless devices by using a radio map database. Hence, in contrary to our solution, the conventional k-NN method is victim of false positive

alarms when its output is compared to a radio trusted zone without taking into account the localization error range. Finally, in the proposed system, the k-NN process considers multiple nearest neighbors to compute the k^{dh} fingerprint distribution as follows

$$k^{dh} = \min \sqrt{\sum_{y=1}^{Y} \left(\mathbf{RSS}_u - \mathbf{RSS}_y\right)^2}, \tag{2.3}$$

where $\mathbf{RSS}_y$ is the RSS vector stored in the radio trusted zone. The resultant k^{dh} is used to identify the corresponding location in the trusted radio zones database, taking into account the localization error range, to prove the legitimacy of the radio device. In the next subsection, we will detail the key exchange process; handover through the cross-layer authentication protocol.

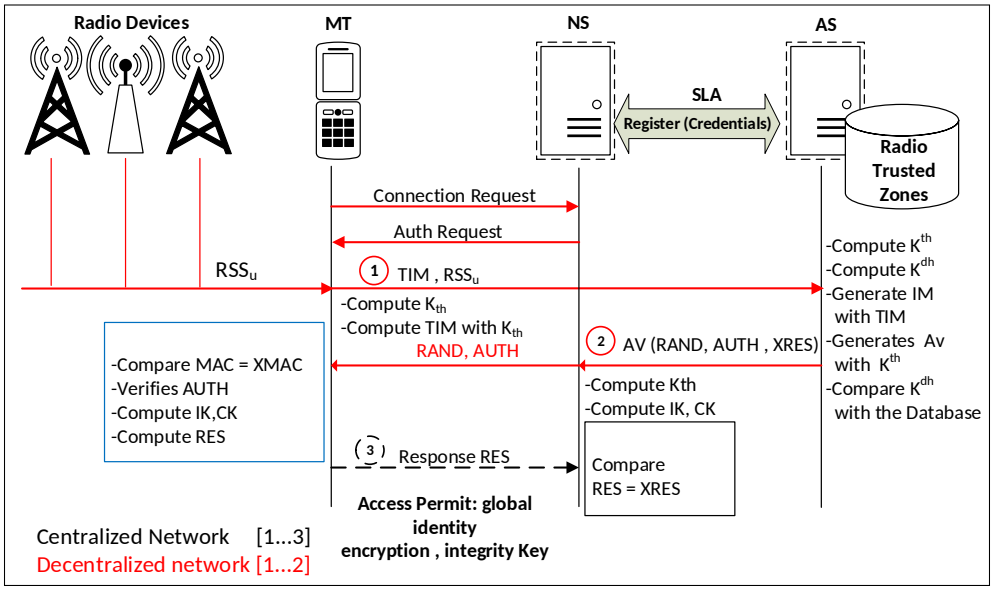


Figure 2.2 Cross-layer authentication handover procedure

2.3.3 Cross-layer Authentication Protocol

The procedure of keys' exchange between different network entities is exhibited in Figure 2.2. In this context, we assume that NS possesses previous credentials to coordinate with the AS. The

following steps within the authentication protocol are executed only if the MT is a new user or enters a certain trusted zone for the first time.

Step 1:

- MT computes the k^{th} fingerprint based on Eq. (6.2) and masquerades IM with the k^{th} resulting TIM.
- MT sends TIM and RSS vectors to AS in response to the demand made by the NS.

Step 2:

- AS generates the k^{th} fingerprint based on RSS vectors and IM from TIM, and k^{th}.
- AS estimates k^{dh} fingerprint distribution and search its corresponding legitimate localization in the radio trusted zones database that has been previously built.
- AS generates AV only if the legitimate localisation is found in the database.

Hence, AV will contain the following keys:

- MAC = $f_1(\ k^{\text{th}}$, AMF, SQN, RAND)
- XRES = $f_2(\ k^{\text{th}}$, RAND)
- CK = $f_3(\ k^{\text{th}}$, RAND)
- IK = $f_4(\ k^{\text{th}}$, RAND)
- AK = $f_5(\ k^{\text{th}}$, RAND)
- AUTH = SQN $\oplus$ AK||AMF||MAC

where $\oplus$ and || denote the bitwise XOR and the concatenation operations, respectively. The notions f_1 to f_5 are the AES cryptographic hash functions, SQN is the fresh sequence number, AMF denotes a public authentication management field handled by the network operator, RAND signifies a random number, IK symbolizes the integrity key, CK refers to the cipher key, AK is the anonymity key, MAC denotes message authentication code, XRES is the expected response, XMAC is the expected MAC and AUTN implies the authentication token.

It is important to note that for the decentralized network, the cross layer authentication algorithm ceases in step 2 thus AS sends the AV[RAND, AUTH] to MT without passing by NS, then MT verifies SQN and compares XMAC with the MAC to validate the network. Therefore, for the case of the centralized network, the AS sends AV[RAND, AUTH, XRES] to the NS and then the NS sends AV[RAND, AUTH] to MT. Subsequently, the MT calculates different keys as follows:

- AK = f_5(k^{th}, RAND)
- SQN= 1st(AUTN) $\oplus$ AK
- XMAC= f_1(k^{th}, 2nd(AUTN), SQN, RAND)
- RES = f_2(k^{th}, RAND)
- CK = f_3(k^{th}, RAND)
- IK = f_4(k^{th}, RAND)

After calculating the keys, the following is performed:

Step 3:

- If SQN is in the correct range, then the XMAC is compared with MAC to validate the network.
- If SQN is not in the correct range, then the connection is rejected.
- Once validated, MT calculates its RES value and sends it to the NS for validation.
- NS compares RES with XRES that is already present in the authentication vector.
- If RES is equal to XRES, then the MT is also authenticated by NS and mutual authentication is achieved. Otherwise, it is rejected.

2.4 Security and Performance Analyses

In the following, we perform automated security analysis to asses the security level of the proposed cross-layer authentication protocol using the Avispa tool to verify its resistance against various attacks. Moreover, we leverage a JAVA API to estimate the computational cost of the proposed scheme.

2.4.1 Security Analysis

In this section, we analyze the security of the conventional authentication protocol and the proposed authentication protocol. In the first scenario, we assess the security of the conventional AKA protocol. Since this protocol sends its pre-shared key over the air, we consider herein that an intruder in the network has the knowledge about the key. In contrast, in the second scenario related to the proposed protocol, the intruder is unable to acquire knowledge about the pre-shared key given that this protocol does not send the key over the air. In both scenarios, the intruder performs several typical attacks (i.e., man-in-the-middle, redirection, replay, etc.) on the protocols.

2.4.1.1 Scenario 1

In this scenario, the MT sends the IM and the secret key k on the fly to AS to initiate the authentication process. This process is formalized and then assessed using Avispa tool, As depicted in Figure 2.3 the protocol analysis indicates **UNSAFE**, revealing that the protocol is vulnerable to various analyzed threats.

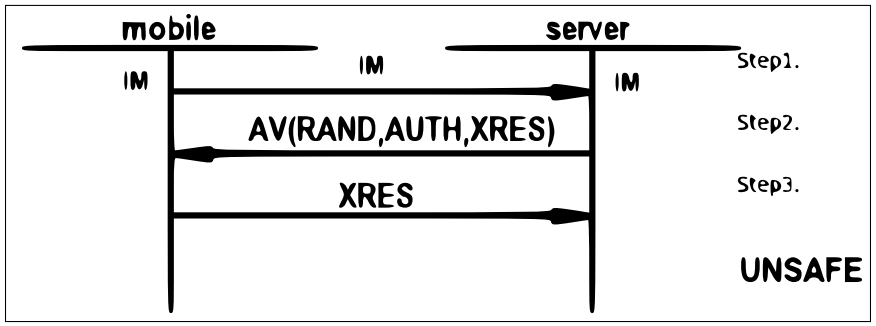


Figure 2.3 Avispa simulation for scenario 1

2.4.1.2 Scenario 2

As described in our protocol, MT sends IM encrypted with RSS_u on the fly to AS. In contrast to the conventional mechanism, MT, SN and AS generate the k^{th} fingerprint separately which improve the security as the fingerprint is never sent on the fly. This is corroborated by conducting

protocol analysis using Avispa tool, which indicates that this protocol is **SAFE** (against the analyzed threats) as shown in Figure 2.4.

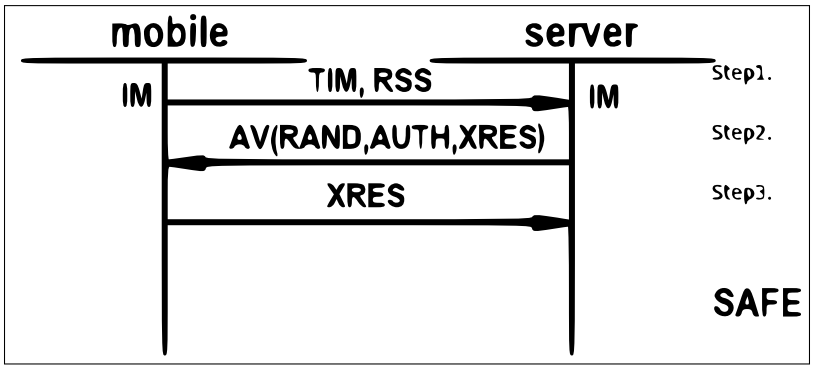


Figure 2.4 Avispa simulation for scenario 2

In the following, we detail how different attacks could be performed under scenario 2 and how our protocol design is resilient against such threats.

2.4.1.2.1 Redirection attacks and black-hole attacks

The mobile identification is not protected in the current mobile network and can be altered by an adversary with some devices such as an IM catcher, which leads to the redirection attack. In our protocol, the k^{th} fingerprint is used to masquerade the IM and thereby protects 5G networks against redirection attacks.

Accordingly, the attack fails if the malicious user is unable to obtain the legitimate user information from the MT. In the proposed protocol, the MT computes the IM embedded with the k^{th} fingerprint generating TIM and sends it to the AS. The authentication request is denied if the AS fails to match the IM sent by the MT. Such a technique solves the problem of miss-charged billing in the 5G network. Thus, the proposed scheme immunes the 5G network from black-hole attacks.

2.4.1.2.2 Replay attacks

The cross-layer protocol is resilient against this attack by solely sending the RSS vectors and TIM during the transmission of information over the network. This prevents the misuse of valid information; an adversary typically can delay the message over the network and sends it later for some malicious purpose if no random number or fingerprint is involved in the transmitted message.

2.4.1.2.3 Man-in-the-middle attacks

A man-in-the-middle attack occurs when an adversary eavesdrops the communicated information between the MT and the NS. In the context of the our proposed cross-layer protocol, the k^{th} key is independently generated in the MT, AS and NS. This key prohibits the communication from being eavesdropped.

2.4.1.2.4 Impersonation attacks

Over the 5G network, the corruption of the control plane endangers the security of the whole network. Following are some scenarios in which an adversary may attempt to impersonate the 5G network.

1. Consider the presence of a fake NS where an intruder can eavesdrop all its messages. The adversary must reply with a valid response RES to the NS in order to impersonate the MT, but the intruder cannot obtain the correct RES since this latter is exchanged exclusively between the MT and an uncorrupted AS.
2. If the intruder attempts to impersonate an uncorrupted network, the attempt would fail as the MT can verify that previously, there was no initiated request for AV. Furthermore, MT only exchanges traffic with trusted radio devices (i.e., the radio trusted zones database).

2.4.1.2.5 Denial of Service (DoS) attacks

The DoS attack and its variants are discussed in the following scenarios; the attacker MT's flood the victim control plane with authentication requests by spoofing the IM/TIM, the k key and a request number.

1. The attacker MT floods the NS victim with self IM. If the malicious MT does not respond within the threshold time duration to the proxy, then the connection is simply terminated. Accordingly, NS resets the authentication request and releases the resources that are used to maintain the authentication request status. In addition, if the request is originating from a malicious user, then the proxy will not acquire the k^{th} key or would simply receive an invalid k^{th} key. There is a timeout period for each MT to maintain the state of half-opened authentication requests. If the malicious MT attempts to cause an overflow at the victim NS with the half-open authentication requests, NS would not be able to accept any new incoming authentication requests.
2. The attacker MT floods the victim NS by spoofing IM. In this scenario, if the actual MT that receives a message is not active, then the AS will not receive any information from the MT, and this process becomes similar to first case; the NS waits for a threshold time to hear from the AS. After the timeout period, the NS resets the authentication request and releases the resources that are used to maintain the authentication request status.

In fact, in this protocol, the AS is supposed to receive an RSS vectors from the MT, which is neither an actual IM of the MT nor a TIM for the NS. An actual IM or TIM with a fake k^{th} key will not be able to extract the correct IM of the MT and thus the connection will be terminated. Hence, there is no chance that the attacker would be able to generate the same k^{th} from a victim MT's IM. Indeed, given the aforementioned information, we assert that the proposed cross-layer AKA protocol protects the network from DoS attacks.

2.4.2 Computational cost analysis

We further thought that it would be insightful to analyze the computational cost of our proposed cross-layer protocol. In this context, it is important to note that the SDWN paradigm introduces the cloud radio access networks (C-RAN) paradigm, which aims at reducing the computational cost as most of the processing activities are executed on the distributed cloud. Moreover, the well-trusted radio zones database is formed by small cells; a mechanism which avoids frequent authentication of the MT within each small cell. We perform comparisons of the non-cryptographic and cryptographic authentication algorithms against the proposed cross-layer protocol under an environment which does not employ radio trusted zones. For our analysis, we exploit a dataset of 25 radio signal strength samples collected for 280 combinations of user locations and orientations.

Since our proposed cross-layer protocol is implemented in Java, a Java API is developed for this evaluation purpose to be coherent and to generate real time perspectives of the computational cost. Moreover, we use an Intel Core i7-6700 CPU with 3.4 GHz X64 based processor and 16 GB RAM to conduct the computations. The results of this comparison is shown in Figure 2.5, which demonstrates the computational cost of cryptographic, non-cryptographic and the proposed cross-layer protocol across small cells with and without employing the trusted zone approach at the AS level. In the case where the proposed protocol operates without employing the radio trusted zones, we observe a clear increment in computational cost in comparison with non-cryptographic and cryptographic procedures, respectively, and this gap increases when the number of cells increases. The augmentation is due to the fact that our proposed cross-layer protocol operates in this specific case without a trusted zone and uses machine learning algorithm to authenticate the radio devices. The absence of a trusted zone increases the recurrence of authentication procedures, which leads to more complexity.

Once the radio trusted zones' approach is employed, the computational cost of the proposed cross-layer protocol drops in contrast with the first approach. This renders the deployment of a

radio trusted zones a better choice to achieve a lower complexity and thus reduce latency.

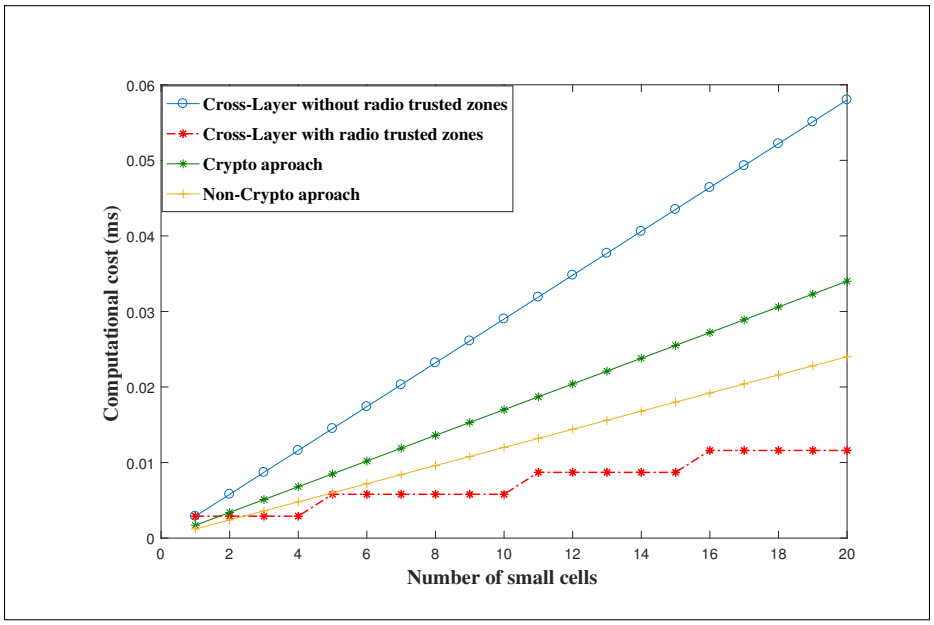


Figure 2.5 Cross-layer authentication protocol with and without radio trusted zones, in comparisons with cryptographic and non-cryptographic approaches

2.5 Conclusion

In this paper, we propose a software-defined wireless network (SDWN)-enabled fast cross authentication scheme that combines non-cryptographic and cryptographic algorithms to tackle the challenges of latency and weak security in 5G HetNets. First, the radio trusted zone database concept is introduced aiming to reduce the authentication recurrence. Consequently, the cross-layer algorithm is designed, implemented and evaluated. By executing automated protocol analysis using the Avispa environment, the security posture of our cross-layer authentication protocol in terms of resilience to various attacks is analyzed. The results show that the proposed scheme satisfies 5G security requirements and its advantages have been verified by simulations. Further, the proposed protocol causes considerable deduction of traffic authentications, thanks to the introduction of the radio trusted zone unit. Finally, a Java API is developed to compute

the complexity of our system and to compare it against cryptographic and non-cryptographic approaches. It is shown that if a radio trusted zone is employed, the computation complexity is significantly reduced in comparisons with the two latter approaches, by limiting the authentication recurrence. As for future work, we will be focusing on employing machine learning techniques to properly classify the various RSS profiles of a HetNet in an attempt to build reliable and efficient radio trusted zones.

CHAPTER 3

INTRUSION PREVENTION SCHEME AGAINST RANK ATTACKS FOR SOFTWARE-DEFINED LOW POWER IOT NETWORKS

Christian Miranda[1] , Georges Kaddoum[2] , Amine Boukhtouta[3] , Taous Madi[4] , Hyame Assem Alameddine[5]

[1,2,3,4,5] Département de Génie Électrique, École de Technologie Supérieure, 1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Article published in IEEE Access, January 2023

3.1 Abstract

The 6LoWPAN [IPv6 over low-power wireless personal area networks] standard enables resource-constrained devices to connect to the IPv6 network, blending an IPv6 header compression protocol. For this network technology, a new routing protocol called Routing Protocol for low power Lossy network [RPL] has been designed. The latter is a lightweight protocol that determines the route across the nodes based on rank values. This protocol is known to be non-resilient against Rank attacks, which aim at creating non-optimized routes for packet forwarding, hence overwhelming the constrained 6LoWPAN. With 5G, Software-Defined Networks [SDNs] have been developed to facilitate simple programmable control plane, Quality of Service [QoS] provisioning, and route configuration services for 6LoWPAN. However, there is still a lack of optimization mechanisms to protect 6LowPAN against Rank attacks in the SDN-based deployment. To this end, in this paper, a Reinforcement-Learning [RL] agent is leveraged to assist and complement a SDN controller in achieving cost-efficient route optimization, and QoS provisioning packet forwarding to prevent rank attacks. Experimental results confirm that our approach effectively prevents Rank attacks, while providing an adequate delay and radio duty cycle. Meanwhile, it maximizes the packet delivery ratio, facilitating practical implementations in software-defined Low Power Internet of Things (IoT) Networks.

3.2 Introduction

Wireless sensor networks [WSNs] are considered as one of the most important applications of the Internet of Things [IoT] (Kocakulak & Butun, 2017a). In general, WSNs can be considered as Low Power and Lossy Networks [LLNs], presenting some constraints on their deployment, especially in critical and large-scale scenarios (e.g., massively distributed, and heterogeneous networks). The resource-constrained limitations prevent the deployment of WSNs in scenarios where the operation is subject to strict reliability and performance requirements. At the same time, the lack of flexibility stems from the rigidity of WSNs towards policy changes, making these networks difficult to adapt. Internet Protocol (IP) technology considerably brings direct and bidirectional access to devices reducing the mentioned difficulties, but some issues emerge concerning interconnections' complexity.

In WSNs, IP networks aim to provide end-to-end communication, which allows devices to be accessed without the necessity for gateways to use adaptation techniques to boost efficiency and quality of wireless transmissions (Bharadia, Choi, Jain, Katti, Kim & Levis, 2019). In this context, the 6LoWPAN standard uses IPv6 addresses IPv6 addresses eliminating adaptation techniques (Al-Kashoash, 2019a). Moreover, 6LowPAN is a network standard that defines header compression mechanisms and encapsulation rather than being an IoT application protocol technology (e.g., Bluetooth, ZigBee (Fisser, Ipach, Timm-Giel & Becker, 2020)). Nevertheless, due to common factors, such as the node failures, limited bandwidth, etc., the wireless links in multihop 6LoWPAN are unstable, and therefore not reliable. These difficulties can severely impact the performance of the entire network (Miguel, Jamhour, Pellenz & Penna, 2018a; Kobo, Abu-Mahfouz & Hancke, 2017b).

IP-based networks adopt distributed protocols (eg., Open Shortest Path First [OSPF], Border Gateway Protocol [BGP], Routing Information Protocol [RIP]) for routing decisions and to preserve topology while decreasing the overhead in the entire network (Nedyalkov, 2019). Since low-power devices reduce the radio range compared to when all nodes communicate with a single base station, a multihop grid allows systems to extend over a larger area. Consequently,

from the introduction of multiple hops, the link uncertainty is aggravated along the hop distance and may increase the possibility of dropped packets on the way. Specifically, RPL is a protocol based on rank values that rely on an Objective Function [OF] to determine the route across the nodes (Shin, Sharma, Kim, Kwon & You, 2017a). An OF defines how an RPL node selects and optimizes routes to build a Destination Oriented Directed Acyclic Graph [DODAG] rooted at the network's border router. Further, the OF defines how the nodes should consider the metrics and constraints in the rank value, which is roughly the node's distance to the DODAG root. Even though the rank values in RPL helps for multiple objectives, including route discovery and distribution, loops prevention, and control overhead management, this protocol is exposed to a wide variety of routing attacks (i,e., Sinkhole attacks, Wormhole attacks, Rank attacks (Kamble, Malemath & Patil, 2017a)). These attacks can significantly impact the resource utilization and the network performance (Kamble *et al.*, 2017a). Precisely, in rank attacks, malicious nodes broadcast messages to advertise lower ranks than their original ones to corrupt routing cost values, which forces neighboring nodes to choose them as a preferred parent and change their rank accordingly. Thus, Rank attacks create non-optimal routes and introduce loops that overwhelm the network resources and increase resource consumption (Rai & Asawa, 2017a).

With the arrival of 5G, Software-Defined Networks [SDNs] have been developed to introduce scalability and programmability to accomplish QoS provisioning and fast routing configuration services over the 6LoWPAN. It has shown promising advances in network configurability, virtual network functions plugin, and reduction in capital expenditure (Miguel *et al.*, 2018a). In this context, Software-Defined 6LoWPAN wireless sensor network [SD6WSN] is proposed. This architecture aims to manage data plane forwarding in 6LoWPAN according to the SDN approach (Charfi, Mouradian & Vèque, 2020a).

SD6LowPAN has several positive aspects, including a centralized SDN architecture that allows flexibility and scalability, presenting further opportunities to move beyond the traditional notions of low-power IoT driving from small to various networks connected across a network backbone and protocols such as 6LoWPAN, to dynamically serve multiple applications, such as data collection, actuation, and monitoring with varying QoS requirements.

However, SD6LowPAN faces considerable challenges, such as the non-negligible overhead introduced by SDN devices caused by the continuous exchange of messages and the vast distances between the data plane and the controller, and is likely to suffer from Single Point of Failure (SPoF). It is valid to mention that the problem of SPoF is out of the scope of this paper. Therefore, a lightweight SDN controller is leveraged in the border router to promote northbound and southbound communication with the data plane and applications correspondingly and reduce the non-negligible overhead introduced by SD6LowPAN (Baddeley, Nejabati, Oikonomou, Sooriyabandara & Simeonidou, 2018a). Furthermore, the incorporation of RPL in the routing layer for network discovery and the lack of routing optimization procedures to optimize the routes defined by the RPL make SD6LowPAN susceptible to Rank attacks. Hence, to tackle this concern, in this paper, we propose an RL approach for routing optimization to prevent Rank attacks in SD6LowPAN.

3.2.1 Motivation

The motivation behind this work is the computational complexity of managing security solutions and the sample complexity of finding the right approach for routing optimization to prevent Rank attacks in SD6LowPAN. In this vein, the centralization of security controls in SD6LowPAN facilitates the network (re) configurability and network slicing which allow resource sharing and the adoption of complex solutions in a multitenant environment where a single instance of an application and its supporting resources serves multiple providers (Miguel *et al.*, 2018a). However, the programmable nature of SDNs increases the network's vulnerability to attacks (Kobo *et al.*, 2017b), as applications can be easily installed.

Accordingly, in SD6LowPAN, authentication and intrusion detection mechanisms are mainly implemented on the IoT nodes (Verma & Ranga, 2020b; Restuccia, D'Oro & Melodia, 2018), while RPL can be performed at the controller or application-level (Ooko, Kadam'manja, Uwizeye & Lemma, 2020). Moreover, the massive deployment of RPL-based low-powered IoT devices makes SD6LowPAN more vulnerable to rank attacks. Hence, the RPL is vulnerable to internal Rank attacks taking advantage of the vulnerable rank property defined by non-optimal

routes established by the OF. Consequently, these attacks jeopardize the network performance, topology, and traffic (Preda & Patriciu, 2020). Illustratively, an attacker can accomplish this attack by misusing the rank property and infringing the routing protocol. Based on the vulnerability analysis related to the rank property, Rank attacks create non-optimal paths for all packets, which pass through malicious nodes and overwhelm the restricted SD6LoWPAN (Sahay, Geethakumari & Modugu, 2018a).

Meta-heuristic algorithms, such as Ant Colony Optimization [ACO], Swarm optimization, and artificial bee colony, are practical and widely used approaches to find solutions to combinatorial optimization problems (Rajesh, Raajini, Rajan, Gokuldhev & Swetha, 2020a; Salem, Salam, Abdelkader & Mohamed, 2019a). However, they are limited by the high sample complexity required to reach a reasonable solution. The sample complexity represents the number of training-samples that an algorithm needs to learn a target function successfully (Chen & Vaidya, 2019). Also, much work has been done in the field of machine learning for routing optimization, but these methods can require an unreasonably large number of samples before a good policy is obtained. Precisely, the lack of exploration in these methods leads to an unreasonably large sample complexity, which is unrealistic for dynamic environments (Nagabandi, Kahn, Fearing & Levine, 2018). In this context, RL seems to be a more promising and realistic solution compared to traditional machine learning approaches as it relies on an RL agent that explores and interact with its environment to generate its own training data. To this end, in this paper, we incorporate a RL approach in the lightweight SDN controller design to achieve routing optimization and QoS provisioning packet forwarding to address the vulnerable rank value and the RPL objective functions' weaknesses while minimizing the overhead and management complexity introduced by SD6LowPAN.

3.2.2 Related Work

Some research works have looked into management complexity and security solutions to address Rank attacks in resource-constrained SD6LowPANs. Precisely, in (Lasso, Clarke & Nirmalathas, 2018a), a software-defined networking framework for IoT based on 6LoWPAN is presented

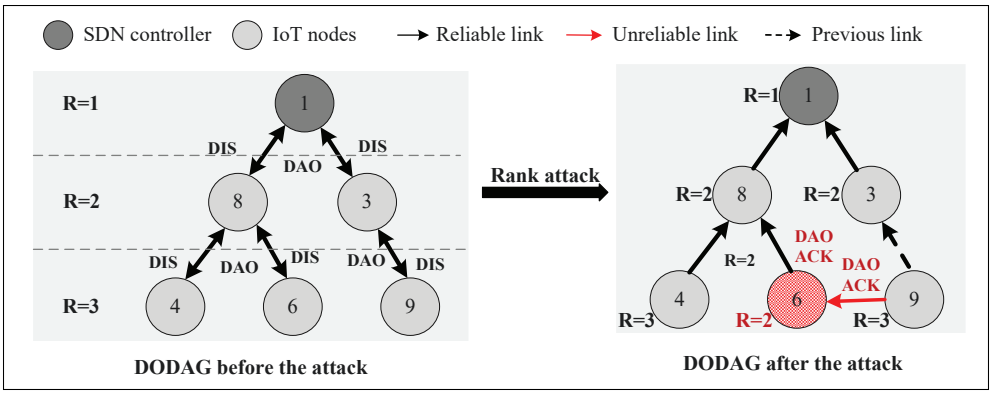


Figure 3.1 DODAG instance before and after Rank attack

to reduce the management complexity in IoT networks. Further, in (Baddeley *et al.*, 2018a), a lightweight SDN framework for Contiki OS is introduced to reduce the control overhead to practical levels. Moreover, in (Lin, Akyildiz, Wang & Luo, 2016a), a QoS-aware adaptive routing [QAR] based on RL with a QoS-aware reward function is introduced for multi-layer hierarchical SDNs achieving time-efficient, adaptive, and QoS-provisioning packet forwarding. In (Raba, Juan, Panadero, Bayliss & Estrada-Moreno, 2019), the authors present a combination of the IoT with a heuristic framework to enhance logistics in an agri-Food Supply Chain. In (Ancillotti, Vallati, Bruno & Mingozzi, 2017a), the authors propose an improved objective function that relies on an RL-based link quality estimation strategy for RPL to minimize the overhead caused by active probing operations. However, the latter work introduces additional computational complexity by incorporating an RL approach in 6LoWPAN. A security service to prevent Rank attacks is proposed in (Dvir, Buttyan et al., 2011), where the authors generate a hash chaining using a random number chosen by the root node to avoid the RPL from publishing an illegitimate reduced rank. Moreover, in (Wadhaj, Ghaleb, Thomson, Al-Dubai & Buchanan, 2020a), a challenge-response scheme is proposed to validate the nodes' authenticity within a DODAG, in (Shin *et al.*, 2017a), a cost-efficient protocol for route optimization is introduced, where the authors include steps for reliable route optimization and mutual authentication. Further, an enhanced RPL protocol is proposed in (Muzammal, Murugesan, Jhanjhi & Jung, 2020), where a rank threshold approach and the hash chain authentication technique are proposed to deal with RPL-based attacks.

In addition, some works propose run-time verification mechanisms to detect unexpected behavior in IoT system nodes. These mechanisms monitor the real-time events coming from the IoT system elements and trigger self-healing actions if unexpected behaviour is detected at an IoT device. For instance, in (İnçki & Ari, 2018), the use of complex event processing techniques for detecting failures in the system is proposed by monitoring the run-time event occurrences with regards to the system constraints denoted by event calculus. In (İnçki, Arı & Sözer, 2017), a run-time monitoring approach for IoT systems is presented where the event relations expressed in terms of the sequential interaction messaging model of Constrained Application Protocol (CoAP) are explored. Nevertheless, this technique helps to detect IoT nodes' misbehaviour; it also introduces an overhead due to the recurrent monitoring system installed on each DODAG node. Furthermore, this technique does not prevent SD6lowPAN from being compromised by a Rank Attack because rank attack alters the assigned rank value but does not change the node's behavior, overloading the network with few resources. Indeed, the attacker's main objective is to overload the network using the behavioral patterns of the nodes in an RPL network.

Although essential works have been proposed in the literature to target management complexity and Rank attacks in 6LowPAN, all these deployments are not satisfactory to simultaneously guarantee efficient Intrusion Prevention System (IPS), Low Management Complexity (LMC), and considerable Overhead Reduction (OR) in software-defined Low Power Networks (Vohra & Srivastava, 2015a). A comparison between some current research work and the proposed Software-Defined Reinforcement Learning (SDRL) scheme is presented as follows.

Table 3.1 Related works comparison

Solution	OR	LMC	IPS
[12],[22],[23]	✓	✗	✓
[25]	✓	✗	✓
[26]	✗	✗	✗
[27]	✗	✓	✓
[28]	✓	✗	✓
[29],[30]	✗	✗	✗
SDRL	✓	✓	✓

3.2.3 Contribution

In this paper, a security scheme for preventing Rank attacks in SD6LowPAN is designed. The novelty of the proposed work lies in devising and evaluating an intrusion prevention scheme that amalgamates SDN applications in the control plane, achieving efficient topology discovery, flow control management, and route optimization SD6LowPAN. The RPL-based topology discovery service is deployed to cluster the SD6lowPAN and create the route tables used for the topology optimization service. Subsequently, a coordinator flow control application is developed to coordinate the communication between the application, control, and data planes. Further, an RL-enabled topology optimization, achieving route optimization in SD6LowPAN, is designed. It is worth mentioning that nodes' authentication and integrity are out of the proposed work scope. Thus, the main contributions of this work are summarized as follows:

1. A lightweight SDN controller is leveraged in the border router to reduce the non-negligible overhead introduced by SD6LowPAN.
2. A coordinator flow control application is integrated into the SDN controller to handle the interaction between the layers of SD6LowPAN.
3. In the SDN controller, a northbound and southbound interfaces are enhanced to facilitate the communication between the SDN controller and the data plane and applications.
4. An RPL-based topology discovery application is employed for network discovery from the IoT nodes towards the SDN controller.
5. An RL approach is developed in the SDN controller to optimize the RPL routing paths to prevent Ranking attacks' harmful effects in SD6LowPAN.
6. Moreover, analysis of the duty cycle and computational complexity are provided, while simulations showing the effectiveness of the proposed scheme are executed by leveraging the Contiki Cooja tool.

The remainder of this paper is organized as follows: Section II introduces the background and network model, in Section III, we describe the RL based intrusion prevention scheme, which falls into: the stack scheme, intrusion prevention algorithm and RL agent modeling and

inner-workings. In Section IV, the simulation setup and the experimental results are conducted. Finally, the paper is concluded in Section V, where future endeavors are also put forward.

3.3 Background and Network Model

In this section, we provide a brief background on RPL, Rank attacks and RL. Further, we present the impact of Rank attacks on SD6LowPAN, and the considered network model.

3.3.1 Background

It is worth mentioning that the proposed approach does not detect or eliminate the attacker node. Instead, this work devises an RL-based intrusion prevention system against RPL Rank attacks' harmful effects through route optimization for low power IoT networks. The basic concepts underlying these algorithms are detailed in what follows.

3.3.1.1 RPL Operation

RPL is an IPv6 routing protocol designed and standardized by the Internet Engineering Task Force [IETF] (Wadhaj, Ghaleb, Thomson, Al-Dubai & Buchanan, 2020b). To build the network topology, RPL employs Directed Acyclic Graphs [DAGs], which can be segregated by one or more DODAGs, where each DODAG has a root node. Multiple root nodes are integrated within a backbone network that consists of border routers that connect them to the internet. RPL is a routing protocol for wireless systems with low power consumption that starts to find routes based on the OF established in a setup stage. The OF is utilized to deliver traffic to different routes according to traffic requirements. The OF encoded these traffic requirements to be used by the RPL during routing operations. RPL applies three types of control messages, i.e DODAG Information Object [DIO], DODAG Information Solicitation [DIS], and DODAG Advertisement Object [DAO], as shown in Fig. 3.1. The root node broadcasts DIO messages at regular periods defined by a trickle algorithm (Levis, Clausen, Hui, Gnawali & Ko, 2011a). The DIO message gives the IoT nodes information to explore the DODAGs, acquire the setting parameters, and

select the favored parent set. To choose the parent set, RPL applies the OF, which contains some routing metrics (Magubane, Tarwireyi, Abu-Mahfouz & Adigun, 2019a). A DODAG uses DIS message to request the DIO from its neighboring node to join the DODAG. DAO messages are disseminated by the IoT nodes to the root node to update the DODAG. Thus the composition of the DODAG topology is supported by the root node. The RPL operations include topology discovery, DAG construction, route generation, data path validation, and loop detection based on rank values (Yassein, Flefil, Krstic, Khamayseh, Mardini & Shatnawi, 2019a).

A rank value defines the relative position of a node within the DODAG. The 6loWPAN has unique characteristics that require the specification of new routing metrics and constraints (Khallef, Molnar, Benslimane & Durand, 2017a), which can be used by the RPL in the path computation. These metrics/constraints can be categorized into two basic types:

- Node metrics and related constraints (e.g., hop counts, energy state.),
- Link metrics and related constraints (e.g., throughput, latency, packet loss).

3.3.1.2 Rank Attacks

The OF is an essential factor in the parent's selection, along with the rank. Once a node receives a valid rank, the OF's setting based on the routing metrics must be determined before modifying the selected parent node. For instance, if the routing metric relies on the Expected Transmission Count [ETX], the OF is determined to hold the routing path with the lowest ETX value, and a node will receive both the rank and ETX for the chosen parent node. Mainly, to successfully originate a Rank attack, the attacking node must alter the routing metric advertised by the parent node so that the OF of the neighboring nodes is exposed to be attacked.

In this regard, Rank attacks have raised serious concerns about the weakness of the objective function of the RPL. This protocol usually implements two objective functions: the Minimum Rank with Hysteresis Objective Function [MRHOF] and the Objective Function Zero [OF0]. The OF0 constructs a Directed Acyclic Graph [DAG] with the lowest number of hops (Safaei, Monazzah & Ejlali, 2020), while MRHOF constructs a DAG with the lowest ETX to select

the best path (Pradeska, Najib, Kusumawardani et al., 2016a). Since the existing OFs take into account only one (Khallef *et al.*, 2017a) or two metrics (Djedjig, Tandjaoui, Medjek & Romdhani, 2017a), the DODAGs cannot fully satisfy some recent applications which require several QoS constraints such as packet loss, duty cycle, and end-to-end delay (Pradeska *et al.*, 2016a). For example, OF0 chooses the shortest path; however, it does not necessarily ensure the end-to-end delay requirement, which is an essential constraint for interactive applications (Safaei *et al.*, 2020). Furthermore, in the MRHOF, the objective function aims to minimize the expected total number of packet transmissions required to deliver a packet to the ultimate destination successfully (Pradeska *et al.*, 2016a).

It is worth mentioning that a DODAG only uses one OF for its formation and maintenance. For instance, to illustrate a Rank attack, in this paper, we consider the ETX as the principal routing metric for a network topology creation, an attacker node with a legitimate rank R_l, and R_n, which is a minimum rank between the neighbors. In this example, the attacker node will promote a rank value of less than R_n to launch the attack. Consequently, the attacker alters his rank to below R_n, where $R_a < R_n$ is the rank announced for the attacker R_a. Thus, the attacker's neighbors will drop the rank value if the announced rank of R_a is too low because the RPL recommends that the rank setting is within a threshold. Otherwise, the unexpected rank can induce unstable network topology. Accordingly, in Rank attacks, the attacker advertises a rank with the ratio $R_p < R_a < R_n$, where R_p is the attacker's preferred parent node rank.

In this vein, the updated rank advertised by the attacker is smaller than most neighboring nodes (Rehman, Khan, Lodhi & Hussain, 2016a). Also, to boost the severity of the attack, the ETX advertised in the DIO message is diminished compared to the minimum observed between neighbors. In real 6lowPAN, routing metrics are subject to more variations than the rank; therefore, RPL does not propose any measures to control the routing metric values. As depicted in Fig. 3.1, the neighboring nodes of attacker (compromised) node six select the latter as their new preferred parent because it changes its rank from R=3 to R=2 and the ETX announced in the DIO message is lower than the minimum perceived between neighbors. As a result of such

ranking misuse, new non-optimal links are considered (depicted through red lines in Fig. 3.1), which impacts the network performance implicitly.

3.3.1.3 Reinforcement learning

RL is an area of machine learning that allows an agent to learn in an interactive environment by trial and error using feedback from its actions and experiences (Lin *et al.*, 2016a). Specifically, it addresses how an agent/decision-maker tries to learn the dynamic system's behavior through interactions with the environment. The agent receives the current state and the reward from the dynamic system at each iteration and takes an action that increases the long-term revenue. The agent obtains the state and the system's reward values, whereas the system captures the action as an input from the agent (Recht, 2019a). RL can increase automation or optimize sophisticated systems' operational efficiency, eg., networking, robotics, manufacturing, and supply chain logistics (Arulkumaran, Deisenroth, Brundage & Bharath, 2017). However, RL's practical implementations generally, we do not have information on the subjacent model. In such a scenario, model-free learning algorithms are more suitable. The most widely used approaches in this area are Monte Carlo [MC] and Temporal Difference [TD] learning. While MC learns directly from episodes of experience without any previous knowledge of Markovian decision Process [MDP] transitions, TD learns by bootstrapping from the current estimate of the value function (Arulkumaran *et al.*, 2017).

3.3.1.4 Rank attack impact

SD6lowPAN defines a controller that communicates with the data-plane through a Software Defined 6LoWPAN Wireless Sensor Network Protocol [SD6WSNP], that employs IPv6 and RPL at the routing layer, UDP at the communication layer, and CoAP at the application layer (Miguel *et al.*, 2018a). SD6WSNP uses CoAP messages to send rules dictated by SDN applications, such as wireless link quality, geolocation, and power transmission level, to the nodes. Consequently, RPL creates DODAGs of different sizes (hops) stored in flow tables for forwarding data plane packets. Therefore, when a Rank attack is performed, the DODAGs communicated by RPL with

the SDN controller contain a non-optimal set of paths. As a consequence, these non-optimized paths impact the routing messages between the nodes and the SDN controller. They also affect the routing rules of the messages exchanged between the nodes in the data plane; thus, they overwhelm the SD6lowPAN. It is worth mentioning that this work focuses on the messages between the nodes and the SDN controller in the experimental results.

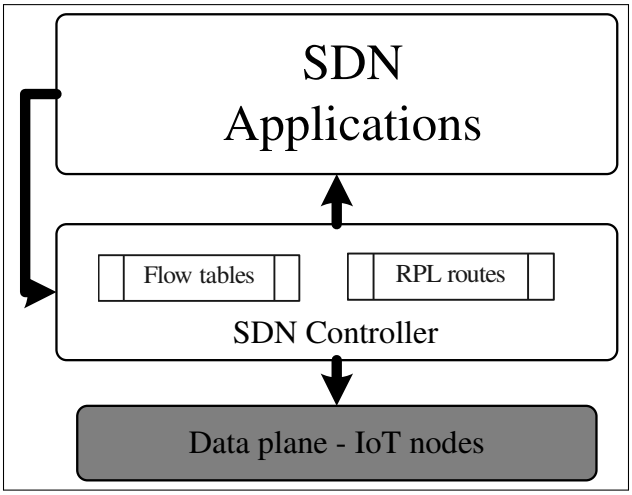


Figure 3.2 Network Model

3.3.2 Network Model

As depicted in Fig. 3.2, the network model in the proposed scheme is a typical SDN-based network architecture where, in the data plane, multi-hop low-power IoT nodes, connected by IPv6 to the Internet through a gateway (or border router), are deployed. These nodes are characterized by a low power, low data rate, short radio range, and low cost. The control plane then consists of a lightweight SDN controller on the border router that makes decisions about where traffic is sent from the underlying data plane to selected destinations with a coordinator flow control. Precisely, a lightweight SDN controller is used to minimize the signaling delay in traditional SDNs. Finally, at the top of the architecture, the application plane is designed to discover the network and optimize the topology in Low Power IoT Networks. The proposed stack scheme is presented in the following section.

3.4 Proposed Scheme

This stack scheme creates an enhanced version of the architecture concepts proposed in (Baddeley *et al.*, 2018a) while incorporating architectural, protocol, memory, and controller optimization to mitigate control overload and improve scalability. Precisely, it takes advantage of a northbound Application Programming Interface (API) to facilitate the control plane's communication with the SDN core applications and a southbound API to facilitate the control's communication with the data plane. The interaction between the northbound and southbound APIs is handled by the coordinator flow control, located in the control plane, as shown in Fig. 3.3.

In summary, the proposed stack scheme incorporates three layers as follows. At the bottom of the stack, typical IoT nodes in the data plane combine the following communication functions: data plane forwarding, border routing and sensing applications. In the middle, the control layer, the coordinator flow control is executed. At the top of the application layer, the SDN core applications (topology discovery and topology optimization) are integrated. This architecture is presented in Fig. 3.3 and is fully integrated with the IEEE 802.15.4-2012 protocol stack.

3.4.1 SDN data plane

In the data plane, the low power IoT network is executed. Due to the small packet size and low bandwidth, the SDN data plane requires resource-saving to maximize the lifetime of IoT nodes. The low power IoT node has at least three components: the data plane forwarding, routing agent, and sensing components, which use large arrays of sensors to collect data from a particular environment. The IoT network interacts with the control layer through control messages. The main functions of the SDN IoT nodes are:

- Send information to the control plane;
- Examine data plane packet headers;
- Send or deny data plane packets according to matching entries in the flow table;
- Send packet-in notifications to the control plane when there is no matching entry.

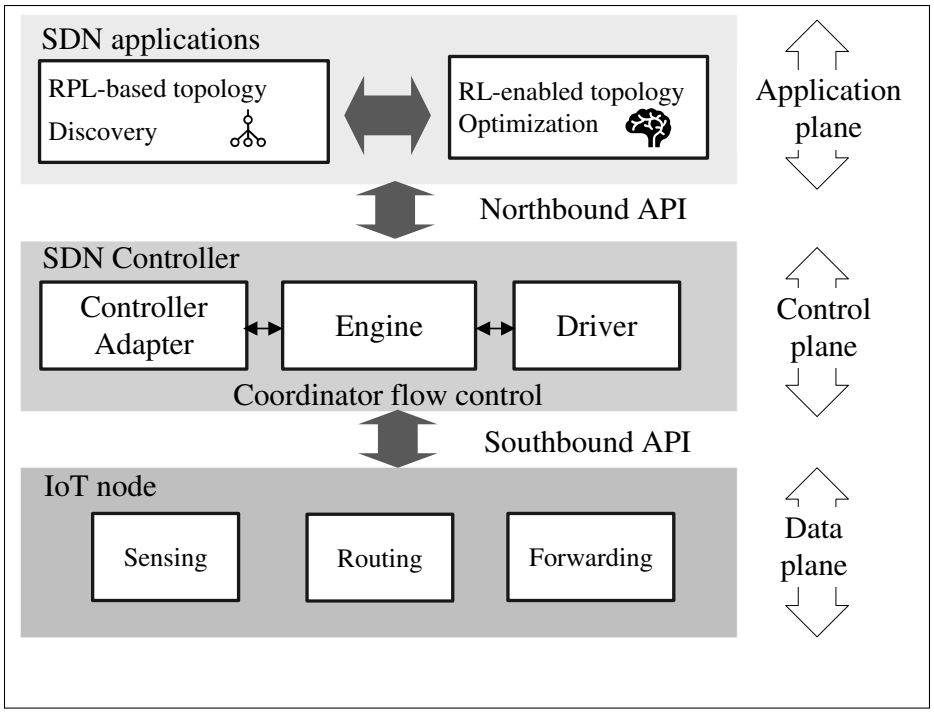


Figure 3.3 Network's stack scheme

Moreover, the SDN data plane modifies packet forwarding at the operating system as follows. The routing agent inspects packet headers and checks if the incoming packet is a control message. If the control message requests an RPL discovery, it is routed through the control plane following the 6LoWPAN-RPL routing standard. If the control message contains a flow table instruction, it is routed through the data plane. Otherwise, the packet is delivered to the local sensing application to perform the data plane forwarding function (Tanganelli, Virdis & Mingozzi, 2019b).

3.4.2 SDN control plane

To provide a platform for SDN experimentation in low power IoT networks, we have implemented a lightweight SDN control plane introduced in (Baddeley *et al.*, 2018a). The lightweight SDN controller provides a coordinator flow control and an enhanced southbound and northbound APIs, detailed as follows.

3.4.2.1 Coordinator flow control

In the control plane, a coordinator flow control is developed to facilitate the communication in the proposed SD6LowPAN architecture. In this context, the coordinator flow control integrates three SDN functions that rely on (Baddeley *et al.*, 2018a) to handle specific requirements of the SDN implementation. A brief explanation of the SDN functions are detailed below.

3.4.2.1.1 SDN controller adapter

The controller adapter exposes a controller interface to the SD6LowPAN architecture, allowing the control plane to implement third party interfaces.

3.4.2.1.2 SDN driver

The SDN driver determines how to manage the flow table. It provides high-level functions to accomplish particular tasks by setting up flow table entries, such as aggregating or removing flows, setting routing paths through the network, and creating security policy entries. It also handles flow table actions and determines how and when nodes communicate to the controller with specific rules.

3.4.2.1.3 SDN engine

The SDN engine defines the northbound and southbound communication (application plane with the controller and the control plane with the data plane, respectively) for both incoming and outgoing messages to the controller.

3.4.2.2 Southbound API

The coordinator flow control utilizes a southbound API to ensure that packets are transported through the User Datagram Protocol [UDP] to enable a secure DTLS [Datagram Transport Layer Security] and provide better communication between the data plane and the controller. Also,

this API ensures that each node's information is continuously sent to the controller. To this end, the API employs control messages.

3.4.2.3 Northbound API

The coordinator flow control uses a northbound API to communicate the SDN controller with the application plane. To this end, the northbound API employs control messages that are encapsulated in TCP packets. This API continuously updates the routing table's contents with the routes built by the RPL and registers the optimized routes in the SDN flow table with the RL agent's decisions. The control messages implementation, which dictates how the data and application planes handle controller communication, is explained as follows.

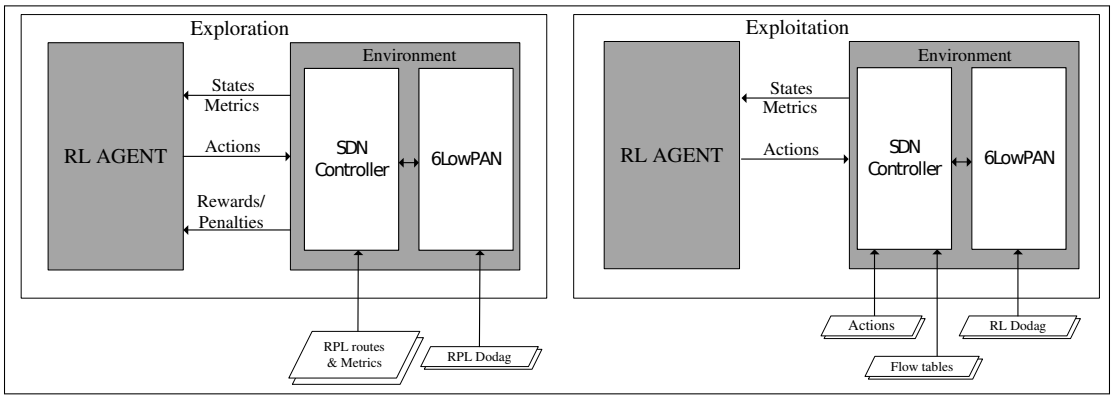


Figure 3.4 RL model

3.4.2.4 Control messages implementation

In the control plane, the coordinator flow control determines four control messages, i.e. *node-mod*, *info-get*, *flow-mod*, and *packet-in*. Accordingly, the control messages are categorized depending on the process to which they are associated. *Node-mod* and *info-get* are utilized for topology discovery and optimization applications, while *flow-mod* and *packet-in* are employed toward for flow control. These messages operate depending on the SDN core applications' demand. Initially, as shown in Fig. 3.5, the northbound API initiates a node-mod message from the RPL-based topology discovery application to the control plane to determine the network

topology, requesting a notification every time a new node is identified. Once the notification is received, the control plane transmits info-get through the southbound API to obtain the discovered node's neighbors and the respective wireless links' quality. Subsequently, the northbound API records the RPL routes in a routing table. After that, the RL-enabled topology optimization is executed, optimizing the routes based on the data collected from the topology discovery-based RPL application. Consequently, the northbound API registers the optimized routes in the SDN flow table. Afterwards, the coordinator flow control sends an Info-get message to the data plane to instruct the nodes to send back a notification when they receive packets that do not match any entry in the flow table.

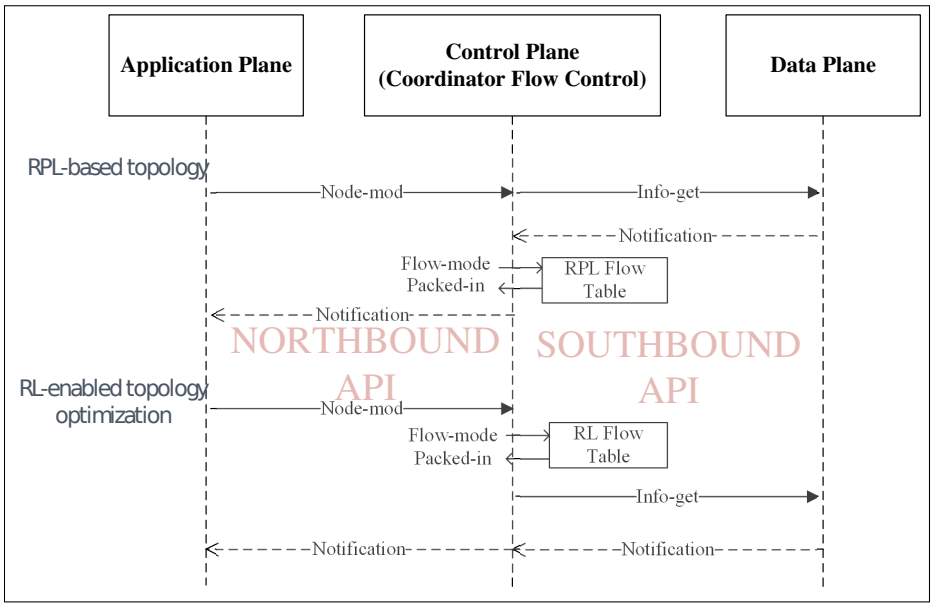


Figure 3.5 Control message sequence diagram

It is worth mentioning that the Flow-mod message is used to insert and remove entries from flow tables, and to establish flows according to the SDN application's purpose. The SDN core applications can also request the controller to send an info-get whenever the applications need information from the IoT nodes. The control message structure is summarized in TABLE 3.2.

Table 3.2 Control messages

Message	Method	Observe	Process
node-mod	GET	Required	Topology discovery, Topology optimization
info-get	GET	Optional	Topology discovery, Topology optimization
flow-mod	PUT	Required	Flow control
packet-in	GET	Required	Flow control

Accordingly, our approach's flow tables are composed of two fields, i.e., match and action. The match field records the incoming packet header's features distinguishing the corresponding flow, whereas the action field records the operation for a matching packet, as illustrated in Table 3.3 (Miguel *et al.*, 2018a). Moreover, a set of attributes related to the standard SDN flow table entries is included in the match field.

Table 3.3 Flow table entry match fields

Match	Length(Bits)	Description
ipv6src	128	IPv6 source address
srcmask	8	Mac source address)
ipv6dst	128	IPv6 destination address
dstmask	8	Mask destination address
srcport	16	Source port
dstport	16	Destination port
ipproto	8	IP protocol (UDP, TCP, ICMPv6)

3.4.3 SDN application layer

In the SDN application layer, the core applications are performed. The SDN engine performs the integration with the SDN controller.

3.4.3.1 RPL-based topology discovery

Since, the SDN controller needs to have a unified view of the SD6LowPAN and the neighbors that each node sees, including the quality of the wireless links connecting them, a network discovery protocol is mandatory. In this context, this scheme employs the RPL protocol in non-storing mode. In this mode, the routing table entries are maintained only on the controller to ensure that the IoT nodes always attempt to find a path to the controller.

3.4.3.2 RL-enabled topology optimization

In this work, we consider a route optimization approach that aims to find an adaptive QoS-aware forwarding policy by applying an RL technique to allow each node to learn the proper forwarding rate to cooperate in the routes optimization process. This application's main objective is to minimize energy consumption, packet delivery ratio, and end-to-end delay caused by the Rank attack, thus preventing the latter from overwhelming the SD6LowPAN.

3.4.4 RL Model

The RL model consists of two main entities: the agent and the environment, as shown in Fig. 3.4. The agent is a quick learner who can make decisions according to its learning experiences and the environment is an anonymous entity that affects the performance of the agents. In the proposed solution, the agent lacks knowledge of the environment. Therefore, a model-free like State Action Reward State Action [SARSA], a well-known temporal difference [TD] algorithm, is adopted (Lin *et al.*, 2016a). SARSA is an iterative dynamic programming algorithm to find the optimal solution based on a limited environment. It is worth mentioning that SARSA has a faster convergence rate than Q-learning and is less computationally complex than other RL

algorithms (Habib, Khan & Uddin, 2016a). Also, since our environment is resource-constrained and limited by the number of nodes per DODAG (30), different deep reinforcement learning algorithms such as Deep Q-Learning [DQL] and Deep Deterministic Policy Gradient [DDPG] are not considered in this paper, where we leave their integration in our scheme and test in a real IoT testbed for future work.

In particular, in the proposed scheme, the state is the current node, and the action is the link to follow to reach a neighboring node. Specifically, at each node, following the link to each neighbor, the agent has to exploit past actions with great rewards and simultaneously explore the system for better unknown actions. In this context, there are three components for the RL agent's design: the action policy, the quality function, and the reward function. These components are detailed as follows:

3.4.4.1 Action selection policy

The action selection policy defines an agent's action selection, which correlates an action to a state. This function evaluates the trade-off between action exploitation and exploration to maximize the reward value. Accordingly, the agent explores the state space in an unknown environment. To this end, in our proposed routing model, we consider the Boltzmann softmax policy (Iwata, 2016a), where the probability $\pi_t(s_t, s_a)$ of choosing an action a_t given the current state s_t is given by

$$\pi_t(s_t, s_a) = \frac{\exp(Q_t(s_t, a_t)/\tau_n}{\sum_{b=1}^{n} \exp(Q_t(s_t, b_t)/\tau_n)}, \tag{3.1}$$

where n is the number of possible actions, $Q_t(s_t, a_t)$ is the corresponding quality function, and τ_n is a temperature control. The temperature control measures the trade-off between exploration and exploitation. As a result, if this parameter obtains high values, all actions are reasonably probable (i.e., exploration). In contrast, low values sustain the action with the maximum quality (i.e., exploitation), which causes the policy to tend to a greedy one. Therefore, in highly dynamic

environments τ_n should be set to a high value while it should decrease to a low value in static environments. In this context, to guarantee a learning convergence on limited time, temperature control is set to a linear function of the time and is expressed by

$$\tau_n = -\frac{(\tau_0 - \tau_T)n}{T} + \tau_0 \qquad n \leq T, \tag{3.2}$$

where T denotes the time to reach the convergence, and τ_0 and τ_T are the initial and last value at time T of the temperature control, respectively.

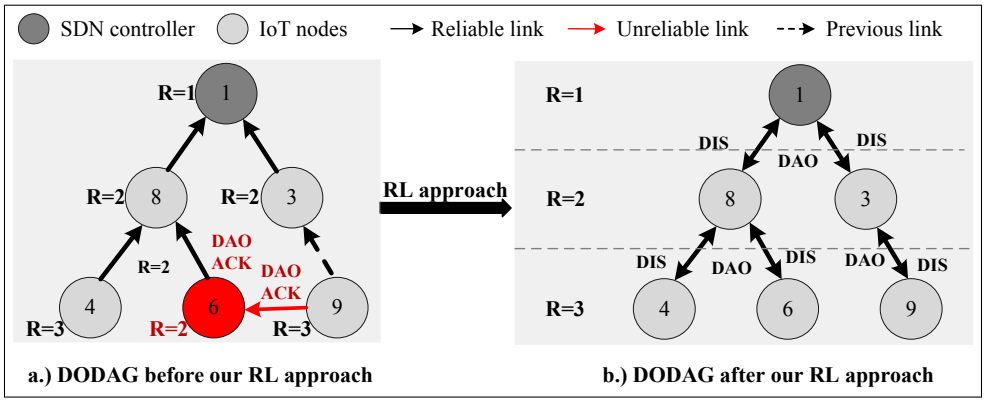


Figure 3.6 DODAG instance before and after the proposed RL approach

3.4.4.2 Quality function

The quality function estimates the quality that can be achieved by the possible next system state, which can be determined by the agent based on the state and action. Significantly, in this paper, the quality function $Q_{t+1}(s_t, a_t)$ relies on SARSA, as mentioned above, where the agent at time $t + 1$ applies the action and the state to update the quality value. Indeed, SARSA uses the expected quality value, taking into account how likely each action is under the current policy, which indicates that the agent can utilize the future reward earned, rather than considering the optimal action with the highest reward (Erdol, Gormus & Aydogdu, 2017) as follows:

$$Q_{t+1}(s_t, a_t) = Q_t(s_t, a_t) + \alpha[R_t + \gamma Q_t(s_{t+1}, a_{t+1}) - Q_t(s_t, a_t)], \tag{3.3}$$

where $\gamma \in [0, 1]$ is the discount factor that defines the purpose of future rewards, $\alpha \in [0, 1]$ is the learning rate that represents the override measure of the recently acquired information to the past one, and R_t is the reward at time t. As a consequence, in Eq. (3.3), the agent updates the quality value based on the maximum potential quality value among the actions. Concretely, the agent selects and takes action for the current state s_t through the action selection policy. Accordingly, the agent observes R_t and the state s_{t+1} and updates the Q function.

Table 3.4 QoS requirements. Taken from (Shu *et al.*, 2016a)

Traffic type	Application	QoS
Classic	Telnet, FTP	Delay, losses
	HTTP, FTP	Delay, Throughput
	STMP,POP3,IMAP	Losses
	TELNET	Losses
Real-time	Multimedia	Delay, Throughput
	Control messages	Delay

3.4.4.3 Reward function

In this section, we recommend a reward function based on the network QoS requirements that are linked with the design of our route optimization approach. Specifically, the RL agent discovers the routing path with the highest QoS-aware reward based on the types of traffic and user applications. Precisely, TABLE 3.4 summarizes the QoS requirements and traffic type of several applications (Shu *et al.*, 2016a). For example, classic and real-time traffic adapts the packet transmission rate and has significant QoS awareness. For this purpose, the reward function is evaluated as

$$R_t = -g(a_t) + \beta_1(\text{ delay}_{i,j} + \text{queue}_{i,j}) + \beta_2 \text{PLR} \tag{3.4}$$

This indicates that the system at state s_t, using an action a_t, forwards packets from node i to node j. In Eq. (3.4), $g(a_t)$ indicates the cost to take action at time t, and $\beta_1, \beta_2 \in [0, 1]$ are the weights values determined by the QoS requirements of the packet flow. Unfortunately, one of the significant concerns with RL algorithms is that, as the agent iterative estimates the action values, the initial stages' learning process is extensively random exploration, which might affect the network performance. Therefore, since this work's primary purpose is to prevent Rank attacks from overwhelming the performance of SD6LowPANs, we introduce an exploration strategy that incorporates QoS aware functions in the action selection process to guide the learner agent, especially in the initial stages of the learning process (Tatsis & Parsopoulos, 2020), avoiding excessive consumption of resources.

Since the impact of doing an action mainly relies on the QoS aware functions, the cost g is equal to a constant value over all the actions. The QoS provisioning functions are defined as

$$\text{delay}_{i,j} = \frac{2}{\pi} \arctan\left[d^l_{i,j} - \frac{\sum_{k=1}^{A(i)} d^l_{i,k}}{A(i)} \right] \tag{3.5a}$$

$$\text{queue}_{i,j} = \frac{2}{\pi} \arctan\left[d^q_{i,j} - \frac{\sum_{k=1}^{A(i)} d^q_{i,k}}{A(i)} \right] \tag{3.5b}$$

$$\text{PLR} = (100 - \text{PDR}) \tag{3.5c}$$

where $d^l_{i,j}$ and $d^q_{i,j}$ are the link transmission and packet queueing delays from node i to node j, respectively. $A(i)$ is node i's number of neighbors in the DODAG, and PLR characterizes the packet loss from node i to the controller. Eq. (3.5a) estimates the link delay of link $i - j$ compared to other possible next hops, Eq. (3.5b) includes the queueing delay while accounting

for the average delay over the DODAG, and Eq. (3.5c) represents the Packet Loss Ratio [PLR], which shows the performance of the protocol in terms of percentage of Packets Delivery Ratio [PDR], i.e. the packets successfully delivered to the controller (Musaddiq, Zikria, Kim et al., 2020a).

3.4.5 Intrusion prevention algorithm

As shown in Fig. 3.6 this architecture consists of several IoT nodes connected to a border router that plays the role of a lightweight SDN controller. In this reference frame, the SDN controller gathers the routing paths and the global state of the network with the aid of RPL. Consequently, a Rank attack is performed over an existing node in the network, affecting node six, which alters its rank from R=3 to R=2, and the ETX announced in the DIO message that is lower than the minimum perceived between neighbors. Hence, node nine selects node six as its parent instead of node 3, affecting the entire network's performance.

Subsequently, the SDN controller is in charge of path computation based on the network state received for each incoming route path. After that, a new DODAG is created with an optimized path based on the continuously received control messages, where node three is selected instead of node six as parent node to node nine. Hence, through our RL approach, the controller dynamically optimizes the best data flow routes according to the QoS requirements and dynamic traffic patterns, and sets up the routing tables of the border router along the optimal path via the SDN controller, thus enabling high security while providing efficient data transmissions and superior link utilization (Tuncer, Charalambides, Clayman & Pavlou, 2016a; Moreira, Kaddoum & Bou-Harb, 2018c; Miranda, Kaddoum, Bou-Harb, Garg & Kaur, 2020a). It is worth mentioning that the resulting optimized paths could be different from those of DODAG without the Rank attack before applying our RL approach. In Fig. 3.6, we assume a representation of the possible optimized paths recovered by our RL approach. However, in the experimental results section, we validated the optimization of DODAG paths based on some performance metrics analysis. The intrusion prevention algorithm is summarized in two procedures that are explained in detail in Algorithms 3.1 and 3.2.

Algorithm 3.1 Intrusion prevention algorithm

1: *Flow f arrives to the controller C_f in the DODAG;*
2: *Set of paths and NS are in introduced in C_f;*
3: *QoS requirements are configured in C_f;*
4: *The QoS provisioning functions are calculated in C_f;*
5: *C_f executes Algorithm 2;*
6: *Set of optimized paths are stored in the flow table;*
7: *The flow is forwarded following the flow tables in C_f;*

Algorithm 3.2 RL agent

1: *Initialize $Q_0(S_0, a_0) = 0$ and R_0 from Eq. 3.3;*
2: *At time t:*
3: *Choose next-hop using softmax in Eq. 3.1;*
4: *Observe R_t and s_{t+1};*
5: *Update Q_{t+1} function using Eq. 3.4;*
6: *update t = t+1;*
7: *Continue from step 3 to choose next-hop;*
8: *Exit;*

First, when a flow (f) appears at controller C_f, it demands the forwarding path, and the controller refreshes the current Network State (NS). Accordingly, the QoS requirements are configured in C_f and the QoS provisioning functions are computed. Subsequently, C_f exploits Algorithm 3.2 to select a possible path with regard to the QoS requirements of the flow. Consequently, C_f stores the forwarding tables of the IoT nodes along with the optimized path in the flow tables.

3.5 Simulation Setup and Experimental Results

In this section, we start by presenting the scenarios, network parameters, assumptions, and metrics used in the evaluation. Afterwards, we go through the experimental results and the corresponding analysis.

3.5.1 Simulation Setup

We assume the composition of one DODAG with multiple sets of paths, one SDN controller, one control channel, and a real-time network state.

To measure the impacts of rank attackers on the Operating System [OS], we choose an open-source OS namely Contiki OS, designed for resource-constrained devices (Tanganelli, Virdis & Mingozzi, 2019a). The benign nodes were placed at different locations and circle around a malicious node as shown in Fig. 3.6. Here node 1 is the SDN controller/border router in SD6LowPAN. The network parameters used in the simulations are listed in TABLE 3.5, and nodes characteristics are mirrored according to the EXP5438 platform with TI MSP430F5438 CPU and CC2420 radio.

Table 3.5 Network Parameters

Parameter	Value
Simulation runtime	3600s
MAC layer	ContikiMAC
Objective function	MRHF, ETX
Number of IoT nodes	30
Transmitting nodes	All
Receiving node	Root/Controller
Link quality	90%
Radio medium	UDGM
RPL mode	Non-Storing
Sending rate	1 packet every 10 sec
Number of attacking nodes	1
TX range	100 m
Interference range	0-30m
Packet size	50 Bytes
SDN update period	180s
SDN flow table lifetime	10min
Initial latency	60 ms
Maximum number of hops	5

We measure the results of the experiment with the following performance metrics.

- Average Packet Delivery Ratio [PDR]: This is the ratio between the number of packets sent to the destination and the number of packets received by the destination.
- Average end-to-end Delay [Delay]: This refers to the time to transmit a packet over the network from the source to the destination.
- Radio Duty Cycle [RDC]: This is the energy consumed by an IoT node considering the time it spends in the following states: listen, receive [Rx], and transmit [Tx]. In other words, it is the ratio between the time spent by a node in those three states and in wake-up state.

3.5.2 Experimental Results

This section analyzes the results obtained from the experiments conducted using the Cooja simulator testbed for Contiki OS (Tutunović & Wuttidittachotti, 2019). To this end, we consider a low-power wireless network composed of 30 IoT nodes where 29 are benign and 1 is considered malicious. The network is deployed in a simulated outdoor area.

It is worth mentioning that the results are obtained considering a static scenario in which there are no wireless nodes. However, we emphasize that our testbed is deployed in a dynamic wireless environment. Thus, our testbed's radio channel conditions are susceptible to changes due to interference (e.g., from other 802.15.4 and 802.11 radios), where this interference is time-varying. Further, the underlying MAC protocol is ContikiMAC (Ali, Ishak, Zawawi, Seman, Bhatti & Yusoff, 2020). To better illustrate the proposed solution's performance better, we first demonstrate the performance evaluation of our RL approach; afterward, a comparative scenario analysis is presented.

3.5.2.1 Performance analysis of our RL approach

Initially, we analyze our RL approach's performance to determine the best configuration settings to minimize the Delay and RDC while maximizing the PDR. To this end, we present the training phase as follows.

3.5.2.1.1 Training Phase

It is essential to mention that the RL model's training is made offline to record the first flow table; after that, the model delivers the optimized routes online. Since this work aims to prevent Rank attacks' harmful effects based on network QoS metrics continuously received by the control plane, to train the model, we select the step size parameters (α,γ).

These parameters govern the RL agent's performance, as defined in Eq. (3.3). Precisely, α adjusts the error in the Q value update; $\gamma \epsilon$ [0, 1) takes a value of zero if the routing estimates the current reward and acts like a greedy algorithm, and a value close to one if the routing takes the long-term revenue. As we consider the long-term revenue to be significant, for this experiment, we set the value of γ to 1. Moreover, we set the number of episodes to 1000, and each episode contains 100 steps.

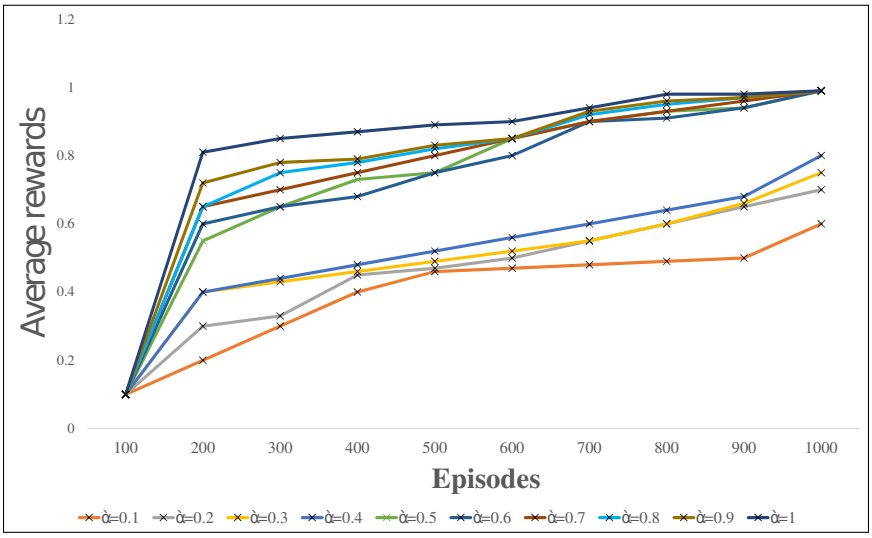


Figure 3.7 Learning process with respect to the number of episodes vs. the average reward in the proposed approach.

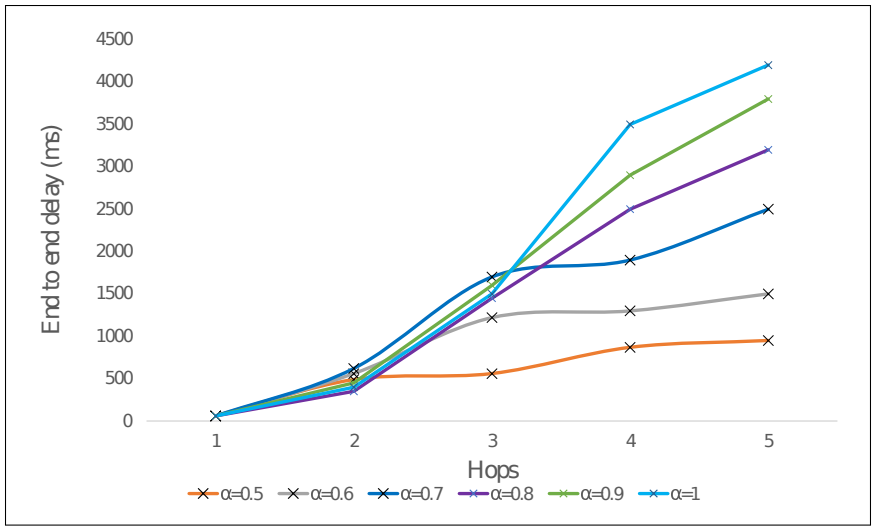


Figure 3.8 Delay-An illustrative comparison of our approach using $\alpha \in$ (0,5-1)

The results shown in Fig. 3.7 demonstrate that our RL approach learns to reach a reward of 99% when the step size converges between 0.5 and 1 with a number of episodes of 1000. Hence, to analyze the Delay, RDC, and PDR, we vary the learning rate α from 0.5 to 1 with 1000 episodes. Additionally, $g(a_t)$ is set to 0.5 and the QoS provisioning values $\beta_1 = 1$ and $\beta_2 = 0.5$. The QoS provisioning values indicate that a longer convergence time is required when considering the end-to-end link and queue delay in the experiments. Fig. 3.8 shows the number of hops of a suitable path through our RL agent for a given (α, γ). It shows that there exists a trade-off between algorithm convergence and end-to-end delay.

Therefore, the Delay increases with increases in the value of α. Additionally, the results demonstrate that when $0.5 \leq \alpha < 0.7$, with a number of paths between one and three hops, the Delay is higher than for other values of α. On the contrary, when $0.7 < \alpha \leq 1$ with paths with a maximum of 2 hops, the Delay is lower than for other values of α. This means that the smaller the network's size, the lower the latency when the value of α is greater than 0.7.

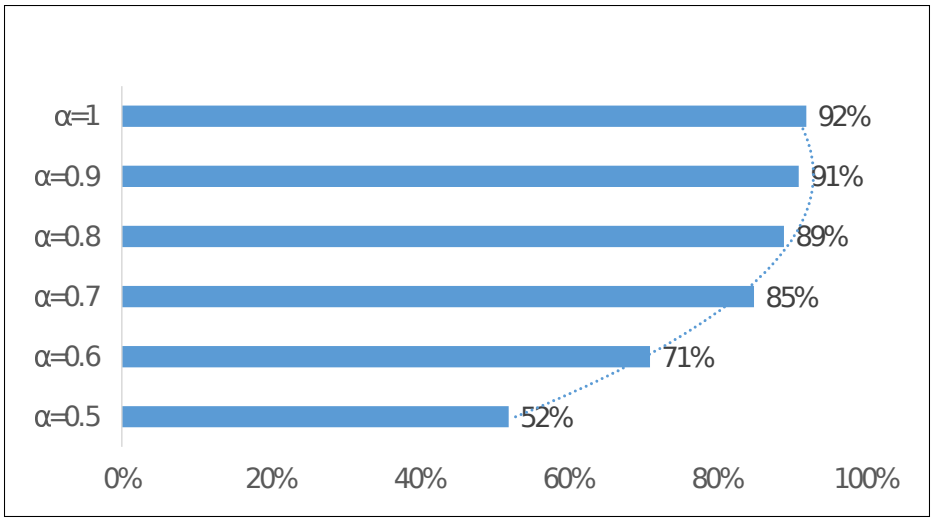


Figure 3.9 PDR-An illustrative comparison of our approach using $\alpha \in (0,5\text{-}1)$

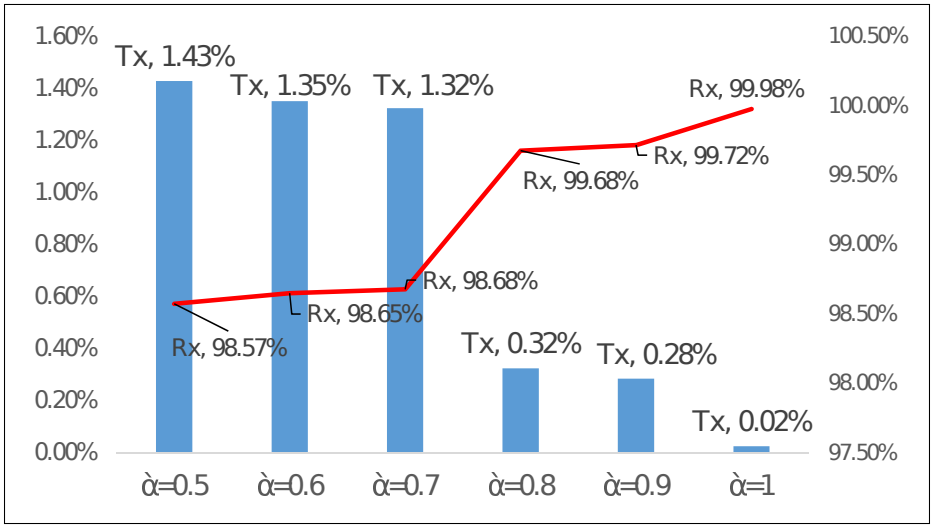


Figure 3.10 RDC-An illustrative comparison of our approach using $\alpha \in (0,5\text{-}1)$

Moreover, in Fig 3.9, the results reveal that the PDR exponentially increases when α increases, reflecting a significant decrement when α takes a value of 0.6 or 0.5. In Fig 3.10, the results illustrate that high values of α are associated with higher RX and lower TX in the network. Consequently, the energy consumption exponentially increases with the increase of α. Since IoT

nodes often have a small battery, measured in millivolts, extra power consumption can reduce the device's battery life by forcing the node to change its state to off.

Although, the condition $0.7 < \alpha \leq 1$ introduces the lowest Delay in small DODAGs, it is not suitable for our scenario because we consider a network with a maximum of 5 hops. Moreover, for $0.5 \leq \alpha < 7$ with paths created with more than 2 hops, the Delay is lower than for other values of α. However, there is a meaningful decrement in the PDR. Accordingly, to ensure a suitable analysis in terms of Delay, PDR, and RDC, we set the value of α to 0.7 in subsequent performance comparisons.

3.5.2.2 Performance comparison

In what follows, we compare the Delay, PDR, and RDC with the following four scenarios:

- **S1**: An RPL scenario with no SDN implementation under Rank attack.
- **S2**: An RPL scenario with SDN implementation without Rank attack.
- **S3**: An RPL scenario with SDN implementation under Rank attack.
- **S4**: An RPL scenario with our RL-based SDN approach under Rank attack (our approach).

3.5.2.2.1 Delay

In what follows, we analyze the delay of the four scenarios considering the path with the maximum number of hops. As a result, Fig. 3.11 demonstrates that in S1, the delay reaches 1600 milliseconds. Further, in S2, the latency in SD6LowPAN reaches 2950 milliseconds. As a consequence, the latency is 45.72% higher than in S1. This is because an additional overhead is introduced due to the messages exchanged from the controller to the data plane. In S3, the latency reaches 4400 millisecond, which is 63.63% and 32.95% higher than S1 and S2, respectively. This is due the Rank attack, requiring the data plane to navigate downwards along the RPL topology across multiple non-optimized paths. Furthermore, in S4, the results show that the latency reaches 2500 milliseconds, which is 56.81% lower than S3 and 15.25% lower than S2.

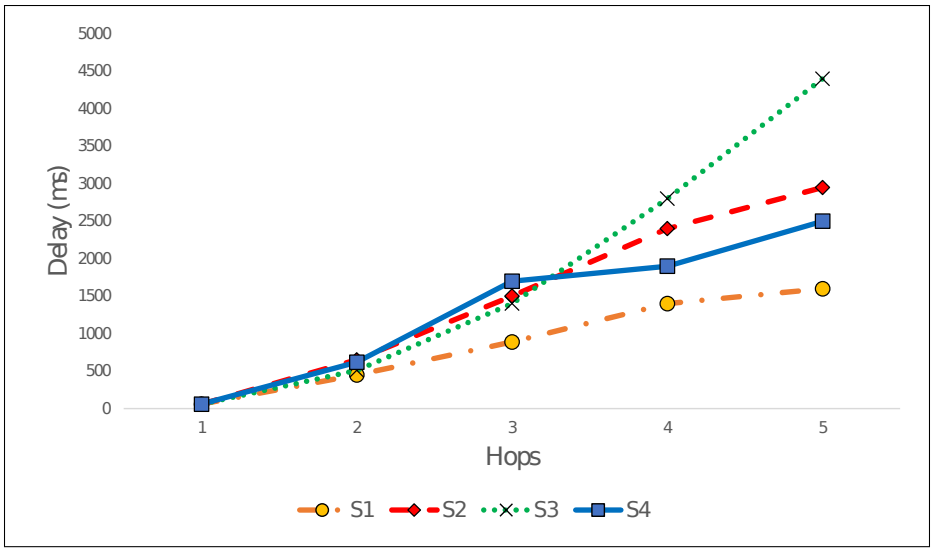


Figure 3.11 Delay-An illustrative comparison between S1,S2,S3, and S4

Although this scenario is 36% higher than the scenario where the SDN implementation is not used, the proposed solution restores and even optimizes the typical behavior in SD6LowPAN. This is because the number of SDN messages is decreased since the optimized paths are only delivered once the RL approach's exploration process is finished, rather than not every time the RPL collects data from the data plane. It is worth mentioning that our solution obtains the best results with DODAGs created with more than 3 hops.

3.5.2.2.2 PDR

In what follows, we analyze the four scenarios' PDR. To this end, we consider the path with the maximum number of hops and an average of 360 control packets delivered from the data plane to the controller. Consequently, the results illustrated in Fig 3.12, demonstrate that 151 packets were successfully delivered to the border router in S1. This means that this scenario reaches a PDR of 48%.

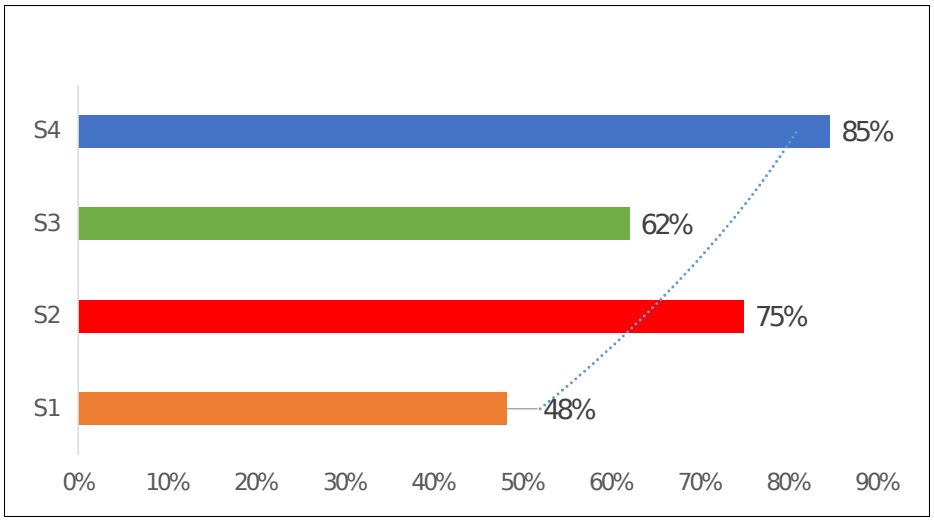


Figure 3.12 PDR-An illustrative comparison between S1, S2, S3, and S4

Further, in S2, the average delivery variation reaches 270 packets per second, reaching a PDR of 75%. This is 27% more than S1 because the SDN approach helps speed up the packets delivery. Subsequently, a SD6LowPAN under Rank attack introduces a packet loss ratio of 38%. Thus, this scenario reaches a PDR of 62% which is 13% lower than S2 and 14% higher than S1. Finally, in our method, the results demonstrate that the PDR reaches 85%, which is 23%, 10%, and 37% more efficient than S3, S2, and S1, respectively. This is because the RL optimization algorithm optimizes the network routes in SD6LowPAN.

3.5.2.2.3 RDC

In S1, as illustrated in Fig. 3.13, the Rx reaches 99.972% and Tx 0.028%. Meanwhile, in S2, the Rx reaches 99.902% and Tx 0.098%. As a result, this scenario consumes less energy than S1 because the centralized SDN architecture optimizes the power consumption by not overloading the data plane with continuous execution of the RPL. Subsequently, in S3, the Rx reaches 98.676%, and Tx is 1.324%. Therefore, this scenario introduce a higher duty cycle than S2 due to the Rank attack execution. Conclusively, in S4, the Rx is 99.432%, and Tx is 0.568%.

Consequently, this scenario consumes less energy than the third scenario restoring the excessive energy consumption introduced by the Rank attack.

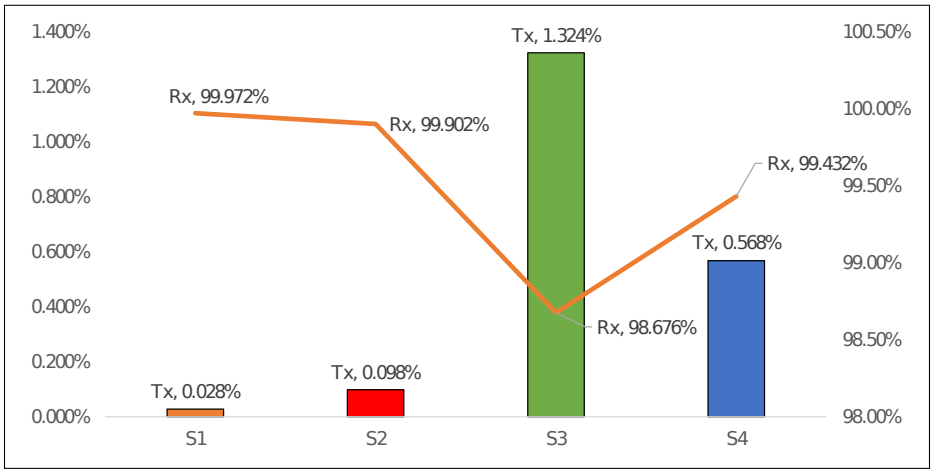


Figure 3.13 RDC-An illustrative comparison between S1, S2, S3, and S4

Although our approach introduces more latency than the other scenarios where the route consists of a maximum of 3 hops, the latency is decreased in the fourth and fifth hop due to the exploration of the RL agent's environment. Moreover, the proposed scheme provides better performance in packet delivery than S1 and S2 and restores the Rank attack's energy consumption in S3.

It is worth mentioning that since the results obtained demonstrate that our approach provides network performance efficiency, thus preventing rank attacks from overwhelming the constrained SD6LowPAN, we did not create more test scenarios, including more malicious nodes. To the best of our knowledge, the concept of a unified SDN-based intrusion prevention stack scheme, integrating RPL for fast network discovery and RL for route optimization to avoid ranking attacks, has never been attempted in any previous research works.

3.6 Conclusion

The core of our solution is the elaboration of a security preventive control that takes advantage out of programmability of SDN in 6LowPAN to build a self-learning agent that capture states

through flow tables and metrics collected from the control plane. The learning consists of optimizing RPL routing based on QoS metrics like delays and packet loss rate. The control plane and the application plane stack can be used into a wireless border router supporting 6LowPAN, introducing therefore a QoS awareness intelligence and avoid RPL rank attacks sensitivity. Such solution can be a support for 5G agnosticism with respect different wireless networks like 6LowPAN networks. To analyze the performance of the proposed scheme, we leverage Contiki Cooja. The results demonstrate that the proposed scheme satisfies the requirements of SD6loWPAN, provides low computational complexity, and considerably prevents ranking attacks, thanks to the introduction of the learning agent reinforcing the route optimization approach. As for future work, we will implement the proposed security scheme in an IoT-centric testbed.

Moreover, our research will explore the use of network slicing to tailor our approach for heterogeneous networks with the help of hierarchical SDN drivers distributed between the cloud and the edge. Such a deployment will promote decentralized decision making and introduces our solution in large-scale scenarios.

CHAPTER 4

QL VS. SARSA: PERFORMANCE EVALUATION FOR INTRUSION PREVENTION SYSTEMS IN SOFTWARE-DEFINED IOT NETWORKS

Christian Miranda[1] , Georges Kaddoum[2]

[1,2] Département de Génie Électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Article submitted to International Wireless Communications and Mobile Computing Conference (IWCMC), Marrakesh, Morocco, 2023

4.1 Abstract

The resource-constrained IPV6-based low power and lossy network (6LowPAN) is connected through the routing protocol for low power and lossy networks (RPL). This protocol is subject to a variety of attacks. This work specifically examines a routing attack called rank attack (RA). It presents a performance evaluation where model-free reinforcement-learning [RL] algorithms are leveraged to help the software-defined network (SDN) controller achieve a cost-efficient solution to prevent the harmful effects of RA. Experimental results demonstrate that the state action reward state action [SARSA] algorithm is more efficient than the Q-learning (QL) algorithm, facilitating the implementation of intrusion prevention systems (IPSs) in software-defined 6LowPANs.

4.2 Introduction

The massive deployment of low-powered IoT devices has exposed them to ranking attacks. These attacks have raised serious concerns about the strength of routing protocols. The RPL specifically builds acyclic graphs and applies an objective function (OF) for the selection of parents, along with the rank. RPL commonly implements two objective functions, the minimum rank with hysteresis objective function (MRHOF) and the objective function zero (OF0). Consequently, an adversary can accomplish this by misusing the rank property and infringing on the routing

protocol. Based on the analysis of vulnerabilities related to the rank property, RAs create non-optimal paths for all packets, which pass through malicious nodes and thus overwhelm the restricted 6LowPAN (Sahay, Geethakumari & Modugu, 2018b). To address RPL vulnerabilities, a new security service for preventing the misbehaving node from decreasing rank values is presented in (Mangelkar, Dhage & Nimkar, 2017a). The authors avoid RPL publishing an illegitimate reduced rank by generating a hash chaining using a random number chosen by the root node. Moreover, in (Boudouaia, Ali-Pacha, Abouaissa & Lorenz, 2020a), a challenge-response scheme is used to validate the authenticity of the nodes within a destination oriented directed acyclic graph (DODAG). In (Shin, Sharma, Kim, Kwon & You, 2017b), a secure and efficient protocol for route optimization is proposed. It includes steps for reliable route optimization and handover management, where mutual authentication, key exchange, perfect forward secrecy, and privacy are supported. Although essential works have been proposed in the literature to target RAs in 6LowPANs, these deployments are not satisfactory to simultaneously guarantee efficient intrusion prevention and low management complexity in low power IoT networks (Kamble, Malemath & Patil, 2017b). Additionally, heuristic algorithms such as ant colony optimization (ACO), swarm optimization, and artificial bee colony are practical and widely used approaches to find solutions to combinatorial optimization problems (Rajesh, Raajini, Rajan, Gokuldhev & Swetha, 2020b). However, they are limited by the high sample complexity required to reach a reasonable solution.

With the advent of 5G, SDNs have been deployed to facilitate simple programmability, quality of service (QoS) provisioning and fast routing configuration services over the 6LowPAN. In this context, this paper uses a software-defined 6LowPAN (SD6LowPAN) architecture (Charfi, Mouradian & Vèque, 2020b) to address the management complexity introduced by security solutions and control data plane forwarding in the 6LowPAN according to the SDN approach. In addition, an RL approach in the SDN application plane is proposed to achieve routing optimization for packet forwarding in order to address the vulnerable rank value and the weakness of RPL objective functions in 6LowPAN. However, it is well known that RL introduces a non-negligible overhead into the network. To tackle this concern, this paper presents a

performance evaluation where an RL-based QoS function using QL and SARSA algorithms is leveraged for routing optimization to prevent the harmful effects of RAs in SD6LowPAN. The novelty of the proposed work lies in devising and evaluating model-free RL algorithms to achieve a cost-effective IPS through route optimization in SD6LowPAN. The main contributions of this work are summarized as follows:

1. An RL-based IPS approach is proposed to optimize the RPL routing paths to prevent the harmful effects of RAs in software-defined low power IoT networks.
2. A performance analysis of the computational complexity of the QL and SARSA algorithms is provided.

Moreover, simulations showing the proposed method's effectiveness are executed by leveraging the Contiki Cooja tool. This remainder of this paper is organized as follows: Section II introduces the proposed solution's system model and intrusion prevention algorithm. Section III, details the performance evaluation. Finally, the paper is concluded in Section IV, where some future endeavors are also put forward.

4.3 System Model

To prevent RAs in SD6LowPAN and introduce intelligent application support to the SDN control plane, we introduce an RL agent into the application plane to interact with a lightweight SDN controller, namely, µSDN (Baddeley, Nejabati, Oikonomou, Sooriyabandara & Simeonidou, 2018b). The agent's objective is to optimize routing to avoid RA overwhelm the resource-constrained SD6LowPAN. The agent is a programmable asset that hooks into the control plane to decide on building routes. The agent and its interaction with the control plane constitute a stack supported by a border router for 6LowPANs. To this end, our work is focused on utilizing model-free RL algorithms such as SARSA and QL. Since this evaluation is based on the software-defined architecture, it comprises three layers, as shown in Fig. 4.1. At the bottom of the framework, the low-power IoT network is developed in the data plane. In the middle, i.e., the control plane, the µSDN functions are executed (Baddeley *et al.*, 2018b), and in the application plane, SDN applications are designed, as shown in Fig. 4.1. In what follows, we

provide a brief background on model-free RL and its main algorithms, such as QL and SARSA. Further, we present the impact of RAs on SD6LowPAN.

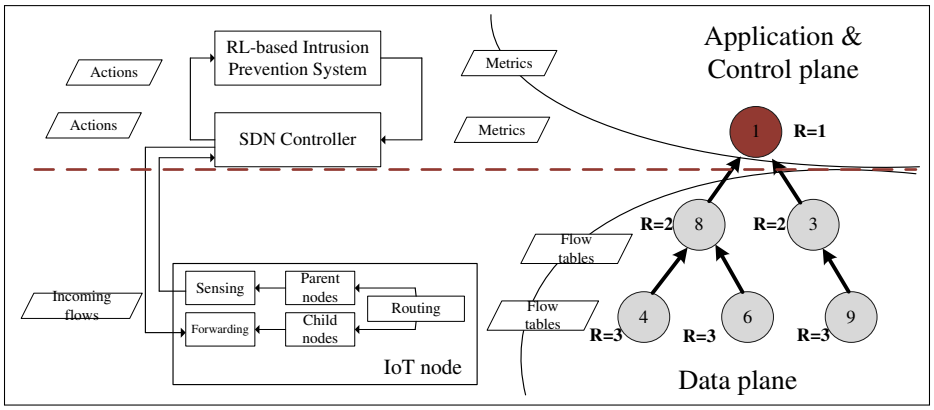


Figure 4.1 System model

4.3.1 Background

Since this work proposes an IPS-based RL approach to avoid RAs for low-power IoT networks, the basics concept underlying model-free RL algorithms are detailed in what follows.

4.3.1.1 Model-free RL methods

Practical RL applications generally deal with environments for which we do not have information on the underlying model. In such a situation, model-free RL algorithms are more appropriate. The most widely used approaches in this area are Monte Carlo and temporal difference (TD) learning (Mammeri, 2019a). TD learning and the Monte Carlo method are similar in that they both learn value functions directly from experience to obtain the optimal policy. However, contrary to with the Monte Carlo method, TD learning is a step-by-step method and does not need to wait for the agent to complete an episode and update its estimated value. In what follows, we introduce two well-known model-free RL methods: QL and SARSA.

4.3.1.2 The QL algorithm

The essence of the QL algorithm (Wang, Liu, Ma, Liu & Ma, 2020c) is to derive the estimated value of Q directly from the Bellman optimality equation. It is combined with the idea of TD learning, once we know the optimal action value $Q(s_t, a_t)$ corresponding to all possible actions a_t of state s_t of the next time step, we need only to select the action with the max action value according to the greedy policy. Subsequently, we can obtain the estimate of $Q(s_t, a_t)$ for the current time step from

$$Q_{t+1}(S_t, a_t) = Q_t(S_t, a_t) + \alpha[R_t + \gamma Q_t(S_{t+1}, a_t) - Q_t(S_t, a_t)], \tag{4.1}$$

where $\gamma \epsilon [0, 1]$ is the discount factor that defines the importance of future rewards, $\alpha \epsilon [0, 1]$ is the learning rate that determines the override measure of the newly acquired information to the old one, and R_t is the reward at time t.

4.3.1.3 The SARSA algorithm

Unlike QL, SARSA is an on-policy TD algorithm that learns the Q values based on the action performed by the current policy. The SARSA algorithm differs from the QL algorithm by the way it sets up the future reward. In SARSA, the agent uses the action and the state at time $t + 1$ to update the Q-value as follows (Wang, Yao, Wang & Jornet, 2020a):

$$Q_{t+1}(S_t, a_t) = Q_t(S_t, a_t) + \alpha[R_t + \gamma Q_t(S_{t+1}, a_{t+1}) - Q_t(S_t, a_t)], \tag{4.2}$$

4.3.2 Impact of Rank attack

Rank information is used to select the parent set and the preferred parent according to the rank rule, which states that the parents' rank always has to be smaller than the child's rank, and the preferred parent should be the parent with the best rank. The malicious node is programmed to compromise the rank rule so that instead of choosing the best node for its preferred parent,

it determines the worst one. As depicted in Fig. 4.2, the neighboring nodes of the attacker (compromised) node nine selects node six as their new preferred parent because it changes its rank from R=3 to R=2 and the ETX announced in the DIO message is lower than the minimum perceived between neighbors. As a result of such ranking misuse, new non-optimal links are considered (depicted by a red line in Fig. 4.2), which implicitly impacts network performance.

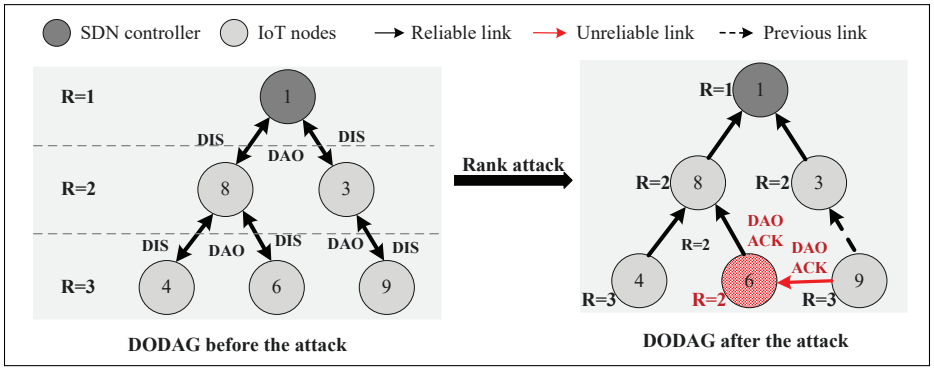


Figure 4.2 DODAG instance before and after an RA

4.3.3 RL Model

The SD6LowPAN RL life cycle consists of two phases as shown in Fig. 4.1. In the first phase, the agent enters an exploration stage to explore potential states and actions to optimize routing in SD6LowPAN networks. The second phase consists of deploying the agent and entering the exploitation phase, where the agent engages the SD6LowPAN control plane, where actions are triggered to decide on the routing of uplink packets. By adding or removing links from the DODAGs, the agent can return to the exploration phase to enforce its routing optimization again. In the proposed scheme in particular, the state is the current node, and the action is the link to follow to reach a neighbor node. Unfortunately, one of the significant concerns with RL applications is that since the agent iterative estimates the action values, the initial stages' learning process is extensively random exploration, which might affect network performance. To address this concern, we introduce an exploration strategy that incorporates a QoS provisioning

function in the action selection process to guide the learner agent (Wang *et al.*, 2020c) and avoid excessive consumption of resources.

4.3.3.1 QoS provisioning function

For a given update on node i within a DODAG, the action selection policy is made based on QoS provisioning delay on transmission and packet loss on link (i, j). QoS provisioning is calculated based on how a metric value compares to potential parent candidates' average. For nodes i, j, the gauging is done on range $[-1, 1]$ through arctan normalization, which is maintained as a parent or selected as a new parent from the set of neighboring nodes. The QoS provisioning function is computed as follows:

$$\text{delay}_{i,j} = \frac{2}{\pi} \arctan \left[d^l_{i,j} - \frac{\sum_{k=1}^{A(i)} d^l_{i,k}}{A(i)} \right], \tag{4.3}$$

where $d^l_{i,j}$ and $d^l_{i,k}$ are the link transmission and packet queueing delays from node i to node j, respectively. $A(i)$ is node i's number of neighbors in the DODAG. Eq. (4.3) estimates the link delay of link i, j compared to other possible next hops.

4.3.3.2 Reward function

The reward function is based on the QoS provisioning function and is meant to measure the reward behind choosing an action for route optimization. The RL agent discovers the uplink routing path with the highest QoS-aware reward. For this purpose, the reward function is evaluated as follows:

$$R_t = -g(a_t) + \text{ delay}_{i,j} \tag{4.4}$$

This indicates that the system at state s_t, using an action a_t, forwards packets from node i to node j. In Eq. (4.4), $g(a_t)$ indicates the cost to take the action at time t. Since the impact of

doing an action mainly relies on QoS-aware functions, the cost g is equal to a constant value over all the actions.

4.3.4 Intrusion Prevention-Based RL

Intrusion prevention-based RL relies on the states capture interface, which receives ground truth from the control plane and the RL agent, implementing the self-learning recursive process. The interface component receives flow tables and metrics indexed by existing node in the observed DODAGs. As depicted in Fig. 4.2, an RA affecting node nine occurs and changes its parent from node three to node six. Then, our RL approach is executed in the SDN controller, which is in charge of path computation based on the network states (NS) received for each incoming route path. After that, a new DODAG is created with an optimized path based on the continuously received control messages, where node six is selected instead of node three as parent node to node nine. The intrusion prevention algorithm is summarized as follows:

Algorithm 4.1 Intrusion prevention algorithm

1: *Flow f arrives to the controller C_f in the DODAG.*
2: *A set of paths and NS are introduced in C_f.*
3: *QoS requirements are configured in C_f.*
4: *The QoS provisioning function is calculated in C_f.*
5: *C_f executes the RL agent.*
6: *A set of optimized paths are stored in the flow table.*
7: *The flow is forwarded following the flow tables in C_f.*

First, when flow f arrives at controller C_f, it requests the forwarding path and the controller updates the current network state. Then, the QoS requirements are configured accordingly in C_f, and the QoS provisioning function is computed. Subsequently, C_f uses algorithm 6.1 to select a possible path with regard to the QoS requirements of the flow. Lastly, C_f stores the forwarding tables of the IoT nodes along with the optimized path in the flow tables.

4.4 Performance Evaluation

This section analyzes the results obtained from the experiments conducted using the Cooja simulator testbed for Contiki OS (Simha, Mathew, Sahoo & Biradar, 2020a). The environment was created with one DODAG having multiple paths, one SDN controller, one control channel, and a real-time network state. Our low-power wireless network was composed of 30 IoT nodes deployed in a simulated outdoor area. It is worth mentioning that the results are achieved considering a scenario in which there are no mobile nodes. However, our testbed was deployed in a dynamic wireless environment. Hence, our testbed was susceptible to changes in radio channel conditions due to interference (e.g., from other 802.15.4 radios and 802.11 radios), where this interference is time-varying. Furthermore, the underlying MAC protocol is ContikiMAC. The network parameters used in the simulations are listed in TABLE 4.1, and node characteristics are reflected according to the EXP5438 platform with TI MSP430F5438 CPU and CC2420 radio.

Table 4.1 Network Parameters

Parameter	Value
Simulation runtime	3600000 ms
Objective function	mrhf, ETX
Number of sensor nodes	30
Link quality	90%
RPL mode	Non storing
Sending rate	1 packet every 10 s
Number of attacking nodes	1
TX range	100 m
Interference range	0-30 m
Packet size (excluding header)	50 Bytes
Initial latency	60 ms
Maximum number of hops	5

In what follows, we analyze the performance of the proposed solution in comparison with the following scenarios: S1 - A RPL scenario with SDN implementation without RA, S2 - A RPL scenario with SDN implementation under RA, and S3 - A RPL scenario with an RL-based SDN approach under RA.

4.4.1 Off-Policy vs On-Policy

In this section, we compare on-policy and off-policy control algorithms. Let us take QL (off-policy) and SARSA (on-policy) as examples. To this end, we present the training model as follows.

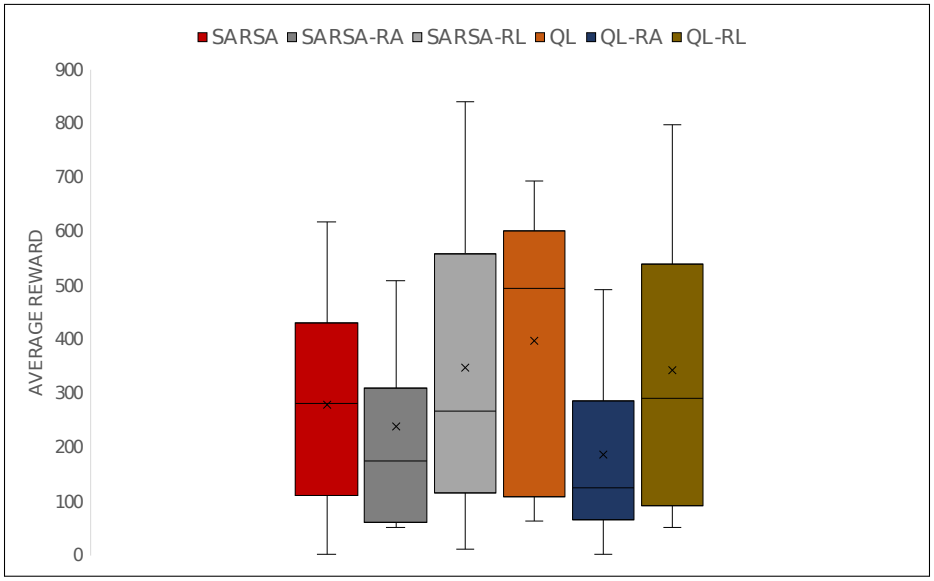


Figure 4.3 Average reward of QL and SARSA under scenarios 1, 2, and 3 with respect to different episodes

4.4.1.1 Training model

The step size parameters (α,γ) govern the performance of the RL agent, as defined in Eq. (4.1,4.2). More precisely, α adjusts the error in the Q value update and $\gamma \epsilon$ [0, 1) takes a value of zero if the routing estimates the current reward and acts like a greedy algorithm or a value close to one if the routing takes the long-term revenue. Since we consider the long-term revenue to be significant, we set the value of γ to 1 for this experiment. Let the agent perform 100 episodes and operate for a total of 100000 steps. Based on the results presented in (Lin, Akyildiz, Wang & Luo, 2016b), we set the value of α to 0.7, which is suitable for IoT networks with a maximum of 5 hops. It is worth mentioning that since this work aims to prevent the harmful

effects of RA based on network metrics continuously received by the control plane, the step size parameters (α,γ) are still selected whether the model is trained online or offline.

As shown in Fig. 4.3, by averaging over 100 runs, when the algorithms tend to converge in S1, QL's performance indicates that the episodes' average reward is 11% better than that of SARSA. This is because SARSA searches for the optimal path, whereas QL searches for the shortest one. On the contrary, in S2, both algorithms present a decrement in their episodes' average reward. However, QL demonstrates 29% worse average reward than SARSA does. This is because the entire network's performance has been affected by the RA, which interferes with QL's shortest path method. Moreover, SARSA's optimal path approach helps to mitigate the negative effects of the rank attack. In S3, SARSA's optimization approach provides 5% better performance than QL. This is because the QoS provisioning function used in the RL approach diminishes the gap existing between SARSA and QL when the algorithm converges to 100% of the episodes.

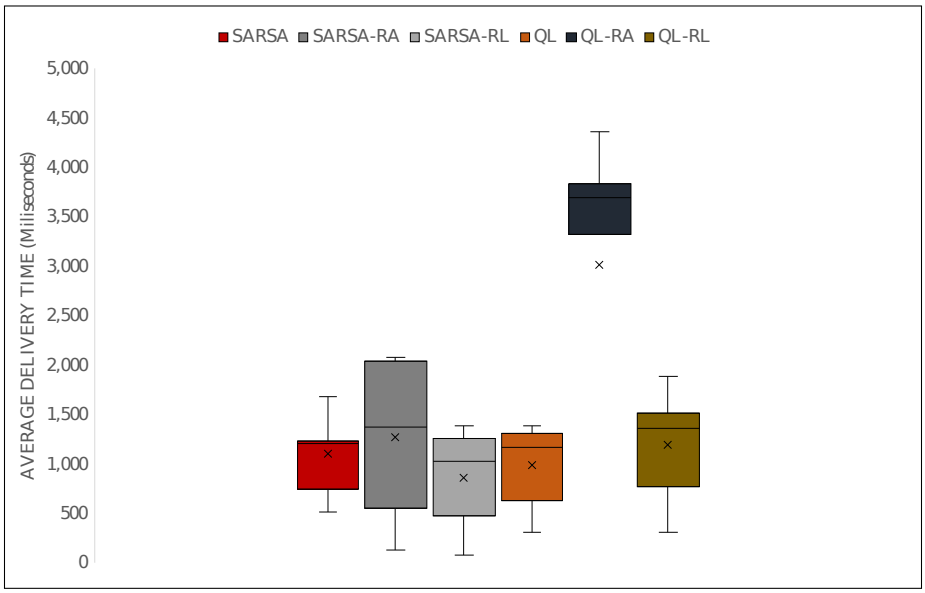


Figure 4.4 Average packet delivery time of QL and SARSA under scenarios 1, 2, and 3 with respect to different episodes

Fig. 4.4 illustrates that when it comes to the length of the time step used during the episodes, in S1, QL has a significantly shorter time step than SARSA, which means that QL finds shorter

optimal paths than SARSA does. Moreover, in S2, network performance using QL is affected by RA and reaches 317% of its S1 value, whereas network performance using SARSA increases 21% in comparison to S1 but remains far less than QL's value, which means that QL is more affected by the non-optimal routes created by the RA. In S3, QL restores the performance obtained in S1, but SARSA delivers the packets 73% faster than QL. SARSA also improves on its performance obtained in S1. Furthermore, Fig. 4.4 demonstrates that in S1, QL delivers an average of 65 packets after the run of 100% of the episodes, whereas SARSA delivers 76 packets, which means that SARSA is 14% more effective in packet delivery than QL. In S2, network performance is affected by the RA for both algorithms , with packet delivery impacted by 50% after the episodes' execution. In S3, SARSA restores and improves on average packet delivery, reaching 107 packets. On the contrary, QL reaches 76 packets after the implementation of the episodes, which means that SARSA is 71% more efficient in packet delivery than QL.

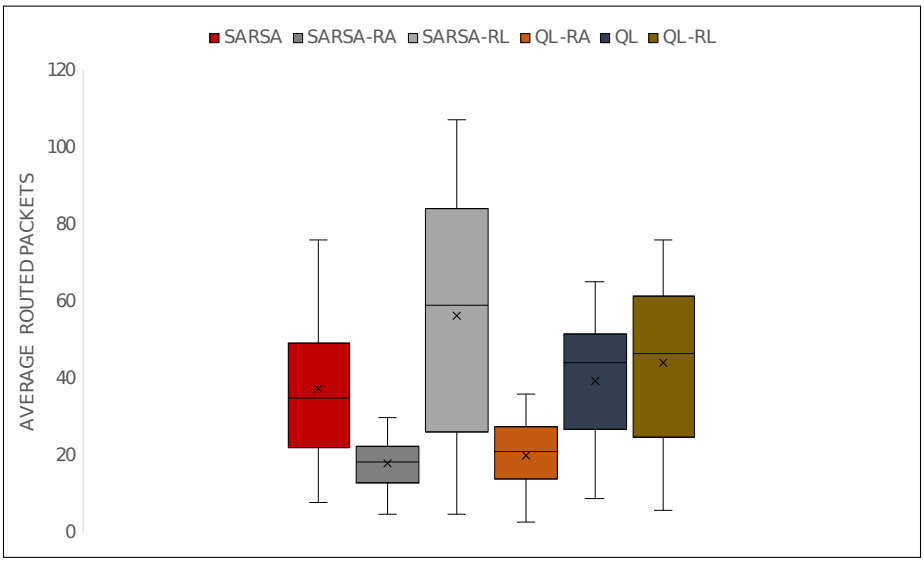


Figure 4.5 Average number of routed packets of QL and SARSA under scenarios 1, 2, and 3 with respect to different episodes

4.5 Conclusion

An intrusion prevention-based RL solution to avoid RAs for software-defined low-power IoT networks is proposed in this paper. This solution combines the advantages of software-defined networks with routing optimization using an RL approach. We leveraged Contiki Cooja to analyze the performance of the RL algorithms. The results demonstrate that the SARSA-RL approach provides considerably better performance than the QL-RL approach and prevents the harmful effects of RAs. As for future work, our research will analyze the use of deep reinforcement algorithms for intrusion prevention systems for software-defined IoT networks.

CHAPTER 5

SD6LOWPAN SECURITY: ISSUES, SOLUTIONS, RESEARCH CHALLENGES AND TRENDS

Christian Miranda[1] , Georges Kaddoum[2]

[1,2] Département de Génie Électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Article submitted in IEEE IoT Magazine, January 2023.

5.1 Abstract

Internet Protocol v6 (IPv6) for low-power wireless personal area networks (6LoWPAN) has been developed to facilitate and support IP stack communication over IPv6 networks. In RFC 6550, the Internet Engineering Task Force (IETF) specifies the IPv6 Routing Protocol for low power and lossy networks (RPL) to promote efficient routing in 6LoWPAN. However, this technology is not mature enough to offer secure mechanisms and communications. In this context, Software-Defined Networking (SDN) has been developed to provide programmability to the resource-constrained 6LoWPAN architecture creating a new paradigm called SD6LoWPAN. Moreover, researchers have proposed machine learning (ML) to provide fast reconfigurability and intelligence for SD6LoWPAN. This paper aims to provide an overview pertaining to security issues in SD6LoWPAN, considering its resource, topology, and traffic. In addition, a study is presented of the SDN- and ML-based security solutions that are suggested in the literature. Security research challenges and trends are also put forward. In conclusion a performance analysis of an SDN-based ML solution is presented.

5.2 Introduction

The Internet of Things (IoT) is deployed using heterogeneous low-power and lossy networks (LLNs) that are commonly characterized by communication connections with high packet loss and low throughput. These networks are expected to increase in abundance by more than 2.4

trillion per year by 2027. IPv6 has been developed to enable communication to support the IP stack in LLNs. This new paradigm is called Internet Protocol v6 for low-power wireless personal area networks (6LoWPAN). As this new architecture increases in use, it meets different challenges, including ones pertaining to network management and heterogeneity. To address these challenges, the software-defined networking (SDN) approach to 6LoWPAN aims to highlight the efficiency and sustainability of LLNs. SDN endeavors to centralize network intelligence in a network component by decoupling the network packet forwarding process (data plane) from the routing process (control plane). SDN typically uses the OpenFlow protocol for remote communication with data plane elements to determine the routing of network packets through network switches.

The amalgamation of these technologies gives a new architecture named software-defined 6LoWPAN (SD6LoWPAN). There are a wide range of communication protocols commonly used in SD6LoWPAN, e.g., WiFi, IEEE 802.15.4, RFID, and Bluetooth, that are used depending on the characteristics of the devices, their environment and the communication range. In this paper, we consider the standardized IPv6 Routing Protocol for LLNs (RPL) to facilitate efficient routing in LLNs. This protocol has become very popular in both industry and academia. The motivation behind using RPL is to provide efficient routing between resource-constrained nodes, adaptability to other network topologies, and quality of service (QoS). RPL build acyclic graphs and applies an objective function (OF) to select the parents and rank. RPL implements two objective functions in particular, the minimum rank objective function with hysteresis (MRHOF) and the objective function zero (OF0). The OF defines how the nodes should consider the metrics and constraints of the rank value, which is approximately the node's distance to the destination oriented directed acyclic graph (DODAG) root. Although the rank value helps RPL with multiple objectives, such as route discovery and distribution, loop prevention, and control overhead management, the protocol is exposed to many routing attacks. Wireless sensor network (WSN)-inherit attacks (i.e., sinkhole attacks, wormhole attacks) and IPv6-based attacks(i.e., rank attacks, DIO suppression attacks) have raised serious doubts about the robustness of RPL.

Furthermore, RPL features, such as self-organization, self-healing, and resource limitation, expose SD6LoWPAN to various attacks that compromise the user's security and privacy.

Some cryptography solutions have been proposed to address those threats. However, the resource-constrained nature of SD6LoWPAN poses many key management challenges related to establishing, storing, distributing, revoking, and replacing secure keys in LLNs, making current cryptography solutions inadequate for LLNs. In this context, the limitations of SD6LoWPAN represent a critical menace to RPL security because traditional cryptography-based solutions rely on secure key distribution. Hence, an intruder can access a large set of preloaded keys if a reliable node is compromised. An adversary can carry out a routing rank attack (RA) by misusing the rank property and breaching the routing protocol. Based on the analysis of rank-related vulnerabilities, RAs create non-optimal paths for all packets, which bypass malicious nodes and thus overwhelm the constrained 6LoWPAN architecture. To this end, a new security service is presented to prevent the misbehaving node from decreasing rank values to cope with RPL vulnerabilities (Miguel, Jamhour, Pellenz & Penna, 2018c). Specifically, the authors propose to prevent RPL from publishing an illegitimate reduced rank by generating hash chaining using a random number chosen by the root node. Moreover, in (Boudouaia, Ali-Pacha, Abouaissa & Lorenz, 2020b), a challenge-response scheme is used to validate the authenticity of the nodes within a DODAG. In (Shin, Sharma, Kim, Kwon & You, 2017c), a secure and efficient route optimization protocol is proposed. It includes steps for reliable route optimization and handover key management, that include mutual authentication and privacy. Although essential works have been proposed in the literature to target RAs in 6LoWPAN networks, these deployments are not satisfactory to simultaneously guarantee efficient intrusion prevention and low management complexity in 6LoWPAN networks. In addition, heuristic algorithms, e.g., ant colony optimization (ACO), swarm optimization, and artificial bee colonies are widely used to find solutions to combinatorial optimization problems. However, they are limited by the high sample complexity required to reach a reasonable solution. Therefore, the contributions of this paper can be summarized as follows:

1. A taxonomy of SD6LoWPAN security issues is presented, including key attributes such as resources, topology and traffic.
2. A study of existing SDN- and ML-based security solutions is introduced.
3. Security research challenges and trends are also put forward.

The remainder of this paper is organized as follows: Section II introduces the taxonomy of RPL security issues. Section III details existing SDN and ML-based security solutions. Section IV presents SD6LoWPAN security research challenges and trends. In Section V, a reinforcement learning-based solution's performance thwarting RAs by leveraging the Contiki Cooja tools is evaluated. Finally, paper's conclusion is presented in Section VI.

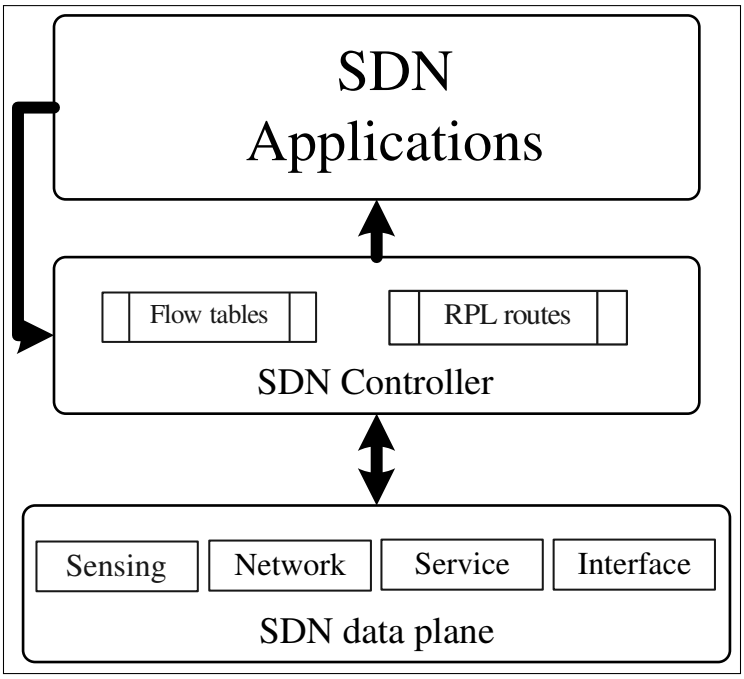


Figure 5.1 SD6LoWPAN Architecture

5.3 SD6LoWPAN security issues

SD6LoWPAN architecture incorporates three layers. At the bottom of the stack, in the data plane, typical IoT nodes combine the following communication layers: the sensing layer, the

network layer, the service layer, and the interface layer. In the middle, the control layer, the coordinator flow control handles the OpenFlow and RPL routes. At the top, in the application layer, the SDN applications are integrated. This architecture is fully integrated with the IEEE 802.15.4-2012 protocol stack, as shown in Fig. 5.1. In this paper, we will focus on security issues in the data plane. The main data plane concerns are briefly explained below

5.3.1 Sensing layer

Three kinds of attacks are considered in the sensing layer: cyber-physical, eavesdropping, and radio frequency identification (RFID) attacks. A cyber-physical attack results when a sensor in an SD6LowPAN network is physically compromised by a cyber-attacker called a faulty node. An eavesdropping attack happens when an attacker eavesdrops on the information sent by the nodes in the network. An RFID attack employs a physical device to spoof the victim. As a result, the attacker alters the information attached to a tag, which is sent back to the victim's device.

5.3.2 Network layer

The network layer comprises two sublayers: the routing layer, which manages packet transfer from source to destination, and the encapsulation layer that produces the packets. Since the network's availability, manageability, and scalability are crucial for SD6LowPAN network operation, an attacker can use different mechanisms to compromise the routing and encapsulation layers and to overwhelm and cause harm to the network.

5.3.3 Service layer

The service layer serves as a gateway between the sensing layer and the interface layer. An attack on the service layer could impact critical functions such as device and information management, resulting in end users not receiving a service. Access control, user authentication, communications security, data integrity and confidentiality are vital aspects of service layer security.

5.3.4 Interface layer

The interface layer is the most vulnerable part of the SD6LoWPAN infrastructure. This layer sits at the top of the IoT ecosystem and is a gateway to the other layers. For instance, if the authentication and authorization mechanisms are compromised at the interface layer, there is a ripple effect through the other layers. In this sense, the end-user is a potential attack mechanism, as attackers could obtain sensitive information through impersonation. In addition, web application interfaces can be subject to frequent SQL injection and cross-site scripting attacks. This manuscript takes an in-depth look at the most common problems encountered in the network layer. Bellow, we present an overview of RPL and the security issues specific to the RPL-based SD6LoWPAN.

5.3.5 Overview of RPL

The Internet Engineering Task Force (IETF) designed and standardized RPL, the IPv6 Routing Protocol for LLNs. RPL builds the network topology using directed acyclic graphs (DAGs) segmented by one or more DODAGs, each of which has a root node. Multiple root nodes are integrated into a backbone network that consists of border routers that connect them to the Internet. RPL is a routing protocol for mobile systems with low power consumption that find routes based on the objective function (OF) established in the initial stage. The OF delivers traffic to different routes according to traffic requirements it encoded to be used by RPL during routing operations. RPL applies some control messages such as DODAG Information Object (DIO), DODAG Information Solicitation (DIS), and DODAG Advertisement Object (DAO), as shown in Fig. 5.3. RPL operations include topology discovery, DAG construction, route generation, data path validation, and loop detection based on rank values.

5.3.6 RPL attacks

RPL is vulnerable to various types of internal and external attacks. In the resource-constrained SD6LoWPAN environment, these attacks are hard to mitigate and detect. Also, mobility

and easy node manipulation represents critical challenges for the network. RPL deployments typically do not provide for grant security methods due to the overhead they can produce during implementation. Although some works have proposed security mechanisms for RPL networks, including encryption and security protocol techniques, the mechanisms effectively defend against only external attacks, not internal ones. This is because an internal attacker can evade RPL's security mechanisms and interrupt network operations. A summary of RPL attacks based on their primary target is shown in Fig. 5.2. Each type of RPL attack is briefly discussed below.

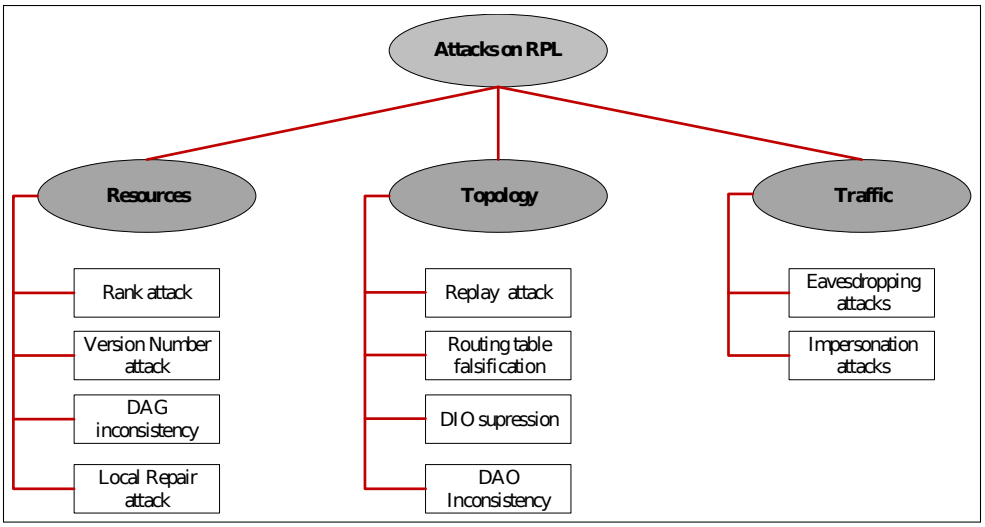


Figure 5.2 Taxonomy of RPL-based attacks

5.3.6.1 Replay attack

In this attack, a malicious node copies and multicasts the DIO messages received from its parent. Neighboring nodes receiving the DIO message thus believe it is from a legitimate node. In addition, if the DIO message includes routing information such as the rank value, the victim neighbor node adds the rank node as its preferred parent. Consequently, it changes the routes of the original DODAG, causing the network to be saturated.

5.3.6.2 DAO inconsistency attack

This attack happens when an adversary node periodically sends the wrong DAO messages to its parent nodes. Consequently, the parent nodes, command updates the routing table by overwhelming the network with acquired DAO messages that swamp network resources.

5.3.6.3 Routing table spoofing attack

A routing table forgery attack occurs when a malicious node spoofs routing information in DAO messages. The attacker convinces benign nodes to construct a fake route. Thus, the benign nodes attempt to forward data to non-existent nodes. This situation causes DODAG inconsistencies, packet delays and increased control overhead.

5.3.6.4 DIS attack

A DIS attack occurs when a malicious node transmits periodic DIS messages to neighboring nodes. Consequently, victim nodes restart their trickle timer and respond with DIO messages. This attack is carried out by forwarding DIS messages to a single node or multicasting DIS messages to multiple nodes to disrupt routing, increase power consumption and control packet overhead.

5.3.6.5 Version number attack

A version number attack occurs when an attacker modifies the version number field of the DIO message and then forwards it to neighboring nodes. This adjustment unnecessarily pushes DODAG reconstruction, causing routing loops, control packet overhead, end-to-end delay, and increased power consumption. It is worth mentioning that RPL does not specify a mechanism to prevent nodes other than the border router from illegitimately modifying the version number field in the DIO message.

5.3.6.6 Local repair attack

RPL carries out a local repair procedure when a node misses the link to its preferred parent. In the case of a local repair attack, a malicious node changes the DODAG ID value field of DIO messages or updates the node's rank to infinity. As a result, it multicasts the DIO message to its neighbors, making them search for a new preferred parent. In this context, the malicious node unnecessarily triggers the local repair mechanism, increasing the DODAG's energy consumption and disturbing the routing process.

5.3.6.7 DODAG inconsistency attack

RPL uses different flags to detect and fix loops in DODAGs. In this context, an intruder can misuse RPL flags to perform a DODAG inconsistency attack. A malicious node sets the RPL header flag to "0", meaning the rank relationship with the node that sent the packet is not traced, and the intruder set flag "R" to 1 before transmitting the packet to its neighbor. As a result, when a node receives a packet with the flag set to "R", it cancels and restarts its timer to perform a local repair unnecessarily.

5.3.6.8 DIO suppression attack

In a DIO suppression attack, a malicious node removes the transmission of DIO control messages in the SD6LoWPAN data plane, forcing nodes to explore new routing paths. Consequently, this attack creates unoptimized routes.

5.3.6.9 Rank attack

OF is an essential factor in the parent and rank selection. Once a node receives a valid rank, the OF's setting must be determined based on the routing metrics before the selected parent node is modified. For instance, if the routing metric relies on the expected transmission count (ETX), the OF holds the routing path with the lowest ETX value, and a node will receive both the rank and ETX for the chosen parent node. As shown in Fig. 5.3, to successfully originate a rank

attack, the attacking node must alter the routing metric advertised by the parent node so that the OF of the neighboring nodes is exposed to be attacked.

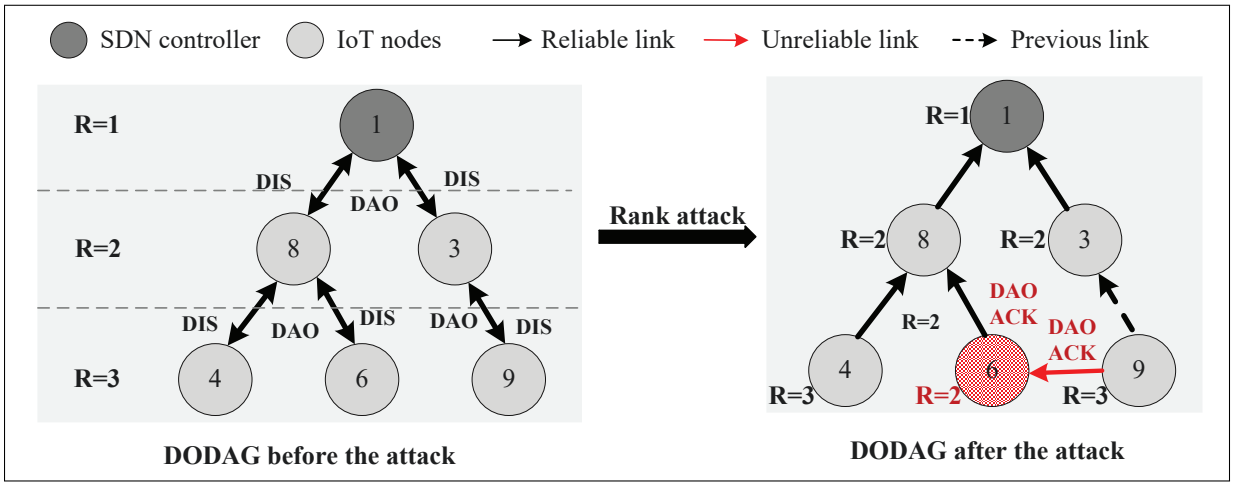


Figure 5.3 DODAG instance before and after an RA

5.4 SDN- and ML-based security solutions

Using ML to deploy RPL-based security solutions remains a significant task due to 6LowPAN's resource limitations and heterogeneity. Although ML has proven itself effective in securing resource-intensive wired and wireless networks, ML algorithms must be customized for 6LoWPAN networks with limited resources. In this regard, an SDN-based 6LoWPAN configuration can help overcome some of these challenges. Since the SDN controller supposedly has more resources than a typical 6LoWPAN configuration, the border router can accomplish some network operations, e.g., intelligent configurability and routing. Therefore, the 6LoWPAN architecture's security requirements can be addressed by integrating existing SDN functions into the border router. Some SDN- and ML-based security solutions that are presented in the literature are detailed below.

5.4.1 SDN-based security solutions

SDN-based security solutions have been deployed to provide programmability and intelligence to the resource-constrained 6LoWPAN architecture. The architecture consists of a central SDN controller that manages the data plane, including IoT operations, such as sensing, delay and sleep scheduling. Unfortunately, control overhead and end-to-end delay need to be addressed in the proposed system. In (Theodorou & Mamatas, 2020), the authors propose innovative SDN-based control of WSNs to decrease the data plane's energy consumption. More specifically, the border router plays the role of central controller located at the network edge to command the packet forwarding mechanism in the data plane. Furthermore, in (Miguel *et al.*, 2018c), an SDN architecture is introduced to provide end-to-end connectivity to 6LoWPAN. The proposed architecture uses SDN and network function virtualization (NFV) methods to minimize delay and reduce the data plane's energy consumption. In addition, (Baddeley, Nejabati, Oikonomou, Sooriyabandara & Simeonidou, 2018c) proposes an architecture called μSDN that aims to provide interoperability between different protocol stacks. The μSDN protocol uses an adapter to communicate with other protocols. In addition, it includes a discovery module to discover new nodes in the data plane. The module uses RL to help the network nodes discover the controller. The limitation of this study is having the SDN controller included in the border router, which may increase the system's total processing time. Moreover, in (Lasso, Clarke & Nirmalathas, 2018c), an SD6LoWPAN architecture is presented that introduces an SDN agent at each node in the network. The SDN agent communicates with the SDN controller by using the software-defined IPv6 wireless sensor network protocol (SD6WSNP) to interact with the northbound and southbound interfaces. The authors claim that latency and network overhead are reduced. Furthermore, some works propose an SD6LoWPAN architecture in which RPL is used for communication between the data and control planes. More specifically, the SDN controller communicates with the SD6LoWPAN data plane through CoAP messages. The adaptation layer adapts the data plane of this architecture, which manages packet forwarding routes via RPL. Although this architecture aims to reduce delay and increase SD6LoWPAN's reliability and

availability, it has a limitation in handling heterogeneity, as each sensor node used must have the SDN system enabled.

5.4.2 ML-based security solutions

ML techniques have successfully addressed classified dilemmas in variety of areas including speech recognition, spam detection, computer vision, and fraud detection. Although ML solutions can be considered a developed field, some authors consider their applicability for LLNs to be complicated due to the resource-constrained nature of the network nodes. For example, in (Zhang, Restuccia, Melodia & Pudlewski, 2018), the authors propose a framework that is based on applying Bayesian learning to detect and mitigate cross-layer wireless attacks. More specifically, the framework builds a relationship between a hypothesis (an attack is expected to occur) and the proof of it (proof of attack activities). This relationship allows the hypothesis to be dynamically updated when new evidence becomes available. Furthermore, in (Khan, Harous, Hassan, Khan, Iqbal & Mumtaz, 2019), a neural network is used to deploy a self-learning mechanism that legitimates the information produced by IoT nodes. Moreover, in (Zareen & Karam, 2018), an artificial immune system is proposed that leverages ML procedures to generate an adaptive immune system. The system evolves and branches based on observations and past experiences, and incorporates desirable features such as error tolerance, distributed computing, and self-monitoring. Although the system proposed facilitates adaptive applications, the evolved code may be faulty and could possibly be exposed to security attacks. Furthermore, in (Chaabouni, Mosbah, Zemmari, Sauvignac & Faruki, 2019), ML is used to build an intelligent system that automatically detects security threats, and in (Al-Garadi, Mohamed, Al-Ali, Du, Ali & Guizani, 2020), the author uses ML to develop a vulnerability assessment mechanism in order to identify and classify IoT devices based on their trustworthiness.

5.5 Security research challenges and trends

SD6LoWPAN networks face serious problems identifying and detecting intrusions due to their resource-constrained nature and massive development. Some of these challenges include:

1. System throughput in the data plane as many nodes are connected.
2. SD6LoWPAN scalability issues due to SDN node heterogeneity.
3. Computation complexity due to the resource-constrained data plane.

Some RPL-based security challenges are also presented below.

5.5.1 Security against new routing attacks

In RPL networks, some attacks , such as DIO suppression and rank attacks, can degrade network performance silently. To this end, efforts have been made to develop defence mechanisms against these attacks. However, due to new attacks' dynamics and intelligence, these defence techniques need to be improved to defend SD6LoWPAN accordingly. Reinforcement learning (RL) methods can be suitable to address these challenges and thereby prevent and detect new routing attacks.

5.5.2 Scalability

Existing defence security solutions have been recreated in small network scenarios, but in reality, the SD6LoWPAN data plane is composed of an extensive network of heterogeneous nodes with limited resources. Moreover, the performance of existing solutions may be inadequate in a more extensive and heterogeneous network, thereby leaving SDN applications exposed to attackers. Critical applications demand minimal delay in regards to packet forwarding. Therefore, high-speed and lightweight defence solutions are needed to perform complete network operations. In addition, these solutions must avoid degrading the network's QoS and, at the same time, support high scalability.

5.5.3 Mobility

RPL analysis demonstrates that mobile nodes critically affect RPL performance. This is because the RPL specification does not provide mechanisms to support such mobility. Network performance therefore deteriorates in the presence of mobile nodes. In addition, mobile features

increase the probability of link disconnections, packet loss and collisions, which means if malicious mobile nodes are compromised, network performance drastically decreases. It is therefore necessary to thoroughly study the security issues related to RPL attacks in a mobile environment. Most RPL-based defence solutions consider only the static environment and may not apply to mobile scenarios.

5.5.4 Cryptography challenges

Key management is a critical challenge for the resource-constrained SD6LoWPAN protocol. To this end, some defence solutions have used cryptographic techniques such as dynamic key, hash chain, and Merkle tree authentication. These methods require computational, memory and power consumption which makes them not suitable for resource-constrained devices. These overloads change the lifetime of nodes, which is a crucial principle for critical IoT applications. In this vein, the construction of lightweight cryptography-based security solutions for SD6LoWPAN remains a significant challenge to be addressed.

5.5.5 ML challenges

ML is efficient for securing resource-abundant WSNs. However, the deployment of ML algorithms must be improved to minimize their computational complexity in SD6LoWPAN networks with limited resources. Attempts to address this challenge will lead to the development of lightweight security solutions, which can help provide efficient prevention and detection mechanisms. In addition, selecting the suitable dataset, consecutive training and labelling remain ongoing challenges researchers face.

5.5.6 SDN challenges

We highlight bellow some of the requirements that need to be taken into account in the design of SD6LoWPAN networks.

5.5.6.1 Duty cycle

The SD6LoWPAN architecture should promote duty cycling, i.e., idle radio communication when not in use. There are ways to achieve this, either reactively on-demand or periodically through constant synchronization. Since high-duty cycling could degrade energy efficiency, it is recommended that SD6LoWPAN networks have low duty cycle operations.

5.5.6.2 Data aggregation

The SD6LoWPAN protocol must support network data aggregation to avoid sending bulk data to the controller. The goal of data aggregation approaches is to organize the data and send only the processed information. These methods are based on factors, such as source, destination, or application attributes. Determining which of these factors to consider requires a proper structural evaluation.

5.5.6.3 Flexible rules definition

The SD6LoWPAN architecture must support flexible policy and rule definition and application. Also, a mechanism to reverse and prevent rule or policy collisions is recommended to be implemented.

5.5.6.4 Wireless link unreliability

The SD6LoWPAN data plane is composed of radio wireless communication links. Wireless links frequently experience some instability due to common factors such as limited bandwidth, and node failures and are therefore unreliable (Al-Kashoash, 2019c). In this regard, the design of the SD6LoWPAN architecture should consider the rapid topological changes caused by temporary node unavailability.

5.5.6.5 Self-healing ability

The mobile nature of the SD6LoWPAN networks can trigger failures at data plane nodes. The network must therefore be efficient and able to rapidly reorganize to cope with such occurrences. Moreover, the controller must be logically centralized but operate logically as a single controller to avoid a single-point-of-failure scenario.

5.5.6.6 Backward compatibility

The SD6LoWPAN network should be compatible with existing WSNs other than OpenFlow and SDN-based sensor nodes should interoperate with normal sensor nodes. In addition, the SD6LoWPAN protocol should be integrated with the IoT framework and its protocols.

5.5.6.7 Southbound and northbound interfaces

The southbound and northbound interfaces are essential in the SD6LoWPAN architecture for fluid communication between layers. However, some work has been done on the southbound interface and less on the northbound one. As yet, there is no standardized API for northbound communication.

5.5.7 Security research trends

In addition to the research challenges already discussed, we list possible research trends for other researchers in this field.

5.5.7.1 IPv6 defense moving target

A proper mechanism against eavesdropping and IPv6-based attacks can continuously change the device's IPv6 address. Accordingly, lightweight IPv6 defense moving target mechanisms should be explored to secure the resource-constrained SD6LoWPAN networks. The use of temporary private IPv6 addresses can also be examined.

5.5.7.2 Defence mechanisms against coordinated routing attacks

Coordinated routing attacks severely degrade network performance without detection. Most well-known intrusion detection systems (IDSs) are vulnerable to coordinated routing attacks. It is, therefore, necessary to deploy efficient attack mitigation and detection solutions to defend SD6LoWPAN networks from coordinated routing attacks. One such mitigation solution is tasking solutions that allocate tasks to efficiently determine the optimal route for managing constrained resources (Baek, Kaddoum, Garg, Kaur & Gravel, 2019; Baek & Kaddoum, 2020; Amande, Kaur, Garg & Guizani, 2022; Cao, Garg, Kaddoum, Hassan & AlQahtani, 2022). For example, in (Miranda, Kaddoum, Baek & Selim, 2021), the authors propose a hybrid meta-heuristic algorithm that uses a task allocation framework to determine the optimal path for efficient task allocation management. This framework can help to minimize the risk that a coordinated routing attack overwhelms the limited network resources.

5.5.7.3 Collaborative IDSs

Collaborative IDSs have been created to leverage collaboration among sensor nodes and the border router to detect efficient and quick attackers. Some research works have proposed deploying collaborative security frameworks, but they still need further exploration. For instance, in (Miranda, Kaddoum, Bou-Harb, Garg & Kaur, 2020c), a software-defined security framework for software-defined, wireless sensor networks (SDWSNs) is proposed that combines intrusion prevention and collaborative anomaly detection systems.

5.5.7.4 Active learning

Insufficient dataset quantity and quality are critical issues for ML-based security solutions. This problem can be addressed with active learning mechanisms, which optimizes model learning through a training phase. In recent years, RL domain has obtained the attention of researchers. The RL model consists of two main entities: the agent and the environment, as shown in Fig. **??**. The agent is a fast learner who can make decisions based on past experiences, and the

environment is an entity that affects agent performance. In this vein, an in-depth study is recommended to leverage RL in the development of SD6LoWPAN prevention and detection mechanisms.

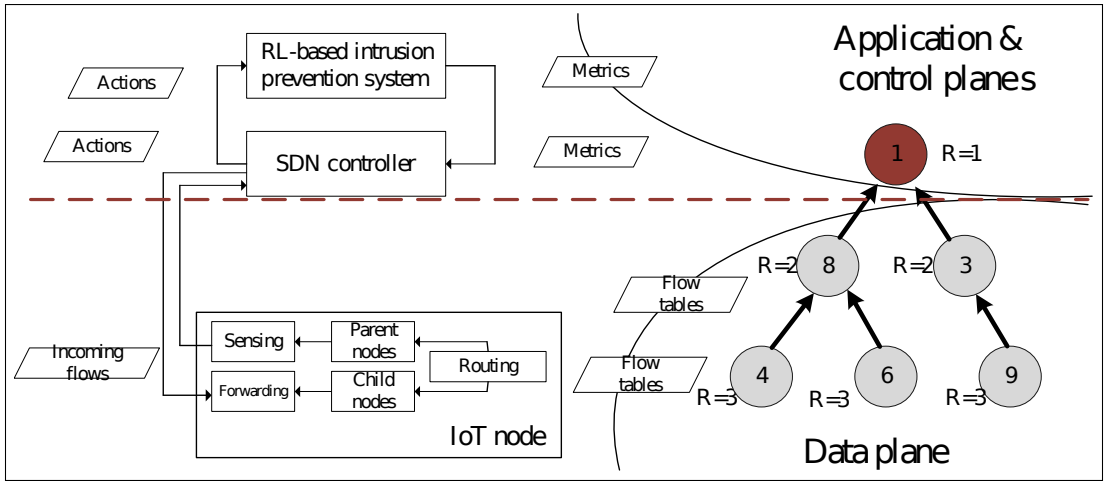


Figure 5.4 RL model

5.5.7.5 Key management and energy-efficient cryptography mechanisms

The construction of efficient and scalable key management mechanisms such as generation and storage, is a booming area of RPL security. Since security keys are loaded in IoT nodes in RPL secure mode, it can represent a security risk for SD6LoWPAN networks due to the centralized controller's single point of failure. In addition, classical cryptographic algorithms can achieve strong security as well. However, these algorithms are computationally and intensive. Thus, they cannot be used directly in the SDN6LoWPAN data plane because of its resource-constrained nature. Deploying energy-efficient cryptographic methods that meet the security requirement with minimal energy consumption is a critical challenge for the SD6LoWPAN protocol. For example, in (Moreira, Kaddoum & Bou-Harb, 2018f), a software-defined wireless network-enabled fast cross-authentication scheme combines non-cryptographic (radio signal strength and cryptographic algorithms) to address the challenges of latency and weak security. Additionally, quantum computers are expected to be available for computing applications in the coming years.

All existing cryptographic technologies will fail because current cryptographic methods can be decrypted. Quantum cryptography is essential to handle such complexities. Blockchain technology could be developed for authentication schemes for SD6LoWPAN and take the form of a distributed peer-to-peer network to manage the ledger that stores data plane-related information. In the next section, an RL-based security system's performance is analyzed to understand how rank attacks work and exemplify how RL can prevent this type of attack from being executed is presented in what follows.

5.6 Analysis of an SDN-based RL security solution's performance thwarting RAs

We consider a 6LoWPAN network composed of 30 IoT nodes where 29 are benign and 1 is malicious. The network is deployed in a simulated outdoor area. It is worth mentioning that the results are obtained considering a static scenario in which there are no mobile nodes. However, our emulation scenario is deployed in a dynamic wireless environment. Thus, our testbed's radio channel conditions are susceptible to changes due to interference (e.g., and from other 802.15.4 and 802.11 radios), and this interference is time-varying. Furthermore, the underlying MAC protocol is ContikiMAC. The following four scenarios are presented in our analysis:

1. **S1**: An RPL network with no SDN implementation under rank attack.
2. **S2**: An RPL network with SDN implementation without rank attack.
3. **S3**: An RPL network with SDN implementation under rank attack.
4. **S4**: An RPL network with our RL-based SDN approach under rank attack.

We analyzed the delay of the four scenarios considering a path with 5 hops. Fig. 5.5 demonstrates that in S1, there is a 1600-millisecond delay, and in S2, the latency is 2950 milliseconds, meaning S2 is 45.72% slower than S1. This is because additional overhead is introduced by the messages exchanged between the controller and the data plane. In S3, the latency is 4400 millisecond, which is 63.63% slower than S1 and 32.95% slower than S2. This is due to the rank attack requiring the data plane to navigate downwards along the RPL topology across multiple non-optimized paths. In S4, the latency is 2500 milliseconds, which is 56.81% quicker than S3 and 15.25% quicker than S2.

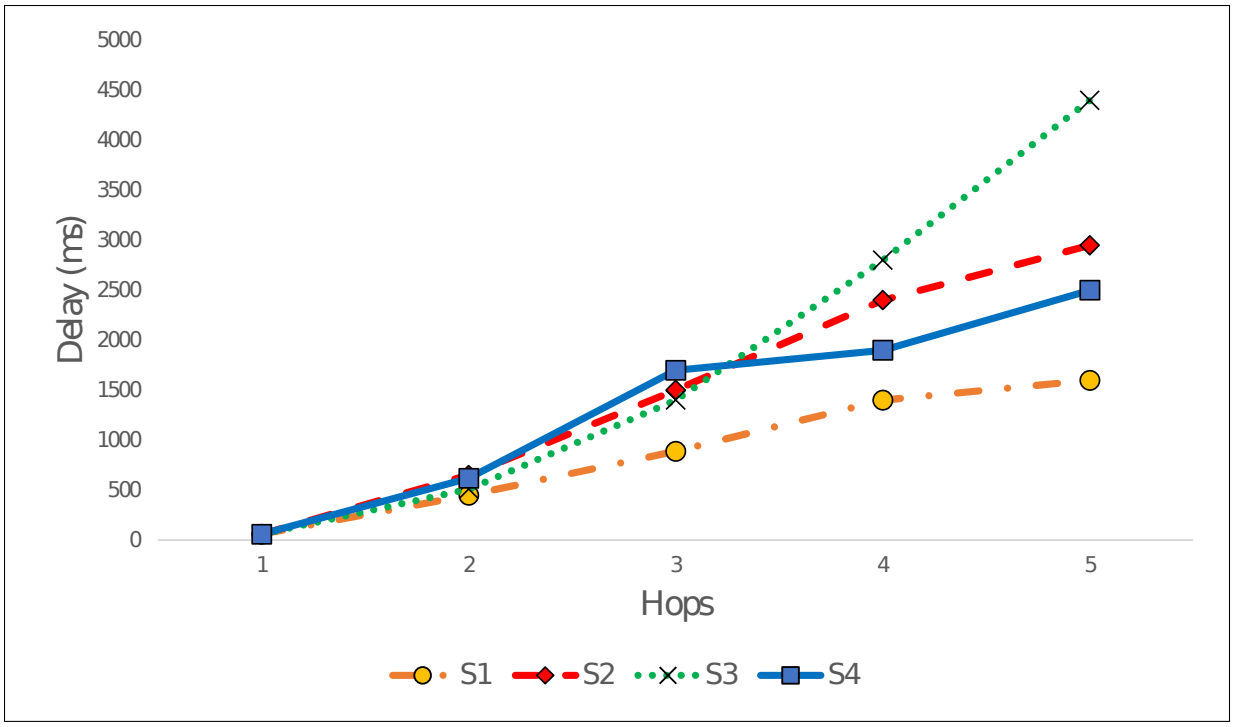


Figure 5.5 Delay-An illustrative comparison between S1, S2, S3, and S4

Although S4 (our approach) is 36% slower than the scenario in which SDN is not implemented (S1), it restores and even optimizes typical behavior in the SD6LoWPAN network. This is because there are fewer SDN messages since the optimized paths are delivered only once the RL approach's exploration process is finished, rather than every time the RPL collects data from the data plane. It is worth mentioning that S4 obtains the best results with DODAGs having more than 3 hops.

5.7 Conclusion

The SD6LoWPAN protocol's characteristics, such as global connectivity, heterogeneity, self-healing and resource limitation, make it an ideal environment to be compromised by attackers. In particular, the mobile nature of the SD6LoWPAN data plane make it a favorite target for malicious activity because the SDN nodes communicate using wireless links. The RPL protocol

has been standardized to support efficient routing in LLNs. However, it is vulnerable to a variety of attacks, including legacy SDN, WSN and RPL attacks. In this paper, we present a comprehensive study of common RPL attacks and related defence solutions. First, we discuss the security issues in the SD6LoWPAN architecture. Then, we present a taxonomy of existing SDN- and ML-based security solutions. We also discuss some research challenges and future trends. Finally, we present an analysis of an RL-based security solution's performance thwarting rank attacks. The research related to security solutions specific to SD6LoWPAN is still young and requires more attention to provide comprehensive security for SDN applications.

CHAPTER 6

A COLLABORATIVE SECURITY FRAMEWORK FOR SOFTWARE-DEFINED WIRELESS SENSOR NETWORKS

Christian Miranda[1] , Georges Kaddoum[2] , Elias Bou-Harb[3] , Sahil Garg[4] , Kuljeet Kaur[5]

[1,2,3,4,5] Département de Génie Électrique, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Article published in Transaction on Information Forensics and Security, February 2020

6.1 Abstract

With the advent of 5G, technologies such as Software-Defined Networks (SDNs) and Network Function Virtualization (NFV) have been developed to facilitate simple programmable control of Wireless Sensor Networks (WSNs). However, WSNs are typically deployed in potentially untrusted environments. Therefore, it is imperative to address the security challenges before they can be implemented. In this paper, we propose a software-defined security framework that combines intrusion prevention in conjunction with a collaborative anomaly detection systems. Initially, an IPS-based authentication process is designed to provide a lightweight intrusion prevention scheme in the data plane. Subsequently, a collaborative anomaly detection system is leveraged with the aim of supplying a cost-effective intrusion detection solution near the data plane. Moreover, to correlate the true positive alerts raised by the sensor nodes in the network edge, a Smart Monitoring System (SMS) is exploited in the control plane. The performance of the proposed model is evaluated under different security scenarios as well as compared with other methods, where the model's high security and reduction of false alarms are demonstrated.

6.2 Introduction

Wireless Sensor Networks (WSNs) provide infrastructure-free communications over the shared wireless channels without the need for fixed infrastructures or centralized access points. Sensor networks comprise of a set of dynamic cooperating nodes; forming one of the most promising

wireless technologies which introduce a new wireless transmission paradigm by employing multi-hops for information transfer. WSNs have significant potential applications in the fields of transportation, agriculture, industrial automation, process monitoring, military surveillance, environment monitoring, health-care, etc. According to (Rashid & Rehmani, 2016), these wireless sensors need to be self-configured into a network to process and interpret sensor measurements, and convey this information to a centralized control location.

Moreover, traditional WSNs typically consist of routers and switches as network devices. Therefore, as they grow, they become difficult to monitor and update. Meanwhile large-scale WSNs are also heterogeneous due to the use of different communication protocols, which fundamentally means they consist of different network clusters that only cooperate at low level of communication (Kobo, Abu-Mahfouz & Hancke, 2017a). Since the distributed management of a communication protocol determines which node can receive or transmit data, this makes the global vision and the applicability of security mechanisms in the network a very complex task. Further, as the scale of the WSN expands, it is faced with several constraints, such as resource and energy restrictions, processing, memory, and communication capabilities. To address these constraints, the deployment of a lightweight security framework which includes the centralization of intelligent features becomes essential.

With the emergence of 5G, promising technologies such as Software-Defined Networks (SDNs) and Network Function Virtualization (NFV) have been designed to support innovations and enable simple programmable control of data paths in wireless sensor nodes (Sun, Gong, Rong & Lu, 2015). These technologies provide WSNs with the capability of being programmed upon request. In addition, they allow multiple isolated sensor functions, by addressing and forwarding mechanisms, to share the same physical infrastructure. Furthermore, SDNs allow network administrators to manage network services through the abstraction of lower level functionalities. This is done by decoupling the control plane that makes decisions about where traffic is sent from the underlying data plane to the selected destinations. As a consequence, computational complexity is reduced while throughput is enhanced. In addition, the SDN approach to WSNs seeks to alleviate most of the challenges and ultimately foster efficiency and

sustainability in WSNs. Thus, the control plane can dynamically enforce flow rules when the data plane requires it. However, this control operation can cause serious problems when there are excessive requests from the data plane to the control plane. On the other hand, if the data plane receives many requests in a short period of time, it can flood the messages to the control plane. Moreover, a flow table in the constrained data plane can also be flooded by rules for handling requests (Fawcett, Scott-Hayward, Broadbent, Wright & Race, 2018).

Despite the high programmability and automation of WSNs gained from 5G, these networks are not immune to malicious users. Since, network intelligence is centralized in SDN controllers, protecting the communications throughout the data and the control planes is critical (De Gante, Aslan & Matrawy, 2014). For instance, the centralized network intelligence might become victim of malware (Pritchard, Hancke & Abu-Mahfouz, 2017).

In the SDN environment, some WSN-unique data plane threats can take place. Under such scenarios, fake traffic flows caused by both flawed devices and malicious sensor nodes can compromise the entire SDN architecture. Similarly, OpenFlow switches and resource-constrained nodes can be disrupted by network elements infected with Denial of Service Attacks (DoS) such as Black hole attacks, Selective Forwarding attacks, Hello Flood attacks, and Sybil attacks (Pritchard *et al.*, 2017; Liyanage, Ylianttila & Gurtov, 2014b). It is evident from the above discussion that the disruptive SDN technology is also prone to different attack vectors.

In this vein, several works have been proposed to leverage the benefits of the SDN architecture for enhanced network security such as virtual firewall, access control, and deep packet inspector systems (Pritchard *et al.*, 2017). Motivated by their findings, the major contribution of the proposed work is on addressing the security issues prevalent in the SDN's data plane. In this direction, the work emphasizes the problem of authentication and high-precision anomaly detection in the untrusted and resource-constrained data plane of SDNs.

6.2.1 Motivation

Along this line of thought, a hierarchical security framework is proposed in this work. The proposed framework amalgamates a lightweight authentication with a collaborative anomaly detection system (Boggs, Hiremagalore, Stavrou & Stolfo, 2011), which correlates the alerts of the lightweight IDSs distributed across the WSN.

The lightweight authentication system for the SDN's resource-constrained data plane demands an efficient Intrusion Prevention System (IPS)-based authentication scheme for Software Defined Wireless Sensor Networks (SDWSNs). This scheme protects the network by allowing only correct information to be inserted by the authenticated nodes. Thus, authentication of the nodes needs to be performed continuously and frequently; thereby considerably increasing its complexity (Habib, Makhoul, Darazi & Salim, 2016b). Furthermore, an IPS-based authentication scheme can be performed by using one or more validation factors including credentials, knowledge factors (keys interchange), possession factors (tokens), and biometric factors (eg., fingerprint recognition, iris, face, retina, etc.) (Perera & Patel, 2018). Although validation factors might present a low-latency solution, they also introduce complexity due to recurrent authentication handovers. Nonetheless, traditional IPS-based authentication procedures rely on cryptographic keys and multiple handshakes, such as Authentication and Key Agreement (AKA) protocols. However, due to their high latency, infrequent handovers, and high computational cost, they were found unsuitable for the requirements of SDWSNs (Zhang & Fang, 2005). Although IPS-based authentication procedures can effectively identify malicious nodes, they cannot eliminate all of them, especially the ones launched from inside the network. Further, the captured nodes can quickly lunch attacks as they have total control over the encryption and authentication keys. Consequently, mobile nodes without an additional protection are prone to be compromised, corrupted, and hijacked. To address these issues, IDS-based solutions can be an indispensable second line of defense to safeguard the data plane from insider attacks in SDWSNs. To this end, machine learning procedures like Support Vector Machine (SVM) and neural networks (Ma, Yu, Wang, Zhang & Chen, 2016) are usually employed. Nevertheless, such techniques typically introduce a non-negligible overhead and high computational cost in SDWNs (Shon & Moon,

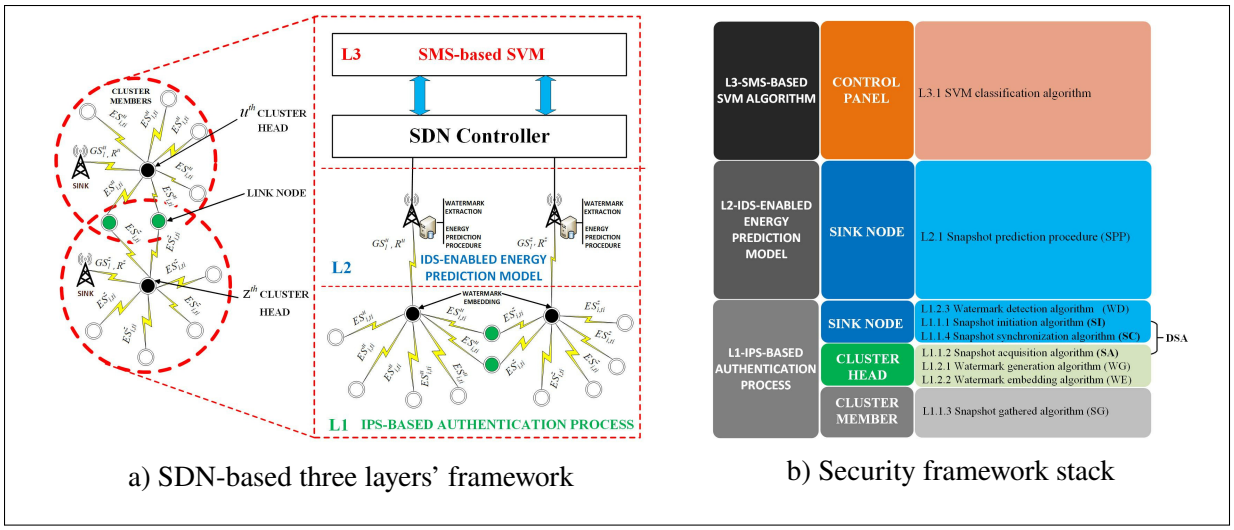
2007). To minimize the overhead introduced by machine learning solutions, edge-based energy prediction models might be used (Han, Jiang, Shen, Shu & Rodrigues, 2013b).

However, the sensor nodes are individually prone to generate a tremendous number of alerts. According to (Milenkoski, Jayaram, Antunes, Vieira & Kounev, 2016), an alert does not always implies a problem; instead, it may just be an indication that the sensor has inspected some traffic which has matched a signature or a pattern. Thus, the malicious and trusted activity are considered an anomaly. These alerts are called false positives and can overwhelm a sensor network. This is because the sensor nodes only have local visibility of the network behavior. On the other hand, the stochastic nature of energy features in wireless communications contributes to an IDS-enabled energy prediction model might cause false positives as well. Accordingly, to minimize false alarms and make the decision-making process more efficient by correlating the decisions already taken by an IDS, the deployment of a real-time Smart Monitoring System (SMS) with the aid of a machine learning algorithm in the control plane becomes an encouraging solution.

Since the proposed SMS is located in the control plane, it can be customized with additional security services that address the topology and network operator specific requirements/issues. Consequently, instead of isolated security schemes, this work proposes a collaborative software-defined security framework to coordinate different security controls on each framework layer. Each security control is designed based on the criticality of the wireless environment, its security criteria, and its resource constraints.

6.2.2 Related work

A plethora of research works have been performed to address high security and low-latency solutions for resource-constrained WSNs. In this context, some of the existing IPS-based authentication procedures have been developed using classical key management authentication mechanisms. For example, an IPS combining Internet Protocol (IP) trace-back with an enhanced adaptive acknowledgment (EAACK) was proposed in (Murugesan, Saravanan & Vijyaraj,



a) SDN-based three layers' framework

b) Security framework stack

Figure 6.1 A collaborative security framework for SDWSNs

2014b). Moreover, Location-Based Keys (LBKs), binding private keys of individual nodes to both their identifications and geographic locations was proposed in (Zhu, Leung, Yang & Shu, 2015). These approaches improved the security at the cost of increasing the latency of the network. To address the challenges associated with the low-latency requirements, some works used physical layer features. For instance, a two-factor user authentication mechanism was recommended in (Wang, He, Wang & Chu, 2015), where the authors devised an authentication mechanism comprising of registration and authentication phases. Furthermore, the authors in (Jagadiswary & Saraswady, 2016; Akyildiz *et al.*, 2015a; Gonzalez *et al.*, 2016), explored a biometric-based continuous authentication technique, without the the need for an authentication server. These approaches reduced the latency but at the cost of increasing the complexity of the authentication procedures.

Furthermore, some works also exploited physical layer features in IDS to achieve low-latency in WSNs. In this context, a novel intrusion detection scheme based on energy prediction for cluster-based WSNs was introduced in (Amjad, Qureshi, Lestas, Mumtaz & Rodrigues, 2018), wherein the authors used the energy states of wireless sensor nodes to predict malicious behaviors at a given time. Excessive false alarms are a common artifact of these approaches.

Consequently, machine learning procedures have been widely used to develop IDS-based solutions. For instance, the use of neural networks and watermarking techniques was suggested in (Yin, Zhu, Fei & He, 2017). A SVM methodology was proposed in (Ambusaidi, He, Nanda & Tan, 2016), while a hybrid machine learning approach for network anomaly detection was put forward in (Shon & Moon, 2007). A hybrid anomaly-based IDS was recommended in (Ma *et al.*, 2016) which employed SVM and multi-layer perceptron (MLP) to identify anomalies in the network. Further, the authors in (Kim, Kim, Thu & Kim, 2016) presented an intrusion detection engine based on neural networks combined with a protection method-based on a watermarking technique. While these algorithms improve the accuracy of network anomaly detection models, they also introduce high computational cost which is inadequate for WSNs. Even though relevant works have been proposed in the literature to target security issues in SDWSNs, challenges such as high security, excessive false alarms, low-latency, and high computational cost still remain unaddressed.

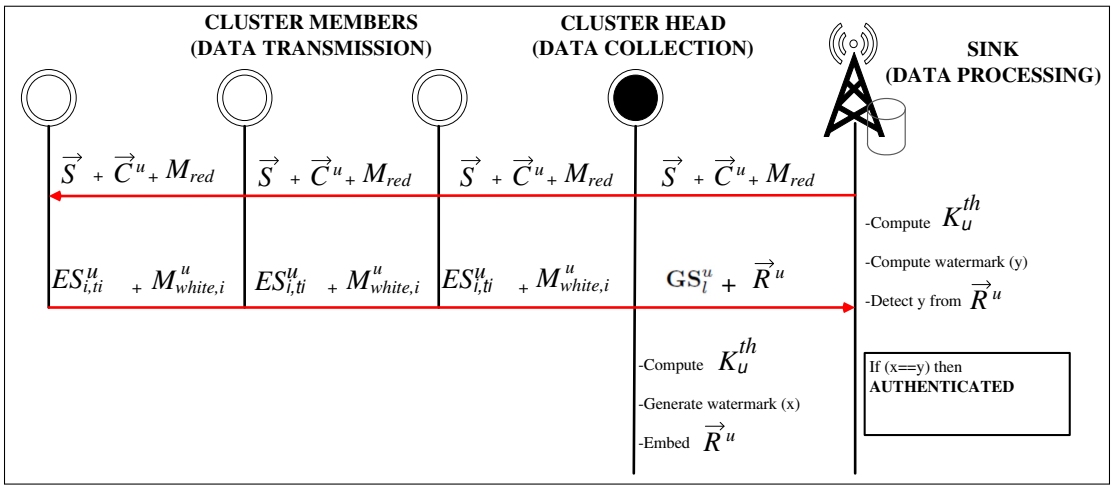


Figure 6.2 DSA-based authentication and a watermarking technique

6.2.3 Contributions

To address these imperative challenges, in this paper, a bottom-up security framework is designed. The novelty of the proposed work lies in devising and evaluating a collaborative framework which amalgamates a recurrent lightweight authentication method in conjunction with an intrusion

detection and a real-time smart monitoring system; achieving lightweight authentication and enhanced anomaly detection mechanisms in SDWSNs.

Since a single-gateway (cluster head) architecture is not scalable and might cause an incremental overhead in large-scale WSNs, the proposed work uses a cluster-based SDWSN architecture that provides a hierarchical organization to a flat sensor network topology, considerably reduces the latency of the network (Younis, Youssef & Arisha, 2002). This architecture consists of four kinds of dynamic nodes, namely, cluster members, cluster heads, link nodes, and sink nodes. Further, in this framework, a Distributed Snapshot Algorithm (DSA) is executed to capture network snapshots periodically so as to obtain the global energy state of the WSN; wherein the global energy state corresponds to a map of the energy state for each node at a given moment. Moreover, the DSA is also used to dynamically adapt the network topology within the cluster to reduce the energy consumed for communication; thus, extending the lifetime of the network while achieving an acceptable performance for data transmission (Han *et al.*, 2013b).

The proposed framework hierarchically combines three security layers. At the bottom of this approach (Layer L1), an IPS-based authentication process is designed to provide a lightweight security scheme in the data plane. In the middle of the framework (Layer L2), an IDS-enabled energy prediction model within the edge is designed with the aim of supplying a cost-effective intrusion detection solution near the data plane. Finally, at the top of this framework (Layer L3), in the control plane, a SMS-based SVM algorithm is introduced to achieve isolation, high performance, enhanced anomaly detection, and efficient mitigation by segregating malicious nodes over the SDWSNs. Since the SMS-based SVM algorithm has global visibility of the sensor network, it can see the correlations between true positives, which lets it filter out the false positives. Thus, the main contributions of this work are summarized as follows:

1. A novel security scheme based on network snapshot readings, providing continuous authentication in large-scale SDWSNs, is proposed.
2. A watermarking technique is exploited to guarantee the accuracy of concurrent authentications while performing data integrity checks for the entire SDWSN.

3. The authentication method is improved by introducing a link node, which creates a connection between all the cluster of sensors.
4. An edge computing empowered IDS is leveraged to efficiently handle the limited resources in SDWSNs.
5. A two label dataset is generated in the edge, with the aim to train an SVM classification algorithm that is subsequently used by the SMS; wherein the latter is deployed at the control plane and is designed to correlate the alerts from the low-delay IDSs distributed across the edge network.

Moreover, analysis of the computational complexity is provided and simulations showing the effectiveness of the proposed framework are executed by leveraging the AVISPA tool and MATLAB. The results demonstrate an accuracy of 84.75%.

The remainder of this paper is organized as follows: Section II and Section III introduce the different layers of the proposed framework. In Section IV, security analysis and performance evaluation are conducted. Finally, the paper is concluded in Section V, where some future endeavors are also put forward.

6.3 System Model

Aiming to achieve high-security, address the limited resources constraints and take advantage of SDN architectures, our work proposes a collaborative security framework design, as depicted in Fig. 6.1a. To summarize, the proposed security framework possesses a hierarchical structure and comprises of three layers. At the bottom of the framework stack, in the data plane, in L1, an IPS-based authentication process is performed. At the middle, at the edge, in L2, an IDS-enabled energy prediction model is executed, and finally, in the control plane, in L3, the SMS-based SVM algorithm is designed. In this context, in L1, a cluster-based WSN is created (Han *et al.*, 2013b) and DSA is employed, where the sink nodes initiate the snapshot acquisition process by sending a marker message to their cluster heads in order to form a global energy state of the network. Afterwards, the marker message is propagated to the cluster members. Each

member sends its energy state back to its cluster head post receiving the message. Once the cluster head collects the global energy state from its cluster members, it protects the data using a watermarking-embedded method with the aid of a generated public key and other security parameters to ensure that the derived data will not be altered on the fly by possible malicious attackers. Consequently, the network snapshot and the watermarked data is forwarded to the sink node. Likewise, the sink sends a copy of the energy map to the control plane, which is located in the cloud. Moreover, in the edge, the sink node periodically receives the snapshot readings aiming to detect the embedded watermark for the sake of continuous authentication and for the subsequent energy consumption prediction procedure. Furthermore, the appropriate watermarked data is considered reliable, while the data without a correct watermark is marked as unreliable. Subsequently, in L2, an IDS-enabled energy prediction model is executed, where a Markov chain prediction procedure is used to detect nodes' misbehavior. Conclusively, to amalgamate this framework, in the control plane, in L3, an SMS-based SVM algorithm is designed where the dataset resulting from L2 is processed by employing a SVM classification algorithm. A summary of the security framework stack is presented in Fig. 6.1b.

6.4 Proposed Scheme

In the following subsections, the proposed L1, L2, and L3 layers along with their corresponding stack of algorithms are elaborated.

6.4.1 IPS-based authentication process

In SDWSN applications, the reliability and the integrity features of the cluster nodes should not be compromised. However, if the data transmission is not reliable, the integrity of the whole network is affected. To handle this security challenge, this work considers deploying an IPS-based authentication mechanism which is an amalgamation of the DSA and watermarking techniques. The designed mechanism aims to provide a two-way authentication handover between the cluster node, the cluster head, and the sink node.

In the following subsections, the sublayers, the DSA-based authentication procedure, and the watermarking-based authentication technique are detailed.

6.4.2 DSA-based authentication procedure

As illustrated in Fig. 6.2, this procedure starts when the sink node initiates snapshot acquisition by sending the first message to its cluster head; from there, the request message is propagated to every cluster member. After receiving this message, every cluster member sends its energy state back to its cluster head which is then used to generate the key fingerprint with other security parameters. It is worth mentioning that a link node could receive multiple request messages from multiple clusters' heads. Thus, each link node must send a reply back to all of them, in order to provide scalability for large-scale WSN and maximize the efficiency of the authentication procedure. Before data transmission, the energy state of the cluster heads is embedded into the global energy state gathered by them. The concurrent snapshot readings gathered in a given time by the u^{th} cluster head are represented as follows.

$$\mathbf{GS}_l^u = [ES_{1,t_1}^u, ES_{2,t_2}^u \ldots, ES_{i,t_i}^u], \tag{6.1}$$

where $\mathbf{GS}_l^u$ represents the snapshot readings collected in l cycles at t_i time of arrival from the i^{th} cluster member ES_{i,t_i}^u to the u^{th} cluster head. This time of arrival significantly reduces the possibility of impersonation of the $\mathbf{GS}_l^u$ vector by an intruder. This is due to the random behavior of wireless communications which makes the time of arrival unforeseeable (Moreira, Kaddoum & Bou-Harb, 2018b). The cluster head then averages the $\mathbf{GS}_l^u$ vector to generate the k_u^{th} fingerprint using the following equation.

$$k_u^{\text{th}} = \text{E}[\mathbf{GS}_{\text{l}}^{\text{u}}], \tag{6.2}$$

where E[.] is the mean operator.

Afterwards, the k_u^{th} fingerprint is encrypted with the advanced encryption standard (AES) algorithm with a key length of 128 bits (Lu & Tseng, 2002). The generated k_u^{th} fingerprint contributes to making the public key unpredictable.

Further, the aim of the DSA is to obtain a distributed network global state by recording the consistent energy state at a specific time (Uslu, Serdaroglu & Baydere, 2013). In this sense, as shown in Fig. 6.1b, the DSA is divided in four algorithms hierarchically distributed as follows:

- The Snapshot-Initiation (SI) algorithm, launched by the sink node;
- The Snapshot-Acquisition (SA) algorithm, exploited by the cluster head;
- The Snapshot-Gathering (SG) algorithm, executed by the cluster members;
- The Snapshot-Synchronization (SC) algorithm, exploited by the sink and the cluster head nodes.

Next, we detail the four algorithms which use the notations presented as follows.

6.4.3 Snapshot-initiation algorithm

Since DSA collects snapshots through messages, it is important to ensure message delivery. Thus, in order to solve this problem, we implement a two-way handshake between the cluster node and the sink node. Here, the authentication procedure relies on the SI algorithm, which assumes that the number of sensor nodes and their first snapshot is known by the sink in a setup stage. The sink ensures reliable ES^u_{i,t_i} delivery by keeping a table indexed with nodes' identification. In this context, the sink node sends an initial M_{red} message to its cluster head. The SI algorithm execution ends only when the sink node acquires the network snapshot from all functioning nodes. In this manner, the sink node waits until timeout t_w expires. Once the sink receives $\vec{\mathbf{R}}^u$, a flag is set to true for all the nodes that have already sent their corresponding ES^u_{i,t_i}, otherwise, it remains false as shown in Algorithm 6.1. After the timeout expiration, the sink node checks the content of the table in order to explore the nodes which have not yet sent their energy state.

Table 6.1 Algorithms' notations

Notation	Description
$\vec{\mathbf{S}}$	Represents the vector of cluster heads' identification
$\vec{\mathbf{C}}^u$	Represents the vector of cluster members' identification
$\vec{\mathbf{Z}}^u$	Is the vector of cluster members' identification whose snapshot is not collected by the sink at timeout
$\vec{\mathbf{R}}^u$	Is the watermarked data
M_{red}	Is a request message from the sink node to the i^{th} cluster members
$M^u_{white,i}$	Is a response message from the i^{th} cluster members to the sink
t_w	Illustrates the timeout for generating a new snapshot message at the sink node
W^u	Is a random position used to select the most significant bits (MSB) at the u^{th} cluster head
v^u	Is a value used to control the proportion of the marked data at the u^{th} cluster head
α^u	Is a value used to calculate the embedded location of the marked data at the u^{th} cluster head

Algorithm 6.1 SI algorithm

procedure SNAPSHOT-INITIATION()
$mMessage \leftarrow M_{red}$
while $t_w \neq timeout$ **do**
$\vec{\mathbf{R}}^u \leftarrow$SNAPSHOT-ACQUISITION($\vec{\mathbf{S}}$, $\vec{\mathbf{C}}^u$, $mMessage$)
if $ES^u_{i,t_i} \neq null$ **then**
$flag \leftarrow true$
WATERMARK-DETECT($\vec{\mathbf{R}}^u$,$\vec{\mathbf{S}}$, $\vec{\mathbf{C}}^u$, k^{th}_u,W^u,v^u, α^u) **else**
$flag \leftarrow false$

6.4.4 Snapshot-acquisition algorithm

In response to the sink's request, the SA algorithm is executed. Initially, the u^{th} cluster head takes a backup of their current ES^u_{i,t_i} to be used, if necessary, by the SC algorithm, if necessary. Subsequently, the periodic snapshot acquisition is performed where the u^{th} cluster head acquires

the initial M_{red}, which is propagated to its cluster members. This procedure continues until the cluster head collects the energy states of all the cluster members. The acquisition of the initial message is achieved by the SA algorithm as follows.

Algorithm 6.2 SA algorithm

procedure SNAPSHOT-ACQUISITION($\vec{\mathbf{S}}$, $\vec{\mathbf{C}}^u$, $mMessage$)
  while $\vec{\mathbf{S}} \neq null$ **do**
    $\mathbf{GS}_l^u \leftarrow$SNAPSHOT-GATHERED(($\vec{\mathbf{S}}$,$\vec{\mathbf{C}}^u$, $mMessage$)
  $mMessage \leftarrow M^u_{white,i}$
  return WATERMARK-EMBED($\mathbf{GS}_l^u$,$data$,k_u^{th},W^u,v^u, α^u)

6.4.5 Snapshot-gathering algorithm

Once a cluster member receives M_{red} from its cluster head, it takes a backup of their current ES^u_{i,t_i}. Then, it sets its marker message to $M^u_{white,i}$. Afterwards, as noted in Algorithm 6.3, it sends its ES^u_{i,t_i} and the marker message to its cluster head. As soon as the cluster head gathers ES^u_{i,t_i} from all its cluster members, it averages the $\mathbf{GS_l^u}$ vector to generate the k_u^{th} fingerprint.

Algorithm 6.3 SG algorithm

procedure SNAPSHOT-GATHERED(($\vec{\mathbf{S}}$, $\vec{\mathbf{C}}^u$, $mMessage$)
  while $\vec{\mathbf{C}}^u \neq null$ **do**
    $mMessage \leftarrow M^u_{white,i}$
    return ES^u_{i,t_i} , $mMessage$

6.4.6 Snapshot-synchronization algorithm

The SC algorithm aims to achieve reliability in detecting the missing control states within a defined acquisition time frame and forces these specific nodes to resend their backed-up states to the sink node. In this manner, if a node receives a retransmission request from its cluster head, it means that the sink did not gather yet its energy state.

The synchronization algorithm is designed to handle two scenarios, which might cause premature delivery. The first scenario is when the initial message is not picked by the node, (*i.e.,* snapshot is not taken), and the ES^{u}_{i,t_i} is not generated. The second scenario is when the initial message is received, and the ES^{u}_{i,t_i} is sent but it does not reach the sink node. Once the sink node receives the global energy states from its cluster heads, it sets the flag belonging to the sender node to indicate successful reception of the state information. When t_w expires, if there are flags containing false, the sink performs the synchronization procedure to the nodes in $\vec{\mathbf{Z}}^{u}$, *i.e.,* the nodes from which the ES^{u}_{i,t_i} is not gathered yet. The synchronization procedure is provided in Algorithm 6.4.

Algorithm 6.4 SC algorithm

procedure SNAPSHOT-SYNCHRONIZATION($\vec{\mathbf{S}}$, $\vec{\mathbf{Z}}^{u}$, M_{red})
  while $\vec{\mathbf{Z}}^{u} \neq null$ **do**
SNAPSHOT-ADQUISITION($\vec{\mathbf{S}}$, $\vec{\mathbf{Z}}^{u}$, M_{red})

Intuitively, a snapshot reading can be visualized as a representation of the energy map collected from the entire sensor network, where each node is analogous to a pixel, and its reading indicates the pixel's intensity. Therefore this snapshot can be embedded within a watermark (Hameed, Khan, Ahmed, Reddy & Rathore, 2018).

In the following subsection, a continuous watermarking-based authentication technique is considered to ensure the reliability of data transmission by authenticating the identity of sensor nodes.

6.4.7 Watermarking-based authentication technique

The watermarking-based authentication technique is designed to determine the authenticity of the data transmitting node and guarantee the integrity of the data. For this purpose, the proposed technique is composed of three algorithms distributed hierarchically as follows:

- The Watermark-Generation (WG) algorithm, executed by the cluster head;
- The Watermark-Embedding (WE) algorithm, performed by the cluster head;

- The Watermark-Detection (WD) algorithm, launched by the sink node.

According to this model, the proposed technique operates in three phases: data transmission, data collection and data processing as depicted in Fig. 6.2. In this context, an approximation of the algorithm in (Boubiche, Boubiche & Bilami, 2015) is used with the aid of the k_u^{th} fingerprint, which was previously built in the data processing phase.

6.4.8 Watermark-generation algorithm

WG algorithm employs the most significant bit (MSB) and the least significant bit (LSB) techniques to improve the integrity of the procedure (Solé & Zinoviev, 2004; **?**). Each element of the collected data is given by Eq. (6.1). For each data element, $\mathbf{GS}_l^u$ and k_u^{th} are inputted into a one-way hash function following which $h = Hash\ (k_u^{\text{th}}, \mathbf{GS}_l^u)$ is calculated. A bit of watermark $\mathbf{WM}\ [i]$ is obtained by calculating the XOR of the W^u bits of the MSB (h), which represents the most significant bits of h. The watermark **WM** is the collection of $\mathbf{WM}\ [i]$. Thus, the snapshot is only authenticated by the watermark generation algorithm which is shown in Algorithm 6.5.

Algorithm 6.5 WG algorithm

procedure WATERMARK-GENERATE($\mathbf{GS}_l^u$,k_u^{th},W^u)
  for each $\mathbf{GS}_l^u$ **do**
    $h \leftarrow Hash\ (k_u^{\text{th}}, \mathbf{GS}_l^u)$
    $\mathbf{WM}\ [i] \leftarrow$XOR *(MSB* ($h$), W^u*)*
  end for
  return $\mathbf{WM}\ [i]$

6.4.9 Watermark-embedding algorithm

The aim of this algorithm is to embed the watermark generated in WG into the sent data. Towards this end, we use the LSB technique which is executed before inserting some random values to the sent data of each watermark bit **WM**. The random value of each snapshot is calculated by introducing the most significant bits of the sent data, $\mathbf{GS}_l^u$ and the k_u^{th} key into a random function. The k_u^{th} key is the same as in WG. The parameter v^u is chosen in a range from two to

nine to control the proportion of the marked data. The watermark is embedded into each data item only when the random value can be split precisely by the proportion of the marked data, v^u. Consecutively, the random values are used to calculate the embedding location in the least significant bits. Conclusively, the x^{th} LSB of each data item is replaced by the watermark bits **WM** generated by Algorithm 6.5. The Watermarking-Embedding (WE) technique is shown in Algorithm 6.6.

Algorithm 6.6 WE Algorithm

procedure WATERMARK-EMBED($\mathbf{GS}_l^u$,$data$, k_u^{th},W^u,v^u, α^u) WATERMARK-GENERATE($\mathbf{GS}_l^u$,k_u^{th},W^u)
  for each WM do
    $g \leftarrow$ **Rand** (k_u^{th}, $\mathbf{GS}_l^u$, MSB ($data$))
    if (g mod(v^u) == 0) **then**
      $x \leftarrow g\ mod(\alpha^u)$
      x^{th} LSB ($data$) $\leftarrow$**WM** [i]
  end for

6.4.10 Watermark-detection algorithm

Once the watermark message is constructed by the cluster head with the energy state of each cluster member, the k_u^{th} key, and other security parameters, the cluster head is then able to forward it in a distributed manner to the sink node. As soon as the watermarked message is received by the sink, a watermark-detection algorithm is initiated which extracts and verifies the watermark to determine each node's authenticity. The Watermark-Detection (WD) technique is described in Algorithm 6.7. If the watermark-detection rate is larger than a threshold β, then the watermark is detected which corroborates the node's authenticity. The value of β is given by each energy state and its corresponding energy consumption threshold, which needs to be set up in the configuration stage (Shanthi & Rajan, 2016). To maintain the security framework's performance, only the data transmission process among the cluster head and the sink node is watermarked. It is worth mentioning that the unwatermarked ES_{i,t_i}^u transmitted between the member nodes does not affect the reliability of the proposed architecture. This is because a

cluster member could share the ES^u_{i,t_i} with more than one cluster head, creating a link between the cluster nodes rendering the continuous network snapshots and readings unpredictable.

Algorithm 6.7 WD Algorithm

procedure WATERMARK-DETECT($\vec{\mathbf{R}}^u$, $\mathbf{GS}^u_l$,k^{th}_u,W^u,v^u, α^u)
  $tot \leftarrow 0$
  $match \leftarrow 0$ WATERMARK-GENERATE($\mathbf{GS}^u_l$,k^{th}_u,W^u)
  for each WM do
    $g \leftarrow$ **Rand** (k^{th}_u, $\mathbf{GS}^u_l$, MSB ($\vec{\mathbf{R}}^u$))
    if $g \bmod(v^u) = 0$ **then**
      $x \leftarrow g \ mod(\alpha^u)$
      $tot \leftarrow tot + 1$
      if x^{th} LSB ($\vec{\mathbf{R}}^u$) =**WM** [i] **then**
        $match \leftarrow match + 1$
  end for
  $rate \leftarrow tot/match$
  if $rate > \beta$ **then return** $true$ **else return** $false$

Furthermore, it is important to highlight that the snapshot synchronization and watermark detection processes are added to the data processing phase to address the limited computational capabilities and storage capacity in SDWSNs.

6.4.11 IDS-enabled energy prediction model

To execute DoS attacks, malicious nodes have to use additional energy. In this context, energy thresholds are set to identify malicious attacks (Pacheco, Gondim, Barreto & Alchieri, 2016). Once the network nodes are authenticated, a second line of defense is initiated, taking advantage of physical layer features. Precisely, an IDS-enabled energy prediction model is employed at the edge with the aim of detecting DoS attacks such as Black hole attacks, Selective Forwarding attacks, Hello Flood attacks and Sybil attacks. Towards this end, we propose a snapshot prediction procedure (SPP) to detect the nodes' misbehavior. Further, a Markov chain model (Han *et al.*, 2013b) is leveraged in order to predict energy states of SDWSNs.

6.4.12 Snapshot prediction procedure

In this framework layer, a Markov chain model is presented as a promising solution to predict wireless sensor nodes' snapshots behavior. Towards this end, the nodes' energy states are represented by the transition states of a Markov chain model. In this context, each sensor node has m transition states. Therefore, the m transition states are classified into $m \epsilon$ {0-sensing, 1-transmitting, 2-receiving and 3-sleeping}. Eq. (6.1) is used as a sequence of random vectors to represent the transition probability of staying at each state in a given time. Thus, $ES^{u}_{i,t_i,l} = m$, assuming that the energy sate of the i^{th} cluster node to the u^{th} cluster head, gathered at t_i time and l cycles, is in mode of operation m (Cammarano, Petrioli & Spenza, 2016). Furthermore, the transition probability of $P_{m,j}$, a node which is presently in state m will be in state j at the next transition is represented by:

$$P_{m,j} = P\{ES^{u}_{i,t_i,l+1} = j | ES^{u}_{i,t_i,l} = m\}, \tag{6.3}$$

The two-stage transition probability can be defined as

$$P^{(2)}_{m,j} = P\{ES^{u}_{i,t_i,l+2} = j | ES^{u}_{i,t_i,l} = m\}, \tag{6.4}$$

where $P^{(2)}_{m,j}$ can be computed from $P_{m,j}$ using the following equation.

$$P^{(2)}_{m,j} = \sum_{d=1}^{N} P_{m,d} P_{d,j}, \tag{6.5}$$

In cluster-based sensor networks, each cycle l contains q transition probabilities. Therefore, the transition probability q, denoted as $P^{(q)}_{m,j}$, is defined by the Chapman-Kolmogorov equation (Haken & Mayer-Kress, 1981).

$$P_{m,j}^{(q)} = \sum_{d=1}^{N} P_{m,d}^{(r)} P_{d,j}^{(q-r)}, \text{for } 0 < r < q, \tag{6.6}$$

Indeed, if the sink node is aware of the probabilities $P_{m,j}^{(q)}$ for all the network nodes and its initial state $ES_{i,t_i,l}$, it is easy to predict the energy transition of each sensor node. Thus, the prediction process can be described as follows:

1. When a sensor node is in a state m, the sink node counts the number of q transition probabilities that a node will stay in state j each cycle l. Since each cycle l contains q transition probabilities, the calculation is represented by $\sum_{q=1}^{l} P_{m,j}^{(q)}$.
2. Hence, the sink node predicts the energy consumption of the sensor node as follows

$$E_p = \sum_{j=1}^{4} \left(\sum_{q=1}^{l} P_{m,j}^{(q)} \right) E_{i,j}^{u}, \tag{6.7}$$

where $E_{i,j}^{u}$ represents the energy consumption of the i^{th} cluster member to the u^{th} cluster head in state j after one transition. Aiming to predict a sensor node's energy state, given its initial node operation E_{p_1}, the procedure uses the first network snapshot collected by the sink node in the setup stage. Accordingly, once the snapshot is received, the next cycle for the sink node is the residual energy state E_{r_1}. Thus, the actual energy state E_{a_1} is given by:

$$E_{a_1} = E_{p_1} - E_{r_1}. \tag{6.8}$$

Subsequently, the residual energy E_{r_1} received from all the nodes in the next cycle is denoted as $\hat{E}_{r_1}$. The next energy state is represented as follows.

$$E_{a_1} = E_{r_1} - \hat{E}_{r_1}. \tag{6.9}$$

Therefore, if the actual energy state E_{a_1} is different from the predicted one E_{p_1}, the sensor node is labeled malicious in the operating environment. On the contrary, if the current energy state E_{a_1} is equal to the predicted one E_{p_1} or within the allowed threshold, the sensor node is labeled trusted in the same environment. Afterwards, this dataset is watermarked using Algorithm 6.6 and forwarded to the control plane.

On the other hand, since a cluster member might become a cluster head in the next iteration, its actual energy consumption will be higher than the previous iteration due to the collecting and watermarking processes. Hence, this means that its increasing energy state transition likelihood will be inaccurate when the energy prediction procedure runs on the edge. This might cause a prediction error.

In addition, because they only have local visibility, the sensor nodes deployed across the data plane are individually prone to false positives. Both trusted and malicious activities cause changes in energy patterns on these nodes, thus, both can be considered as anomalous activities. In this sense, there will be a lot of similarity between true positive alerts generated by different nodes in the network. Further, the prediction error is impacted by several environmental parameters such as the number of sensor nodes, the sink node's position, the network size, the communication range, and so on. Thus, these parameters might generate excessive false alarms as well. To this end, it becomes necessary to empower our IDS located in the edge with an additional layer of detection, which allows it to see the correlations between multiple instances of an attack. This is explained in the sequel.

6.4.13 SMS-based SVM algorithm design

At the top of the security framework, as depicted in Fig. 6.1a, a collaborative anomaly detection mechanism is introduced as a real time centralized smart monitoring system based on SVM (Shon & Moon, 2007). Towards this end, the information of trusted and malicious nodes, which is continuously received by the sink, is used to create a training dataset that contains 200 features (*i.e.,* energy state transitions), and is labeled as either trusted or malicious node. Thus, the

dataset is watermarked and delivered to the control plane. Since the SMS-based SVM has a global visibility of the WSN, it can see the correlations between true positives from a large number of weak sensors' classifiers providing a higher detection rate and considerable reduction of false alarms.

The use of SVM in the IDS domain introduces several advantages, including the support for kernels and binary classification. However, it has some limitations since SVM, being a supervised learning method, requires labeled information for efficient learning. Thereby, it is essential to mention that such restrictions do not affect our proposed solution since the smart monitoring system receives marked information by the edge. On the other hand, the SVM classification algorithm was chosen because of its ability to provide a higher detection accuracy in pattern recognition problems (Venkatesan, Karthigaikumar, Paul, Satheeskumaran & Kumar, 2018; Kim, Stanković, Johansson & Kim, 2015).

Nevertheless, once the control plane receives the watermarked dataset, Algorithm 6.7 is immediately executed to verify the sink node's authenticity and recover the labeled dataset to execute the SVM classification algorithm. As a result, the malicious misclassified nodes will be segregated from the data plane by removing them from the OpenFlow table.

6.4.14 SVM classification algorithm

The SVM classification algorithm has a slack function and a penalty function to organize non-separable models (Kim *et al.*, 2015). Initially, given a set of points $X_i \epsilon R^d; i = 1, \ldots, N$, where each X_i belongs to one of the two classes with tags $Y_i \epsilon (-1, 1)$. These two classes define the detection of nodes. Assuming there is a hyperplane which separates the positive class (S) from the negative class (G), the positive ones represent the behavior of the trusted nodes and the negative ones represent the behavior of the malicious ones. All the training class is satisfied in Eq. (6.10).

$$\begin{aligned} \mathbf{w}^T X_i + b \geq 1, \text{for all } X_i \, \epsilon \, S \\ \mathbf{w}^T X_i + b \leq -1, \text{for all } X_i \, \epsilon \, G, \end{aligned} \tag{6.10}$$

where $\mathbf{w}$ is an adjustable weight vector, X_i represents the input set of points, and b is the bias term as shown in Eq. (6.11).

$$Y_i(\mathbf{w}^T X_i + b) \geq 1, \text{for all } i = 1 \ldots N, \tag{6.11}$$

Therefore, the set of data received by the control plane is linearly separable, where the distance between the hyperplane and the set of points X_i is $\frac{1}{\mathbf{w}}$. Therefore, the margin of the separation hyperplane is defined by $\frac{2}{\mathbf{w}}$. The learning problem is reformulated, since by minimizing $\mathbf{w}^2 = \mathbf{w}^T$, $\mathbf{w}$ becomes subject to the linear separation limitations shown in Eq. (6.12). This formulation is equivalent to maximizing the hyperplane distance between the two classes, for which the maximum distance is called a support vector.

$$\begin{aligned} \text{Minimize}_{\mathbf{w},b} \quad \phi(\mathbf{w}) = \frac{1}{2} \|\mathbf{w}\|^2 \\ \text{s.t. } Y_i(\mathbf{w}^T X_i + b) \geq 1 \quad X_i \geq 0, i = 1 \ldots N, \end{aligned} \tag{6.12}$$

Since $\phi(\mathbf{w}) = \frac{1}{2} \|\mathbf{w}\|^2$ is convex in $\mathbf{w}$ and the constraints are linear in $\mathbf{w}$ and b, we can guarantee an optimum solution. For this solution, the parameters in the quadratic programming (QP) only affect the training time and not the quality of the solution. On the other hand, the anomalies in the energy state sensors' transitions present characteristics of non-linearity and as a result are very difficult to classify. In this sense, to proceed with the non-linear approach, the Lagrange solution for this problem is described as

$$L(\mathbf{w}, b, \Lambda) = \frac{1}{2}\|\mathbf{w}\|^2 - \sum_{i=1}^{N} \lambda_i [Y_i(\mathbf{w}^T X_i + b) - 1], \tag{6.13}$$

where $\Lambda = (\lambda_i \ldots \lambda_h)^T$ are the Lagrange multipliers, one for each data point. The solution to this quadratic programming problem is obtained by maximizing L with respect to $\Lambda \geq 0$ and minimizing $\frac{1}{2}\mathbf{w}^2$ with respect to $\mathbf{w}$ and b. Lagrange multipliers are only non-zero when $Y_i(\mathbf{w}^T X_i + b) = 1$, and the vectors for this case are called support vectors, since they are closest to the separating hyperplane. Furthermore, in the non-separable case, forcing zero training error leads to poor generalization. The SVM classification method uses a vector of slack variables $\sigma = (\xi_i \ldots \xi_h)^T$ that measure the amount of violation of the constraints, taking into account the fact that some data points might be misclassified. The current optimization problem becomes the following:

$$\begin{aligned} &\text{Minimize}_{\mathbf{w},b,\sigma} \quad \phi(\mathbf{w}, b, \sigma) = \frac{1}{2}\|\mathbf{w}\|^2 + D\sum_{i=1}^{N} \xi_i^2 \\ &\text{s.t. } y_i\phi(\mathbf{w}^T X_i + b) \geq 1 - \xi_i, \quad \xi_i \geq 0, i = 1 \ldots N, \end{aligned} \tag{6.14}$$

where D is a regularization parameter that handles the balance between maximizing the margin and minimizing the training error. The value of D is of importance since if D is too small, insufficient stress is placed on fitting the training data, whereas if D is too high, the algorithm might overfit the dataset.

a) Without watermarked message b) With watermarked message

Figure 6.3 Simulation results using Security Protocol Animator for AVISPA (SPAN)

6.5 Security Analysis and Performance evaluation

In the following subsections, we analyze the security features of the proposed IPS-based authentication process using the AVISPA tool. Moreover, a performance evaluation of the collaborative anomaly detection system is also conducted using MATLAB.

6.5.1 Formal Security Analysis

In SDWSNs, the nodes could function as routers that discover and maintain the routing path among network nodes. The predicament is that the path relies on the trustworthiness of all the cluster nodes. Therefore, DoS attacks can easily be executed against routing paths in SDWSNs. DoS attacks attempt to suspend network operations by injecting malicious packets into the data stream or by modifying packets. For this purpose, DoS attacks based on our proposed PS-based authentication process are analyzed.

Foremost, a comparison of a conventional authentication procedure against the proposed authentication method is conducted under two use cases. In the first use case, the security of the traditional AKA protocol is executed (Zhang & Fang, 2005). Since this protocol shares its public key over the air, this use case considers that a malicious cluster head in the network knows the key. Hence, a fake node can perform a coordinated hijacking attack, taking control of the communication over the wireless data channel. On the contrary, in the second use case, in our proposed protocol, a malicious cluster head is unable to acquire knowledge about the key. This is because the proposed protocol does not send the key and other parameters over the air. These uses cases are formalized and then assessed using the AVISPA tool as follows.

1. The Cluster Head (CH) sends $\mathbf{GS}_l^u$ and the k_u^{th} fingerprint in plain text on the fly to authenticate themselves at the sink. As depicted in Fig. 6.3a, the analysis indicates **UNSAFE**, revealing that the protocol is vulnerable to being impersonated.
2. In the proposed protocol, CH sends $\mathbf{GS}_l^u$ and the k_u^{th} fingerprint obscured by a watermarked message on the fly to the sink. In contrast to the conventional algorithm, the cluster head, the sink, and the control plane generate the k_u^{th} fingerprint and the watermark message

separately which improves the security as the k_u^{th} key is never sent in plain text on the fly. The results shown in Fig. 6.3b indicate that this protocol is **SAFE** against the analyzed threats.

6.5.2 Informal Security Analysis of the IPS-based authentication mechanism

In the following, we analyze how different DoS attacks might be performed, and how our proposed IPS prevents such attacks.

- Black hole attacks. This is an active attack (Gurung & Chauhan, 2017), where the intruder node listens to a route request packet in the network, and responds with a claim of having a shorter route to the destination node thus intercepting the packets, without actually having access to the route. As a result, the intruder node could easily redirect big loads of network traffic to itself and can manipulate all the packets passing through it. Accordingly, this attack fails if the malicious node is unable to obtain the legitimate node's identity from the sink. In the proposed solution, the sink node extracts the watermark message with the k_u^{th} fingerprint and other parameters. In this manner, the authentication request is denied if the sink node fails to match the watermarked data sent by the cluster head. Such a technique solves the problem of miss-charged billing in SDWSNs (Liu, Dong, Ota & Liu, 2016). Thus, the proposed scheme immunes SDWSNs from black hole attacks.
- Selective Forwarding attacks. A selective forwarding attack is a network layer attack described in (Ren, Zhang, Zhang & Shen, 2016). In multi-hop SDWSNs, the nodes send packets to their neighbors assuming that they have forwarded the messages to the destinations faithfully. In selective forwarding attacks, malicious nodes purposely refuse some packets and drop them. In this active attack, an intruder that is interested to eavesdrop packets originating from a few selected nodes can reliably forward the remaining traffic by limiting the chances of being detected. In this matter, to identify and mitigate this attack, the proposed authentication method prevents the intruder from manipulating the traffic if the sink fails to match the watermarked data sent by the cluster head.

- Hello Flood attacks. Within SDWSNs, an intruder typically attempts to drain the energy of a node or exhaust its resources. An intruder with vast transmission power could broadcast HELLO packets to convince every other node in the network that the adversary is within one-hop communication range, causing a large number of nodes to waste energy in sending packets to this imaginary neighbor (Gurung & Chauhan, 2017). Subsequently, this active attack might be easily prevented if the sink is aware of the energy state of each network node. For this purpose, our IPS that operates at the edge, performs a watermarking technique, validating the authenticity of the data transmitting node and guaranteeing the integrity of the send data.
- Sybil attacks. This active attack was introduced in (Jan, Nanda, He & Liu, 2015), wherein the attacker (Sybil node) tries to forge multiple identifications in a particular region. A Sybil node can fix the vote on group-based decisions and cause disruption in network services. When these nodes can no longer communicate, the attacker sends fake traffic, impersonating the network nodes. Therefore, to address this security threat, the first layer of the framework prevents the nodes from being imitated. Hence, the watermark message, the k_u^{th} fingerprint, and other parameters are used to strengthen the two-way authentication process. These parameters are independently generated between the cluster nodes and the sink node to safeguard nodes and provide data authenticity. Furthermore, the links between the link node and its cluster heads reinforce the nodes and data authenticity. This is because the link node shares its energy states with more than one cluster head. Thus, each cluster head generates the watermarked message based on those energy states. Thereby, the more the link nodes, the more reliable our solution becomes.

6.5.3 Performance Evaluation of the Collaborative anomaly detection system

In order to evaluate the performance of our collaborative anomaly detection approach across its layers, it is essential to mention that the SDN paradigm aims to reduce the non-negligible overhead introduced by IDS-based machine learning algorithms (Pranata, Jun & Kim, 2019). For this reason, we assume the SMS (L3) is deployed in a SDN controller located in the cloud

Table 6.2 Network parameters of the data plane

Parameters	Value
Number of nodes	400
Energy state transitions	200
Node placement	Random
Location of the Sink	50, 50
Transmission range	25m
Channel bandwidth	1 Mbps
Simulation time	1000 seconds
Propagation mode	Free Space
Packet size	512 bytes
Initial energy	5 $\mu J/bit$

and the IDS-enabled energy prediction procedure (L2) is performed in a edge architecture nearby the end devices.

Even though the edge architecture aims to avoid the overhead of processing requests from the data plane towards the control plane, there are inaccuracies in the cluster-based energy model due to the overhead, packet dropping and propagation delay of refresh messages exchanged between the control plane, the sink, and the sensor nodes. To the best of our knowledge, the model approximation is still suitable for SDWNs since frequent refreshing, and fine-tuning of routing parameters, can keep deviation within permissible limits (Younis *et al.*, 2002). Indeed, the overload analysis of the proposed SDN-based framework will be addressed in a future work.

In the proposed work, we employed MATLAB to simulate various DoS attacks such as Black hole, Selective Forwarding, Hello Flood, and Sybil attacks in SDN setups. During these simulations, we compared the energy state transitions with the predicted results using the Markov chain model (Jinhui, Yang, Feiyue, Leina, Juan & Yao, 2018). Towards this end, we employed different network parameters to depict the SDN data plane characteristics as shown in the following Table.

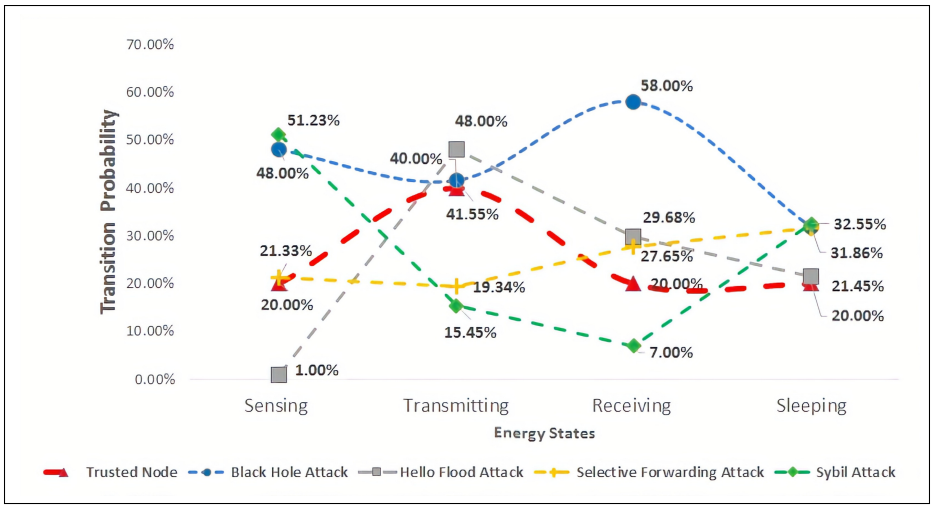


Figure 6.4 Energy state transitions probability of trusted vs. malicious nodes

As depicted in Fig. 6.4, the obtained results illustrate the differences between the energy state transitions of a trusted node and the malicious one across the SDWSN. In black hole attacks, the malicious node maximizes its broadcast range as well as the signal strength. Thus, the energy consumption is significantly larger than the energy predicted. Subsequently, in Hello Flood attacks, the malicious node attracts the communications of cluster heads coming from the cluster nodes. Thus, the gap between the energy state of Hello Flood attack and the predicted result is higher at the beginning but it decreases gradually through the simulation. Additionally, the energy state transitions in Sybil attack is far beyond the predicted result, thus, is the easiest to detect. Moreover, the IDS-enabled energy prediction procedure of our framework recognizes Selective Forwarding attacks as well, where the malicious node could be undetected at the beginning of the simulation but the probability of being inferred increases due to its signal strength variation in a given time.

In addition, it is worth mentioning that the energy state transitions interconnect to each other at certain periods of time, which means that the gap between the attacks and the predicted results is minimal. Thus, false alarms are generated.

Furthermore, Fig. 6.5, illustrates the gap generated between the energy state transitions based on the Markov chain model of trusted nodes and malicious nodes. Hence, the average detection probability of the energy transitions of the malicious nodes reaches 24.92% which implies that the detection rate probability of a trusted node is 75.08%. As a result, 210 nodes were found to be trusted, whereas 190 nodes were marked as malicious.

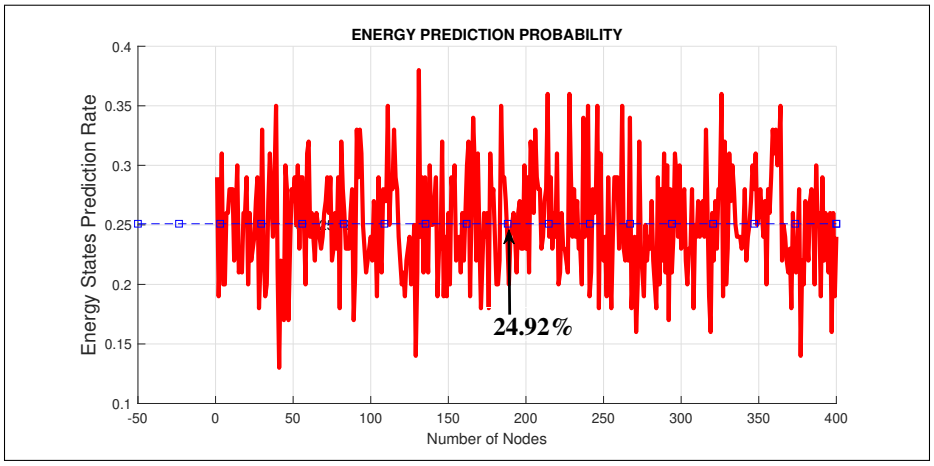


Figure 6.5 IDS-based Markov chain model

Some feature comparisons between layer L1 and layer L2 against cryptographic (Murugesan *et al.*, 2014b; Zhang & Fang, 2005), and machine learning (ML) approaches (Ma *et al.*, 2016; Kim *et al.*, 2015), respectively, are introduced. It can be noted that although our L1 provides important security features (F1:Mutual Authentication, F2:Frequent Handover, F3:Outsider Attacks' Resiliency), thus is suitable for SDWSN, it is still not sufficient to address insider attacks (F4) as shown as follows.

Table 6.3 IPS-based Authentication Solutions' Comparison

Solution	F1	F2	F3	F4
Crypto (Murugesan *et al.*, 2014b; Zhang & Fang, 2005)	✓	✗	✓	✗
Layer L1	✓	✓	✓	✗

As a consequence, L2 appears to tackle insider attacks (F4:Insider Attacks' Resiliency) while providing low latency features (F5) as presented in the Table as follows. Additionally, a computational complexity (F6) comparison between our L2 and ML approaches is shown in Fig. 6.6. As a result, the proposed L2, maintains a linear complexity while ML grows exponentially as the number of nodes increases which makes it unsuitable for edge computing ecosystems. Nevertheless, L2 generates excessive false alerts (F7) as well.

Table 6.4 An illustrative comparison of IDS-based solutions

Solution	F4:	F5	F7
ML (Ma *et al.*, 2016; Kim *et al.*, 2015)	✓	✗	✓
Layer L2	✓	✓	✗

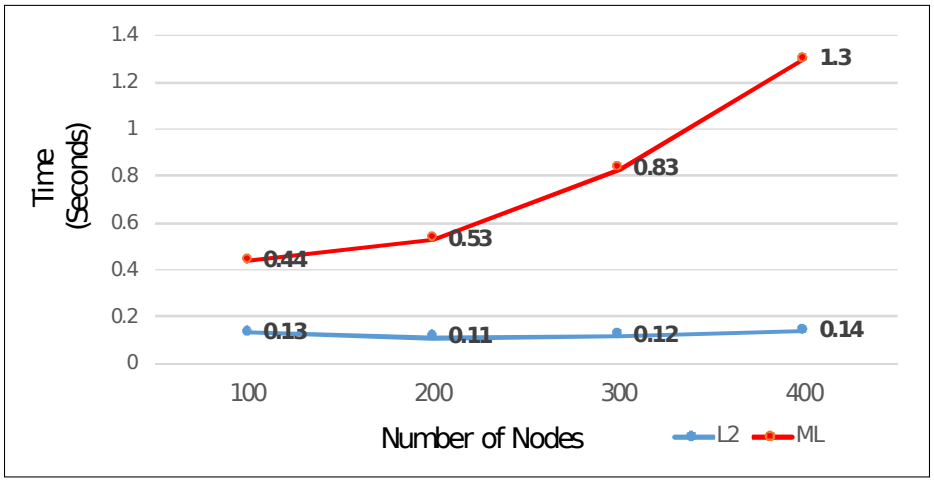


Figure 6.6 An illustrative comparison of computational complexity analysis (F6)

In this context, to minimize the number of false alarms, determine the accuracy, and correlates the detection rate of the IDS performed at the edge, L3 is executed in the control plane. For this purpose, a binary SVM classifier is developed and employed in the control plane. Since the optimal parameter search plays a crucial role in building a prediction model with high accuracy, we employ a grid-search technique using 5-fold cross-validation to find out the optimal parameter values of the kernel function for SVM (Venkatesan *et al.*, 2018).The results shown in Fig. 6.7 were modeled using a Radial Basis Function (RBF).

The evaluation of L3's classifier accuracy uses L2's output as ground truth, where trusted and malicious nodes are represented by a non-linear classification model. The obtained results demonstrate that there are 61 False Alarms (FA) as shown as follows.

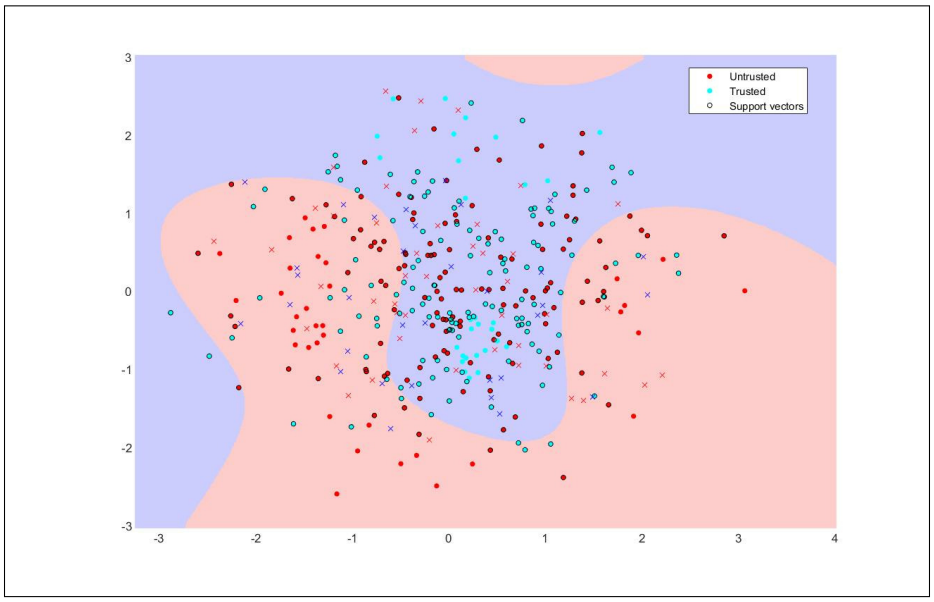


Figure 6.7 SMS-based SVM algorithm hyperplane

Table 6.5 False alarm details

Layer	TP	TN	FP	FN	FA (FP+FN)
L3	183	155	26	35	61

where TP is the true positive (a malicious node detected as a malicious node), TN is the true negative (a trusted node identified as a trusted node), FP represents a false positive (a trusted node detected as a malicious node), and FN is a false negative (a malicious node recognized as a trusted node). The performance evaluation of the experiment is carried out by evaluating the accuracy A_c of the framework, the detection rate D_r, and the false alarm F_a rate by using the following equations (Venkatesan *et al.*, 2018).

$$A_c = (TP + TN)/(TP + TN + FP + FN), \tag{6.15}$$

$$D_r = TP/(TP + FP), \tag{6.16}$$

$$F_a = FP/(FP + TN), \tag{6.17}$$

From the experimental results and the performance evaluation, A_c is found to be 84.75%, D_r is equal to 87.55%, which was increased in comparison with the second layer, whereas the false alarm rate is equivalent to 14.36%. To the best of our knowledge, the concept of a unified SDN-based security framework stack, integrating IPS, and a hierarchical collaborative anomaly detection system has never been attempted in any previous research works.

6.6 Conclusion

In this paper, an SDN-based collaborative security framework, which combines IPS, IDS, and smart monitoring systems, taking the advantage of energy snapshot readings, is proposed and evaluated. Initially, a distributed snapshot algorithm along with a watermarking technique is introduced aiming to decrease the latency and enhance the recurrent authentication in wireless sensor nodes. Subsequently, the security features of the proposed multi-layer authentication approach regarding resiliency against various attacks are analyzed by executing automated protocol analysis using the AVISPA tool. Consequently, an IDS-enabled energy prediction model is designed at the network edge. Finally, to correlate the detection rate and reduce the false alarms that could be generated at the network edge, an SMS-based SVM algorithm is executed and tested in the control plane. In order to compute the accuracy and complexity of the proposed framework against the trusted and malicious traffic collected in the lower layers, we leveraged MATLAB. The results show that the proposed framework satisfies 5G security

requirements and simultaneously provides high security, low-computational complexity, and a considerable reduction of false alarms in SDWSNs, thanks to the introduction of the multilayer approach and recurrent snapshot readings. Furthermore, it is shown that the employment of the SMS-based SVM algorithm significantly improves the anomaly detection rate.

As for future work, we will implement the proposed security framework in an IoT-centric testbed. Moreover, our research will explore deep learning techniques to accurately classify and identify unknown anomalies in SDWSN environments with the aid of distributed SDN controllers at the edge. Such a deployment will promote decentralized decision-making and reduce the overhead introduced by the SDN controller located in the cloud.

CONCLUSION AND RECOMMENDATIONS

7.1 Conclusion

In 5G, mobile networks must guarantee specific requirements, such as ultra-low latency, network densification, ultra-low energy consumption, network virtualization, etc. Therefore, to address these requirements, the introduction of intelligence may provide cost-efficient solutions in which a particular application, security service, and quality provision are achieved. In this context, SDNs have been developed to facilitate simple programmable control of WSNs. However, WSNs are typically deployed in potentially untrusted environments. Therefore, addressing the security challenges before they can be implemented is imperative.

SDNs enhance network security by enabling global visibility of the network state. In SDNs, a standard distribution layer gathers information about the security requirements of the different services, resources, and hosts. It disseminates security by establishing commands to network elements to enforce security policies. Centralizing the network control plane and enabling network programmability can result in robust and scalable security enforcement. Therefore, in this thesis, we have presented the weaknesses and strengths of SDWNs. In doing so, we have highlighted security vulnerabilities in the data plane and communication channels of SDWNs and presented security solutions using the control and application planes. We also summarized security techniques that can strengthen network-wide security in SDWNs. Moreover, we showed security solutions that fit the 5G requirements and briefly described the costs associated with the developed solutions. To be specific, the thesis contributions are summarized as follows:

In chapter two, we proposed a cross-layer approach that amalgamates physical layer information (i.e., non-cryptographic) in conjunction with cryptographic procedures to simultaneously provide high security and low latency. Moreover, an Advanced Encryption Standard (AES)

algorithm in conjunction with the RSS dataset was leveraged to create the authentication protocol.

In chapter three, a Software-Defined Low Power IoT Network with the aim of preventing Rank attacks was presented. An RL agent using SARSA was leveraged to assist and complement an SDN controller in achieving cost-efficient route optimization and QoS provisioning packet forwarding to prevent rank attacks.

In chapter four, we presented a performance evaluation where model-free RL algorithms help the SDN controller achieve a cost-efficient solution to prevent RA harmful effects. Experimental results demonstrated that SARSA is more efficient than QL, facilitating the implementation of intrusion prevention systems in software-defined 6LowPAN.

In chapter five, we provide an overview of security issues in SD6LoWPAN, considering its resource, topology, and traffic. In addition, a study of the SDN- and ML-based security solutions that are suggested in the literature is presented. Security research challenges and trends are also put forward. In conclusion, a performance analysis of an SDN-based ML solution is presented.

Conclusively in chapter six, we addressed the security issues in the SDN's data plane. In this direction, the work introduced authentication and high-precision anomaly detection in the untrusted and resource-constrained data plane of the SDNs. To this end, a hierarchical security framework was proposed. This work amalgamated a lightweight authentication with a collaborative anomaly detection system.

7.2 Related publications

The author's Ph.D. research contributed to the following published and submitted research articles. The journal publications and conference proceedings are denoted by "J" and "C," respectively.

J1: Moreira, C. M., Kaddoum, G., Bou-Harb, Garg Sahil & kaur Kulijeet, (2019, Dic). "A Collaborative Security Framework for Software-Defined Wireless Sensor Networks" IEEE Transaction on Information and Forensics Security 2020.

J2: Moreira, C. M., Kaddoum, G., J. Baek & B.Selim, (2020, Oct). Task Allocation Framework for Software-Defined Fog v-RAN," IEEE Internet of Things journal 2021.

J3: Moreira, C. M., Kaddoum, (2021, Oct). QL vs. SARSA: Performance evaluation for intrusion prevention systems in software-defined low-power IoT networks, Submitted to International Wireless Communications and Mobile Computing Conference (IWCMC), 2023.

J4: Moreira, C. M., Kaddoum, (2021, Sept). SD6LoWPAN Security: Issues, Solutions, Research Challenges, and Trends, submitted to IEEE IoT Magazine.

C1: Moreira, C. M., Kaddoum, G., & Bou-Harb, E. (2018, May). Cross-layer authentication protocol design for ultra-dense 5G HetNets. IEEE International Conference on Communications (ICC), 2018.

C2: Moreira, C. M., Kaddoum, G., A. Boukhtouta, T.Madi & H. Alameddine, (2020, Oct). Intrusion Prevention Scheme against Rank Attacks for Software-Defined Low Power IoT Networks submitted to IEEE Access, 2022.

Besides the above articles that contribute to the main contents of this thesis, a complete list of publications that the author was involved in and which are not included in this thesis is given at the end of this thesis.

7.3 Future Work

Based on the literature review and the research outcomes of this Ph.D. thesis, following future research directions could be worth investigating.

7.3.1 Intrusion Detection Systems using Deep Reinforcement Learning approaches for Software-Defined Low Power IoT Networks

6LowPaN introduces new challenges to the conventional communication model, such as object heterogeneity and scalability, which require revolutionary solutions. Currently, there is no universal security framework for 6LowPAN. In this context, we will use an architecture based on SDNs to introduce network programmability and centralization which facilitate network abstraction and simplify network management. In this research work, we will explore SDN as a novel communication architecture for 6LowPAN to enhance the security and resilience of IoT devices. The study will investigate an Intrusion detection system based on Deep Reinforcement Learning.

7.3.2 Virtual microservices to detect and mitigate nodes misbehavior in Software-Defined IoT Networks.

As IoT network adoption is growing in diverse disciplines, cybersecurity attacks involving low-cost end-user devices are also increasing, weakening the expected deployment of IoT solutions. To address this challenge, our work will address an intrusion detection and mitigation system using NFV and SDN technologies. In this sense, virtual honeynets can be deployed with the support of the SDN and NFV support in IoT scenarios, thereby strengthening overall security. IoT honeynets are virtual microservices that emulate real IoT network deployments to distract attackers from the real target. In this direction, we will present a novel mechanism leveraging SDN and virtual microservices to deploy and detect malicious behavior on Software-defined IoT Networks.

7.3.3 Intrusion Detection Systems using Quantum Machine Learning approaches for Software-Defined Low Power IoT Networks

Intrusion Detection Systems are commonly used to detect malicious activities. Quantum computers, despite not being practical yet, are becoming available for experimental purposes. In this context, we will explore an approach for applying unsupervised Quantum Machine Learning (QML) in the context of intrusion detection for Software-Defined IoT networks from the perspective of quantum information based on the concept of quantum-assisted ML. The main goal of Quantum Machine Learning is to speed things up by applying what we know from quantum computing to machine learning. The theory of Quantum Machine Learning takes elements from classical Machine Learning theory and views quantum computing from that lens. The proposed approach will be evaluated using IBM QX in simulation mode. Moreover, we will compare the proposed method with other highly considered state-of-the-art techniques, e.g., SVM, Reinforcement Learning.

7.3.4 Quantum Cryptography solutions for 6G Networks

With the introduction of the quantum computing paradigm, some algorithms can quickly be resolved, such as asymmetric cryptographic methods. If large-scale quantum computing becomes a reality, these cryptographic primitives must be replaced by quantum-secure ones (Nanda, Puthal, Mohanty & Choppali, 2018). While large-scale quantum computing can be expected to take longer, it is time to prepare for the shift to crypto-based authentication procedures that are secure in the post-quantum world. According to current knowledge, contemporary symmetric cryptography will mostly remain safe even after the advent of quantum computing. In general, it suffices to double the size of the symmetric keys due to Grover's algorithm. The problem lies in asymmetric primitives based on integer factorization and the discrete logarithm (Ng, Conti, Long, Muller, Sayeed, Yuan & Hanzo, 2020). In this context, we want to address this challenge with an authentication procedure using a polynomial time on a quantum computer for 6G HetNets using Shor's algorithm.

4. AUTHOR'S PUBLICATIONS

During the Ph.D. research, the author contributed to the following published and submitted research articles.

Moreira, C. M., Kaddoum, G., Bou-Harb, Garg Sahil & kaur Kulijeet. "A Collaborative Security Framework for Software-Defined Wireless Sensor Networks" IEEE Transaction on Information and Forensics Security 2019.

Moreira, C. M., Kaddoum, G., J. Baek & B.Selim. Task Allocation Framework for Software-Defined Fog v-RAN," IEEE Internet of Things journal, 2020.

Moreira, C. M., Kaddoum, (2021, Oct). QL vs. SARSA: Performance evaluation for intrusion prevention systems in software-defined low-power IoT networks, Submitted to International Wireless Communications and Mobile Computing Conference (IWCMC), 2023.

Moreira, C. M., Kaddoum, (2021, Sept). SD6LoWPAN Security: Issues, Solutions, Research Challenges, and Trends, submitted to IEEE IoT Magazine.

Moreira, C. M., Kaddoum, G., & Bou-Harb, E. Cross-layer authentication protocol design for ultra-dense 5G HetNets. IEEE International Conference on Communications (ICC), 2018.

Moreira, C. M., Kaddoum, G., A. Boukhtouta, T.Madi & H. Alameddine, (2020, Oct). Intrusion Prevention Scheme against Rank Attacks for Software-Defined Low Power IoT Networks submitted to IEEE Access, 2022.

Illy, P., Kaddoum, G., Moreira, C. M., Kaur, K., & Garg, S. Securing fog-to-things environment using intrusion detection system based on ensemble learning. IEEE Wireless Communications and Networking Conference (WCNC), 2019.

BIBLIOGRAPHY

Aazam, M., Zeadally, S. & Harras, K. A. (2018). Fog computing architecture, evaluation, and future research directions. *IEEE Commun. Magazine*, 56(5), 46–52.

Abdo, J. B., Demerjian, J., Chaouchi, H. & Pujolle, G. (2013, Jan). EC-AKA2 a revolutionary AKA protocol. *2013 International Conference on Computer Applications Technology (ICCAT)*, pp. 1-6.

Abdo, J. B. B., Chaouchi, H. & Aoude, M. (2012, May). Ensured confidentiality authentication and key agreement protocol for EPS. *Symposium on Broadband Networks and Fast Internet (RELABIRA)*, pp. 73-77.

Agarwal, S., Malandrino, F., Chiasserini, C. F. & De, S. (2019). VNF placement and resource allocation for the support of vertical services in 5G networks. *IEEE ACM Trans. on Networking*, 27(1), 433–446.

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M. & Gurtov, A. (2017, Sept). 5G security: Analysis of threats and solutions. *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 193-199.

Akyildiz, I. F., Wang, P. & Lin, S.-C. (2015a). SoftAir: A software defined networking architecture for 5G wireless systems. *Computer Networks*, 85, 1–18.

Akyildiz, I. F., Wang, P. & Lin, S.-C. (2015b). SoftAir: A software defined networking architecture for 5G wireless systems. *Computer Networks*, 85, 1–18.

Akyildiz, I. F., Wang, P. & Lin, S.-C. (2015c). SoftAir: A software defined networking architecture for 5G wireless systems. *Computer Networks*, 85, 1–18.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I. & Guizani, M. (2020). A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, 22(3), 1646–1685.

Al-Kashoash, H. (2019a). *Congestion Control for 6LoWPAN Wireless Sensor Networks: Toward the Internet of Things*. Springer.

Al-Kashoash, H. (2019b). *Congestion Control for 6LoWPAN Wireless Sensor Networks: Toward the Internet of Things*. Springer.

Al-Kashoash, H. (2019c). *Congestion Control for 6LoWPAN Wireless Sensor Networks: Toward the Internet of Things*. Springer.

Alavi, B. & Pahlavan, K. (2006). Modeling of the TOA-based distance measurement error using UWB indoor radio measurements. *IEEE communications letters*, 10(4), 275–277.

Ali, O., Ishak, M. K., Zawawi, M. A. M., Seman, M. T. A., Bhatti, M. K. L. & Yusoff, Z. Y. M. (2020). A MAC Protocol for Energy Efficient Wireless Communication Leveraging Wake-Up Estimations on Sender Data. *IEEE Int. Conf. Electrical Engineering*, pp. 45–50.

Altinok, A. & Turk, M. (2003). Temporal integration for continuous multimodal biometrics. *Proceedings of the Workshop on Multimodal User Authentication*.

Amande, V., Kaur, K., Garg, S. & Guizani, M. (2022). LASUA: A Lightweight Authentication Scheme with User Anonymity for IoT-Enabled Mobile Cloud. *IEEE Global Communications Conference*, pp. 3563–3568.

Ambusaidi, M. A., He, X., Nanda, P. & Tan, Z. (2016). Building an intrusion detection system using a filter-based feature selection algorithm. *IEEE Trans. Comput.*, 65, 2986–2998.

Amjad, M., Qureshi, H. K., Lestas, M., Mumtaz, S. & Rodrigues, J. J. (2018). Energy Prediction Based MAC Layer Optimization for Harvesting Enabled WSNs in Smart Cities. *IEEE Veh. Technology Conf.*, pp. 1–6.

Ancillotti, E., Vallati, C., Bruno, R. & Mingozzi, E. (2017a). A reinforcement learning-based link quality estimation strategy for RPL and its impact on topology management. *Computer Communications*, 112, 1–13.

Ancillotti, E., Vallati, C., Bruno, R. & Mingozzi, E. (2017b). A reinforcement learning-based link quality estimation strategy for RPL and its impact on topology management. *Computer Communications*, 112, 1–13.

Ancillotti, E., Vallati, C., Bruno, R. & Mingozzi, E. (2017c). A reinforcement learning-based link quality estimation strategy for RPL and its impact on topology management. *Computer Communications*, 112, 1–13.

Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C. K. & Zhang, J. C. (2014). What Will 5G Be? *J. Sel. Areas Commun.*, 32(6), 1065-1082.

Arış, A. & Oktuğ, S. F. (2020). Analysis of the RPL Version Number Attack with Multiple Attackers. *IEEE Int. Conf. Cyber Situational Awareness, Data Analytics and Assessment*, pp. 1–8.

Arnob, S. S., Shovon, I. I., Ahmed, T., Ullah, M. S. & Shelim, R. (2020). Dual-Order Resource Allocation in 5G H-CRAN Using Matching Theory and Ant Colony Optimization Algorithm. *IEEE Ind. Elect. Soc.*, pp. 2101–2107.

Arulkumaran, K., Deisenroth, M. P., Brundage, M. & Bharath, A. A. (2017). Deep reinforcement learning: A brief survey. *IEEE Signal Processing Magazine*, 34(6), 26–38.

Asif, M. & Muneer, T. (2007). Energy supply, its demand and security issues for developed and emerging economies. *Renewable and Sustainable Energy Reviews*, 1388–1413.

Babbar, H., Rani, S., Garg, S., Kaddoum, G., Piran, M. J. & Hossain, M. S. (2021). A secure multi-layer architecture for software-defined space information networks (SDSINs). *IEEE Consumer Electronics Magazine*.

Baddeley, M., Nejabati, R., Oikonomou, G., Sooriyabandara, M. & Simeonidou, D. (2018a). Evolving SDN for low-power IoT networks. *IEEE Conf. Network Softw. and Workshops*, pp. 71–79.

Baddeley, M., Nejabati, R., Oikonomou, G., Sooriyabandara, M. & Simeonidou, D. (2018b). Evolving SDN for low-power IoT networks. *IEEE Conf. Network Softw. and Workshops*, pp. 71–79.

Baddeley, M., Nejabati, R., Oikonomou, G., Sooriyabandara, M. & Simeonidou, D. (2018c). Evolving SDN for low-power IoT networks. *IEEE Conf. Network Softw. and Workshops*, pp. 71–79.

Baek, J.-y., Kaddoum, G., Garg, S., Kaur, K. & Gravel, V. (2019). Managing fog networks using reinforcement learning based load balancing algorithm. *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7.

Baek, J. & Kaddoum, G. (2020). Heterogeneous task offloading and resource allocations via deep recurrent reinforcement learning in partial observable multifog networks. *IEEE Internet of Things Journal*, 8(2), 1041–1056.

Baghani, A. S., Rahimpour, S. & Khabbazian, M. (2021). The DAO Induction Attack: Analysis and Countermeasure. *IEEE Internet of Things Journal*.

Baliga, A., Kamat, P. & Iftode, L. (2007). Lurking in the shadows: Identifying systemic threats to kernel data. *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pp. 246–251.

Bauer, C. I. & Rees, S. J. (2002). Classification of handover schemes within a cellular environment. *Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on*, 5, 2199–2203.

Bays, L. R., Oliveira, R. R., Barcellos, M. P., Gaspary, L. P. & Madeira, E. R. M. (2015a). Virtual network security: threats, countermeasures, and challenges. *Journal of Internet Services and Applications*, 6(1), 1.

Bays, L. R., Oliveira, R. R., Barcellos, M. P., Gaspary, L. P. & Madeira, E. R. M. (2015b). Virtual network security: threats, countermeasures, and challenges. *Journal of Internet Services and Applications*, 6(1), 1.

Benton, K., Camp, L. J. & Small, C. (2013). OpenFlow vulnerability assessment. *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pp. 151–152.

Bettoumi, B. & Bouallegue, R. (2021). Efficient Reduction of the Transmission Delay of the Authentication Based Elliptic Curve Cryptography in 6LoWPAN Wireless Sensor Networks in the Internet of Things. *IEEE Int. Wireless Commun. and Mobile Computing*, pp. 1471–1476.

Bharadia, D., Choi, J.-I., Jain, M., Katti, S., Kim, T. M. & Levis, P. (2019). Adaptive techniques for full duplex communications. Google Patents. US Patent 10,230,419.

Bhutani, G. (2010). A near-optimal scheme for tcp ack pacing to maintain throughput in wireless networks. *Communication Systems and Networks (COMSNETS), 2010 Second International Conference on*, pp. 1–7.

Bikos, A. N. & Sklavos, N. (2013). LTE/SAE security issues on 4G wireless networks. *IEEE Security & Privacy*, 55–62.

Boggs, N., Hiremagalore, S., Stavrou, A. & Stolfo, S. J. (2011). Cross-domain collaborative anomaly detection: So far yet so close. *Int. Workshop on Recent Advances in IDS*, pp. 142–160.

Boubiche, D. E., Boubiche, S. & Bilami, A. (2015). A cross-layer watermarking-based mechanism for data aggregation integrity in heterogeneous WSNs. *IEEE Commun. Letters*, 19(5), 823–826.

Boudouaia, M. A., Ali-Pacha, A., Abouaissa, A. & Lorenz, P. (2020a). Security Against Rank Attack in RPL Protocol. *IEEE Network*, 34(4), 133–139.

Boudouaia, M. A., Ali-Pacha, A., Abouaissa, A. & Lorenz, P. (2020b). Security Against Rank Attack in RPL Protocol. *IEEE Network*, 34(4), 133–139.

Brik, V., Banerjee, S., Gruteser, M. & Oh, S. (2008). Wireless device identification with radiometric signatures. *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pp. 116–127.

Broumi, S., Bakal, A., Talea, M., Smarandache, F. & Vladareanu, L. (2016). Applying Dijkstra algorithm for solving neutrosophic shortest path problem. *IEEE, Int. Conf. on Adv. Mechat. Syst.*, pp. 412–416.

Bu, S., Yu, F. R., Liu, X. P., Mason, P. & Tang, H. (2011). Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. *IEEE transactions on vehicular technology*, 60(3), 1025–1036.

Cammarano, A., Petrioli, C. & Spenza, D. (2016). Online energy harvesting prediction in environmentally powered wireless sensor networks. *IEEE Sensors Journal*, 16(17), 6793–6804.

Cao, H., Garg, S., Kaddoum, G., Hassan, M. M. & AlQahtani, S. A. (2022). Intelligent virtual resource allocation of QoS-guaranteed slices in B5G-Enabled VANETs for intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 23(10), 19704–19713.

Cao, K., Cai, Y., Wu, Y. & Yang, W. (2018). Secure transmission for MISOME wiretap channels with finite alphabet inputs. *IEEE Wireless Communications Letters*, 7(4), 570–573.

Capossele, A. T., Cervo, V., Petrioli, C. & Spenza, D. (2016). Counteracting denial-of-sleep attacks in wake-up-radio-based sensing systems. *IEEE Int. Conf. Sensing, Commun. and Networking*, pp. 1–9.

Cardellini, V., Colajanni, M. & Yu, P. S. (1999). Dynamic load balancing on web-server systems. *IEEE Internet Comput.*, 3(3), 28–39.

Carloni, L. P. (2015). From latency-insensitive design to communication-based system-level design. *Proceedings of the IEEE*, 103(11), 2133–2151.

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C. & Faruki, P. (2019). Network intrusion detection for IoT security based on learning techniques. *IEEE Communications Surveys & Tutorials*, 21(3), 2671–2701.

Chakrabarty, S. & Engels, D. W. (2016). A secure IoT architecture for smart cities. *IEEE Conference Communications & Networking*, pp. 812–813.

Chang, C.-C., Hsiao, J.-Y. & Chan, C.-S. (2003). Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, 36, 1583–1595.

Chang, R.-S., Chang, J.-S. & Lin, P.-S. (2009). An ant algorithm for balanced job scheduling in grids. *Future Generation Computer Systems*, 25(1), 20–27.

Charfi, M., Mouradian, A. & Vèque, V. (2020a). Networking Functions for Wireless Sensor Network Applications: an SDN-based Approach. *IEEE Int. Conf. Commun.*, pp. 1–7.

Charfi, M., Mouradian, A. & Vèque, V. (2020b). Networking Functions for Wireless Sensor Network Applications: an SDN-based Approach. *IEEE Int. Conf. Commun.*, pp. 1–7.

Charfi, M., Mouradian, A. & Vèque, V. (2020c). Networking Functions for Wireless Sensor Network Applications: an SDN-based Approach. *IEEE Int. Conf. Commun.*, pp. 1–7.

Checko, A., Christiansen, H. L., Yan, Y., Scolari, L., Kardaras, G., Berger, M. S. & Dittmann, L. (2015). Cloud RAN for mobile networks—A technology overview. *IEEE Commun. surveys & tutorials*, 17(1), 405–426.

Chen, M., Qian, Y., Mao, S., Tang, W. & Yang, X. (2016). Software-defined mobile networks security. *Mobile Networks and Applications*, 729–743.

Chen, Y., Yang, J., Trappe, W. & Martin, R. P. (2010). Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks. *IEEE Trans. on Vehicular Technol.*, 59(5), 2418-2434.

Chen, Y. & Vaidya, U. (2019). Sample Complexity for Nonlinear Stochastic Dynamics. *IEEE Americ. Ctrl Conf.*, pp. 3526–3531.

Chettibi, S. & Chikhi, S. (2012a). An adaptive energy-aware routing protocol for MANETs using the SARSA reinforcement learning algorithm. *IEEE Conf. Evolv. and Adapt. Intel. Syst.*, pp. 84–89.

Chettibi, S. & Chikhi, S. (2012b). An adaptive energy-aware routing protocol for MANETs using the SARSA reinforcement learning algorithm. *IEEE Conf. Evolv. and Adapt. Intel. Syst.*, pp. 84–89.

Chin, W. H., Fan, Z. & Haines, R. (2014). Emerging technologies and research challenges for 5G wireless networks. *IEEE Wireless Communications*, 106–112.

Cho, H.-H., Lai, C.-F., Shih, T. K. & Chao, H.-C. (2014). Integration of SDR and SDN for 5G. *IEEE Access*, 2, 1196–1204.

Chu, Z., Zhou, F., Zhu, Z., Hu, R. Q. & Xiao, P. (2018). Wireless powered sensor networks for internet of things: Maximum throughput and optimal power allocation. *IEEE Internet Things*, 5(1), 310–321.

Cisco, C. V. N. Global Mobile Data Traffic Forecast Update, Cisco White Paper.

Consortium, O. et al. (2017). OpenFog Reference Architecture for Fog Computing.(February 2017).

Costa-Requena, J., Santos, J. L., Guasch, V. F., Ahokas, K., Premsankar, G., Luukkainen, S., Pérez, O. L., Itzazelaia, M. U., Ahmad, I., Liyanage, M. et al. (2015). SDN and NFV integration in generalized mobile network architecture. *Networks and Communications (EuCNC), 2015 European Conference on*, pp. 154–158.

Dai, B. & Luo, Y. (2018). An improved feedback coding scheme for the wire-tap channel. *IEEE Transactions on Information Forensics and Security*, 14(1), 262–271.

Dandachi, G., Chahed, T., Elayoubi, S. E., Taher, N. C. & Fawal, Z. (2017a). Joint allocation strategies for radio and processing resources in Virtual Radio Access Networks (v-RAN). *IEEE Int. Symp. Personal, Indoor, and Mobile Radio Commun.*, pp. 1–6.

Dandachi, G., Chahed, T., Elayoubi, S. E., Taher, N. C. & Fawal, Z. (2017b). Joint allocation strategies for radio and processing resources in Virtual Radio Access Networks (v-RAN). *IEEE Int. Symp. Pers., Ind., and Mobile Radio Commun.*, pp. 1–6.

Dandachi, G., Chahed, T., Elayoubi, S. E., Taher, N. C. & Fawal, Z. (2017c). Joint allocation strategies for radio and processing resources in Virtual Radio Access Networks (v-RAN). *IEEE Int. Symp. Personal, Indoor, and Mobile Radio Commun.*, pp. 1–6.

Danev, B., Luecken, H., Capkun, S. & El Defrawy, K. (2010). Attacks on physical-layer identification. *Proceedings of the third ACM conference on Wireless network security*, pp. 89–98.

Dastjerdi, A. V. & Buyya, R. (2016). Fog computing: Helping the Internet of Things realize its potential. *IEEE Computer*, 49(8), 112–116.

De Araujo-Filho, P. F., Pinheiro, A. J., Kaddoum, G., Campelo, D. R. & Soares, F. L. (2021). An efficient intrusion prevention system for CAN: Hindering cyber-attacks with a low-cost platform. *IEEE Access*, 9, 166855–166869.

de Araujo-Filho, P. F., Kaddoum, G., Naili, M., Fapi, E. T. & Zhu, Z. (2022). Multi-objective GAN-based adversarial attack technique for modulation classifiers. *IEEE Communications Letters*, 26(7), 1583–1587.

De Gante, A., Aslan, M. & Matrawy, A. (2014). Smart wireless sensor network management based on software-defined networking. *IEEE Commun. Biennial Symp.*, pp. 71–75.

de Oliveira, D. A. S. & Wu, S. F. (2009). Protecting kernel code and data with a virtualization-aware collaborative operating system. *Computer Security Applications Conference, 2009. ACSAC'09. Annual*, pp. 451–460.

Deng, H., Zeng, Q.-A. & Agrawal, D. P. (2003). SVM-based intrusion detection system for wireless ad hoc networks. *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, 3, 2147–2151.

Deng, H., Sun, X., Wang, B. & Cao, Y. (2009a). Selective forwarding attack detection using watermark in WSNs. *IEEE Int. Colloq. Computing, Communication, Control, and Management*, 3, 109–113.

Deng, Y., Fu, H., Xie, X., Zhou, J., Zhang, Y. & Shi, J. (2009b, Nov). A novel 3GPP SAE authentication and key agreement protocol. *IEEE Int. Conf. Network*, pp. 557-561.

Devipriya, S. & Ramesh, C. (2013). Improved Max-min heuristic model for task scheduling in cloud. *2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE)*, pp. 883–888.

Djedjig, N., Tandjaoui, D., Medjek, F. & Romdhani, I. (2017a). New trust metric for the RPL routing protocol. *IEEE Int. Conf. Inf. and Commun. Sys.*, pp. 328–335.

Djedjig, N., Tandjaoui, D., Medjek, F. & Romdhani, I. (2017b). New trust metric for the RPL routing protocol. *IEEE Int. Conf. Inf. and Commun. Sys.*, pp. 328–335.

Djedjig, N., Tandjaoui, D., Medjek, F. & Romdhani, I. (2017c). New trust metric for the RPL routing protocol. *IEEE Int. Conf. Inf. and Commun. Sys.*, pp. 328–335.

Dorigo, M., Maniezzo, V. & Colorni, A. (1996). Ant system: optimization by a colony of cooperating agents. *IEEE Trans. Syst., Man, Cybern.*, 26(1), 29–41.

Dos Santos, J., Terrasson, G. & Llaria, A. (2020a). Improving Low Power Listening (LPL) Mechanism to Save Energy Consumption in WSN. *IEEE Sensors*, pp. 1–4.

Dos Santos, J., Terrasson, G. & Llaria, A. (2020b). Improving Low Power Listening (LPL) Mechanism to Save Energy Consumption in WSN. *IEEE Sensors*, pp. 1–4.

Du, J., Zhao, L., Feng, J. & Chu, X. (2018). Computation offloading and resource allocation in mixed fog/cloud Comput. systems with Min-max fairness guarantee. *IEEE Trans. Commun.*, 66(4), 1594–1608.

Duan, X. & Wang, X. (2016, May). Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer. *IEEE International Conference on Communications (ICC)*, pp. 1-6.

Dvir, A., Buttyan, L. et al. (2011). VeRA-version number and rank authentication in RPL. *IEEE Int. Conf. Mobile Ad-Hoc and Sensor Syst.*, pp. 709–714.

Engblom, J. & Ermedahl, A. (2000). Modeling complex flows for worst-case execution time analysis. *null*, pp. 163.

Erdol, H., Gormus, S. & Aydogdu, M. C. (2017). A novel energy aware routing function for Internet of Things networks. *IEEE Int. Conf. Electrical Engineering*, pp. 1314–1318.

Ericsson, W. P. 5G Security, Ericsson White Paper.

ETSI, W. P. NFV, ETSI White Paper.

Fan, Q. & Ansari, N. (2018). Towards workload balancing in fog computing empowered IoT. *IEEE Trans. on Network*.

Farzaneh, B., Koosha, M., Boochanpour, E. & Alizadeh, E. (2020). A new method for intrusion detection on RPL routing protocol using fuzzy logic. *IEEE Int. Conf. Web Research*, pp. 245–250.

Fawcett, L., Scott-Hayward, S., Broadbent, M., Wright, A. & Race, N. (2018). Tennison: a distributed SDN framework for scalable network security. *IEEE Journal on Sel. Areas in Commun.*, 36(12), 2805–2818.

Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M. & Inácio, P. R. (2014). Security issues in cloud environments: a survey. *International Journal of Information Security*, 13(2), 113–170.

Ferrag, M. A. & Shu, L. (2021). The Performance Evaluation of Blockchain-based Security and Privacy Systems for the Internet of Things: A Tutorial. *IEEE Internet of Things Journal*.

Fisser, L., Ipach, H., Timm-Giel, A. & Becker, C. (2020). Evaluation of LTE based Communication for Fast State Estimation in Low Voltage Grids. *IEEE Int. Conf. Commun.*, pp. 1–7.

Fragkiadakis, A. G., Tragos, E. Z. & Askoxylakis, I. G. (2012). A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys & Tutorials*, 15(1), 428–445.

Gajera, V., Gupta, R., Jana, P. K. et al. (2016). An effective multi-objective task scheduling algorithm using Min-max normalization in cloud Comput. *IEEE Conf. Theoretical Comp. and Commun. Technol.*, pp. 812–816.

Garg, S., Kaur, K., Kaddoum, G., Garigipati, P. & Aujla, G. S. (2021). Security in IoT-driven mobile edge computing: New paradigms, challenges, and opportunities. *IEEE Network*, 35(5), 298–305.

Glissa, G., Rachedi, A. & Meddeb, A. (2016a). A secure routing protocol based on RPL for Internet of Things. *IEEE Global Commun. Conf.*, pp. 1–7.

Glissa, G., Rachedi, A. & Meddeb, A. (2016b). A secure routing protocol based on RPL for Internet of Things. *IEEE Global Commun. Conf.*, pp. 1–7.

Gonzalez, C., Charfadine, S. M., Flauzac, O. & Nolot, F. (2016). SDN-based security framework for the IoT in distributed grid. *IEEE international multidisciplinary conference on computer and energy science (SpliTech)*, pp. 1–5.

Guan, Q., Yu, F. R., Jiang, S. & Wei, G. (2010). Prediction-based topology control and routing in cognitive radio mobile ad hoc networks. *IEEE Transactions on Vehicular Technology*, 59(9), 4443–4452.

Guo, F. & Chiueh, T.-c. (2005a). Sequence number-based MAC address spoof detection. *International Workshop on Recent Advances in Intrusion Detection*, pp. 309–329.

Guo, F. & Chiueh, T.-c. (2005b). Sequence number-based MAC address spoof detection. *International Workshop on Recent Advances in Intrusion Detection*, pp. 309–329.

Guo, G. (2021). A Lightweight Countermeasure to DIS Attack in RPL Routing Protocol. *IEEE Comput. and Commun. Conf.*, pp. 0753–0758.

Gupta, A. & Garg, R. (2017). Load balancing based task scheduling with ACO in cloud Computing. *IEEE Int. Conf. Computer and Applications*, pp. 174–179.

Gures, E., Shayea, I., Alhammadi, A., Ergen, M. & Mohamad, H. (2020). A Comprehensive Survey on Mobility Management in 5G Heterogeneous Networks: Architectures, Challenges and Solutions. *IEEE Access*.

Gurung, S. & Chauhan, S. (2017). A review of black-hole attack mitigation techniques and its drawbacks in mobile ad-hoc network. *IEEE Trans. Signal Process.*, pp. 2379–2385.

Habib, A., Khan, M. I. & Uddin, J. (2016a). Optimal route selection in complex multi-stage supply chain networks using SARSA (λ). *IEEE Int. Conf. Comp. and Inf. Technol.*, pp. 170–175.

Habib, C., Makhoul, A., Darazi, R. & Salim, C. (2016b). Self-adaptive data collection and fusion for health monitoring based on body sensor networks. *IEEE Trans. Ind. Inform.*, 12, 2342–2352.

Hajizadeh, H., Nabi, M., Vermeulen, M. & Goossens, K. (2021). Coexistence Analysis of Colocated BLE and IEEE 802.15. 4 TSCH Networks. *IEEE Sensors Journal*.

Haken, H. & Mayer-Kress, G. (1981). Chapman-Kolmogorov equation and path integrals for discrete chaos in presence of noise. *Zeitschrift für Physik B Condensed Matter*, 43(2), 185–187.

Hamandi, K., Sarji, I., Chehab, A., Elhajj, I. H. & Kayssi, A. (2013, March). Privacy Enhanced and Computationally Efficient HSK-AKA LTE Scheme. *27th International Conference on Advanced Information Networking and Applications Workshops*, pp. 929-934.

Hameed, K., Khan, A., Ahmed, M., Reddy, A. G. & Rathore, M. M. (2018). Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks. *Future Generation Computer Systems*, 82, 274–289.

Hamid, M. A., Rashid, M. & Hong, C. S. (2006). Routing security in sensor network: Hello flood attack and defense. *IEEE ICNEWS*, 2–4.

Han, G., Jiang, J., Shen, W., Shu, L. & Rodrigues, J. (2013a). IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks. *IET Information Security*, 7(2), 97–105.

Han, G., Jiang, J., Shen, W., Shu, L. & Rodrigues, J. (2013b). IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks. *IET Inform. Security*, 7(2), 97–105.

Hao, P., Wang, X. & Behnad, A. (2014, Jun). Performance enhancement of I/Q imbalance based wireless device authentication through collaboration of multiple receivers. *IEEE International Conf. on Commun. (ICC)*, pp. 939-944.

Hawilo, H., Shami, A., Mirahmadi, M. & Asal, R. (2014). NFV: state of the art, challenges, and implementation in next generation mobile networks (vEPC). *IEEE Network*, 18–26.

Hennebert, C. & Dos Santos, J. (2014a). Security protocols and privacy issues into 6LoWPAN stack: A synthesis. *IEEE Internet of Things Journal*, 1(5), 384–398.

Hennebert, C. & Dos Santos, J. (2014b). Security protocols and privacy issues into 6LoWPAN stack: A synthesis. *IEEE Internet of Things Journal*, 1(5), 384–398.

Hill, M. D. & Marty, M. R. (2008). Amdahl's law in the multicore era. *IEEE Computer*, 41(7), 33–38.

Hong, S., Xu, L., Wang, H. & Gu, G. (2015). Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures. *NDSS*, 15, 8–11.

Honkavirta, V., Perala, T., Ali-Loytty, S. & Piche, R. (2009, March). A comparative survey of WLAN location fingerprinting methods. *6th Workshop on Positioning, Navigation and Communication*, pp. 243-251.

Hou, W., Wang, X. & Chouinard, J. Y. (2012, Jun). Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates. *IEEE International Conference on Communications (ICC)*, pp. 3559-3563.

Hsieh, Y.-C., Hong, H.-J., Tsai, P.-H., Wang, Y.-R., Zhu, Q., Uddin, M. Y. S., Venkatasubramanian, N. & Hsu, C.-H. (2018). Managed edge computing on Internet-of-Things devices for smart city applications. *IEEE/IFIP Network Operations and Management Symp.*, pp. 1–2.

Illy, P., Kaddoum, G., Moreira, C. M., Kaur, K. & Garg, S. (2019). Securing fog-to-things environment using intrusion detection system based on ensemble learning. *2019 IEEE wireless communications and networking conference (WCNC)*, pp. 1–7.

Illy, P., Kaddoum, G., de Araujo-Filho, P. F., Kaur, K. & Garg, S. (2022a). A hybrid multistage DNN-based collaborative IDPS for high-risk smart factory networks. *IEEE Transactions on Network and Service Management*.

Illy, P., Kaddoum, G., de Araujo-Filho, P. F., Kaur, K. & Garg, S. (2022b). A hybrid multistage DNN-based collaborative IDPS for high-risk smart factory networks. *IEEE Transactions on Network and Service Management*.

Illy, P., Kaddoum, G., Kaur, K. & Garg, S. (2022c). ML-based IDPS enhancement with complementary features for home IoT networks. *IEEE Transactions on Network and Service Management*, 19(2), 772–783.

İnçki, K. & Ari, I. (2018). A novel runtime verification solution for IoT systems. *IEEE Access*, 6, 13501–13512.

İnçki, K., Arı, İ. & Sözer, H. (2017). Runtime verification of iot systems using complex event processing. *Int. Conf. Networking, Sensing, and Control*, pp. 625–630.

Index, C. V. N. Global Mobile Data Traffic Forecast Update, Cisco White Paper.

Iova, O., Picco, P., Istomin, T. & Kiraly, C. (2016a). RPL: The routing standard for the internet of things... or is it? *IEEE Communications Magazine*, 54(12), 16–22.

Iova, O., Picco, P., Istomin, T. & Kiraly, C. (2016b). RPL: The routing standard for the internet of things... or is it? *IEEE Communications Magazine*, 54(12), 16–22.

Iova, O., Picco, P., Istomin, T. & Kiraly, C. (2016c). RPL: The routing standard for the internet of things... or is it? *IEEE Communications Magazine*, 54(12), 16–22.

Islam, T. & Hasan, M. S. (2017). A performance comparison of load balancing algorithms for cloud computing. *IEEE Int. Conf. on the Frontiers and Advances in Data Science*, pp. 130–135.

Iwata, K. (2016a). Extending the peak bandwidth of parameters for softmax selection in reinforcement learning. *IEEE trans. neural networks and learning systems*, 28(8), 1865–1877.

Iwata, K. (2016b). Extending the peak bandwidth of parameters for softmax selection in reinforcement learning. *IEEE trans. neural networks and learning systems*, 28(8), 1865–1877.

Iwata, K. (2016c). Extending the peak bandwidth of parameters for softmax selection in reinforcement learning. *IEEE trans. neural networks and learning systems*, 28(8), 1865–1877.

Jagadiswary, D. & Saraswady, D. (2016). Biometric authentication using fused multimodal biometric. *Procedia Computer Science*, 85, 109–116.

Jan, M. A., Nanda, P., He, X. & Liu, R. P. (2015). A sybil attack detection scheme for a centralized clustering-based hierarchical network. *IEEE Trustcom/BigDataSE/ISPA*, 1, 318–325.

Jana, S. & Kasera, S. K. (2010). On fast and accurate detection of unauthorized wireless access points using clock skews. *IEEE Transactions on Mobile Computing*, 9(3), 449–462.

Jang, H.-C. & Lin, T.-K. (2018a). Traffic-Aware Traffic Signal Control Framework Based on SDN and Cloud-Fog Computing. *IEEE Vehic. Technol. Conf.*, pp. 1–5.

Jang, H.-C. & Lin, T.-K. (2018b). Traffic-Aware Traffic Signal Control Framework Based on SDN and Cloud-Fog Computing. *IEEE Vehic. Technol. Conf.*, pp. 1–5.

Jang, H.-C. & Lin, T.-K. (2018c). Traffic-Aware Traffic Signal Control Framework Based on SDN and Cloud-Fog Computing. *IEEE Vehic. Technol. Conf.*, pp. 1–5.

Jaswal, G., Kaul, A. & Nath, R. (2019). Multimodal Biometric Authentication System Using Hand Shape, Palm Print, and Hand Geometry. In *Computational Intel.: Theories, App. and Future Directions* (pp. 557–570). Springer.

Javaid, S., Javaid, N., Tayyaba, S. K., Sattar, N. A., Ruqia, B. & Zahid, M. (2018). Resource allocation using Fog-2-Cloud based environment for smart buildings. *IEEE Int. Wireless Commun.*, pp. 1173–1177.

Ji, S., Chen, T. & Zhong, S. (2015). Wormhole attack detection algorithms in wireless network coding systems. *IEEE Trans. mobile computing*, 14, 660–674.

Jinhui, X., Yang, T., Feiyue, Y., Leina, P., Juan, X. & Yao, H. (2018). Intrusion detection system for hybrid DoS attacks using energy trust in wireless sensor networks. *Procedia computer science*, 131, 1188–1195.

Kamble, A., Malemath, V. S. & Patil, D. (2017a). Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. *IEEE Int. Conf. Emerging Trends & Innovation in ICT*, pp. 33–39.

Kamble, A., Malemath, V. S. & Patil, D. (2017b). Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. *IEEE Int. Conf. Emerging Trends & Innovation*, pp. 33–39.

Kamble, A., Malemath, V. S. & Patil, D. (2017c). Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. *IEEE Int. Conf. Emerging Trends & Innovation in ICT*, pp. 33–39.

Kamble, A., Malemath, V. S. & Patil, D. (2017d). Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. *IEEE Int. Conf. Emerging Trends & Innovation*, pp. 33–39.

Kamble, A., Malemath, V. S. & Patil, D. (2017e). Security attacks and secure routing protocols in RPL-based Internet of Things: Survey. *IEEE Int. Conf. Emerging Trends & Innovation in ICT*, pp. 33–39.

Kaur, K., Garg, S., Kaddoum, G. & Guizani, M. (2020). Secure authentication and key agreement protocol for tactile internet-based tele-surgery ecosystem. *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–6.

Kaur, M. & Singh, A. (2016). Detection and mitigation of sinkhole attack in wireless sensor network. *IEEE Int. Conf. micro-electronics and Telecommun. engineering*, pp. 217–221.

Keramati, M. & Keramati, M. (2014a, Sep.). Novel security metrics for ranking vulnerabilities in computer networks. *IEEE Int. Symp. Telecommun.*, pp. 883-888.

Keramati, M. & Keramati, M. (2014b, Sep.). Novel security metrics for ranking vulnerabilities in computer networks. *IEEE Int. Symp. Telecommun.*, pp. 883-888.

Keramati, M. & Keramati, M. (2014c, Sep.). Novel security metrics for ranking vulnerabilities in computer networks. *IEEE Int. Symp. Telecommun.*, pp. 883-888.

Khallef, W., Molnar, M., Benslimane, A. & Durand, S. (2017a). Multiple constrained QoS routing with RPL. *IEEE Int. Conf. on Commun.*, pp. 1–6.

Khallef, W., Molnar, M., Benslimane, A. & Durand, S. (2017b). Multiple constrained QoS routing with RPL. *IEEE Int. Conf. on Commun.*, pp. 1–6.

Khallef, W., Molnar, M., Benslimane, A. & Durand, S. (2017c). Multiple constrained QoS routing with RPL. *IEEE Int. Conf. on Commun.*, pp. 1–6.

Khan, A., Javed, Y., Abdullah, J., Nazim, J. & Khan, N. (2017). Security issues in 5G device to device communication. *IJCSNS*, 366.

Khan, M. Z., Harous, S., Hassan, S. U., Khan, M. U. G., Iqbal, R. & Mumtaz, S. (2019). Deep unified model for face recognition based on convolution neural network and edge computing. *IEEE Access*, 7, 72622–72633.

Kiani, A., Ansari, N. & Khreishah, A. (2019). Hierarchical capacity provisioning for fog computing. *IEEE/ACM Trans. on Networking*.

Kim, J., Kim, J., Thu, H. L. T. & Kim, H. (2016). Long short term memory recurrent neural network classifier for intrusion detection. *IEEE Int. Conf. Plat. Technol. and Service*, pp. 1–5.

Kim, W., Stanković, M. S., Johansson, K. H. & Kim, H. J. (2015). A distributed support vector machine learning over wireless sensor networks. *IEEE Trans. Cybernetics*, 45, 2599–2611.

Kloti, R., Kotronis, V. & Smith, P. (2013a). Openflow: A security analysis. *Network Protocols (ICNP), 2013 21st IEEE International Conference on*, pp. 1–6.

Kloti, R., Kotronis, V. & Smith, P. (2013b). Openflow: A security analysis. *Network Protocols (ICNP), 2013 21st IEEE International Conference on*, pp. 1–6.

Kobo, H. I., Abu-Mahfouz, A. M. & Hancke, G. P. (2017a). A survey on software-defined wireless sensor networks: Challenges and design requirements. *IEEE access*, 5, 1872–1899.

Kobo, H. I., Abu-Mahfouz, A. M. & Hancke, G. P. (2017b). A survey on software-defined wireless sensor networks: Challenges and design requirements. *IEEE access*, 5, 1872–1899.

Kobo, H. I., Abu-Mahfouz, A. M. & Hancke, G. P. (2017c). A survey on software-defined wireless sensor networks: Challenges and design requirements. *IEEE access*, 5, 1872–1899.

Kobo, H. I., Abu-Mahfouz, A. M. & Hancke, G. P. (2017d). A survey on software-defined wireless sensor networks: Challenges and design requirements. *IEEE access*, 5, 1872–1899.

Kocakulak, M. & Butun, I. (2017a). An overview of Wireless Sensor Networks towards internet of things. *Computing and Commun. Workshop and Conf.*, pp. 1–6.

Kocakulak, M. & Butun, I. (2017b). An overview of Wireless Sensor Networks towards internet of things. *Computing and Commun. Workshop and Conf.*, pp. 1–6.

Kocakulak, M. & Butun, I. (2017c). An overview of Wireless Sensor Networks towards internet of things. *IEEE Computing and Commun.*, pp. 1–6.

Koien, G. M. (2011, July). Mutual entity authentication for LTE. *7th International Wireless Communications and Mobile Computing Conference*, pp. 689-694.

Kong, L. & Kaddoum, G. (2019). Secrecy characteristics with assistance of mixture gamma distribution. *IEEE Wireless Communications Letters*, 8(4), 1086–1089.

Koreman, J., Morris, A., Wu, D., Jassim, S., Sellahewa, H., Ehlers, J., Chollet, G., Aversano, G., Bredin, H., Garcia-Salicetti, S. et al. (2006). Multi-modal biometric authentication on the SecurePhone PDA.

Kreutz, D., Ramos, F. & Verissimo, P. (2013). Towards secure and dependable software-defined networks. *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pp. 55–60.

Kumar, M., Mukherjee, P., Verma, K., Verma, S. & Rawat, D. B. (2021). Improved Deep Convolutional Neural Network based Malicious Node Detection and Energy-Efficient Data Transmission in Wireless Sensor Networks. *IEEE Tran. Network Science and Engineering*.

Küpper, A. & Treu, G. (2006). Efficient proximity and separation detection among mobile targets for supporting location-based community services. *ACM SIGMOBILE Mobile Computing and Communications Review*, 10(3), 1–12.

Lal, S., Taleb, T. & Dutta, A. (2017). NFV: Security threats and best practices. *IEEE Communications Magazine*, 55(8), 211–217.

Lasso, F. F. J., Clarke, K. & Nirmalathas, A. (2018a). A software-defined networking framework for IoT based on 6LoWPAN. *2018 Wireless Telecommunications Symposium*, pp. 1-7.

Lasso, F. F. J., Clarke, K. & Nirmalathas, A. (2018b). A software-defined networking framework for IoT based on 6LoWPAN. *2018 Wireless Telecommunications Symposium*, pp. 1-7.

Lasso, F. F. J., Clarke, K. & Nirmalathas, A. (2018c). A software-defined networking framework for IoT based on 6LoWPAN. *2018 Wireless Telecommunications Symposium*, pp. 1-7.

Lasso, F. F. J., Clarke, K. & Nirmalathas, A. (2018d). A software-defined networking framework for IoT based on 6LoWPAN. *IEEE Wireless Telecommunications Symposium*, pp. 1-7.

Levis, P., Clausen, T., Hui, J., Gnawali, O. & Ko, J. (2011a). The trickle algorithm. *Internet Engineering Task Force, RFC6206*.

Levis, P., Clausen, T., Hui, J., Gnawali, O. & Ko, J. (2011b). The trickle algorithm. *Internet Engineering Task Force, RFC6206*.

Levis, P., Clausen, T., Hui, J., Gnawali, O. & Ko, J. (2011c). The trickle algorithm. *Internet Engineering Task Force, RFC6206*.

Li, X. & Wang, Y. (2011, Sept). Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network. *Int. Conf. Wireless Commun.*, pp. 1-4.

Liang, C. & Yu, F. R. (2015). Wireless virtualization for next generation mobile cellular networks. *IEEE wireless communications*, 22(1), 61–69.

Liang, K., Zhao, L., Chu, X. & Chen, H.-H. (2017). An integrated architecture for software defined and virtualized radio access networks with fog Comput. *IEEE Network*, 31(1), 80–87.

Liang, X., Li, X., Shen, Q., Lu, R., Lin, X., Shen, X. & Zhuang, W. (2012). Exploiting prediction to enable secure and reliable routing in wireless body area networks. *INFOCOM, 2012 Proceedings IEEE*, pp. 388–396.

Liang, Y., Poor, H. V. & Shamai, S. (2009). *Information theoretic security*. Now Publishers Inc.

Lin, C.-H., Chien, W.-C., Chen, J.-Y., Lai, C.-F. & Chao, H.-C. (2019). Energy Efficient Fog RAN (F-RAN) with Flexible BBU Resource Assignment for Latency Aware Mobile Edge Computing (MEC) Services. *IEEE Vehicular Tech. Conf.*, pp. 1–6.

Lin, S.-C., Akyildiz, I. F., Wang, P. & Luo, M. (2016a). QoS-aware adaptive routing in multi-layer hierarchical software defined networks: A reinforcement learning approach. *IEEE Int. Conf. Serv. Comp.*, pp. 25–33.

Lin, S.-C., Akyildiz, I. F., Wang, P. & Luo, M. (2016b). QoS-aware adaptive routing in multi-layer hierarchical software defined networks: A reinforcement learning approach. *IEEE Int. Conf. Serv. Comp.*, pp. 25–33.

Lin, S.-C., Akyildiz, I. F., Wang, P. & Luo, M. (2016c). QoS-aware adaptive routing in multi-layer hierarchical software defined networks: A reinforcement learning approach. *IEEE Int. Conf. Serv. Comp.*, pp. 25–33.

Liu, J., Yu, F. R., Lung, C.-H. & Tang, H. (2009). Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks. *IEEE transactions on wireless communications*, 8(2), 806–815.

Liu, Y., Dong, M., Ota, K. & Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. *IEEE Trans. Inform. Forensics and Security*, 11, 2013–2027.

Liyanage, M., Ylianttila, M. & Gurtov, A. (2014a, June). Securing the control channel of software-defined mobile networks. *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, pp. 1-6.

Liyanage, M., Ylianttila, M. & Gurtov, A. (2014b). Securing the control channel of software-defined mobile networks. *IEEE Int. Symp. World of Wireless, Mobile and Multimedia Networks*, pp. 1–6.

Liyanage, M., Abro, A. B., Ylianttila, M. & Gurtov, A. (2016). Opportunities and challenges of software-defined mobile networks in network security. *IEEE Security & Privacy*, 14(4), 34–44.

Liyanage, M., Braeken, A., Jurcut, A. D., Ylianttila, M. & Gurtov, A. (2017). Secure communication channel architecture for software defined mobile networks. *Computer Networks*, 32–50.

Lu, C.-C. & Tseng, S.-Y. (2002). Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. *IEEE Int. App. Sys., Architectures and Processors*, pp. 277–285.

Ma, T., Yu, Y., Wang, F., Zhang, Q. & Chen, X. (2016). A hybrid methodologies for intrusion detection based deep neural network with support vector machine and clustering technique. *Int. Conf. Frontier Computing*, pp. 123–134.

Magubane, Z., Tarwireyi, P., Abu-Mahfouz, A. M. & Adigun, M. O. (2019a). RPL-Based on Load Balancing Routing objective Functions for IoTs in Distributed Networks. *IEEE Int. Mult. Inf. Technol. Eng. Conf.*, pp. 1–6.

Magubane, Z., Tarwireyi, P., Abu-Mahfouz, A. M. & Adigun, M. O. (2019b). RPL-Based on Load Balancing Routing objective Functions for IoTs in Distributed Networks. *IEEE Int. Mult. Inf. Technol. Eng. Conf.*, pp. 1–6.

Magubane, Z., Tarwireyi, P., Abu-Mahfouz, A. M. & Adigun, M. O. (2019c). RPL-Based on Load Balancing Routing objective Functions for IoTs in Distributed Networks. *IEEE Int. Mult. Inf. Technol. Eng. Conf.*, pp. 1–6.

Mammeri, Z. (2019a). Reinforcement learning based routing in networks: Review and classification of approaches. *IEEE Access*, 7, 55916–55950.

Mammeri, Z. (2019b). Reinforcement learning based routing in networks: Review and classification of approaches. *IEEE Access*, 7, 55916–55950.

Mangelkar, S., Dhage, S. N. & Nimkar, A. V. (2017a). A comparative study on RPL attacks and security solutions. *IEEE Int. Conf. Intell. Comput.*, pp. 1–6.

Mangelkar, S., Dhage, S. N. & Nimkar, A. V. (2017b). A comparative study on RPL attacks and security solutions. *IEEE Int. Conf. Intell. Comput.*, pp. 1–6.

Marinho, J., Granjal, J. & Monteiro, E. (2015). A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. *EURASIP Journal on Information Security*, 4.

Martini, B., Paganelli, F., Cappanera, P., Turchi, S. & Castoldi, P. (2015). Latency-aware composition of virtual functions in 5G. *IEEE Conference on Network Softwarization (NetSoft)*, pp. 1–6.

Menezes, A. J., Van Oorschot, P. C. & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC press.

Meyer, C. & Schwenk, J. (2013). Lessons Learned From Previous SSL/TLS Attacks-A Brief Chronology Of Attacks And Weaknesses. *IACR Cryptology EPrint Archive*, 49.

Miguel, M. L., Jamhour, E., Pellenz, M. E. & Penna, M. C. (2018a). SDN architecture for 6LoWPAN wireless sensor networks. *Sensors*, 18(11), 3738.

Miguel, M. L., Jamhour, E., Pellenz, M. E. & Penna, M. C. (2018b). SDN architecture for 6LoWPAN wireless sensor networks. *Sensors*, 18(11), 3738.

Miguel, M. L., Jamhour, E., Pellenz, M. E. & Penna, M. C. (2018c). SDN architecture for 6LoWPAN wireless sensor networks. *IEEE Sensors Journal*, 18(11), 3738.

Mijumbi, R., Serrat, J., Gorricho, J.-L., Bouten, N., De Turck, F. & Boutaba, R. (2016). Network function virtualization: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, 18(1), 236–262.

Miki, T., Ohya, T., Yoshino, H. & Umeda, N. (2005). The overview of the 4 th generation mobile communication system. *Information, Communications and Signal Processing, 2005 Fifth International Conference on*, pp. 1600–1604.

Milenkoski, A., Jayaram, K., Antunes, N., Vieira, M. & Kounev, S. (2016). Quantifying the attack detection accuracy of intrusion detection systems in virtualized environments. *IEEE Int. Symp. Soft. Rel. Eng*, pp. 276–286.

Miranda, C., Kaddoum, G. & Bou-Harb, E. (2018). Cross-Layer Authentication Protocol Design for Ultra-Dense 5G HetNets.

Miranda, C., Kaddoum, G., Bou-Harb, E., Garg, S. & Kaur, K. (2020a). A Collaborative Security Framework for Software-Defined Wireless Sensor Networks. *IEEE Trans. Inf. Forensics and Security*, 15, 2602–2615.

Miranda, C., Kaddoum, G., Bou-Harb, E., Garg, S. & Kaur, K. (2020b). A Collaborative Security Framework for Software-Defined Wireless Sensor Networks. *IEEE Trans. Inf. Forensics and Security*, 15, 2602–2615.

Miranda, C., Kaddoum, G., Bou-Harb, E., Garg, S. & Kaur, K. (2020c). A Collaborative Security Framework for Software-Defined Wireless Sensor Networks. *IEEE Trans. Inf. Forensics and Security*, 15, 2602–2615.

Miranda, C., Kaddoum, G., Baek, J.-y. & Selim, B. (2021). Task allocation framework for software-defined fog v-RAN. *IEEE Internet of Things Journal*.

Mitra, P. (2016). A Statistical Model for Hybrid Wireless Network on Chip. *IEEE Int. Conf. Embedded Syst.*, pp. 75–80.

Mitrokotsa, A., Komninos, N. & Douligeris, C. (2007). Intrusion detection with neural networks and watermarking techniques for MANET. *Pervasive Services, IEEE International Conference on*, pp. 118–127.

Mittal, V., Gupta, S. & Choudhury, T. (2018). Comparative analysis of authentication and access control protocols against malicious attacks in wireless sensor networks. In *Smart Computing and Informatics* (pp. 255–262). Springer.

Moghtadaiee, V. & Dempster, A. G. (2014). Indoor Location Fingerprinting Using FM Radio Signals. *IEEE Trans. on Broadcasting*, 60(2), 336-346.

Monir, M. B., Abdelkader, T. & Ei-Horbaty, E.-S. M. (2019). Trust Evaluation of Service level Agreement for Service Providers in Mobile Edge Computing. *IEEE Int. Conf. Intell. Comput. and Inf. Syst.*, pp. 362–369.

Moon, A. H., Shah, N., Khan, U. I. & Ayub, A. (2013). Simulating and Analysing Security Attacks in Wireless Sensor Networks Using QualNet. *IEEE Trans. Pattern Anal. Mach. Intell.*, pp. 68–76.

Moreira, C. M., Kaddoum, G. & Bou-Harb, E. (2018a). Cross-layer authentication protocol design for ultra-dense 5G HetNets. *IEEE International Conference on Communications (ICC)*, pp. 1–7.

Moreira, C. M., Kaddoum, G. & Bou-Harb, E. (2018b). Cross-layer authentication protocol design for ultra-dense 5G HetNets. *IEEE Int. Conf. on Commun.*, pp. 1–7.

Moreira, C. M., Kaddoum, G. & Bou-Harb, E. (2018c). Cross-layer authentication protocol design for ultra-dense 5G hetnets. *IEEE Int. Conf. Commun.*, pp. 1–7.

Moreira, C. M., Kaddoum, G. & Bou-Harb, E. (2018d). Cross-layer authentication protocol design for ultra-dense 5G hetnets. *IEEE Int. Conf. Commun.*, pp. 1–7.

Moreira, C. M., Kaddoum, G. & Bou-Harb, E. (2018e). Cross-layer authentication protocol design for ultra-dense 5G hetnets. *IEEE Int. Conf. Commun.*, pp. 1–7.

Moreira, C. M., Kaddoum, G. & Bou-Harb, E. (2018f). Cross-layer authentication protocol design for ultra-dense 5G HetNets. *IEEE Int. Conf. Commun.*, pp. 1–7.

Motroni, A., Buffi, A. & Nepa, P. (2021). A survey on indoor vehicle localization through RFID technology. *IEEE Access*, 9, 17921–17942.

Murugesan, R., Saravanan, M. & Vijyaraj, M. (2014a). A node authentication clustering based security for ADHOC network. *Communications and Signal Processing (ICCSP), 2014 International Conference on*, pp. 1168–1172.

Murugesan, R., Saravanan, M. & Vijyaraj, M. (2014b). A node authentication clustering based security for ADHOC network. *IEEE Int. Conf. on Commun. and Signal Process*, pp. 1168–1172.

Musaddiq, A., Zikria, Y. B., Kim, S. W. et al. (2020a). Routing protocol for Low-Power and Lossy Networks for heterogeneous traffic network. *Journal on Wireless Communications and Networking*, 2020(1), 21.

Musaddiq, A., Zikria, Y. B., Kim, S. W. et al. (2020b). Routing protocol for Low-Power and Lossy Networks for heterogeneous traffic network. *Journal on Wireless Communications and Networking*, 2020(1), 21.

Musaddiq, A., Zikria, Y. B., Kim, S. W. et al. (2020c). Routing protocol for Low-Power and Lossy Networks for heterogeneous traffic network. *Journal on Wireless Communications and Networking*, 2020(1), 21.

Muzammal, S. M., Murugesan, R. K., Jhanjhi, N. Z. & Jung, L. T. (2020). SMTrust: Proposing Trust-Based Secure Routing Protocol for RPL Attacks for IoT Applications. *IEEE Int. Conf. Comput. Intell.*, pp. 305–310.

Nagabandi, A., Kahn, G., Fearing, R. S. & Levine, S. (2018). Neural network dynamics for model-based deep reinforcement learning with model-free fine-tuning. *IEEE Int. Conf. Robotics*, pp. 7559–7566.

Nain, Z., Musaddiq, A., Qadri, Y. A., Nauman, A., Afzal, M. K. & Kim, S. W. (2021). RIATA: A Reinforcement Learning-Based Intelligent Routing Update Scheme for Future Generation IoT Networks. *IEEE Access*.

Nanda, A., Puthal, D., Mohanty, S. P. & Choppali, U. (2018). A Computing Perspective of Quantum Cryptography [Energy and Security]. *IEEE Consumer Electronics Magazine*, 7(6), 57–59.

Nawir, M., Amir, A., Yaakob, N. & Lynn, O. B. (2016a). Internet of Things (IoT): Taxonomy of security attacks. *2016 3rd International Conference on Electronic Design (ICED)*, pp. 321–326.

Nawir, M., Amir, A., Yaakob, N. & Lynn, O. B. (2016b). Internet of Things (IoT): Taxonomy of security attacks. *2016 3rd International Conference on Electronic Design (ICED)*, pp. 321–326.

Nawir, M., Amir, A., Yaakob, N. & Lynn, O. B. (2016c). Internet of Things (IoT): Taxonomy of security attacks. *2016 3rd International Conference on Electronic Design (ICED)*, pp. 321–326.

Nedyalkov, I. (2019). Studying of a Modeled IP–Based Network Using Different Dynamic Routing Protocols. *IEEE Nat. Conf.*, pp. 1–4.

Ng, S. X., Conti, A., Long, G.-L., Muller, P., Sayeed, A., Yuan, J. & Hanzo, L. (2020). Guest editorial advances in quantum communications, computing, cryptography, and sensing. *IEEE Journal on Selected Areas in Communications*, 38(3), 405–412.

Nguyen, M.-D., Chau, N.-T., Jung, S. & Jung, S. (2014). A demonstration of malicious insider attacks inside cloud iaas vendor. *International Journal of Information and Education Technology*, 4(6), 483.

Nguyen, T. N. (2018). The challenges in ML-based security for SDN. *IEEE Cyber Security in Networking Conference*, pp. 1–9.

Olade, I., Liang, H.-n. & Fleming, C. (2018). A Review of Multimodal Facial Biometric Authentication Methods in Mobile Devices and Their Application in Head Mounted Displays. *IEEE SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI*, pp. 1997–2004.

Ooko, S. O., Kadam'manja, J., Uwizeye, M. G. & Lemma, D. (2020). Security Issues in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): A Review. *IEEE Int. Conf. Inf. Technol.*, pp. 1–5.

Osterlind, F., Dunkels, A., Eriksson, J., Finne, N. & Voigt, T. (2006a). Cross-level sensor network simulation with cooja. *IEEE Conf. Local Computer Networks*, pp. 641–648.

Osterlind, F., Dunkels, A., Eriksson, J., Finne, N. & Voigt, T. (2006b). Cross-level sensor network simulation with cooja. *IEEE Conf. Local Computer Networks*, pp. 641–648.

Oueis, J., Strinati, E. C. & Barbarossa, S. (2015). The fog balancing: Load distribution for small cell cloud Comput. *IEEE Veh. Technol*, pp. 1–6.

Pacheco, L. A. B., Gondim, J. J., Barreto, P. A. S. & Alchieri, E. (2016). Evaluation of Distributed Denial of Service threat in the Internet of Things. *IEEE Int. Symp. on Network Computing and App.*, pp. 89–92.

Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T. & Ladid, L. (2016). Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications*, 510–527.

Pang, J., Greenstein, B., Gummadi, R., Seshan, S. & Wetherall, D. (2007). 802.11 user fingerprinting. *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pp. 99–110.

Patwari, N. & Kasera, S. K. (2007). Robust location distinction using temporal link signatures. *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pp. 111–122.

Peng, M., Li, Y., Zhao, Z. & Wang, C. (2015a). System architecture and key technologies for 5G heterogeneous cloud radio access networks. *IEEE network*, 29(2), 6–14.

Peng, M., Li, Y., Zhao, Z. & Wang, C. (2015b). System architecture and key technologies for 5G heterogeneous cloud radio access networks. *IEEE Network*, 29(2), 6–14.

Pepple, K. (2011). *Deploying openstack*. " O'Reilly Media, Inc.".

Perera, P. & Patel, V. M. (2018). Efficient and low latency detection of intruders in mobile active authentication. *IEEE Trans. Inform. Forensics and Security*, 13, 1392–1405.

Perrin, S. (2017). Evolving to an Open C-RAN Architecture for 5G. *Fujitsu Heavy reading White Paper*.

Pradeska, N., Najib, W., Kusumawardani, S. S. et al. (2016a). Performance analysis of objective function MRHOF and OF0 in routing protocol RPL IPV6 over low power wireless personal area networks (6LoWPAN). *IEEE Int. Conf. Inf. Technol. and Elect. Eng.*, pp. 1–6.

Pradeska, N., Najib, W., Kusumawardani, S. S. et al. (2016b). Performance analysis of objective function MRHOF and OF0 in routing protocol RPL IPV6 over low power wireless personal area networks (6LoWPAN). *IEEE Int. Conf. Inf. Technol. and Elect. Eng.*, pp. 1–6.

Pradeska, N., Najib, W., Kusumawardani, S. S. et al. (2016c). Performance analysis of objective function MRHOF and OF0 in routing protocol RPL IPv6 over low power wireless personal area networks (6LoWPAN). *IEEE Int. Conf. Inf. Technol. and Elect. Eng.*, pp. 1–6.

Prakasam, A. & Savarimuthu, N. (2016). Metaheuristic algorithms and probabilistic behaviour: a comprehensive analysis of Ant Colony Optimization and its variants. *Artificial Intelligence Review*, 45(1), 97–130.

Pranata, A. A., Jun, T. S. & Kim, D. S. (2019). Overhead reduction scheme for SDN-based Data Center Networks. *Computer Standards & Interfaces*, 63, 1–15.

Prasad, P. S. & Agrawal, P. (2009). Mobility prediction for wireless network resource management. *System Theory, 2009. SSST 2009. 41st Southeastern Symposium on*, pp. 98–102.

Prasad, P. S. & Agrawal, P. (2010). Movement prediction in wireless networks using mobility traces. *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*, pp. 1–5.

Preda, M. & Patriciu, V.-V. (2020). Simulating RPL Attacks in 6lowpan for Detection Purposes. *IEEE Int. Conf. . Commun.*, pp. 239–245.

Premsankar, G., Di Francesco, M. & Taleb, T. (2018). Edge computing for the Internet of Things: A case study. *IEEE Internet of Things Journal*, 5(2), 1275–1284.

Pritchard, S. W., Hancke, G. P. & Abu-Mahfouz, A. M. (2017). Security in software-defined wireless sensor networks: Threats, challenges and potential solutions. *2017 IEEE Int. Conf. Ind. Inform.*, pp. 168–173.

Purkhiabani, M. & Salahi, A. (2011, May). Enhanced authentication and key agreement procedure of next generation evolved mobile networks. *IEEE 3rd International Conference on Communication Software and Networks*, pp. 557-563.

Qi, Q., Zhang, L., Wang, J., Sun, H., Zhuang, Z., Liao, J. & Yu, F. R. (2020). Scalable Parallel Task Scheduling for Autonomous Driving Using Multi-Task Deep Reinforcement Learning. *IEEE Trans. on Vehic. Technol.*, 69(11), 13861–13874.

Raba, D., Juan, A. A., Panadero, J., Bayliss, C. & Estrada-Moreno, A. (2019). Combining the internet of things with simulation-based optimization to enhance logistics in an Agri-food supply chain. *IEEE Winter Simul. Conf.*, pp. 1894–1905.

Rai, K. K. & Asawa, K. (2017a). Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network. *IEEE Int. Conf. Contemporary Computing*, pp. 1–5.

Rai, K. K. & Asawa, K. (2017b). Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network. *IEEE Int. Conf. Contemporary Computing*, pp. 1–5.

Rai, K. K. & Asawa, K. (2017c). Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network. *IEEE Int. Conf. Contemporary Computing*, pp. 1–5.

Rajesh, G., Raajini, X. M., Rajan, R. A., Gokuldhev, M. & Swetha, C. (2020a). A Multi-objective Routing Optimization Using Swarm Intelligence in IoT Networks. In *Intell. Comp. and Innovation on Data Science* (pp. 603–613). Springer.

Rajesh, G., Raajini, X. M., Rajan, R. A., Gokuldhev, M. & Swetha, C. (2020b). A Multi-objective Routing Optimization Using Swarm Intelligence in IoT Networks. In *Intell. Comp. and Innovation on Data Science* (pp. 603–613). Springer.

Rajesh, G., Raajini, X. M., Rajan, R. A., Gokuldhev, M. & Swetha, C. (2020c). A Multi-objective Routing Optimization Using Swarm Intelligence in IoT Networks. In *Intell. Comp. and Innovation on Data Science* (pp. 603–613). Springer.

Rashid, B. & Rehmani, M. H. (2016). Applications of wireless sensor networks for urban areas: A survey. *Journal of Network and Computer Applicat.*, 60, 192–219.

Rass, S. (2013). On game-theoretic network security provisioning. *Journal of network and systems management*, 21(1), 47–64.

Rathee, G., Garg, S., Kaddoum, G. & Choi, B. J. (2020). Decision-making model for securing IoT devices in smart industries. *IEEE Transactions on Industrial Informatics*, 17(6), 4270–4278.

Rathee, G., Garg, S., Kaddoum, G., Choi, B. J., Hassan, M. M. & AlQahtani, S. A. (2022). TrustSys: Trusted decision making scheme for collaborative artificial intelligence of things. *IEEE Transactions on Industrial Informatics*, 19(1), 1059–1068.

Ravi, R. J. & PonLakshmi, R. (2013). A New Lifetime Prediction Algorithm Based Routing For VANETs. *International Journal of Computer Science & Applications (TIJCSA)*, 1(12).

Recht, B. (2019a). A tour of reinforcement learning: The view from continuous control. *Annual Review of Control, Robotics, and Autonomous Systems*, 2, 253–279.

Recht, B. (2019b). A tour of reinforcement learning: The view from continuous control. *Annual Review of Control, Robotics, and Autonomous Systems*, 2, 253–279.

Recht, B. (2019c). A tour of reinforcement learning: The view from continuous control. *Annual Review of Control, Robotics, and Autonomous Systems*, 2, 253–279.

Rehman, A., Khan, M. M., Lodhi, M. A. & Hussain, F. B. (2016a). Rank attack using objective function in RPL for low power and lossy networks. *IEEE Int. Conf. Ind. Inf. and Comp. Syst.*, pp. 1–5.

Rehman, A., Khan, M. M., Lodhi, M. A. & Hussain, F. B. (2016b). Rank attack using objective function in RPL for low power and lossy networks. *IEEE Int. Conf. Ind. Inf. and Comp. Syst.*, pp. 1–5.

Rehman, A., Khan, M. M., Lodhi, M. A. & Hussain, F. B. (2016c). Rank attack using objective function in RPL for low power and lossy networks. *IEEE Int. Conf. Ind. Inf. and Comp. Syst.*, pp. 1–5.

Ren, J., Zhang, Y., Zhang, K. & Shen, X. (2016). Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks. *IEEE Trans. Wireless Commun.*, 15, 3718–3731.

Restuccia, F., D'Oro, S. & Melodia, T. (2018). Securing the internet of things in the age of machine learning and software-defined networking. *IEEE Internet of Things Journal*, 5(6), 4829–4842.

Riggio, R., Bradai, A., Harutyunyan, D., Rasheed, T. & Ahmed, T. (2016). Scheduling wireless virtual networks functions. *IEEE Trans Net. and Serv. Management*, 13(2), 240–252.

Rocha, F. & Correia, M. (2011). Lucy in the sky without diamonds: Stealing confidential data in the cloud. *Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on*, pp. 129–134.

Rodriguez, V. Q., Guillemin, F. & Boubendir, A. (2019). Automating the deployment of 5G network slices using ONAP. *IEEE International Conference on Networks of the Future (NoF)*, pp. 32–39.

Rost, P., Banchs, A., Berberana, I., Breitbach, M., Doll, M., Droste, H., Mannweiler, C., Puente, M. A., Samdanis, K. & Sayadi, B. (2016). Mobile network architecture evolution toward 5G. *IEEE Communications Magazine*, 84–91.

Routray, S. K., Jha, M. K., Sharma, L., Nyamangoudar, R., Javali, A. & Sarkar, S. (2017). Quantum cryptography for iot: Aperspective. *IEEE Int. Conf. IoT and App.*, pp. 1–4.

royalsociety, r. Machine learning: the power and promise of computers that learn by example, royalsociety White Paper.

Sabahi, F. (2011). Cloud computing security threats and responses. *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, pp. 245–249.

Safaei, B., Monazzah, A. M. H. & Ejlali, A. (2020). ELITE: An Elaborated Cross-Layer RPL Objective Function to Achieve Energy Efficiency in Internet-of-Things Devices. *IEEE Internet of Things Journal*, 8(2), 1169–1182.

Saghar, K., Tariq, M., Kendall, D. & Bouridane, A. (2016). RAEED: A formally verified solution to resolve sinkhole attack in Wireless Sensor Network. *IEEE Int. Bhurban Conf. on Applied Sciences and Technology*, pp. 334–345.

Sahay, R., Geethakumari, G. & Modugu, K. Attack graph based vulnerability assessment of rank property in RPL-6LoWPAN in IoT. *IEEE Internet of Things journal*.

Sahay, R., Geethakumari, G. & Modugu, K. (2018a). Attack graph—Based vulnerability assessment of rank property in RPL-6LoWPAN in IoT. *IEEE World Forum IoT*, pp. 308–313.

Sahay, R., Geethakumari, G. & Modugu, K. (2018b). Attack graph—Based vulnerability assessment of rank property in RPL-6LoWPAN in IoT. *IEEE World Forum IoT*, pp. 308–313.

Sahoo, K. S., Sahoo, B. & Panda, A. (2015). A secured SDN framework for IoT. *IEEE International Conference on Man and Machine Interfacing (MAMI)*, pp. 1–4.

Säily, M., Estevan, C. B., Gimenez, J. J., Tesema, F., Guo, W., Gomez-Barquero, D. & Mi, D. (2020). 5G radio access network architecture for terrestrial broadcast services. *IEEE Trans. broad.*, 66(2), 404–415.

Salem, R., Salam, M. A., Abdelkader, H. & Mohamed, A. A. (2019a). An artificial bee colony algorithm for data replication optimization in cloud environments. *IEEE Access*, 8, 51841–51852.

Salem, R., Salam, M. A., Abdelkader, H. & Mohamed, A. A. (2019b). An artificial bee colony algorithm for data replication optimization in cloud environments. *IEEE Access*, 8,

51841–51852.

Salem, R., Salam, M. A., Abdelkader, H. & Mohamed, A. A. (2019c). An artificial bee colony algorithm for data replication optimization in cloud environments. *IEEE Access*, 8, 51841–51852.

Samanta, A. & Chang, Z. (2019). Adaptive service offloading for revenue maximization in mobile edge computing with delay-constraint. *IEEE IoT Journal*, 6(2), 3864–3872.

Samanta, A. & Tang, J. (2020). Dyme: Dynamic microservice scheduling in edge computing enabled IoT. *IEEE IoT Journal*, 7(7), 6164–6174.

Samanta, A., Chang, Z. & Han, Z. (2018). Latency-oblivious distributed task scheduling for mobile edge computing. *IEEE Global Commun. Conf.*, pp. 1–7.

Saxena, N., Roy, A., Sahu, B. J. & Kim, H. (2017). Efficient IoT gateway over 5G wireless: A new design with prototype and implementation results. *IEEE Commun.*, 55(2), 97–105.

Schehlmann, L., Abt, S. & Baier, H. (2014). Blessing or curse? Revisiting security aspects of Software-Defined Networking. *Network and Service Management (CNSM), 2014 10th International Conference on*, pp. 382–387.

Scott-Hayward, S., O'Callaghan, G. & Sezer, S. (2013). SDN security: A survey. *Future Networks and Services (SDN4FNS), 2013 IEEE SDN For*, pp. 1–7.

Shanthi, S. & Rajan, E. (2016). Comprehensive analysis of security attacks and intrusion detection system in wireless sensor networks. *IEEE Int. Conf. Next Gen. Comput. Technologies*, pp. 426–431.

Sharma, A. K. & Parihar, P. S. (2013). An effective dos prevention system to analysis and prediction of network traffic using support vector machine learning. *International Journal of Application or Innovation in Engineering & Management*, 2(7), 249–256.

Shen, H., Huo, S., Yan, H., Park, J. H. & Sreeram, V. (2019). Distributed dissipative state estimation for Markov jump genetic regulatory networks subject to Round-Robin scheduling. *IEEE Trans. neural networks and learning syst.*, 31(3), 762–771.

Shi, L., Zhang, Z. & Robertazzi, T. (2017). Energy-aware scheduling of embarrassingly parallel jobs and resource allocation in cloud. *IEEE Trans. Parallel Distrib. Syst.*, 28(6), 1607–1620.

Shin, D., Sharma, V., Kim, J., Kwon, S. & You, I. (2017a). Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. *IEEE Access*, 5, 11100–11117.

Shin, D., Sharma, V., Kim, J., Kwon, S. & You, I. (2017b). Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. *IEEE Access*, 5, 11100–11117.

Shin, D., Sharma, V., Kim, J., Kwon, S. & You, I. (2017c). Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. *IEEE Access*, 5, 11100–11117.

Shin, S. & Gu, G. (2013). Attacking software-defined networks: A first feasibility study. *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking*, pp. 165–166.

Shin, S., Song, Y., Lee, T., Lee, S., Chung, J., Porras, P., Yegneswaran, V., Noh, J. & Kang, B. B. (2014). Rosemary: A robust, secure, and high-performance network operating system. *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pp. 78–89.

Shon, T. & Moon, J. (2007). A hybrid machine learning approach to network anomaly detection. *Inform. Sci.*, 177, 3799–3821.

Shu, Z. & Taleb, T. (2020). A novel QoS framework for network slicing in 5G and beyond networks based on SDN and NFV. *IEEE Network*, 34(3), 256–263.

Shu, Z., Wan, J., Lin, J., Wang, S., Li, D., Rho, S. & Yang, C. (2016a). Traffic engineering in software-defined networking: Measurement and management. *IEEE access*, 4, 3246–3256.

Shu, Z., Wan, J., Lin, J., Wang, S., Li, D., Rho, S. & Yang, C. (2016b). Traffic engineering in software-defined networking: Measurement and management. *IEEE access*, 4, 3246–3256.

Shu, Z., Wan, J., Lin, J., Wang, S., Li, D., Rho, S. & Yang, C. (2016c). Traffic engineering in software-defined networking: Measurement and management. *IEEE access*, 4, 3246–3256.

SIMalliance. An analysis of the security needs of the 5G market.

SIMalliance, W. P. An analysis of the security needs of the 5G market, SIMalliance White Paper.

Simha, S. V., Mathew, R., Sahoo, S. & Biradar, R. C. (2020a). A Review of RPL Protocol Using Contiki Operating System. *IEEE Int. Conf. Electron.*, pp. 259–264.

Simha, S. V., Mathew, R., Sahoo, S. & Biradar, R. C. (2020b). A Review of RPL Protocol Using Contiki Operating System. *IEEE Int. Conf. Electron.*, pp. 259–264.

Solé, P. & Zinoviev, D. (2004). The most significant bit of maximum-length sequences over/spl Zopf/2/sup l: autocorrelation and imbalance. *IEEE Trans. Inf. Theory*, 50, 1844–1846.

Suh, G. E. & Devadas, S. (2007). Physical unclonable functions for device authentication and secret key generation. *Proceedings of the 44th annual design automation conference*, pp. 9–14.

Sun, B., Osborne, L., Xiao, Y. & Guizani, S. (2007). Intrusion detection techniques in mobile ad hoc and wireless sensor networks. *IEEE Trans. Wireless Commun.*, 14.

Sun, S., Gong, L., Rong, B. & Lu, K. (2015). An intelligent SDN framework for 5G heterogeneous networks. *IEEE Commun. Mag.*, 53(11), 142–147.

Sun, Z., Balakrishnan, S., Su, L., Bhuyan, A., Wang, P. & Qiao, C. (2021). Who Is in Control? Practical Physical Layer Attack and Defense for mmWave-Based Sensing in Autonomous Vehicles. *IEEE Trans. Inf. Forensics and Security*, 16, 3199–3214.

Suntharam, S. (2015). Load balancing by Max-min algorithm in private cloud environment. *Int. J Sci Res*, 4(4), 2462–2466.

Tanganelli, G., Virdis, A. & Mingozzi, E. (2019a). Implementation of software-defined 6LoWPANs in Contiki OS. *IEEE Int. Symp. Wireless Networks*, pp. 1–6.

Tanganelli, G., Virdis, A. & Mingozzi, E. (2019b). Enabling Multi-hop Forwarding in 6LoWPANs through Software-Defined Networking. *IEEE Int. Symp Mobile and Multimedia Networks*, pp. 1–9.

Tanganelli, G., Virdis, A. & Mingozzi, E. (2019c). Enabling Multi-hop Forwarding in 6LoWPANs through Software-Defined Networking. *IEEE Int. Symp Mobile and Multimedia Networks*, pp. 1–9.

Tanganelli, G., Virdis, A. & Mingozzi, E. (2019d). Enabling Multi-hop Forwarding in 6LoWPANs through Software-Defined Networking. *IEEE Int. Symp Mobile and Multimedia Networks*, pp. 1–9.

Tatsis, V. A. & Parsopoulos, K. E. (2020). Reinforced Online Parameter Adaptation Method for Population-based Metaheuristics. *IEEE Symp. Comput. Intell.*, pp. 360–367.

Theodorou, T. & Mamatas, L. (2020). SD-MIoT: A software-defined networking solution for mobile Internet of Things. *IEEE Internet of Things Journal*, 8(6), 4604–4617.

Thubert, P. et al. (2012a). Objective function zero for the routing protocol for low-power and lossy networks (RPL).

Thubert, P. et al. (2012b). Objective function zero for the routing protocol for low-power and lossy networks (RPL).

Tsai, C. & Moh, M. (2017a). Load balancing in 5G cloud radio access networks supporting IoT Commun. for smart communities. *IEEE Signal Process. and Inf. Technol.*, pp. 259–264.

Tsai, C. & Moh, M. (2017b). Load balancing in 5G cloud radio access networks supporting IoT Commun. for smart communities. *IEEE Signal Process and Inf. Technol.*, pp. 259–264.

Tsiftes, N., Eriksson, J. & Dunkels, A. (2010a). Low-power wireless IPv6 routing with ContikiRPL. *IEEE Int. Conf. Inf. Processing in Sensor Net.*, pp. 406–407.

Tsiftes, N., Eriksson, J. & Dunkels, A. (2010b). Low-power wireless IPv6 routing with ContikiRPL. *IEEE Int. Conf. Inf. Processing in Sensor Net.*, pp. 406–407.

Tuncer, D., Charalambides, M., Clayman, S. & Pavlou, G. (2016a). Flexible traffic splitting in OpenFlow networks. *IEEE Trans. Net. and Serv. Manag.*, 13(3), 407–420.

Tuncer, D., Charalambides, M., Clayman, S. & Pavlou, G. (2016b). Flexible traffic splitting in OpenFlow networks. *IEEE Trans. Net. and Serv. Manag.*, 13(3), 407–420.

Tuncer, D., Charalambides, M., Clayman, S. & Pavlou, G. (2016c). Flexible traffic splitting in OpenFlow networks. *IEEE Trans. Net. and Serv. Manag.*, 13(3), 407–420.

Tutunović, M. & Wuttidittachotti, P. (2019). Discovery of suitable node number for wireless sensor networks based on energy consumption using Cooja. *IEEE Int. Conf. Commun. Technol.*, pp. 168–172.

Uslu, G., Serdaroglu, K. C. & Baydere, S. (2013). Ds+: Reliable distributed snapshot algorithm for wireless sensor networks. *J. of Comput. Networks and Commun.*, 2013.

Valenzuela-Valdés, J. F., Palomares, A., González-Macías, J. C., Valenzuela-Valdés, A., Padilla, P. & Luna-Valero, F. (2018). On the ultra-dense small cell deployment for 5G networks. *IEEE 5G World Forum*, pp. 369–372.

Vargaftik, S., Keslassy, I. & Orda, A. (2017). No packet left behind: Avoiding starvation in dynamic topologies. *IEEE/ACM Trans. Networking*, 25(4), 2571–2584.

Venkatesan, C., Karthigaikumar, P., Paul, A., Satheeskumaran, S. & Kumar, R. (2018). ECG signal preprocessing and SVM classifier-based abnormality detection in remote healthcare applications. *IEEE Access*, 6, 9767–9773.

Verma, A. & Ranga, V. (2020a). Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review. *IEEE Sensors Journal*, 20(11), 5666–5690.

Verma, A. & Ranga, V. (2020b). Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review. *IEEE Sensors Journal*, 20(11), 5666–5690.

Verma, A. & Ranga, V. (2020c). Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review. *IEEE Sensors Journal*, 20(11), 5666–5690.

Verma, A. & Ranga, V. (2020d). Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review. *IEEE Sensors Journal*, 20(11), 5666-5690.

Vohra, S. & Srivastava, R. (2015a). A survey on techniques for securing 6LoWPAN. *IEEE Int. Conf. Commun. Sys. and Network Technol.*, pp. 643–647.

Vohra, S. & Srivastava, R. (2015b). A survey on techniques for securing 6LoWPAN. *IEEE Int. Conf. Commun. Sys. and Network Technol.*, pp. 643–647.

Vohra, S. & Srivastava, R. (2015c). A survey on techniques for securing 6LoWPAN. *IEEE Int. Conf. Commun. Sys. and Network Technol.*, pp. 643–647.

von Tschirschnitz, M., Peuckert, L., Franzen, F. & Grossklags, J. (2021). Method confusion attack on bluetooth pairing. *IEEE Symp. on Security and Privacy*.

Wadhaj, I., Ghaleb, B., Thomson, C., Al-Dubai, A. & Buchanan, W. J. (2020a). Mitigation mechanisms against the DAO attack on the routing protocol for low power and lossy networks (RPL). *IEEE Access*, 8, 43665–43675.

Wadhaj, I., Ghaleb, B., Thomson, C., Al-Dubai, A. & Buchanan, W. J. (2020b). Mitigation mechanisms against the DAO attack on the routing protocol for low power and lossy networks (RPL). *IEEE Access*, 8, 43665–43675.

Wang, C. X., Haider, F., Gao, X., You, X. H., Yang, Y., Yuan, D., Aggoune, H. M., Haas, H., Fletcher, S. & Hepsaydir, E. (2014a). Cellular architecture and key technologies for 5G wireless communication networks. *IEEE Communications Magazine*, 52(2), 122-130.

Wang, C.-C., Yao, X., Wang, W.-L. & Jornet, J. M. (2020a). Multi-hop Deflection Routing Algorithm Based on Reinforcement Learning for Energy-Harvesting Nanonetworks. *IEEE Trans. Mobile Computing*.

Wang, C.-C., Yao, X., Wang, W.-L. & Jornet, J. M. (2020b). Multi-hop Deflection Routing Algorithm Based on Reinforcement Learning for Energy-Harvesting Nanonetworks. *IEEE Trans. Mobile Computing*.

Wang, D., He, D., Wang, P. & Chu, C.-H. (2015). Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. *IEEE Trans. Dep. and Secure*

Comput., 12, 428–442.

Wang, D., Bai, B., Zhao, W. & Han, Z. (2018). A survey of optimization approaches for wireless physical layer security. *IEEE Communications Surveys & Tutorials*, 21(2), 1878–1911.

Wang, F., Xu, C., Song, L. & Han, Z. (2014b). Energy-efficient resource allocation for device-to-device underlay communication. *IEEE Trans. on Wireless Commun.*, 14(4), 2082–2092.

Wang, Y. & Xie, J. (2000a). Ant colony optimization for multicast routing. *IEEE Conf. Electron. Commun. Syst.*, pp. 54–57.

Wang, Y. & Xie, J. (2000b). Ant colony optimization for multicast routing. *IEEE Conf. Electron. Commun. Syst.*, pp. 54–57.

Wang, Y. & Xie, J. (2000c). Ant colony optimization for multicast routing. *IEEE Conf. Electron. Commun. Syst.*, pp. 54–57.

Wang, Z., Liu, Y., Ma, Z., Liu, X. & Ma, J. (2020c). LiPSG: Lightweight Privacy-Preserving Q-Learning-Based Energy Management for the IoT-Enabled Smart Grid. *IEEE IoT Journal*, 7(5), 3935–3947.

Wang, Z., Liu, Y., Ma, Z., Liu, X. & Ma, J. (2020d). Lipsg: Lightweight Privacy-Preserving Q-Learning-Based Energy Management for the IoT-Enabled Smart Grid. *IEEE IoT Journal*, 7(5), 3935–3947.

Watanabe, K. & Machida, M. (2012). Outdoor LTE infrastructure equipment (enodeb). *FUJITSU Sci. Tech. Journal*, 48(1), 27–32.

Wolinsky, D. I., Agrawal, A., Boykin, P. O., Davis, J. R., Ganguly, A., Paramygin, V., Sheng, Y. P. & Figueiredo, R. J. (2006). On the design of virtual machine sandboxes for distributed computing in wide-area overlays of virtual workstations. *Proceedings of the 2nd International Workshop on Virtualization Technology in Distributed Computing*, pp. 8.

Wu, H., Ding, Y., Winer, C. & Yao, L. (2010). Network security for virtual machine in cloud computing. *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on*, pp. 18–21.

Wu, J., Dong, M., Ota, K., Li, J. & Yang, W. (2020). Application-aware consensus management for software-defined intelligent blockchain in IoT. *IEEE Network*, 34(1), 69–75.

Xia, W., Zhang, J., Quek, T. Q., Jin, S. & Zhu, H. (2020). Mobile edge cloud-based industrial internet of things: Improving edge intelligence with hierarchical sdn controllers. *IEEE Vehicular Technology Magazine*, 15(1), 36–45.

Xiao, L., Greenstein, L. J., Mandayam, N. B. & Trappe, W. (2008a). Using the physical layer for wireless authentication in time-variant channels. *IEEE Trans. on Wirel. Commun.*, 7(7), 2571-2579.

Xiao, L., Greenstein, L., Mandayam, N. & Trappe, W. (2008b). A physical-layer technique to enhance authentication for mobile terminals. *Communications, 2008. ICC'08. IEEE International Conference on*, pp. 1520–1524.

Xiao, Q. (2004a). A biometric authentication approach for high security ad-hoc networks. *Information Assurance Workshop, 2004. Proceedings from the Fifth Annual IEEE SMC*, pp. 250–256.

Xiao, Q. (2004b). A biometric authentication approach for high security ad-hoc networks. *SMC*, pp. 250–256.

Xie, N. & Leung, H. (2021). Internet of Things (IoT) in Canadian Smart Cities: An Overview. *IEEE Instrumentation & Measurement Magazine*, 24(3), 68–77.

Xin, J., Zhu, Q., Liang, G. & Zhang, T. (2019). Performance Analysis of D2D Underlying Cellular Networks Based on Dynamic Priority Queuing Model. *IEEE Access*, 7, 27479–27489.

Xu, L., Zhou, Y., Wang, P. & Liu, W. (2018). Max-min resource allocation for video transmission in NOMA-based cognitive wireless networks. *IEEE Trans. Commun.*, 66(11), 5804–5813.

Yang, H., Bai, W., Yu, A., Yao, Q., Zhang, J., Lin, Y. & Lee, Y. (2018). Bandwidth compression protection against collapse in fog-based wireless and optical networks. *IEEE Access*, 6, 54760–54768.

Yang, H., Liang, Y., Yuan, J., Yao, Q., Yu, A. & Zhang, J. (2020). Distributed blockchain-based trusted multi-domain collaboration for mobile edge computing in 5g and beyond. *IEEE Trans. on Industrial Informatics*.

Yang, J., Chen, Y., Trappe, W. & Cheng, J. (2009). Determining the number of attackers and localizing multiple adversaries in wireless spoofing attacks. *INFOCOM 2009, IEEE*, pp. 666–674.

Yang, M., Li, Y., Li, B., Jin, D. & Chen, S. (2016). Service-oriented 5G network architecture: an end-to-end software defining approach. *International Journal of Communication Systems*, 29(10), 1645–1657.

Yassein, M. B., Flefil, A., Krstic, D., Khamayseh, Y., Mardini, W. & Shatnawi, M. (2019a). Performance evaluation of RPL in high density networks for IoT. *Int. Conf. Soft. and Inf. Eng.*, pp. 183–187.

Yassein, M. B., Flefil, A., Krstic, D., Khamayseh, Y., Mardini, W. & Shatnawi, M. (2019b). Performance evaluation of RPL in high density networks for IoT. *Int. Conf. Soft. and Inf. Eng.*, pp. 183–187.

Yassein, M. B., Flefil, A., Krstic, D., Khamayseh, Y., Mardini, W. & Shatnawi, M. (2019c). Performance evaluation of RPL in high density networks for IoT. *Int. Conf. Soft. and Inf. Eng.*, pp. 183–187.

Yi, S., Hao, Z., Qin, Z. & Li, Q. (2015). Fog Comput.: Platform and Applications. *HotWeb*, pp. 73-78.

Yin, C., Zhu, Y., Fei, J. & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, 5, 21954–21961.

Yin, L., Luo, J. & Luo, H. (2018). Tasks scheduling and resource allocation in fog computing based on containers for smart manufacturing. *IEEE Trans. on Ind. Inform.*, 14(10), 4712–4721.

Yoon, C., Lee, S., Kang, H., Park, T., Shin, S., Yegneswaran, V., Porras, P. & Gu, G. (2017). Flow Wars: Systemizing the Attack Surface and Defenses in Software-Defined Networks. *IEEE/ACM Transactions on Networking*, (6), 3514-3530.

Younis, M., Youssef, M. & Arisha, K. (2002). Energy-aware routing in cluster-based sensor networks. *IEEE Int. Symp. of Comput. and Telecommun. Systems*, pp. 129–136.

Yu, P. L., Baras, J. S. & Sadler, B. M. (2008). Physical-Layer Authentication. *IEEE Trans. Inf. Forens. Security*, 3(1), 38-51.

Zahedi, S. M., Llull, Q. & Lee, B. C. (2018). Amdahl's law in the datacenter era: a market for fair processor allocation. *IEEE Int. Symp. High Perform. Comput. Architecture*, pp. 1–14.

Zareen, F. & Karam, R. (2018). Detecting RTL Trojans using artificial immune systems and high level behavior classification. *IEEE Hardware Oriented Security and Trust Symposium*, pp. 68–73.

Zaza, A., Al-Emadi, S. & Kharroub, S. (2020). Modern QoS Solutions in WSAN: An Overview of Energy Aware Routing Protocols and Applications. *IEEE Int. Conf. Inform.*, pp. 581–589.

Zeng, D., Gu, L., Guo, S., Cheng, Z. & Yu, S. (2016). Joint optimization of task scheduling and image placement in fog Comput. supported software-defined embedded system. *IEEE Trans. Comput.*, 65(12), 3702–3712.

Zeng, K., Govindan, K. & Mohapatra, P. (2010a). Non-cryptographic authentication and identification in wireless networks [Security and Privacy in Emerging Wireless Networks].

IEEE Wirel. Commun., 17(5), 56-62.

Zeng, K., Govindan, K. & Mohapatra, P. (2010b). Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]. *IEEE Wireless Communications*, 17(5).

Zhang, L., Shetty, S., Liu, P. & Jing, J. (2014). Rootkitdet: Practical end-to-end defense against kernel rootkits in a cloud environment. *European Symposium on Research in Computer Security*, pp. 475–493.

Zhang, L., Restuccia, F., Melodia, T. & Pudlewski, S. M. (2018). Taming cross-layer attacks in wireless networks: a Bayesian learning approach. *IEEE Trans. on Mobile Comput.*, 18(7), 1688–1702.

Zhang, M. & Fang, Y. (2005). Security analysis and enhancements of 3GPP authentication and key agreement protocol. *IEEE Trans. Wireless Commun.*, 4, 734–742.

Zhang, Q., Wang, X., Lv, J. & Huang, M. (2020). Intelligent Content-Aware Traffic Engineering for SDN: An AI-Driven Approach. *IEEE Network*, 34(3), 186–193.

Zhang, S., Janakiraman, R., Sim, T. & Kumar, S. (2006). Continuous verification using multimodal biometrics. *ICB*, pp. 562–570.

Zhang, Y., An, X., Yuan, M., Bu, X. & An, J. (2019a). Concurrent Multi-Path Routing Optimization in Named Data Networks. *IEEE Internet of Things Journal*.

Zhang, Y., An, X., Yuan, M., Bu, X. & An, J. (2019b). Concurrent Multi-Path Routing Optimization in Named Data Networks. *IEEE Internet of Things Journal*.

Zhang, Y., An, X., Yuan, M., Bu, X. & An, J. (2019c). Concurrent Multi-Path Routing Optimization in Named Data Networks. *IEEE Internet of Things Journal*.

Zhu, C., Leung, V. C., Yang, L. T. & Shu, L. (2015). Collaborative location-based sleep scheduling for wireless sensor networks integrated with mobile cloud computing. *IEEE Trans. Comput.*, 64, 1844–1856.

Zhu, L., Cui, J. & Xiong, G. (2018). Improved dynamic load balancing algorithm based on Least-Connection Scheduling. *IEEE Inf. Technol. and Mechatronics Eng. Conf.*, pp. 1858–1862.