# WIRELESS LOCAL AREA NETWORK MANAGEMENT FRAME DENIAL- OF-SERVICE ATTACK DETECTION AND MITIGATION SCHEMES

ABDALLAH ELHIGAZI ABDALLAH ELHIGAZI

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

DECEMBER 2020

**DEDICATION**

*I dedicate this work to my parents,*

*my brothers, my sisters,*

*my beloved wife, and*

*my lovely daughters*

*"Juwan & Layan"*

## ACKNOWLEDGEMENT

First and foremost, I would like to express my sincere gratitude to ALLAH (SWT), who created, guided, helped, and supported me for everything in my life (ALHAMD ULILLAH firstly and lastly). I would like to express my sincere appreciation and gratitude to my supervisor **Assoc. Prof. Dr. Shukor Abd Razak** for his support, guidance, encouragement and patience throughout this research period. Without his unwavering guidance, support, and valuable advice during the research and writing, this thesis would not have been completed. His dedication and technical expertise proved to be the key elements to my doctoral research. Furthermore, I would like to extend my gratitude to Dr. Coulibaly Yahya for his generous time, fruitful discussions, motivation, and patience to attend to my numerous questions during this study. Finally, my special thanks to my beloved parents, spesial thanks go to my brother Osama for his helping me for financial support that I need and other brothers Hafiz and Mohammed and my sisters Aisha and Abeer for their unending love, sacrifice, encouragement and support. The same goes to my wife Aida Makaram and my daughters Juwan and Layan for their unreserved support, love, and patient towards the success of this thesis.

## ABSTRACT

Wireless Local Area Networks (WLAN) are increasingly deployed and in widespread use worldwide due to its convenience and low cost. However, due to the broadcasting and the shared nature of the wireless medium, WLANs are vulnerable to a myriad of attacks. Although there have been concerted efforts to improve the security of wireless networks over the past years, some attacks remain inevitable. Attackers are capable of sending fake de-authentication or disassociation frames to terminate the session of active users; thereby leading to denial of service, stolen passwords, or leakage of sensitive information amongst many other cybercrimes. The detection of such attacks is crucial in today's critical applications. Many security mechanisms have been proposed to effectively detect these issues, however, they have been found to suffer limitations which have resulted in several potential areas of research. This thesis aims to address the detection of resource exhaustion and masquerading DoS attacks problems, and to construct several schemes that are capable of distinguishing between benign and fake management frames through the identification of normal behavior of the wireless stations before sending any authentication and de-authentication frames. Thus, this thesis proposed three schemes for the detection of resource exhaustion and masquerading DoS attacks. The first scheme was a resource exhaustion DoS attacks detection scheme, while the second was a de- authentication and disassociation detection scheme. The third scheme was to improve the detection rate of the de-authentication and disassociation detection scheme using feature derived from an unsupervised method for an increased detection rate. The effectiveness of the performance of the proposed schemes was measured in terms of detection accuracy under sophisticated attack scenarios. Similarly, the efficiency of the proposed schemes was measured in terms of preserving the resources of the access point such as memory consumptions and processing time. The validation and analysis were done through experimentation, and the results showed that the schemes have the ability to protect wireless infrastructure networks against denial of service attacks.

# ABSTRAK

Rangkaian Kawasan Setempat Tanpa Wayar (WLAN) semakin banyak digunakan dan digunakan secara meluas di seluruh dunia kerana kemudahan dan kosnya yang rendah. Walau bagaimanapun, kerana penyiaran dan sifat media tanpa wayar yang dikongsi bersama, WLAN terdedah kepada pelbagai serangan. Walaupun terdapat usaha bersepadu untuk meningkatkan keselamatan rangkaian tanpa wayar sejak bertahun-tahun kebelakangan ini, beberapa serangan tetap tidak dapat dielakkan. Penyerang mampu menghantar bingkai pembatalan pengesahan atau pemisahan palsu untuk menghentikan sesi pengguna aktif sehingga menyebabkan pelbagai jenayah siber termasuklah penolakan perkhidmatan, kata laluan dicuri, atau kebocoran maklumat sensitive. Pengesanan serangan sedemikian penting dalam aplikasi kritikal masa kini. Pelbagai mekanisme keselamatan telah dicadangkan untuk mengesan masalah-masalah sedemikian dengan berkesan, namun didapati masih mengalami kelemahan yang memungkin beberapa bidang penyelidikan berpotensi untuk diterokai. Tesis ini bertujuan untuk menangani masalah berkaitan pengesanan kehabisan sumber, menyekat masalah serangan DoS, dan membina beberapa skema yang mampu membezakan antara bingkai pengurusan benar dan palsu melalui pengenalan tingkah laku normal stesen tanpa wayar sebelum menghantar sebarang bingkai pengesahan dan pembatalan pengesahan. Oleh itu, tesis ini mencadangkan tiga skema untuk mengesan kehabisan sumber dan penyamaran serangan DoS. Skema yang pertama adalah skema pengesanan serangan DoS yang menghabiskan sumber, sementara yang kedua adalah skema pengesanan pembatalan pengesahan dan pemisahan. Skema ketiga adalah untuk memperbaiki kadar pengesanan skema pembatalan pengesahan dan pemisahan menggunakan fitur berasal dari kaedah yang tidak diawasi untuk peningkatan kadar pengesanan. Keberkesanan prestasi skema yang dicadangkan diukur dari segi ketepatan pengesanan di bawah senario serangan yang canggih. Begitu juga, kecekapan skema yang dicadangkan diukur dari segi melestarikan sumber-sumber titik akses seperti penggunaan memori dan masa pemprosesan. Pengesahan dan analisis dilakukan melalui eksperimen, dan hasilnya menunjukkan bahawa skema yang dicadangkan mempunyai kemampuan untuk melindungi rangkaian infrastruktur tanpa wayar daripada serangan penolakan perkhidmatan.

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | | |
|---|---|---|
| ACE | - | Average Cross-Entropy Error |
| ACK | - | Acknowledgement |
| AES | - | Advanced Encryption Standard |
| AID | - | Association ID |
| ANN | - | Artificial Neural Network |
| AP | - | Access Point |
| AssRF | - | Authentication Request Flooding |
| AST | - | Attack Station |
| BSS | - | Basic Service Set |
| CBR | - | Case Based Reasoning |
| CCMP | - | Counter Mode CBC-MAC Protocol |
| CM | - | Central Manager |
| CPU | - | Central Processing Unit |
| CTS | - | Clear to Send |
| D3S | - | De-authentication and Disassociation Detection Scheme |
| DISS RF | - | DISS Authentication Request Flooding |
| DOS | - | Denial of Service |
| DS | - | Distribution System |
| EAP | - | Extensible Authentication Protocol |
| ESS | - | Extended Service Set |
| FPR | - | False Positive Rate |
| GST | - | Genuine Station |
| IBSS | - | Independent Basic Service Set |
| ICM | - | Integrated Central Manager |
| IDB | - | Intruder Database |
| IEEE | - | Institute of Electrical and Electronics Engineers |
| MAC | - | Media Access Control |
| MIC | - | Message Integrity Check |
| MSE | - | Mean Squared Error |
| PHY | - | Physical Layer |

| | | |
|---|---|---|
| PS-Poll | - | Power Save Poll |
| QOS | - | Quality of Service |
| RADIUS | - | Remote Authentication Dial-In User Service |
| RC4 | - | Rivets Cipher 4 |
| READS | - | Resource Exhaustion Attack Detection Scheme |
| RSN | - | Robust Security Network |
| RSSI | - | Received Signal Strength Indicator |
| RTS | - | Request to Send |
| SOM | - | self-Organizing Maps |
| SSID | - | Service Set Identifier |
| STA | - | Station |
| TGi | - | Task Group I |
| TIM | - | Traffic Indication Map |
| TKIP | - | Temporal Key Integrity Protocol |
| TPR | - | True Positive Rate |
| WEP | - | Wired Equivalent Privacy |
| Wi-Fi | - | Wireless Fidelity |
| WLAN | - | Wireless Local Area Networks |

# CHAPTER 1

# INTRODUCTION

## 1.1 Overview

Accessibility and cost-effectiveness are the characteristics of 802.11-based local area wireless networks, leading to widespread deployment worldwide. However, because of the nature of wireless access, such networks are prone to many malicious attacks. There are a number of vulnerabilities in the field of computer security that cause network resources to become unavailable and violate the confidentiality, integrity, and availability of the network. Denial of Service Attack (DoS) has become one of the most serious security threats on the Internet today, with an increasing variety of DOS threatening both personal and business computing (Bou-Harb and Neshenko, 2020) to counter these attacks, a number of security extensions to 802.11 have been proposed to address vulnerabilities related to unauthorized access and breach of confidentiality. The high demand for access to wireless networks makes it necessary to count for the issue of availability as another important security requirement (Bicakci and Tavli, 2009). Denial-of - Service (DoS) attacks compromise the availability of part or all of the wireless network resources / services. Such attacks are intended to prevent legitimate users from accessing the network. It is worth noting that DoS attacks are different from selfish behaviour motivated by a possible beneficial outcome. Due to the broadcast nature of the wireless network, DoS attacks can be easily carried out, especially in the wireless domain. In addition, several 802.11 specific DoS vulnerabilities have been experimentally demonstrated in literature in recent years (Nwebonyi et al., 2019) (Cheng and Chen, 2016). IEEE 802.11 Wi-Fi networks are prone to large number of Denial of Service (DoS) attacks due to vulnerabilities at the media access control (MAC) layer of 802.11 protocol (Agarwal et al., 2016). Denial-of - Service attacks pose a significant threat to the availability and reliability of wireless network operations in general and to the critical information infrastructure in particular. The World Economic Forum (WEF) has confirmed that the DoS attacks

lead to a severe disruption of critical information infrastructure (Ferreira and Walton, 2005). In particular, the United Kingdom National Infrastructure Security Coordination Centre (NISCC) warned 2005 (Bruce et al., 2005) that denial of service attack could impact the critical national infrastructure.

## 1.2 Problem Statement

Detecting DoS Attack in wireless networks at its early stages is challenging as the attacker can cascade the entity of legitimate nodes or create fake entities. This is due to the unsecured nature of the management frame in the 802.11 protocol used in wireless networks. Unprotected management frames have motivated many adversaries to perform many types of DoS attacks (Hangargi, 2014, Agarwal et al., 2016). Therefore, existing mechanisms suffer from poor accuracy performance in terms of high false alarm and low detection rate in the early stages of the attacks. This study proposed alternative schemes addressing all the aforementioned issues.

## 1.3 Problem Background

Denial-of-Service (DoS) attacks target network availability in an attempt to deny legitimate users access to network resources. It is unlike the selfish attitude of some users that are motivated ulterior motives. DoS attacks are easier to carry out in wireless domains given its broadcast nature. Many of the standard security vulnerabilities in 802.11 have been piloted in the literature in recent years (Kolias et al., 2016, Bicakci and Tavli, 2009). Availability attacks are a form of DoS attack which attempts selectively or completely disable access to the network using several types of MAC frames such as de-authentication and de-association frames (Kolias et al., 2015). Wireless networks and technologies are generally more vulnerable to DoS attacks in comparison to their wired alternatives.

In the wireless security, we mainly consider the 3 protections of any packet transmitted in the air: Confidentiality, Integrity, Availability. Confidentiality and Integrity are

mainly managed by various protocols such as WEP (wired equivalent privacy), WPA (wi-fi protected access), WPA2 (wi-fi protected access version2), but WLAN is still vulnerable from availability attacks such as DOS (denial of service) attacks (Arockiam and Vani, 2011, Weixiong et al., 2020).

DoS attacks target the data link layer of either the clients or access point in the WLAN by spoofing the Media Access Control (MAC) address and sending multiple forged frames to flood the network and deny legitimate clients access to the network (Yong et al., 2008). These attacks leverage the management frames because they are unencrypted; thereby rendering the MAC address of the access point or station vulnerable to hackers (Ferreri et al., 2004) (Vani et al., 2011b).

Existing solutions that address the detection of denial of service attacks on 802.11 networks can be categorized into rule-based, statistical-based, and machine learning-based techniques. Rule-based techniques rely on pre-defined rules that define the specific behaviour of the attack. In their study, (Kirongo, 2017) employed the timing behaviour of different management frames to detect and mitigate different types of wireless data link layer attacks like de-authentication and flooding attacks. Similarly, (Letsoalo and Ojo, 2018) utilized the received signal strength (RSS), round trip time (RTT), and de-authentication frames analysis (DFA) to detect de-authentication attacks. However, relying on pre-defined rules is not sufficient to detect such attacks as the attacker could evasively change its behaviour to deceive the detection system.

Statistical-based detection techniques employ the data generated by the communicating stations with the APs to discover the suspicious activities that goes beyond the predefined threshold. The study conducted by (Lee et al., 2008) employed a statistical approach to detect probe request attacks. The solution monitored the rate of probe requests issued by the communicating stations and raises an alarm if the number of those requests exceeded a threshold. In addition, (Hussain, 2005); (Kaushik and Gautam, 2013) and (Goel et al., 2013) proposed a Forge Resistance Relationship (FRR) It is the method that combines the window of sequence numbers and traffic access statistics for MAC spoofing attacks detection. Statistically based approaches

rely on assumptions about the linearity of distribution of the data, which might not be realistic in the light of the dynamic nature of the attackers' behaviour.

Similar to statistical-based detection solutions are the machine learning-based solutions that utilize the data collected from the communication channels between the stations and APs to build a model that represents the behaviour of either the normal or rogue nodes. Based on the nature of training data, the detection model could be anomaly-based or misuse-based. The former (anomaly-based) is built by profiling the behaviour of normal nodes whereas the latter (misuse-based) is built using the behaviour of the attackers. The study conducted by (Gajbhiye and Daruwala, 2016) and (Lackner et al., 2009) utilized the patterns extracted from the sequence number field to build a pattern recognition-based model that detects MAC spoofing attacks. Similarly, (RazaCheema et al., 2018) proposed a model trained with the data related to signal print in order to detect MAC spoofing attacks. In addition, (Lin et al., 2019, Wang et al., 2018) utilized the ANN model to detect MAC spoofing attacks. (Wang et al., 2018, Mikhail et al., 2019) built a machine learning-based model to detect probe request attacks using the data in the sequence number field of the management frame. Furthermore, (Ratnayake et al., 2011) utilized the data of delta-time, sequence number, Signal Strength Indicator (SSI), and frame sub-type of traffic captured on a home WLAN to train ANN-GA based probe request attacks detection model. Similarly, (Ratnayake et al., 2014) proposed an ANN model to detect the probe request attacks. However, the proposed models focused only on two types of attacks, MAC spoofing and probe request attacks, thus, are unable to deal with other types of DoS attacks. DoS attacks compromise the availability of wireless network services and make it difficult to detect and mitigate. The 802.11-based wireless systems are susceptible to denial of service attack attacks (Buriachok and Sokolov, 2019, Rahman and Tomar, 2018) for two reasons. The first is that there are no natural limits to radio waves which makes it necessary to share the communication media among all nodes in the communication areas. Thus, RF jamming is a common occurrence in wireless networks. Communications on the 802.11-based systems have normal ranges of 2.4 GHz (for 802.11b and g) and 5GHz (for 802.11a). Hence, a high-power Rouge signal can interfere with wireless transmissions of the existing network. The second reason is lack of authentication mechanism in 802.11 management frames (Rahman and Tomar, 2018). The implied trust among communicating wireless devices is reflected

in the unprotected and exposed nature of management frames makes it easy for an attacker to parody legitimate devices and drop individual hosts (Nguyen et al., 2008).

Although DoS attacks target both wired and wireless networks alike, wireless networks have become an interesting target of hackers over the years. By doing, important network connectivity features such as anonymity, security, and privacy are consistently infringed. In 802.11i, an intruder attacks the access point by sending multiple packets with a wrong key every second as a result of which the access point will be automatically shut down for a minute. The intruder keeps sending these wrong-keyed packets even after the access point comes back online in order to deny legitimate users access to the network (Salem et al., 2007). Detecting DoS Attack in wireless networks at its early stages is challenging as the attacker can cascade the entity of legitimate nodes or create fake entities. The Scenario of the DoS attack is a huge number request of flooding which Wasting network performance and Filling the AP buffer. There are many Existing solutions for detecting DoS attacks just like Encryption based methods, Sequence number-based methods, and Machine learning. to face the DoS attack problem there many Challenges need to require changes in the 802.11 protocol stack to support authentication and encryption of frames which are currently non authenticated, Patching client and AP software and up-gradation to newer 802.11 standards. A sufficient feature that reduces the detection accuracy is a gap of detecting DoS attack in WLAN which the researchers try to find the desired solution to get a High accuracy DoS detection  Figure1.1 illustrates the scenario leading to the problem addressed by this research.

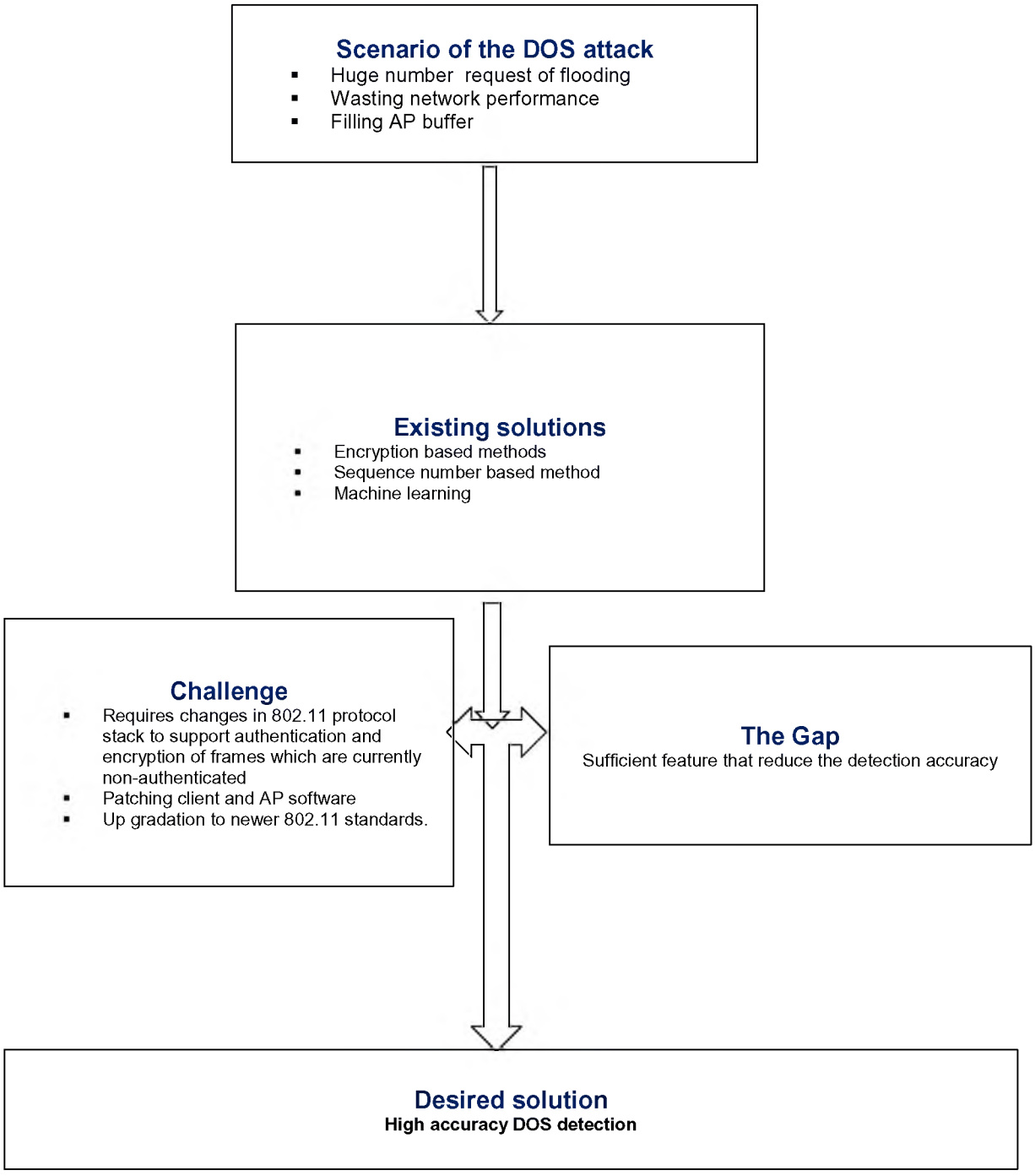


Figure 1.1 Scenario leading to the problem statement

## 1.4 Research Questions

This research is intended to deal with the problems related to flooding based DoS attack detection in WLAN infrastructure. This research seeks to answer the following questions:

(a) How can the accuracy of resource exhaustion based DoS attacks be effectively increased under sophisticated attack scenarios?

(b) How can the discriminative features related to de-authentication and disassociation attacks that help decrease false alarms be derived?

(c) How can the DoS attack detection scheme under sophisticated attacks be enhanced to increase the accuracy of DoS attack detection?

(d) How can the detection rate of de-authentication and disassociation attacks be increased?

## 1.5 Research Objectives

The aim of this study is to design and develop resource exhaustion and Masquerading based DoS attacks detection scheme. The main objectives of this research are:

1) To investigate the management frame resource exhaustion attack detection scheme using an artificial neural network to increase detection accuracy.

2) To design and develop a de-authentication and disassociation detection scheme by deriving features with an artificial neural network to reduce false alarm rate.

3) To further improve the detection rate of the scheme proposed in scheme two using feature derived from the unsupervised method developed in scheme one.

4) To verify and compare the proposed schemes against the well-known schemes from the literature.

## 1.6 Scope of the Study

In achieving the objectives of the study as highlighted in the previous section, this study is limited to the following scope:

- 802.11 infrastructure mode.
- Resource Exhaustion Attack and masquerading DoS attack in infrastructure network mode.
- This study uses Recieved Signal Strenght Indicater (RSSI) to make detection of the attacker.
- The study focuses mostly on detecting flooding based DoS attacks to enhance effectiveness and efficiency.

## 1.7 Significance of the Study

- Wireless LANs are very common and have found widespread use:
- among different communication technologies,
- DoS attacks are particularly possible due to the open and unprotected nature of the management frames that carry the MAC address of the source.
- This vulnerability exposes the network to layer attacks on wireless connections.
- Low detection performance in the early stages of the current Resource Exhausted Attack Detection Schemes is due to the bad characteristics

representing the attackers during the training process, which has created difficulties in distinguishing between false and legitimate management frames.

- This research proposes new improved schemes which increase the detection accuracy and decrease the false alarm rate (Aung and Thant, 2017)

## 1.8 Research Contributions

This research introduces new schemes to improve DoS detection accuracy and detection rate. The following represents the contribution of the study:

1) A scheme for detecting and a resource exhaustion Denial-of-Service (DoS) attack in WLANs.

2) New detection scheme for DE-authentication and Di-association flooding attack in WLAN.

3) Scheme for Detecting Management-Frames-Based Denial-of-Service (DoS) Attack in WLAN.

## 1.9 Thesis Organization

The introduction of the study has been presented in this chapter. An introduction to 802.11 WLAN infrastructure mode and DoS detection topics and problems as well as the motivation for the research by reviewing the background to the problem has been presented. The problem statement and the objectives of the research are also outlined here. In addition, the contribution of the proposed research has also been highlighted. Chapter 2 reviews the pertinent literature related to DoS detection along with the existing methods and techniques. The methodology of achieving the objectives of this study is explained in Chapter 3. Chapter 4 focuses on

designing and developing a Resource Exhaustion Attack Detection Scheme (READS), which is the outcome of the first phase in this study. Chapter 5 focuses on designing and developing a De-authentication and Disassociation Detection Scheme (D3S) which is the outcome of the second phase in this study. Chapter 6 focuses on designing and developing an enhanced De-authentication and Disassociation Detection Scheme (ED3S). Finally, Chapter 7 concludes the study

## REFERENCES


ABDALLAH, A. E., RAZAK, S. A. & GHALIB, F. A. Deauthentication and Disassociation Detection and Mitigation Scheme Using Artificial Neural Network. International Conference of Reliable Information and Communication Technology, 2019. Springer, 857-866.

ABDULKARIM, S. & GARKO, A. 2016. Effectiveness of firefly algorithm based neural network in time series forecasting. *Bayero Journal of Pure and Applied Sciences,* 9**,** 6-10.

AGARWAL, M., BISWAS, S. & NANDI, S. Detection of de-authentication dos attacks in wi-fi networks: A machine learning approach. 2015 IEEE International Conference on Systems, Man, and Cybernetics, 2015. IEEE, 246-251.

AGARWAL, M., PASUMARTHI, D., BISWAS, S. & NANDI, S. 2016. Machine learning approach for detection of flooding DoS attacks in 802.11 networks and attacker localization. *International Journal of Machine Learning and Cybernetics,* 7**,** 1035-1051.

AHAD, N., QADIR, J. & AHSAN, N. 2016. Neural networks in wireless networks: Techniques, applications and guidelines. *Journal of network and computer applications,* 68**,** 1-27.

AL-OMARI, S. A. K. & SUMARI, P. 2010. An overview of mobile ad hoc networks for the existing protocols and applications. *arXiv preprint arXiv:1003.3565.*

ALLIANCE, W.-F. 2006. Wi-Fi protected setup specification version 1.0. *Online], Dec.*

ALOTAIBI, B. & ELLEITHY, K. 2016. Rogue access point detection: Taxonomy, challenges, and future directions. *Wireless Personal Communications,* 90**,** 1261-1290.

ARBAUGH, W. & MISHRA, A. 2005. An Initial Security Analysis of IEEE 802.1 X Estandard. 2002. 12f. *University of Maryland. Disponível em: http://www. cs. umd. edu/~ waa/1x. pdf Acesso em,* 6.

ARBAUGH, W. A. 2003. *Real 802.11 security: Wi-Fi protected access and 802.11 i*, Addison-Wesley Longman Publishing Co., Inc.

ARBAUGH, W. A., SHANKAR, N. & WAN, Y. J. 2003. Your 802.11 Wireless network has No clothes (March 2001). *WWW page http://www. cs. umd. edu/waa/wireless. pdf Accessed July.*

AROCKIAM, L. & VANI, B. 2010. A Survey of Denial of Service Attacks and It's Countermeasures on Wireless Network.

AROCKIAM, L. & VANI, B. 2011. A Survey of Denial of Service Attacks and it's Counter measures on Wireless Network (Flooding attacks).

ASLAM, B., ISLAM, M. H. & KHAN, S. Pseudo randomized sequence number based solution to 802.11 disassociation denial of service attack. Mobile Computing and Wireless Communication International Conference, 2006. MCWC 2006. Proceedings of the First, 2006. IEEE, 215-220.

ASSOCIATION, I. S. 2012. IEEE Standard for Information Technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements, Part 11: Wireless LAN

Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std,* 802**,** 2793.

AUNG, M. A. C. & THANT, K. P. Detection and mitigation of wireless link layer attacks. 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA), 2017. IEEE, 173-178.

BANKS, J. 2016. *Online gambling and crime: Causes, controls and controversies*, Routledge.

BARNICKEL, D. J., WILLIS III, T. M., ZARSKY, D., LIU, K., BARZEGAR, F., GERSZBERG, I., BOGDAN, P. A., PIMM, B., BRITZ, D. M. & HENRY, P. S. 2019. Method and apparatus for collecting data associated with wireless communications. Google Patents.

BENCEL, R., KACHMAN, O. & NAGY, M. 2019. Information Sciences and Technologies Bulletin of the ACM Slovakia.

BENZAÏD, C., BOULGHERAIF, A., DAHMANE, F. Z., AL-NEMRAT, A. & ZERAOULIA, K. Intelligent detection of mac spoofing attack in 802.11 network. Proceedings of the 17th International Conference on Distributed Computing and Networking, 2016. 1-5.

BERGLUND, J. E. J. & LI, Z. 2016. Providing station context and mobility in a wireless local area network having a split MAC architecture. Google Patents.

BIANCHI, G. 2000. Performance analysis of the IEEE 802.11 distributed coordination function. *Selected Areas in Communications, IEEE Journal on,* 18**,** 535-547.

BICAKCI, K. & TAVLI, B. 2009. Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. *Computer Standards & Interfaces,* 31**,** 931-941.

BOGDANOSKI, M., LATKOSKI, P. & RISTESKI, A. 2016. Analysis of the Impact of AuthRF and AssRF Attacks on IEEE 802.11 e-based Access Point. *Mobile Networks and Applications***,** 1-10.

BOLAND, H. & MOUSAVI, H. Security issues of the IEEE 802.11 b wireless LAN. Electrical and Computer Engineering, 2004. Canadian Conference on, 2004. IEEE, 333-336.

BORISOV, N., GOLDBERG, I. & WAGNER, D. Intercepting mobile communications: the insecurity of 802.11. Proceedings of the 7th annual international conference on Mobile computing and networking, 2001. ACM, 180-189.

BOU-HARB, E. & NESHENKO, N. 2020. Taxonomy of IoT Vulnerabilities. *Cyber Threat Intelligence for the Internet of Things.* Springer.

BRUCE, R., DYNES, S., BRECHBUHL, H., BROWN, B., GOETZ, E., VERHOEST, P., LUIIJF, E., DEFENCE, T. & HELMUS, S. 2005. International policy framework for protecting critical information infrastructure: A discussion paper outlining key policy issues. *The Hague: TNO***,** 73.

BURIACHOK, V. & SOKOLOV, V. 2019. Using 2.4 Ghz Wireless Botnets to Implement Denial-Of-Service Attacks. *arXiv preprint arXiv:1902.08425.*

CHATZIMISIOS, P., BOUCOUVALAS, A. & VITSAS, V. Optimisation of RTS/CTS handshake in IEEE 802.11 Wireless LANs for maximum performance. IEEE Global Telecommunications Conference Workshops, 2004. GlobeCom Workshops 2004., 2004. IEEE, 270-275.

CHEN, J.-C. & WANG, Y.-P. 2005. Extensible authentication protocol (EAP) and IEEE 802.1 x: tutorial and empirical experience. *IEEE communications magazine,* 43**,** supl. 26-supl. 32.

CHEN, K., ZHANG, S., LI, Z., ZHANG, Y., DENG, Q., RAY, S. & JIN, Y. 2018. Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice. *Journal of Hardware and Systems Security,* 2**,** 97-110.

CHEN, X., MAKKI, K., YEN, K. & PISSINOU, N. 2009. Sensor network security: a survey. *IEEE Communications Surveys & Tutorials,* 11.

CHENG, S.-M. & CHEN, P.-Y. Ecology-based DoS attack in cognitive radio networks. 2016 IEEE Security and Privacy Workshops (SPW), 2016. IEEE, 104-110.

CILFONE, A., DAVOLI, L., BELLI, L. & FERRARI, G. 2019. Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies. *Future Internet,* 11**,** 99.

COMMITTEE, I. C. S. L. M. S. 1999. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. *ANSI/IEEE Std. 802.11-1999.*

DASGUPTA, D., GOMEZ, J., GONZALEZ, F., KANIGANTI, M., YALLAPU, K. & YARRAMSETTI, R. MMDS: multilevel monitoring and detection system. Proceedings of the 15th Annual Computer Security Incident Handling Conference, 2003. 22-27.

DE CARVALHO, J. A. P., VEIGA, H., PACHECO, C. F. R. & REIS, A. D. Performance Evaluation of IEEE 802.11 a 54 Mbps WEP Multi-Node Laboratory Links. 2018 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2018. IEEE, 1-6.

DZUNG, D., NAEDELE, M., VON HOFF, T. P. & CREVATIN, M. 2005. Security for industrial communication systems. *Proceedings of the IEEE,* 93**,** 1152-1177.

EGLI, P. 2006. Susceptibility of wireless devices to denial of service attacks. *Technical white paper, Netmodule AG.*

FALL, K. A delay-tolerant network architecture for challenged internets. Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, 2003. ACM, 27-34.

FANG, X., MISRA, S., XUE, G. & YANG, D. 2012. Smart grid—The new and improved power grid: A survey. *IEEE communications surveys & tutorials,* 14**,** 944-980.

FERREIRA, F. H. & WALTON, M. 2005. *World development report 2006: equity and development*, World Bank Publications.

FERRERI, F., BERNASCHI, M. & VALCAMONICI, L. 2004. Access points vulnerabilities to DoS attacks in 802.11 networks. *2004 IEEE Wireless Communications and Networking Conference, WCNC 2004,* 1**,** 634-638.

FLORIO, L. & WIERENGA, K. Eduroam, providing mobility for roaming users. Proceedings of the EUNIS 2005 Conference, Manchester, 2005.

FLUHRER, S., MANTIN, I. & SHAMIR, A. Weaknesses in the key scheduling algorithm of RC4. Selected areas in cryptography, 2001. Springer, 1-24.

FOTOUHI, A., QIANG, H., DING, M., HASSAN, M., GIORDANO, L. G., GARCIA-RODRIGUEZ, A. & YUAN, J. 2019. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Communications Surveys & Tutorials,* 21**,** 3417-3442.

FRANKEL, S., EYDT, B., OWENS, L. & KENT, K. 2006. Guide to ieee 802.11 i: Establishing robust security networks. *National Institute of Standards and Technology*.

FRANKEL, S., EYDT, B., OWENS, L. & SCARFONE, K. 2007. Establishing wireless robust security networks: a guide to IEEE 802.11 i. *National Institute of Standards and Technology*.

GAJBHIYE, Y. & DARUWALA, R. RSS-based spoofing detection and localization algorithm in IEEE 802.11 wireless networks. 2016 International Conference on Communication and Signal Processing (ICCSP), 2016. IEEE, 1642-1645.

GHALIB, S., MISHRA, R., BAGHEL, A. S. & SHARMA, S. 2018. Routing protocol development for quality of service optimization of video-on-demand system over mobile ad hoc networks. *International Journal of Communication Systems,* 31**,** e3452.

GOEL, S., KAUSHIK, V. & GAUTAMR, S. 2013. Spoofing Detection Methods in Wireless LAN (WLAN)-A Study with pros and cons. *American Council for an Energy-Efficient Economy (ACEEE)*.

GOEL, S. & KUMAR, S. An improved method of detecting spoofed attack in wireless LAN. 2009 First International Conference on Networks & Communications, 2009. IEEE, 104-108.

GREKHOV, A., KONDRATIUK, V. & ILNITSKA, S. 2019. RPAS Satellite Communication Channel Based on IEEE 802.11 b Standard. *Transport and Aerospace Engineering,* 7**,** 32-40.

GUO, F. & CHIUEH, T.-C. Sequence number-based MAC address spoof detection. International Workshop on Recent Advances in Intrusion Detection, 2005. Springer, 309-329.

HAATAJA, K. M. 2006. Security in Bluetooth, WLAN and IrDA: a comparison. *Retrieved on July,* 1**,** 2006.

HANGARGI, M. 2014. Denial of Service Attacks in Wireless Networks.

HIERTZ, G. R., DENTENEER, D., STIBOR, L., ZANG, Y., COSTA, X. P. & WALKE, B. 2010a. The IEEE 802.11 universe. *IEEE Communications Magazine,* 48**,** 62-70.

HIERTZ, G. R., DENTENEER, D., STIBOR, L., ZANG, Y., COSTA, X. P. & WALKE, B. 2010b. The IEEE 802.11 universe. *IEEE Communications Magazine,* 48.

HOTCHKISS, A., SINGLA, A., KUMAR, A., AMAROSE, N., WHITE, P., KAZIOR, M., BARJAKTAREVIC, M. & VAIDYA, S. 2019. Controlled guest access to wi-fi networks. Google Patents.

HSIEH, W.-C., LO, C.-C., LEE, J.-C. & HUANG, L.-T. The implementation of a proactive wireless intrusion detection system. The Fourth International Conference onComputer and Information Technology, 2004. CIT'04., 2004. IEEE, 581-586.

HUANG, H., AHMED, N. & KARTHIK, P. 2011. On a new type of denial of service attack in wireless networks: The distributed jammer network. *IEEE Transactions on Wireless Communications,* 10**,** 2316-2324.

HUSSAIN, A. N. 2005. *Measurement and spectral analysis of denial of service attacks*, University of Southern California.

IYER, P. J. & NARASIMHAN, P. 2005. System and method for monitoring and enforcing policy within a wireless network. Google Patents.

JIANG, P., WU, H., WANG, C. & XIN, C. Virtual MAC spoofing detection through deep learning. 2018 IEEE International Conference on Communications (ICC), 2018. IEEE, 1-6.
KANNAMMAL, A. & ROY, S. S. Survey on secure routing in mobile ad hoc networks. 2016 International Conference on Advances in Human Machine Interaction (HMI), 2016. IEEE, 1-7.
KAUR, J. MAC layer management frame denial of service attacks. 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), 2016. IEEE, 155-160.
KAUSHIK, V. & GAUTAM, S. Wireless LAN (WLAN) spoofing detection methods-Analysis and the victim Silent case. 2013 INTERNATIONAL CONFERENCE ON SIGNAL PROCESSING AND COMMUNICATION (ICSC), 2013. IEEE, 155-160.
KHOROV, E., KIRYANOV, A., LYAKHOV, A. & BIANCHI, G. 2018. A tutorial on IEEE 802.11 ax high efficiency WLANs. *IEEE Communications Surveys & Tutorials,* 21**,** 197-216.
KIRONGO, A. C. 2017. *A vulnerability model for wireless local area networks in an insecure wardriving setting.*
KOLIAS, C., KAMBOURAKIS, G., STAVROU, A. & GRITZALIS, S. 2015. Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset. *IEEE Communications Surveys & Tutorials,* 18**,** 184-208.
KOLIAS, C., KAMBOURAKIS, G., STAVROU, A. & GRITZALIS, S. 2016. Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset. *IEEE Communications Surveys & Tutorials,* 18**,** 184-208.
KUMAR, A. & PAUL, P. Security analysis and implementation of a simple method for prevention and detection against Evil Twin attack in IEEE 802.11 wireless LAN. Computational Techniques in Information and Communication Technologies (ICCTICT), 2016 International Conference on, 2016. IEEE, 176-181.
KWAK, J. A. 2010. Method and apparatus for network management using periodic measurements of indicators. Google Patents.
LACKNER, G., PAYER, U. & TEUFL, P. 2009. Combating Wireless LAN MAC-layer Address Spoofing with Fingerprinting Methods. *IJ Network Security,* 9**,** 164-172.
LAI, Y.-N., WANG, C.-X., TONG, W. & WANG, X. 2014. Research on the key technology and main issues of power wireless communication network. *Electric Power Information and Communication Technology,* 12**,** 10-14.
LANEMAN, J. N. & WORNELL, G. W. 2003. Distributed space-time-coded protocols for exploiting cooperative diversity in wireless networks. *IEEE Transactions on Information theory,* 49**,** 2415-2425.
LASHKARI, A. H., MANSOOR, M. & DANESH, A. S. Wired equivalent privacy (WEP) versus Wi-Fi protected access (WPA). 2009 International Conference on Signal Processing Systems, 2009. IEEE, 445-449.
LEE, K., KIM, J., KWON, K. H., HAN, Y. & KIM, S. 2008. DDoS attack detection method using cluster analysis. *Expert systems with applications,* 34**,** 1659-1665.
LEHEMBRE, G. 2005. Wi-Fi security–wep, wpa and wpa2. *Hackin9 (January 2006).*

LETSOALO, E. & OJO, S. Survey of Media Access Control address spoofing attacks detection and prevention techniques in wireless networks. 2016 IST-Africa Week Conference, 2016. IEEE, 1-10.
LETSOALO, E. & OJO, S. A Model to Mitigate Session Hijacking Attacks in Wireless Networks. 2018 IST-Africa Week Conference (IST-Africa), 2018. IEEE, Page 1 of 10-Page 10 of 10.
LI, J. & GARUBA, M. Encryption as an effective tool in reducing wireless LAN vulnerabilities. Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on, 2008. IEEE, 557-562.
LI, Q. & TRAPPE, W. Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks. 2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, 2006. IEEE, 50-59.
LI, Q. & TRAPPE, W. 2007. Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships. *IEEE Transactions on Information Forensics and Security,* 2**,** 793-808.
LIN, X. CAT: Building couples to early detect node compromise attack in wireless sensor networks. Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, 2009. IEEE, 1-6.
LIN, Y., ZHU, X., ZHENG, Z., DOU, Z. & ZHOU, R. 2019. The individual identification method of wireless device based on dimensionality reduction and machine learning. *The Journal of Supercomputing,* 75**,** 3010-3027.
LINDQVIST, J., AURA, T., DANEZIS, G., KOPONEN, T., MYLLYNIEMI, A., MÄKI, J. & ROE, M. Privacy-preserving 802.11 access-point discovery. Proceedings of the second ACM conference on Wireless network security, 2009. ACM, 123-130.
LIU, K. 2019. *Security Analysis in Device-to-Device Wireless Networks.* Illinois Institute of Technology.
LOPEZ-AGUILERA, E., GARCIA-VILLEGAS, E. & CASADEMONT, J. 2019. Evaluation of IEEE 802.11 coexistence in WLAN deployments. *Wireless Networks,* 25**,** 87-104.
MA, D. & TSUDIK, G. 2010. Security and privacy in emerging wireless networks. *IEEE Wireless Communications,* 17.
MADORY, D. C. 2006. *New methods of spoof detection in 802.11 b wireless networking.* Dartmouth College.
MALEKZADEH, M., GHANI, A. A. A., SUBRAMANIAM, S. & DESA, J. M. 2011. Validating Reliability of OMNeT++ in Wireless Networks DoS Attacks: Simulation vs. Testbed. *IJ Network Security,* 13**,** 13-21.
MARTINOVIC, I., ZDARSKY, F. A. & SCHMITT, J. B. Regional-based authentication against dos attacks in wireless networks. Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks, 2007. ACM, 176-179.
MIKHAIL, J. W., FOSSACECA, J. M. & IAMMARTINO, R. 2019. A Semi-Boosted Nested Model With Sensitivity-Based Weighted Binarization for Multi-Domain Network Intrusion Detection. *ACM Transactions on Intelligent Systems and Technology (TIST),* 10**,** 28.
MILE, A., OKEYO, G. & KIBE, A. 2018. Hybrid IEEE 802.15. 6 Wireless Body Area Networks Interference Mitigation Model for High Mobility Interference Scenarios. *Wireless Engineering and Technology,* 9**,** 34.
MISHRA, A., SHIN, M. & ARBAUGH, W. 2002. Your 802.11 network has no clothes. *IEEE Communications Magazine,* 9**,** 44-51.

MISRA, S., GHOSH, A. & OBAIDAT, M. S. Detection of identity-based attacks in wireless sensor networks using signalprints. 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, 2010. IEEE, 35-41.

MORÉ, J. J. 1978. The Levenberg-Marquardt algorithm: implementation and theory. *Numerical analysis*. Springer.

MUKHERJEE, A., KESHARY, V., PANDYA, K., DEY, N. & SATAPATHY, S. C. 2018. Flying ad hoc networks: A comprehensive survey. *Information and Decision Sciences*. Springer.

NANDI, S. Elliptic curve cryptography based mechanism for secure Wi-Fi connectivity. Distributed Computing and Internet Technology: 15th International Conference, ICDCIT 2019, Bhubaneswar, India, January 10–13, 2019, Proceedings, 2019. Springer, 422.

NARAYANAN, S., LIU, P. & PANWAR, S. S. On the advantages of multi-hop extensions to the IEEE 802.11 infrastructure mode. Wireless Communications and Networking Conference, 2005 IEEE, 2005. IEEE, 132-138.

NGUYEN, T. N., TRAN, B. N. & NGUYEN, D. A lightweight solution for Wireless LAN: Letter-envelop protocol. Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on, 2008. IEEE, 17-21.

NWEBONYI, F. N., MARTINS, R. & CORREIA, M. E. 2019. Reputation based approach for improved fairness and robustness in P2P protocols. *Peer-to-Peer Networking and Applications,* 12**,** 951-968.

ODHIAMBO, O. N., BIERMANN, E. & NOEL, G. An integrated security model for WLAN. AFRICON, 2009. AFRICON'09., 2009. IEEE, 1-6.

OSTERHAGE, W. 2018. *Wireless Network Security*, CRC Press.

PACK, S., CHOI, J., KWON, T. & CHOI, Y. 2007. Fast-handoff support in IEEE 802.11 wireless networks. *Communications Surveys & Tutorials, IEEE,* 9**,** 2-12.

PALLAS, D., MAASSMANN, E. & BARBER, S. 2019. Wireless network steering. Google Patents.

PARK, P., DI MARCO, P., NAH, J. & FISCHIONE, C. 2020. Wireless Avionics Intra-Communications: A Survey of Benefits, Challenges, and Solutions. *arXiv preprint arXiv:2006.12060*.

PERSIA, A., DURAIRAJ, M. & SIVAGOWRY, S. Study of thwarting DoS attacks by detecting MAC spoof in WLAN infrastructure networks. Advanced Communication Control and Computing Technologies (ICACCCT), 2012 IEEE International Conference on, 2012. IEEE, 264-268.

RAGER, A. T. WEPCrack–An 802.11 key breaker. *Website],[cited 2003 Jan 30], Available HTTP: http://wepcrack. sourceforge. net*.

RAHMAN, R. U. & TOMAR, D. S. 2018. Security Attacks on Wireless Networks and Their Detection Techniques. *Emerging Wireless Communication and Network Technologies*. Springer.

RAPPAPORT, T. S., ANNAMALAI, A., BUEHRER, R. & TRANTER, W. H. 2002. Wireless communications: past events and a future perspective. *IEEE Communications Magazine,* 40**,** 148-161.

RATNAYAKE, D. N., KAZEMIAN, H. B. & YUSUF, S. A. Improved detection of Probe Request Attacks: Using Neural Networks and Genetic Algorithm.

Proceedings of the International Conference on Security and Cryptography-Volume 1: SECRYPT, 2012. SciTePress.
RATNAYAKE, D. N., KAZEMIAN, H. B. & YUSUF, S. A. 2014. Identification of probe request attacks in WLANs using neural networks. *Neural Computing and Applications,* 25**,** 1-14.
RATNAYAKE, D. N., KAZEMIAN, H. B., YUSUF, S. A. & ABDULLAH, A. B. 2011. An intelligent approach to detect probe request attacks in IEEE 802.11 networks. *Engineering Applications of Neural Networks*. Springer.
RAZACHEEMA, A., ALSMADI, M. & IKKI, S. Survey of Identity-Based Attacks Detection Techniques in Wireless Networks Using Received Signal Strength. 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE), 2018. IEEE, 1-6.
REDDY, S. V., RAMANI, K. S., RIJUTHA, K., ALI, S. M. & REDDY, C. P. Wireless hacking-a WiFi hack by cracking WEP. Education Technology and Computer (ICETC), 2010 2nd International Conference on, 2010. IEEE, V1-189-V1-193.
REN, J. & LI, T. CDMA physical layer built-in security enhancement. Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, 2003. IEEE, 2157-2161.
REZVY, S., LUO, Y., PETRIDIS, M., LASEBAE, A. & ZEBIN, T. An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks. 2019 53rd Annual Conference on Information Sciences and Systems (CISS), 2019. IEEE, 1-6.
ROSHAN, P. & LEARY, J. 2004. *802. 11 Wireless Lan Fundamentals*, Cisco Systems.
ROSS, J. 2008. *The Book of Wireless: A Painless Guide to Wi-Fi and Broadband Wireless*, No Starch Press.
RUDOLF, M., DICK, S. G., HUNKELER, T. J., RAHMAN, S. A. & KWAK, J. A. 2017. Method and system for transferring information between network management entities of a wireless communication system. Google Patents.
RUMALE, A. & CHAUDHARI, D. 2011. IEEE 802.11 x, and WEP, EAP, WPA/WPA2. *Tech. Appl,* 2**,** 1945-1950.
SALEM, M., SARHAN, A. & ABU-BAKR, M. 2007. A DOS Attack Intrusion Detection and Inhibition Technique for Wireless
Computer Networks. *ICGST- CNIR,* 7.
SARMA, H. K. D. & KAR, A. Security threats in wireless sensor networks. Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International, 2006. IEEE, 243-251.
SHAFIQ, M. Z. & FAROOQ, M. 2007. Defence against 802.11 DoS attacks using artificial immune system.
SHARMA, M., TANDON, A., NARAYAN, S. & BHUSHAN, B. Classification and analysis of security attacks in WSNs and IEEE 802.15. 4 standards: A survey. 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall), 2017. IEEE, 1-5.
SHELDON, F. T., WEBER, J. M., YOO, S.-M. & PAN, W. D. 2012. The insecurity of wireless networks. *IEEE Security & Privacy,* 10**,** 54-61.
SHIU, Y.-S., CHANG, S. Y., WU, H.-C., HUANG, S. C.-H. & CHEN, H.-H. 2011. Physical layer security in wireless networks: A tutorial. *IEEE wireless Communications,* 18.

SINGH, J. 2009. Quality Of service in wireless Lan Using OPNET Modeller. *Computer Science and Engineering Department Thapar University*.

SINGH, P., MISHRA, M. & BARWAL, P. Analysis of security issues and their solutions in wireless LAN. Information Communication and Embedded Systems (ICICES), 2014 International Conference on, 2014. IEEE, 1-6.

SINGH, R. & SHARMA, T. P. 2015. On the IEEE 802.11 i security: a denial-of-service perspective. *Security and Communication Networks,* 8**,** 1378-1407.

SINHA, P., JHA, V., RAI, A. K. & BHUSHAN, B. Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. Signal Processing and Communication (ICSPC), 2017 International Conference on, 2017. IEEE, 288-293.

SOUILAH, H., BAADACHE, A. & BOUALLOUCHE-MEDJKOUNE, L. 2019. A challenge-based countermeasure against the spoofed PS-Poll-based DoS attack in IEEE 802.11 networks. *International Journal of Critical Computer-Based Systems,* 9**,** 193-214.

SOYINKA, W. 2010. *Wireless Network Administration: A Beginner's Guide*, McGraw-Hill.

STUBBLEFIELD, A., IOANNIDIS, J. & RUBIN, A. D. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. NDSS, 2002.

SUGANTHA, K. & SHANMUGAVEL, S. Anomaly detection of the NAV attack in MAC layer under non-time and time-constrained environment. 2006 IFIP International Conference on Wireless and Optical Communications Networks, 2006. IEEE, 5 pp.-5.

SUHERMAN, S. Packet size impact on the 802.11 network performances. IOP Conference Series: Materials Science and Engineering, 2018. IOP Publishing, 012275.

SZCZYPIORSKI, K. HICCUPS: Hidden communication system for corrupted networks. International Multi-Conference on Advanced Computer Systems, 2003. 31-40.

TASKIN, M. I. & GOKTURK, M. S. 2019. System and method for connection and hand-over management across networks and SSIDs. Google Patents.

TEWS, E. & BECK, M. Practical attacks against WEP and WPA. Proceedings of the second ACM conference on Wireless network security, 2009. ACM, 79-86.

THING, V. L. IEEE 802.11 network anomaly detection and attack classification: A deep learning approach. 2017 IEEE Wireless Communications and Networking Conference (WCNC), 2017. IEEE, 1-6.

TRESEANGRAT, K. 2014. *Performance analysis of defense mechanisms against UDP flood attacks*.

VANI, B., AROCKIAM, L., PERSIA, A. & SIVAGOWRY, S. 2011a. Inhibition of Denial of Service Attack in WLAN using the Integrated Central Manager. *International Journal of Computer Applications,* 29**,** 28-33.

VANI, B., AROCKIAM, L., PERSIA, A. & SIVAGOWRY, S. 2011b. Inhibition of Denial of Service Attack in WLAN

using the Integrated Central Manager. *International Journal of Computer Applications,* 29.

VASSIS, D., KORMENTZAS, G., ROUSKAS, A. & MAGLOGIANNIS, I. 2005. The IEEE 802.11 g standard for high data rate WLANs. *IEEE network,* 19**,** 21-26.

WALIULLAH, M. & GAN, D. 2014. Wireless LAN security threats & vulnerabilities. *International Journal of Advanced Computer Science and Applications,* 5.

WALIULLAH, M., MONIRUZZAMAN, A. & RAHMAN, M. S. 2015. An Experimental Study Analysis of Security Attacks at IEEE 802. 11 Wireless Local Area Network. *International Journal of Future Generation Communication and Networking,* 8**,** 9-18.

WALKER, J. 2000. Unsafe at any key size; an analysis of the WEP encapsulation. *IEEE document,* 802**,** /362.

WANG, S.-L., WANG, J., FENG, C. & PAN, Z.-P. Wireless Network Penetration Testing and Security Auditing. ITM Web of Conferences, 2016. EDP Sciences, 03001.

WANG, S., LI, B., YANG, M. & YAN, Z. Intrusion Detection for WiFi Network: A Deep Learning Approach. International Wireless Internet Conference, 2018. Springer, 95-104.

WEI, Y., ZENG, K. & MOHAPATRA, P. Adaptive wireless channel probing for shared key generation. INFOCOM, 2011 Proceedings IEEE, 2011. IEEE, 2165-2173.

WEIXIONG, Y., LEE, R. & SENG, A. K. S. 2020. Security and Privacy Concerns in Wireless Networks-A Survey.

WELCH, D. & LATHROP, S. Wireless security threat taxonomy. IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003., 2003. IEEE, 76-83.

YANG, Y., WU, L., YIN, G., LI, L. & ZHAO, H. 2017. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal,* 4**,** 1250-1258.

YONG, S., TAN, K., GUANLING, C., KOTZ, D. & CAMPBELL, A. Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, 13-18 April 2008 2008. 1768-1776.

YOU, T.-Q. & LIU, J. 2010. Research on Application of Wireless Local Area Network in Smart Power Grid. *Jilin Electric Power,* 38**,** 20-23.

YU, J., KIM, E., KIM, H. & HUH, J. A framework for detecting MAC and IP spoofing attacks with network characteristics. 2016 International Conference on Software Security and Assurance (ICSSA), 2016. IEEE, 49-53.

## LIST OF PUBLICATIONS

Abdallah Elhigazi Abdallah, Shukor Abd Razak, Fuad A. (2019) 'Deauthentication and Disassociation Detection and Mitigation Scheme Using Artificial Neural Network', *International Conference of Reliable Information and Communication Technology*, Springer, pp.857-866.

Abdallah Elhigazi Abdallah, Shukor Abd Razak, Yahya Coulibaly (2015) 'DETECTION AND PREVENTION OF DENIAL OF SERVICE ATTACKS (DOS) IN WLANS INFRASTRUCTURE', *Journal of Theoretical & Applied Information Technology,* Vol. 71, No. 3.

Abdallah Elhigazi Abdallah, Shukor Abd Razak, Fuad A. Ghalib, Yahya Coulibaly (2020) 'Artificial Neural Network based Detection and mitigation Scheme of Deauthentication and Disassociation DoS Attacks on Wireless 802.11 Networks. *Submitted to International Journal of Machine Learning and Cybernetics*

Abdallah Elhigazi Abdallah, Shukor Abd Razak, Fuad A. Ghalib, Yahya Coulibaly (2020)"Resource exhaustion attack detection and mitigation using artificial neural network'. *Submitted to Plos One Journal*

Abdallah Elhigazi Abdallah, Shukor Abd Razak, Fuad A. Ghalib, Yahya Coulibaly (2020) 'Scheme For Detection And Mitigating Management-Frames-Based Denial-Of-Service Attack For Wireless Lan Network Using Artificial Neural Network'. *Submitted to IEEE Access Journal*