DNA-BASED CLIENT PUZZLE FOR WLAN ASSOCIATION PROTOCOL AGAINST CONNECTION REQUEST FLOODING

ALI ORDI

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

Advanced Informatics School
Universiti Teknologi Malaysia

May 2016

Dedicated to
my beloved wife Elahe and my parents.

ACKNOWLEDGEMENT

First and foremost praise and gratitude be to ALLAH, almighty, without whose gracious help it would have been impossible to accomplish this work. I was extraordinarily fortunate in having Dr. Mazdak Zamani and Dato' Prof. Dr. Norbik Bashah Idris as my supervisors in UTM AIS. I would like to express my thanks and appreciation to them, who have supported me during my research with their patience and knowledge. I am profoundly and forever indebted to my parents for their inseparable support, love and prayers throughout my whole life. I am also very grateful to my dear and loving wife, Elahe for her effective support of my soul.

ABSTRACT

In recent past, Wireless Local Area Network (WLAN) has become more popular because of its flexibility. However, WLANs are subjected to different types of vulnerabilities. To strengthen WLAN security, many high security protocols have been developed. But those solutions are found to be ineffective in preventing Denial of Service (DoS) attacks. A 'Connection Request Flooding' DoS (CRF-DoS) attack is launched when an access point (AP) encounters a sudden explosion of connection requests. Among other existing anti CRF-DoS methods, a client puzzle protocol has been noted as a promising and secure potential solution. Nonetheless, so far none of the proposed puzzles satisfy the security requirement of resource-limited and highly heterogeneous WLANs. The CPU disparity, imposing unbearable loads on legitimate users, inefficient puzzle generation and verification algorithms; the susceptibility of puzzle to secondary attacks on legitimate users by embedding fake puzzle parameters; and a notable delay in modifying the puzzle difficulty – these are some drawbacks of currently existing puzzles. To deal with such problems, a secure model of puzzle based on DNA and queuing theory is proposed, which eliminates the above defects while satisfying the Chen puzzle security model. The proposed puzzle (OROD puzzle) is a multifaceted technology that incorporates five main components include DoS detector, queue manager, puzzle generation, puzzle verification, and puzzle solver. To test and evaluate the security and performance, OROD puzzle is developed and implemented in real-world environment. The experimental results showed that the solution verification time of OROD puzzle is up to 289, 160, 9, 3.2, and 2.3 times faster than the Karame-Capkun puzzle, the Rivest time-lock puzzle, the Rangasamy puzzle, the Kuppusamy DLPuz puzzle, and Chen's efficient hash-based puzzle respectively. The results also showed a substantial reduction in puzzle generation time, making the OROD puzzle from 3.7 to 24 times faster than the above puzzles. Moreover, by asking to solve an easy and cost-effective puzzle in OROD puzzle, legitimate users do not suffer from resource exhaustion during puzzle solving, even when under severe DoS attack (high puzzle difficulty).

ABSTRAK

Pada masa lalu *Wireless Local Area Network* (WLAN) menjadi semakin popular kerana fleksibilitinya. Walau bagaimanapun, WLAN adalah tertakluk kepada beberapa jenis kelemahan. Untuk mengukuhkan keselamatan WLAN, banyak protokol keselamatan yang tinggi telah dibangunkan. Tetapi penyelesaian ini didapati tidak berkesan dalam mencegah serangan *Denial of Service* (DoS). Satu serangan permintaan banjir DoS (CRF DoS) dilancarkan apabila pusat akses (AP) menghadapi permintaan sambungan yang tinggi secara tiba-tiba. Antara kaedah anti-CRF-DoS lain yang sedia ada protokol *puzzle* pelanggan yang telah diambil sebagai penyelesaian yang baik dan boleh dipercayai. Walau bagaimanapun, setakat ini tidak ada satu jangkaan yang dicadangkan pun memenuhi syarat-syarat keselamatan sumber yang terhad dan WLAN yang heterogen. CPU perbezaan beban yg tidak berdasarkan pada pengguna yang sah, generasi teka-teki yang tidak cekap dan algoritma pengesahan untuk pengenalan; kelemahan teka-teki untuk serangan kedua pada pengguna yang palsu; mengubah dan kelewatan yang luar biasa dalam kesukaran teka-teki - ini adalah beberapa kelemahan teka-teki kini yang sedia ada. Untuk menguruskan masalah ini, satu model teka-teki yang selamat berdasarkan DNA dan teori teratur telah dicadangkan yang pasti menghapuskan kelemahan di atas dengan melengkapkan model keselamatan teka-teki. Teka-teki yang dicadangkan (Teka-teki OROD) adalah teknologi yang kompleks, yang menggabungkan lima komponen utama termasuk pengesanan DoS, pengurus barisan, generasi teka-teki, teka-teki termasuk pengesahan dan teka-teki penyelesaian. Untuk menguji dan menilai keselamatan dan prestasi, OROD *Puzzle* dibangunkan dan dilaksanakan dalam persekitaran dunia sebenar. Keputusan eksperimen menunjukkan bahawa masa pengesahan penyelesaian Teka-teki OROD adalah sebanyak 289, 160, 9, 3.2, dan 2.3 kali lebih cepat daripada teka-teki karamel Capkun, masa-kunci teka-teki Rivest teka-teki Rangasamy teka-teki Kuppusamy DLPuz dan teka-teki cekap berdasarkan hash Chen. Keputusan juga menunjukkan pengurangan yang ketara daripada masa generasi teka-teki, menjadikan OROD teka-teki 3,7-24 kali lebih cepat daripada teka-teki di atas. Selain itu, dengan menyelesaikan teka-teki yang mudah dan kos efektif dalam teki OROD, pengguna yang sah tidak mengalami kekurangan sumber semasa menyelesaikan teka-teki walaupun di bawah serangan DoS (Teka-teki kesukaran tinggi).

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AID	-	Association ID
AP	-	Access Point
ARP	-	Address Resource Protocol
BSA	-	Basic Service Area
BSS	-	Basic Service Set
CPP	-	Client Puzzle Protocol
CPU	-	Circuit Processing Unit
CSMA/CA	-	Carrier Sense Multiple Access with Collision Avoidance
DLS	-	Direct Link Setup
DNA	-	Deoxyribonucleic acid
DoS Attack	-	Denial of Service Attack
DSS	-	Distribution System Service
ESS	-	Extended Service Set
FH	-	frequency-hopping
GAN	-	Global Area Network
HDP	-	Hide difficulty Puzzle
HDX	-	Half Duplex
IBSS	-	Independent Basic Service Set
IEEE	-	Institute Electrical and Electronics Engineer
IRS	-	Internal Revenue Service
ISM	-	Industrial, Scientific, Medical

ITU-R	-	International Telecommunication Union-Radio communication sector
K/M/Gbps	-	Kilo/Mega/Giga bit per second
LAN	-	Local Area Network
LLC	-	Logical Link Control
MAC	-	Media Access Control
MAN	-	Metropolitan Area Network
MANET	-	Mobile Ad-hoc Network
MD5	-	Message Digest
MSDU	-	MAC Service Data Unit
NIC	-	Network Interface Card
NS2	-	Network Simulator version 2
NST	-	Neighborhood Signal Threshold
OFDM	-	orthogonal frequency division multiplexing
OSI	-	Open System Interconnection
OTCL	-	Object-Oriented Tool Command Language
PAN	-	Personal Area Network
PC	-	Personal Computer
PCS	-	Personal Communications Service
PDA	-	Personal Digital Assistant
PHY	-	Physical Layer Specification
POW	-	proof-of-work system
PSK	-	Pre-Shared Key
QoS	-	Quality of Service
RF	-	Radio Frequency
RSNA	-	Robust Security Network Association
SAE	-	Simultaneous Authentication of Equals
SDR	-	software-defined radio

SS	-	Station Service
SSID	-	Service Set Identifier
STA	-	Wireless-capable Station
TCP/IP	-	Transmission Control Protocol/Internet Protocol
UAV	-	autonomous unmanned aerial vehicle
USB	-	Universal Serial Bus
VANET	-	Vehicular Ad-hoc Network
WAN	-	Wide Area Network
WiMAX	-	Worldwide Interoperability for Microwave Access
WLAN	-	Wireless LAN

CHAPTER 1

INTRODUCTION

1.1 802.11 based Network Authentication

IEEE standard 802.11 defines two classes of security algorithms for 802.11 based networks (IEEE LAN/MAN Standards Committee, 2012):

i. Robust security network association or RSNA algorithm

ii. Pre-RSNA algorithm

This standard defines a number of authentication algorithms under both security classes. Open system and shared key authentication algorithms are classified under the pre-RSNA algorithm class, while the RSNA security class introduces 802.1x and SAE (simultaneous authentication of equals) as its authentication algorithms.

It should be stressed that an open system authentication is a null authentication algorithm. In other words, any STA requesting open system authentication may be authenticated if the recipient STA (e.g. AP) operates in open system authentication mode. Open System authentication is the default authentication algorithm for pre-RSNA equipment.

1.2 Wireless Threats

Due to the broadcast nature of wireless access, however, the future of WLAN, as they get more popular, presents challenges (Tupakul et al., 2011; Gherghina and Petrică, 2013) that can only be met by a reliable and secure wireless communication system (Arockiam et al., 2012).

In order to simplify the attachment of STAs to a wireless network, the connection procedure in wireless networks has been designed without providing an authentication mechanism on MAC frame header fields (Soryal and Saadawi, 2014) particularly in open authentication mode. This security hole makes forging the source address of an MAC frame so easy that identifying the source of traffic is virtually impossible. The following critical evaluations have been made:

i. While a number of security enhancements to the standard 802.11 have already been proposed and implemented to protect WLANs, a key challenge for defense is how to discriminate legitimate requests for service from malicious access attempts.

ii. In the public area, there is no mechanism to check the authorization of a source wishing to gain access to a service. Thus, to deliver MAC frames to their destination, only the AP - at the heart of the network - can decide whether or not these requests are accepted and served.

iii. The pervasiveness of wireless communication demands sophisticated resource sharing mechanisms - which unfortunately become security loopholes in the whole system.

iv. Sending bogus connection requests is much cheaper than validating those requests. When the authentication server is not protecting limited-resource AP against false requests (whose aim is to exhaust available resources), the solution becomes more challenging.

Even though a series of security extensions to the standard 802.11 have already been proposed and implemented to protect WLANs, most of them are primarily effective against attacks seeking to create unauthorized APs, or to breach confidentiality. As we depend ever more on wireless access, the issue of availability must be also considered, thus becoming another important security requirement (Bicakci and Tavli, 2009; Singh and Sharma, 2015).

As in all information technologies, the three core security objectives for wireless networks are confidentiality, integrity, and availability. The first two are easier to resolve than the third. The confidentiality objective is mostly encountered through passive attacks, which are carried out by eavesdropping. Confidentiality can be solved by data encryption. Integrity is threatened by active attacks, while the availability is usually placed in the arena of active attacks (Jing and Wen, 2011).

The necessary availability of wireless networks means that it is vulnerable to denial of service (DoS) attacks (Eian and Mjølsnes, 2011). A DoS attack intends to deny legitimate users access to shared services or resources (Rangasamy et al., 2011). Because wireless networks rely on broadcasting signals, launching DoS attacks remains straightforward. Furthermore, there are numerous DoS vulnerabilities to the standard 802.11 – as demonstrated through experiments noted in the literature.

Note that the effort required by an attacker is relatively limited, while the wireless networks quickly exhausts its resources by allocating them to the unfinished access attempts (Malik and Singh, 2015). Moreover, not only do DoS attacks on wireless systems cripple the communication infrastructure of an organization, they can also be the first phase of more sophisticated attacks (Thapa, 2012). After making a wireless network disappear, a forged system belonging to the attacker can pose as the main system and launch a ‘man-in-the-middle attack’. An attacker mounting a DoS attack on a wireless network used in safety critical applications could cause injury or death, as well as significant material damage.

Guarding against DoS attacks should be a critical component of a security system in the current modern day era (Jerschow and Mauve, 2013). Threats like virus, worm, and malware are old school when compared to DoS attacks because DoS attacks in wireless data networks have a potential to undermine the advantages that come with wireless networks. A WLAN AP, in general, has limited capacity and limited resources like processing power and memory. Hence, an AP can easily fall prey to DoS attacks as its queue can be easily choked and flooded by attack packets (Sharma and Barwal, 2014). The aftermath of DoS attacks range from crippling the network performance to completely bringing it down. So for an organization that has critical operations like point of sales, security cameras over wireless network, surveillance systems and so on, any hiccups in the network can cause severe impact on their business (Hangargi, 2015; Ragupathy and Sharma, 2014). Easy availability of DoS attack tools and mechanisms deteriorates the situation (Singh and Sharma, 2015). For traditional wired networks DoS have been extensively studied but there has been a lack of research study to prevent such attacks on wireless data networks (Singh and Sharma, 2014).

Similarly with wired networks, DoS attacks are very commonplace in wireless networks (Mendyk-Krajewska et al., 2012; Jing and Wen, 2011) and no security mechanisms or standards to date can resist them (Fragkiadakis et al., 2014; Sharma and Barwal, 2014; Singh and Sharma, 2015). In order to demonstrate the potential severity of the problem, an overview will be conducted of the literature pertaining to DoS attacks on 802.11 standard wireless networks.

It is well-known that in the case of wireless LANs, Wi-Fi sniffer tools make it an easy task for attackers to learn authorized MAC addresses. Other available tools help him to change his MAC address accordingly. Thus authenticating STAs via their MAC is not a secure process.

Moreover, the association protocol, designed as a stateful procedure, is susceptible to a depletion attack on the AP's resources. The idea which underlies this is to transmit a flurry of connection requests (probe requests, authentication requests, and association requests (Sharma and Barwal, 2014)) identified by MAC addresses of spoofed sources – thus forcing a heavy workload onto an AP.

Among WLAN security protocols, WEP and WPA have no consideration for DoS attacks. IEEE 802.11i does not give enough priority to AP security because of computational limitations and for accommodating a large number of existing authentication methods (Gherghina and Petrică, 2014). During initial entity authentication, the STA is authenticated to authentication server (AS) only, but not to the AP. Because of this, attacks like DoS pose a threat and deprive services to legitimate users (Singh and Sharma, 2015).

MAC layer DoS attacks are perpetrated by spoofing messages exchanged between a client and Access Point. There are vulnerabilities in the protocols at the MAC layer (Sharma and Barwal, 2014). Although protection for data frames is addressed through encryption, there is lack of protection methodologies implemented for control and management frames (Arockiam et al., 2012). 802.11 management frames like authentication/association and deauthentication/disassociation remained unprotected and unauthenticated; that is, they are neither authenticated nor encrypted. Also the first message of the four-way handshake proposed by standard 802.11i is not protected; it can be utilized in DoS attacks for blocking the protocol (Singh and Sharma, 2013). This means that these unauthenticated STA frames can be used to cause a DoS attack. In fact, there is no cryptographic mechanism to determine if a frame is sent by a genuine client or AP (Tupakul et al., 2011). IEEE 802.11w (2009) is developed as a solution against DoS conducted using management frames, but it is not useful against connection request flooding DoS attacks (Ahmad and Tadakamadla, 2011; Eian and Mjolsnes, 2012). Thus, no security protocol protects effectively against connection request flooding DoS attacks while various control frames and management frames are subject to manipulation by an intruder making it feasible for him to carry out connection request flooding DoS attacks.

At the 802.11 layer, shared-key authentication by WEP (wired equivalent privacy) is flawed and rarely used. The other alternative is the open system authentication (null authentication), which relies on higher-level authentication such as 802.1x or VPN. Open system authentication allows any client to be authenticated and then associated. An attacker, can take advantage of such vulnerability, and exhaust an AP’s resources (most importantly the client association table) by emulating a large

number of wireless STAs with spoofed MAC addresses. Each one of these emulated STAs attempts association and authentication with the target AP, but exits the protocol transaction before completion. When the AP's client association table is filled up with these emulated STAs and their incomplete authentication states, legitimate STAs can no longer be serviced by the attacked AP – the DoS attack has succeeded.

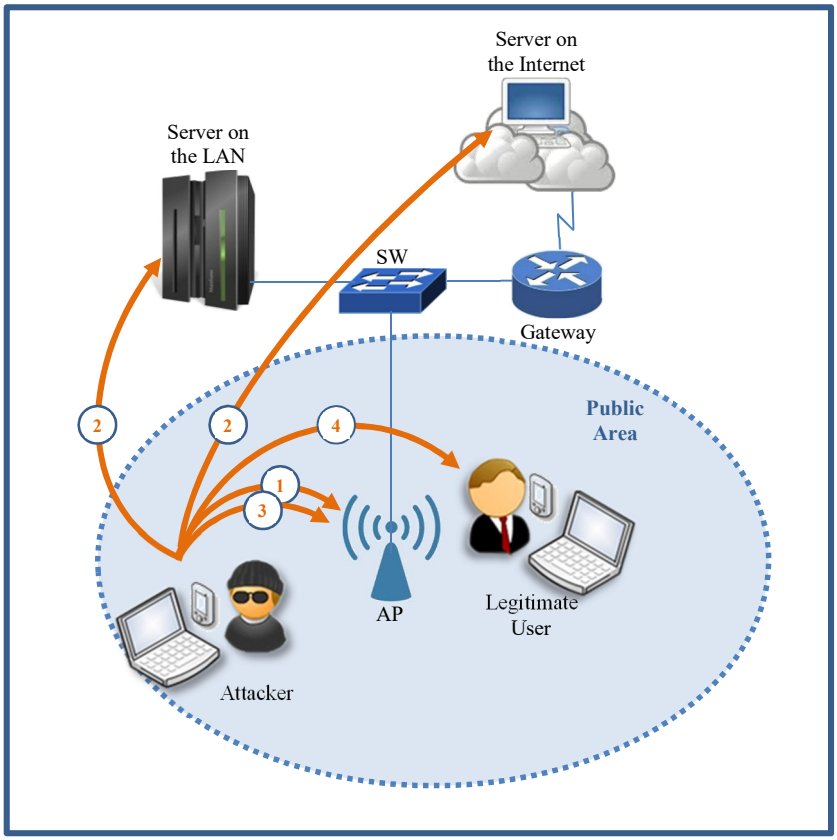

Figure 1.1 Different targets on which to launch DoS attacks in WLAN deployment

Authentication methods such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi-Protected Access 2 (WPA2) are standards used to authenticate users so that only authorized clients can access the network. Being computationally intensive process, however, there is evidence that shows when an AP accepts such authentication methods as the security protocol, it must deal with more of a load, thus can be overloaded with comparatively less traffic (Singh and Sharma, 2014; Singh and Sharma, 2015; Jerschow and Mauve, 2013). Moreover, frequent association requests are responded to by many APs when the requester is in the initial stages. This flaw allows the attacker to fill up the EAP packet identifier's capacity

(since it is only 8-bits long) by association request flooding (in situations where the standard 802.11i has been implemented (Arockiam et al., 2012)).

In wireless networks, various targets are threatened by connection request flooding DoS attacks. As shown in Figure 1.1, the wireless infrastructure, specific service, and mobile devices (STAs) are all vulnerable (Ratnayake et al., 2014).

1.3 Background of the Problem

Even though the impact of distributed denial of service attack (DDoS) is provably high (Sharma and Barwal, 2014), it needs tremendously more investment to launch than DoS attack. Despite of spreading mobile devices, gathering numerous zombies in a certain place at a certain time is not possible without paying a high cost. Consequently, launching connection request flooding DoS attack on WLANs is much more likely than DDoS attack. Hence, almost all researchers have mainly focused on WLAN connection request flooding DoS attack (Jerschow and Mauve, 2013; Soryal and Saadawi, 2014; Ragupathy and Sharma, 2014; Abraham and Vincent, 2012).

Over the past decades, a whole set of countermeasures have been proposed by researchers to mitigate or even eliminate the harmful effects of DoS attacks, particularly the connection request flooding (CRF) DoS attacks on computer networks (Loukas and Öke, 2010; Singh and Sharma, 2015; Arockiam et al., 2012; Soryal and Saadawi, 2014). However, a key challenge for DoS defense schemes is how to discriminate legitimate requests for service from malicious access attempts (Rangasamy et al., 2012). A number of countermeasures both in the physical and MAC layers have been discussed by researchers (Bicakci and Tavli, 2009; Singh and Sharma, 2015). These solutions are: cryptographic protection, security protocol repair, client puzzle, intrusion detection systems (IDS), decreasing the retry limit, identifying with signal strength info, identifying through RF fingerprint.

The cryptographic solution, such as authentication by WEP, is a promising way to treat DoS attacks by restricting connections to only authorized users. However, authentication itself is typically a computationally intensive process. Hence, the authentication protocol may become a valuable target for CRF DoS attacks as the attackers may force the AP to perform expensive operations by sending a large number of bogus connection requests (Hwanga et al., 2010). To eliminate any security hole in current protocols, backward compatibility is vital. However, undertaking efficient reparations are a serious challenge to any new standardization effort, without risking compatibility. IDS/IPS systems such as Cisco adaptive wireless intrusion prevention system (WIPS) detect DoS attacks based on attack signatures and trigger an alarm when bogus MAC addresses are noticed. However, these systems require a human interaction to react to DoS attacks. Moreover, false positive errors are significantly high in IDS/IPS systems (Morais and Cavalli, 2014). On top of this, attackers can easily bypass this system, just like a wired IDS. There are many signs that WIPS are vulnerable – they have become an epicenter of failure. Using RSSI (receiver signal strength indicator) measurements to identify spoofed MAC addresses is a practical and effective defense against CRF DoS attack (Faria and Cheriton, 2006). However, this technique is not applicable when all the STAs are served by a single AP. Moreover, distinguishing two devices in close physical proximity is almost impossible with an RSSI measurement. It is also unable to identify STAs that use multiple antennas.

Undoubtedly, by standardizing cryptographic defenses, the overall resistance of WLANs against DoS attack can be improved. There is a good understanding of the necessity of protecting servers which employ a cryptographic protocol with a client puzzle: several developing Internet standards (Moskowitz et al., 2008) have already adopted this combination. In WLANs, where highly heterogeneous STAs are often hosted, these wire-adopted standards need to stand up to close scrutiny. Nevertheless, it is clear that client puzzle protocols need to be researched, studied and developed further before being incorporated into WLAN standards which rely on cryptographic protection. One of the most active research areas in wireless networking currently is puzzles (Chibiao et al., 2011; Groza and Warinschi, 2013). The goal is to find out whether a truly effective puzzle can be designed for wireless network security - a puzzle that is easy for legitimate STAs to solve with moderate resources, but difficult

enough to hinder attackers who might be undertaking a flooding attack. Some of the issues in existing client puzzles include CPU disparity, inefficiency, overloading legitimate STAs, forgeability, imposing attack on legitimate STAs, and impractical puzzle difficulty system.

1.4 Problem Statement

Despite promising role of client puzzle to combat DoS attack, there are several reasons which make client puzzle impractical in wireless environment.

i. Basically mobile devices are categorized in low end devices where resources are limited. Hence, a computational-intensive process like client puzzle is not a desirable countermeasure.

ii. Due to the broadcast nature of wireless access, exhausting the target resources are much easier than those in wired environment. Hence, applying puzzles designed for wired networks in a WLAN environment may allow an attacker to launch a secondary DoS attack on APs or STAs - where all three phases of the client puzzle protocol (puzzle generation, verification, and solving) become valuable targets for attackers.

iii. Often wireless networks host highly heterogeneous devices. Puzzle difficulty changes have a big impact on wireless network quality so that no wireless vendors accepted client puzzle so far to combat DoS attack.

Even though many puzzles have been proposed in literature, above reasons make those puzzles unsuitable in WLANs. Hence, there is a big need to design a WLAN specific puzzle with following properties to combat CRF DoS attack while saving resources.

The statement of the problem can be put as follows:

i. Designing a secure puzzle which imposes an extra cost only on the attacker is yet to be achieved. Solving puzzles demands more computational and/or memory resources from a legitimate STA. This situation becomes worse when an attacker increases the attack intensity, hindering or stopping legitimate STAs from joining the network (Singh and Sharma, 2015).

ii. Designing an efficient puzzle that eliminates the problem of CPU disparity in WLANs is yet to be achieved. CPU disparity is a serious issue in existing puzzles, particularly for implementation in wireless networks where highly heterogeneous devices are often hosted (Tang and Jeckmans, 2011). Even though some researchers have tried to remove the harmful effect of CPU disparity from their puzzles, they significantly increased the work overload of the AP (Wu et al., 2015).

iii. A secondary CRF DoS attack can be launched on client puzzle protocol if the puzzle is not efficient enough on the AP's side (Abraham and Vincent, 2012; Jerschow and Mauve, 2013). Puzzle setup, generation, and verification must cost as little as possible to achieve the puzzle goal.

iv. A puzzle which maintains the property of uniqueness for requests while delegating the uniqueness of processing to the STA without any security breach is yet to be designed. Puzzle uniqueness is an important property to prevent bogus puzzle solutions (Wu et al., 2015). To achieve this, the AP has to produce a unique puzzle for every request, which leads to a security hole for the network. One solution is to delegate puzzle generation to client. However, that raises another issue called pre-computation attack (Jerschow and Mauve, 2012).

v. Designing a puzzle which makes puzzle solving a worthless target for launching a second DoS attack on benign STAs is yet to be achieved. Forging a connection request bearing a bogus MAC address is much easier in a wireless network, thereby forging puzzles with a high level of difficulty is very commonplace (Jerschow and Mauve, 2013; Jerschow and Mauve, 2012).

vi. A puzzle which is able to modify the current puzzle difficulty instantaneously based on the current attack status is yet to be designed. So far, for all existing puzzles, the modification of puzzle difficulty always suffers from a significant lag behind changes in attack intensity (Koh et al., 2013; Abraham and Vincent, 2012). Consequently, the current puzzle is solved with an old and inefficient difficulty level, while only the new puzzle generated in the next cycle will carry the new difficulty level.

1.4.1 Research Question

The main questions which this research aims to answer are:

i. What features should have a puzzle before it can be used in WLANs?

ii. How does a puzzle exhaust only attacker's resources while legitimate STAs stay safe from any resource exhaustion?

iii. How does a puzzle consume the same resources in all types of devices while the operational environment, like WLANs, hosts a highly heterogeneous devices?

iv. Considering resource constraint, how should a WLAN puzzle be designed that all STAs, but attacker, can easily solve it even under sever attack?

v. Why is the puzzle uniqueness vital and how does it achieved?

vi. How does the attacker make the puzzle difficulty ineffective to prevent DoS attack and how does the proposed puzzle stop him?

1.5 Research Aim

The aim of this study is to examine and analyze a common DoS attack on wireless networks; namely resource depletion or connection request flooding attacks which are run through flooding connection requests including probe, authentication, and association requests on APs. Also, it aims to propose a solution based on a client puzzle protocol, which will protect the AP's resources by forcing an attacker to exhaust their resources, while at the same time, allowing legitimate users to pass the association procedure with only a negligible payment.

1.6 Research Objectives

This research focuses mainly on connection request flooding DoS attacks on WLANs. Hence, the ultimate goal of this project will be to achieve the following objectives:

i. To determine which properties and features a client puzzle protocol (CPP) should have to suit WLANs

ii. To propose a WLAN puzzle to impose resource cost only on attacker while it takes the same time to solve for heterogeneous STAs.

iii. To develop a WLAN puzzle to protect all puzzle phases against a second CRF DoS attack while controlling the puzzle difficulty instantaneously

iv. To analyze the security of WLAN association and authentication procedure based on developed puzzle

v. To evaluate the performance of the proposed client puzzle protocol.

1.7 Significance of the Study

Secure wireless communication is not only important in the military field, but has an equal significance in civilian and commercial fields as well. Wireless applications monitor national landmarks and critical infrastructures, wireless networks administer aviation traffic, and wireless communication allows for remote access of patients' medical records. All of these uses of wireless communication need a robustness[1] and security similar to that of a wireless reconnaissance mission on the battlefield, even if the immediate importance of the latter may be greater (Thapa, 2011; Rangasamy et al., 2012).

Finding and developing an efficient and effective puzzle improves and secures wireless communication, so users can safely connect to wireless networks whenever they need to get access to it (particularly the Internet). Additionally, implementing the proposed puzzle in a real wireless infrastructure will result in a significant increase in the cost of DoS attacks, so that it dissuades an attacker from launching them.

1.8 Research Scope

This research will focus mainly on the 802.11-based networks in infrastructure mode, where they are using open system authentication. It proposes a solution to protect WLANs against connection request flooding DoS attacks. Figure 1.2 demonstrates diagrammatically how this research has been narrowed down to cover the existing gap, the arrows show the path.

[1] A secure system is robust (Stapko, 2010)

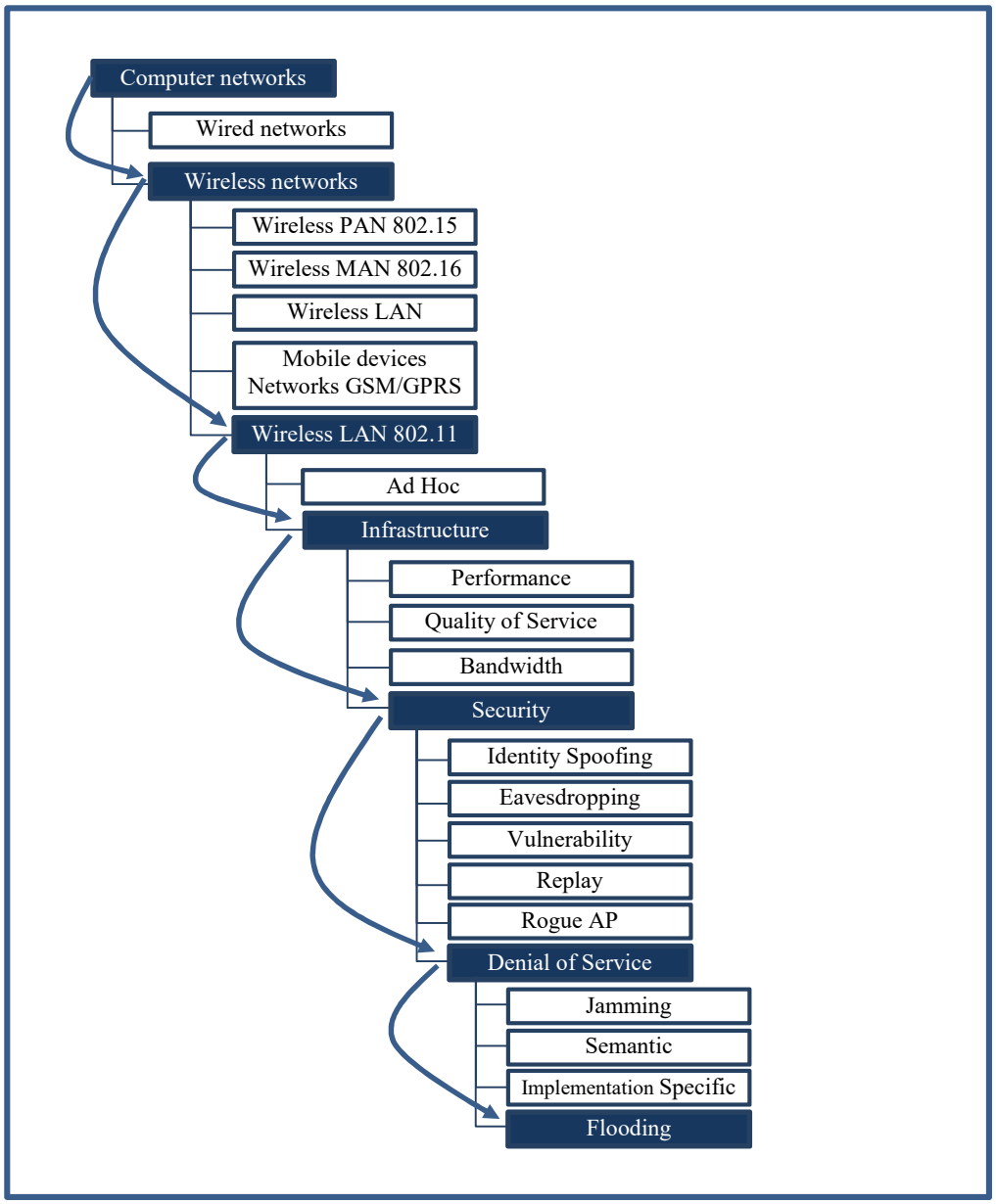

Figure 1.2 The Narrow-down View of the Research Scope

Based on the availability of the software and hardware, this research has been narrow down within the following scopes:

i. To implement and test the proposed solution, two open source device drivers are used, namely RT73_Linux_STA_Drv1.0.4.0 and hostapd-0.5.8, for wireless cards which use rt73 and prism chipset running on Linux operating systems. Other wireless NIC cards can be used as long as the device drivers for LINUX can be obtained.

ii. The above drivers will be modified using C/C++ programming language to add the proposed solution to the wireless association procedure.

iii. The research will not target other DoS attacks on WLANs such as jamming attacks. Hence, it is assumed that the test environment is immune to other types of DoS attacks.

iv. This research will not support ad hoc wireless networks, but it will be recommended as a support for ad hoc wireless networks in future work.

v. This research targets those WLANs that have been deployed in public area so that no MAC filtering scheme is in place.

1.9 Outline of the Thesis

Chapter 1 introduce the WLAN security challenges and highlighted the harmful impact of connection request flooding (CRF) Denial of Service (DoS) attack on WLANs. In addition, the countermeasures were introduced and compelling reasons that why the current puzzle are not suitable to protect WLAN were provided. Ultimately, the chapter presented the objectives that this research is going to achieve. Chapter 2 provides a fact-finding mission on WLANs technologies and security challenges it has been faced. The client puzzles are studied deeply in three classified groups including hash-based puzzles, number theoretic puzzles, and other payment schemes ,while the weaknesses and strengthens of each are detailed. Moreover, the chapter presents the DNA protein synthesizing process in four steps: Transcription, Initiation, Elongation (Translation), and Elongation and Termination.

Chapter 3 provides an academic pathway to achieve the research objectives. The chapter specifies the security and performance analysis models. Chapter 4 mainly focuses on design and implementing the proposed puzzle (OROD puzzle). It also displays the results coming from implementing the real-world test-bed of proposed puzzle. Chapter 5 analyzes the results deeply and a comprehensive performance

comparison between OROD puzzle and current puzzle is presented. In addition, the OROD puzzle is studied from a security perspective where the Chen security model is employed. This research comes to end with Chapter 6 where a comprehensive conclusion is reached. All achieved objectives and contributions of the research are exhibit in this chapter.

REFERENCES

Abadi, M., Burrows, M., Manasse, M., and Wobber, T. (2005, May). Moderately hard, memory-bound functions. *ACM Transactions on Internet Technology (TOIT), 5*(2), 299 - 327.

Abliz, M., and Znati, T. (2009). A Guided Tour Puzzle for Denial of Service Prevention. *2009 Annual Computer Security Applications Conference*. IEEE Computer Society, 279-288.

Abraham, A. M., and Vincent, S. (2012). Defending DoS Attacks Using a Puzzle-Based Approach and Reduction in Traceback Time towards the Attacker . *Communications in Computer and Information Science, Springer, 269*, 425-433.

Alruban, A., and Everitt, E. (2011). Two Novel 802.1x Denial of Service Attacks. *IEEE Computer Society*, 183-190.

Anuradha, and Singhrova, A. (2011). A Host Based Intrusion Detection System for DDoS Attack in WLAN. *International Conference on Computer & Communication Technology (ICCCT)-2011.* IEEE.

Arockiam, L., Vani, B., Sivagowry, S., and Persia, A. (2012). A Solution to Prevent Resource Flooding Attacks in 802.11 WLAN. *Communications in Computer and Information Science, Springer,* 269(1), 607-616.

Assoc., P. C. (2006). *Test TCP (TTCP) Benchmarking Tool for Measuring TCP and UDP Performance*. (Printing Communications Assoc.) Retrieved from PCAUSA Test Lab (PCATTCP "Classic" - PCAUSA's Port Of TTCP To Windows Sockets): http://testlab.pcausa.com/ttcp/classic/pcattcp.htm

Aura, T., Nikander, P., and Leiwo, J. (2001). DOS-resistant Authentication with Client Puzzles. *Sringer Lecture Notes in Computer Science: Security Protocols, 2133/2001*, 170-177.

Back, A. (2002). *Hashcash–a denial of service counter-measure.* Technical report. Retrieved from http://www.hashcash.org/papers/hashcash.pdf

Beard, C., and Stallings, W. (2015). *Wireless Communication Networks and Systems* (1st ed.). Pearson.

Bicakci, K., and Tavli, B. (2009, September). Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. *Computer Standards & Interfaces,* 31(5), 931–941.

Boneh, D., and Naor, M. (2000). Timed Commitments. *Advances in Cryptology ,* 1880(1), 236-254.

Burleigh, S., G. Cerf, V., Crowcroft, J., and Tsaoussidis, V. (2014). Space for Internet and Internet for space. *Ad Hoc Networks, Elsevier, 23*, 80-86.

Cai, J.-Y., Lipton, R., Sedgewick, R., and Yao, A. C.-C. (1993). Towards uncheatable benchmarks. *Structure in Complexity Theory Conference.*

Carl, G., Kesidis, G., Brooks, R. R., and Rai, S. (2006). Denial-of-Service Attack-Detection Techniques . *IEEE Internet Computing, 10*(1), 82- 89.

Chen, L., Morrissey, P., and Smart, N. (2009). Security Notions and Generic Constructions for Client Puzzles. *ASIACRYPT '09 Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, (pp. 505 - 523).

Chen, Y., Kowalik, K., and Davis, M. (2009). MeshScan: Performance of Passive Handoff and Active Handoff. *International Conference on Wireless Communications & Signal Processing, 2009. WCSP 2009.* Nanjing : IEEE, 1-5.

Chen, Y., Trappe, W., and Martin, R. P. (2007). Detecting and Localizing Wireless Spoofing Attacks. *4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, (SECON '07).* San Diego, CA : IEEE, 193-202.

Chibiao, L., Chugui, X., Jinming, Q., and Changjing, L. (2011, December). Experimental and Theoretical Study of Authentication Request Flooding Attack on 802.11 WLAN. *Elsevier, 13*, 6800-6808.

Dahshan, H., and Irvine, J. (2008). Analysis of Key Distribution in Mobile Ad Hoc Networks Based on Message Relaying. *IEEE International Conference on Wireless & Mobile Computing, Networking & Communication* . IEEE Computer Society, 538-542.

D'Ambrosia., J. (2012, Aug). Retrieved from IEEE 802 LAN/MAN Standards Committee: http://www.ieee802.org/

Das, R., and Doshi, S. (2004). *Network Security Final Report Memory Bound Client Puzzles.* Universty Project, John Hopkins University, Baltimore, Maryland.

Dong, Q., Gao, L., and Li, X. (2010). A New Client-Puzzle Based DoS-Resistant Scheme of IEEE 802.11i Wireless Authentication Protocol. *3rd International Conference on Biomedical Engineering and Informatics (BMEI 2010)*. IEEE, 2712-2716.

Dong, Q., Gao, L., and Li, X. (2010). A New Client-Puzzle Based DoS-Resistant Scheme of IEEE 802.11i Wireless Authentication Protocol. *3rd International Conference on Biomedical Engineering and Informatics (BMEI 2010)*. IEEE, 2712-2716.

Dong, Q., Li, L., and Li, X. (2011, December). Quadratic Residue Based Client Puzzle Distributed by Beacon Frame in DoS-Resistant Wireless Access Authentication . *Advances in Information Sciences and Service Sciences (AISS) , 3*(11), 79-86.

Doshi, S., Monrose, F., and Rubin, A. D. (2006). Efficient Memory Bound Puzzles Using Pattern Databases. *Applied Cryptography and Network Security, 3989*, 98–113.

Dwork, C., and Naor, M. (1992). Pricing via processing or combatting junk mail. *Springer-Verlag.A*, 139-147.

Dwork, C., Goldberg, A., and Naor, M. (2003). On Memory-Bound Functions for Fighting Spam . *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference*. Santa Barbara, California, USA. 426-444.

Eian, M. (2012). *Robustness in Wireless Network Access Protocols.* Norwegian University of Science and Technology.

Eian, M., and Mjølsnes, S. F. (2011). The modeling and comparison of wireless network denial of service attacks. *Proceedings of the 3rd ACM SOSP Workshop on Networking, Systems, and Applications on Mobile Handhelds*, (pp. 1-6).

Faria, D. B., and Cheriton, D. R. (2006). Detecting Identity-Based Attacks in Wireless Networks Using Signalprints. *Proceedings of the 5th ACM Workshop on Wireless Security*, 43–52.

Fayssal, S., and Kim, n. U. (2010). Performance Analysis Toolset for Wireless Intrusion Detection Systems. *IEEE International Conference on High Performance Computing and Simulation (HPCS)*, 484-490.

Feng, W.-c., Kaiser, E., Feng, W.-c., and Luu, A. (2005). The Design and Implementation of Network Puzzles. *24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005).* Miami, Florida: IEEE, 2372- 2382 vol. 4.

Ferreri, F., Bernaschi, M., and Valcamonici, L. (2010). Research on the security of IEEE 802.1× authentication mechanism in wireless LAN. *2nd International Conference on Information Science and Engineering (ICISE)*. Hangzhou, China: IEEE, 2350-2353.

Fragkiadakis, A., Askoxylakis, I., and Chatziadam, P. (2014). Denial-of-Service Attacks in Wireless Networks Using Off-the-Shelf Hardware. *Distributed, Ambient, and Pervasive Interactions, Springer,* 8530(1), 427–438.

Gao, Y. (2005). Efficient *trapdoor-based client puzzle system against DoS attacks.* Technical Report.

Gast, M. (2005). *802.11 Wireless Networks The Definitive Guide.* O'Reilly.

Gast, M. (2005). 802*.11 Wireless Networks The Definitive Guide.* Sebastopol, CA: O'Reilly.

Gherghina, C., and Petrică, G. (2013). Wireless LAN Security Issues (I). Types of Attacks. *International Journal of Information Security and Cybercrime, 2*(2), 61-68.

Groza, B., and Warinschi, B. (2013). Cryptographic puzzles and DoS resilience, revisited. *Design, Codes and Cryptography - Springer*.

Gu, Q., Liu, P., Lee, W.-C., and Chu, C.-H. (2009, JULY/SEPTEMBER). KTR: An Efficient Key Management Scheme for Secure Data Access Control in Wireless Broadcast Services. *IEEE Transactions on Dependable and Secure Computing, 6*(3), 188-201.

Hangargi, M. (2015). *Denial of Service Attacks in Wireless Networks.* Retrieved from Paket Storm Security: https://packetstormsecurity.com/files/130092/DoS_attacks_in_wireless_networks.pdf

Hao, W., Qiaoli, W., and Min, W. (2010). Research and implementation of an anti-replay method based on WIA-PA network. *2nd International Conference on Industrial Mechatronics and Automation (ICIMA)*. Wuhan, China: IEEE, 68-71.

Hlavacs, H., Gansterer, W., Schabauer, H., and Zottl, J. (2008). Enhancing ZRTP by using Computational Puzzles. *Journal of Universal Computer Science, 14*(5), 693-716.

Hofheinz, D. U. (2006). Simulatable security and polynomially bounded concurrent composability. *IEEE Symposium on Security and Privacy*. Berkeley/Oakland, CA: IEEE, 1081-6011.

Hwanga, M.-S., Chong, S.-K., and Chen, T.-Y. (2010, January). DoS-resistant ID-based password authentication scheme using smart cards. *Journal of Systems and Software, Elsevier, 83*(1), 163–172.

IEEE LAN/MAN Standards Committee. (2007, June 12). *IEEE Std 802.11.* New York, USA: IEEE Computer Society.

IEEE LAN/MAN Standards Committee. (2012). General description. In *Part 11: Wireless LAN Medium Access Control , IEEE Std 802.11™-2012*. New York, USA: IEEE, 44-91.

IEEE LAN/MAN Standards Committee. (2012). Overview. In *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) S pecifications* (p. 1). NY, USA: IEEE.

IEEE LAN/MAN Standards Committee. (2012). Security. In *Part 11: Wireless LAN Medium Access Control , IEEE Std 802.11-2012*. NY: IEEE, 1170-1191.

Jeckmans, A. (2009). *Practical client puzzle from repeated squaring.* Master Essay, University of Twente, Electrical Engineering, Mathematics and Computer Science.

Jerschow, Y. I., and Mauve, M. (2012). Secure Client Puzzles Based on Random Beacons. *Networking,* 7290(1), 184-197.

Jerschow, Y. I., and Mauve, M. (2013). Modular square root puzzles: Design of non-parallelizable and non-interactive client puzzles. *Elsevier: computers & security,* 35(1), 25-36.

Jerschow, Y., and Mauve, M. (2011). Non-parallelizable and non-interactive client puzzles from modular square roots. *Sixth International Conference on Availability, Reliability and Security, ARES 2011.*

Jerschow, Y., Scheuermann, B., and Mauve, M. (2009). Counter-Flooding: DoS Protection for Public Key Handshakes in LANs. *ICNS '09. Fifth International Conference on Networking and Services.*

Jing, H., and Wen, W. (2011, March). A Solution to a Dos Attack in Wireless Networks. *Energy Procedia, Elsevier, 13*, 3932–3936.

Jules, A., and Brainard, J. (1999). Client Puzzle: A Cryptographic Countermeasure against Connection Depletion Attacks. *Proceedings of the Network and Distributed System Security Symposium*. San Diego: 151-165.

Karame, G. O., and Čapkun, S. (2010). Low-Cost Client Puzzles Based on Modular Exponentiation. *Computer Security - Springer, 6345(1)*, 679-697.

Karumanchi, N., A, D. D., and M, D. S. (2014). *Elements of Computer Networking: An Integrated Approach* (1st ed.). CareerMonk Publications.

Koh, J. Y., Ming, J. T., and Niyato, D. (2013). Rate limiting client puzzle schemes for denial-of-service mitigation. *Wireless Communications and Networking Conference* . IEEE.

Koike, D. (2002, December 4). Client Puzzles as a Defense Against Network Denial of Service. ECS, 1-10.

Kuppusamy, L., Rangasamy, J., Stebila, D., Boyd, C., and González Nieto, J. (2012). Practical Client Puzzles in the Standard Model. *ACM Computer and Communications Security*, 42-43.

Kurose, J. F., and Ross, K. w. (2010). *Computer Networking, A Top-Down Approach* (Fifth Edition ed.). Pearson.

Laishun, Z., Minglei, Z., and Yuanbo, G. (2010). A Client Puzzle Based Defense Mechanism to Resist DoS Attacks in WLAN. *2010 International Forum on Information Technology and Applications - IEEE Computer Society*, 424-427.

Lei, Y., Pierre, S., and Quintero, A. (2006). Client Puzzles Based on Quasi Partial Collisions Against DoS Attacks in UMTS. *Vehicular Technology Conference, 2006. VTC-2006 Fall.* 2006 IEEE 64th, (pp. 1-5).

Lenstra, K., A., Lenstra Jr., H. W., and Lovász, L. (1982, December). Factoring polynomials with rational coefficients. *Mathematische Annalen, 261*(4), 515-534.

Li, J.-y., and Yang, Y. (2012). Research on DoS Attacks and Resist Method Based on 4-way Handshake in 802.11i. In *Electrical, Information Engineering and Mechatronics*. Springer, 631-637.

Liu, C., and Yu, J. (2008). Rogue Access Point Based DoS Attacks against 802.11 WLANs. *The Fourth Advanced International Conference on Telecommunications* . IEEE Computer Society, 271-276.

Loukas, G., and Öke, G. (2010). Protection Against Denial of Service Attacks: A Survey. *The Computer Journal (Oxford journal), 53*(7), 1020-1037.

Malik, M., and Singh, Y. (2015). A Review: DoS and DDoS Attacks. *International Journal of Computer Science and Mobile Computing, 4*(6), 260-265.

Mao, W. (2001). Timed-Release Cryptography. *Selected Areas in Cryptography, 2259*, 342-357.

Martinovic, I., Zdarsky, F. A., Wilhelm, M., Wegmann, C., and Schmitt, J. B. (2008). Wireless Client Puzzles in IEEE 802.11 Networks:Security by Wireless. *WiSec '08 Proceedings of the first ACM conference on Wireless network security*, (pp. 36-45).

Mendyk-Krajewska, T., Mazur, Z., and Mazur, H. (2012). Threats to Wireless Technologies and Mobile Devices and Company Network Safety. *Internet - Technical Developments and Applications, Springer, 118*, 209-225.

Merkle, R. C. (1978). Secure communications over insecure channels. *Communications of the ACM, 21*(4), 294 - 299 .

Moorthy, M., and Sathiyabama, S. (2012). Effective Authentication Technique for Distributed Denial of Service Attacks in Wireless Local Area Networks. *Journal of Computer Science, 8*(6), 828-834.

Morais, A., and Cavalli, A. (2014). A Distributed and Collaborative Intrusion Detection Architecture for Wireless Mesh Networks. *Mobile Networks and Applications, 19*(1), 101-120.

Moskowitz, R., Nikander, P., Jokela, P., and Henderson, T. (2008). *RFC 5201 — Host Identity Protocol (HIP).* Network Working Group. The Internet Engineering Task Force (IETF). Retrieved from http://www.ietf.org/rfc/rfc5201.txt

Naqvi, A. (2013). Utilising Fuzzy Logic to Improve Wi-Fi Security. *11th International Conference on ICT and Knowledge Engineering (ICT&KE)*. Bangkok : IEEE, 1- 5.

Narasimhan, H., Varadarajan, V., and Rangan, C. P. (2010). Game Theoretic Resistance to Denial of Service Attacks Using Hidden Difficulty Puzzles. *ISPEC'10 Proceedings of the 6th international conference on Information Security Practice and Experience*, (pp. 359-376).

Newman, M. (2010). *Networks: An Introduction* (First ed.). USA: Oxford University Press.

Odom, W. (2008). *CCENT/CCNA ICND1.* Indiana: Cisco Press.

Orebaugh, A., Ramirez, G., and Burke, J. B. (2006). *Wireshark & Ethereal Network Protocol Analyzer Toolkit* (Fisrt ed.). Elsevior.

Perahia, E., and Stacey, R. (2013). *Next Generation Wireless LANs: 802.11n and 802.11ac* (2nd ed.). Cambridge University Press.

Ragupathy, R., and Sharma, R. (2014). Detecting Denial of Service Attacks by Analysing Network Traffic in Wireless Networks. *International Journal of Grid Distribution Computing, 7*(3), 103-112.

Rangasamy, J., Stebila, D., Boyd, C., and Nieto, J. (2011, March). An Integrated Approach to Cryptographic Mitigation of Denial-of-Service Attacks. *ASIACCS '11 Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, 114-123.

Rangasamy, J., Stebila, D., Kuppusamy, L., Boyd, C., and Nieto, J. G. (2012). Efficient Modular Exponentiation-Based Puzzles for Denial-of-Service Protection. *Information Security and Cryptology, Springer, 7259*, 319-331.

Ratnayake, D. N., Kazemian, H. B., and Yusuf, S. A. (2014). Identification of probe request attacks in WLANs. *Neural Computing & Applications, Springer, 25*, 1-14.

Rehman, S. U., Ullah, S., and Ali, S. (2010). On Enhancing the WEP Security Against Brute-force and Compromised Keys. *InternationalConference on Computer Information Systems and IndustrialManagement Applications (CISIM)*. IEEE, 250-254.

Rivest, R. L., Shamir, A., and Wagner, D. A. (1996, March 10). *Time-lock Puzzles and Timed-release Crypto.* Massachusetts Institute of Technology. Cambridge, USA: MIT/LCS/TR-684, MIT Laboratory for Computer Science.

Rosenthal, D. S. (2003, Nov). On The Cost Distribution of a Memory Bound Function. *Computing Research Repository (CoRR)*, 1-7.

Sandberg, B. (2015). *Networking The Complete Reference, Third Edition* (3rd ed.). McGrow-Hill Education.

Schaller, P., Čapkun, S., and Basin, D. (2007). BAP: Broadcast Authentication Using Cryptographic Puzzles. *Applied Cryptography and Network Security, 4521*, 401-419.

Sharma, N., and Barwal, P. N. (2014). Study of DoS Attacks on IEEE 802.11 WLAN and its Prevention/Detection Techniques. *International Journal of Engineering Science and Innovative Technology, 3*(3), 245-252.

Shi, T.-j., and Ma, J.-f. (2006). Design and analysis of a wireless authentication protocol against DoS attacks based on Hash function. *Aerospace Electronics Information Engineering and Control*, (pp. 122-126).

Shoup, V. (2004). *Sequence of Games: A Tool for Taming Complexity in Security Proofs.* IACR Cryptology ePrint Archive, Report 2004/332. Retrieved from http://eprint.iacr.org/.: http://eprint.iacr.org/

Singh, R., and Sharma, T. P. (2014). A Key Hiding Communication Scheme for Enhancing the Wireless LAN Security. *Wireless Personal Communications, 77*(2), 1145-1165.

Singh, R., and Sharma, T. P. (2015). On the IEEE 802.11i security: a denial-of-service perspective. *Security and Communication Networks, Wiley, 8*(7), 1378–1407.

Smith, C., and Collins, D. (2014). *Wireless Networks* (3rd ed.). McGrow-Hill Education.

Smith, C., and Collins, D. (2014). *Wireless Networks* (3rd ed.). Mc Graw Hill Education.

Soryal, J., and Saadawi, T. (2014). IEEE 802.11 DoS attack detection and mitigation utilizing Cross Layer Design. *Ad Hoc Networks, Elsevier, 14*, 71-83.

Stapko, T. (2010). *EETimes design*. Retrieved October 10, 2012, from http://www.eetimes.com/design/embedded-internet-design/4019862/Practical-Embedded-Security--Part-3-Wireless-technologies?pageNumber=1

Stebila, D., Kuppusamy, L., Rangasamy, J., Boyd, C., and Gonzalez Nieto, J. (2011). Stronger Difficulty Notions for Client Puzzles and Denial-of-Service-Resistant Protocols. *Topics in Cryptology – CT-RSA 2011, springer, 6558*, 284-301.

Tanenbaum, A. S., and J. Wetherall, D. (2010). *Computer Network* (Fifth Edition ed.). Prentice Hall.

Tang, Q., and Jeckmans, A. (2010). *On Non-Parallelizable Deterministic Client Puzzle Scheme with Batch Verification Modes.* University of Twente, Centre for Telematics and Information Technology, Netherland (Enschede). Retrieved from http://doc.utwente.nl/69557/

Tang, Q., and Jeckmans, A. (2010). *On Non-Parallelizable Deterministic Client Puzzle Scheme with Batch Verification Modes.* University of Twente, Centre for Telematics and Information Technology, Netherland (Enschede). Retrieved from http://doc.utwente.nl/69557/

Tang, Q., and Jeckmans, A. (2011). Towards a security model for computational puzzle schemes. *International Journal of Computer Mathematics, Taylor & Francis, 88*(11), 2246–2257.

Thapa, B. (2011). *Robust Wireless Communication in Adversarial Settings.* PhD Thesis, Northeastern University, Boston, Massachusetts.

Thapa, B. (2012). *Robust Wireless Communication in Adversarial Settings.* Northeastern University. ProQuest. Retrieved from Lyrtech RD: http://lyrtechrd.com/en/products/view/+tunable-rf-modules

Tritilanunt, S., Boyd, C., Foo, E., and Nieto, J. M. (2007). Toward Non-parallelizable Client Puzzles. *Cryptology and Network Security, 4856*, 247-264.

Tupakul, U., Varadharajan, V., and Vuppala, S. K. (2011). Counteracting DDoS Attacks in WLAN. *Proceedings of the 4th international conference on Security of information and networks* , (pp. 119-126).

Von Ahn, L., Blum, M., Hopper, N. J., and Langford, J. (2003). CAPTCHA: Using Hard AI Problems for Security. *Advances in Cryptology, 2656*, 294-311.

Walfish, M., Vutukuru, M., Balakrishnan, H., and Karger, D. (2006). DDoS defense by offense. *SIGCOMM '06 Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications.* NY.

Wan, M., Shang, W., Zhao, J., and Zhang, S. (2014). C2Puzzle: A Novel Computational Client Puzzle for Network Security. *Advanced Materials Research, 846-847*, 1615-1619.

Wang, L., Srinivasan, B., and Bhattacharjee, N. (2011, March). Security Analysis and Improvements on WLANs. *Journal of Networks, 6*(3), 470-481.

Wang, X., and Reiter, M. K. (2008). A multi-layer framework for puzzle-based denial-of-service defense. *International Journal of Information Security, 7*(4), 243-263.

Waters, B., Juels, A., Halderman, J. A., and W. Felten, E. (2004). New client puzzle outsourcing techniques for DoS resistance. *CCS '04 Proceedings of the 11th ACM conference on Computer and communications security* , (pp. 246 - 256). Washington D.C, USA.

WiFi. (2015). Retrieved 2015, from http://www.wi-fi.org/who-we-are

Wu, Y., Zhao, Z., Bao, F., and Deng, R. H. (2015). Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks. *IEEE Transactions on Information Forensics* and Security, 10(1), 168-177.

Ying, X., and Yu, C. (2010). Research on Key Authentication Mechanisms of Wireless Local Area Network. *2nd International Workshop on Intelligent Systems and Applications (ISA)*. Wuhan: IEEE, 1 - 4.

Zeynep Gurkas, G., Zaim, A. H., and Aydin, M. A. (2006). Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks. *International Symposium on Computer Networks* (pp. 1 - 5). Istanbul: IEEE.

Zhang, Y., and Sampalli, S. (2010). Client-based Intrusion Prevention System for 802.11 Wireless LANs. *EEE 6th Intemational Conference on Wireless and Mobile Computing. Networking and Communications*. IEEE, 100-107.

Zhao, Y., Vemuri, S., Chen, J., Chen, Y., Zhou, H., and Fu, Z. (. (2009). Exception Triggered DoS Attacks on Wireless Networks. *IEEE/IFIP International Conference on Dependable Systems & Networks, 2009. DSN '09.* Lisbon: IEEE, 13 - 22.