MAC Layer DoS Attacks in IEEE 802.11 Networks

Taimur Farooq, David Llewellyn-Jones, Madjid Merabti
School of Computing and Mathematical Sciences, Liverpool John Moores University, UK
Email: T.Farooq@2007.ljmu.ac.uk, {D.Llewellyn-Jones, M.Merabti}@ljmu.ac.uk

***Abstract*- The wide scale deployment of IEEE 802.11 based wireless networks have led to a number of security challenges. The MAC and Physical layers of IEEE 802.11 wireless networks possess various vulnerabilities to Denial of Service (DoS) attacks. In this work we discuss DoS attacks which exploit the MAC layer vulnerabilities of IEEE 802.11 networks. In recent years, DoS attacks in wireless networks have been getting the attention of researchers and it has been demonstrated that MAC layer related DoS attacks can easily be launched by using off the shelf equipment. In most cases the attacker forges the MAC addresses of wireless devices in order to halt the operation of the wireless network. MAC address spoofing is possible because the IEEE 802.11 standard does not provide per frame source authentication for control and management frames. Even the new WLAN security standard IEEE 802.11i does not solve these problems. Many tools are easily available for attackers to launch such types of attack. In this paper we classify MAC layer DoS attacks into three categories, and we compare the existing countermeasures to such attacks. We also identify the issues with existing countermeasure and provide future research directions.**

I. INTRODUCTION

With the growing use of wireless networking in every size of organization, security has become an ever important issue. Recently, there has been a lot of research about security protocols and key exchange mechanisms in IEEE 802.11 networks [1-3]. However, these networks are still vulnerable to DoS attacks because these attacks commonly happen before security protocols are evoked. Security of the wireless networks can be divided into three categories: confidentiality, integrity and availability. DoS attacks belong to third category, *i.e.* availability. The main purpose of DoS attacks is to stop legitimate client from accessing resources. It can also lead to other serious attacks such as introducing rogue access points. So far very little attention has been given to DoS attacks, and most of the wireless security research has focused on confidentiality and integrity of wireless networks. However, because of widespread deployment of IEEE 802.11 wireless networks in homes and businesses, DoS attacks in wireless networks have become prominent. In spite of this, there is no proper solution proposed for these problems.

The peculiar features of the wireless medium suggest a greater exposure to Denial of Service (DoS) attacks than wired networks [4]. Researchers have focused on different DoS attacks on the Physical and Mac layers of the IEEE 802.11 standards [4, 5]. However, most of this research investigated how DoS attacks can be carried out rather than providing solutions to the problem. Various DoS attacks can be launched against the IEEE 802.11 MAC layer because of its use of unauthenticated Control and Management frames.

In the following section we briefly describe the IEEE 802.11 standard which is relevant to MAC Layer DoS attacks. In Section 3, we classify and briefly describe the MAC layer DoS attacks. In Section 4, we discussed the existing countermeasures to DoS attacks on the MAC layer. In Section 5 we discuss issues related to DoS attacks and further countermeasure. Finally in Section 6, we draw conclusion and suggest future research directions in this area.

II. IEEE 802.11 STANDARD

In this section, we describe the IEEE 802.11 control and management frames which are vulnerable to DoS attacks and processes which use these types of frames.

A. Media Access Control (MAC) of IEEE 802.11

The IEEE 802.11 standard defines the lower two layers of the OSI model for wireless communication. The 802.11 standards defines two modes of communication: ad hoc mode, in which wireless stations communication directly with each other and Infrastructure mode, in which all communication take place through a fixed access point (AP). In this paper we consider Infrastructure mode only. In the 802.11 standard the area orchestrated by the AP is called the Basic Service Set (BSS).

Frame Types

There are three major types of frame used in IEEE 802.11 networks, known as data frames, control frames and management frames. Data frames carry higher-level protocol data in the frame body. Control frames assist in the delivery of data frames by providing area-clearing operations, channel acquisition and carrier-sensing maintenance functions, and MAC-layer reliability functions. Management frames perform supervisory functions; they are used to join and leave the wireless network and move associations from access point to access point [6]. Table 1 provides a list of some important control and management frames.

Certain of the control and management frames listed in Table 1 can be exploited by adversaries to launch DoS attacks against IEEE 802.11 networks.

TABLE 1
MANAGEMENT AND CONTROL FRAMES

Management Frames	Control Frames
Probe Request / Response	Request to Send (RTS)
Authentication / Deauthentication	Clear to Send (CTS)
Association Request / Response	Acknowledgement (ACK)
Reassociation Request / Response	Power Save Poll (PS-Poll)
Disassociation	

ISBN: 978-1-902560-24-3 © 2010 PGNet

Client and AP Association Process

All APs periodically transmit a beacon frame. Clients listen to the beacon frames to identify the APs within range. Alternatively 802.11 clients can transmit probe request frames to find active wireless network within their reach. Before any client can send data on the wireless network it goes through a message exchange process, as depicted in Figure 1. The process starts with the client searching for a specific network by sending a probe request out on multiple channels. All access points that are configured to respond to this type of query respond. Access points with the broadcast SSID feature disabled do not respond. The only difference between probe requests and periodic beacon frames is that beacons contain a Traffic Indication Map (TIM) showing which stations in sleep mode have data frames waiting for them in the AP's buffer. After discovering an existing BSS, authentication request and response frames are exchanged between client and AP. Authentication could be open authentication or more secure authentication using the IEEE 802.11i standard. After the authentication process, association request and response frames are exchanged between client and AP. As a part of this process, the client learns the AP's MAC address and the AP maps a logical port known as an association identifier (AID) to the wireless client. An 802.11 client can be authenticated by multiple APs, however it should be associated with only one AP at a time.

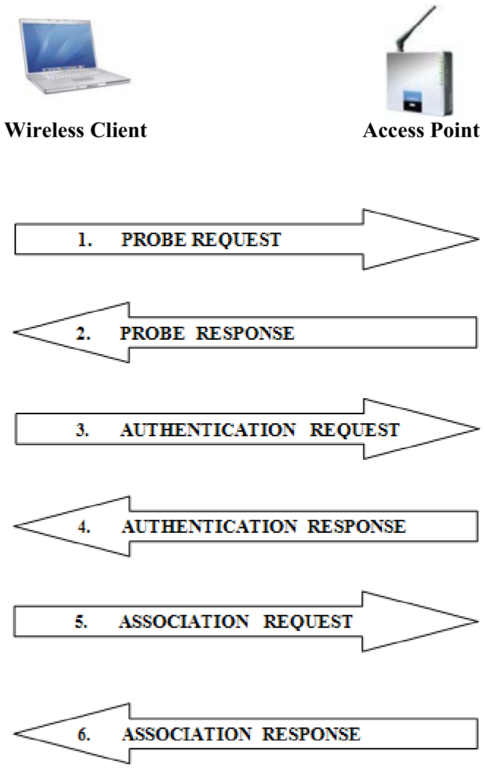

Figure 1: Wireless Client and AP Association.

B. *Distributed Coordination Function (DCF) of IEEE 802.11*

IEEE 802.11 wireless networks are based on the use of a distributed coordination function (DCF). The DCF provides a Carrier Sense Multiple Access/Collision Avoidance mechanism (CSMA/CA) protocol, which regulates every node such that it must check the availability of the channel before transmitting data. A station wishing to transmit will first select a random backoff value bounded by the value of the station specific variable CW (Contention Window) and starts to sense the channel. A CCA (Clear Channel Assessment) module is used to determine the status of the Channel [7].

In a CSMA/CA environment if two stations cannot hear each other they might end up in transmitting simultaneously and causing data collisions. This problem is known as the hidden node problem. To address this problem, CSMA/CA employed a virtual carrier sense mechanism. Under this mechanism, each 802.11 frame carries a duration field indicating the time that the channel is reserved for. This time is then used to program the Network Allocation Vector (NAV) on each node. The NAV can be thought of as a timer indicating the amount of time for which the medium has been reserved. Transmitting nodes set the value of their NAV to the time for which they expect to use the medium; other nodes set up a process to count down the NAV. Only when the NAV on a node reaches zero is it allowed to transmit. The above principle is used by the Request To Send (RTS)/Clear To Send (CTS) handshake to synchronise access to the Channel and prevent the hidden terminal problem [8].

III. MAC Layer DoS Attacks on IEEE 802.11 Networks

DoS attacks on wireless networks attempt to halt access to shared network resources. DoS attacks on the MAC layer can be classified as Masquerading attacks, Resource Depletion attacks or Media Access attacks as shown in Figure 2. The Masquerading attack refers to an attack in which an adversary targets a specific client by spoofing its MAC address or the address of its current access point. The Resource Depletion attack refers to an attack in which an adversary generates high rates of requests with random MAC addresses in order to consume shared resources. Finally Media Access attacks refer to attacks against the Distributed Coordinated Function (DCF) of 802.11 networks. These attacks are also called Jamming attacks. Another way of classifying DoS attacks is based on layers. Our focus in this research is on the bottom two layers: the Physical and MAC layers. In particular we will explore DoS attacks against the MAC layer.

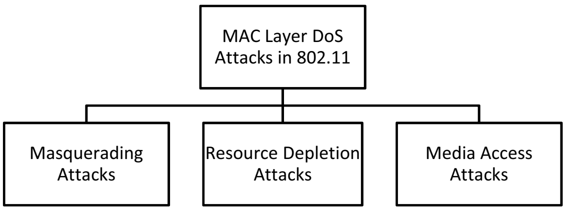

Fig 2: Classification of MAC Layer DoS Attacks in IEEE 802.11 Networks.

A. Masquerading Attacks

In masquerading attacks, an attacker spoofs the MAC address of a specific station or AP. Due to the open nature of the wireless medium, an attacker can easily sniff wireless traffic in order to find the identities of the devices on the network. Those identities can then be easily spoofed by using device driver software. Below is a list of the attacks discussed in the literature until now.

De-authentication Attacks

Every IEEE 802.11 client must authenticate itself to some AP in its range before it actually starts communication. A part of that authentication process is a message that allows clients and APs to explicitly request deauthentication from each other. Unfortunately, this message itself is not authenticated using any keying procedure. This vulnerability can be exploited by the attacker to launch a deauthentication attack against an AP or the client by spoofing this message. In response the AP or the client will exit the authenticated state and will refuse all further packets until authentication is re-established. If the attack is sustained, the stations will no longer be connected to the network. These attacks can be targeted at specific client or all clients in the BSS [5]. Several tools such as Airjack, Void11, KisMAC, *etc.* are easily available to launch this attack.

Disassociation Attack

A very similar vulnerability may be found in the association protocol that follows authentication. The IEEE 802.11 standard allows clients to associate with only one AP at a time. Similarly to the authentication process, the IEEE 802.11 standard allows clients and AP to explicitly request disassociation from each other. As with authentication, association management frames are also unauthenticated. Exploiting this vulnerability is functionally identical to the deauthentication attack. However, it is worth noting here that deauthentication attacks are more severe than disassociation as they can cause stations to lose more time re-associating with the AP [5].

Power Saving attacks

In order to conserve power, the IEEE 802.11 clients can enter a sleep mode during which they are unable to transmit or receive. During this time the AP buffers all inbound data for the sleeping node until the client polls the AP for its data. By spoofing the polling message on behalf of the client, an attacker can cause the access point to discard the client's packets while it is asleep. Along with spoofing polling messages, clients can also be tricked by spoofing the TIM to convince the client that there is no pending data present at the AP. Another vulnerability that arises from a power saving mechanism is due to the unauthenticated management frames used for synchronisation purposes, such as TIM intervals or timestamp broadcasts. By forging these management frames, an attacker can cause a client node to fall out of sync with the AP and fail to wake up at the appropriate times [5].

B. Resource Depletion Attacks

Resource depletion attacks normally target shared resources such as the AP to exhaust its processing and memory power so that it can no longer provide services to other (legitimate) stations. These attacks can be accompanied by more sophisticated attack such as introducing rouge access points to hijack the abandoned stations. Some common resource depletion attacks discussed in the literature are described below.

Probe Request Flood

Stations in IEEE 802.11 wireless networks use Probe Requests to scan the wireless environment for existing wireless networks. APs respond to these requests with information about the wireless network to allow wireless clients to associate with it. An attacker can transmit bursts of such probe requests with different random fake MAC addresses to simulate the presence of large number of scanning stations. This attack can consume all of the memory and processing resources of an AP, preventing it from responding to legitimate clients' requests [4].

Authentication Request Flood

During an authentication flood attack, an attacker transmits authentication request frames with spoofed MAC addresses that attempt to authenticate to the AP. The attacker floods the AP with such frames to exhaust its processing and memory resources. In response to authentication request frames the AP has to allocate memory to keep information about each new station that successfully authenticates. An AP under attack will not be able to allow legitimate clients to connect to the wireless network [4].

Association Request Flood

The AP inserts the data supplied by a station in its Association Request into a table called the association table that the AP maintains in its memory. The IEEE 802.11 standard specifies a maximum value of 2007 concurrent associations to an AP. The actual size of this table varies among different models of APs. When this table overflows, the AP would refuse further clients. Having cracked WEP, an attacker can authenticate several non-existing stations using legitimate-looking but randomly generated MAC addresses. The attacker then sends a flood of spoofed associate requests so that the association table overflows [9]If an access control list is not in place for MAC address filtering then the authentication and association request flood attacks are considerably easier for an attacker to launch.

According to the MAC protocol, an AP will not accept an Association Request sent by a station in unauthenticated and unassociated state. However, it is surprising to see that contrary to the specification, many APs also respond to association requests in their initial states [4].

Media Access Attack

The virtual carrier sense mechanism is employed by the IEEE 802.11 standard to solve the hidden terminal problem as described in Section 2. Control and management frames such as RTS, CTS, ACK *etc.* used by the virtual carrier sense mechanism are unauthenticated frames and they all contain a duration field. An attacker can easily defer the legitimate clients' transmission by continuously asserting a large duration field at an appropriate frequency to ensure the value of the NAV on each node is greater than zero [4, 5, 8].

IV. Countermeasures in the MAC Layer

A. *System Level Defences with Low Overhead*

Bellardo and Savage [5] provide an experimental analysis of 802.11 DoS attacks and potential low overhead implementation changes to mitigate the underlying vulnerabilities. They explored two types of 802.11 vulnerabilities to DoS attacks, identity vulnerabilities and Media Access vulnerabilities. An attacker can spoof the identities of other devices and then request MAC layer services on their behalf in order to launch several distinct types of DoS attacks. The identity based attacks explored by Bellardo and Savage [5], include de-authentication, disassociation and power saving. The Media Access vulnerabilities include the virtual carrier sense mechanism in 802.11 as explained earlier in Section 2.B. They demonstrated these attacks by using commodity hardware. They analyzed the impact of the deauthentication attack and virtual carrier sense attack and proposed preliminary defence mechanisms, as explained below.

Delaying the Effects of Requests

Bellardo and Savage [5] proposed system-level defences with low-overhead to identity based attacks such as De-authentication attacks. In particular, by delaying the effects of de-authentication or disassociation requests (*e.g.* by queuing such requests for 5-10 seconds) an AP has the opportunity to observe subsequent packets from the client. If a data packet arrives after a de-authentication or disassociation request is queued, that request is discarded as a legitimate client would never generate packets in that order. The same approach can be used in reverse to mitigate forged de-authentication packets sent to the client on behalf of the AP. However, this solution opens a new vulnerability for roaming mobile stations, although this is likely not a significant limitation from practical point of view.

Limiting Duration Field Value

Bellardo and Savage [5] also implemented virtual carrier sense attacks by modifying the media access function in the NS2 simulator. As we saw in Section 2.3, virtual carrier sense attacks are based on control and management frames for media access such as ACK, RTS and CTS. The four key frames that contain duration values are ACK, data, RTS, and CTS. These frames can cause a Denial of Services (DoS) by modifying the network allocation vector (NAV). Bellardo and Savage recommend placing a limit on the duration values of the above mentioned control frames acceptable by the nodes. They also stressed that the foolproof solution to such attacks is to extend the explicit authentication to 802.11 control frames.

B. *Signal Print*

Faria and Cheriton [10] introduced signal print techniques to tackle identity based attacks. A signal print is defined by the tuple of signal strength values reported by the access points acting as sensors. They show that signal prints are a better way of identifying devices as attackers, since they have little control of their signal prints as compared to other identity measures such as MAC address. As most of the DoS attacks in 802.11 networks are carried out through spoofing MAC addresses of a particular device or changing unidentified MAC addresses, having a robust identity measure can help to reduce such attacks. In their experiment they showed that signal prints are strongly correlated with physical location of clients, with similar signal prints found mostly in close proximity. This helps in detecting an attacker who is not in close proximity to the victim device.

They also demonstrated that packet bursts transmitted by a stationary device generate similar signalprints with high probability [10]. Consequently, an attacker that mounts a resource depletion attack using random MAC addresses can be easily spotted. While not all signalprints may match each other, the network would still be able to detect that a single transmitter is responsible for a high rate of requests. Signalprints allow a centrally controlled WLAN to reliably single out clients. Instead of identifying them based on MAC addresses or other data they provide, signalprints allow the system to recognize them based on what they look like in terms of signal strength levels.

Faria and Cheriton [10] worked on two different types of DoS attacks. The first was a resource depletion attack in which an attacker sends a large number of authentication requests with many different MAC addresses in order to consume the access point's resources. The second attack was a masquerading attack in which an attacker targets a specific client or an access point by cloning its MAC address. If an attacker is sending a de-authentication request for an already authenticated station then the attack can be identified by comparing two conflicting signal prints coming for the same MAC address.

However, with the scheme being based on signal prints it is difficult to distinguish between devices located physically close to each other as they will produce similar signal prints. Another drawback with the approach is that it will not work if there is only one AP in the network. Moreover, Signal Print can distinguish between stations located at different positions, however it cannot locate the exact location of the station which may help in identifying malicious station.

C. *MAC Address Spoof Detection*

One further method to detect MAC address spoofing is based on the sequence number field, whose value is incremented by one for each non-fragmented frame. An attacker does not have the ability to alter the value of this sequence number as they generally can't control the firmware functionality of their wireless card [11, 12]. Through the analysis of sequence number patterns of the captured wireless traffic, detection systems were shown to be capable of detecting MAC address spoofing to identify deauthentication/disassociation attacks [12]

Sequence number based MAC address spoof detection systems are also valuable until reverse-engineered "attack cards" allowing frames with arbitrary sequence numbers become common place [7, 12].

D. *Wireless Client Puzzle*

Martinovic *et al.* [13] provide a client puzzle solution to DoS Attacks in IEEE 802.11 networks. Any client wanting to join the network will first listen to their radio neighbourhood. The puzzle is conditioned on the signal strength relationship to other stations due to the fact that an attacker can easily change its transmission power, antenna orientation or its physical position. Any alteration influencing a signal's vicinity re-defines the puzzle and imposes the further costs of solving it. The client puzzle technique is only slowing down the DoS attacks and not completely preventing 802.11 networks from such attacks.

E. *Explainability of Collisions*

Toledo *et al.* [14] propose a detection mechanism for intelligent jamming attacks in an IEEE 802.11 DCF network. They presented a nonparametric detection mechanism for the media-access control layer DoS attacks that don't require any modification to existing protocols. Their technique was based on M-truncated sequential Kolmogrov-Smirnov statistics, which monitors the successful transmissions and the collisions of the terminal in the network and determines how explainable the collisions are given such observations. A jamming attack will result in an increase in the number of collisions in the network. To differentiate between normal and abnormal (jamming) operation they observed the variability in the distribution of the collisions.

The scope of this mechanism is limited to only those intelligent jamming attacks which result in collisions. It cannot detect any resource depletion attacks, masquerading attacks or any other identity base attack discussed in Section 3. It only gives the alarm of unexplained collisions and provides no information about the station causing those collisions.

F. *Channel Surfing and Spatial Retreats*

Xu *et al.* [15] present two strategies for the prevention of MAC and Physical layer jamming style DoS attacks in wireless networks (instead of resource depletion attacks). Their first strategy, channel surfing, is a form of spectral evasion that involves legitimate wireless devices changing the channel that they are operating on. The second strategy, spatial retreats, is a form of spatial evasion whereby legitimate mobile devices move away from the locality. They examine both strategies for three classes of networks: two party radio communication, infrastructure network and ad hoc networks.

In order to detect channel access failures in infrastructure networks they propose a thresholding mechanism based on sensing time to discriminate between normal MAC-Layer delays and abnormal delays due to malicious activity. If the sensing time is above the threshold it will declare it as a DoS attack. However, their detection strategy could not distinguish false positive alarms.

Instead of solving the problem they proposed escape strategy which require station under DoS attack to physically move away from that area. Moreover, this method gives no information about the attacker which may help to prevent further attacks.

V. Discussion

We have seen that all three classes of DoS attacks are possible because the networks lack a reliable client identifier before IEEE 802.11i security mechanisms are evoked. Several solutions [11, 12] for MAC spoof detection are not useful because there are more sophisticated tools easily available for attackers to launch these attacks. Physical layer attributes such as signal prints [10] can distinguish between two clients' positions however they cannot identify the exact location of the client and also when two device are physically close to each other they produce similar or the same signal prints. The Client Puzzle scheme [13, 16] can effectively provide attack containment for authentication flooding attacks by reducing the effect of the attack, however an attacker can still find weak positions in the network by using brute force attacks and then flooding the AP from those weak positions. In addition, this scheme does not provide any information about the location of an attacker to the network managers which can be useful to prevent further attacks by the same attacker.

In Table 2, we have summarized the various types of DoS attack and their existing countermeasures.

TABLE 2
TYPES OF DOS ATTACKS AND COUNTERMEASURES

Attack	**Target**	**Existing countermeasures**
Probe Request Attack	AP	Signal Print
Authentication Request Attack	AP	Signal Print, Client Puzzle
Deauthentication Attack	Station and AP	Signal Print, MAC Spoof Detection, Delaying the effects of request
Association Request Flood	AP	Signal Print
Deassociation Attack	Station and AP	Signal Print, MAC Spoof Detection, Delaying the effects of request
Virtual Carrier Sense Attacks	Medium Access	Explainability of Collision, Spatial Retreats
Sleeping Node Attack	Station and AP	Limiting Duration Field Value, Signal Print, MAC Spoof Detection

VI. Conclusion and Future Work

Various DoS attacks on wireless LANs remain possible because these networks lack reliable authentication mechanisms for control and management frames before upper-layer authentication mechanisms are evoked and user credentials are securely established. In this paper we classify the MAC Layer DoS attacks into three broad categories and describe related DoS attacks that have been identified by researchers until now. We also discussed the existing countermeasures to these attacks and identify that there is no complete solution which can prevent MAC Layer DoS attacks. All existing countermeasures provide partial solution to the problem. Some solutions such as Signal Print and Client Puzzle can reduce the effect of a DoS attack but cannot provide user friendly information to network managers that can help them to identify the location of an attacker to prevent future DoS attacks, or at least scare them off the network.

As we have seen, there remains a significant need for authentication mechanisms to cover the control and management frames of the IEEE 802.11 Standard. This would therefore make a sensible focus for future work. Research can also be carried out into ways to identify, efficiently isolate and locate an attacker and make this information available in a user friendly manner for network managers.

REFERENCES

[1] S. Adam, I. John, and D. R. Aviel, "A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP)," *ACM Trans. Inf. Syst. Secur.*, vol. 7(2), pp. 319-332.

[2] R. F. Scott, M. Itsik, and S. Adi, "Weaknesses in the Key Scheduling Algorithm of RC4", Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography, 2001,pp. Pages,

[3] A. Atul, "Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks," *MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking*, pp. 30-44.

[4] M. Bernaschi, F. Ferreri, and L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks," *Wirel. Netw.*, vol. 14(2), pp. 159-169, 2008.

[5] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," *2003 Location,Berkeley, CA, USA,* pp. 15-27, 2003.

[6] M. Gast, *802.11 wireless networks*, 2nd ed. Sebastopol, CA: Farnham: O'Reilly, 2005.

[7] B. Kemal and T. Bulent, "Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks," *Comput. Stand. Interfaces*, vol. 31(5), pp. 931-941.

[8] B. Chen and V. Muthukkumarasamy, "Denial of Service Attacks Against 802.11 DCF," in *Proceedings of the IADIS International Conference: Applied Computing 2006, 2006 Location,School of Information and Communication Technology, Griffith University, Australia.*

[9] Prabhaker Mateti, *The Handbook of Information Security*. Dayton: John Wiley & Sons, Inc, 2005.

[10] B. F. Daniel and R. C. David, "Detecting identity-based attacks in wireless networks using signalprints," in *Proceedings of the 5th ACM workshop on Wireless security, 2006 Location,Los Angeles, California,* pp. 43-52.

[11] F. Guo and T.-c. Chiueh, "Sequence Number-Based MAC address spoof Detection," in *Proceedings of 8th Recent Advances in Intrusion Detection Symposium (RAID 2005), 2005 Location,Seattle, Washington, USA* pp. 309-329.

[12] J.Wright, "Detecting Wireless LAN MAC address spoofing," 21/01/2003.

[13] M. Ivan, A. Z. Frank, W. Matthias, W. Christian, and B. S. Jens, "Wireless client puzzles in IEEE 802.11 networks: security by wireless", Proceedings of the first ACM conference on Wireless network security, Alexandria, VA, USA, 2008,pp. Pages,

[14] A. L. Toledo and W. Xiaodong, "Robust Detection of MAC Layer Denial-of-Service Attacks in CSMA/CA Wireless Networks," *IEEE Transactions on Information Forensics and Security*, vol. 3(3), pp. 347-358.

[15] X. Wenyuan, W. Timothy, T. Wade, and Z. Yanyong, "Channel surfing and spatial retreats: defenses against wireless denial of service", Proceedings of the 3rd ACM workshop on Wireless security, Philadelphia, PA, USA, 2004,pp. Pages,

[16] M. Ivan, A. Z. Frank, and B. S. Jens, "Regional-based authentication against dos attacks in wireless networks", Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks, Chania, Crete Island, Greece, 2007,pp. Pages,