An Anti-DoS Attack Architecture for Wireless IT Infrastructure

K'Ondiwa, N. O.
Business Market R&D
Telkom Orange (K)
Nairobi, Kenya
nkondiwa@orange-tkl.co.ke

Ochola, E.O.
School of Computing
University of South Africa
Pretoria, South Africa
ocholeo@unisa.ac.za

***Abstract*— Widespread deployment of wireless solutions in corporate and government computing infrastructure implies that lots of sensitive information and data is carried over the air. The threats of intrusion and denial of service is real since wireless networks have broadcasted traffic. IEEE 802.11 defines WEP, WPA and WPA2 security protocols as possible countermeasures. The most recent model defined by IEEE, the WPA2 emphasizes data confidentiality, integrity and authentication but pays little attention to availability issues. Management and control frames in WPA2 are still sent in clear making the model vulnerable to DoS attacks. The failure recovery processes require re-authentication and re-association a fact which makes the model easily exploited by various DoS attacks that includes authentication and association frames flooding. In this paper, we propose a drop policy for DoS authentication and Association flooding. We assume deployment of the current IEEE 802.11i provides enough confidentiality, integrity and authentication schemes. We use simulation in OPNET to show that our security model performs better to provide improved security in terms of availability under Denial of service attack.**

***Index Terms*—802.11i, 802.11w security, availability, denial of service, threats, attacks.**

I. INTRODUCTION

The popularity of WLAN in business cycles means that quite sensitive information, data and transactions are broadcasted over the air [1]. WLANs use Radio Frequency (RF) signals to transmit and receive signals. Being broadcasted and the fact that IEEE 802.11 operates in the unlicensed band means any malicious individual equipped with moderate tools [16][10][20] would easily capture traffic, analyze or deny valid users the normal access to Network services. Thus, WLANs comes with certain special vulnerabilities besides the inherited vulnerabilities of the wired infrastructure [21]. IEEE 802.11 networks communicate at the MAC layer mainly by exchanging three classes of frames, namely the data frames, control frames and management frames [22]. A complete and comprehensive security at the MAC layer requires that all frames exchanged are adequately provided with maximum confidentiality, integrity, authenticity and availability. In order to provide security for the IEEE 802.11 networks, IEEE defines two classes of security models, the Pre-Robust Security Networks (Pre-RSN) and Robust Security Networks (RSN) [17]. The Pre-RSN includes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) while RSN model defines a 4-way handshake to confirm that both communicating devices posses a secrete key as part of the authentication process [17][23].

Both RSN and Pre-RSN models provide confidentiality, integrity and authentication of devices and processes, but little or nothing to mitigate the possible availability vulnerabilities. More availability vulnerabilities are created by the fact that most of the attempts to secure the WLANs are aimed at the confidentiality and integrity of the data frames [16][20]. While securing control frames will look illogical, management frames can easily be exploited to achieve effective Denial of Service attacks (DoS) [17].

In this paper we propose a packet drop policy DoS prevention module (DPM) at the WLAN MAC. Our model makes use of a drop policy at the MAC layer for the frames. We use OPNET simulation to evaluate the Impact of our model on the performance of a video conferencing application. We prove by the delay and throughput of the application that our model performs better against some of the DoS attacks such as De-association and association flooding, de-authentication and Authentication flooding attacks. Our result indicates a significant improvement in the Quality of Service (QoS) metrics performance when our drop policy is used and we conclude that this drop policy is an effective model that can be used to provide a comprehensive security for WLANS in corporate networks.

The rest of this paper is organized as follows. We give a brief overview of related works which basically are some of the models that have been proposed to mitigate the possible DoS attacks in WLAN. We then explore the state transition of WLAN network, vulnerabilities and possible threats and attacks. In section VI we propose a security model which we simulate in OPNET in section VII and the results and discussion of the model effectiveness is presented in section VIII. We conclude the paper by proving that our model performs well in improving the QoS performance of a video conferencing application.

II. Related Work

Mina Malekzadeh et al. [14] proposed the use of HMAC-SHA1 algorithm to protect management frames. Her argument is that when management frames are properly authenticated then de-authentication, authentication and disassociation and re-association flooding attacks [19] are effectively mitigated. Chibiao Liu et al [15] propose a DoS anti flooding tool that uses traffic pattern filtering mechanism. Changua [18] proposed an alteration to the IEEE 802.11i protocol execution so that IEEE 802.1x/EAP authentication is done before association. While Mina's proposal requires pre-ownership of keys, which means key handling algorithms must be re-introduced with all its vulnerabilities [10]. The Chibiao and Changua's proposal [15][18] come with a large number of upgrade requirements, besides the overheads associated with such upgrades. In addition, they give a more specific treatment of the threats [10].

III. WLAN State Diagram

Every station (STA) undergoes the state transitions shown in the Fig.1. Initially the STA is unauthenticated and unassociated. The first process for STA to communicate is authentication. The STA must be authenticated by the access point (AP). The authentication process could be simple authentication of challenge and response or it could be a rigorous process that involves identity verification by the authentication server usually remote authentication dial in user service (RADIUS) server. After successful authentication, the AP enters state 2 which requires association to communicate. Association involves checks on the network load and QoS requirements. When successfully associated, the wireless STA enters the state 3 which means the STA can send and receive data. The frames exchanged depend on the state.

In state 1, only beacon frames, authentication frames and de-authentication frames are communicated. In state 2, probe, authentication, de-authentication, association and disassociation frames are exchanged. In state 3, after successful authentication and association all the frames including data frames are exchanged. State 3, represents a state where a legitimate host is communicating with another device usually through application layer protocol.

It can be seen that WLAN networks basically communicate by exchanging three types of frames, the control frames, management frames and data frames. Authentication frames are only relevant to 802.11 and the frames are pre-802.1x and there is no acknowledgement of these frames which makes these frames a security issue. The frames that aren't allowed at each stage are blocked. Roaming becomes an issue since authentication takes a long time. De-authentication and disassociation frames are notification frames; they cannot be rejected by the receiver while Authentication and Association frames are requests that require successful results from the process.

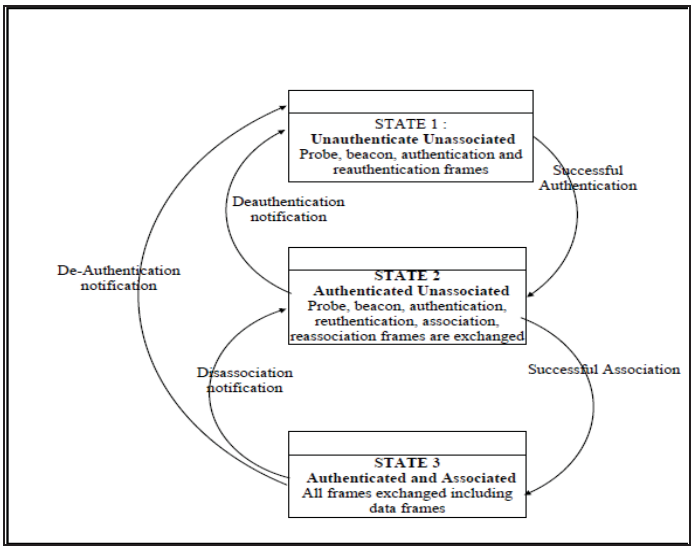

Fig. 1. IEEE 802.11 WLAN State Diagram

IV. Evaluation of WLAN State Transitions and Possible Vulnerabilities

The state transition of a WLAN shows a real possibility of DoS attack. Authentication and Association frames are sent in clear text. De-authentication and Disassociation frames are notification frames and therefore cannot be ignored by the AP and the STA and they are also sent in plain text. An attacker therefore can successfully forge these frames since they are not authenticated. Even more dangerous is the attacker's ability to launch a DoS attack using these frames. When the AP receives an authentication request, the processing takes quite some time. When disassociation frame is received by the AP or STA, the device is forced to go through re-association process. When de-authentication frame is received, the state transitions to unauthenticated state. An attacker therefore by forging and flooding authentication and or association frames can keep a valid AP busy processing the Association and authentication requests. The AP memory is limited thus this request can easily overwhelm the AP processing ability all at the expense of valid traffic. Performance of a network would easily be degraded by this attack. For Quality of service sensitive applications like voice and video conferencing, this degradation in performance may mean total unavailability of the service.

Currently, there is no known solution to this problem. IEEE 802.11W working group is proposing authentication of the management frames using pre-shared keys. The pre-shared key brings along with it the key handling infrastructure. The key handling complexities is what made the TKIP be replaced with WPA2. Authentication of management frames can be complex in that additional encapsulation that comes with authentication of the frames means an additional traffic overhead. Secondly, management frames are sent so frequently which means any additional data in the frame will mean equally higher bandwidth utilization.

V. WLAN DoS Attacks

After a successful MAC spoofing, an attacker can ensure that each fake management frame from his device has a unique fake MAC address. Thus, attacker would simulate a network scenario where many stations send requests to AP. In this scenario the attacker is capable of launching the following denial of service attacks.

A. Authentication Request Flooding

The attacker fakes the MAC address and sends a flood of authentication requests simulating a busy network with many stations [16].The AP has to check the frames for authentication of the station and responds with appropriate response message. Authentication processes and association response consumes computational resources and degrades the performance of the network by denying legitimate station the computational resources.

B. Association request flooding

The attacker pumps a flood of association requests to the AP. Each association request frame has a faked MAC address and unique to fool the AP that they are from different STA. The processing of the frames consumes resources and responses are not acknowledged. Thus, the attack keeps the AP busy at the expense of legitimate host.

C. De-authentication flooding

The attacker fakes the MAC address of a legitimate device. The attacker then sends a faked de-authentication frame to the AP. The AP de-authenticates the STA since de-authentication frames are notification frames that cannot be ignored. The legitimate device is therefore disassociated and will be required to re-authenticate before accessing network resources. The attacker can continuously repeat the process each time disrupting the services to the legitimate network hosts. For applications that are sensitive to throughput and delay this can seriously degrade the performance of the application and the quality of service to the users [17].

D. Disassociation flooding

This works the same way as the disassociation flooding [24]. The attacker forces AP or the STA to disassociate. The disassociation frames just like de-authentication frames are notification frames and therefore cannot be ignored by the device. The attacker can repeatedly carry out the disassociation each time forcing the device to go through association process.

E. Distributed Denial of Service Attacks

An attacker installs MAC spoofing and flooding software [20] in many stations to act as slaves while the attacker remains the master to trigger the stations to act. The attacker then triggers the devices either to all send beacon frames at a higher rate or authentication flooding and or de-authentication flooding. This attack has the capability of completely bringing down the network [3].

VI. Our Proposed Model

We propose an anti denial of service attack packet drop model that punishes the attacker's traffic thus improving the throughput and delay performance of the valid network traffic. The drop policy we propose is a subcomponent of an integrated security architecture, that comprises of CCMP for confidentiality, IEEE 802.1X RADIUS integrated with dynamic VLAN for authentication thus, the evaluation of the DoS performance assumes a perfect solution for confidentiality, integrity and authentication. The DoS attack control module consists of a drop policy that drops more of attack traffic than the normal valid traffic. The principal and assumption of this drop policy is that Normal network traffic like TCP responds to congestion at the Access Point by reducing the sending rate, while attack traffic like authentication flooding will always be at a constant rate. Since attack traffic will be constant regardless of whether there is congestion or not, the valid traffic under DoS attack will always determine the traffic level at the AP. At lower traffic levels therefore, most of the packets are attack traffic. If more packets are dropped at lower traffic levels, we are likely to drop more attack traffic as opposed to using queue length as the basis.

Our drop policy considers the maximum and the minimum packet arrival rate and derives a drop probability in terms of packet arrival rate. The drop function is inversely proportional to the arrival rate and operates within the range between the maximum and minimum. The arrival rate is measured using time sliding window (TSW) rate estimator as shown in Fig. 2.

The drop probability is calculated by Eq. 1 below:

$$P = \max P\left(\frac{\max\_R - R}{\max\_R - \min\_R}\right)^n \quad (1)$$

Using Eq. 1, R is the Current arrival rate, max_R and min_R are the maximum and minimum local arrival rate within the update interval, maxP is maximum drop probability and n is a configurable parameter to control the differentiation of drop probability. maxP and n can be varied. Differentiation of P increases as n increases; we initialized max_R and min_R to 11 and 2 Mbps respectively. For the results in this paper, the values of n and maxP are 20 and 0.5 respectively. Other results for different values of maxP and n are omitted in this paper.

```
For Every arriving packet
 R=((R*win_len)+pkt_size)/(win-len + now - last_arrival)
 last_arrival = now
 win_len: 0.000119
 R: flows estimated sending rate
 pkt_size: the packet size of the arriving packet
```

Fig. 2. Time sliding window rate estimator Algorithm

```
1: Measure R using TSW rate estimator
2:
3:
4: if(R<temp_min) temp_min = R
5:
6: else if(R>temp_max) temp_max=R
7:
8: if(now - last_update > update_interval)
9:     update min_R and max_R with temp_min and temp_max
10:
11: last_update = now
12:
13: if (R<min_R) drop this packet
14:
15: else
16: p=maxP *((max_R - R)/(max_R-min_R))^n
17:
18:
19: drop the packet with probability P
```

Fig. 3. Proposed drop policy algorithm

A. The drop policy Algorithm

We measure the arrival rate (R) using the time sliding window rate estimator. The next step (lines 4-9 of Fig. 3) measures the maximum and minimum rates and update them every update interval (1 sec). Next, the drop probability is calculated. We use maxP and n to control P and since network traffic through any Access Point changes over time even when not under attack, it's important to make these values adaptive. In this paper however, the values of n and maxP are static. We demonstrate the performance of this algorithm through simulation in OPNET as illustrated in section VII.

VII. Simulation

OPNET modeler has a rich functionality for computer networks simulation. With OPNET, it's possible to simulate any layer of the OSI protocol. Since security issues are often cross layer issues and the fact that availability aspects of security can only be measured in terms of performance of the applications, we needed a simulation set up that can model the MAC layer while at the same time giving performance impacts at the application layer. OPNET modeler was the only simulation environment that was capable of providing this kind of setup. Using OPNET modeler, we set up 2 simulation scenarios. Scenario1: without our security model. Scenario2: with our security model. We define the AES (CCMP) as the encryption protocol and define two VLAN at the AP. The general scenario set up is as shown in Fig.4.

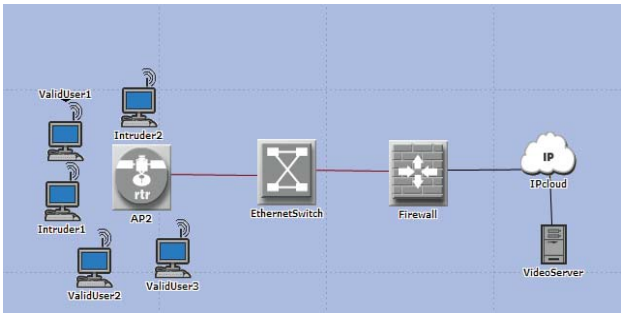

Fig. 4. OPNET Simulation set up

We modified the MAC layer of the AP2 as shown in Fig.2. Other simulation settings for workstations include; BSSID identifier: 1, Access Point Functionality: Disabled, Physical characteristics: Direct sequence, Data rate: 11 Mbps. Channels settings: Transmit power 00.001, Packet reception power: -67 dbM. For the valid users we set up Video conferencing profile with traffic generators. The video conferencing application was chosen since its sensitive to QoS parameters such as throughput and delay and hence the degradation of either throughput or delay performance would actually be a denial of service to the users. For the intruders, we set up traffic generators for authentication and de-authentication at a rate of 250 frames per sec and identified them with BSSID of 1. The simulation run was set to 1hour with collection of global attributes that includes the video traffic throughput and end-to-end delay.

VIII. Simulation Results

The simulation of the two scenarios shows that the continuous flooding of authentication and de-authentication frames degrades the performance of the video conferencing application. The authentication and de-authentication requests keep the AP busy at the expense of the valid frames including the video traffic. Thus valid packets are dropped resulting in the drastic drop in the throughput of the application. When we apply the Anti-DoS regular module, the video traffic packet throughput is drastically improved showing the effectiveness of our module in dealing with the DoS attacks. Figure 5 and Fig. 6 compare the successful attack packets with and without the Anti-DoS architecture deployed. There is a marked reduction of attack traffic when Anti-DoS is implemented. While Fig. 7 shows the effect of the module without attack (collateral effect), Fig. 8 illustrates that the solution improves network resilience and the effect in network throughput is minimized. Another QoS parameter evaluated for the Video traffic was the end to-end-delay. The end-to-end delay here refers to the average time taken for a video packet to move from one of the client nodes to the video server. This time is critical since if the delay is high it would mean higher distortion on the video throughput, which could severely degrade the quality of the video output to unacceptable levels. Fig. 9 indicates that under attack, the average end to end delay is less than in the scenario where we implement our Anti-Dos Attack model. Under attack, the end-to-end delay is high because the received queue of the AP is constantly long due to flooding.

Our model performs better in terms of delay under attack. The performance under normal operation without attack could show better performance but these are the trade off to make for better security. For completeness we show in Fig.8 and Fig. 9 that the overall network throughput is improved when ISM is implemented.

IX. Conclusion

In this paper we analyzed the RSN security model's possible vulnerabilities. Our analysis shows that while RSN Association provides higher confidentiality, integrity and good authentication. Little attention is given to the possible DoS

vulnerabilities. We proposed a DoS regulation improvements and our simulation in OPNET modeler shows a marked improvement on the network performance in terms of throughput and delay when our model is implemented. As part of our future work we intend to use dynamic VLAN to mitigate possible authentication exploitation of RSNA processes in the form of security level roll back attack. With VLAN and anti-Dos regulator, the integrated security model will be complete and robust against nearly all the threats to WLAN.

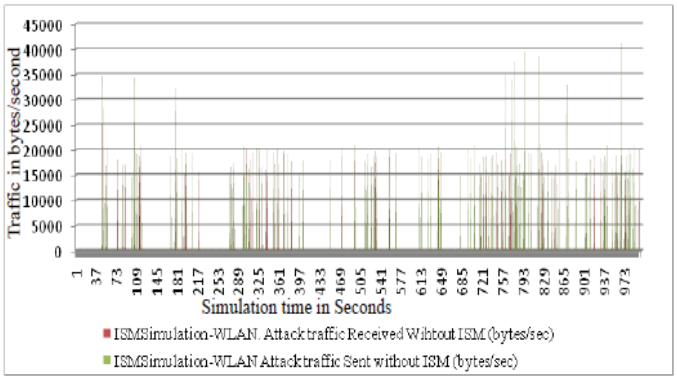

Fig. 5. Successful attack traffic without Anti-DoS

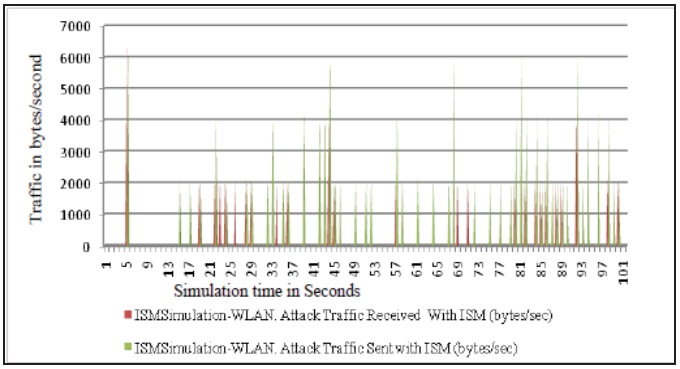

Fig. 6. Successful attack traffic with Ant-DoS

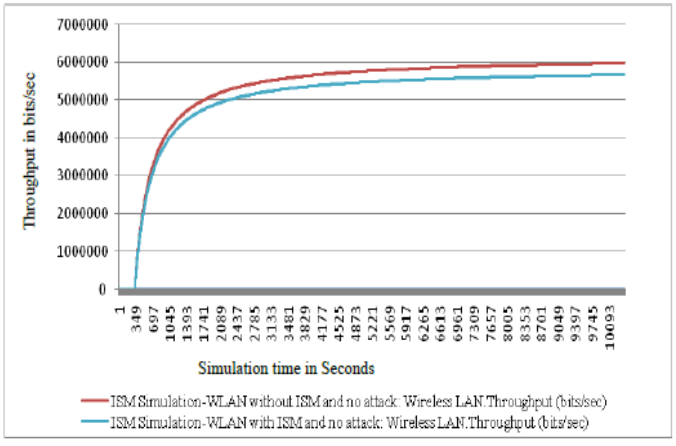

Fig. 7. Comparative overall Network throughput without DoS

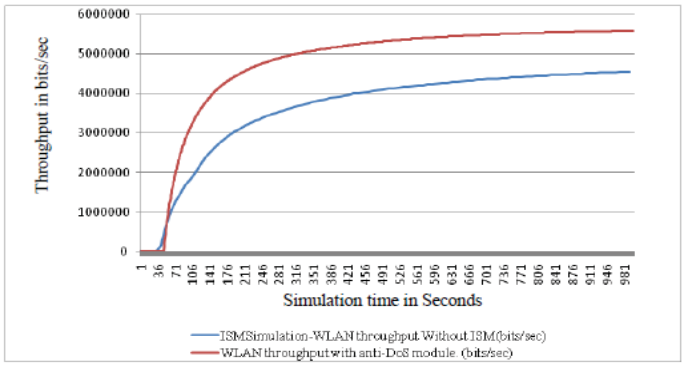

Fig. 8. Overall network throughput under heavy DoS attack

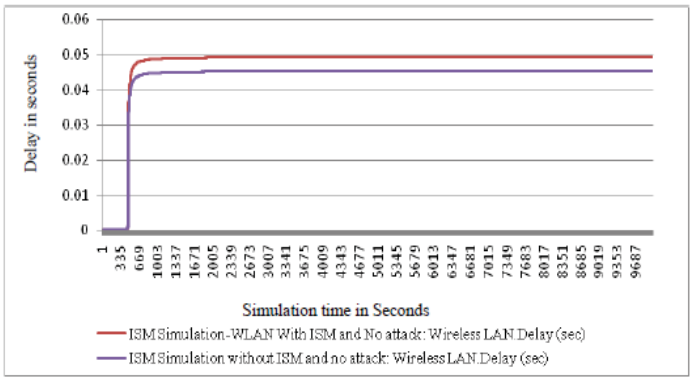

Fig. 9. Comparative End-to-End Network Delay

REFERENCES

[1] T. Kocak, and M. Jogetia, "WEP Post-Processing Algorithm for Robust 802.11 WLAN Implementation," Computer Communication, vol. 31, no. 14, 2008, pp. 3405-3409.

[2] S. Frankel, P. Hoffman, A. Orebaugh, and R. Park, "Guide to SLL VPNs: Recommendations of the National Institute of Standards and Technology," Nist Special Publication 800-113, 2008.

[3] T. Roosta, S. Shieh, and S. Sastry, "Taxonomy of Security Attacks in Sensor Networks and Countermeasures," in The First IEEE International Conference on System Integration and Reliability, 2006.

[4] S. Convery, "Network Authentication, Authorization, and Accounting: Part One," The Internet Protocol Journal, vol. 10, no. 1, 2007.

[5] L. Vokorokos, M. Chovanec, O. Latka, and J. Halasz, "Centralized Network Security Model Using Dynamic VLAN and Client Authentication," Department of Computers and Informatics, Technical University of Kosice, Slovakia, 2006.

[6] N. Mazhar, and M. Farooq, "Vulnerability Analysis and Security Framework (BeeSec) for Nature Inspired MANET Routing Protocols," in Proceedings of the 9th annual conference on Genetic and evolutionary computation, 2007, pp. 102-109.

[7] K. Masica, "Securing WLAN using 802.11i," Lawrence Livermore National Laboratory, 2007.

[8] D-Y. Yoo, J-W. Shin, and J-Y. Choi, "Home-Network Security Model in Ubiquitous Environment," World Academy of Science, Engineering and Technology, vol. 36, 2007, pp. 167-170.

[9] K. Doyle, and I. Pieterse, "Mobile will be under Attack", iTWeb Malware, 2008.

[10] S. Convery, "Network Security Architectures: Expert Guidance on Designing Secure Networks," Cisco Systems, 2004.

[11] K. K. Gupta, B. Nath, and K. Ramamohanarao, "Network Security Framework," IJCSNS International Journal of Computer Science and Network Security, vol.6 no.7, 2006, pp. 151-157.

[12] A. D. Myers, and S. Basagni, "Wireless Media Access Control," in I. Stojmenovic (Ed.): Handbook of Wireless Networks and Mobile Computing, John Wiley & Sons, 2002, pp. 119-144.

[13] D. J. Welch and S. D. Lathrop, "A Survey of 802.11a Wireless Security Threats and Security Mechanisms," United States Military Academy, New York, 2003.

[14] M. Malekzadeh, A. A. A. Ghani, Z. A. Zulkarnain, and Z. Muda, "Security Improvement for Management Frames in IEEE 802.11 Wireless Networks," IJCSNS International Journal of Computer Science and Network Security, vol. 7, no. 6, 2007, pp. 276-284.

[15] C. Liu, and J. Yu, "A Solution to WLAN Authentication and Association DoS Attacks," IAENG International Journal of Computer Science, vol. 34, no. 1, 2007, pp. 7-14.

[16] J. R. Vecca, "Guide to Wireless Network Security," Springer, 2006.

[17] S. Frankel, B. Eydt, L. Owens, and K. Scarfone, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i," NIST Special Publication 800-97, 2007.

[18] C. He, and J. C. Mitchell, "Security Analysis and Improvements for IEEE 802.11i," in Proceedings of the 12th Annual Network and Distributed System Security Symposium, 2005, pp. 90-110.

[19] A. Balinsky, D. Miller, K. Sankar, and S. Sundaralingam, "Cisco Wireless LAN Security," Cisco press, 2004.

[20] N. O. K'Ondiwa, E. Biermann, and G. Noel, "A Denial of Service Attack Prevention Model for WLAN," in 3rd IEEE Broadcom Conference of Telecommunication and Biomedical Applications, Wroclaw Poland, July 2009.

[21] N. O. K'Ondiwa, E. Biermann, and G. Noel, "Integrated Security Architecture for WLAN," in 23rd IEEE Africon Conference on Communication, Nairobi Kenya, 2009.

[22] D. Lee, and D. Won, "A Study on Security Management Service System for Wireless Network Environment," Applied Mathematics & Information Sciences, vol. 6, no. 1, 2012, pp. 209-220.

[23] M. A. Ameen, J. Liu, and K. Kwak, "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications," Journal of Medical Systems, vol. 36, no. 1, 2012, pp. 93-101.

[24] K. Nasr, A. A. E. Kalam, and C. Fraboul, "Generating Representative Attack Test Cases for Evaluating and Testing Wireless Intrusion Detection Systems," International Journal of Network Security & Its Applications, vol. 4, no. 3, 2012, pp. 1-19.