Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DETECTION AND PREVENTION OF DENIAL OF SERVICE ATTACKS (DOS) IN WLANS INFRASTRUCTURE

[1]AABDALLAH ELHIGAZI ABDALLAH, [2] SHUKOR ABD RAZAK, [3] COULIBALY YAHAYA
[1,2,3] Universiti Teknologi Malaysia(UTM), Faculty of Computing
E-mail: [1]abdoo_hegazi78@yahoo.com , [2]coulibaly@utm.my [3]shukorar@utm.my ,

Wireless networks are very common today because of their flexibility, portability and ease of installation. Users working through wireless connections have to be aware of the environments due to the vulnerability of the infrastructure and various types of attacks that can be made by the intruders to compromise valuable and critical data. Denial of Service attack (DOS) is the most significant attack in the wireless 802.11 WLANs. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) security protocols are used to protect wireless network infrastructure against intruders. Despite remarkable advances, both WEP and WPA protocols still suffer from DOS attack because their management and control frame is not encrypted. Integrated Central Manager (ICM) algorithm was proposed to detect and prevent DOS attacks. However, in ICM, time needed to detect DOS attack is too long. The algorithm maintains five tables for observing activities in the network. When a client requests for a connection, all the five tables needs to be processed; this is increases both network overhead and latency. In This paper, we proposed an algorithm called Enhanced Integrated Central Manager (EICM) to enhance DOS detection and prevention time. The algorithm was evaluated by gathering MAC addresses using Wireshark software and MATLAB was used for simulation. The obtained results demonstrate that that the proposed algorithm outperforms its predecessor in terms of DOS detection and prevention time by decreasing network overhead.
Keywords: *WLAN Security, Denial of Service, MAC Spoofing, EICM*

1. INTRODUCTION

Recently, Wireless Local Area Networks (WLANs) have gained increased acceptance as compared to wired networks due to its flexibility, low cost and easy deployment plans. WLANs are generally used by laptop and smart mobile devices users in companies and educational environments for their convenience. However, the weaknesses of wireless access medium makes the infrastructure more vulnerable to attacks[1].
A wireless network enables one or more devices to communicate without using physical connections. The main differences between wireless technologies and wired networks can be summarized as follows: Wireless technologies use radio frequency transmissions for transmitting data, while wired technologies use cables either copper or fiber [2].

WLANs offer permission to move in the cell of a network device while maintaining the connection, which is not available in wired LAN. Roaming capability is also available through linkage of access points. In spite of this flexibility, WLAN is exposed to large number of security threats. The most critical attack is spoof attack which further facilitates many other forms of security threats [3].

The security methods for securing communications in 802.11 wireless networks are based on the following protocols:

- Wired Equivalent Privacy (WEP);
- Wi-Fi Protected Access (WPA);
- Wi-Fi Protected Access (WPA2).

IEEE 802.11 is the adopted standard for WLANs. The standard was approved in 1999 and reasserted in 2003. WLAN uses Wired Equivalent Privacy (WEP) as the security protocol to achieve Confidentiality, Authentication and Integrity services. WEP offers two authentication schemes – open system authentication and shared key authentication. It uses Rivets Cipher 4 (RC4) for confidentiality and Cyclic Redundancy Check 32 (CRC 32) for integrity [4] but the architecture does not provide solutions to the discovered security weaknesses[5].
All three protocols described earlier provide strong key management and authentication access control for wireless LANs. In spite of the fact that WPA2 is the best one of the three protocols in security and controlling wireless LANs, unfortunately, it misses the goal of (DOS) attack. Thus, it is clear that all of the three protocols are unable to protect WLAN

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

from denial of service attacks because of the unprotected management and control frames [6].

Denial of service attacks try to spoof MAC addresses of wireless clients or access points and it is a vital vulnerability of wireless networks[7].

There are many types of Denial of Service attacks such as de- authentication/disassociation, power saving attack, session hijacking [8] [9].

This paper focuses on Extensible Authentication Protocol over LAN (EAPOL) attacker in WLAN 802.11 infrastructures where a solution is proposed to detect and protect WLAN users against DoS attacks.
The rest of this paper is organized as follows. Section 2 discusses main DoS types in WLANs. Section 3 highlights significant related work. In Section 4, we provide the description of the proposed EICM algorithm. Experiment setup and parameters ate elaborated in Section 5. Results analysis is carried out in Section 6. Finally, concluding remarks and future work are reported in Section 7.

2. DENIAL OF SERVCE ATTACKS TYBES

Denial of Service (DOS) attack is a crucial problem in WLANs. There are many types of DOS attacks in WLANs. In this Section, we describe three types of these attacks: De-authentication/Disassociation DOS, power saving DOS and EAPOL Attack.

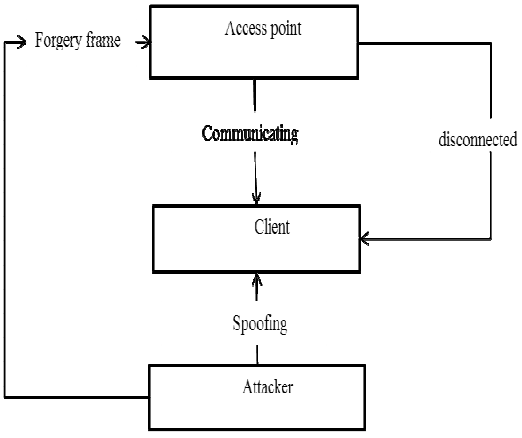

Figure 1: Logical development of DoS attack

2.1 Authentication/Disassociation Dos

The IEEE 802.11 standard provides DE authentication and disassociation frames for the STA or AP to terminate the connection between them. Unfortunately, the DE authentication and disassociation frames themselves do not come with sender authentications. Consequently, an attacker can send a spoofed DE authentication and/or disassociation frame on behalf of the AP to STA or vice versa and eventually stop the data communication between the STA and AP. When a STA receives a spoofed DE authentication frame, it will stop communicating with the AP, scan all available APs and repeat the authentication and association process. By repeating this attack on a STA, the attacker can effectively prevent the STA from transmitting or receiving data indefinitely because repeated re-authentication and re-association disrupt transport-layer protocol operation [10]

2.2 Power Saving Dos

The IEEE 802.11 standard provides a power save mode to conserve a STA's energy. In power save mode, a STA can enter a sleep state during which it is unable to receive or transmit. To enter the power save mode, the STA informs the AP by setting the power management bit within the frame control field of a transmitted frame. Then the AP starts to buffer frames destined to this STA. Periodically the STA wakes up and examines the traffic indication map (TIM)[11] In the power save mode, an attacker can spoof a PS-Poll frame on behalf of a STA while it is asleep. The AP then sends buffered frames even though the spoofed STA cannot receive frames in sleep state. As a result, an attacker can block the victim STA from receiving frames from the AP.

2.3 EAPOL ATTACK

This kind of attacks has four types which described as follows:

2.2.1 Eapol Start Frame Over The Ap

Wireless stations gain access to the network after sending an EAPOL start frame to the AP. Communication between AP and legitimate station starts after AP agrees to the legitimate station request by checking the identity of the legitimate station. While the legitimate station is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

communicating with the AP, an intruder sends a fake EAPOL start frame to the AP by spoofing the legitimate client's MAC address to make the AP busy with the intruder. Hence, the communication between the AP and the legitimate client will be discarded [12].

2.2.2 Eapol Start Frame Over The Client

The intruder sends a forgery EAPOL start frame to the client in the mid of normal transmission by spoofing AP's MAC address.

2.2.3 Eapol Logoff Frame Over Ap

When a legitimate station needs to logoff from WLAN, it sends EAPOL logoff frame to the AP. By using this opportunity, an intruder spoofs the legitimate station MAC address and sends EAPOL logoff. In this case, the AP considers this request from one of the client and responses with logoff message to the legal client and disassociates it from the transmission.

2.2.4 Eapol Logoff Frame Over Client

In this type of attack the attacker sends an EAPOL logoff frame to the targeted legitimate station by spoofing AP's MAC address. The client thinks that the legitimate AP wants to logoff because of heavy traffic and accepts the logoff request.

3- RELATED WORKS

Many studies had introduced detection solutions to DOS attack.
For instance, the study by authors of [13] proposed Intruder Database (IDB) algorithm The simulation results of this technique measures the probability of denied service with respect to the number of attacks and the maximum number of connections that the AP allows. The simulation result shows that the Probability of Denied Service (PDS) is decreased at different attack rates and increases the number of connections that the AP allows after using the IDB. The IDB algorithm cannot detect new intruder which is not yet installed in the database. It can only detect the intruder based on the MAC address which it has. Usually intruders spoof the legitimates MAC address and make the attacks.
Authors of [14] proposed algorithm to enhance the performance of the correlation of two Wireless Intrusion Detection Technique (WIDT) in detection of MAC spoof DOS attacks. The two techniques are Received Signal Strength Detection Technique (RSSDT) and Round Trip Time Detection Technique (RTTDT). The detection results can be interrelated across the (WIDT) sensor this technique also does not provide a complete solution to prevent DoS attacks in wireless infrastructure network.

The authors in [15] proposed a solution to avoid DOS attacks for WLAN using Central Manager (CM). CM is installed in the backend server which controls the Access Point (AP). It is used to detect the attack using three tables and a timer. Apart from detecting DoS attacks, CM dynamically manages Access Points and Clients In the case of Central Manager, the CM itself can be hacked by an attacker. By doing this, whole network transmission may get collapsed.

The researchers of [11] proposed an algorithm to detect spoofing by leveraging the sequence number field in the link-layer header of IEEE 802.11 frames, and demonstrated how it can detect various spoofing without modifying the APs or wireless stations. The false positive rate of the proposed algorithm is zero, and the false negative rate is close to zero. Spoofed frames are detected by using the sequence number technique. But it cannot detect all the spoofed frames, only detect some. Little modification is needed in WLAN interface driver on every AP and station for sequence number extraction and analysis. The disadvantage is applying it to existing AP's and Station's is difficult.

The study in [16] proposed a method against DOS attacks which works as authenticated server by maintaining five tables and a timer to make detection and protection to the network. These maintaining tables make the timer complexity very high.

The study in [17] created new extension module is to make OMNeT++ capable to simulate various types of wireless DOS attacks using forgery control frames. They designed a real 802.11 wireless network test bed to experiment a wireless DOS attacks as same as the simulation model . From the test bed and simulation model, the performance, throughput, end-to-end delay and packet loss ratio are measured No complete solution to prevent DoS attacks by using OMNeT++. It performs quite well. DoS attacks by exploiting unprotected control frames can highly degrade wireless network performance.

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ICM algorithm is proposed in [16] to detect and prevent WLANs infrastructure from EAPLO start & EAPOL logoff frame by maintaining a timer and five tables. These maintaining tables make the detection time for DOS attack too high. It takes long time to check in the database when a client is requesting for a connection. Maintaining duplicate ICMs is a reason of high network overhead [18]

The proposed enhanced algorithm in this paper uses two tables compared to ICM [16] which uses five tables. The aim is to reduce the complexity overhead and reduce the detection time.

4. THE PROPOSED (EICM) ALGORITHM

The proposed EICM algorithm is an enhanced version of ICM proposed in [16]. The aim EIC detect and prevent DOS attacks in WI infrastructure with minimum network overh The algorithm uses two tables to observe network activities of client and access point (AP) instead of five (5) tables as in ICM. The maintenance of duplicate ICM tables increases detection time. Using two tables decreases searching complexity and detection time.

In DOS attack, the attacker sends EAPOL start frame to the AP by spoofing the authenticated client's MAC address. Then EICM checks the MAC address in T1. If the address is found, the request is ignored. Otherwise, checks T2. If the particular MAC address is already in T2, EICM infers that the request is from an attacker and it spoofs the attacker's MAC address and ignores the request and moves the MAC address to T1. Else, EICM grants the connection to the requesting client. Figure 2 depicts EICM operation.

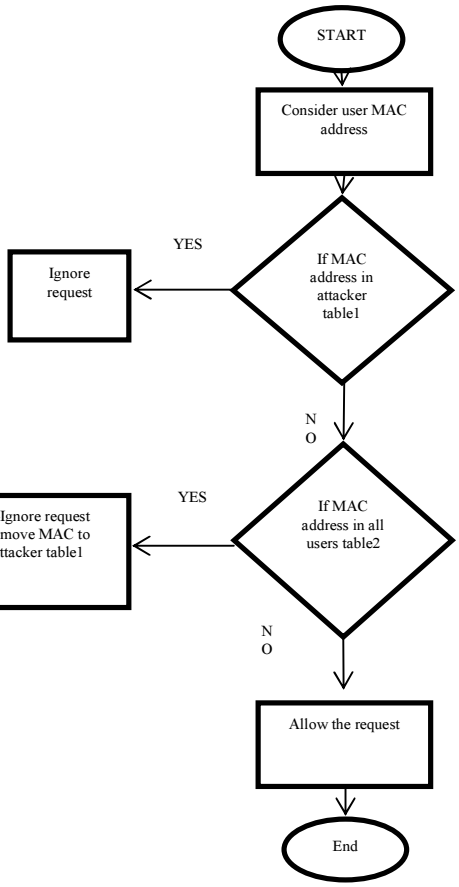

Figure 2: Eicm Operation Flowchart

4.1 Tables Description

As mentioned earlier, EICM deploys two tables to detect and prevent DOS attacks in WLANs. The two tables are denoted as T1 and T2 respectively. T1 contains the MAC addresses of attacker detected by the algorithm, while T2 contains all authenticated
Clients MAC addresses.

The motivations for using two tables instead of five are to reduce complexity and time consumption experienced by ICM [6]. Maintaining five tables in ICM for detection DOS attack does increase time of detection and searching of tables take more time. We have eliminated table three in

Journal of Theoretical and Applied Information Technology
31st January 2015. Vol.71 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ICM algorithm arguing that attackers cannot spoof MAC address in sleep mode [19].

5 EXPERIMENT SETUP AND PARAMETERS

To evaluate the performance of EICM, the MAC addresses of WLAN under test were gathered using Wireshark software and MATLAB was used for simulation.

We implemented both EICM and ICM algorithms in the real time and simulation environments. The solution is validated by measuring the time detection consumption in both algorithms. Evaluation metric is detection time.

We used the paired sample T-test to test the hypothesizes:
Null hypothesis: there is no difference between ICM and EICM detection time against the hypothesis that the EICM detection time is less than ICM detection time. We found the P-value =0.047 which indicates the significance of the result with 95% confidence. Based on this result we concluded that the EICM detection time is less than that of ICM. Thus, EICM is better than ICM in terms of detection time.

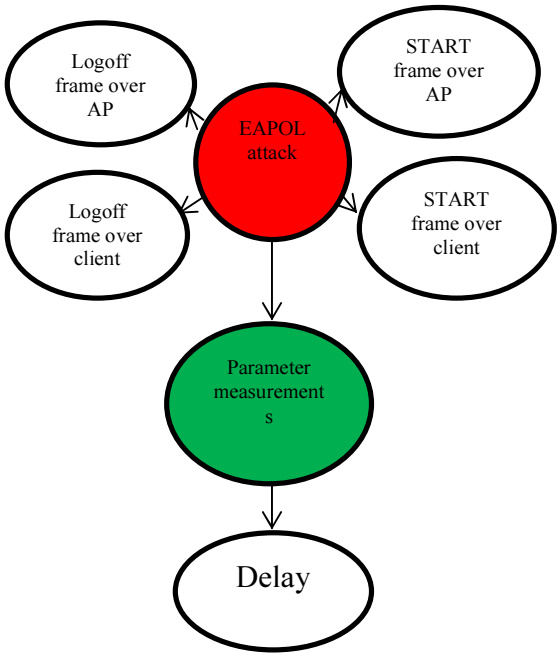

Figure 3: Attacks evaluation

6. RESULTS AND DISCUSSION

This section discusses the results of the existing and proposed solution which is approved out to be more effective to detect and prevent DoS attacks. From the results in figure3 and table1, it is shown that the proposed EICM is better in terms of detection time of DoS attacks when compared to the existing ICM method.

The solution is validated by measuring the time consumption for detecting and preventing DOS attackers in our network using ICM method and our method. AP and client are in communication with each other. At that time, intruder spoofs the MAC address of client and makes attack after that the EICM start the works. By using EICM, it is observed that the detection time of attack is reduced comparing with ICM. Numerical values are shown in Table 3.

Table 3: Detection Time Comparison

Number of users	Detection Time (sec)	
	ICM	EICM
10	0.01248008	0.00936006
20	0.007020045	0.00624004
30	0.006760043	0.005720037
40	0.005460035	0.005070033
50	0.005304034	0.004992032

In the case of ICM, the maintenance of five tables makes the searching complicated
The authentication process is based on an open shared key authentication. Since the key is open to all, the intruder easily finds the key.

The EICM studies the history of attackers by creating two tables and stores the MAC addresses of attackers and authenticated clients in two tables. This is observed through the graph generated by MATLAB taking number of user in X axis and detection time in Y axis. After implementing the solution the attacker cannot do the attack because the client authentication is based on the tables maintained by EICM. Hence EICM can easily identify the intruder and block him. The time detection shown in the Figure 4.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

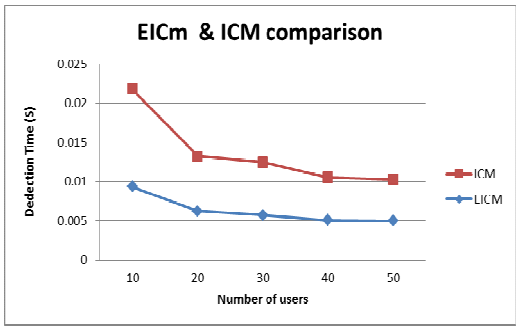

Figure 4: Detection Time Results

The time detection of DOS attack of the EICM and ICM are compared and the result observed that clearly our proposed EICM obtained better time detection than ICM.

7. CONCLUSION

This paper introduces an enhanced integrated central manager (EICM) algorithm to decrease the time detection of the DOS attack of the network. The obtained results indicate that, the proposed algorithm outperforms its competitors in terms of detection and searching time due to the decreasing of network time detection. The results show that the EICM has the ability to protect wireless infrastructure network against denial of service attacks by studying the history of the attack and storing the MAC addresses of intruders and the authenticated clients in tables. The results shows that the detection time was decreased compared to integrated central manager (ICM) and, moreover it prevents users of wireless local area networks (WLANs) from DoS attackers

REFERENCES

[1] SIMIC, D. AND R. PRODANOVIC, *A SURVEY OF WIRELESS SECURITY*. CIT. JOURNAL OF COMPUTING AND INFORMATION TECHNOLOGY, 2007. 15(3): P. 237-255.

[2] 2. KARYGIANNIS, T. AND L. OWENS, *WIRELESS NETWORK SECURITY*. NIST SPECIAL PUBLICATION, 2002. 800: P. 48.

[3] 3. MISHRA, A. AND W.A. ARBAUGH, *AN INITIAL SECURITY ANALYSIS OF THE IEEE 802.1 X STANDARD*. 2002.

[4] 4. HASSAN, H.R. AND Y. CHALLAL. *ENHANCED WEP: AN EFFICIENT SOLUTION TO WEP THREATS*. IN *WIRELESS AND OPTICAL COMMUNICATIONS NETWORKS, 2005. WOCN 2005. SECOND IFIP INTERNATIONAL CONFERENCE ON*. 2005. IEEE.

[5] 5. WONG, S., *THE EVOLUTION OF WIRELESS SECURITY IN 802.11 NETWORKS: WEP, WPA AND 802.11 STANDARDS*. URL: HTTP://WWW. SANS. ORG/RR/WHITEPAPERS/WIRELESS/1109. PHP RETRIEVED, 2003. 28(7): P. 05.

[6] 6. LASHKARI, A.H., M.M.S. DANESH, AND B. SAMADI. *A SURVEY ON WIRELESS SECURITY PROTOCOLS (WEP, WPA AND WPA2/802.11 I)*. IN *COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, 2009. ICCSIT 2009. 2ND IEEE INTERNATIONAL CONFERENCE ON*. 2009. IEEE.

[7] 7. SHENG, Y., ET AL. *DETECTING 802.11 MAC LAYER SPOOFING USING RECEIVED SIGNAL STRENGTH*. IN *INFOCOM 2008. THE 27TH CONFERENCE ON COMPUTER COMMUNICATIONS. IEEE*. 2008. IEEE.

[8] 8. GILL, R.S., ET AL., *PASSIVE TECHNIQUES FOR DETECTING SESSION HIJACKING ATTACKS IN IEEE 802.11 WIRELESS NETWORKS*. 2005.

[9] 9. GILL, R., J. SMITH, AND A. CLARK. *EXPERIENCES IN PASSIVELY DETECTING SESSION HIJACKING ATTACKS IN IEEE 802.11 NETWORKS*. IN *PROCEEDINGS OF THE 2006 AUSTRALASIAN WORKSHOPS ON GRID COMPUTING AND E-RESEARCH-VOLUME 54*. 2006. AUSTRALIAN COMPUTER SOCIETY, INC.

[10] 10. BELLARDO, J. AND S. SAVAGE. *802.11 DENIAL-OF-SERVICE ATTACKS: REAL VULNERABILITIES AND PRACTICAL SOLUTIONS*. IN *USENIX SECURITY*. 2003.

[11] 11. GUO, F. AND T.-C. CHIUEH. *SEQUENCE NUMBER-BASED MAC ADDRESS SPOOF DETECTION*. IN *RECENT ADVANCES IN INTRUSION DETECTION*. 2006. SPRINGER.

[12] 12. DING, P., J. HOLLIDAY, AND A. CELIK. *IMPROVING THE SECURITY OF WIRELESS LANS BY MANAGING 802.1 X DISASSOCIATION*. IN *CONSUMER COMMUNICATIONS AND NETWORKING CONFERENCE, 2004. CCNC 2004. FIRST IEEE*. 2004. IEEE.

[13] 13. SALEM, M., A. SARHAN, AND M. ABU-BAKR, *A DOS ATTACK INTRUSION DETECTION AND INHIBITION TECHNIQUE FOR WIRELESS COMPUTER NETWORKS*. ICGST INTERNATIONAL JOURNAL ON COMPUTER NETWORK AND INTERNET RESEARCH, CNIR}, 2007.

[14] 14. SAMRA, A.A. AND R. ABED, *ENHANCEMENT OF PASSIVE MAC SPOOFING DETECTION TECHNIQUES*. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 2010. 1(5).

[15] 15. DING, P., *CENTRAL MANAGER: A SOLUTION TO AVOID DENIAL OF SERVICE ATTACKS FOR*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

WIRELESS LANS. IJ NETWORK SECURITY, 2007. 4(1): P. 35-44.

[16] 16. VANI, B., ET AL., *INHIBITION OF DENIAL OF SERVICE ATTACK IN WLAN USING THE INTEGRATED CENTRAL MANAGER.* INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS, 2011. 29.

[17] 17. MALEKZADEH, M., ET AL., *VALIDATING RELIABILITY OF OMNET IN WIRELESS NETWORKS DOS ATTACKS: SIMULATION VS. TESTBED.* INTERNATIONAL JOURNAL OF NETWORK SECURITY, 2011. 3(1): P. 13-21.

[18] 18. PERSIA, A., M. DURAIRAJ, AND S. SIVAGOWRY. *STUDY OF THWARTING DOS ATTACKS BY DETECTING MAC SPOOF IN WLAN INFRASTRUCTURE NETWORKS.* IN *ADVANCED COMMUNICATION CONTROL AND COMPUTING TECHNOLOGIES (ICACCCT), 2012 IEEE INTERNATIONAL CONFERENCE ON.* 2012. IEEE.

[19] 19. BANSAL, R., S. TIWARI, AND D. BANSAL. *NON-CRYPTOGRAPHIC METHODS OF MAC SPOOF DETECTION IN WIRELESS LAN.* IN *NETWORKS, 2008. ICON 2008. 16TH IEEE INTERNATIONAL CONFERENCE ON.* 2008. IEEE.