Journal of Computer Science 8 (6): 828-834, 2012
ISSN 1549-3636

Effective Authentication Technique for Distributed Denial of Service Attacks in Wireless Local Area Networks

[1]Moorthy, M. and [2]S. Sathiyabama
[1]Department of MCA, Muthayammal Engineering College, Rasipuram, India
[2]Department of Computer Science, Thiruvalluvar Govt. Arts College, Rasipuram, India

Abstract: Problem statement: In 802.11-based Wireless LAN (WLAN), there is an mproved risk of security attacks. To defeat concealed attacks, there is a necessity to authenticate both access points and wireless stations. **Approach:** We propose a defensive technique for DDoS attack in WLAN. This authentication technique includes an Authentication Server (AS) in addition to the Wireless Station (WS) and Access Point (AP). **Results:** The authentication server holds both normal and attacker databases. The attacker database can be constructed from the outcome of fuzzy decision making. After WS and AP registers itself with AS, WS sends authentication request message to AS through the nearest AP. Before granting the session key for the WS, the AS checks the occurrence of WS in the attacker database. If it is found to be an attacker, AS denies the session key for the WS, there by isolating the WS from further communications. In order to prevent the authentication request flooding attacks, traffic pattern filtering rule is implemented. **Conclusion/Recommendations:** By simulation results, we show that the proposed technique is more efficient defensive mechanism against DDoS attack.

Key words: Wireless Local Area Networks (WLAN), Authentication Server (AS), Wireless Station (WS), Access Point (AP), Intrusion Detection System (IDS)

INTRODUCTION

Wireless LAN: The network that offers wireless access to data rates of 1mbps or more for both indoor and outdoor applications are termed as Wireless Local Are Networks (WLANs). It provides option for reposition and reconfiguration of equipment as well as new node addition to the network. This facility is accomplished with reduced cost of re-cabling and very less endeavor and thus it is more economic and simple for future applications. http://en.wikipedia.org/wiki/Wireless_LAN).

DDoS attacks: The most commonly occurring attacks which severely threatens the internet constancy is called as Distributed Denial of Service (DDoS) attack. The three main classifications of DDoS attacks as per CERT Coordination Center (CERT/CC) are flood attack, protocol attack and logical attack (Xia *et al*., 2010).

The feature of DDoS has a capability to stop the rightful utilization of the service. This is achieved by deploying several attackers.

The DoS aims at interrupting the services by limiting the service access as self-alternative way to weaken the service. It also causes network inability by affecting the networks bandwidth or connectivity (Bicakci and Tavli, 2009).

Particularly, DDoS attack is intended to the accessibility of the network. This is done by network access blockage, extreme delays, network resources consumption (Sharma, 2011).

Intrusion Detection System (IDS): The technique that observes the events occurring in the computer system or network which is different from normal activities and further proceeds with detection of those events is termed as intrusion detection technique. An Intrusion Detection System (IDS) takes events occurring in the system into consideration at the time of execution and depending on intimations of few strange warnings it detects whether the system is misused. In the field of the network security, intrusion detection is a serious problem. The common scheme of the intrusion detection includes misuse and anomaly detection. The IDS collects and verifies the data regarding the consciousness of the intrusion in the computer network (Syurahbil *et al*., 2009).

Issues in intrusion detection: The issues corresponding to the intrusion detection system are as follows.

External break ins: This occurs when the illegal user attempts to achieve access to a computer system.

Corresponding Author: Moorthy, M., Department of MCA, Muthayammal Engineering College, Rasipuram, India

Masquerader (internal) attacks: This occurs when the legal user tries to presume the uniqueness of new user. This attack is termed as internal attacks as they are resultant of the action of previously authorized users.

Penetration attack: This attack directly tries to deny the security policy of the system.

Leakage: This causes the potentially sensitive data to shift away from the system.

Denial of service: This causes the resources to be in busy condition which results in the refusing other users in using the system resources.

Malicious use: The miscellaneous attacks like file deletion, viruses, resource hogging etc comes under the malicious type.

The purpose of the real time IDS is to broadcast the data across a network among sensors and core area. These data can be stored and investigated which is termed as correlation server. This new network traffic considerably affects the network performance which necessitates the adequate bandwidth.

The air resistance guard or distributed air-magnet, exploit misuse signature depending on IDS. This results in a issue that they behave as perfect signature files only for the recognized files given to them (Singh *et al*., 2010).

Existing defense techniques for solving DOS attacks:
MAC Addressing Filtering (MAF): After initializing the MAC filtering approach, the access point compares the source MAC address of the received authentication request frame with the contents in the access point control table. In case the received MAC address is matched with contents in the access point control table, the received authentication request will be processed. Otherwise received authentication request will be dropped.

Traffic Pattern Filtering (TPF): In case the access point receives excess number of frames per second, the process of authentication request or association request will be stopped which is technique of traffic pattern filtering. The wireless traffic is small and irregular under normal situation. The access point has a capability to receive and activate around five 802.11 frames per second (Arockiam and Vani, 2011).

Intrusion detection and inhibition technique: This approach involves the creation of Intruder Database (IDB) which includes all intruder clients for avoid them to transmit transmission of two packets in one second. This overcomes the drawback of occurrence of DoS attack (Singh *et al*., 2005).

Path Identification method: In order to defend the victim server from the DDoS, several methods have been proposed. One of the most efficient methods is by Path identification (Pi). The Pi method has advantages such as trivial operation, filtering on a per-packet and independency on router for blocking over the other trace back methods (Beak *et al*., 2007).

Problem identification: In study (Christine *et al*., 2009), we proposed a hybrid intrusion detection system for wireless local area networks, based on Fuzzy logic. In this Hybrid Intrusion Detection system, anomaly detection is performed using the Bayesian network technique and misuse detection is performed using the Support Vector Machine (SVM) technique. The overall decision of system is performed by the fuzzy logic. This study focuses on the detection of attacks, but does not offer any defense mechanism.

In this study, we propose to design a defensive technique for misuse and DDoS attacks in Wireless Local Area Networks (WLAN).

Related work: Onofrei *et al*. (2010) and Moorthy and Sathiyabama (2011) introduced a light weight security mechanism based on firewall pin holing, that effectively prevents many DDoS attacks on the IMS based emergency framework. The proposed mechanism controls a firewall to generate pinholes that are necessary to effectively protect the emergency framework. This approach is especially effective against flooding bots that utilize spoofed IP addresses.

Liu *et al*. (2010) have proposed a AP based WLAN queuing model to analyze TCP/UDP traffic under these attacks. Their queuing model analysis leads to the development of four solutions: Request Authentication (RA), Reduction of Duplicate Requests (RDR), Reduction of Response Retransmissions (RRR) and Round Robin Transmission (RRT). They also studied the effects of authentication request flooding (AuthRF) and association request flooding (AssRF) on Wireless Voice Over IP (WVoIP).

Lee (2009) proposed a random bit authentication mechanism as a defense against DoS attacks. Random bits are placed into unused fields of the management frames. Access Point (AP) and Station (STA) can then authenticate each other according to these authentication bits. The defensive power is derived from the unpredictability of a random bitstream. Hence, the consumption of the computation and bandwidth resources is lightweight.

Singh *et al.* (2010) and Lee (2009) proposed to design the MAC layer based defense architecture for RoQ attacks in Wireless LAN which includes the detection and response stages. The attackers are detected by checking the RTS/CTS packets from the MAC layer and the corresponding attack flows are blocked or rejected.

Dong *et al*. (2010) have proposed a client-puzzle based DoS-resistant scheme of IEEE 802.11i wireless authentication protocol. They made use of beacon frame to distribute the puzzle to avoid the DoS attacks in association procedure. But the generation of puzzle always depends on devices hardware performance, which is restricted in some mobile devices.

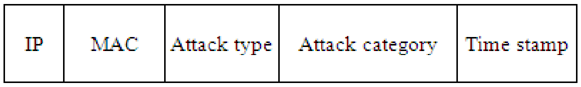
MATERIALS AND METHODS

Overview: In this study, we propose a defensive technique for DDoS attack in WLAN. The attack defense is based on the authentication technique which includes an Authentication Server (AS), a Wireless Station (WS) and an Access Point (AP). AS possess normal as well as attacker database. Initially WS registers with AS and obtains a secret key and sequence number. Similarly AP also registers with AS and obtains a secret key and nonce. Then WS forwards the authentication request to nearest AP. The AP that handles this request, creates its request message and concatenates it WS's request's message and then forwards it to AS. Upon verification, if AS detects slightly abnormal attack, it obtains the records of the attack type from the database and computes the average time interval (Tavg). When T_{avg} is below threshold, the session key is generated among WS and AP and fedback to AP. After verifying the sequence number and nonce, AP forwards the session key to WS. If Tavg is above threshold, the session key will not be generated and user request is rejected. On detection of completely abnormal attack, the session key is not generated and user request is denied directly. In order to prevent the authentication request flooding DoS attacks, traffic pattern filtering rule is implemented.

Intrusion detection technique: The hybrid intrusion detection system (Christine *et al*., 2009) ensures the security in the system from the possible attacks. In this system, a misuse detection module is connected to the anomaly detection module.

Table 1: Conditions for decision making in fuzzy logic

Bayesian network output	Support vector machine output	Decision making based on the fuzzy logic
Normal	Normal	Normal
Normal	Abnormal	Slightly abnormal
Abnormal	Normal	Slightly abnormal
Abnormal	Abnormal	Completely abnormal



IP	MAC	Attack type	Attack category	Time stamp

Fig. 1: Attacker's database

The anomalous detection system is based on Bayesian Networks (Lee, 2009) technique which is used to address the security problems related to attacks in wireless networks. The misuse detection system is based on Support Vector Machine (SVM) (Chen *et al*., 2009) which is used to create a pattern or a signature form so that the attack is detected when repeated.

The intrusion Detection System (IDS) maintains attacker's database (as per section 3.3) consisting of the signature of the possible attacks. The fuzzy logic methodology is handled for deciding the intrusion in the system which is more suitable module. This module performs the decision making based on input from Bayesian classifier system and SVM. Based on these inputs, the three output possibilities in fuzzy system are normal, slightly abnormal and completely abnormal.

The following Table 1 shows the conditions for decision making in fuzzy logic for inputs from Bayesian network and Support Vector Machine.

The condition for making the decision follows an if-then rule where if the output of both the modules are normal without any attack or problem causing component, then the decision is made as normal output, if the output of one module is normal and the other module is abnormal then the decision made is slightly abnormal, if the output of both the modules is abnormal then the decision made is completely abnormal.

Attacker database: The Intrusion Detection System (IDS) maintains a pattern database called Attacker Database (AD). This database is used to identify the intruders and thus inhibits them from gaining access to the network. The AD contains the IP address, MAC address, attack type, attack category and time of detection. This AD is updated each time when an intruder is detected.

Figure 1 represents the format of attacker's database. Here the IP refers to the users IP address. Based on the output of the fuzzy logic, the attack type is decided whether it is slightly or completely abnormal. The attack category is based on anomaly as well as misuse attacks such as DoS, remote to user attack, user to root attack, probing. The time stamp (T) corresponds to the time the attack is prevailing.

When a user tries to submit a packet which needs the access to the network, the users IP is first verified against AD. If this user is found in AD, the Access Point (AP) will prevent it from sending another wrong packet in 1 sec. This prevents the intruding node from bringing the WLAN down and causing DoS.

Authentication technique: The attack defense is based on the following authentication technique. It involves an Authentication Server (AS), a Wireless Station (WS) and an Access Point (AP). The AS consists of two databases: a Normal Database (ND) and Attacker Database (AD) (which is described in the previous section).

We assume the following parameters for the authentication technique:

K_{sec}(WS)	=	Secret key of WS
K_{sec}(AP)	=	Secret key of AP
K_{ses}	=	Session key among WS and AP
SN	=	Sequence number used by WS
N	=	Nonce utilized by AP
MAC [WS]	=	MAC address of WS
MAC [AP]	=	MAC address of AP
$AuthREQ_{SN}$	=	Authentication Request from WS
$AuthREQ_N$	=	Authentication request from AP
T_{avg}	=	Average time interval
Th	=	Threshold for time interval

ND includes the MAC [WS] and MAC [AP], K_{sec} [WS] and K_{sec} [AP], K_{ses} [WS] and K_{ses}[AP], SN and N. The SN is used to count the attacks and should be incremented by one for every new authentication request.

The following algorithm describes the authentication technique.

WS registers with AS to provide its MAC and get a shared secret key K_{sec} [WS] and initial SN from AS:

$$WS \xrightarrow{MAC[WS]} AS$$

Registration:

$$AS \xrightarrow{K_{sec}[WS]+SN} AP$$

Similarly, AP registers with AS to provide its MAC and get shared secret key K_{sec} [AP] and initial N from AS:

$$AP \xrightarrow{MAC[AP]} AS$$

Registration:

$$AS \xrightarrow{K_{sec}[AP]+N} AP$$

WS broadcast AuthREQ message to the nearest AP when it requires access to the WLAN:

$AuthREQ_{SN}$: [MAC [WS], SN, K_{sec} [WS]]

$$WS \xrightarrow{AuthREQ_{SN}} AP$$

The AP that handles $AuthREQ_{SN}$, creates $AuthREQ_N$ and concatenates it with $AuthREQ_{SN}$ and then forwards it to AS.

$AuthREQ_N$: [MAC [AP], N, K_{sec} [AP]]:

$$AP \xrightarrow{AuthREQ_{SN}+AuthREQ_N} AS$$

In order to share K_{ses} [AP] and K_{ses} [WS], AS verifies its database as per following cases.

Case 1:

```
If Attack type = slightly abnormal,
Then
AS fetches matched records of the attack type from the database and calculates $T_{avg}$:
    If $T_{avg}$ < Th
    Then
$K_{ses}$ is generated and sent back to AP.
    The AP forwards $K_{ses}$ to WS after verifying SN and N.
Else
    The $k_{ses}$ is not generated and the user request is denied
End if
    End if
```

Case 2:

```
    If attack type = completely abnormal
Then
    The $k_{ses}$ is not generated and user request is rejected directly
        End if
```

In case of the slightly abnormal attack detection, the authentication server obtains the records of the attack types from the database and computes the average time interval. When the average time interval is below the threshold, the session key is generated among WS and AP and feedback to AP. Then AP forwards the session key to WS after verifying the sequence number and nonce. Otherwise the session key is not generated and user is rejected. In case of the completely abnormal attack detection, the session key is not generated and user request is denied directly. This denial results in reduction of authentication request flooding.

Filtering rule: During the normal condition, it is usual for AP to receive and access approximately five 802.11 frames per second. But when there is authentication request flooding (RF_{au}) DoS attacks, the wireless traffic follows various patterns. For every faked authentication request frame, the hacker sends it five times and AP responds with five 802.11 ACK frames. In addition, the AP might receive and process up to hundred authentication request frames per second (ps).

Thus in order to prevent the authentication Request Flooding (RF_{au}) DoS attacks, Traffic Pattern Filtering Rule (TFR) (Arockiam and Vani, 2011) is implemented. This rule is applied when AP retrieves the header information from the received authentication requests. In this phase, in spite of having sufficient information from the sender for implementing TFR, wastage of AP resources is avoided to process faked authentication request frames:

```
If n $(RF_{au})_{ps}$> 5,
Then
 The received frames will be dropped
 Else
The frames will be processed.
 End if
```

When the number of the authentication request flooding frames is greater than five, the received frames will be dropped otherwise the frames will be further processed.

RESULTS AND DISCUSSION

Deals with the experimental performance evaluation of our algorithm through simulations. In order to test our protocol, the NS2 simulator (Bridges and Vaughn, 2000) is used. We compare our proposed ETA technique with the HFIDS (Christine *et al*., 2009) technique.

Simulation setup: In the simulation, the number of nodes is kept as 8. The simulation topology is as shown in the Fig. 2. There are 5 wireless clients connected with a BS, which is attached with a Correspondent Node (CN) and an AS. The nodes are arranged in a 500×500 m square region for 60 sec of simulation time. The client MS1 is considered as an attacker which performs Authentication flooding attacks. All nodes have the same transmission range of 250 m. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summarized in Table 2.

Table 2: Simulation settings

Total number of nodes	8
Attack type	Authentication flooding
Area	500×500
Routing protocol	DSDV
MAC	802.11
Radio range	250 m
Packet size	512
Attacker	1
Attack traffic rate	50-250 Kb
Simulation time	50 sec
Traffic source	CBR

Simulation parameters: The following parameters are used to evaluate the performance of our proposed technique. The proposed technique is compared with our previous technique HFIDS (Christine *et al*., 2009):

Packet delivery ratio: This is the ratio between the number of packets received and the number of packets sent to the receiver.

Drop ratio: This is the ratio of number of packets dropped due to the attack and the number of packets sent.

Received bandwidth: This is the total bandwidth obtained by the receiver measured in Mb/s.

Received packets: It is the number of packets successfully received by the receiver.

Simulation results: In the initial experiment, we vary the attack traffic rate from 50-250 kb and measure the above metrics. Since the attacker is efficiently detected and isolated, the effect packet drop is reduced there by increasing the number of packet received and packet delivery ratio.

From the Fig. 3, we can see that the delivery ratio of our proposed ETA protocol achieves higher than the existing HFIDS protocol. From Fig. 4, we can see that our proposed ETA has less packet drop than the existing HFIDS protocol.

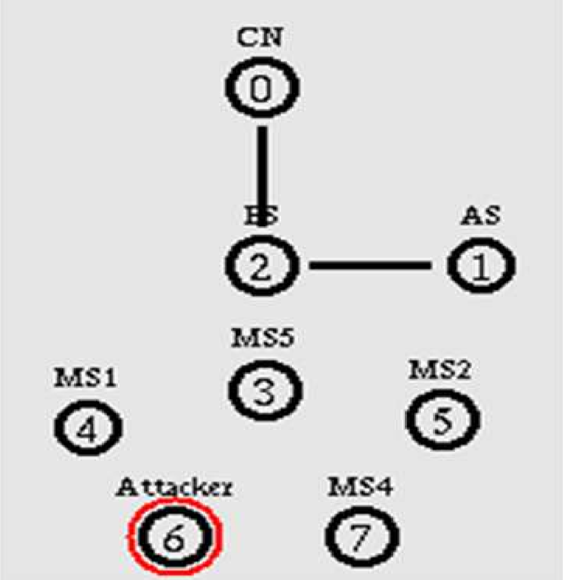


Fig. 2: Simulation topology

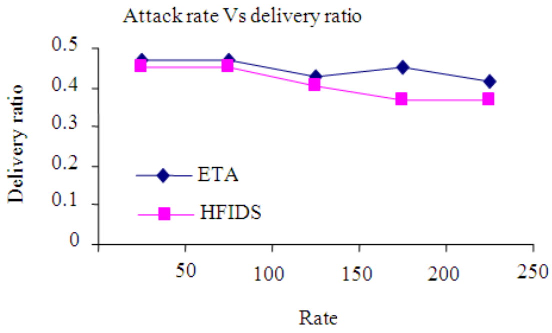


Fig. 3: Rate Vs delivery ratio

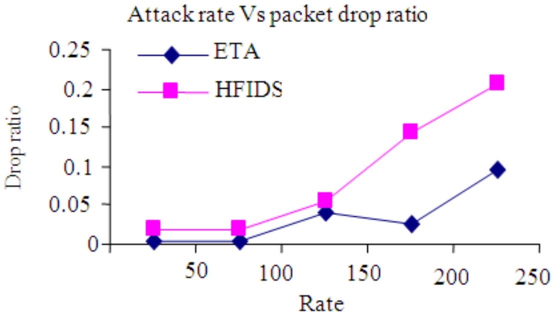


Fig. 4: Rate Vs packet drop

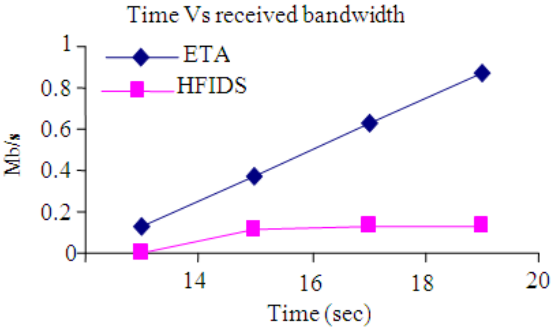


Fig. 5: Time Vs received bandwidth

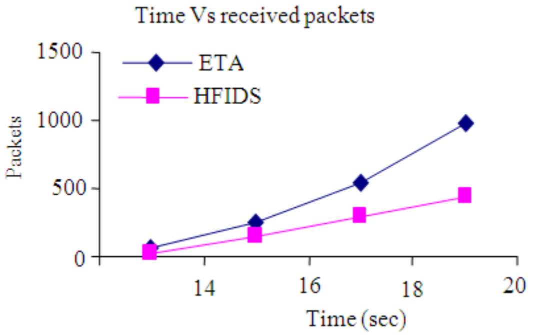


Fig. 6: Time Vs received packets

In the second experiment, we measure the performance metrics during various time intervals. Figure 5 shows that our proposed ETA protocol achieves better bandwidth received ratio than the existing HFIDS protocol. Figure 6 shows that our proposed ETA protocol achieves high packet received ratio than the existing HFIDS protocol.

CONCLUSION

In this study, we have proposed a defensive technique for DDoS attack in WLAN. This approach is based on the authentication technique which includes an Authentication Server (AS), a Wireless Station (WS) and an Access Point (AP). The authentication server holds both normal and attacker database. The attacker database can be constructed from the outcome of fuzzy decision making. After WS and AP registers itself with AS, WS sends authentication request message to AS through the nearest AP. Before granting the session key for the WS, the AS checks the occurrence of WS in the attacker database. If it is found to be an attacker, AS denies the session key for the WS, there by isolating the WS from further communications. In order to prevent the authentication request flooding attacks, traffic pattern filtering rule is implemented. By simulation results, we have shown that the proposed technique is more efficient defensive mechanism against DDoS attack.

REFERENCES

Bridges, S.M and R.B. Vaughn, 2000. Intrusion detection via fuzzy data mining. Proceedings of the 12th Annual Canadian Information Technology Security Symposium, Jun. 19-23, 2000, The Ottawa Congress Centre.

Arockiam, L and B. Vani, 2011. A comparitive study of the available solutions to minimize denial of service attacks in wireless LAN. Int. J. Comput. Technol. Appli., 2: 619-625.

Beak, C., J.A. Chaudhry, K. Lee, S. Park and M. Kim, 2007. A novel packet marketing method in ddos attack detection. Am. J. Applied Sci., 741-745. DOI: 10.3844/ajassp.2007.741.745

Bicakci, K and B. Tavli, 2009. Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. Comput. Stand. Interfaces, 31: 931-941. 10.1016/j.csi.2008.09.038

Chen, R.C., K.F. Cheng, Y.H. Chen and C.F. Hsieh, 2009. Using rough set and support vector machine for network intrusion detection system. Proceedings of the 1st Asian Conference on Intelligent Information and Database Systems, Apr. 1-3, IEEE Xplore Press, Dong Hoi, pp: 465-470. DOI: 10.1109/ACIIDS.2009.59

Christine C.G., F. Zhang, R. Manji, S. Arora and M. Bornfreund *et al*., 2009. Evaluation of multiple test methods for the detection of the novel 2009 influenza A (H1N1) during the New York City outbreak. Int. J. Comput. Sci., Netw. Security, 9: 45: 191-195. DOI: 10.1016/j.jcv.2009.06.005

Dong, Q., L. Gao and X. Li, 2010. A new client-puzzle based DoS-resistant scheme of IEEE 802.11i wireless authentication protocol. Proceedings of the 3rd International Conference on Biomedical Engineering and Informatics (BMEI), Oct. 16-18, IEEE Xplore Press, Yantai, pp: 2712 -2716. DOI: 10.1109/BMEI.2010.5639818

Liu, C., J. Yu and G. Brewster, 2010. Empirical studies and queuing modeling of denial of service attacks against 802.11 WLANs. Proceedings of the IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM), Jun. 14-17, IEEE Xplore Press, Montreal, QC, Canada, pp: 1-9. DOI: 10.1109/WOWMOM.2010.5534920

Lee, Y.S., 2009. The role of genes in the current obesity epidemic. Ann. Acad. Med. Singapore, 38: 45-53. PMID: 19221670

Moorthy, M. and S. Sathiyabama, 2011. Hybrid fuzzy based intrusion detection system for wireless local area networks. Eur. J. Sci. Res., 53: 431-446.

Onofrei, A.A., Y. Rebahi and T. Magedanz, 2010. Preventing distributed denial-of-service attacks on the IMS emergency services support through adaptive firewall pinholing. Int. J. Next Generation Netw., 2: 1-17.

Sharma, M.A., 2011. Network intrusion detection system for denial of service attack based on misuse detection. Int. J. Comput. Eng. Manage.

Singh, J., S. Gupta and L. Kaur, 2010. A MAC layer based defense architecture for Reduction-of-Quality (RoQ) attacks in wireless LAN. Int. J. Comput. Sci. Inform. Security, 7: 284-291.

Singh, U.K. A.K. Ramani, N.S. Chaudhari and V. Gupta, 2005. Increasing effectiveness of IDS to improve security in intranet. Am. J. Applied Sci., 1032-1035. DOI: 10.3844/ajassp.2005.1032.1035

Syurahbil, N.A., M.F. Zolkipli and A.N. Abdalla, 2009. Intrusion preventing system using intrusion detection system decision tree data mining. Am. J. Eng. Applied Sci., DOI: 10.3844/ajeassp.2009.721.725

Xia, Z., S. Lu, J. Li and J. Tang, 2010. Enhancing DDoS flood attack detection via intelligent fuzzy logic. Informatica (Slovenia), 34: 497-507.