Research Journal of Applied Sciences, Engineering and Technology 10(9): 1012-1020, 2015
DOI: 10.19026/rjaset.10.1868
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: December 29, 2014 Accepted: April 2, 2015 Published: July 25, 2015

Research Article

Secure Framework for DDoS Attack Detection and Defense in IEEE 802.11 WLAN

[1]S. Suganthi and [2]M. Aramudhan
[1]Tagore Arts College, Govt. of Puducherry, India
[2]Department of Information Technology, Perunthalivar Kamarajar Institute of Engineering and Technology, Nedungadu, Karikal, India

Abstract: Security is one of the most important problems to be considered in the Wireless Local Area Networks (WLANs). Several security techniques were initiated to solve the available security bugs. In this study, we propose to design a detection and defense mechanism against DDoS attacks. Initially GIDA module is deployed, so that DDoS attack is detected using the game theory decision model in the Access Point (AP). A Master Session Key (MSK) is calculated and a hash function is created for security. For the authentication and association of frames a client puzzle based defense mechanism is used in the AP. Here the client solves a puzzle which has been send by the AP. In the next phase, de-authentication or disassociation of frames of AP or client can be protected by the random bit authentication mechanism. It inserts the current 3-bit unit into the unused bit positions of each frame and then advances the index to point to the next unit. The respective frames can be protected by the hash function and master session key. This framework provides a complete solution for the DDoS attacks targeted at both clients and AP.

Keywords: Access point, authentication, client puzzle, Denial of Service (DoS) attack, detection, framework, IEEE 802.11, Wireless Local Area Networks (WLAN)

INTRODUCTION

Wireless Local Area Network (WLAN): A Wireless Local Area Network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio). WLAN provides a connection through an access point to the wider Internet. This gives users the ability to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name. It is a type of local-area network with the aim of high-frequency radio waves rather than wires to communicate between nodes. Wireless LANs introduce the concept of complete mobility; communication is no longer limited to the infrastructure of wires (Salem *et al*., 2007).

WLAN brings up many security problems. Due to the lack of physical connection between a wireless station and its access point, the wireless station has no way to figure out whether the access point it is communicating with is a legitimate access point or not. This situation makes access points as untrustworthy as wireless stations. To counter masquerading attacks in wireless LANs, it needs to authenticate both access points and wireless stations. Several mutual authentication protocols for wireless LANs, including the new IEEE 802.11i standard have been proposed for the wireless station and the access point to authenticate each other (Zheng *et al*., 2005).

DDoS attack and detection in WLAN: The main goal of Denial-of-Service (DoS) attacks is to inhibit or even worse prevent legitimate users from accessing network resources, services and information. More specifically, this sort of attack targets the availability of the network i.e., by blocking network access, causing excessive delays, consuming valuable network resources, etc. A denial of service occurs when an attacker has engaged most of the resources a host or network has available, rendering it unavailable to legitimate users (Anuradha and Singhrova, 2011).

DoS attacks are commonly characterized as events where legitimate users or organizations are deprived of certain services like web, e-mail or network connectivity that they normally expect to have. Therefore they attempt:

- To inhibit legitimate network traffic by flooding the network with useless traffic
- To deny access to a service by disrupting connections between two parties
- To block the access of a particular individual to a service
- To disrupt the specific system or service itself (Gupta *et al*., 2008)

Corresponding Author: S. Suganthi, Tagore Arts College, Govt. of Puducherry, India

Some specific and particularly popular and dangerous types of DDoS attacks include:

Smurf attack: This attack works on the mechanism of flooding the victim's bandwidth.

UDP Flood: This DDoS attack leverages the User Datagram Protocol (UDP), a session less networking protocol.

ICMP (ping) flood: ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies.

SYN flood: A SYN flood DDoS attack exploits an known weakness in the TCP connection sequence.

Ping of death: A Ping of Death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer.

Slowloris: Slowloris is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network.

Zero-day DDoS: "Zero-day" are simply unknown or new attacks, exploiting vulnerabilities for which no patch has yet been released.

DoS can be detected using various tools and commands. One among this is Wireshark. Wireshark or ethereal are the packet monitoring tools that capture traffic entering or exiting a specific port. This software is an open source analyzer that breaks down into finer details of the packets. The best feature of this tool is that it can capture live traffic for analysis. The traffic pattern could also be stored for future detailed analysis (Subramani, 2011).

Problem identification: Security is one of the most important issues to be considered in the WLANs. There are many weakness points of security in WLANs due its nature. Since management frames are not authenticated, 802.11 WLAN susceptible to Denial of Service (DoS) attacks. One of the common attacks is to flood the surroundings with huge amounts of de-authentication or disassociation frames. The other types of attacks are Authentication and Association attack which leads to exhaustion of wireless access points.

Authentication and Association attack has been addressed in Laishun *et al*. (2010). Whereas de-authentication or disassociation attacks are address in Lee *et al*. (2009). The work in Bedi *et al*. (2011) reduces the DoS and DDoS attacks for TCP-friendly flows. Here Game Inspired Defense Architecture (GIDA) module which acts as a defender is used to reduce the DoS attack, which is the combination of Game decision agent and firewall.

But, no work has been done to provide complete solution to defense against all these DDoS attacks in WLAN. Hence in this study, we propose to design a secure framework for detection and defense against DDoS attacks for WLAN.

LITERATURE REVIEW

Anuradha and Singhrova (2011) have presented an architecture of Host based Intrusion Detection System for DoS attack in distributed WLAN (HIDS). The proposed system is an intelligent system that will detect the intrusion dynamically and periodically on estimating the intruder association respective to the current node with its neighbor nodes. It also uses the concept of Bloom filter, in which it stores destination IP address that is used to detect an intruder with misuse detection approach. This approach is more reliable and efficient, as it implemented on distributed nodes and not on single server system. Therefore, all nodes of wireless network will collaboratively participate in detecting intruder in WLAN. It is more reliable as all destination IP addresses are stored in Bloom Filter using hashing technique. However it is cost effective.

Lina and Dongzhao (2009) have presented a research on attack model and principle of LDOS which can help us know the features of the attack and provide a basis for further research. The aim of their detection measure is to detect and defense LDOS in time with calculation resource as little as possible. At the end of this study, they have shown the new way can break up the attack burst into parts. However filtering algorithm or choking algorithm will make flow packets lose more or less.

Moorthy and Sathiyabama (2011) have proposed to develop 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. The outputs of both anomaly detection and misuse detection modules are applied by the fuzzy decision rules to perform the final decision making. This scheme is very scalable and accurate since incorrect interpretation is not possible due double check in this technique. However there is packet loss due to the number of attackers.

Liu and Yu (2007) have presented a solution to detect and resolve Authentication Request Flooding (AuthRF) and Association Request Flooding (AssRF). They have developed an experimental framework to demonstrate and quantify AuthRF and AssRF attacks against TCP and Wireless Voice over IP (WVoIPs) communications. This solution is theoretically cost-effective with no performance degradation to TCP or UDP traffic. However AssRF causes a high effect of packet loss.

Lee *et al*. (2009) have designed 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. However the efficiency of the system is very low.

Bedi *et al*. (2011) have presented the game models for DoS/DDoS attacks and their possible countermeasures. They also considered the interaction between the attacker and the defender (network administrator) as a two-player game. Results show that the total bytes sent by the attacker remain constant. However it is cost effective.

Wu *et al*. (2010) have modeled the interaction between the attacker and the defender as a two-player non-zero-sum game in two attack scenarios:

- One single attacking node for Denial of Service (DoS)
- Multiple attacking nodes for Distributed DoS (DDoS)

The defender's challenge is to determine optimal firewall settings to block rogue traffics while allowing legitimate ones. However both the attacker and the defender are not able to change strategies during their attack.

PROPOSED METHODOLOGY

Overview: In this study, we propose to design a secure framework for DDoS detection and defense in WLAN. Figure 1 shows the block diagram of the proposed framework. The framework consists of three modules. In the first module, the UDP flooding attack is detected using the game theory decision model (Bedi *et al*., 2011) by analyzing the flows. These attacked flows are then identified and the corresponding clients are marked as attackers by the AP. Next a Master Session Key (MSK) (Singh and Sharma, 2011) is calculated and a hash function is created. In the second module, for the authentication and association attacks, a client puzzle based defense mechanism (Laishun *et al*., 2010) is used in the AP. Here the client solves a puzzle which has been send by the access point. The difficulty of degree of the puzzle could be easily adjusted by the AP. The puzzle can be protected by means of the created hash function.

In the third module, de-authentication or disassociation attacks on AP or client can be protected by the random bit authentication mechanism (Lee *et al*., 2009). It inserts the current 3-bit unit into the unused bit positions of each frame and then advances the index to point to the next unit. The respective frames can be protected by the hash function and master session key.

Game theory based DDoS attack detection: The Game theory based DDoS attack detection is a decision module (Bedi *et al*., 2011) which analyzes the incoming flow for UDP flooding attack by restricting or providing access to the Target Server (TS) based on its computed decisions. This decision is based on the certain properties of the incoming flow.

The Game theory model mainly consists of two major components such as Game Decision System and a firewall. Using the Game decision system the incoming flows are analyzed and the appropriate defensive decisions were computed which are then implemented using the firewall. Decisions taken by the GIDA Module on incoming flow encompass the actions possible by the defender to prevent attacks and protect the target server.

Attack detection: The attack detection consists of allowing the traffic to the Target Server (TS), redirecting them to Honey Pot (HP) or dropping the same.

The detector selects two thresholds T_1 & T_2 for deciding the actions for the incoming flows. For a source node the total flow rate is calculated as:

$$x = r \, . \, n \tag{1}$$

r : Bit-rate per flow
n : Number of flows per node

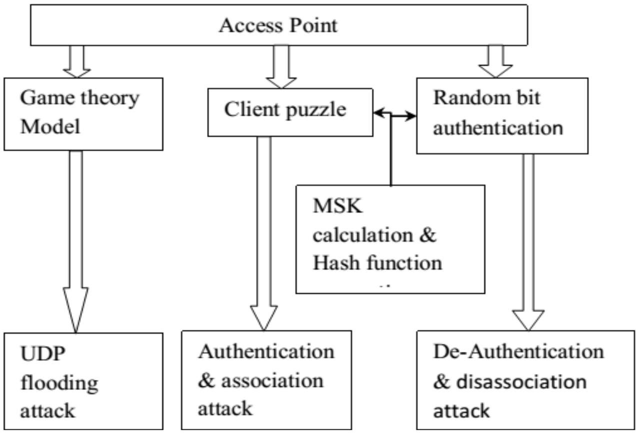
Access Point
Game theory Model
Client puzzle
Random bit authentication
MSK calculation & Hash function
UDP flooding attack
Authentication & association attack
De-Authentication & disassociation attack

Fig. 1: Block diagram

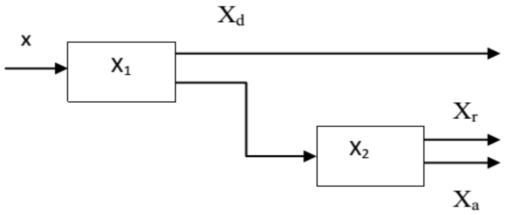

Fig. 2: Filter arrangement

In this module the detector observes in such a way that, if the total flow rate $r.n<T_2$ then the firewall allows the set of flows to reach the TS.

If $r.n>T_2$ and $r.n<T_1$, all the flows from the source node K is directed to the HP.

If $r.n>T_1$, all the flows from the source node is dropped by the firewall.

The thresholds T_1 & T_2 are used for creating two sigmoid filters X_1 & X_2. These two filters are modeled for allowing, dropping and redirecting the probabilities of flow per source node. It is designed as:

$$\mathrm{X}_1(x)=\left(1+e^{-\sigma\left(\frac{x-T_1}{b}\right)}\right)^{-1} \tag{2}$$

$$\mathrm{X}_2(x)=\left(1+e^{-\sigma\left(\frac{x-T_2}{b}\right)}\right)^{-1} \tag{3}$$

where,

T_1 & T_2 = Flow rate for which the probability of dropping and redirecting a flow is 0.5, respectively

σ = Scaling parameter

b = The variable which represents the bandwidth consumed per node

b = B/t

The firewall drops the flow of rate with a probability X_1 (x) and redirects with a probability of X_2 (x).

In order to make a decision, the detector designs three probabilistic functions such as, for dropping X_d (T_1, T_2, x), for allowing X_a (T_1, T_2, x) and for re-directing X_r (T_1, T_2, x).

The working of the filter (Fig. 2) with three probabilistic functions is designed.

The filters X_1 and X_2 is arranged together for creating three probabilistic functions X_d, X_r and X_a which are used for computing the probabilities for flows from a node that should be allowed to reach the target server, redirected to the honeypot or dropped by the firewall. The total bit-rate x from each source is the input for the first filter X_1. This filter X_1 decides the probability whether flows from a node should be dropped or not. The probability for dropping flows from a user is directly obtained from this first filter and is denoted by X_d. The probability functions are defined as:

$$\mathrm{X}_d = \mathrm{X}_1 \tag{4}$$

$$\mathrm{X}_r = \mathrm{X}_2 \cdot (1-\mathrm{X}_1) \tag{5}$$

$$\mathrm{X}_a = (1-\mathrm{X}_1)\cdot(1-\mathrm{X}_2) \tag{6}$$

Generation of Master Session Key (MSK): Apart from detecting the DDoS Flooding attack, in order to provide defense against various other DDoS attacks, a Master Session Key (MSK) is generated. This is used for encrypting the randomly generated and working key. The operation for MSK generation is given as follows (Singh and Sharma, 2011):

- At first the STA sends probe Request (R_{p1}) to AP. The AP has a pre generated pool of random numbers Φ_t along with pre computed private Key (K_{AP}) and corresponding Public Key (PK_{AP}) pairs. The pairs are generated using Elliptic Curve Cryptosystem (ECC). Elliptic Curve parameters (EC_{Param}) define an Elliptic Curve (EC) over finite field. AP selects one of the Public Keys (PK_{AP}) from its group for the current STA session.
- The AP response to STA includes R_{p2}, selected public key PK_{AP}, set of random numbers Φ_t and Elliptic Curve parameters (EC_{Param}).
- If STA wants only to probe the network. It generates its pair of keys, Key (K_{STA}) and Public Key (PK_{STA}). It then utilizes its Key (K_{STA}) and the Public Key (PK_{AP}) of AP for generating the Master Key (MK).
- STA also selects one of the numbers (R_1) from the random number set which was received from AP. STA selects another Random number (R_2). This number along with MK is used to calculate the Master Session Key (MSK) using Pseudo Random Function (PRF):

$$\mathrm{MSK} = \mathrm{PRF}\ \{\mathrm{R2}, \mathrm{MK}\} \tag{7}$$

- STA calculates hash H of R_1 and σ as indicated by (8). This hash is used for AP protection under DoS attacks. STA stores MK, MSK and H for use in authentication phase.

Hash function generation: Next a hash function (Singh and Sharma, 2011) is created which is given by:

$$\mathrm{H} = \mathrm{h}\ (\mathrm{R}_1, \sigma) \tag{8}$$

where,

σ = - xh (Π (Γ)) -λ
x = Private key
h = A collision resistant one-way hash function from Z^*_p to Z^*_p
Γ = STA public information generation
λ = Random number

Client puzzle mechanism for authentication and association attacks: This puzzle based mechanism (Laishun *et al*., 2010) is used to resist the authentication and association attacks. Here the attacker computes a puzzle send by AP when it produce authentication and association frames. The puzzle degree of difficulty is simply adjusted by the AP. The steps involved in the client puzzle mechanism are illustrated in Fig. 3 and in the following algorithm.

Algorithm:

Step 1: Initially the station STA generates and stores a random number $N_{STA} = _R\{0,1\}^{64}$ in order to send to the AP. It embeds N_{STA} into the probe request frame and sends it to the AP.

Step 2: The AP after receiving the probe request generates the random number NAP, a time stamp T_{AP} and a puzzle according to the current remain resources and attack degree. Next the AP embeds the N_{AP}, T_{AP} and the puzzle into the probe response and sends it to the STA:

$$N_{AP} = H\ (\text{secret},\ N_{STA}|MAC_{STA}) \tag{9}$$

where, H = h (R, σ) which is a hash function used for protecting the puzzle.

Here the secret will be changed periodically. The puzzle can be created as Puzzle = k, the length of k is one byte and the value range is from 0 to 64. AP can dynamically decide the value of k. STA should solve the puzzle and answer with the solution satisfying the following equation:

$$\text{Hash}\ (N_{STA}|N_{AP}|\text{solution}) = (\text{left k})\ 0^{64} \tag{10}$$

Step 3: The STA after receiving the probe response frame from the AP, solves the puzzle by brute force. Then embeds the solution puzzle T_{AP}, N_{AP} and N_{STA} into the authentication request frame and sends to the AP.

Step 4: AP after receiving the authentication request frame checks whether N_{AP} is right or not. If the check procedure solution is acceptable, the mechanism is continued. Next to this AP will generate a new N_{AP} and T_{AP} and puzzle′ when the secret is refreshed. AP then embeds $N_{AP'}$, $T_{AP'}$, puzzle′ into authentication response frame and sends to STA.

Step 5: After receiving the authentication response from AP, STA solves the puzzle′ and embed the solution of the puzzle′, $N_{AP'}$, T_{AP} and N_{STA} into the authentication request frame. And then send the frame to the AP.

Step 6: After receiving an association request frame, AP will first check whether N_{AP} is right or not, then continue check the solution. When check procedure is satisfactory, AP will allocate memory space for this STA. Before this step, AP does not allocate any space for STA. AP will answer an association response frame to STA.

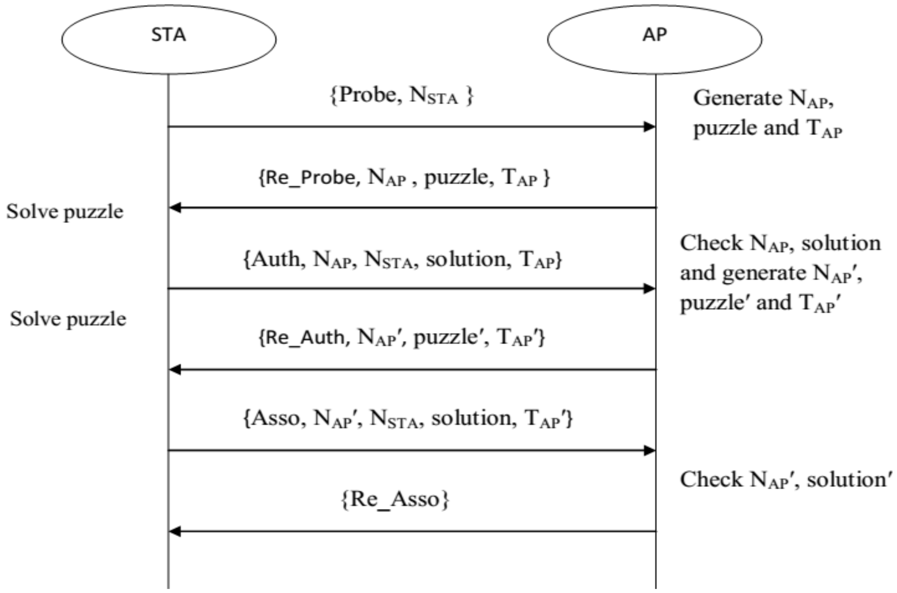
STA
AP
{Probe, N_STA }
Generate N_AP, puzzle and T_AP
{Re_Probe, N_AP , puzzle, T_AP }
Solve puzzle
{Auth, N_AP, N_STA, solution, T_AP}
Check N_AP, solution and generate N_AP′, puzzle′ and T_AP′
Solve puzzle
{Re_Auth, N_AP′, puzzle′, T_AP′}
{Asso, N_AP′, N_STA, solution, T_AP′}
Check N_AP′, solution′
{Re_Asso}

Fig. 3: Mechanism of client-based puzzle

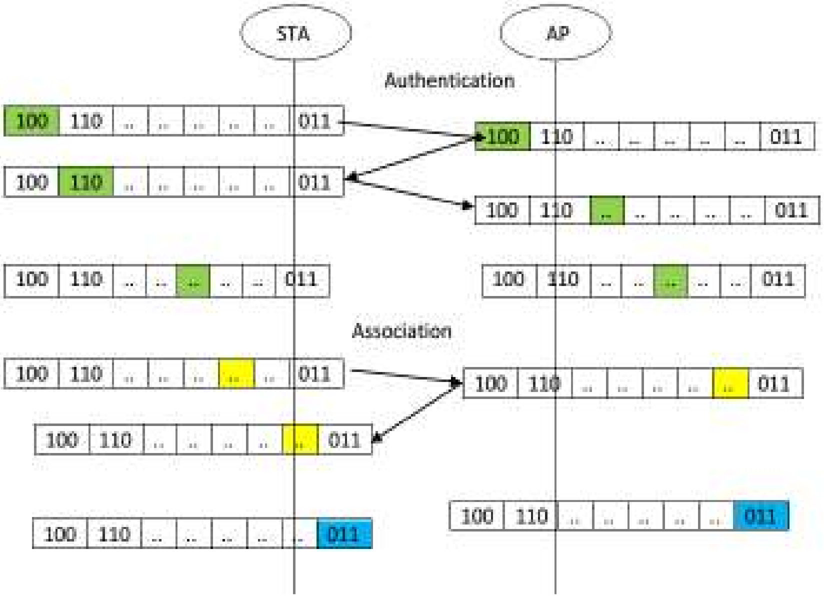

Fig. 4: Random bit authentication method

Random bit authentication for de-authentication or disassociation attacks: The de-authentication or disassociation of frames for AP or client can be protected by means of the Random Bit Authentication (RBA) mechanism (Lee *et al*., 2009). Here the hash function and master session key is used in order to protect the respective frames. In this random bit authentication, random bits are placed into unused fields of the management frames.

An identical random bit stream is independently generated. The stream is divided into equal-sized chunks, each having "N" authentication bits called as "N random bits". Each chunk is given an index number. In our design we are using only 8 chunks in 802.11.

In this Random bit authentication, when a node AP or STA sends de-authentication or disassociation frames RBA inserts current 3-bit unit, along with this a hash key H and the MSK is also inserted into the unused bit positions of each frame and then it is moved forward the index to point to the next unit. The receiving node checks whether the random authentication bits from the incoming bits matches the corresponding bit stream unit on the receiver side. If not, the incoming frame is rejected.

Figure 4, the 5th and the 8th units would be matched for legitimate de-authentication and disassociation frames, correspondingly. Though, the attacker would not know the values for those units for certain it keeps deducing the authentication bits until it is equal.

The attacker also takes a brute force and cycles via all the possible values and random bits. In case of 3-bit random authentication unit, the attacker can successively substitute the values from 0 to 7 as the authentication bits used in the attacking frame. Here one out of the 8 spoofed de_auth/dis_assoc frames would pass the authentication test. The success rate of an attacker to disconnect the session between the AP and the STA is thus 1/8 per cycle in the 3-bit random authentication case. If the number of authentication bits used is increased, the success rate for achieving DoS is decreased exponentially.

Overall algorithm:

- Initially the detector sets two threshold values for deciding the incoming flows.
- If the total flow rate $x<T_2$ then the firewall allows the set of flows to the target server TS.
- If $x>T_2$ and $x<T_1$, all the flows from the source node K is directed to the honey pot HP.
- If $x>T_1$, all the flows from the source node is dropped by the firewall FW.
- Next the probabilities of flow per source node such as allowing, dropping and redirecting were decided by using the two filters X_1 & X_2.
- The firewall drops the flow of rate with a probability X_1 (x) and redirects with a probability of X_2 (x).
- Next to this a MSK is created and a hash function H is generated.
- Using this hash function H a puzzle is created by AP, which is used for the attacker to compute the puzzle.
- AP sends the N_{AP}, T_{AP} and the puzzle to STA.
- STA solves the puzzle by satisfying the equation Hash (NSTA|NAP|solution) = (left k) 0^{64}.
- And embeds the solution puzzle T_{AP}, N_{AP} and N_{STA} into the authentication request frame and sends to the AP.

- AP by receiving the authentication request checks whether N_{AP} is right, if not AP will generate new puzzle.
- Next STA sends association request frame to AP so that AP will first check whether N_{AP} is right or not and then continue check the solution. When check procedure is satisfactory, AP will allocate memory space for this STA.
- When a node AP or STA sends de-authentication or disassociation frames, a current 3-bit unit is inserted into the frame, along with this a hash key H and the MSK is inserted into the unused bit positions of each frame and then it is moved forward the index to point to the next unit.
- If the random authentication bits from the incoming bits do not match with the corresponding bit stream unit on the receiver side, the incoming frame is rejected.

Performance evaluation: The proposed Secure Framework for DDoS Attack Detection and Defense (SFDADD) is evaluated through NS-2 1995 simulation. We consider a wired-wireless network deployed in an area of 500×500 m. The number of wireless nodes as 10 and no. of wired nodes as 2. The simulated traffic is CBR with UDP and TCP with FTP. The transmission rate is 250 kb.

The simulation topology is given in Fig. 5. The simulation settings are shown in Table 1.

Performance metrics: The performance of SFDADD is compared with the GIDA (Bedi *et al*., 2011) scheme. The performance is evaluated mainly, according to the following metrics.

Delay: It is the average time taken by the packets to reach the destination.

Table 1: Summarization of the simulation parameters

No. of nodes	12
Area size	500×500
Mac	802.11
Routing protocol	DSDV
Simulation time	20 sec
Traffic source	CBR and TCP
Packet size	512 bytes
Rate	250 kb
Transmission range	100 m
No. of flows	2, 4, 6, 8 and 10
Antenna	Omni antenna

Average packet delivery ratio: It is the ratio of the number of packets Received successfully and the total number of packets transmitted.

Packet drop: The number of packets dropped during the data transmission.

RESULTS

Based on flows (CBR): In our first experiment we vary the number of flows as 2, 4, 6, 8 and 10 for CBR traffic.

Figure 6 shows the delay of SFDADD and GIDA techniques for different number of nodes scenario. We can conclude that the delay of our proposed SFDADD approach has 59% of less than GIDA approach.

Figure 7 shows the delivery ratio of SFDADD and GIDA techniques for different number of nodes scenario. We can conclude that the delivery ratio of our proposed SFDADD approach has 37% of higher than GIDA approach.

Figure 8 shows the drop of SFDADD and GIDA techniques for different rate scenario. We can conclude that the drop of our proposed SFDADD approach has 67% of less than GIDA approach.

Based on flows (TCP): In our second experiment we vary the number of flows as 2, 4, 6, 8 and 10 for TCP traffic.

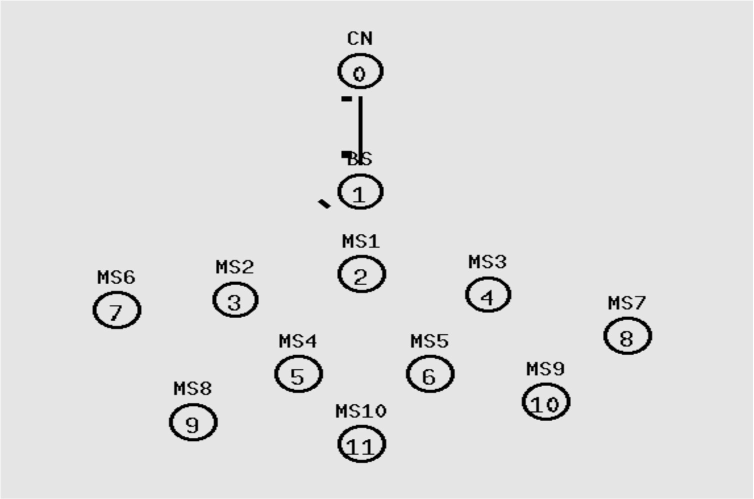

Fig. 5: Simulation topology

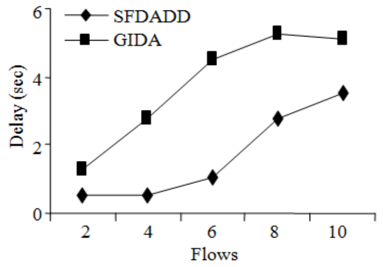

Fig. 6: Flows vs. delay (CBR)

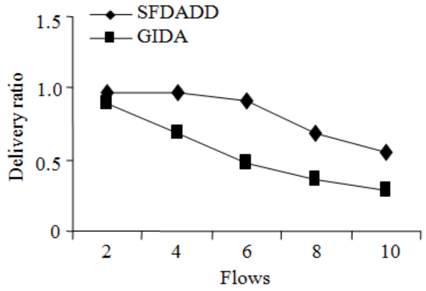

Fig. 7: Flows vs. delivery ratio (CBR)

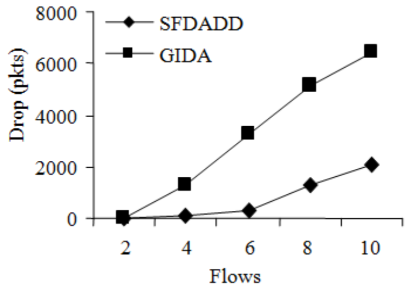

Fig. 8: Flows vs. drop (CBR)

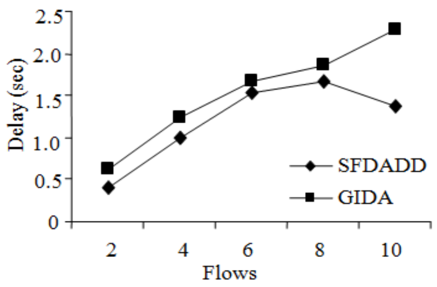

Fig. 9: Flows vs. delay (TCP)

Figure 9 shows the delay of SFDADD and GIDA techniques for different number of nodes scenario. We can conclude that the delay of our proposed SFDADD approach has 23% of less than GIDA approach.

Figure 10 shows the delivery ratio of SFDADD and GIDA techniques for different number of nodes scenario. We can conclude that the delivery ratio of our proposed SFDADD approach has 3.19% of higher than GIDA approach.

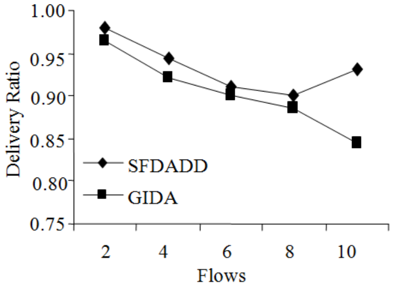

Fig. 10: Flows vs. delivery ratio (TCP)

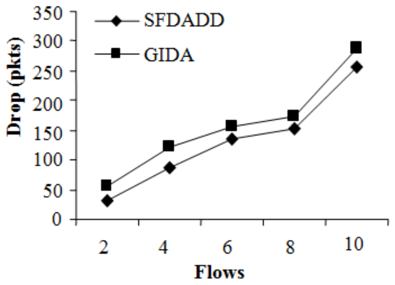

Fig. 11: Flows vs. drop (TCP)

Figure 11 shows the drop of SFDADD and GIDA techniques for different rate scenario. We can conclude that the drop of our proposed SFDADD approach has 21.4% of less than GIDA approach.

CONCLUSION

In our study we have proposed to design a detection and defense mechanism against DDoS attacks. Initially GIDA module is deployed, so that DDOS attack is detected using the game theory decision agent in the Access Point (AP). A Master Session Key (MSK) is calculated and a hash function is created for security. For the authentication and association of frames a client puzzle based defense mechanism is used in the AP. The client solves the puzzle which has been send by the AP. In the next phase, de-authentication or disassociation of frames of AP or client is by the random bit authentication mechanism. It inserts the current 3-bit unit into the unused bit positions of each frame and then advances the index to point to the next unit. The respective frames can be protected by the hash function and master session key. This framework provides a complete solution for the DDoS attacks targeted at both clients and AP.

REFERENCES

Anuradha and A. Singhrova, 2011. A host based intrusion detection system for DDoS attack in WLAN. Proceeding of the 2nd International Conference on Computer and Communication Technology (ICCCT, 2011). Allahabad, pp: 433-438.

Bedi, H.S., S. Roy and S. Shiva, 2011. Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows. Proceeding of the IEEE Symposium on Computational Intelligence in Cyber Security (CICS, 2011), Paris, pp: 129-136.

Gupta, B.B., M. Misra and R.C. Joshi, 2008. An ISP level solution to combat DDoS attacks using combined statistical based approach. Int. J. Inform. Assur. Secur., 3(2): 102-110.

Laishun, Z., Z. Minglei and G. Yuanbo, 2010. A client puzzle based defense mechanism to resist DoS attacks in WLAN. Proceeding of the International Forum on Information Technology and Applications (IFITA, 2010). Kunming, pp: 424-427.

Lee, Y.S., H.T. Chien and W.N. Tsai, 2009. Using random bit authentication to defend IEEE 802.11 DoS attacks. J. Inf. Sci. Eng., 25: 1485-1500.

Lina, Z. and Z. Dongzhao, 2009. A router-based technique to detect and defend against low-rate denial of service. Proceeding of the International Symposium on Web Information Systems and Applications (WISA' 09). Nanchang, P.R. China, May 22-24, pp: 257-260.

Liu, C. and J. Yu, 2007. A solution to WLAN authentication and association DoS attacks. Int. J. Comput. Sci., 34: 1-4.

Moorthy, M. and S. Sathiyabama, 2011. Hybrid fuzzy based intrusion detection system for wireless local area networks. Eur. J. Sci. Res., 53(3).

Salem, M., A. Sarhan and M.A. Bakr, 2007. A DOS attack intrusion detection and inhibition technique for wireless computer networks. ICGST-CNIR, 7(1).

Singh, R. and T.P. Sharma, 2011. Detecting and reducing the denial of service attacks in WLANs. Proceeding of the World Congress on Information and Communication Technologies (WICT). Mumbai, pp: 968-973.

Subramani, R., 2011. Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis. Retrieved from: http://www.sans.org/reading- room/whitepapers/ detection/denial- service-attacks- mitigation-techniques-real-time- implementation-detailed-analysi-33764.

Wu, Q., S. Shiva, S. Roy, C. Ellis and V. Datla, 2010. On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks. Proceeding of the Spring Simulation Multiconference Article No. 159. Society for Computer Simulation International, San Diego, CA, USA, ISBN: 978-1-4503-0069-8.

Zheng, X., C. Chen, C. Tser, H. Manton, M. Matthews and N. Santhapuri, 2005. A dual authentication protocol for IEEE 802.11 wireless LANs. Proceeding of the 2nd IEEE International Symposium on Wireless Communication Systems, pp: 1-5.