International Journal of Computer Networks and Communications Security

VOL. 5, NO. 12, DECEMBER 2017, 277–284
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Detection and Defense against Distributed Denial of Service Attack Using Packet Filtration in Wireless Sensor Networks

Tariq Ahamed Ahanger[1] and Abdullah Aljumah[2]

[1, 2] College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Saudi Arabia

[1]*t.ahanger@psau.edu.sa,* [2]*aljumah@psau.edu.sa*

ABSTRACT

Ranging from household to health to battlefield plays a significant role in many useful applications. Due to the distinctive feature of region and selforganizing, WSN (regarded as resource constraint type of network), is formed by a group of sensor nodes to detect physical phenomenon like light, heat, pressure with processing ability. Due to their resource constraint characteristics of limited memory and energy they are vulnerable to many cyber threats and attacks. The most common possible threat is DDoS. These attacks flood target with plentiful fake packets in order to drain the battery, prevent the genuine packets to pass thru and thwart the legitimate user to get the desired response. In this research article, we propose a detection and defense mechanism using packet filtration which deploys mitigation constraints to save the wireless sensor networks from the causes of DDoS.

Keywords: *DDoS, WSN, Cyber Attack.*

1 INTRODUCTION

The Wireless Sensor Network or WSN as it is used frequently are easy to adopt, easy to customize and easy to maintain solution. Their lower cost of implementation and effectiveness has made them more useful in Armed Forces, Industrial Manufacturing, and Terrestrial Monitoring and even in Personal Health care, but these same features of WSN has made them vulnerable to various security threats [1]. Different deployments requires different security standards and mechanism notably confidentiality, integrity and authentication which are prime requirement of their usability. Apart from a long list of internal attacks, DoS has been most widely used attack mechanism on WSN till now [2]. A possible reason for this is, DoS aims for subjugating services provided by WSN rather than sabotaging services infrastructure themselves. Which can be easily attained by victimizing network bandwidth, it's connectivity or its power supply. As sensor nodes are deployed at hazardous geographical and often difficult to access locations, DoS becomes most suitable attack mechanism for attackers [3].

Over the period of time attack mechanism and severity of attack has evolved from annoying to devastating. However as network infrastructure (Hardware, Software and routing protocols) has also made substantial development during course of time; DoS has diminished it strength to cause any significant damage to network performance and even some times fails to impart any detectable effect on network service of modern networks [4]. Subsequently an upgraded form of DoS is used to launch attack where more than one server takes part in attack. These attacks are highly coordinated, synchronized and coherent. These servers act as command and control center, they launch attack through a chain of compromised nodes which have been already overtaken without the knowledge of their owner viz. bots. This is known as Distributed Denial of Services or DDoS attack in short [5]. Although DDoS itself is quite capable of casting devastating effects, days by day advancement in computer science provide more sophistication in attack launch mechanism and give more camouflaging to attackers to avoid attack detections [6].

2 DDOS

Distributed Denial of Services attack is a powerful and devastating attack for the networks. A DDoS attack uses group of computers to launch fully coordinated denial of service attack as shown in figure 1 against single target or multiple targets simultaneously [7]. DDoS is performed or executed by overwhelming victim server with request messages thus consuming all or nearly all

of the available bandwidth depriving legitimate users from services or even downing the server to entertain any further request [8]. Few of the common approaches adapted and incorporated by DDoS attackers involve sending ICMP Echo Request for victims network, using victim's IP address as source of request which starts a storm of ICMP echo reply messages making this(victim) node saturated, this attack is called SMURF attack [9]. Similar to this, sometime attacker exploits TCP mechanism for making connection viz. TCP SYN, here attacking node sends repeated connection requests to target server while emulating its IP to some unreachable IP address as source of the request, target server on receiving these request responds with ACK and SYN of TCP suite to that unreachable address and consequently waits for ACK from that unreachable host, resulting into situation where server runs out of memory resources. Other types of attacks involve TCP, UDP and ICMP attacks, flooding the target machine with burst of messages requesting replies and thus clogging network [10].

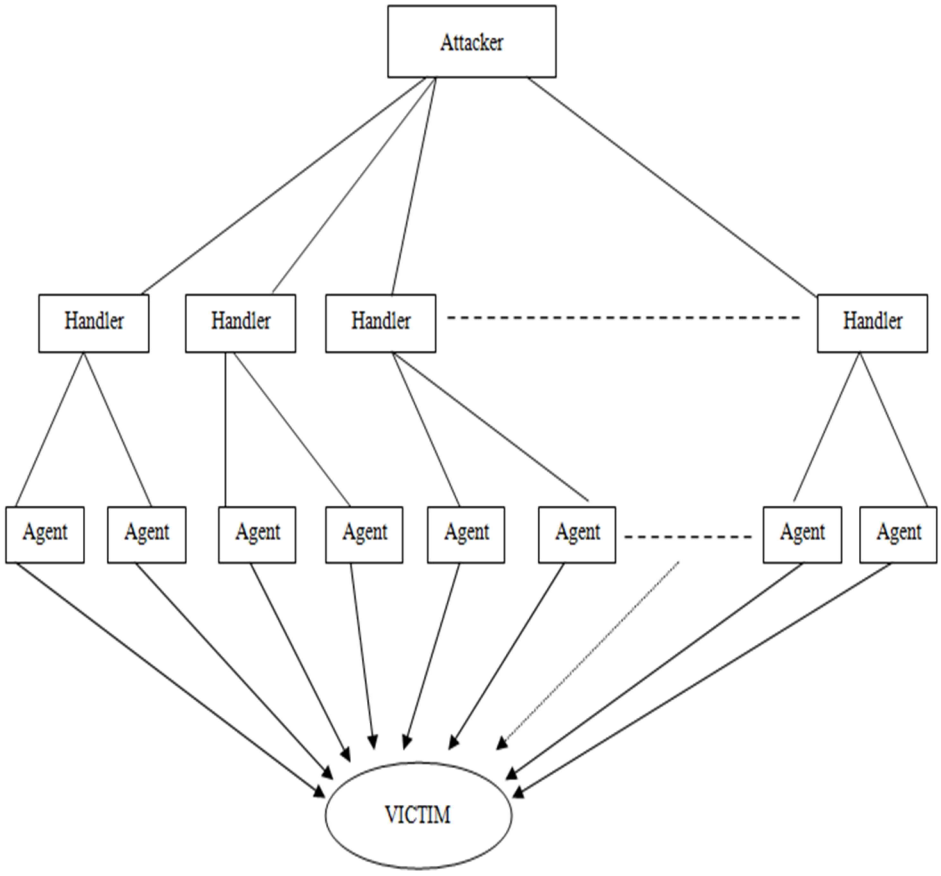


Fig. 1. Architecture of DDoS Attack

3 RELATED WORK

B. Mopari et.al.[11] has proposed a filtering technique against DDoS attacks by dropping fake packets. The authenticity of data packets is certified by evaluating the number of nodes (region) used by a data packet to reach its destination. A mapping table IP to Hop Count is created and learning state is used to scan the network to identify the fake data packets and discard the identified data packets using filtering state. In spite of the fact that Hop count filtering needs enough storage and in the end system can be deployed easily but the IP to Hop mapping table updating repeatedly after a selected threshold time can be weighty and more energy will be consumed by Time to Live communication.

Y Zhang et. al.[12] has proposed a model against DDoS that is based on marking packets. The routes that are attacked are market and by using the

information from the marked packets the affected routes are reconstructed. Then the packets are filtered by using the information from the attacked packets. The advantages include low cost, No extra storage is needed, low false alarm rate but the drawback is that if we want to trace the source of the attack then all the data packets that go through the router need to be marked.

Huey-Ing Liu et.al. [13] Has proposed a defense model against DDoS by examining the users' behavior to decide whether the user is fake or real. On the basis of users varying behavior different levels of services are provided. The model includes a filter, a scheduler and a rate limiter that are deployed in the system for reducing the malicious and intruder nodes. The throughput shows an enhanced throughput and the accuracy of detecting the intruders is high.

Yang-Seo Choi et.al. [14] has presented a general purpose methodology for detecting DDoS attacks. The basic characteristics of attack are analyzed along with their phases. An integrated defensive methodology is proposed that is required to mitigate every attack phase. Detecting the basic attacks is possible with method but of the amount of traffic in the network is huge then this method might fail to handle the data flood and rate of false negatives will be high.

Yu Chen et.al., [15] an effective framework is proposed to save the networks from DDoS attacks. A logical method of puzzle generator, verifier and resolver is incorporated. If an attack is identified in the network, a puzzle is generated by the puzzle generator to trace the victim and change aggregation tree is created. The puzzle verifier sends an identifier and a puzzle to the clients, and the solution of the puzzle found by the client is verified. The puzzle solvers job is to solve the puzzle. The proposed mechanism secures the established connections and makes it reliable for the client and server but the edge router have the chances to get affected by a DDoS attack.

4 PROPOSED FRAMEWORK

The main purpose of malicious nodes is to flood the target network in order to deny the services to the legitimate nodes provided by the nearest server or at least decline the quality of service by consuming battery, bandwidth etc. therefore, it is very important to detect them and once they are detected, the proposed mechanism will restrain their endeavor in declining the target and its action with abundant false packets.

We propose a filtering mechanism for traffic flow in wireless sensor networks having numerous nodes including genuine nodes, suspicious nodes and malicious nodes as well as shown in figure 2. The node in wireless sensor networks tend to send the packets to base station and legitimate nodes broadcast the data packet where as the malicious nodes will forward the data packets swiftly in shorter period of time.

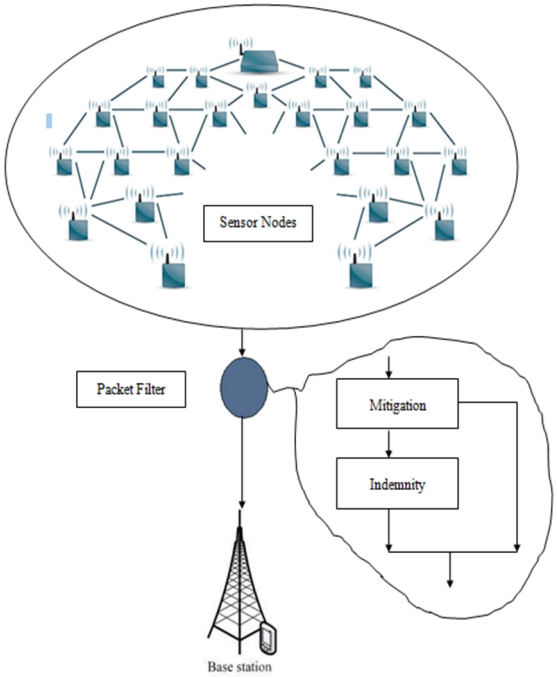


Fig. 2. Packet Filter in wireless sensor network

The unusual traffic rate is observed at the downstream layer and before forwarding these malicious and frequent data packets towards the base station, the traffic filter is invoked by intermediate node. The traffic filter has two parts: mitigation and indemnity. The DDoS will be restrained by mitigation part of traffic filter by determining the traffic rate of traffic flow. When the data traffic floods in enormous form within a short period of time, the traffic flow rate is declined by perceiving the potency of the flow. When the rate of data packets flow declines beneath a threshold value (certifies that the attackers have decreased their rate of traffic flow), the indemnity routine is invoked where they get an opportunity to transfer the data packets in a normal way.

This certifies that their rate of data transfer is raised. The data packets received from malicious node whose traffic is declined, the indemnited data packets (assuming them to have become normal)

and the data packets from legitimate nodes are forwarded towards the base station. After receiving all these packets, the base station responds after analyzing those data packets accordingly.

5 SIMULATION AND RESULTS

For simulation we adopted Castalia 3.2 for our proposed method as it suits best for our designed method because it can be used for WSN, BAN and most importantly for the networks that use low-energy embedded devices. Most of the researchers around the globe use this tool simulate and verify their distributed protocols and algos' in pragmatic models of radio and wireless channels with a practical conduct of node primarily to radio access [16]. The parameters used for simulation are described in table 1.

Table 1: Simulation Parameters

Parameters	Value
No. of Nodes	30
No. of Attackers	1-5
Simulation Time	300Sec
Deployment	6x6
X,Y	60,60

The function call flow between selected functions is shown in figure A, where the flow is shown using arrows i.e., Startup->Callback_TimerX<-> Network layer. The startup function is invoked and executed by every node once. The Callback_TimerX function gets invoked only when a specified timer expires. It transmits the data packets and are received by the network layer function.

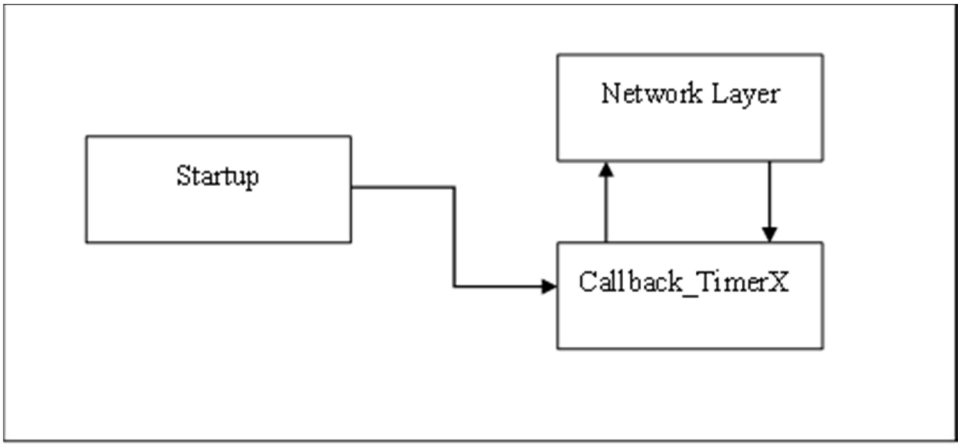


Fig. 2. Flow of Function calls

5.1 Startup

1. Initialization
   a. Int c=0;
   b. Boolean malicious=0;
   c. Flag=true;
2. Malicious nodes are separated from normal nodes using basic selected conditions.
3. Timer1 and Timer2 are set for malicious nodes and normal nodes respectively.

5.2 Callback_Timer

Timer1

1. Create packet and broadcast packet.
2. The timer is invoked after every 100ms.

Timer2

1. Create packet and broadcast packet.
2. If flag=false

2.1 Set timer3 to get invoked after every 15 sec.
2.2 Flag = True.
3. End If
4. Set timer2 to get invoked after every 20 seconds and keep changing this time duration after every transaction.

Timer3

1. The random value of timer2 is calculated mathematically so that the

genuine nodes can send their data packets in different amount of time.

2. Timer3's value is set to be invoked after 15Seconds repeatedly.

TimerX

In case a node finds an attacker node, it invokes this timer at a specific interval of time,"sntrt", that has been calculated by that node at network layer function itself.

The traffic flow broadcast is delayed by the node in TimerX by sending data packets at "sntrt" time interval as if the amount of data packets received by a node is from a malicious node is "x", then the rate of sending those data packets downstream will be decreased relatively to the value of "sntrt".

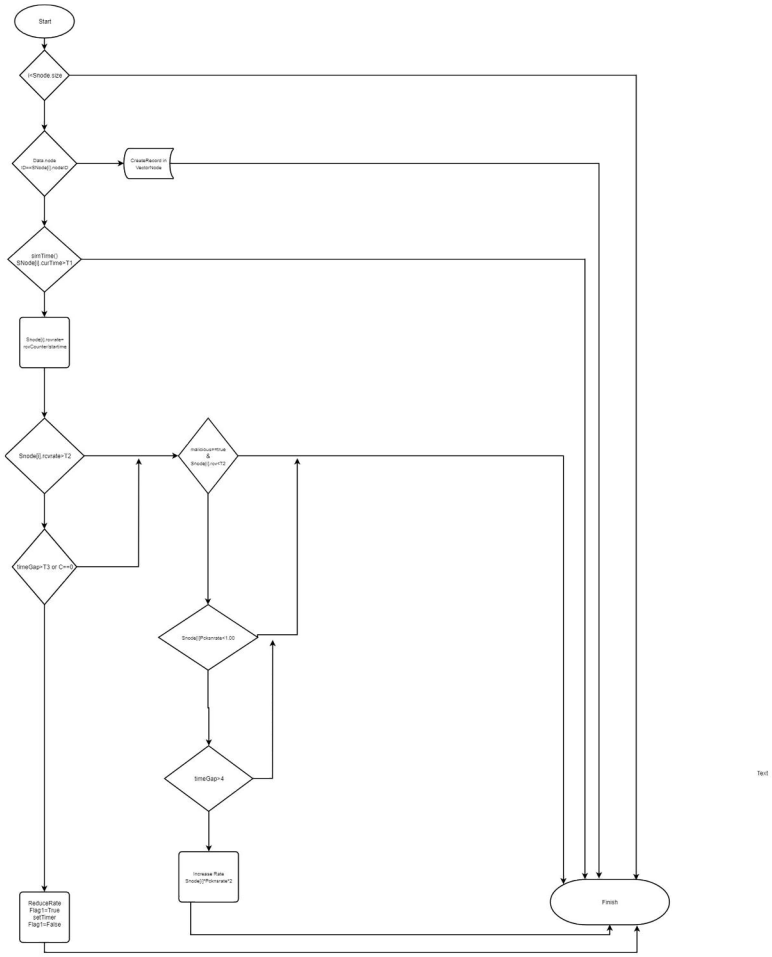
5.3 Network Layer

The flowchart and technique used in this section is shown in figure 3.A vector SNode is created with the parameters shown in table 2.

Table 2: Parameters for SNode

NID	*Node ID*
RevCounter	*Reset Counter*
Pcksntrate	*Packet Sent Rate*
Revrate	*Receive rate*
Curtime	*Current Time*
Srtrtime	*Start Time*
Suspicious	*Boolean Value*

Whenever a data packet is received by the network layer, its node ID is compared with node ID present vector. If the ID matches then 'present is set true as it certifies that a record has already been created for that packet. In case a data packet from a specific node arrives for the first time then the start and current time are kept same. If the time gap between the arrivals of the data packets is higher than the specified threshold value't1', then this data flood will not occur as the packets are not forwarded in an attack manner. Thus this source node is treated as genuine node otherwise it will be treated as suspicious node. The 'networklayer' function also calculates the rate at which data packets arrive from the intermediate node within a specified period time. If this rate of receiving data packets is higher than the specified value 't2', then the source node is declared as attacker and is treated as malicious node. In case, this happens for the first time from a specific node and the source is found to be attacker, then the packet sent rate received from this node is declined probabilistically. 'sntrt' is calculated and the value is sent to 'TimerX'. It mean that if data packet was sent previously in two seconds now it will take four seconds to send it again and this delaying will control the flooding in the data packet transmission. If the data packet sending rate declines then the receive rate will decline automatically and if receiving rate from particular node (attacker or malicious) declines below a certain threshold value then it will appear as normal in the network. After observing the behavior and receive rate from this node for a specified duration of time, packet sent rate is increased to cause indemnity. This certifies that if strangely behaving nodes (attacker/malicious) have declined their rate of packet sending for a greater period of time then their rate of packed sending is increased to allow them to transmit their data packets at a normal rate. This may also help a node in case it was wrongly considered as attacker or malicious one.



6 RESULTS

Case1: a network of 30 nodes is taken into account and 26 normal nodes and 4 malicious nodes which only send data packets rather than sending and receiving both. Collective values are recorded for every two nodes. The average value of data packets send and packets drop during the attack occurrence between normal nodes is shown in figure 4.

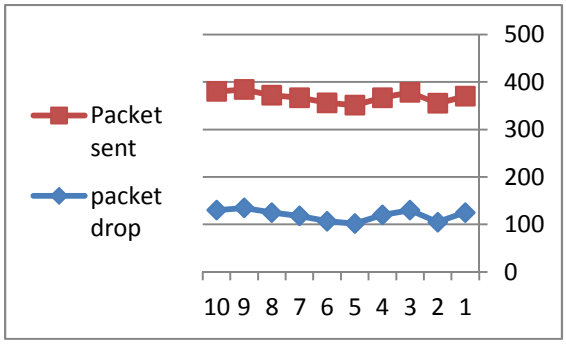


Fig. 4. Packet Sent v/s Packet Drop

The exact value of dropped packets is depicted by the deviation between the data packets sent and received by the nodes except malicious nodes. This is the first framework without applying our proposed mechanism. This result proved that the number data packets sent is greater than the number of data packets received. This difference is due to the presence of malicious nodes and due to the collision in the network as well.

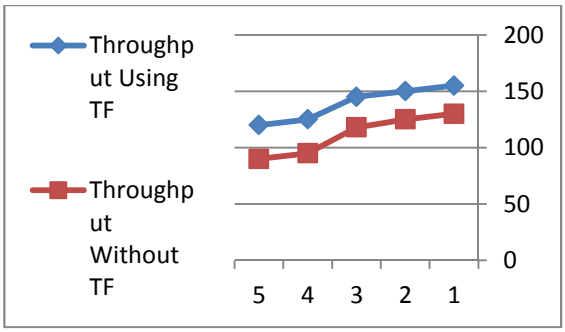


Fig. 5. Throughput Using TF v/s Throughput without Using TF

Case2: A network of 30 nodes in taken into account. Since the number of attackers change so does the throughput (No. of data packets received from legitimate nodes by the base station) at the base station. The throughput falls (when our mechanism is not adopted) when there is incline in the number of malicious node.

After we applied our method, the throughput was slightly higher than the values obtained without it as shown in figure 5.

Case3: the summation of number of data packets acquired by a node from the malicious nodes and the total number of data packets forwarded by that node towards node present in the downstream path of the network as shown in figure 6.

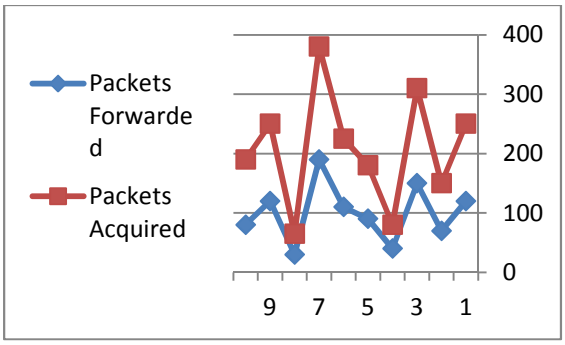


Fig. 6. Packet Forwarded v/s Packets Acquired

Ten nodes are selected randomly. The number of data packets transmitted by the hop nodes is almost half when applying our method as compared to the number of data packets received from attackers' side. These results proved that the rate of packets transmission is declined towards downwards. This in turn results in mitigation of data traffic from the malicious nodes.

7 CONCLUSION

DDoS attacks are prevailing in wireless sensor networks and are emerging as devastating threat. Therefore it requires more consciousness to subjugate the attack where the attack aims to flood the network and base station with abundant false packets. The nodes in the experimental study suing the proposed scheme were flooded with malicious and genuine packets which in turn flooded the base station and slow it down. As the rate of sending packets by the first hop nodes towards base station is declined resulting in the declined pace in receiving packets by the sensor nodes which are present in the lower layers and forward the same packets to the base station at a controlled rate. This certifies that the attackers attempt to flood the network is prevented. Once the base station collects the filtered packets, it responds accordingly after analyzing them. These results proved that the attempts of causing DDoS by attackers in the wireless sensor networks have been prevented. To make the method more effective and efficient node density can be used in the future to prevent packet loss and increase the probability of declining the DDoS attacks in wireless sensor networks.

8 ACKNOWLEDGEMENT

This research was funded and conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2016/2017.

9 REFERENCES

[1] Baroutis, Nikolaos, and Mohamed Younis. "Load-conscious maximization of base-station location privacy in wireless sensor networks." Computer Networks 124 (2017): 126-139.

[2] Rehan, Waqas,. "A comprehensive survey on multichannel routing in wireless sensor networks." Journal of Network and Computer Applications 95 (2017): 1-25.

[3] Puthal, Deepak, et al. "A dynamic prime number based efficient security mechanism for big sensing data streams." Journal of Computer and System Sciences 83.1 (2017)

[4] Tuna, G., Kogias, D.G., Gungor, V.C., Gezer, C., Taşkın, E. and Ayday, E., 2017. A survey on information security threats and solutions for machine to machine (M2M) communications. Journal of Parallel and Distributed Computing, 109, pp.142-154.

[5] Bhushan, B. and Sahoo, G., 2017. Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. Wireless Personal Communications, pp.1-41.

[6] Bang, J.H., Cho, Y.J. and Kang, K., 2017. Anomaly detection of network-initiated LTE signaling traffic in wireless sensor and actuator networks based on a Hidden semi-Markov Model. Computers & Security, 65, pp.108-120.

[7] Abdullah Aljumah, Tariq Ahamad,"A Novel Approach for Detecting DDoS using Artificial Neural Networks". International Journal of Computer Science and Network Security, 132 VOL.16 No.12, December 2016.

[8] Abdullah Aljumah, Tariq Ahamad,"Futuristic Method to Detect and Prevent Blackhole Attack in Wireless Sensor Networks",

International Journal of Computer Science and Network Security,VOL.17 No.2, February 2017

[9] Tariq Ahamed Ahanger," An Effective Approach of Detecting DDoS Using Artificial Neural Networks", IEEE international Conference on Wireless Communications, Signal Processing and Networking March 2017

[10] Ahamad T and Aljumah A . "Preventive mechanism against DDoS attacks in MANET". International Journal of Advanced and Applied Sciences, 4(5): 94-100, May 2017.

[11] B. Mopari, S. G. Pukale, M. L. Dhore," Detection and Defense against DDoS Attack with IP Spoofing", International Conference on Computing, Communication and Networking, IEEE,2008,pp. 1-5

[12] Yongping Zhang, Zhuqing Wan, Mingming Wu," An Active DDoS Defense Model Based on Packet Marking", Second International Workshop on Computer Science and Engineering, IEEE, 2009, pp. 35-38

[13] Huey-Ing Liu, Kuo-Chao Chang," Defending Systems against Tilt DDoS Attacks", 6th International Conference on Telecommunication Systems, Services, and Applications, IEEE, 2011,pp. 22-27

[14] Yang-Seo Choi, Jin-Tae Oh, Jong-Soo Jang," Integrated DDoS Attack Defense Infrastructure for Effective Attack Mitigation", 2nd International Conference on Information Technology Convergence and Services, IEEE, 2010, pp. 1-6

[15] Yu Chen, Wei-Shinn Ku, Kazuya Sakai, Christopher DeCruze,"A Novel DDoS Attack Defending Framework with Minimized Bilateral Damages", 7th IEEE Consumer Communications and Networking Conference, 2010, pp. 1-5.

[16] Zhang, Yongping, Zhuqing Wan and Mingming Wu. “An Active DDoS Defense Model Based on Packet Marking.” 2009 Second International Workshop on Computer Science and Engineering 1 (2009): 435-438.