A survey of Distributed Denial of Service attack

Mr.K.Narasimha Mallikarjunan
Assistant Professor
Computer Science and Engineering
Thiagarajar College of Engineering
Madurai
arjunkambaraj@tce.edu

K.Muthupriya
P.G Student
Computer Science and Engineering
Thiagarajar College of Engineering
Madurai
priya2631993@gmail.com

Dr.S.Mercy Shalinie
Associate Professor
Computer Science and Engineering
Thiagarajar College of Engineering
Madurai
shalinie@tce.ed

***Abstract*— Information security deals with a large number of subjects like spoofed message detection, audio processing, video surveillance and cyber-attack detections. However the biggest threat for the homeland security is cyber-attacks. Distributed Denial of Service attack is one among them. Interconnected systems such as database server, web server, cloud computing servers etc., are now under threads from network attackers. Denial of service is common attack in the internet which causes problem for both the user and the service providers. Distributed attack sources can be used to enlarge the attack in case of Distributed Denial of Service so that the effect of the attack will be high. Distributed Denial of Service attacks aims at exhausting the communication and computational power of the network by flooding the packets through the network and making malicious traffic in the network. In order to be an effective service the DDoS attack must be detected and mitigated quickly before the legitimate user access the attacker's target. The group of systems that is used to perform the DoS attack is known as the botnets. This paper introduces the overview of the state of art in DDoS attack detection strategies.**

Keywords—DDoS; botnets; UDP; TCP; server; resources.

I. INTRODUCTION

A Distributed denial of service (DDoS) attack is very simple to implement, but is a very powerful technique to attack the internet distributed systems. This type of attack can "unplug "the internet from the country. One such example is the incident that happened in Estonia in 2007 which unplugged the internet from the country. DDoS is considered to be the part of cyber warfare tactics [13]. But is often used for the purpose of Blackmailing and extortion. This DDoS attack can be implemented in both wired and wireless environment [1] by flooding the packets to a particular server to make it unresponsive. So that the legitimate users will not get any proper service from the server. DoS attack is an attempt to make a machine or network resources unavailable to its legitimate users, such as temporarily or indefinitely interrupt services of a host connected to the internet. DoS attack has become a growing problem over the last few years resulting in the increase of victims regarding the quality of services.

In DoS attack, the attacker who is known as a master zombie tries to control many systems and these systems are known as slave zombies. By using these slave zombies the master zombie tries to attack the system by flooding the packet. With the increased features in the technology the DDoS attack is very easy to implement. It can also be done using the automated tool [3]. By using this fast automated tool, if an attacker finds a system with very week security then he immediately attacks the system using the automated tool.

DoS attack not only attacks a system or a server it can also attack cloud environment [5]. DDoS is a major trouble to the available resources. In a cloud environment, the attackers can degrade the quality of service or breakdown the victims' connectivity. The attacker first tries to take control over many agents or systems and then uses these agents to perform the attack. The main intension here is to make the resource unavailable to the users. Mostly the target will be the web server, CPU storage and other network resources. In the cloud environment DDoS will reduce the performance of the cloud services by damaging the virtual servers [5].

The attacker will try to attack the system using the spoofed IP address, since he does not want to be identified and got caught by the defensive measures of the victim. Attacks can also occur in various other environments which can be analyzed using TCP Congestion Window Analysis [9]. In most of the methods DDoS Detection and mitigation methods deals only with detecting and identifying the attack no one concentrates on the IP trace back since it involves reflectors which is quite difficult to achieve. This reflector is used for storing the huge amount of traffic logs and regulated traffic during the attack. Reverse *iTrace* is the only existing method that will identify the IP but this method creates a large amount of traffic in the reflectors [23].

II. TYPES OF DDOS ATTACK

A. *Denial of sleep attack*

Denial of sleep attack aims at nodes power consumption. In this type of attack the adversaries have knowledge about the MAC layer protocol and it possess an ability to bypass authentication and encryption protocols. MAC layer protocol is especially designed for wireless sensor nodes for the purpose of saving battery power of the node by placing radio in low power modes [4]. When the node is not active MAC protocol has the ability to overcome radios primary sources of energy loss such as collision and control packet overhead.

B. UDP flood attack

User datagram protocol (UDP) is a deceptive protocol because information packets or request may arrive out of order, may appear to be duplicate or may be delayed. So the UDP allows the information and request to be sent to a server without requiring a response or acknowledgement that the request was received [4]. UDP protocols generate a larger bandwidth DDoS attack because they are connectionless and is easy to generate as it does not require any permission to transfer packets. This consist of messages larger than the normal size sent by the malicious node to target, consuming network bandwidth.

C. ICMP(Ping)flood

Internet Control Message Protocol (ICMP) is similar to UDP. ICMP Ping request continuously sends packets as fast as possible without expecting any replies. So that both incoming and the outgoing bandwidth will be increased leading to attack on the queue size of the ports

D. SYN flood

Here the attacker tries to send packets continuously to the server in order to prevent the connection being closed. During the connection period other systems will not be able to access the server this is one type of DDos attack [7]. In a spoofed SYN flood the attacker tries to send a huge amount of TCP SYN packets with a false IP address [10].

E. Ping Of Death(POD)

POD is a very old attack which is not a threat to the system anymore. The IP protocol consist of maximum allowances for packets sent between two machines. The maximum allowance under IPv4 is 65,535 bytes [19]. When a larger amount is sent exceeding the number then it will cause the receiving server to crash as it looks for the packet data larger than the maximum buffer size.

III. RELATED WORKS FOR DDOS DETECTION

A. Detection using Fast Entropy approach

Adaptive threshold algorithm is used to detect the DoS attack. In this method the traffic flow is continuously monitored and the flow count value at particular time interval is noted. The traffic flow is calculated for every channel. If the flow count value is high then there is an attack, entropy drops drastically, because there is one flow count that is dominating. But in case of normal flow the entropy will be in constant range.

This method is purely based on the packet header information. The header consist of the IPs of sender and the receiver and also the details of the flow of traffic so it doesn't care about the data in the flow. The attackers may try to send packets with less traffic flow from many systems so that the fast entropy method cannot identify this as an attack this is one of the disadvantage of this method. The result of the Fast Entropy Method is analyzed using the header information and then the attack is detected.

B. Detection using Naïve Bayesian classification method

Naïve Bayesian classification method uses feature selection as one of the important process for obtaining the minimal or non-predictable data from the available data sets. The data mining will contain a huge data about the network flow. Among the available data it is important to give priority to the data that is needed for detection and the data that is not necessary. The selection of the data is done using the following formula

$$Merit_{s_k} = \frac{kr_{cf}}{\sqrt{k + k(k-1)r_{ff}}}$$

Where,
k =Number of features in feature subset S
r_{cf} =Average of feature-classification correlations
r_{ff} =Average of feature-feature correlations
$Merit_{s_k}$ = Feature selected

By gathering all the information from the feature selection method Information gain is calculated this information gain is further used in the naïve Bayesian classification method. Bayes formula is used for detecting the attack in real time. Naïve Bayesian classification method will work better when combined with numeric to Binary data preprocessing.

C. Detection using Tennessee Eastman Challenge

This paper deals with the idea to maintain the security and stability of Networked critical Infrastructures (NCI). Due to the development of technologies in the recent times, the security for industrial equipment are exposed to intelligent cyber-attacks [2]. Since these equipment rely on networked systems which grant full access to the attacks and they disrupt the equipment. In this paper, they have chosen Tennessee Eastman Plant-wide challenge process (TEP) as representing as NCI controlled by an industrial control system (ICS).

The solution for the problem is approached with one of the data mining process which is clustering. TEP measured variables are grouped into 2 dimensional clusters. Clustering is done by Gaussian mixed model. This method helps in identifying the normal data and malicious data.

Thus by combining the measured variables and bi-dimensional plots, a global system is obtained. Later internal evaluation technique (Silhouette) is applied on the cluster. This emphasizes the outlier data points which are caused by attackers. Thus by clustering, the effects of DoS attacks can be identified efficiently.

D. Detection using TCP Congestion Window Analysis

In this method the detection is done using the TCP based flooding attacks by using TCP congestion window which is analyzed using the cumulative sum (CUSUM). Initially this method clears the victim traffic based on the criteria such as address, port or protocol. This method requires only less memory and computations while compared to other change point detection algorithm [9].

It is used for detecting a two sided function both the positive side and the negative side of the flow. After the analysis of the CUSUM value congestion window detection (CWCT) will be used to detect the attack. During the attack the congestion window will be affected while the CUSUM finds that the congestion window is affected it will immediately alert the CWDT about the attack. Here the attacker sends traffic as much as possible to exhaust the target machine and disrupt other machines from target. Due to heavy attack the congestion window will fail and stay at a low value. The slow start of the congestion window value will be one and decreases constantly on receiving a negative signal. By using the congestion window value the attack will be detected.

IV. CHARACTERISTICS OF DDOS

Implementation of the DDoS attack cannot be done using a single system or two [22]. Even though, when it is done with a single system the effect of the attack will not be much. In order to make adverse effects on the target system the attacker tries to make the attack more vulnerable. While using single system this is not possible so the attacker tries to control many systems by using their IP and then takes control over the systems. These systems which are under the control of one system is called as the zombies. The master system which controls all the other system is known as the master zombies. These collection of zombies together is known as the botnets.

The botnets are collectively malware infected machines which are remotely controlled and coordinated by a single entity. These botnets can be converted into digital weapon which involve cybercrime activities of attacking a system. Their life time may range from 1 day to 18 months [17] they all work on a single subnet in the internet. These botnets can also be created using the mobile nodes [24]. Due to the increased use of mobile the malwares can also be created using the mobile nodes these can be detected only using the android application since it is a mobile node.

The DoS attack is a network related threat and is a class of attack that makes the computer memory too busy or full to handle resources from other systems. This attack prevents the server from servicing its client and makes the legitimate users lose hope over the site or the server. During the DDoS attack the server will receive thousands of request at a time as a result the system memory will be filled and will not be able to handle any further request given by the client. When it receives more and more request the system will be not responding sometimes the system will be shut down for certain amount of time. The shutdown may last from few seconds to hours based on the effect of the attack.

In the Denial of sleep attack the case is different while a node is not transferring any packets it will be in inactive mode in order to save power of the node. When the security system is very week intruders try to attack these systems by sending unwanted packets through the inactive node and make them to lose power [6]. As a result the nodes will lose the power due to the flooding of packets through them and when the legitimate users tries to use these systems they will be shut down due to low power. These are the effects of flooding packets in Denial of sleep attack. Intrusion Detection System will help in identifying the behavior of these attacks [18].

With increased features in the technology the DDoS attack has become very easy to implement and their effects are much worse than before. In wireless sensor nodes the behavior of the attack is very different [11]. On the basis of this it is understood that the DDoS attack will react differently in different systems. In the case of Wireless sensor nodes the attack must be faster this is also known as black hole attack [25]. So it has become an important issue to detect these attacks and mitigate them. In order to bring more effective solution the attack must be detected before it affects our system.

V. MITIGATION OF DDOS ATTACK

In DDoS attacks the main aim is to identify the attack and rectify them effectively. DDoS attack happens because of flooding the packets to the victim machine. Here, the legitimate users may also try to send large number of packets they must also be considered and service must be provided for them. Some of the methods that are used for the mitigation purpose are

A. Fuzzy Estimator Approach

In this approach, the denial of service attack is detected during the runtime of the attack. In the previous existing systems attack was identified only after its effect is felt. But in this approach the DoS attack is identified before it affects the system [13]. The fuzzy estimator is used on the network traffic to identify weather a DoS attack has taken place and to identify the suspect participating the host. Here the identification of the attack is based on the packet arrival interval and the number of packets sent. In fuzzy estimator the maximum amount of packet the server or system can accept will be set prior. If the amount of packets received exceeds the maximum number then this will be considered as an attack. The packets from the particular server will be dropped immediately. The main disadvantage of this work is that the identification of false positives. That is when a legitimate users tries to send a maximum amount of packets then he will also be considered as an attacker.

B. Mitigation using Multivariate Correlation Analysis(MCA)

MCA-Based analysis method used anomaly based detection in recognition of the attack. This helps in detecting of the known and unknown DDoS attacks effectively by learning the patterns of legitimate network traffic. The distinction between a new incoming traffic record and the respective normal profile is investigated by the proposed detection scheme. The traffic record is flagged as an attack when the distinctive value is above a pre-determined threshold value [16].

If lesser than the threshold traffic then it is labeled as a legitimate traffic record. Obviously, normal profiles and thresholds have candid impact on the performance of a threshold-based detector. A low quality normal profile causes an inaccurate characterization to legitimate network traffic.

A proposed triangle area-based MCA approach to analyze legitimate network traffic is applied and generated Triangular Area MCAs (TAMs) are then used to supply quality features for normal profile generation. Triangle area based MCA technique and the anomaly based detection technique has been the astonishing factor for MCA-based DoS attack detection system. More precise characterization for network traffic deeds are analyzed using geometrical correlations concealed in discrete pairs of two distinct features within each network traffic record quoted from the former techniques [14]. Both known and unknown DoS attacks are differentiated from the legalize network traffic by means of latter technique facilities.

The efficacy and performance of the proposed detection scheme to mitigate DoS attack is evaluated using KDD Cup 99 dataset. The results have revealed that when working with non-normalized data, this detection system achieves maximum95.20% detection accuracy although it does not work well in identifying Land, Neptune and Teardrop attack records.

This issue can be addressed by utilizing statistical normalization technique to eliminate the bias from the data. The results of computing with the normalized data have produced a more reassuring detection accuracy of 99.95% and almost 100.00% DRs for the different kinds of DoS attacks. Moreover, the comparison assessment has recognized that our detection system achieves two state-of-the-art approaches in terms of detection accuracy. Detection techniques for real data in the world and retain more comfortable techniques for classification are considered as future enhancement.

C. *Stone Method*

In this approach a new method called as STONE is used for the mitigation purpose. Here, Vincenzo Gulisano developed STONE machines separately which can run STONE algorithm and is connected to other machines for detecting and mitigating DDoS attack. It can be used for the purpose of protecting both single host and multiple host [15]. The work of the STONE system is to monitor the network, to detect the possible attack and to filter the traffic when it exceeds the maximum threshold bandwidth. Detection Control Center (DCC) is used here to detect the suspicious traffic in the system.

DCC information is used for identify the attack characteristics and the tolerance level of a system by using this basic information the attack detection is done and further the solution for mitigating is given by the Mitigation Center (MC) [15]. The MC filtering protocol is used for discarding the packets that is with the high load and bandwidth. In case of legitimate users if the load is very high then the packets will be monitored and then dropped. This is how the STONE approach works.

D. *Mitigation using Active Queue Management (AQM) method*

In this AQM method Deterministic fair sharing method is used to identify the false positives [12].

The AQM method works on identifying the malicious network flow and to ensure least damage to the legitimate flows, it should drop all the identified malicious packets while protecting the legitimate flows. It should not detect a legitimate flow as a malicious flow and should be able to find the difference between the various flows for this purpose DFS is used. DFS performs a set of operation before it receives or accepts the packets using the ENQUE and DEQUE functions.

The DFS maintains a series of attributes based on the flow of the network by using these information the attack detection is done. In some cases the packets might be initially identified as a legitimate flow and after the acceptance it may change to a malicious flow. So the DFS is designed in a careful way to identify these attacks. If the DFS finds the malicious flow of then it immediately drops all the packets from that particular flow.

VI. LIMITATIONS OF EXSISTING METHODS

Based on the survey done (Table1) differentiating the normal traffic from attack traffic and identifying them correctly with negligible false positives has to be implemented.

VII. PROPOSED METHOD

Detection of the false positives and rectifying them in a proper manner can be done by predicting the attackers behavior and the different ways in which the can try to make the attack. Behavior of the attacker is obtained from the historic data. For example larger bandwidth data, spoofed IP address, bottle neck bandwidth, data flow size, type of congestion window.

And identifying the difference between the low rate and high rate traffic flow in the network and then mitigating them in a proper way in order to avoid the DDoS attack and protect the system from its adverse effects.

Fig1: Prediction Overview

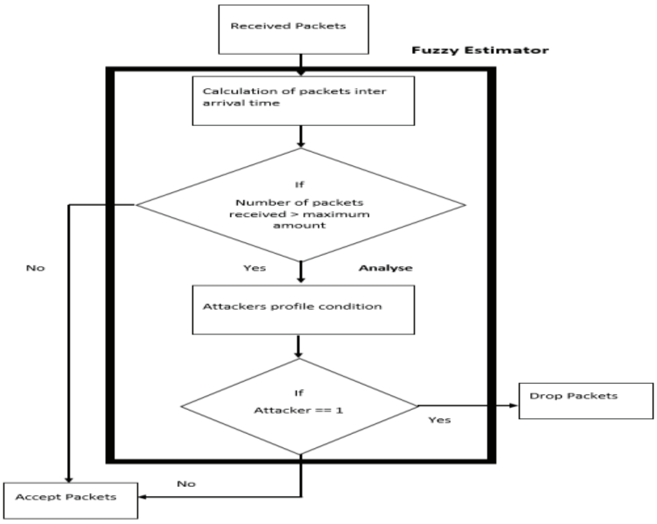
Received Packets
Fuzzy Estimator
Calculation of packets inter arrival time
If
Number of packets received > maximum amount
No
Yes
Analyse
Attackers profile condition
If
Attacker == 1
Yes
Drop Packets
No
Accept Packets

Table1:Existing method for Detection and Mitigation of DDos

Schemes	**Detection / Mitigation**	**Simulation tool**	**Publication year**	**Results**
Fast Entropy Approach (Jisadavid, Cizathomas, 2015)	Detection	Trin00	2015	Adaptive threshold algorithm is used to monitor the continuous flow of network. Since the Detection is based on the header details of the packet IP Spoof detection has to be considered as the source and destination could be forged.
Naive Bayesian Classification Method (Vijay, et al, 2013)	Detection	Weka Tool	2013	This uses feature selection method to filter the available data to give priority. This may lead to loss of data since the data is aggregated together and classified.
Tennessee Eastman Challenge (Istvan Kiss, et al, 2015)	Detection	Java	2015	Clustering of TEP measured variables are grouped into 2 dimensional clusters is done by Gaussian mixed model. This method helps in identifying the normal data and malicious data. It is graph based technique Where system is considered ad power node. But in real time network this assumption is hard to be satisfied as the load of the system keeps varying.
Congestion Window Analysis (Mohammed Alenezi, et al, 2013)	Detection	Ns-2	2013	CUSUM analyses the network traffic in congestion window and Detects the attack based on the congestion value. Since the congestion window value is dependent on the number of participating systems the value has to be calculated for each packet transfer.
Fuzzy Estimator (Stavros, et al, 2012)	Detection and Mitigation	TCP dump log analyzer	2012	Packet arrival interval and number of packet received is used for detection of attack. Here legitimate users with large number of packets are identified as an attacker since they carry a heavy network traffic.
Multivariate Correlation Analysis (Zhiyuan Tian, et al, 2013)	Detection and Mitigation	glomosim	2013	Detection technique for real data in the world. Since it learns from the real data and all normal traffic data signatures must be stored which is hard to predict.
Stone method (Vincenzo, et al, 2015)	Detection and Mitigation		2015	Data control center and the Stone system identifies and mitigates the traffic. Here initial installation cost is high as a separate system is needed to monitor and the probability of monitoring system being attacked is pretty high.
Active queue management (AQM) (Harkeerat Bedi, et al 2013)	Detection and Mitigation		2013	Effectively monitors incoming and outgoing packets. Since Queue management needs to monitor Enque and Deque the detection time and memory utilization is large.

In this proposed method when the packets are received it check the packet arrival interval. After verifying the packet arrival interval it checks weather the number of packets received is greater than the number of packets sent. If this condition is satisfied then it will immediately drop the packets since the number of packets received is greater than the number of packets sent. If the initial condition is not satisfied the packet enters the predictive profiling method in which the attacker prediction is done. During this prediction the above mentioned condition will be checked, if any one of the condition is satisfied then he will be identified as an attacker.

VIII. CONCLUSION

On surveying and analyzing the various DDoS attack detection and mitigation schemes we have come to a conclusion that the DDoS attack has a very great threat to the shared and internet distributed systems and it is important to protect our system from such kinds of attacks. Even though there are a lot of solution for detection and mitigating of the DDoS attack the major drawback in all the system is that the system detects the legitimate users with large bandwidth of data as an attacker.

Since this is a passive attack it is very important to identify the attack before it affects our system.

IX. REFERENCES

[1] Ashish Patil,Rahul Gaikwad, ”Comparative analysis of the Prevention Techniques of Denial of Service attacks in Wireless Mesh Network, “in ICCC, vol.48,Bhubaneswar,2015,pp.387-393.

[2] Istvan Kiss, Piroska Haller,Adela Beres, ”Denial of Service attack Detection in case of Tennessee Eastman challenge process, “ 8th INTER-ENG 2014, vol.19,Romania,2015,pp.835-841.

[3] Jisa David,Ciza Thomas, ”DDoS Detection using Fast Entropy Approach on Flow Based Network Traffic, “ 2nd International Symposium on Big Data and cloud computing(ISBCC’ 15), vol.50,2015,pp.30-36.

[4] Kiattikul Treseangrat, Samad Salehi Kolahi,Bahman Sarrafpour,”Analysis of UDP DDoS cyber Flood Attack and Defence Mechanism on Windows Serevr 2012 and Linux Ubuntu 13, “in IEEE,2015.

[5] Rashmi V. Deshmukh, Kailas K. Devadkar, ”Understanding the DDoS attack & its Effects In Cloud Environment, “in ICAC3-15, vol.49,2015,pp.202-210.

[6] Vijay D.Katkar, Deepti S.Bhatia, “Lightweight approach for the denial of service attacks using numeric to binary preprocessing, “in International conference on Circuit, System, Communication and Information Technology Application(CSCITA), in IEEE 2014.

[7] Paul c. Hershey, Charles B.Silio, ”Procedure for detection of and response to Distributed Denial of Service Cyber-attack on complex enterprise systems, “in IEEE 2012.

[8] Vijay D.Katkar,Mr.Siddhant Vijay Kulkarni, “Experiments on Detection of Denial of Service attacks using Naïve Bayesian Classifier, “ in IEEE 2013.

[9] Mohammed Alenezi, Martin J.Reed, ”Denial of Service Through TCP Congestion Window Analysis, “in World congress on Internet Security,2013,pp.145-150.

[10] J.Sathya priya, M.Ramkrishnan, S.P. Rajagopalan, “Detection of DDoS attacks using IP Traceback and Network Coding Technique, “ in journal of theoritical and applied Information Technology,chennai,2014,pp.99-106.

[11] Michael riecker, Daniel Thies, Matthias Hollick, “Measuring the Impact of Denial of Service attack on Wireless Sensor Networks, “in IEEE conference,Germany,2014,pp.296-304.

[12] Harkeerat Bedi, Sankardas Roy, Sajjan Shiva, “Mitigating Congestion-Based Denial of Service Attacks with Active Queue Management, “in IEEE,2013,pp.1440-1445.

[13] Starvos N.Shiaeles, Vasilios Katos, Alexandros S.Karakos, Basil K.Papadopoulos, “Real time DDoS stection using Fuzzy estimators, “in Elsevier Computer and Security,vol.13,2012,pp.782-790.

[14] Yongdong Wu, Zhigang Zhao, Feng Bao, Robert H.Deng, “Software Puzzle: A Countermeasure to Resource-Inflated Denial of Service attacks, “ in IEEE Transactions on Information Forensics and security,vol.10,2015,pp.168-177.

[15] Vincenzo Gulisano, Mar Callau-Zori, Zhang Fu, Ricardo Jimenez-Peris, Marina Papatriantafilou, Marta Patino-Martinez, “STONE:A Streaming DDoS defense framework, “in elsevier Expert system with application,vol.42,2015,pp.9620-9633.

[16] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu, “A System for Denial of Service Attack Detection Based on Multivariate Correlation Analysis, “ in IEEE Transactions on parallel and distributed system,2013.

[17] Olivier THONNARD, Wim MEES, marc DACIER, “Behaviour Analysis of Zombie Armies, “ in Symantech Research Labs,France.

[18] Omar Al-Jarrah, Ahmad Arafat, “Network intrusion Detection System using attack Behaviour classification, “ in IEEE International Conference on Information and Communication Systems,2014.

[19] Jaipal Singh Parihar, Jitendra Singh Rathore, Kzvita Burse, “Agent Based intrusion Detection Sytem to find Layers Attack, “in IEEE International conference on Communication Systems and Network Technologies, 2014,pp.685-689.

[20] Sumit Pote,Ashis nikalaje, Rahul Bhalerao,Prashant Gade, Kunal halkandar, “Low rate DoS attack detection Mechanism, “Asian Journal of Engineering and technology Innovation,vol.6,2015,pp.60-64.

[21] Munish Dhar, Rajeshwar Singh, “A Review of Security Issues and Denial of Service Attacks in Wireless Sensor Networks, “in International Journal of Computer Science and Information Technology Reasearch,vol.3,2015,pp.27-33.

[22] Jamal Raiyn, “A Survey of Cyber attack Detection Startegies, ”in International Journal of Security and its application,Isreal,vol.8,pp.247-256.

[23] S.Saurabh, A.S.Sairam, “ICMP based IP traceback with negligible overhead for highly distributed reflector attack using bloom filters, “in Elsevier Computer communication,vol.42,2014,pp.60-69.

[24] Liberios Vokorokos, Pavol Drienik, Olympia Fortotira, Ján Hurtuk, “Abusing mobile devices for Denial of Service attacks, “ in IEEE, Slavokia,2015,pp.21-24.

[25] Michael Riecker, Daniel Thies and Matthias Hollick, “Measuring the Impact of Denial of Service attack in wireless Sensor nodes, “in 39th annual IEEE conference on Local Computer Networks,2014,pp.296-304.