###### INVENTION DISCLOSURE FORM

**Client Asset Reference: Date:**

**Use the following guidelines while filling out the form:**

* Please provide as much detailed information about the technology as possible, citing all relevant sponsorship and publication information.
* Please give a schematic diagrams / drawings or images relating to the invention or the disclosure to be made by you. This will assist FORMULATEIP to technically understand and rewrite the specifications, as may be required. If you are using a particular software format for the production of the drawing, please do attach the e-copy of the drawing together with the name of the specific software used to develop the same.
* Please state the names of competitors and similar products in the domain.
* Please give references of any document that you may have referred to during the phase of invention and development. A detailed bibliography of the reference material, with details of any existing or expired patents relating to the said invention or development, would assist in a more efficient process for protection and commercialization of your invention and development.

**1. TITLE OF INVENTION (Please indicate a title for the invention and technology of the invention)**

A System and Method to Prevent DDoS TCP Flood Attack using Virtual Layer in Wireless Sensor Network.

**2. LIST OF KEYWORDS PERTAINING TO THE INVENTION (Please list five to ten keywords that cover your invention or technology)**

Denial of Service (DoS), Distributed Denial of Service (DDoS), TCP Flood Attack, Threshold based detection, Virtual Layer.

**3. PRIOR METHODS, APPARATUS, DEVELOPMENTS AND PUBLICATIONS (What are the problems addressed by your proposal and how may it be approached according to present knowledge?)**

Wireless Sensor Networks (WSN) is a growing and emerging technology used in many applications such as health care system, environmental monitoring system, military application, etc. The sensors in the network gather the environmental data such as temperature, motion, pressure etc , healthcare data such as Heart beat rate, blood pressure, sugar level etc, The sensed data are forwarded to the gateway node where the data are aggregated and send to the centralized control system or Internet. The gateway node is also able to receive the information from centralized control system and send them to sensors and react on behalf of the commander/user. Therefore the reliability and availability of the gateway node are most important in the wireless sensor network. But the denial-of-service attacker attempts to exhaust the gateway's resources such as bandwidth, processing capacity, storage etc. by sending huge unwanted traffic to gateway node. By doing so, the attacker makes the gateway node to prevent the legitimate nodes from accessing the resources or degrade the services provided by gateway node. Hence the gateway of WSN becomes greater risk. Another one denial-of-service called distributed denial-of-service attack is a large-scale attack which launches the many DoS attacks directly or indirectly in the distributed manner. When a WSN is being targeted, the huge amount of essential data is being shut down, and the whole process is prevented from its regular scheduled state. The DDoS attack takes large number of compromised nodes in a network to flood the gateway node simultaneously from multiple places. This kind of attacks is unpredictable and leads to deadly consequences.

Gateway

Node 4

Attacker

 Node 3

 Node 1

 Attacker

 Node 2

 Cloud Service

 Machines / Victim

Figure 1 DDoS in a WSN System

To defend the gateway against DDoS attack, traffic control mechanism such as filtering and rate limiter is used. Filtering technique is most popularly used to prevent the gateway from DDoS attack and unaware attackers. This technique ensures that the legitimate traffic can get access to the gateway. Ingress filtering technique filters the malicious traffic destined to a local network and prevents the traffic with spoofed IP [ferguson]. The ingress filtering allows the traffic to enter into the network by matching with the predefined range of domain prefix of the network. Egress filtering drops the malicious traffic leaving a local network. The effectiveness of filtering techniques depends on global deployment of filtering in the WSN which is difficult. RFC 1812 proposes an address filtering technique that filters the spoofed IP addresses generated from a limited set of addresses. It does not forward any packet with an invalid source or destination IP address. For example, it does not allow the packets with the destination IP address 255.255.255.255/32 and discards them. In [tao], history based IP filtering technique is proposed to protect from DDoS attack. The history of the normal traffic is used to filter out the malicious traffic. The victim node maintains a database of IP addresses that are commonly known IP address or determined as legitimate users. When a bandwidth of victim node is overwhelmed by the unwanted traffic generated by the attacker, the victim node only allows the traffic from the IP addresses available in the database and all other IP packets are discarded. However, if an attacker can simulate its attack traffic as a normal traffic, this filtering technique cannot successfully detect and discard the malicious flow

Rate limiter is a another DDoS prevention mechanism that controls the date rate in the link of a victim by controlling the traffic in the link. Wei et al propose a mechanism that monitors the traffic pattern in the network and assign the normal users to a high priority queue and suspected attackers to a low priority queue. In this mechanism, it takes the interval of transmission time of the incoming packet to distinguish the normal user and malicious user. The time interval is to be small enough for classifying the users otherwise the malicious user is assigned with high priority queue [wei]. Rate limiter is suitable for the attacks having high data rate on a link but not suitable for the attacks with low data rate [Kejie].The rate limiting techniques are very simple and easy to understand also but it is hard to set up proper threshold values for detecting the attacks [sang].

An attractive alternative approach to prevent DDoS attacks is honeypot which can protect the network while consuming less resource. A honeypot pretends to be normal servers and receives the all unwanted traffic from the attackers and drop them. [wang][dimi][wang]. But the attacker uses anti-honeypot to identify and detect the honeypot that acts like a normal server. The anti-honeypot detects the honeypot proxy server in the network by transmitting the probe packets. Once the honeypot server is identified, the attackers bypass the honeypot and access to the victim node through other channels [Krawetz]. In [Natalie], a cluster of physical honeypot servers are implemented that mimic the activities of real servers. Every physical server needs a separate honeypot which results in wastage of resources and high maintenance costs. Vinu et al proposes a prevention mechanism to mitigate the denial of service attacks in which every production server is hidden behind the active server that acts as gateway to the production server. The legitimate traffic is passed to the production server whereas the malicious traffic are halted at active server itself. This solution is robust and secure but it slow down the processing of requests for production servers since each and every request needs to pass through an additional active server. Moreover, separate honeypot servers for each production server wastes resources and is quite expensive [Vinu][Hrishikesh].

The gateway node of the wireless sensor network collects the data from the all sensors and performs the data aggregation and sends the result to the centralized control system. The sensed data may be health care data, environmental data or domain specific data such as military application. Among the various type of attacks in these applications, DDoS is a typical attack that severely threatens availability of the communication network resources and affects the proper execution of the network. It makes the resource inaccessible for legitimate users. Therefore, we propose a prevention mechanism using virtual layer that is set in the gateway node of the wireless sensor network. The packets from both legitimate sensor node and malicious sensor node are received by the virtual layer before being processed by the gateway. The virtual layer comprises of three components: Attack Detection (AD), Attack Information Management (AIM), and Attack Prevention (AP). The attack detection uses two techniques to detect the DDoS attack ie Threshold based and History based. Attack Information Management maintains three log files: one file stores the details of incoming packets, second file maintains the details about number of incoming packets within the time interval from an IP, and third file maintains the history of attacks.

Huge number of requests from a particular IP within a limited period of time, which satisfies the Attack Qualifier Condition (AQC) is marked suspicious. A general attack vector is created from these requests which are then compared with the DCAP (DDos captured attack pattern database), If the attack pattern is similar to that of the stored data, those IP addresses are marked Malicious preventing any further transaction towards that IP.

**4. DESCRIPTION OF THE INVENTION (Please describe specifically and in detail what you consider the invention to be with a working example. Kindly attach drawings, reports, papers, charts or other materials that may aid in better understanding of your description. Software-related inventions should be supported with flow charts.)**

The overview of proposed mechanism is shown in Fig. 2. A virtual layer is created on the gateway node to prevent the DDoS attack. Any interactions with the gateway have to pass through attack detection component of virtual layer. The attack detection method checks the incoming packets to know whether the packets are from attacker based on threshold limit allotted to each user and the history of attack. In this project, we consider three different way of DDoS attack that are

1. Attacker uses its own bots/machines to generate the unwanted traffic
2. Attacker uses a fake IP addresses generated by multiple bots to generate unwanted traffic
3. Attacker steals the IP address of a legitimate user and pretends like a legitimate user and generates the unwanted traffic.

**Request from attacker**

**Request from legitimate user**

**Filtered Requests**

**A1**

**A2**

**An**

**U1**

**U2**

**Un**

**VIRTUAL LAYER**

**GATEWAY**

**DDoS Attackers**

**Legitimate Users**

**Responses to the user**

**Attack Detection**

**Attack**

**Prevention**

**Attack Information Management**

Fig. 2 Architecture of proposed method

Therefore the gateway node doesn’t know which one of the ways is used by the attacker to generate the unwanted traffic. The threshold and history based attack detection method determines it and update the attack information management for future reference. Further if the attacker spoofs the IP address of legitimate user, the gateway node cannot ignore the particular IP address because it belongs to legitimate user. Hence in the proposed method, the particular IP address is banned for a limited time. Banning an IP address that belong to a legitimate user for a limited time would not be a noticable issue comparable with damage caused by the attackers. In the proposed system, the gateway node is hidden behind the virtual layer, the gateway node is protected from DDoS attack. The attack prevention method cuts the connection between the virtual layer and gateway node to prevent any data being stolen or lost or any resource being exhausted. The connection is temporarily terminated and the connection is refreshed after a time period. Even the connection is refreshed after a time period, the IP address is marked as blacklist in the tables maintained in the AIM.

**A. Identify the general purposes of the invention.**

The purpose of the proposed invention is related to the procedure of the gateway in the WSN and in particular it is a system and a method for preventing the DDos TCP flood attack using virtual layer in the gateway of WSN

**B. Include all essential features, their relationship to each other and their mode of operation (along with drawings).**

**C. Identify and describe all elements/components that are considered novel and inventive.**

A system and method that prevents the DDoS attack happening at the gateway of wireless sensor network is proposed here. Accordingly the proposed invention comprises the following steps,

1. Detecting the DDos attack using a threshold and history of attack.
2. Maintaining the details of incoming packets and history of attack
3. Preventing the DDoS attack by blocking the requested service to attackers

Accordingly the method of protecting the gateway of WSN from the DDos attack is performed.

**Attack Detection Method**

A log file is created, which stores information regarding the requests that contains the Time Interval, Source IP (SIP), and Destination IP (DIP). A flow identifier is created where Fn is the request flow from the host. A node could manage only a limited number of requests, to protect the system from over loading we set a threshold value for the number for requests that could be processed at a moment. If the incoming requests qualify the Attack qualifier condition (ACQ), then the flow is marked suspicious which would include all the IP addresses in that particular time interval. A new log file is derived from the data, which contains the suspicious flows including the above parameters.

1. Create a log file in which the number of the incoming requests say N, which is to be compared to the attacks detected in the previous stage where the data are stored in DCAP (DDos captured attack pattern database), that logs the source IP, destination IP and the time interval.
2. Let Fn = { f1, f2 , ………, fn} be the flow identifier, and fn be the request flow from the host, where n = { 1, 2, 3………}. The flow fn may have N number of requests to the server.
3. Let R be the total number of requests obtained from all the flow identifiers within the threshold time T.
4. Let Ts be the threshold value which determines the maximum number of requests that can be handled by the server AQC = R(1/TS)
5. If the AQC (Attack qualifier condition) > 1 then all the flow will be considered as a suspicious attack flow.

Incoming requests

Information Log

AQC Check

Gateway

Mark suspicious

Derive Log file

Flow Comparison

**No**

**Yes**

Figure Attack Detection Method

**Attack Information Management**

Once the new log file is derived, which contains the information such as Source IP (SIP), Destination IP (DIP), Time interval; Number of requests, three new fields are added to the log file namely Suspicious Requests, Attack Conformation and Blacklist Log. This information is compared with the Dataset to process the detection and prevention mechanism.

1. Calculate the similarity measure E using Normalized Absolute Distance between the GAV and FV using Eqn(1):

|  |  |
| --- | --- |
| E=[(GAV)-(FV)]/FV |  |

1. If E > T\_GAV, then it is an Attack. Else it is not an attack
2. If E > T\_GAV, then determine the similarity measure S between FV and different attack signatures A1,…..An stored in DCAP using formula in Eqn (2):

E=[(GAV)-(FV)]/FV

NO

YES

Suspicious Flow

Derived Log

Attack Conformation

Black List

Allow Connection

Prevention System

Figure Attack Information Management

**Attack Prevention Method**

A new Feature Vector is created using the information gathered from the log file, These (FV) Feature Vector is compared with the (GAV) General Attack Vector derived from the (DCAP) DDoS Capture Attack Pattern. The Similarity measure is estimated using the below algorithm, while if E>T\_GAV (Threshold – GAV) ranging from (0-1) the flow contains attack, Thus all the incoming requests from that flow is denied access.

9. If E&gt;T\_GAV, where T is the maximum threshold lying between 0 to 1, then the flow

contains DDOS attack. Else there is no DDos attack in the flow.

10. Update the logfile by setting the ADS(attacks detected). If ADS is set to Y then the

SIP(source ip) are considered blacklist.

11. If E&lt;1 then do not terminate the program, else if E&gt;1 terminate the program, ban the

connection for the source ip(SIP) for temporary time (T t ) , wherer T\_GAV = (0 to 1).

12. Create a logfile of the entire activity, and input new data() for the upcoming process.

Attack Detected

Block IP addresses in the Flow

Allow connection

Update Blacklist Log

Figure Prevention Flow Chart

**5**. **NOVELTY OF THE PRESENT INVENTION (What are the aspects of your disclosure that you want to claim/monopolize?)**

We claim

1. A hardware embeddable system for preventing the DDoS attack comprising of a method that runs inside the hardware.
2. The method as claimed in claim 1 further comprising:
   1. Detection of DDoS attack using threshold based and history based.
   2. Maintaining the details of incoming packets and history of attack
   3. Preventing the DDoS attack by blocking the requested service to attackers

**6. ADVANTAGES OVER OTHER KNOWN ALTERNATIVES** (Please identify the advantages or benefits e.g. efficiency, cost benefit, simplicity, how does your present invention overcome the defects of currently available technologies.)

DDos Prevention Mechanism using a vitrual layer stands of the huge advantage in wiress sensor network. The proposed method uses a temperory time ban on Flow containing DDOS attack pattern which would include all IP addresses, this enables a legitimmate user to use the service after the ban time incase their IP was a part of the flow containg attack signature. Every event and activities are logged into a file which could be used for the further invistigation about DDoS attack. However, short time ban on a legitimate user would be risky, since it results in inconvineance of a legitimate user in some real time system but it is acceptable considering the fact that the security of the netwotk and data should be given highest priority for large networks and service providers. Incase if the server is unable to handle the attack, the system goes offline from the virtual network .The major disadvantage would be that the legitimate user incase bets a ban time out, will not be able to use the service ustil the ban have been lifted. But considering the priority of any large serviec provider its okay to ben an user if found suspesious and later making up to it justifying the reason for ban.

**7. CURRENT DEVELOPMENT STATUS OF YOUR INVENTION**

**A. Has your invention been put to practice? Has any prototype been made on this invention? If yes, kindly provide relevant information.**

Yes. The invention is ready for practice. The invention is tested in the presence of DDoS attack in WSN.

**B. Is further development of your invention necessary or development of invention is in progress, or scheduled?**

No.

**8. POTENTIAL LICENSEES**

**A. What are the different possible commercial applications of your invention? Where do you see the biggest market need for a product/service based on the invention?**

Wireless sensor networks used for pollution monitoring, healthcare monitoring, quality monitoring, environmental monitoring etc which deploys the gateway node to forward the sensed data to the centralized control system.

**B. What industrial sector(s) or firm(s) do you assume to have an interest in your invention and why?**

All the hardware/software development companies who are developing Mechine-To-Mechine (M2M) communication can use this invention because it provides preventive measure against the DDoS attack in wireless sensor network.

**9. DISCLOSURE (PUBLICATIONS/PRESENTATIONS/AND OTHER FORMS OF PUBLIC COMMUNICATION)**

Please identify all past and future seminars, discussions, abstracts, journal publications, conference proceedings, industry meetings, seminars, and web postings describing the invention.

Wei-Shen Lai, Chu-Hsing Lin , Jung-Chun Liu , Hsun-Chi Huang, Tsung-Che Yang: Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks, International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008)

Kejie Lu, Dapeng Wu, Jieyan Fan, SinisaTodorovic, Antonio Nucci, “Robust and efficient detection of DDoS attacks for large-scale internet”, Computer Networks, Vol. 51 (2007), pp. 5036–5056.

Sang Min Lee, Dong SeongKimb, Je Hak Lee, Jong Sou Park, “Detection of DDoS attacks using optimized traffic matrix”, Computers and Mathematics with Applications, Vol. 63 (2012), pp. 501–510

Ferguson, "Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing", RFC 2827

Tao Peng Christopher Leckie Kotagiri Ramamohanarao, " Protection from Distributed Denial of Service Attacks Using History-based IP Filtering",

K. Wang, L. Yuan, T. Miyazhaki, S. Guo, and Y. Sun, “Antieavesdropping with selfish jamming in wireless networks: A Bertrand game approach,” IEEE Trans. Veh. Technol., to be published, doi: 10.1109/TVT.2016.2639827.

C. K. Dimitriadis, “Improving mobile core network security with honeynets,” IEEE Security Privacy, vol. 5, no. 4, pp. 40–47, Jul./Aug. 2007.

K. Wang and M. Wu, “Nash equilibrium of node cooperation based on metamodel for MANETs,” J. Inf. Sci. Eng., vol. 28, no. 2, pp. 317–333, 2012. [19] N. Provos, “A virtual honeypot framework,” in Proc. 13th USENIX Security Symp., San Diego, CA, USA, 2004, p. 1.

N. Krawetz, “Anti-honeypot technology,” IEEE Security Privacy, vol. 2, no. 1, pp. 76–79, Jan./Feb. 2004

Natalie Weiler, “ Honeypots for distributed denial-of-service attacks”, Proceedings of Eleventh IEEE International Worksops on Enabling Technologies, 2002.

Vinu V. Das, “Honeypot Scheme for Distributed Denial-of-Service”, Proceedings of the 2009 International Conference on Advanced Computer Control, January 2009, pp. 497-501.

Hrishikesh Arun Deshpande, “HoneyMesh: Preventing Distributed Denial of Service Attacks using Virtualized Honeypots”, International Journal of Engineering Research & Technology, Vol. 4(8), 2015, pp. 263-267.

**10. INVENTOR(S) AND/OR CONTRIBUTOR(S):**

|  |  |  |  |
| --- | --- | --- | --- |
|  | INVENTOR (1) |  | INVENTOR (2) |
| Signature: |  |  |  |
| Name: | A. Jeyasekar |  |  |
| Address: | Associate Professor/CSE, FET,  SRM IST, Kattankulathur |  |  |
| City and State: | Chennai, Tamilnadu |  |  |
| Citizenship  (Country): | Indian |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | INVENTOR (3) |  | INVENTOR (4) |
| Signature: |  |  |  |
| Name: |  |  |  |
| Address: |  |  |  |
| City and State: |  |  |  |
| Citizenship  (Country): | Indian |  |  |

**11. ASSIGNMENT DETAILS: Assignee is the entity or individual who holds the patent.**

|  |  |
| --- | --- |
| Signature: (To be signed by the authorized signatory on behalf of the assignee) |  |
| Name of the Authorized Signatory and Designation |  |
| Address: |  |
| City and State: |  |
| Citizenship  (Country): |  |