1. **Search the novelty of the Project:**

There isn’t any project specific on using a virtual network to prevent a DDos attack, however there is one project related to this topic which is on intrusion detection patented via Google. As mentioned it’s only a related topic and has no data correlation to our proposal

1. **Title of Invention:**

Prevention of DDos TCP flood attack using virtual layer in wireless sensor network.

1. **List of key words pertaining to the invention:**

DDos, Threshold based detection, TCP flood attack, virtual layer.

1. **Identify general purpose of invention:**

The WSN is subjected to many attacks, due to its broadcasting nature of the networks. It has a wide application in military, health care and to gather data and transmit them, this makes them vulnerable to many attacks due to its high reliability and relatively less security in data transmission. But the denial-of-service attacker attempts to exhaust the victim’s resources such as bandwidth, processing capacity, storage etc. by sending huge unwanted traffic to victim node. By doing so, the attacker makes the victim node to prevent the legitimate nodes from accessing the resources or degrade the services provided by victim node. Hence the network/gateways become greater risk. A 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 victim nodes simultaneously from multiple places. This kind of attacks is unpredictable and leads to deadly consequences.

DDos attacks occur due to the failure of nodes due to malicious triggered actions. In Dos attacks, the resource available at the victim node are not meant to perform that activity. Various types of attacks occur i.e. jamming, tampering exhaustion, collision etc.

As the wireless sensor is growing fast, the position of security to the sensor node is difficult. However, the prevention of the DDos should not degrade the system instead it should maintain the accuracy of the data. A false alarm would only lead to waste of time and resource, thus they should be minimized. The system should be strong enough to survive multiple attacks on a same node and try to counter those attacks.

Path based DOS attack is based on SYN flood messages, the packets is traversed in longest path and causes these types of attacks. There are attacks which drains the power by consuming a huge amount of power on a single node. Vampire attacks are one of such which exhausts the power of the system, forcing it to deny service to other nodes and eventually reducing the efficiency.

We propose a prevention mechanism against the DDoS TCP Flood attack that uses a threshold-based attack detection and prevention mechanism. The proposed mechanism is set on a two Raspberry Pi v3 and few virtual machines of a victim and user node i.e. gateway so that the service requests generated by the attackers are not allowed to the gateway.

1. **Description of the invention:**

A virtual layer is created on a gateway of WSN to prevent the DDoS attack. Any interactions with the gateway have to pass through virtual layer. The attack detection mechanism is plugged in the virtual node to detect the incoming DDoS attack depending upon the threshold limit allotted to each user. We consider three different way of spamming the service requests that are,

1. Attacker uses its own bots/machines to spam service requests
2. Attacker uses a fake IP addresses generated by multiple bots to spam the service requests
3. Attacker steals the IP address of a legitimate user to spam the service requests. Similar to detection mechanism, the prevention mechanism is also integrated with the virtual node.

The prevention mechanism cuts the connection between the virtual layer and WSN 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 in blacklist node.

**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**

**Detection**

**Prevention**

**Log information comparison and updation**

A virtual layer is created on a server to prevent the DDoS attack.

Any interactions with the gateway have to pass through virtual layer.

The attack detection mechanism is plugged in the virtual layer to detect the incoming DDoS attack depending upon the threshold limit allotted to each user.

we consider three different way of spamming the service requests that are

1. Attacker uses its own bots/machines to spam service requests.

2. Attacker uses a fake IP addresses generated by multiple bots to spam the service requests.

3. Attacker steals the IP address of a legitimate user to spam the service requests.

Similar to detection mechanism, the prevention mechanism is also integrated with the virtual node.

The prevention mechanism cuts the connection between the virtual node and gateway 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 in blacklist node

1. **Identify the general purpose 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.

1. **Include essential features and their relationship to each other:**

In a DDoS flood attack the gateway is flooded with IP traffic by the attacker. A huge volume of packets sent by the attacker to the gateway system slows it down, crashes the system or saturates the network bandwidth which prevents any legitimate wireless sensor node from accessing the gateway of wireless sensor network.

There are several other DDos Attacks which shuts down an entire network, such as Smurf Attacks, Fraggle Attacks, Protocol Exploit Attacks, TCP SYN Attacks PUSH + ACK Attacks, Malformed Packet Attacks etc.

1. **Identify and describe all the elements that are considered novel and inventive:**

A system and method of preventing the DDos attack happened at the gateway of a wireless sensor network is proposed here. Accordingly the proposed invention comprises the following steps,

1. Detection of DDos attack.
2. Log file Updation.
3. Prevention of DDos.

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

1. Detection of DDos attack:

The incoming Requests are recorded in a log file A, with essential parameters such as Source IP, Destination IP, Time Interval.

Another log file B is created with the data derived from the previous log file, which consists of two additional parameters such as suspicious flow and attack detected.

Those requests that cross the threshold limit will be marked as suspicious flow in the log file B. These requests are to be compared with the DCAP (DDos captured attack pattern database), if the suspicious flow is qualifies the condition AQC (attack qualifier condition)

then those requests are marked as Positive in log file B under attack detected.

1. Log file updation:

Co-FAIS is an imnuse system for the Dos attacks in WSN which uses six different modules.

Which consist of Sniffer Module, Fuzzy Misuse Detector module, Danger Detector Module, Fuzzy Q-learning Vaccination Module,Cooperative Decision making Module and Response Module.

The snffer module collects the packets from the network which is then sent to the Fuzzy misuse module, these collected logs are stored in a log file.

The Fuzzy base module identifies the malicious packets which are suspected to be harmful to the system.It compares the packets with the nonrmal packers which seams to cross the threshold value.

It works based on various factors such as CPU usage, Connection numbers, Bandwidth saturation etc.

If an attack is detected then the collected information is saved in as a log file to identify any future incoming attacks.

The Q-learning tool learns about the attack and collects valuable resource about the attack.

The consolidate results and analysis of attack source are given by the cooperative decision making module

To make prevention faster an attack signature is produced.

1. Prevention of DDos:

ADOVS and DSR,

The DDos attacks in the network is don ebased on the energy monitoring of different nodes in the network.

It cross checks the energy source of each node and when the node hits either low threshold level or the higher threshold level the system alerts.

Once its conformed to be an attack, the prevention system is invoked.

All nodes in the network will black list the nodes thats supposed to be under attack.

These nodes are further shut down, preventing any energy flow to them.

1. **Novelty of the present invention:**

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 claim1. Further comprising.
3. Detection of DDos attack.
4. Log file updation.
5. Prevention of DDos.
6. **Advantages over other known alternative:**

Prevention of the DDos. Usage of a Virtual network. Preventing permanent ban on an address. Log of data for further investigation. Preventing Data loss or steal.. Recovery phase added.

1. **Current development status of your invention:**
2. Has your invention been put to practice?

Yes the invention is ready for the practice. The invention is based in the presence of DDos attack in WSN.

1. **Reference:**
2. AQEEL SAHI, DAVID LAI, YAN LIAND MOHAMMED, An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment (DIYKH)

2. .B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, ``DDoS attack protection in the era of cloud computing and software-de ned networking,'' Comput. Netw., vol. 81, pp. 308 319, Apr. 2015.

1. (DEFCON, The SHMOO Group, 2011. (http://cctf. shmoo.com/).
2. Harendra Tripathi, Raksha Upadhyay, Salman Khan, Uma Rathore Bhatt, “Detection and prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain”, Department of Electronics &Telecommunication, Institute of Engineering & Technology.
3. Devi Ahilya University, Indore -452017, India.

6. K. Kendall, A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems, Master’s The-sis, MIT, 1999.

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

8. LORI L. DELOOZE, Applying soft computing techniques to intrusion detection, Applying soft computing techniques to intrusion detection, University of Colorado at Colorado Springs Colorado Springs, CO, USA ©2005.

9. Monowar H. Bhuyan, Dhruba K. Bhattacharyya, and Jugal K. Kalita,Towards generating real life Datasets for network intrusion detection May 9, 2015 (International Journal of Network Security.

10. Nathalie Weiler. “Honeypots for Distributed Denial of Service”, Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops, 2002. pp. 109-114. 2002.

11. Neeta sharma , Mayank singh , Anuranjan Mirsha, Prevention against DDos attack using triple pass filter 2016 (International Conference on Computing for Sustainable Global Development).

12. Paul J. Criscuolo. “Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, And Stacheldraht CIAC-2319”. Department of Energy Computer Incident Advisory Capability (CIAC), UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, February 14, 2000.

13. P. E. Ayres, H. Sun, H. J. Chao, and W. C. Lau, ``ALPi: A DDoS defense system for high-speed networks,'' IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1864 1876, Oct. 2006.

14. Saman Taghavi Zargar, Member, IEEE, James Joshi, Member, IEEE, and David Tipper, Senior Member, IEEE, A Survey of Defense Mechanisms Against Distributed Denial of Service (Ddos) Flooding attacks.

15. Sang Min Lee a , Dong Seong Kimb,c,∗ , Je Hak Lee a , Jong Sou Park,Detection of Ddos attacks using optimized traffic matrix (science direct 2012).

16. Sang Min Lee, Dong Seong Kimb, 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.

17. Sangita Chaudhari, Shital Patil, “Dos attack prevention technique in Wireless Sensor Network”, 7th International Conference on Communication, Computing and Virtualization 2016.

18. Stephen Specht. Ruby Lee sspecht@princeton.edu rblee@princeton.edu. Department of Electrical Engineering. Taxonomies of Distributed Denial of Service. Networks, Attacks, Tools, and Countermeasures. Princeton Architecture Laboratory for Multimedia and Security. Technical Report CE-L2003-03.

19. Sunny Behal, Krishan Kumar,Trends in Validations of Ddos Research, International Conference on Computational Modeling and Security (CMS 2016).

20. V. Jacobson, C. Leres, and S. McCanne, “The tcpdump manual page,” Lawrence Berkeley Laboratory, Berkeley, CA, 1989.

21. Wei Zhou, Weijia Jia, Sheng Wen, Yang Xiang, Wanlei Zhou, “Detection and defense of application-layer DDoS attacks in backbone web traffic”, Future generation computer system, Vol. 38(2014), pp. 36-46.

**THEORY :**

Considering all different cases, we have come up with a solution.

1. We don’t know in whick of these three cases the attacker spams the service requests from .
2. We simply cannot ignore an IP address that beongs to legitimate user.
3. We cannot affort our network being attacked.
4. Banning an IP address that belong to a legitimate user for a limited time would not be a noticable issue.

PACKET SOURCE

BLACKLIST

IP’S

DETECTION SYSTEM

NO

PROCESS YES

CLASSIFIER

ITS LEGITIMATE REQUESTS

FORWARD PACKETS TO PREVENTION

TRIGER ALERT

PREVENTION SYSTEM

PROCESS

BLACKLIST LOGS

PACKET TERMINATION

FORWARD PACKETS

PROVIDE SERVICE

GATEWAY

VIRTUAL LAYER

Figure 1Proposed system

Hear we are creating a virtual layer that would eventually act as a decoy to prevent the DDos attacks.

Any interactions with the real system will have to pass through the virtual layer, which would give us an instinct when the actual system would come under attack.

**Intergrate a DDos Detection mechanism with the virtual network:**

In this stage, we plug in a Detection mechanism in the virtual network the was created. This part of the network is responsible to detect the incoming attacks depending upon the threshold limit alloted to each user. This would further allow the system to take preventive measures.

The above diagram shows the architecture of the proposed system in which detection and the prevention process are included. The major process of the proposed system is Detection, Prevention and Recovery phase.

**Taking a preventive measure against the DDos attacks:**

Once the attack have been detected by the virtual network, immediately the preventive measures are toggled by the system. There are more than one way in which this could work since there are 3 different cases that an attacker might spam requests.

Similar to the detection mechanism, this is also intergrated with the virtual network.Since we would not be able to predict on which one of the above mentioned cases the attacker would initiate, we would block any requests that exceeds a threshold limits.

Considering the possiblity that the attacker uses a legitimate users IP address, it would be impossible to block a address permanently. This leads us to set a ban time on a pirticular set of IP addresses, later sending an notification that such suspecious activity was found from their respective IP addresses.

This would enable the user to tighten their security and possible give a good insight on the attacker of further invistigation was processed.

On this point, the connection between the virtual network and the Actual netowrk is cut preventing any data being stolen or data loss.

However, this is a case that is highly unlikely to happen and in case this happens the priority of keeping the data safe than that of running the service without an interruption comes first.

Here, we realise that there might be cases that the attack is going out of hands and the prevention mechanish set in the virtual network can no longer with hold the pressure.

Thus the connection between the virtual and the Actual network would eventually be cut until the virtual network is refreshed.

**Prevention phase:**

When the packets reach the prevention system, they are considered to be attacking packets by the detection sub-system. The prevention subsystem alerts the system administrator of the attacks. Then, the prevention sub-system will add the attacking source address to the attacker blacklist used by the detection sub-system, if it is not already on the list. Finally, the attacking packet will be dropped. By the detection sub-system, if it is not already on the list. Finally, the attacking packet will be dropped.

PREVENTION SYSTEM

SUSPISIOUS ACTIVITY / MAX THRESHOLD REACHED

TIME BAN

SAVE ACTIVITY LOGS

REFRESH

BLACK LIST IP ADDRESS

ANALYSE DATA PACKETS AND SERVICE REQUESTS

CHECK LEGITIMATE USER

PROVIDE SERVICE

Legitimate or not

YES

NO

Figure 2Prevention system

**Recovery phase:**

The connection between the virtual network and the Actual netowrk is terminated preventing any data being stolen or data loss, which also prevents any damage to the hardware caused by the Attack.However, this is a case that is highly unlikely to happen and in case this happens the priority of keeping the data safe than that of running the service without an interruption comes first.

The termination of connection between the gateway and the virtual layer occurs only when the attack is going out of hands and the prevention mechanish set in the virtual network can no longer with hold the pressure and protect the system.

Figure 7 RECOVERY PHASE

GATEWAY

GATEWAY

OVER LOAD

PROCESS DATA PACKETS

PREVENTION PHASE

SAVE ACTIVITY LOG

SHUT DOWN VIRTUAL LAYER

 RE-INITIATE TASKS

 GENERATE REPORT

DETECTION PHASE

Virtual layer

**NO**

**YES**

Thus the connection between the virtual and the Actual network would eventually be cut until the virtual network is refreshed. This would result in a temperory delay in service but the hardware and data are safe and enough time is bought to counter further incoming attacks.

Prevention of the DDos attacks using a vitrual network layer stands of the huge advantage of the proposal. The system uses a temperory time ban on suspected addresses which enables a legitimmate user to use the service after the ban time. Every event and activity have been logged into a file which could be used for the further invistigation process. This prevents any sort of data loss or steal over the gateway. However, short time ban on a legitimate user would be risky, but that’s okay since the protection of the data stands as the first priority for large networks and service providers. Sometimes, the system have to be taken down offline from the virtual network if the attack couldn’t be handled by the vitrual node.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.

**Experimental Setup:**

Customized hardware’s could be used to setup various attacks over a network. Hardwires like raspberry PI allows the user to setup custom operating functional platforms and perform various activities. Being ridiculously portable and efficiency these could be used to generate multiple service requests and target a vulnerable networks. Advanced network tools with the right hardware could be deadly when used offencive. Below is a DDos attack generation setup using a Raspberry PI.

A wire less attackk card, command and control wireless cards, suitable operating system, ethernet cable, power supply, a USB keyboard are few basic requirments to setup a attack.

Raspberry pi/ Attacker Node

 Wireless card

 Power Supply

DDos Generating algorithm

 Target network

 Virtual Node

Gateway

Legitimate Requests

Response

 Power Supply

Node 1 sensor 1

Node 2 sensor 2

Node n sensor n

USERS

Gateway node