IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-18, May 2019 E-ISSN: 2347-2693

DPDOS: A New Heuristic to Detect and Prevent Distributed Denial of Service Attack Present in Vanet

Shalini Priya[1], Koyel Roy[2], Ira Nath[3*], Dharmpal Singh[4]

[1, 2, 3, 4]JIS College of Engineering, Kalyani, Nadia, West Bengal, India

Corresponding Author: ira.nath@gmail.com, Mobile no.:9475697514

Available online at: www.ijcseonline.org

***Abstract*—** Increasing number of vehicles in utilize has conducted in the service to supply human and resource security. The present trend calls for the application of technology to automate safety measures in road traffic and since has been known as Intelligent Transport System (ITS). Vehicular Ad hoc Network is like a fork to Mobile Ad hoc Network, where the nodes are mobile vehicles moving in constrained road topology. VANET networks are visualized to be utilized in practical ITS systems around the world. A network standard has been grown as Wireless Access In Vehicular Environment (IEEE 802.11p) to be utilized in VANET which is an alteration to IEEE 802.11 standard. With each innovative technical applications particularly computers and network appliances, come novel safety challenges. Each network in present time is vulnerable to safety attacks and VANET is not the exception. The most notorious attack among all is the Distributed Denial of Service Attack which is obvious as unlike other safety attacks the data packets utilized in it are genuine and authorized packets. In this paper, a novel offensive measure for detection and prevention has been proposed.

***Keywords*—** VANET, Ad-hoc, ITS, Mobile and DoS.

I. INTRODUCTION [1-5]

Vehicular ad hoc network is a communication network for vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications developed mainly for establishing an Intelligent Transport System (ITS) in road traffic for the intention of avoidance of accident, post-accident inquiry, lessening of traffic jams and other non-security functions. There are three basic components of VANET communication i.e. On board unit (OBU), Road side unit (RSU) and Application unit (AU).

The development of Intelligent Transportation System (ITS) has made a big step in recent years and shortly it has become very popular. The important application of (ITS) is called as VANET. To improve road safety and driving conditions, an unplanned network is formed by vehicles on the road spontaneously is called as Vehicular Ad-hoc Network (VANET). In VANET, driving safety is enhanced via inter-vehicle communication or communication with roadside units. Hence it is also called as a vehicular sensor network. The main aim of VANET technologies is to improve safety on roads by serving real-time traffic information such as vehicle collisions, road condition, curve warnings, emergency breaking, and traffic updates etc. To share this information vehicle establishes a network and can communicate with each other.

VANET are widely used to support the growing number of wireless product which can be used in vehicles. VANET is a special type of mobile ad-hoc network which is divided into V2I and V2V networks. To introduce this many researchers has introduced Media Access Control protocols to improve VANET working. VANET is self-organised network that can be formed by connecting vehicle aiming to improve driving safety and traffic management with internet access by drivers and programmers.

The sections are organized as follows. The section II describes the various attacks present in VANET. In section III, the proposed heuristics for detection and prevention of various attacks in VANET are depicted. The section IV represents the result and discussion. The conclusion is depicted in section V.

II. VARIOUS ATTACKS IN VANET

There are many types of attacks are there in VANET. Some of them are briefly given below:

*1. **Sybil Attack [2, 3]:*** The main aim of the attacker is to cheat other nodes after thinking that they got fewauthorizeddata and they should perform accordingly. One possible scenario is when a driver wants to clear a traffic it can launch attacking by sending multiple messages to other nodes each with a fabricated source that accident has occurred in the road ahead. Sufferer nodes can hold back themselves from yielding that road path while the attacker node can drive in cleaned road without any difficulty.

*2. **Node Impersonation [4, 5]:*** A vehicle node can send a modified message of a victim node claiming to be real originator. The information can be fake or which can create damage to victim node. This kind of attack can be resolved by adding uncommon ID number to nodes. Enclosure of ID can guide to an additional category of attack where sufferers are revealed of their identity where they needed so have few secrecy.

*3. **Sending false information [6, 7]:*** This kind of attack is very common as attacker would want to disrupt the proper functioning of traffic by sending false information and bringing chaos on road.

*4. **Distributed denial of service [8, 9, and 10]:*** It is the most infamous type of denial of service attack. In computer networks the attacker spoof network IP addresses and execute attack on a victim computer denying it resources and accessibility of network. The DDoS can be categorized as according to the layer it is attacking. In VANET context the layer I took for probing is transport layer and assumed existing TCP is used in it. In general DDoS attack is executed by sending redundant messages over time making the victim node unable to respond to other legitimate messages and thus suspending it to either provide service or receive service. The TCP DDoS attack is named as SYN flooding attack. Following is the description of SYN flooding attack. A TCP handshake for two nodes to communicate a TCP connection should be established. A TCP handshaking establishes this connection. It consists of three steps. In first step the packets which are numbered (SYN for synchronization packets) for flow control mechanism is send to the receiver. In the second step the receiver send back SYN-ACK (acknowledge packet). The connection is established when sender send ACK packet and receiver receives it. When only SYN command is sent from one node to another, the receiver saves the SYN message in a data structure. At this position, the connection is said to be partly open. Many nodes can send multiple SYN messages to a node. In DDoS attack the attacker along with compromised nodes (zombie nodes) send multiple SYN messages to victim. The victim node can be deficient of genuine needs by another node when the data structure to hold SYN information is saturated with excessive SYN messages.

III. PROPOSED HEURISTIC

A) Heuristic for DETECTION

The algorithm works as follows. The detection scheme receives SYN, which is a datastructure holding SYN messages of a specific node recognized by synid, MEM which is the assigned memory of SYN database, synid and ACK data structure for a particular SYN. Our objective is to check whether the database to hold is filled or not. When a SYN message arrive line to check if it belongs to the same node or not and whether the MEM database is already filled.If SYN message belongs to same node as received previously then a cookie object is created by merging all SYN messages of the same node and is send back along with ACK. The sender has two options to send back. The first one is it can transmit cookie with ACK or just transmit ACK. Sending of just ACK has no effect as it will not be acknowledged and the connection will be disconnected. If ACK with cookie is received then sum variable is decremented thus maintaining the MEM memory. Whenever sum equals to MEM then the database to hold SYN messages is filled an attack has been detected. The else condition passes control to recursive Detection program with different node id as determined by synid.

B) Heuristic for DETECTION

Input: SYN messages
Output: Alert on datastructure full

```
if (synid==SYN.ID&&i=! MEM.size)
    cookie=merge (SYN)
    send (cookie, ACK)
    sum+=1 //global variable
    if(ack()==ACK&&receive()!=cookie)
    do nothing
    elseif(ack()==ACK&&receive()==cookie)
    sum-=1 //global variable
    if(sum==MEM.size)
        alert("DDOS")
        break
else
Detection(SYN)
end
```

C) Heuristic for PREVENTION

Input: SYN messages
Output: Alert on data structure full

```
Start the Process
```

```
H= Maintain the IP address History;
U=User enter into the website;
I=Store the each Client IP Address;
Check each time U in server,
If (I==H)
{
Else
If(I<5)
{
IP=Get IP address;
MAC1=IP+MAC//Read previous MAC algorithm
Server=MAC1;
Client=MAC1;
If(Server=Client)
{
Accept the request from the client
Send the response for the request
}
Else
{
Add the User IP to the Attacker List,
Print: "Access Denied"
}
}
}
Else
{
Accept the request from the IP
Send the response for the Request
}
End
```

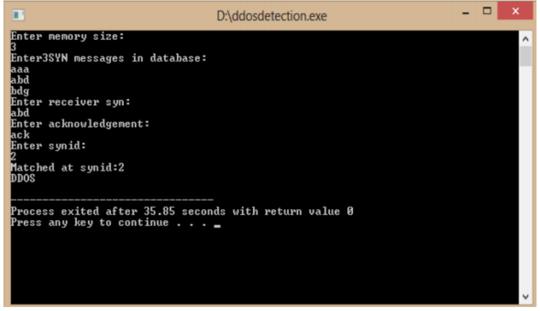
IV. Results and Discussion

The experimental results of this paper are carried out by several attackers list and the website. The browser revises each time the history of the client and the data of the history are supplied with the message such as Mac address, Time, and IP Address contemporarily. Every time the client reached at the website is evaluated depending upon the IP address. When the new user enters into the site continuously, the new cracking algorithm determines whether the user is DDoS attacker or not. In that situation what is sate of web server is calculated. And also the attacker list is maintained and checked the user with the list. If the attacker is detected, the entry is declined by our proposed heuristic. In these circumstances, the web server status also measured. This is extremely helpful, for the clients to decide the effectiveness of our proposed heuristic**.** So in this proposed heuristic to utilize the DDoS to avoid the server from accessing the server and disruption of the performance in server is disperses favorably in this system.

For the simulation results we have used windows 8, 64 bit operating system, 4 GB RAM and DEV C++ as programming purpose.

Figure 1 and 2 shows simulation results for the detection and prevention of DDoS attacks in VANET.

A) Output for detection of DDoS:

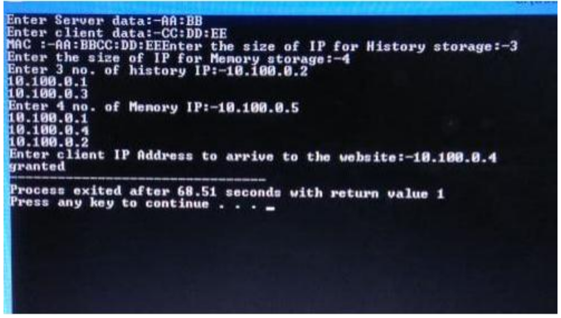


```
Enter memory size:
3
Enter3SYN messages in database:
aaa
abd
bdg
Enter receiver syn:
abd
Enter acknowledgement:
ack
Enter synid:
2
Matched at synid:2
DDOS

--------------------------------
Process exited after 35.85 seconds with return value 0
Press any key to continue . . . _
```

Figure1. Output for detection of DDoS attack in VANET

B) Output for Prevention:



```
Enter Server data:-AA:BB
Enter client data:-CC:DD:EE
MAC :-AA:BBCC:DD:EEEnter the size of IP for History storage:-3
Enter the size of IP for Memory storage:-4
Enter 3 no. of history IP:-10.100.0.2
10.100.0.1
10.100.0.3
Enter 4 no. of Memory IP:-10.100.0.5
10.100.0.1
10.100.0.4
10.100.0.2
Enter client IP Address to arrive to the website:-10.100.0.4
granted
--------------------------------
Process exited after 68.51 seconds with return value 1
Press any key to continue . . . _
```

Figure2. Output for prevention of DDoS attack in VANET

V. CONCLUSION

The predicament of developing VANET protocols and standardization of them do not allow proper implementation of any solutions to security threats. For example there is a naming problem in VANET as existing IP protocol suite cannot be applied because of ad hoc nature of it. Flooding is the basic technique presently in use to carry message from one hop to another. In our proposed solution to DDoS we have assumed the sender node to have unique id throughout. But unlike computer networks where nodes are identified with their IP addresses which are then address resolved to respective MAC address. The nodes in VANET are dynamic and the connection is mostly extemporaneous in nature. Without a proper unique naming scheme the method described cannot be implemented.

References

[1] Kuppusamy, K., and S. Malathi. *"An effective prevention of attacks using GI Time frequency algorithm under DDOS."* International Journal of Network Security & Its Applications 3, no. 6 (2011): 249.

[2] Barford, Paul, Jeffery Kline, David Plonka, and Amos Ron. *"A signal analysis of network traffic anomalies."* In Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement, pp. 71-82, ACM, 2002.

[3] Brutlag, Jake D. *"Aberrant Behavior Detection in Time Series for Network Monitoring."* In LISA, vol. 14, no. 2000, pp. 139-146. 2000.

[4] Naoumov, Naoum, and Keith Ross. *"Exploiting p2p systems for ddos attacks."* In Proceedings of the 1st international conference on Scalable information systems, p. 47. ACM, 2006.

[5] Ahmad, Shaikh Sharique, and HiralalSolunke. *"Survey on VANET Based Self Adaptive Prioritized Traffic Signal Control."* (2018).

[6] Sharma, Richa, and Jyoteesh Malhotra. *"A Survey on Mobility Management Techniques in Vehicular Ad-hoc Network."* In International Conference on Computing, Communication & Systems, 38, vol. 41. 2014.

[7] Agarwal, Pallavi. *"Technical review on different applications, challenges and security in VANET."* Journal of Multimedia Technology & Recent Advancements 4, no. 3 (2018): 21-30.

[8] Zhang, Jie. *"A survey on trust management for vanets."* In 2011 IEEE International Conference on Advanced Information Networking and Applications, pp. 105-112. IEEE, 2011.

[9] Gaikwad, Dhananjay Sudhakar, and Mukesh Zaveri. *"VANET routing protocols and mobility models: A survey."* In Trends in Network and Communications, pp. 334-342. Springer, Berlin, Heidelberg, 2011.

[10] Hamedani, Parisa Saraj, and Arshin Rezazadeh. *"A New Two Level Cluster-Based Routing Protocol for Vehicular Ad Hoc NETwork (VANET)."* In 2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim), pp. 121-126. IEEE, 2018.

Authors Profile

Ms Shalini Priya has completed Bachelor of Technology from JIS College of Engineering, Kalyani, and West Bengal in Year 2019 in Department of Computer Science and Engineering.

Ms Koyel Roy has completed Bachelor of Computer Application from West Bengal University of Technology, West Bengal in 2014 and Master of Computer Application from Maulana Abul Kalam Azad University of Technology, West Bengal in Year 2017. She is Currently Pursuing Master of Technology from JIS College of Engineering, Kalyani, West Bengal in Department of Computer Science and Engineering.

Mrs Ira Nath is presently working as an Assistant Professor in the Department of Computer Science and Engineering of JIS College of Engineering, India. She received the Master of Technology (M.Tech.) degree in Software Engineering from the Maulana Abul Kalam Azad University of Technology, India formerly West Bengal University of Technology, India in 2008. She also received the degree of Bachelor of Technology (B.Tech.) in Computer Science and Engineering from the same university in 2005. She is presently pursuing her Ph.D in Computer Science & Technology at Indian Institute of Engineering Science and Technology (IIEST), Shibpur, India. Her research interests include Network Security regenerator placement, survivability and routing and wavelength assignment in translucent WDM optical Networks.

Mr Dharmpal Singh received his Bachelor of Computer Science and Engineering and Master of Computer Science and Engineering from West Bengal University of Technology. He has done his Ph.D in year 2015. He has about 12 years of experience in teaching and research. At present, he is with JIS College of Engineering, Kalyani, and West Bengal, India as an Associate Professor and Head of the department. He has published 32 papers in referred journal and conferences index by Scopus, DBLP and Google Scholar and editorial team and senior member of many reputed journal index by SCI, Scopus, DBLP and Google Scholar. He has organized seven national levels Seminar/Workshop, published two patent and has applied for the AICTE Research Project (MRP) in year of 2019.