IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 2, Ver. IV (Mar.-Apr. 2017), PP 25-30
www.iosrjournals.org

Believe Function used to Improved Security by Eliminating Malicious Nodes in Vehicular Ad Hoc Network

Ashish singh, Priya Pathak
Department of computer Science GICTS, RGPV Gwalior, India

Abstract: *Vehicular ad hoc network is an emerging field of research in advanced communication and network. It is a sub type of wireless ad hoc network in which there is no central authority to manage the nodes. It is wirelessly communicates which make them vulnerable to attacks like DoS. Denial of Service attack mainly block the services and users are not able to use the services. An existing paper they used Malicious and Irrelevant Packet Detection Algorithm for detecting malicious node on the basis of node velocity and the frequency of packet generated depend on node maximum velocity. Basically vehicles move with high speed which is not efficiently detect malicious nodes. In our proposed work, we calculate the speed of vehicles and check the behavior of vehicles so that we can recognize the true malicious nodes then applying believe function to detect malicious nodes. In our results, we improved packet delivery ratio, routing overhead and throughput of the network.*

Keywords: *VANET, DoS attack, malicious node, believe function*

I. Introduction

VANET (Vehicular Ad hoc Networks) is a self-organized network and is a variant of mobile ad-hoc networks (MANETs). The network consists of infrastructure units such as road side units (RSUs) and wireless communication devices installed on vehicles. VANETs provide many promising applications by exchange of messages between V2V (vehicle to vehicle) and V2I (vehicle to infrastructure) for improvising driving experience. [1].Vehicles Cars may just reward redundant or fallacious warnings to their drivers. If this information is dishonored, the results of the control decisions based on this information could be even more catastrophic. Message can be corrupted as well as disgraced thru two dissimilar mechanisms: malfunction and malice. Likewise, vehicles have two protection mechanisms: one is an external filter and other one is internal reputation info for the vehicle. VANET usages are grouped into two main parts like as are non-safety and safety usages. Safety applications are most important and critical in nature than the non-safety applications. These applications are connected to saving human life either they are static or may be moving on the roads. These formal request supply warmish related ideas to drivers. Non-safety applications are too pleasant the passengers and drivers to make the effective traffic control system. Outdoor car parking availability and their details direction and signals for drivers, traveling map, are examples of this type of applications. At the similar time safety applications correct the required information and also to transmit a correctly reported stream issues to a destination to communicate the accurate and required information to every individual vehicle. Generally, goal of the both applications categories is are to give correct and right information to users/drivers on the roads. Newest research efforts are strongly emphasis on VANET design architectures, and convenience and road situations and traffic efficiency. Nowadays, road traffic activities are one of the major concerned and important daily routines worldwide. Road safety is also a main issue for the safety and security of human life. Passenger and freight transport are essential for human development. Various other specific areas include Quality of Service (QOS), routing, broadcasting and security. Many issues regarding V2I, V2V, and VRC can create a difficult situation in ITSs (Intelligent Transportation Systems). Thus new renovations are attained every day which provide safety [2].

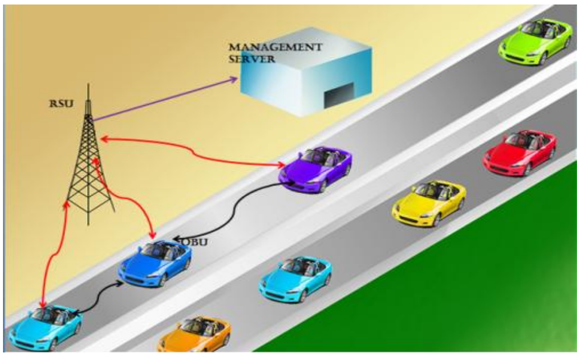

Fig. 1 Vehicular Ad Networks

II. Denial Of Service

DOS (denial of service) attacks are some of the critical issues and a method of stopping such attacks have to be devised as soon as viable. DOS attacks are much more problematical to fight against if IP spoofing is incorporate into such attacks. Vehicle IP spoofing or IP spoofing, denotes to the method of lying concerning the comeback address (i.e., Vehicle request) of a data; With IP spoofing, attackers can obtain unauthorized entry to a vehicle or a community via making it appear that a message has come from a specified depended on automobile by way of "spoofing" the IP deal with of the vehicle. Figure 2 illustrate that the procedure has been exploited thru attackers for years-, and is normally exploited in DOS attacks launched against commercial servers. As the attackers are generally anxious with consuming network bandwidth and resources, they typically don't care concern correctly finalizing transactions and communications. Rather, they simply want to flood the victim vehicle with as many messages as possible within a short period of time. In sequence to amplify the effects of an attack, they spoof the request IP addresses to create tracing and ending the DOS as arduous as probable [3].

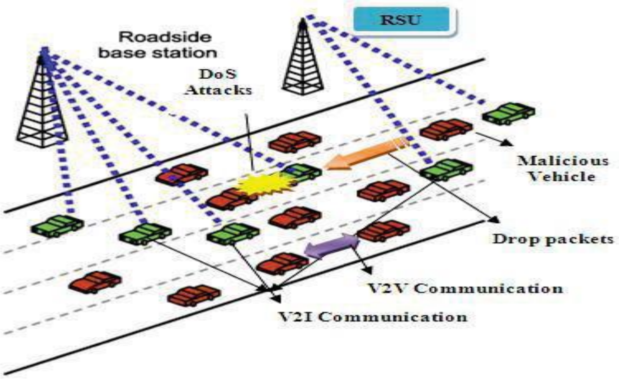

Fig. 2 DOS attacks on a VANET infrastructure

III. Attacks Taxonomy

Perceive the features of the revealed vulnerabilities can be structured into a classification which can be exploited as a grouping system to determine unknown or similar vulnerabilities. In sequence to perceive the DOS attack, we necessity to mull such elements as the attacker perpetrating DOS attack. The attacker has an intent and is competent to do whatever on VANET with one of a kind capabilities. The target of attack can be either network h/w application or infrastructure services thru find out vulnerabilities, causing many impacts on the victims based on the attacker's capabilities.

A. Attackers

It is essential to identify the attackers, their natures, and their capacity to implement an attack. Based on capacity and motive, attackers can be characterized in the following manner;

Vandal: ill-motivated. Just desire to show their capacity to attack

- *Hacker:* motivated by curiosity and interest. They have not any personal benefit from attack.
- *Malicious Hacker:* driven by personal or organizational monetary and/or political gain
- *Terrorist:* highly motivated by political ideology. Well equipped in terms of money, time, and manpower.

Alternatively, views attackers based on capacity as follows:

- *Insider:* authenticated users of the network and have detailed knowledge of network
- *Outsider:* intruders having limited capacity to attack.

B. Capabilities

It is not possible to eliminate all possible vulnerabilities given the limited nature of resources, time, and manpower. Nonetheless, the desire exists to the types of capabilities attackers have in order to craft an efficient defending mechanism. This is especially applicable in the context of VANET, as measuring real world risk and selecting an appropriate defense strategy depends on the attacker's capabilities. A single attacker or multiple attackers can mount an attack. Several attackers can be interpreted in many methods; attempting attack with separate motives, attackers may be free, attackers can attempt attack separately while having shared motives. Further, attackers can attempt attack collaboratively by a possible central controller, as is the case in a distributed DOS attack. Another aspect to consider is the technical expertise of the attackers. An attacker can only sense the network transmission or change the info, transmit wrong message, impersonation (or the like) thru producing network signal. Depending on capabilities and/or the character of the attacker, the scope and level of influence can vary. It can be localized into a part of the n/w service or availability of then network infrastructure.

C. Target

In VANET, the attacker's target can be either the network services or network itself respective to traffic info. Attack on the n/w can be further categorized into network protocol and network infrastructure. E.g, eavesdropping is perhaps the most common attack on secrecy and belongs to a network layer attack. This, however, cannot be considered an example of a DOS attack target but rather, a general security attack. Here, we define the target of the DOS attack to be the service that is being denied or blocked, thus preventing proper transmission of traffic information services. There are various traffic related services such as information of collision warning/avoidance, violation warnings, turn conflict warnings, curve warnings, lane merging warnings, emergency vehicle warnings, and wrong way driving warnings. Effective communication amid vehicles and the RSU cannot be provided and vehicles can fail to receive important traffic information as a outcome of a DOS attack.

D. Vulnerabilities

Vulnerabilities are kind of fault in the network which the attacker can make the most to mount a DOS attack. VANET is applied over a wirelessly network. Therefore, every or most of the constraints of the wirelessly medium and transmission environment can be vulnerable to the unauthorized access of the attacker. Vulnerabilities can also be a outcome of network or service-providing system design and implementation flaws.

E. Impacts

Regardless of the type of attacker, traffic related information services may be disrupted and vulnerable to further disablement during the attack, possibly causing serious damage to human users [4].

IV. Literature Survey

Mohamed Nidha [2016] et al. In this paper a reaction method against DOS attacks in VANET. In this method we have the elect amid two define reaction games. Defined metrics and design approach are inspired from game theory models. To the best of our info, no similar games have been defined earlier. The simulations showed the efficacy of our proposal measured by the performance of the obtained results.

K. Deepa Thilak [2016] et al. in this paper, DOS attack on n/w utility is submitted and its pinhead phase in VANET atmosphere is bandy. This paper also classifies and summarizes the techniques to prevent DOS attack with its pros and cons. Amarpreet Singh [2015] et al. in sequence to resort the VANET from DoS attack we have define Enhanced APDA that inhibit the decay of the n/w perform even under this attack. EAPDA not only verify the nodes and discover malicious nodes but also improves the throughput with minimized delay thus enhancing security. The simulation is done using NS2 and the results are compared with earlier done work.

Abdul Quyoom [2015] et al. in this paper, an Irrelevant and Malicious Packet Detection Algorithm (MIPDA) which is used to analyze and detect the Denial-of Service (DOS) attack. The attack is eventuality limited within its source domains, so avert damaging attack traffic overloading the network infrastructure. It additionally decreases the overhead delay in the info processing, that enhancement the communique speeds and in addition enhances the safety in VANET. Karan Verma [2014] et al. in this paper, the Bloom-filter-depend detection manner, that bestow the accessibility of a service for the legitimate vehicles in the VANET, as exploited to detect and defend against the IP spoofing of addresses of the DOS attacks. The IP spoofing of addresses in the DOS attacks that is restricted thru malicious and fraudulent nodes has been calibrate. This method provides a secure communication and also frees the bandwidth. Usha Devi Gandhi [2014] et al. In this paper, a RRDA that's exploited to becomes aware of DOS later APDA. This enhancement the response time and maximizes the safety in VANET. VANET is exploited to make a mobility network which is depend on mobility vehicles for instance cars. It is a sub category of MANET.

S. Roselin Mary [2013] et al. In this paper, an APDA that is exploited to detect the DOS attacks earlier the checking time. This lessens the overhead delay for approach and enhances the safety in VANET. The security of VANET is vital as their very presence respective to critical life blusterous circumstances. VANET is a sub part of the MANET. Subir Biswas [2012] et al. In this paper, study the prospect of a synchronization depend DDOS attacks on vehicular communications and define mitigation methods to avert such an attack. A VANET which exploits IEEE 802.11p EDCA mechanism is perceptive to an synchronization- rely DDOS attack because of small Contention Window Sizes And Periodicity Of Transmissions.

Problem Statement

In existing Malicious and Irrelevant Packet Detection Algorithm malicious node detect on the basis of node velocity. In this work frequency of packet generation depend on node maximum velocity but it's not the correct way to find out malicious node in VANET because it's not necessary that node highly movable will behave like malicious

Proposed Work

Vehicular ad-hoc network is one of the most interesting areas of research because of its infrastructure or high moveable. There are number of problems to build this network due its heterogeneous behavior. This network easily threaten by attacks, so in this case how to preserve network by attacks is difficult to understand there are lots of technique present to detect or prevent this network by attacks. Preventing network by this attack we apply velocity and behavior based broadcasting path for VANET. In first phase we calculate the speed of vehicles and how frequent a vehicles change its speed, now after speed calculation we check behavior of vehicles so that we can recognize the true malicious nodes in network scenario.

```
Algorithm:
Step1: initialize vehicle network
Step2: calculate speed of vehicles
          V = D/T
  Here, ”d” is the distance travelled, and ”t” elapsed time.
Step3: if(v>=thershold){
          Highly moveable node data does not forward to this node
        Else
              Communication happen between two nodes
Step4: if(v change frequently) {
          Believe function()
         Else
            Normal execution
Step5: if (believe >= thershold2) {
            Normal nodes
         Else
                   Malicious node
                   Believe function()
Step6: exit.
```

BELIEVE FUNCTION:

```
Believe function work for finding malicious nodes in VANET scenario
Step1: if(drop packet is true) {
           Believe—
         If(communication break) {
              Believe –
          }
        Else
           Unchanged
     Else
         Unchanged
Step2: exit.
```

Simulation Result

Simulation of our work done on ns-2.35 below mention parameter of work which is required by our scenario

Tool	Ns-2.35
Protocol	AODV
Antenna	Omni
Number of nodes	20
Simulation time	100ms
Data rate	CBR
Buffer type	DropTail

Packet delivery ratio:

It outlines the proportion of packets deliver from supply toward to destination. The fig. 3 shows a PDR graph among base approach as well as proposed approach. This PDR rate is better in proposed than existing approach.

PDR = No. of packets received / No. of packets sent

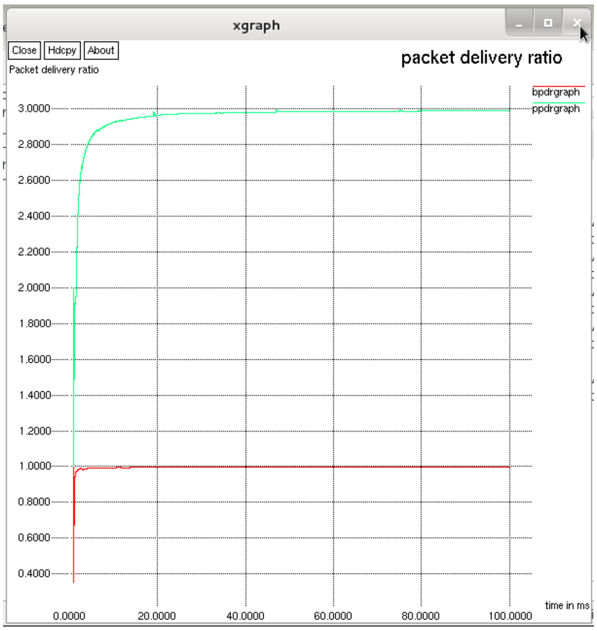

Figure3: packet delivery ratio

Throughput:
The transfer of information lying on information measure is decision as output. The fig. 4 represents a output graph among base approach moreover as projected approach. The output of the projected approach is enhanced than the present approach.

Throughput (kbps) = (Receive size/(stop time - start time)*1/60

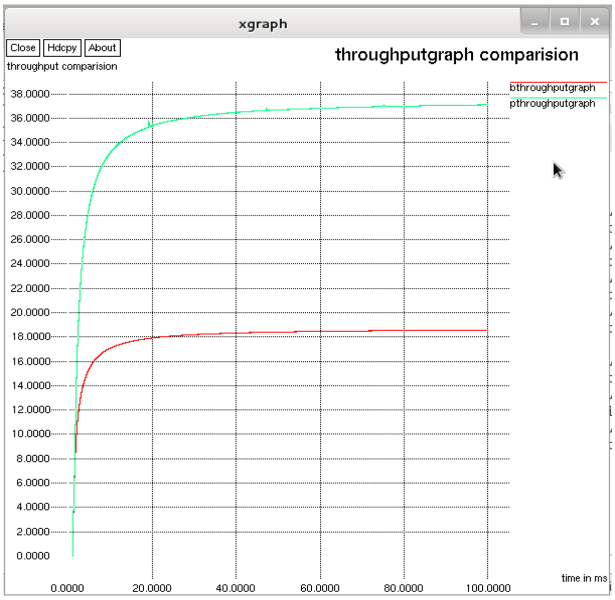

Figure4: throughput graph

Routing overhead:
It is defined as the total number of packets required in the network. The fig.5 represents a routing overhead graph among base approach as well as proposed approach. The proposed approach has an extra overhead than the base approach. Since the overhead be supposed to be minimum except as the routing increases in the proposed work the overhead also increases.

Routing overhead = Number of packets control in particular time.

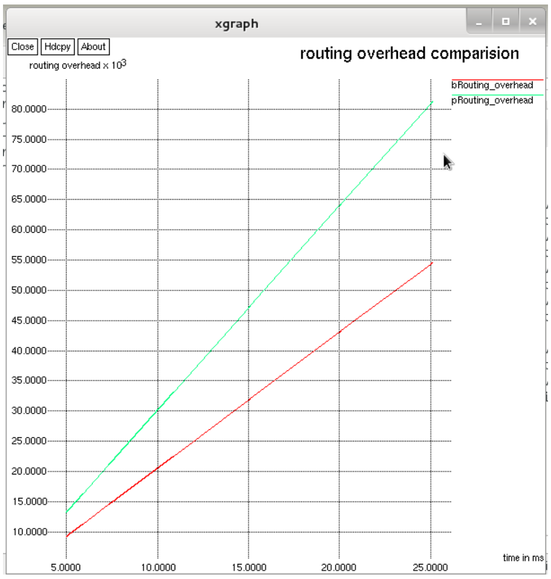

Figure5: routing overhead

V. Conclusion

Wireless Ad Hoc Network (WANET) is ad hoc network in which nodes directly communicate and they acts as a node or a router which make them less dependent on each other. Mobile ad hoc networks (MANETs) are vulnerable to various security attacks conducted by the malicious nodes and attackers. In our proposed work, we improved various quality of services in th network like throughput, routing overhead and packet delivery ratio. Security is also improved by eliminating malicious nodes from the network.

References

[1] Pooja. B, Manohara Pai M.M, Radhika M Pai, Nabil Ajam, Joseph Mouzna, “Mitigation of insider and outsider DoS attacks against signature based authentication in VANETs”, 978-1-4799-4568-9/14/$31.00 ©2014 IEEE.

[2] Abdul Quyoom, Raja Ali and Devki Nandan Gouttam, Harish Sharma, “ A novel mechanism of detection of denial of service attacks(DoS) in VANET using malicious and Irrelevant packet Detection algorithm (MIPDA)” ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE.

[3] Karan Verma, Halabi Hasbullah, Ashok Kumar, “ An efficient Defense method against udp spoofed flooding traffic of denial of service (DoS) attacks in VANET” 978-1-4673-4529-3/12/$31.00_c 2012 IEEE.

[4] Yeongkwun Kim, Injoo Kim, Charlie Y. Shim, “ A Taxonomy for DOS attacks in VANET”, 2014 International Symposium on Communications and Information Technologies (ISCIT).

[5] Mohamed Nidha, Mejrit, Nadjib Achir and Mohamed Ham&i: “A New Security Games Based Reaction Algorithm against DOS Attacks in VANETs” 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC).

[6] K. Deepa Thilak A. Amuthan “DoS Attack on VANET Routing and possible defending solutions-A Survey” International Conference On Information Communication And Embedded System(ICICES 2016).

[7] Amarpreet Singh, Priya Sharma “A novel mechanism for detecting DOS Attack in VANET using Enhanced Attacked Packet Detection Algorithm (EAPDA)” Proceedings of 2015 RAECS UIET Panjab University Chandigarh 21-22nd December 2015.

[8] Abdul Quyoom, Raja Ali and Devki Nandan Gouttam, Harish Sharma “A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)” International Conference on Computing, Communication and Automation (ICCCA2015).

[9] Karan Verma, Halabi Hasbullah “IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DOS) attacks in VANET 2014 IEEE”.

[10] Usha Devi Gandhi, R.y'S.M Keerthana “Request Response Detection Algorithm for Detecting DoS Attack in VANET” ICROIT 2014, MRIU, India, Feb 6-8 2014.

[11] S. RoselinMary, M. Maheshwari, M. Thamaraiselvan “Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)”2013.

[12] Subir Biswas, Jelena Miˇsi´c and Vojislav Miˇsi´c “DDoS Attack on WAVE-enabled VANET” Globecom 2012 - Communication and Information System Security Symposium.