Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA)

S. RoselinMary[1], M. Maheshwari[2], M. Thamaraiselvan[3]
[1]Assistant Professor III, Department of Computer Science and Engineering,
Anand Institute of Higher Technology, Chennai, India.
[2]Lecturer, Department of Computer Science and Engineering,
Anand Institute of Higher Technology, Chennai, India.
[3]P.G Student, Department of Computer Science and Engineering,
thamaraiselva1054@gmail.com, PH: +91 9940202813
Anand Institute of Higher Technology, Chennai, India.

Abstract— The security of VANET (Vehicular Ad Hoc Networks) is crucial as their very existence relates to critical life threatening situations. VANET is a subtype of the MANET. In which the mobile nodes are all vehicles equipped with an On-Board Unit (OBU) that enable them to send and to receive messages to the other Nodes in the network. In addition to communication among the vehicles, VANET interface with communication points provided by on road infrastructure. Many of the Researchers have already proved about the securing safety messages. Moreover VANET face several security attacks. In existing VANET systems is using a detection algorithm to detect the attacks at the verification time in which delay overhead occurred. The various security threats are misbehaving nodes give false information, Sybil attacks, selfish driver attacks, and etc. In this paper we proposed an Attacked Packet Detection Algorithm (APDA) which is used to detect the DOS (Denial-of-Service) attacks before the verification time. This minimizes the overhead delay for processing and enhances the security in VANET.

***Index Terms*—VANET, APDA, OBU, DOS, ATTACKS.**

I. Introduction

VANET is a kind of networks in which vehicles [2] [10] can communicate two or more vehicles fashion with each other on the roadside. VANET application has been tolerant or liberal categorized into safety and non safety applications. Safety applications are most important in nature as these are presently connected to others and their lives. These formal request supply warmish related ideas to drivers such as later inform on a road. VANET are one way to implement Intelligent Transportation System (ITS), a technique for imparting information and communication technology to transport infrastructure and vehicles. It is based on IEEE 802.11p [9] standard for Wireless Access for Vehicular Environment (WAVE).

These networks have no fixed infrastructure, and they rely on themselves for implementing any network [9] functionality. VANET is relevant with safe for human life while these people are moving on the roads. Non-safety applications are too pleasant the drivers and passengers to make the [3] traffic system. Traveling map, outdoor car parking availability their details are examples of this application. Generally, object to be attained of both applications. Categories are to give the correct details to users or drivers on the roads. However, for safety applications, the details not only required to be correct but also transmitted from a stream issues to a destination. Hence, secure condition is an interruption such as not continuous can create problem to the users. This is especially crucial [9] if the censorious lives matter is being communicated between a sender and a receiver. Availability is one of the largest securities needed. Any one of this node wants to work with the other node in the network or communications. The network should be accessible to users. Over the last few years, we have identified many researches, efforts that have investigated various problems related to [9] V2I, V2V and VRC areas. Because of the shorted role they are expected to play intelligently. In various, VANET projects have been executed by various industries, governments and institutions around the world in the last decade or so. We presented the different types of wireless communications, access quality that is being deployed for VANET. And also present some of latest VANET projects undertaken by different groups and organization in the US, JAPAN, EUROPIAN countries. Some of the VANET research challenges that still require innovative solutions are presented.

In this paper we focus on security, misbehavior and attacked packets detection schemes.

A. HOW VEHICULAR NETWORKS WORK

Vehicular Networks [9] System consists of a large number of nodes, approximately number of vehicles exceeding 750 million in the world. Today, these vehicles will require an authority to govern it, each vehicle can communicate with other vehicle using a [5] short radio signals DSRC (Dedicated short range communication) 5.9 GHz, in range 1 KM. This communication is an Ad Hoc communication [3] which where the connected node can move freely, no wires required. The router Road Side Unit (RSU), connects the vehicles on the road and connect to other network devices. Each vehicle has OBU [9] (On board unit), which connects the vehicle with RSU via DSRC radios, and other device is TPD (Tamper Proof Device), this device holding the vehicle secrets, information about the vehicle like keys, driver's identity, trip details, speed, route etc..

Section II briefly introduces the possible attacks in VANET. In Section III, existing works on VANET presented in detail and section IV talks about the proposed security and APDA algorithm. The Section V talks about conclusion of our proposed concept.

II. POSSIBLE ATTACKS IN VANET

VANET is facing many attacks and these attacks are discussed in the following subsections:

1) DENIAL OF SERVICE ATTACKS:

DOS attacks can be done by the [9] network insiders and outsiders and give the network not available to real users by flooding the control channel with high sound of naturally generated messages and stops the network connection. As a result OBU and RSU are unable to process the capacity sufficiently.

2) BROADCAST TAMPERING:

An inside assault may inject [9] false safety messages into the network to cause damage such as causing an accident by suppressing traffic rules or manipulating the flow of traffic around a chosen route.

3) SYBIL ATTACK:

This attack, [6] forges the identity of multiple vehicles. Those identities can be used to cast any type of attack on the system. These false identities also create an illusion that there are additional vehicles on the road and spoof the positions of other nodes in the network.

4) MESSAGE SUPPRESSION ATTACK:

An attacker selectively drops packets from the network, and these packets may hold critical [8] information for the receiver. The attacker suppresses these packets and may use them again when required [8]. The goal of this attack is to prevent registration and insurance authorities from learning about collisions about the vehicle and/or to avoid delivering collision reports to RSU.

5) ALTERATION ATTACK:

This attack happens when an attacker alters an [8] existing data. An alteration attack includes delaying the transmission of the information, replaying earlier transmission, and also altering the actual entry of the data transmitted.

III. EXISTING WORKS

The authors [2] try to solve the security problem of Dos attack with the use of OBU. The model relies on the use of OBU which fits on each vehicle node, to make a decision as to deter a DOS attack. The processing unit passes information to the OBU, to switch channels technology (or) to use frequency hopping technique. Four options are available to detect the received messages, after the [2] decision will be sent to the next OBU in the network. Switching options are channel switching, technology switching, FHSS, multiple radio transceivers.

The authors [7] try to solve the security problems of the Sybil attack detection scheme, which is composed of two complementary techniques. The first one is a localization verification technique, based on receiving signal strength. This technique allows a node to verify the authenticity of another node by locating its future geographical localizations. Compare them to its detected suspect, a second technique [7] is a Sybil detection mechanism, based on the definition of a distinguish ability degree metric. It can be launched individually by every node in the network.

The authors [6] try to solve the problem of the Sybil attack detection based on cryptography in VANET. The proposed schema uses an encryption mechanism to detect attacks and to the four security aspects like authentication, non-repudiation, privacy, and data integrity are introduced. Every vehicle should make sure of message transmitters authority and authenticate it. Non repudiation allows to access personal information of the vehicle, which helps in recognizing the vehicle in case of any claims and crimes. Vehicles identity information's should be attached to the messages, so it can be tracked whenever desired and non-repudiation is established in the network. Privacy of personal information [6] about the vehicles and the drivers are restricted not be accessible by other vehicles. The anonymity can be preserved to avoid tracking. Data integrity is that the transmitted message can contain valid information not to be altered by attackers.

The authors [4] try to solve the problem of Wormhole Attack detection. The nodes participating in the VANET communication should register on the network. In order to avoid the formation of wormhole in the route, this paper proposes a method in which after the route reply from the destination, the source has a complete list of the intermediate nodes forming the route. The author [4] proposes a scheme in which they use a special packet called Decision Packet. After the route has been set up between a source node and destination node, the former gets the information about all nodes in the path from RREP packet. Which contains all nodes identity take which has been forming route from source to destination node in recent [4] identified path. Every node computes the hash value of the decision packet which is verified at the next node, so there is no chance of alteration of the hop count by the attacker. If an attacker by somehow changes [4] the hop count value it will result in a change, in hash value of the packet will be consequently discarded.

IV. OUR SYSTEM MODEL AND ALGORITHM

A. System Model

We introduce a proposed model to detect the attacks using Attacked Packet Detection Algorithm; figure 1 shows the system model of the proposed system. The mechanism is attached with each RSU. Vehicles can send messages to RSU through APDA mechanism. It is to detect a certain position of the messaged vehicles. After detecting the position of vehicle information it is stored in the certain RSU. Each vehicle has OBU and TAMPER PROOF device. These devices, store the detailed information about the vehicles. For example speed, position and etc. Vehicles positions are identified by the frequency and velocity of the vehicles and the use of OBU.

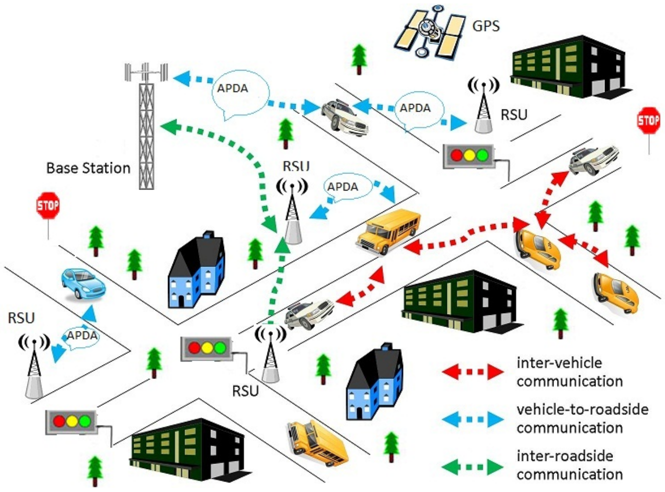
GPS
APDA
APDA
RSU
STOP
Base Station
RSU
APDA
STOP
RSU
APDA
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Figure.1

Figure.1 shows the system model of our proposed system. APDA algorithm is detecting the position of the vehicle and detects the packet of vehicles send. If the packet is not attacked, vehicle will not track else track the particular vehicle.

B. Algorithm

This algorithm based on position changing requirements. Attacked packets are identified by the following parameters [1]. Frequency (f), Velocity (v), α is Coefficient which is determined by the road characteristics and VMax is the maximum speed,

$$f = \alpha * | v - V_{Max} / 2|$$

Frequency (f) is the numbers [1] of broadcast packets per second, Attacked packets are identified by the following conditions. F and V are high because the position will change quickly. F and V are low because the vehicle positions will not change much. Our proposed algorithm based on the change in position and change frequency f, velocity v.

INPUT: Position changing the requirements velocity V, α coefficient, Vmax is the maximum speed and request R.

OUTPUT: V is high and f is high representing attacked packets or invalid request. Otherwise V is low and f is low representing to detect the attacked packets.

Algorithm: APDA

```
Identifies (AP)
Begin
    Find $f = \alpha * | v- V_{Max} / 2 |$
    If ( f >= high && v>= high ) //
        Identify (AP or Invalid Request)
        APDetAlg ( R )
        Begin if Verify  ( Request )
            Return true
        Else if  (f<=low && V<=low)
            Return Invalid Request
        Else
            APDetAlg (R)
        End if
    End if
End
End
```

F - No of broadcast packets per second, set the high and low values.

TABLE I. NOTATIONS

Notation	Descriptions
F	Frequency
AP	Attacked Packets
V	Velocity
A	Co efficient
R	Request
V_{Max}	Maximum speed

APDA can be applied, before the verification time and to increase the security. It is used to detect the invalid request and attacked packets and it is used to avoid the delay overhead.

V. CONCLUSION

Our proposed system APDA algorithm is used to improve the security of VANET system and to avoid the delay overhead in early time. The algorithm can be applied before the verification time delay overhead is minimized and will enhance the security of VANET. In future we are going to apply this algorithm for multiple invalid request send from multiple vehicles at the same time and detect the attacks in the early manner.

REFERENCES

[1] Gongjun Yan, Stephan Olariu, Michele C. Weigle, "Providing VANET Security through active position detection," ELSEVIER, Computer Communication 2008.

[2] Halabi Hasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan, "Denial of Service (DOS) Attack and Its Possible Solutions in VANET," World Academy of Science, Engineering and Technology 65 2010.

[3] Hannes Hartenstein, Kenneth Laberteaux "VANET Vehicular Applications and Inter-Networking Technologies", page no 4 to 10, wiley 2010.

[4] Harbir Kaur, Sanjay Batish & Arvind Kakaria, "An Approach to Detect the Wormhole Attack in Vehicular Ad-hoc Networks," IJSSAN, 2248-9738 Volume-1, Issue-4, 2012.

[5] José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks", Handbook of Research on Mobility and Computing 2010.

[6] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET," IJNSA, Vol.3, No.6, November 2011.

[7] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET," International Journal of Network Security, Vol.9, No.1, PP.22-33, July 2009.

[8] Mushtak Y. Gadkari , Nitin B. Sambre, "VANET: Routing Protocols, Security Issues and Simulation Tools," IOSR Journal of Computer Engineering, July-Aug. 2012

[9] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," Springer Science +Business Media, LLC 2010.

[10] Wikipedia "Vehicular Ad-Hoc Network" http://en.wikipedia.org/wiki/Vehicular_ad-hoc_network this page was this page was last modified on 5 January 2013.