**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 3, Issue. 12, December 2014, pg.416 – 419***

**SURVEY ARTICLE**

# A Survey on Efficient Intrusion Detection in Vehicular Ad-hoc Network

**Ashish B. Raut[1], Nandkishor P. Karlekar[2]**

[1]Department of Computer Science and Engg
Sinhgad Institute of Technology, Lonavala, Pune, Maharashtra, India
[2]Associate Professor, Department of Computer Science and Engg
Sinhgad Institute of Technology, Lonavala, Pune, Maharashtra, India
[1] abraut1990@gmail.com; [2] nkarlekar@gmail.com

***Abstract—Vehicular Ad-hoc Networks (VANETs) are becoming wide technology in traffic system. This type of networks has great potential to improve road safety and reduce the number of accidents via the exchange of alert messages between the neighbourhood vehicles. The unwanted data can disturb the network communication. The wrong information or malicious data can jam the traffic on roads. Security is lost when a user or group of users try to send invalid information into the network. The aim of this paper is to give an overview of intrusion detection techniques and malicious data detection in VANETs.***

***Keywords— VANETs, Intrusion detection, Malicious data, Ontology, security***

## I. INTRODUCTION

Vehicular Network (VANET) is a form of Mobile adhoc network, to provide vehicles to communicate with each other in a peer-to-peer manner without any access points In VANET, there is no fixed infrastructure. This type of network is used to reduce the number of accidents via the exchange of alert messages between the neighbourhood vehicles.

Several solutions to these problems are proposed, such as symmetric cryptography, authentication and secure routing protocols, the problem with these solutions is that they are mostly specialized for a specific attack. In addition, they do not offer the possibility to detect new attacks, nor even to defend the network against internal compromise nodes[5].

Security always remains a challenging task in VANETs due to the high mobility of the nodes[5]. While nodes share the information with other nodes, there are chances of leakage of information sent by one node to other. In such a case, we say that nodes are compromised, i.e., the nodes that access the information of the other nodes in an unauthorized manner to breach the confidentiality, integrity and availability are called as intrusions in the network.

 

An intrusion detection system (IDS) is a mechanism to identify abnormal or suspicious activities through examinations of various parameters such as network traffic, CPU utilization, I/O utilization, user location, and various log file [8].

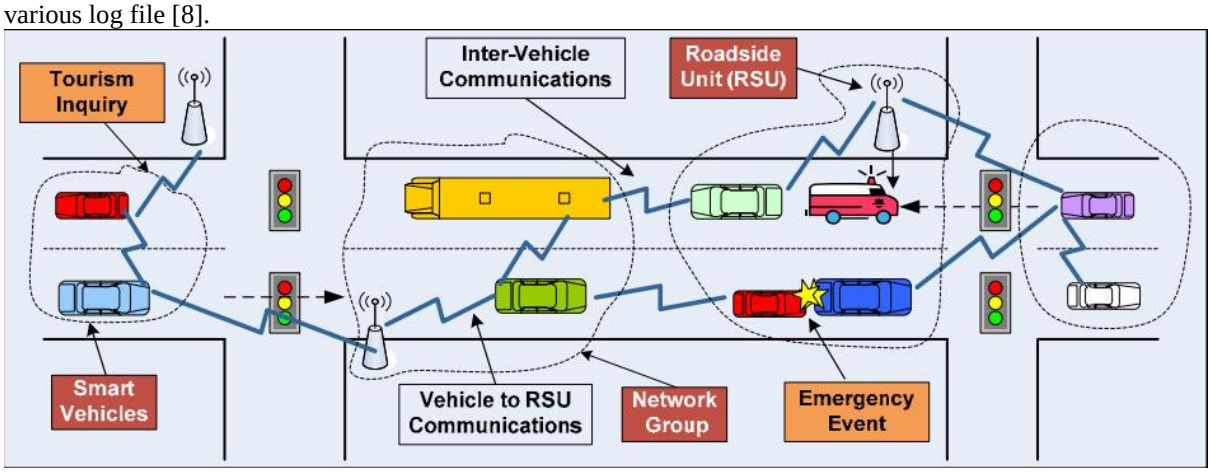


**Fig 1. A basic structure of VANETs**

**Characteristics of Vanet:**

The feature of VANET mostly resembles the operation technology of MANET in the sense that the process of self-organization, self-management, low bandwidth and shared radio transmission criteria remain same. But the key hindrance in operation of VANET comes from the high speed and uncertain mobility of the mobile nodes (vehicles) along the paths [2]. Moreover, VANETs have unique attractive features over MANETs as follows:

- Higher transmission power and storage: The network nodes (vehicles) in VANETs are usually equipped with higher power and storage than those in MANETs.
- Higher computational capability: Operating vehicles can afford higher computing, communication and sensing capabilities than MANETs.
- Predictable Mobility: Unlike MANETs, the movement of the network nodes in a VANET can be predicted because they move on a road network. If the current velocity and road trajectory information are known, then the future position of the vehicle can be predicted.

## II. RELATED WORK

### *2.1 Malicious Data Detection in VANET*

Vehicular Network are wide technology used in traffic system mechanism[1]. A poorly designed VANETs that grant a serious attack on network which can degrade performance and goal of the network. Malicious/wrong information is capable of jamming a traffic on the roads. This types of information is called as malicious/unsolicited data.

In this paper, Gurpreet Singh and seema developed an infrastructure/simulated environment in order to detect fake message on the basis of Intrusion detection system(IDS). IDS compare incoming and outgoing messages with predefined pattern. The trace fie is used to collect the behavior of VANET in given time slot. The file format contains Event ID, Messages send and Received, Source node, Destination node, Route no, and Flag. Check for number of safety messages. if number of safety messages are greater than Threshold then there occurs malicious data and check for route frequency otherwise normal number of messages.

**Impact of attack**: When attack was introduced huge volume of increase in safety messages. Due to this, vehicles starts changing their routes as they receive safety message of accident and lead to traffic jam. While the attacker one who enjoy free road.

### *2.2 AN ONTOLOGY-BASED INTRUSION DETECTION*

The paper aim is to provide a complete classification which takes into account the impact of attacks and intrusions on the offered service. ontology is used in the field of semantic web and refers to a structured set of concepts in a particular field of knowledge[2]. Within an ontology, concepts are defined in relation to each other using a graph model to organize knowledge, which enables reasoning and manipulation of knowledge.

 

Schema associated with four distinct classes constitute:

- ***High Level Ontology:*** Highest level of abstraction The first class, Attacks includes all concepts related to the intrusion.
- ***Ontology types of attacks****:* show a clear separation between the types of attacks.
- ***Ontology of possible vulnerabilities****:* The class vulnerabilities of upper High Level Ontology describes VANETs vulnerabilities such as: shared wireless medium, the highly dynamic network topology, the absence of centralized security service and the cooperatives relationships.
- ***Ontology of consequences:*** Consequences of intrusion in a vehicular ad hoc network may be: Degradation of network performance, flight of personal information, insulation of nodes, lead to road accidents and road congestion.

### *2.3 Providing security in Vehicular ad hoc networks (VANETs) through historical data collection*

Security is lost when user send invalid information into the network for individual purpose.In this paper, Dr.Kamal Jamshidi worked on historical data and helps the driver to make true and proper decisions. Assign unique ID to each vehicle in the network . When a message is sent it contains both the information and ID of the sender. Every vehicle has a data base., Validity probability is affected when the event /incident occurred and it is stored in database for every reported event. we call that history[3].

Validity probability for each event has a primary value at first in the data base, when its first report receives. A When any vehicle reports the incident and others receive its report. If they trust this report they may decide to change their way, but in other hand the message might be invalid. If it is the first time this incident is reported, in other word one vehicle has reported this incident, its validity probability is not enough, but its sender ID and primary probability is saved in data base of both other vehicle and RSU. Trust to this message is not recommended and it can be used just to

inform the driver. This simple approach helps vehicle in making true decisions on the roads. If different vehicles (with different ID) report the incident, it is more probable that it has happened. It is obvious that in area with a large number of vehicles this method is very useful and helps the driver to make true and proper decisions

### *2.4 A Novel Reputation Management Framework for Vehicular Ad Hoc Networks*

In this paper, a novel reputation management framework is presented, which mainly works with the integration of entity-centric mechanism and event-centric mechanism to establish trust in VANETs.[4]. The majority of people drive their vehicles locally for their daily commute. Thus it is feasible to let the RSUs take charge of managing the long-term reputation values for these commute vehicles, event-centric mechanism is adopted if the reputation value of a vehicle cannot be queried based on the fact that this vehicle just has a new route when the traffic event happens.

Attackers can diffuse bogus information in the network to affect other drivers' behaviors and cause intelligent collisions. In this paper , Qing Ding, Xi Li assume that Vehicles in VANETs are equipped with a detection mechanism to identify false information. each vehicle equips with a tamper-proof positioning device, such as GPS. Then its status data, such as speed, and direction, etc. are all carried out by this device. These data can be embedded to messages, and sent to another vehicle automatically by the beacon message. Beacon message which includes a vehicle's status, such as location, velocity, and direction and is broadcasted by this vehicle is encrypted and signed.

If the value of gathered event data is over the predefined safety threshold, the information is sent to the traffic safety application in the vehicle. At the same time, the traffic warning messages will be broadcasted to neighboring vehicles. Its own location information and the reputation value of the event are attached to this message. The message is also encrypted and signed by ER's privacy key. EOs receive the message, and it can decide if this message is from a ER by comparing the event location, vehicle location from warning message and the vehicle location from beacon message it received at the most recent time. Then it will send a reputation query message to the nearby RSU.

If the RSU returns the reputation value of ER during this time, this value will be directly used to determine if the message is bogus. If not, event-centric mechanism is adopted to calculate the reputation value of the event, and decide whether to forward the event again. Then according to the observation to ER's subsequent behavior, the reputation of ER is re-calculated and updated into RSU later. EPs and EOs have the basically same way to process messages, but they do not start the abnormal behavior analysis algorithm since they cannot observe ER's behavior.

 

### *2.5. Collaborative trust aware intelligent intrusion detection in VANETs*

Most of these solutions may not be suited for VANETs as the nodes in the VANETs have high mobility. States of individual vehicles along with the transitions from one state to another change quickly in VANETs[5].

- Signature based scheme can detect only known attacks.
- Anomaly based schemes generates high false alarms and requires large data sets of training data for constructing the normal profile in the network

Hence there is a requirement of system which capture the information about the states and transitions from state to state so that all activities of the vehicles in a particular time interval can be monitored. Keeping in view of the above issues, Neeraj Kumar, Naveen Chilamkurti proposed a new Trust aware Collaborative Learning Automata based Intrusion Detection System (T-CLAIDS) in VANETs.

- A new Collaborative LA based algorithm is proposed for intrusion detection in VANETs. The proposed algorithm takes inputs as the density, mobility and direction of motion of the vehicles and the corresponding automaton performs its action based upon these parameters.
- A Collaborative Trust Index (CTI) is computed for each of the action performed by the automaton. The values in CTI are added or removed according to the successful or unsuccessful operations, i.e., automaton receives the penalty or reward from the environment. Based upon these parameters, the action probability vector of the automaton is updated which is used for the next iteration. Finally, after performing the action for finite number of times, the solution converges to a particular value.

## III. CONCLUSIONS

Detection of an intrusion in VANETs is always a challenging task as the nodes in VANETs have high mobility and varying density on the road. Hence a novel IDS for such networks is required which will detect any misbehaving nodes in the networks under the constraints of high mobility and varying density of the nodes in the network. Keeping in view of the above Detection of an intrusion in VANETs is always a challenging task as the nodes in VANETs have high mobility and varying density on the road. Hence a novel IDS for such networks is required which will detect any misbehaving nodes in the networks under the constraints of high mobility and varying density of the nodes in the network. Keeping in view of the above issue, in this paper we have done literature survey for detecting the malicious data and intrusion detection techniques in Vehicular Ad-hoc Networks (VANETs).

## REFERENCES

[1] Gurpreet Singh, Seema, "Malicious Data Detection in VANET", International Journal of Advanced research in Computer and Communication Engineering Vol. 1, Issue 7, September 2012

[2] M.ERRITALI, B. EL OUAHIDI, B.HSSINA, B. BOUIKHALENE, and A. MERBOUHA , "AN ONTOLOGY-BASED INTRUSION DETECTION FOR VEHICULAR AD HOC NETWORKS" Journal of Theoretical and Applied Information Technology 31st July 2013.

[3] Dr.Kamal Jamshidi et al " Providing security in Vehicular ad hoc networks (VANETs) through historical data collection" International Journal on Computer Science and Engineering (IJCSE)

[4] Qing Ding, Xi Li " A Novel Reputation Management Framework for Vehicular Ad Hoc Networks " , International Journal of Multimedia Technology , Jun. 2013, Vol. 3 Iss. 2, PP. 62-66 .

[5] Neeraj Kumar , Naveen Chilamkurti, " Collaborative trust aware intelligent intrusion detection in VANETs", Computers and Electrical Engineering 40 (2014) 1981–1996

[6] B huvaneshwari.S, Divya.G, Kirithika.K.B3 and Nithya." A SURVEY ON VEHICULAR AD-HOC NETWORK ", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 10, October 2013

[7] M. S. Kakkasageri1 and S. S. Manvi ,"INTELLIGENT INFORMATION DISSEMINATION IN VEHICULAR AD HOC NETWORKS", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.1, March 2011

[8] O. Depren, M. Topallar, E. Anarim, M.K. Ciliz, An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks, Expert Systems with Applications 29 (2005) 713–722

 