ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 7, September 2012

Malicious Data Detection in VANET

Gurpreet Singh[1], Seema[2]

M.Tech. Student (Computer Engineering)[1], Assistant Professor (Computer Engineering) (Supervisor)[2]

Yadavindra College of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo, Bathinda, Punjab, India.

Abstract—***Vehicular networks are becoming wide technology in traffic system. The entities that are part of a vehicular communication system can be private or public vehicles, road-side infrastructure, and authorities, with the latter considered primarily as network entities. Poorly designed VANETs that permit serious attacks on the network can jeopardize the goal of increased driving safety. The unwanted data can disturb the network communication. The wrong information or inject large volume of data can jam the traffic on roads, this type of data is known as malicious data/unsolicited data. Also, the life safety becomes critical and non trusted behaviour of network. Thus the specific characteristics of VANETs result in hard to address security issues, which make the field of secure inter-vehicular communications. Therefore, we have done work on securing VANET and develop a framework for understanding impact of attack. We tried to detect malicious data under VANET environment. In this thesis work, we will present the techniques that have been proposed so far to ensure accurate data transmission between nodes. VANET have configurable no. of nodes and multiple sensors/actuators. Next, To develop a model of all on board sensors based on their past data set. This may be created by using adapting thresholding, Simulate abnormal behaviour in data arrival rate and volume of data arrival. The Proposed work is related to develop simulator with CAN protocol.***

Keywords: Malicious data, VANET attacks, CAN, Intrusion Detection.

I. INTRODUCTION

Vehicular Network (VANET) is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment. It is a cornerstone of the envisioned Intelligent Transportation Systems (ITS). By enabling vehicles to communicate with each other via Inter-Vehicle Communication (IVC) or V2V as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC) or R2V, vehicular networks will contribute to safer and more efficient roads by providing timely information to drivers and concerned authorities. The interesting research area of Vehicular Networks is where ad hoc networks can be brought to their full potential. Both modern high-speed motorways and vehicles that drive upon them are becoming increasingly intelligent. The resulting enhanced situational awareness has the potential to not only facilitate the decision making tasks of the drivers (e.g., trip planning based on traffic congestion on the road), but also to improve highway safety (by bringing information about catastrophic events and road conditions to the driver’s attention). Each vehicle equipped with VANET device will be a node in the Ad-Hoc network and can receive and relay others messages through the wireless network. Collision warning, road sign alarms and in-place traffic view will give the driver essential tools to decide the best path along the way.

II.TYPES OF ATTACKS IN VEHICULAR NETWORK ENVIRONMENT

Attacker create problem in the network by getting full access of communication medium. Here we are discussing some properties and capability of the attackers which has been mentioned in studies [1].The main objective of these attacks is to create problem for legitimate users of network. All attacks will be effect the communication of the network, like Denial of Service (DoS) attack, Distributed Denial of Service (DDOS) attack, Sybil attack, Node Impersonation attack, Application attack, Timing attack, Social attack, Monitoring attack and these classes of attacks varies application wise and depends upon the environmental issues.

III.LITERATURE REVIEW

Golle et. al [2] discussed that sensor-driven technique that allows nodes to detect incorrect information and identify the node or nodes that are the source of this incorrect information with high probability. M. Raya et. al [3] proposed protocols, as components of a framework, for the identification and local containment of misbehaving or faulty nodes, and then for their eviction from the system. Leinmuller et. al [4] discussed that a system that works completely without infrastructure or dedicated hardware. They use the concept of a ‘position cheating detection system’ similar to intrusion detection systems in MANETs. In these systems, every node uses multiple algorithms (so-called sensors) to detect malicious or selfish behavior of other nodes in the network. Rahbari et. al [5] suggested a method based on a fixed key infrastructure for detection impersonation attack, in other words, Sybil attack, in the vehicular ad hoc network. Kaur et. al [6] discussed various Sybil attack detection techniques like Resource Testing, Radio Resource Testing, Public key Cryptography, Signal Strength Based Position Verification Scheme, Privacy Preserving Detection Scheme, Timestamp Series Approach, and Detection using Neighbouring Vehicles.

IV.PROPOSED WORK

There is need to develop an Intrusion detection system that can detect Fake messages transmission in VANET. Following are objectives of proposed work:
1) To Develop a Simulated Environment of VANET
2)To Develop a Threshold based Intrusion Detection based system for anomaly detection
3) To Evaluate the Impact of Malicious, fabricated andfake message attack.

V. METHODOLOGY

We will focus on malicious data/fake message detection because it is critical to life saving and traffic scenario. The malicious data can overload the system by injecting large no. of messages to nodes. There is need to develop a system that can detect the fake node on basis of malicious data using Intrusion detection system. An Intrusion detection system basically works by comparing incoming/outgoing messages with predefines patterns. The system that we have developed works as follows, the methodology steps are as:

A. Development of VANET

First step of proposed system is to develop VANET environment having Configurable no. of Nodes and multiple no. of Sensors/Actuators installed in Vehicles, having 4 routes and RSU located after 1/3 of Road Length. It includes the various parameters like channel type ,Network interface type, frame types, No. of Channels, No. of Nodes, X and Y dimensions of Topography, Antenna model, Packet protocol etc.

B.Collect event data

The trace fie is used to collect the behavior of VANET in given time slot. The system has created a trace file for CAN data. The file format contains Event ID, Messages send and Received, Source node, Destination node, Route no, and Flag.

C. Model Intrusion detection system

The idea here is that if we can establish a normal activity profile for a system .The system can flag all system states varying from the established profile as intrusion attempts, here we have used Pseudo logic for the detection purpose.

D. Pseudo logic

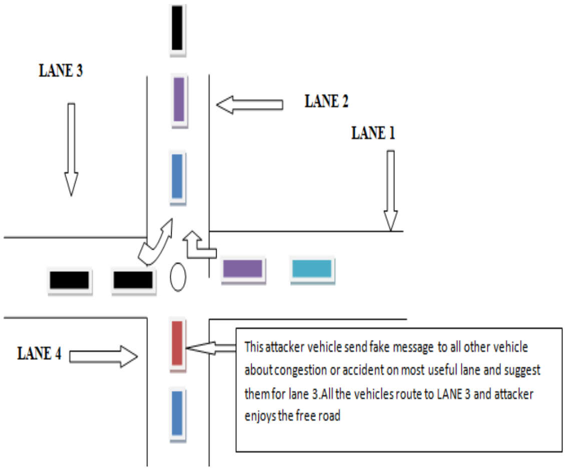
```
For each Event in Network Simulation
  {
  For each Message Arrived
    {
      For each Time Slot
        {
          For Channel in Spectrum
            {
              If channel is Safety Check
                {
      Check No. of safety Messages, Total Messages
      If no. of safety Messages >=Threshold
                  {
          Mark Suspicious, check Route Frequency
                  }
          Else
                  {
                    Normal No. of Messages
                    Check Route Frequency
                  }
                }
              }
            }
          }
        }
```

E.Attack simulation (fake/fabricated/safety attack messages)

Attack simulation defines the way in which fake messages passed by an attacker. it is designed by using 4 lanes numbered as LANE 1,LANE 2,LANE 3 and LANE 4.It is assumed that all the node are choosing a more feasible route or lane.

F.Before attack

As shown in fig. 1, before attack, the traffic is going normal. The no. of messages passed between nodes has normal value. As shown in following figure, the attacker node is coming from Lane 4.The most useful route is lane 2.

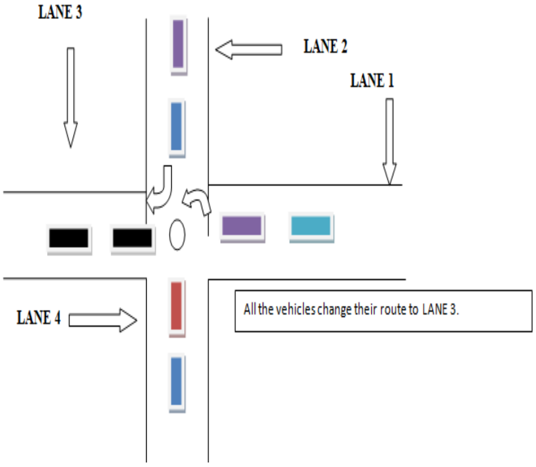


This attacker vehicle send fake message to all other vehicle about congestion or accident on most useful lane and suggest them for lane 3.All the vehicles route to LANE 3 and attacker enjoys the free road

Fig. 1. Traffic scenario before attack

G.After Attack

Here, the attack has occurred. As shown in fig. 2, all the nodes are started to move lane 3, and attacker can enjoy the free full road. The detection of fake message is done by detecting the increase in no. of messages passed by one node to others in given time slot.



All the vehicles change their route to LANE 3.

Fig. 2. Traffic scenario after attack

VI.RESULTS

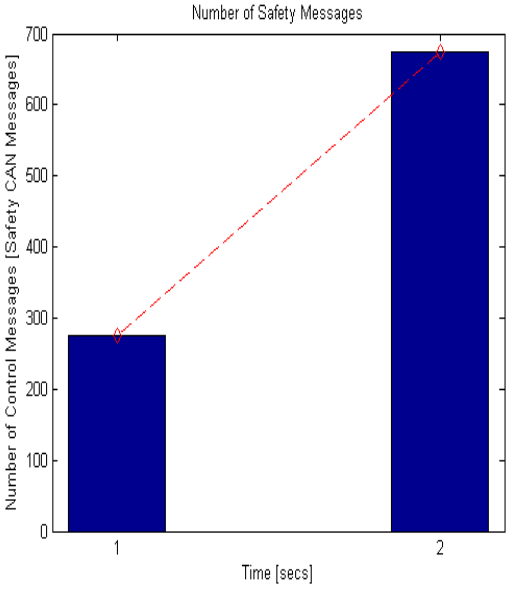


Fig. 3. Number of messages toward time variation

As shown in fig. 3, number of messages varies toward the time variation. The attacker vehicle rebroadcasting faulty messages again and again. As shown in graph, during normal situation , the no. of control messages is approximate 280,but after attack this become approximate 680.

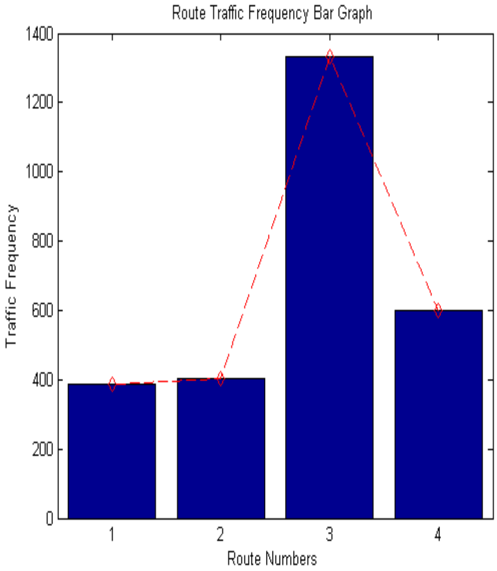


Fig. 4. Traffic frequency at different routes

As shown in fig. 4, the accumulated no. of vehicles passed from particular route has been calculated.

As the simulation proceed, it can be seen from the graph, the highest no. of vehicles either stationary or moving are on route no.3.This may be attributed to the fact that the propagation of false messages is occurring all across the network and moving vehicles toward route no.3.

VII. CONCLUSION

After conducting this simulation, in which we tried to understand and analysis of the fake message attack, this attack leads to disruption of network and routes on which vehicles are running. It apparent from the graph that when attack was introduced, suddenly there was huge volume of increase in total no. of control CAN messages, especially safety messages. It can be seen from the bar graph, there is large difference between the no. of safety messages communicate across the network as compare to normal routine of the network. In this research, we have assumed that it is an automated vehicle network in which the vehicles are passing after a regular set of interval but due to this attack, the vehicles start changing their routes as they are receiving safety message of accident and it can seen from graph, the frequency of traffic is quite high in route no. 3 which might lead also to traffic jam and congestion while attacker enjoys the l free road.

REFERENCES

[1]. J. T. Isaac, S. Zeadally, J. S. Camara (2010), **“Security attacks and solution for vehicular ad hoc networks”**,*IET communication*, pp.894-903.

[2]. P. Golle ,D. Greene, J. Staddon (2004), **“Detecting and correcting malicious data in VANETs”**, *VANET’04,* pp.29–37

[3]. M. Raya, P. Papadimitratos, I. Aad, D. Jungels, J.P. Hubaux (2007), **“Eviction of misbehaving and faulty nodes in vehicular networks”**, *IEEE Journal on selected areas in communications*, pp.1557-1568

[4]. T. Leinmuller, E. Schoch, F. Kargl (2006), **“Position verification approaches for vehicular ad hoc networks”**, *IEEE Wireless Communications*, pp.16–21

[5]. M. Rahbari, M. A. J. Jamali (2011), **“Efficient detection of sybil attack based on cryptography in VANET”,** *International journal of network security & its applications (IJNSA)*,pp.185-195

[6]. K. Kaur, S. Batish, A. Kakaria (2012), **“Survey of various approaches to countermeasure sybil attack”**, *International Journal of Computer Science and Informatics*, pp.96-100

Biography

Gurpreet Singh received his B.Tech degree in computer science and engineering from Guru Gobind Singh College of Engg. & Tech.(GGSCET), Talwandi Sabo(Bathinda), Punjab, India, in 2008, and pursuing M.Tech degree in computer science and engineering from Yadavindra college of engineering, Punjabi University Guru kashi campus, Talwandi sabo(Bathinda), Punjab,India. His research interests include Wireless Network and VANET attacks study.

Mrs. Seema is presently working as Assistant Professor in Computer Engineering at Yadavindra College of Engineering, Punjabi University Guru Kashi Campus, Talwandi Sabo (Distt Bathinda) Punjab w.e.f. year 2008. She has almost seven year of teaching experience of teaching B.Tech. (CSE), MCA and M.Tech. (CE) Classes. She previously worked as Senior Lecturer & Head, Department of Computer Science & Engineering at Bhai Maha Singh College of Engineering, Muktsar and Lecturer (Computer Science & Engineering) at Government Polytechnic, Bathinda. She completed her Bachelor of Technology (CSE) from Institute of Engineering & Technology, Bhaddal, Ropar in year 2004 holding 9th merit position in the University. She completed Master of Technology in Computer Engineering in year 2007 from Punjabi University, Patiala, Punjab. She has guided almost 15 M.Tech. dissertations and a number of B.Tech. Projects. Her research areas include Digital Image Processing, MANET, Adhoc Networks, Video compression and Enhancement, Optimization using GA & PSO etc.