ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

Review To Detect and Isolate Malicious Vehicle in VANET

Jaydeep P. Kateshiya[1], Anup Prakash Singh[2]

P.G. Student, Department of Computer Science,Lovely Professional University, Phagwara, Punjab, India[1]

Associate Professor, Department of Computer Science,Lovely Professional University, Phagwara, Punjab, India [2]

ABSTRACT: Vehicular ad hoc networks (VANETs) are more increasing attentions from academia and deployment efforts from industry, due to the various applications and potential tremendous benefits they offer for future VANET users.VANET does not have any fixed topology and the nodes move from one location to another. To transfer a packet from sender to receiver it should follow a routing mechanism and data can be transferred securely. Many challenges and security attack are in VANET. The application for that which basically for the road side vehicle and transport system for no collision and avoid accident in real life. The data can be route using low cost path in network.so that the route should be trusted and nodes could not be compromised. In this paper we discuss about routing protocol and security attack in VANET.Isolate possible attack on VANET and prevent it with numerous techniques.

KEYWORDS: VANET, Routing, Security, Sybil Attack.

I. INTRODUCTION

VANET's is basically a part of MANET. VANET is a mix of Sensor networks and Ad hoc networks. In VANET, vehicles act as nodes which can exchange data between each other without any infrastructure network establishment. High dynamic behavior and directional mobility of the vehicles are the important characteristics. In order to participate in such a network, a vehicle has to be equipped with a special electronic device which will provide Ad hoc network connectivity for the vehicles. VANETS are spontaneously formed between moving vehicles equipped with wireless interfaces that could have similar or different radio interface technologies, employing short range to medium range communication system. The best example of VANET is Transport System of any travel agency or any company which is joined internally. These Transport System of a vehicles are moving in any parts of city and different routes to pick or drop client or employees if they are connected together, which make an Ad hoc Network and connected wireless.In ad hoc network most capable areas of research is the investigation of the communications among vehicles called Vehicular Ad-hoc Networks (VANETs).

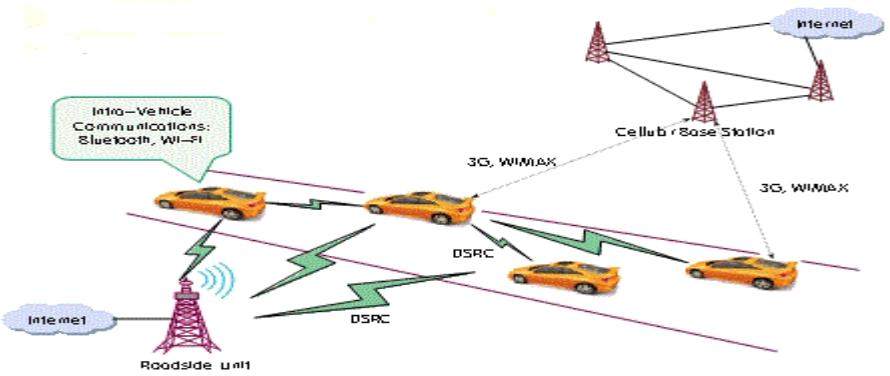

Figure.1. VANET Architecture

The networks are self-configuring networks together of a collection of vehicles and elements of roadside unit structure connected with each other without need any infrastructure, sending and receiving in data of current traffic situation and the way from where it's easy to go. Nowadays, Wi-Fi (*IEEE 802.11 based*) technologies are used for the initialization

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

of VANETs which most frequently today.The communications standard specifically for VANETs is DSRC (Dedicated Short-Range Communication) has been proposed presently. Its attempt very low discontinuation and high data rate for a short medium range communications service. In some scenarios in which buildings and distances discontinue communication channels frequently and where the reachable time for connecting to vehicles could be really very short-lived are especially true in certain time of a VANET. In this without using automatic intelligent design tools is practically impossible efficient protocol configuration for VANETs because of the enormous number of possibilities problem (*NP-problems*). When considering multiple design issues, such as highly dynamic topologies which change very rapidly and reduced scope, it is especially difficult (e.g., for a network designer) [2]. Vehicular adhoc network are wireless networks where all the vehicles are basically called node or mobile node in MANET. It is for the driver comfortable when any certainly action done and road infrastructure safeties, the vehicle to vehicle communications provide them.. It is very bottom line for all the vehicles. Vehicular ad hoc network is individual form of MANET which is vehicle to vehicle roadside wireless changing topology for communication network. It is functioning as independent and self-arranging wireless communication network, where exchanging data and sharing information for all the nodes in VANET involve themselves as servers or client. The VANET network architecture can have three different types of categories such as pure cellular network architecture, pure ad-hoc network architecture and hybrid network architecture.

II. CHARACTERISTICS OF VANET

Vehicular network have some special type of behaviour and characteristics, which distinguishing them from other types of network. As compare to other networks vehicular network have unique and interesting features as follow:

- Unlimited transmission power: In the ad-hoc devices power issues is main constrain but in the case of this network nodes/vehicle provide continuous and sufficient power to computing and communication devices for doing other task.

- Computational capacity very high: Operating vehicles can have very significant computing capacity which done by sensor and circuit in the vehicle with sufficient energy, communication and sensing capabilities.

- Predictable mobility: In the mobile ad-hoc network where the vehicle mobility is very hard to predict, vehicles have very predictable movements that are limited to roadways. Roadways information is often available from positioning systems and map based technologies such as GPS. It can give brief about the vehicle average speed with according to some distance, current speed of the vehicle and path of the future position of vehicle can also be finding them.

- High mobility: vehicular networks operate extremely dynamic and their configurations. If take the example of highway where relatively speed of up to 190-230 Km/h may occur while density 1-2 vehicle in 1 Km on other side where relative speed up to 65-70 Km/h and in rush hours especially very high density of nodes.

- Partitioned network: vehicular network will be frequently divided and dynamic nature of traffic may result in large inter vehicle gaps in sparsely populated scenarios in several unusual clusters of nodes.

- Network topology and connectivity: In the vehicular network scenarios are vary from location to location. When vehicle move and change their position constantly in the dynamic scenarios. As the link between the nodes connect and disconnect very often because of network topology changes frequently. As the network is connected is hugely depend upon the two factors which are the range of wireless links and the fraction of participant vehicles, where only a fraction of vehicle on the road could be equipped with wireless interfaces [8].

III. ROUTING PROTOCOLS

Routing protocol specifies how to communicate with the help of routers. It shares information among intermediate nodes then with the whole network. It helps to search shortest route from source to destination. There are mainly three types of routing protocol available [4]. These are as following:

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

- Reactive Routing Protocol (On-Demand):

It is on-demand a reactive type routing protocol. It is idle approach in which all the node are not comprises the information of the all the nodes and keeps table only on demand. To find the path route discovery process is follow. Reactive routing protocols are bandwidth effective. In this, routes are built as and when they are required. This is achieved by sending route requests across the network. There are shortcomings with this protocol that it offers high latency when finding routes and other is the possibility of network clog when flooding is extreme. In this thesis, we considered AODV, DSR [6].

- Proactive Routing Protocol (Table-Driven):

Proactive protocol contains fresh list of the route and their destination from source. In this type of protocol one node contains more than one table for each node in the network. All the nodes are update regularly. If the topology frequently changes than update information propagate to every node of the network and update table. In that like DSDV, WRP, STAR etc.

- Hybrid Routing Protocol:

Hybrid protocol contains both type of protocol which is explained above. As name suggest this type of protocol like ZRP in which proactive and reactive type of routing protocol are use as its use for increase throughput in routing and it's like divided the part like when use which one

IV. SECURITY THREADS IN VANET

In VANET there are many types of attacks which can disturb the VANET structure and also its privacy. Each types of attack basically affect the type of services in the system. This type of services called in technical term as "CIA" as confidential, Integration and availability. Attacks are done for access, modification, denial of service or repudiation in the data or any other things. Also attackers are divided in some type as outsider, insider, Coverage area or technical expertise.

In VANET many attacks are done which its suffer and this attacks are describe in subsection.

- Denial of Service (DOS): This type of attack is very simple but it's very harmful. In this attack its use other identity and block the services of other or it can stop also VANET communication service. These attacks done by attackers taking control of others and stop the communication services or jam the channel in network. This attack is very harmful to the drivers which are not communicating and also get false information.

- Fabrication Attack: As name suggests it's fabricated or alert the message contain and transfer the false information in network. In this basically modified the data or information and transfer false information and also its clam to another one which are not in that [5] [6].

- Interception Attack: This type of attack like man-in-middle attack .In this attacker is middle in between and intercepts the information between them and its intended to other destination.

- Eavesdropping Attack: This is most common attack which is done on confidentiality. This attack is passive in nature and done on network layer which it's very difficult to find out. In this attack it gets the access of confidential data such as vehicle identity or location or any another which are confidential.

- Impersonate Attack: As in this attack, attacker are impersonate to other. That means attacker pretend to be what they are not and get the access to information on network. As simple some accident are done in highway that time attacker simply impersonate to other and refuse. The attacker may be insider or outsider and attack is done on multilayer means attack can be effect can be either network layer or application layer or in transport layer vulnerability.

- Sybil Attack:It consists of sending multiple messages from one vehicle node with many identities. Sybil attack is always possible except the extreme conditions and expectation of the possibility of resource parity and regulation among entities [3]. When any node creates multiple copies of itself then it creates confusion in the network. Claim all

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

the illegal and fake ID's and Authority. It can create collision in the network. This type of situation is known as Sybil attack in the network. This system can attack both internally and externally in which external attacks can be restricted by authentication but not internal attacks. As there is one to one mapping between identity and entity in the network.

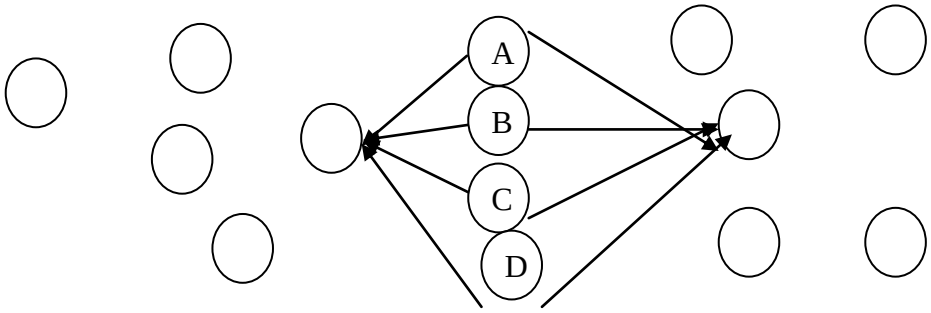

Figure.2. Sybil Attack

A, B, C, D nodes are Sybil nodes which create fake or similar identity in the network and collapse the network. Sybil node which ids are theft by attackers. Attacker uses the ids of Sybil node and done attack on network.

V. LITERATURE REVIEW

In VANET many security attack are more challangeble and which lead to low performance of network.As in network many malicious vehicle are avalible which have any intension for doing wrong things.In this paper,malicious vehicle are attack on the network which can lead to delay packet,routing overhead and throughput.**V.Lakshmi Praba, A.Ranichitra**[10], proposed the technique which avoide the milicious vehicle in network by using MDETECT procedure.In this all vehicle first register in central authority also by malicious vehicle but not given any respone and some change in speed of vehicle then its detected the malicious vehicle and avoid the collision.As using this procedure AODV enhance the perfomance and also analyse the result of AODV protocol based on performance matric.

Jason J. Haas and Yih-Chun Hurepresent a paper based on the performance measurements obtained from simulations of the (VANETs) vehicular ad-hoc networks. These simulations use as input traces of vehicle movements that have been generated by traffic simulators which is based on the traffic model theory. In this work based on the actual large scale recordings of vehicle movements. To our knowledge, no one has published any work on actual large scale recording of vehicle movements in that area. In order to enable analysis on this scale, we have developed a new VANET simulator which can manage more vehicle than ns2. To enable us simulator and present results of cross validation between ns2 and our simulator showing the both simulation produce result that are statistically the same. This simulator use to analyse the proposed authentication mechanism for the vehicles identity, which confide on ECDSA signatures comparing it to broadcast authentication using TESLA. In this paper perform our evaluations using real vehicle mobility. Our comparison shows its strength and weakness for each of these authentication schemes in terms of the resulting reception rates and latency of broadcast packets [11].

RBVT, road based using vehicular traffic information routing which is based on the existing routing protocol in city based vehicular ad-hoc networks (VANETs). **Josiane Nzouonta, Neeraj Rajgure proposed** RBVT protocols leverage real time traffic information to create road based paths consisting of successions of road intersection and high probability, network connectivity among all the systems. In this paper use the geographical forwarding is used to send the packets between intersection path, reducing the sensitivity within the paths to individual node movements. In the dense network high contention and optimize the forwarding using a distributed receiver based election of next hops, it is based on the multi-criteria prioritization function taking into account non-uniform radio propagation. This paper designs the reactive protocol RBVT-R and proactive protocol RBVT-P and compared them against MANETs protocols like AODV, OLSR, GPRS. Other protocol representative is like VANET. In the simulation result shows that in the urban settings shows that RBVT-R protocol best in term of delivery rate, with up to 42% increase compared to some

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

existing protocols. In the protocol terms of average delay, RBVT-P performs best and 85% decreased as compared to other protocols [12].

VANET has security and privacy issue. As in VANET malicious vehicle can attack on network as change with different different identity. As in Sybil attack malicious vehicle can image as multiple vehicle in network.**Tong Zhou, Romit Roy Choudhury, Peng Ning and Krishnendu Chakrabarty**[13]**,** defined the light weight and expandable protocol. In this using the RSB and DMV which can distribute the work calculation load and openness less amount of information with using the hash collusion. By using this technique we can preserve the vehicle privacy which is most important and also provide the security against Sybil attack.

Gang Liu and Han have proposed some aspects of road sweeping vehicle automation [14] a design of framework of intelligent transports system is proposed. The main task of the road condition information transferring module is deal with the information exchange of the car inside, car to car and car to road. They concern the security issues of VANETs from some aspects and provide the appropriate solving measures for VANET security. To make sure that its can be used under the security pattern.

Hao Wu has presented An Empirical Study of Short Range Communications for Vehicles [15] a work on short range of communication over the vehicles. The work includes both V2V and V2I communication under highway scenario. The network characteristics in driving environment is been discussed in this work.

Su-Jin Kwag has proposed Performance Evaluation on IEEE 802.11 Ad-hoc Network in Vehicle to Vehicle Communication performed a work to [16] analyses the performance of the IEEE 802.11 Ad-hoc network for vehicle to vehicle communication under a vehicular environment, focusing on the fairness which very crucial to the safety related services for vehicle and other, and the effect of mobility. Some suggestions for future researches for development are followed.

Vishnu Kumar Sharmal and Dr. Sarita Singh Bhadauria represent a paper on power control in mobile ad-hoc network connectivity and neglect network partition and also provide power efficient operations. The paper purpose congestion and power control techniques based on agent in mobile ad-hoc network. The mobile agent from source starts forwarding the data packets through the path which has low cost and congestion. The capacity of every node is composed and finally it is delivered to destination node. In the power control method all the nodes select the nodes based on the power level. The node with maximum energy level are select as listening node, it is always on active mode on the other hand non listening node which awake in periodic manner. If the nodes getting the data packet is not wakeful after packet sent to destination through the listening node. In the simulation result show the projected techniques provides most proficient congestion and power controls [17].

VI. FUTURE WORKAND CONCLUSION

VANET has many loop holes which breach the security of network. As many vehicles join and leave the network in small amount of time and within the range. In such scenario, there is possibility that malicious vehicles can join the network which will trigger certain type of security attack in the network. We have discussed many techniques to detect and prevent from attack. In our future work we proposed technique which detect and isolate malicious vehicle in VANET by triggering it on AODV protocol. The proposed algorithm will improve network performance. The new algorithm improves **throughput, delay and fuel emission** in VANET.

REFERENCES

1. Hugo Conceicao “Large-Scale Simulation of V2V Environments", ACM Symposium on Applied Computing (SAC), vol. 16-20, pp. 28-33, 2008.
2. Stephan Olariu “An Architecture for Traffic Incident Detection ",The 7th International Conference on Advances in Mobile Computing and Multimedia, pp. 14–16, 2009.
3. Farzad Sabahi, “The Security of Vehicular AdhocNetworks”, Third International Conference onComputational Intelligence, Communication Systemsand Networks, pp. 338-342, 2011.
4. A.Chinnasamy, S.Prakash,P.Selvakumari,”Enhance Trust based Routing Techniques against Sinkhole Attack in AODV based VANET”, International Journal of Computer Applications, vol. 65, pp.22-27, 2013.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2015

5. B. Parno and A. Perrig, "Challenges in securing vehicular networks," in Proceedings of the 4th Workshop on Hot Topics in Networks (HotNets-IV), pp. 1–6, 2005.
6. M Raya, J Pierre Hubaux," The security of VANETs", In Proceedings of SASN, 2005.
7. Rakesh kumar,"A Comparative Study of various protocols in VANET", International Journal of Computer Science Issues (IJCSI), Vol. 8, Issue-4, No.-4, 2011.
8. Salim M.Zaki, M.A ngadi,Maznah Kamat,"A Location based routing prediction service protocol for VANET environment",IEEE,2009.
9. Stephan Olariu,"An Architecture for Traffic Incident Detection ", MoMM2009, vol.26-19, pp. 3, 2009.
10. V.Lakshmi Praba, A.Ranichitra, "Isolating Malicious Vehicles and Avoiding Collision between Vehicles in VANET", International conference on Communication and Signal Processing, April 3-5, Pp. 811 – 815, 2013.
11. Jason J. Hass,"Real world VANET security protocol Performance", Global Telecommunications Conference, IEEE,p1-7, 2009.
12. Josiane Nzouonta, Neeraj Rajgure,," VANET Routing on City Roads using Real-Time Vehicular Traffic Information",IEEE Transactions on Vehicular Technology,p1-18.2009.
13. Tong Zhou, Romit Roy Choudhury, Peng Ning and Krishnendu Chakrabarty,"P2DAP – Sybil Attacks Detection in Vehicular
14. Ad Hoc Networks" IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, 2011.
15. [14] Gang Liu and Han Gup,"Some aspects of road sweeping vehicle automation", IEEE lasme international conference on advanced intelligent mechatronics, 2001.
16. [15] Hao Wu,"An Empirical study of short range communication for vehicles",IJSER, pp. 83-84, 2011.
17. [16] Su-Jin Kwag ,"Performance Evaluation of IEEE 802.11 Ad Hoc Network in vehicle to vehicle communication",Mobility '06 proceedings of 3rd international conference on mobile technology, 2006.
18. [17] Reena Dadhich,"Mobility Simulation Of Reactive Routing Protocols for Vehicular Ad hoc Network", IJCA Journal, 2011.