International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Various Approaches of VANET Routing and Attack Detection

Parminder Kaur[1], Deepinderjeet Kaur Dhaliwal[2]

[1]Research Scholar, DBU, Mandi Gobindgarh, Pb., India

[2]Assistant Professor, DBU, Mandi Gobindgarh, Pb., India

Abstract: ***VANET basically is the part of MANET that provides feasible communication to the vehicles.The RSU's in the phenomena help the vehicles to easily communicate and hence provide collisions. This paper briefly explains about the attack that occurs in the VANET scenario. In this various routing protocols, attack detection approaches used in VANET have been described. In this network safety message delivery without any delay has to be essential to avoid any collision in the network. On the basis of study of different approaches in VANET best approach can be extracted that can be used for VANET network in real world applications.***

Keywords: VANET, Security, Attacks in VANET.

1. Introduction

1.1 VANET

VANET is the advancement of MANET that provides wireless communication in vehicles. Its major concern is to provide safety, privacy and security. It is equipped with on board radar transduction and GPS that provides the location of the vehicle. The communication between vehicles is through wireless network. It is used to implement ITS which is an intelligent advanced application that provides different services. VANETs are infrastructure less, distributed, self-organizing communication networks built upby moving vehicles. Thus VANETs have very high node mobility and limited degrees of freedom in the mobility patterns. Hence, ad hoc routing protocols must adapt continuously to these unreliable conditions, where the growing effort in the development of communication protocols which are specific to vehicular networks.

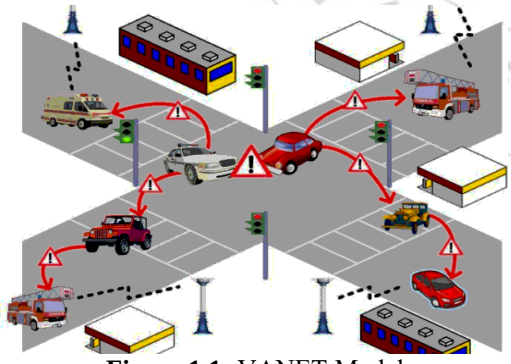

Figure 1.1: VANET Model

In VANET there are different routing protocols. The VANET is very dynamic in nature. Hence the major challenge in VANET is routing packets in effective and efficient manner. There is also lack of infrastructure and shorter communication session. Thus routing protocol plays important role in VANET. Most of the routing protocols use position based and map based approach.

In position based approach global positioning system (GPS)is used to find position of vehicle. GPS provides the information like longitude (x), latitude(y), altitude (z) and time error (st). But in GPS system some positional error is occurs. Thus using this information vehicle locates at wrong position in digital map. In safety application delay is key parameter. Hence using DBR one can overcome this error. In DBR path for routing the data is selected using inter vehicular distance and longest duration of connectivity. The common interests of the prior researches on power control in VANET are the energy consumption, connectivity and throughput/capacity. Power control (or power assignment)in VANET is an effective methodology to enhance network Performance by operating at the most appropriate transmission power to achieve various design objectives ROMSGP is another position based routing protocol. In ROMSGP vehicles are group according to their velocity. Vehicle in same group moving in same group provides high Stability. In ROMSGP LET is used for path selection. The path having longest LET is considered as most stable path.

1.2 Attacks

There are various kinds of attack that can affect the entire system or can degrade the performance of system. The attacks can be categorized into following types.

1.2.1 Denial of Service attack: This strike happens when the aggressor increments control of a vehicle's benefits or jams the channel of correspondence utilized by the Vehicular Network, so it makes tangle to send separating information to its end of the line. It additionally expands the threat to the driver, on the off chance that it needs to rely on upon the application's data.

1.2.2Message Suppression Attack: An assailant specifically dropping packets from the system, these bundles may hold discriminating data for the beneficiary, the aggressor stifle these parcels and can utilize them again as a part of other time.

1.2.3 Fabrication Attack: An aggressor can make this assault by sending wrong information into the system, the information could be wrong or the transmitter could assert that it is another person. This assault incorporates create messages, warnings, declarations, personalities.

1.2.4 Alteration Attack: This assault happens when aggressor modifies current information, it incorporates deferring the transmission of the data, replaying prior transmission, or changing the genuine section of the information transmitted. For example, an aggressor can modify a message telling different vehicles that the current street is clear while the street is congested.

1.2.5 Replay Attack: This assault happens when an aggressor replay the transmission of a prior data to exploit the circumstances of the message at time of sending.

1.2.6Black hole Attack: When some malicious user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black node.

1.2.7 Grey hole Attack: This attack occurs if some node dropping 50% of the packets and rest 50% is sending by altering the message. In this way wrong information is broadcast.

1.2.8 Sybil Attack: In this attack, attacker generates multiple identities to simulate multiple nodes. Each node send messages with multiple identities, in this way other nodes realize that there are many nodes in the network at the same time. This attack is very dangerous because one node can give its various locations at the same time and this creating security risk.

2. Literature Review

Joanne Mum-Yee Lim et al [1] Cognitive VANET with Enhanced Priority Scheme" Vehicular communications are important to ensure emergency messages are transmitted on time to prevent accidents. Therefore, in recent years, various standardization bodies and automobile companies have developed vehicular ad hoc network (VANET) to ensure public road safety. The current IEEE802.11p schemes utilize only traffic type to categorize priority levels. Performance of the proposed EPVS is evaluated in Vehicles in Network Simulation (Veins) with road traffic simulator, Simulation of Urban mobility (SUMO) using a realistic urban map. Simulations results show that the proposed EPVS results in lower average delay, in comparison with the default IEEE802.11p scheme.

Ahn et al [2] "A VANET Routing based on the Real-time Road Vehicle Density in the City Environment". The intelligent transportation system (ITS) can enhance the driver's safety by providing safety-related information such as traffic conditions and accident information to drivers. In this paper, author propose a routing protocol that works based on the real-time road vehicle density in order to provide fast and reliable communications so that it adapts to the dynamic vehicular city environment. In the proposed routing mechanism, each vehicle computes the vehicle density of the road to which it belongs by using beacon messages and the road information table. Based on the real-time road vehicle density information, each vehicle establishes a reliable route for packet delivery.

Gandhi, U.D.et al [3] "Request Response Detection Algorithm for detecting DoS attack in VANET"VANET is used to create a mobile network that is based on mobile vehicles such as cars. It is a sub category of MANET. It allows every participating vehicle into a wireless node, allowing it approximately 100 to 300 meters of each other to connect and in turn, create a wide range network. In this network vehicles can join into one another so that a mobile internet is created. It is used for ITS. Very well-known automotive companies like BMW and Ford promotes this term. In VANET the mobile nodes are well equipped with ORT (On board Radio Transponder) that is useful in communication with other nodes in a network. In this paper we proposed a Request Response Detection Algorithm (RRDA) which is used to detect DOS after APDA. This increases the response time and maximizes the security in VANET.

Nikumbh, D.M.et al [4] "Analysis of distance based routing protocol in VANET" VANET is Ad-hoc network it is V purpose of VANET is to reduce traffic on road, accident and also send some useful information VANET is dynamic topology hence routing the packet in efficient and effective manner is major challenge.

Ravi, K. Praveen, K et al [5] "AODV routing in VANET for message authentication using ECDSA" A Vehicular Ad Hoc Network (VANET) is a part of MANETs that is formed by wireless connections between cars. In VANETs, routing protocols and other routing related techniques must be adaptable to vehicular-specific capabilities and requirements. Along with the routing in VANET, message security is also one of the major concerns. Messages are critical and important like a warning message, so that the message must be authenticated which guarantee's the message integrity. The authentication of these messages is done with the help of an algorithm called Elliptic Curve Digital Signature Algorithm (ECDSA), which provides an efficient message authentication scheme. A combination of AODV, ECDSA and VANET can make the scenario more efficient and perform better in terms of routing and time delay in message delivery.

Carpenter .et al [6] "Obstacle Shadowing Influences in VANET Safety" Wireless communications between vehicles enables both safety applications, such as accident avoidance, and non-safety applications, such as traffic congestion alerts. With the intent of improving safety in driving conditions. Because cost limited test-bed environments constrain prototype testing, VANET researchers often turn instead to simulation toolsets from which a rich set of environmental scenarios are modeled. However, despite the availability of such tools, results are inconsistent. While VANET investigators often model propagation loss deterministically dependent upon transmitter receiver distance, fading and shadowing effects are often modeled stochastically, leading to probabilistic results which are independent of the actual environment and thus fail to consider realistic road topologies and the presence of obstacles.

3. Approaches Used

RREQ

When a source node sends a packet, it generates an RREQ with RoadList, RoadHop and MinDensity, and floods the RREQ after inserting the identity of the road to which it belongs into the RoadList field. The RoadList field in the RREQ message is appended by vehicles along the path until the RREQ reaches the destination. Upon receiving an RREQ message, an intermediate vehicle operates as follows:

1) If the source address in the RREQ message is not in its routing table and the identity of the road which thevehicle belongs to is not in the RoadList, then a new entry with the source address, the road IDs in RoadList, RoadHop and MinDensity of the RREQ is created in the routing table. And the identity of the road is appended to RoadList and MinDensity is changed to the DC value in its RI if the DC value is smaller than MinDensity and, then, the vehicle forwards the RREQ.
2) If the source address exists in the routing table and RoadList in the RREQ is not equal to that in the routing table, and then RoadHop is compared. If the RoadHop in the RREQ is greater than k ($k > 0$) plus that in the routing table, then the RREQ is dropped. Otherwise, MinDensity is compared. If the MinDensity in the RREQ is smaller than that in the routing table, the RREQ is forwarded. Otherwise, the RREQ is dropped.
3) When the destination receives the first RREQ, it waits for the RREQs forwarded through the other paths for a given time duration. Then, it selects the route with the highest MinDensity and sends an RREP back to the source.
4) When the source vehicle receives the RREP, it sends a data packet to the destination by using the road information in the RREP by using the source routing mechanism.

$$\mathrm{T_i}(t_o) - \mathrm{T_i}(t) \geq \delta \quad (1)$$

AODV

AODV is a method of routing messages between VANET nodes. AODV is 'on demand routing protocol' with small delay. It is a Reactive algorithm. That means that routes are only established when needed, to reduce traffic overhead.

AODV supports Uni-cast, Broadcast and Multicast without any further protocols [10]. AODV allows these nodes, to pass messages through their neighboring nodes with which they cannot directly communicate. This is done by discovering the routes along which messages that can be passed. It also makes sure these routes do not contain loops and tries to find the shortest route possible, and is also able to handle changes inroutes and can create new routes if there is an error. AODV uses symmetric links between neighboring nodes. It does not attempt to follow paths between nodes when one of the nodes cannot hear the other one.

Input: (r, s), m,Q

1) Verify r, $sE[l, n-1]$
2) Compute w = s- I mod n.
3) Compute

$u_1 = ewmodnandu_2 = rwmodnwithe = H(m)$.

APDA

The APDA algorithm detects the DOS attack prior to the verification. It considers the position, time stamp, velocity, etc. of the vehicle to find whether it falls under the range of radar and also in detection of false nodes. If the number of packets and the maximum speed is high than the node velocity it is considered to be an attacked as the position of the vehicle changes very quickly .similarly if they are very low they don't change the position much is also considered to be attacked. After the complete process the vehicles are validated and stored in the RSRT database. The second algorithm is used for the further verification of new requests that wants to join the network. This algorithm compares the previous validated data base with new requests and further reduces the false alarms by allowing only the validated nodes. This algorithm reduces the flooding by limiting its counter and also by not allowing the forged vehicles by attacker.

$$\mathrm{N} = \beta * |u - v \div 2| \quad (2)$$

CCC-MAC

Congestion controlled-Coordinator-Based MAC protocol. They have tried to reduce channel congestion by reducing the transmission time of beacons through the use of multiple data rate. For the propagation of emergency message they have used pulse-based reservation mechanism. In this protocol, dynamic partition of beacon interval has to be done.

EDCA (Extended Distributed Channel Access):

Assuming slot homogeneity, we propose a novel DTMC to model the behavior of the EDCA function of any AC at any load. The main contribution of this work is that the proposed model considers the effect of all EDCA QoS parameters (CW, AIFS, and TXOP) on the performance for the whole traffic load range from a lightly-loaded non-saturated channel to a heavily congested saturated medium. Although we assume constant probability of packet arrival per state (for the sake of simplicity, Poisson arrivals), we show that the model provides accurate performance analysis for a range of traffic types.

A-LDMA (Adaptive Location Division Multiple Accesses)

Analysis and simulation results in highway and city scenarios are presented to evaluate the performance of VeMAC and compare it with ADHOC MAC, an existing TDMA MAC protocol for VANETs. It is shown that, due to its ability to decrease the rate of transmission collisions, the VeMAC protocol can provide significantly higher throughput on the control channel than ADHOC MAC. FPRP is proposed, in which nodes are allowed to contend for more than one slot in a reservation frame according to a certain probability/priority. Simulation results indicate that the proposed mechanism performs better than FPRP in time slot utilization and hence the network throughput under various scenarios. Analysis and simulation results in highway and city scenarios are presented to evaluate the performance of VeMAC and compare it with ADHOC MAC, an existing TDMA MAC protocol for VANETs. It is shown that, due to its ability to decrease the rate of transmission collisions, the VeMAC protocol can provide

significantly higher throughput on the control channel than ADHOC MAC.

FPRP is proposed, in which nodes are allowed to contend for more than one slot in a reservation frame according to a certain probability/priority. Simulation results indicate that the proposed mechanism performs better than FPRP in time slot utilization and hence the network throughput under various scenarios.

4. Conclusion

VANET is that part of MANET that helps the vehicles to communicate easily and helps the collision to occur. Thus VANETs have very high node mobility and limited degrees of freedom in the mobility patterns. This paper presents a brief discussion about the VANET scenario, its attacks and approaches presented by the researchers. In this paper different approaches have been used for detection of different attacks in VANET that degrades the performance of automatic auto driven system. In this paper different approaches have been reviewed and discussed that has been used for detection of various malicious nodes available in the network.

References

[1] Joanne Mun-Yee Lim "Cognitive VANET with Enhanced Priority Scheme" IEEE Conf. on International Conference on Telecommunications and Multimedia,2014,pp-116-121.
[2] Hyun Yu , Joon Yoo, Sanghyun Ahn, "A VANET Routing based on the Real-time Road Vehicle Density in the City Environment", IEEE Conf. on Ubiquitous and Future Networks (ICUFN),2013,pp. 333–337.
[3] Gandhi, U.D., Keerthana, R.V.S.M. "Request Response Detection Algorithm for detecting DoS attack in VANET", IEEE Conf. on Optimization, Reliability, and Information Technology,2014,pp.192–194.
[4] Nikumbh, D.M.; Kharadkar, R.D.; Bhoi, A.D.; Deshmukh, A.Y "Analysis of distance based routing protocol in VANET" IEEE Conf. on Computing for Sustainable Global Development, 2014, pp. 829– 834.
[5] Ravi, K. ; Praveen, K "AODV routing in VANET for message authentication using ECDSA" IEEE Conf. on Communications and Signal Processing, 2014,pp. 1389–1393.
[6] Carpenter, S.E. "Obstacle Shadowing Influences in VANET Safety" IEEE Conf. on Network Protocols, 2014, pp. 480 – 482.
[7] Roselin Mary, S.; Maheshwari, M. ; Thamaraiselvan, M. "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)", IEEE Conf. on Information Communication and Embedded Systems, 2013,pp. 237–240.
[8] Verma, K. ;Hasbullah, H. ; Kumar, A "An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET" IEEE Conf. on Advance Computing Conference, 2013,pp- 550 – 555.
[9] Verma, K. ;Hasbullah, H. "IP-CHOCK (filter)-Based detection scheme for Denial of Service (DoS) attacks in VANET" IEEE Conf. on Computer and Information Sciences, 2014,pp- 1 – 6.
[10] Dawei Mu;XianleiGe; Rong Chai "Vertical handoff modeling and simulation in VANET scenarios" IEEE Conf. on Wireless Communications & Signal Processing, 2013, pp. 1 – 6.
[11] Shenglei Xu; Baichuan hen; Sangsun Lee, "A study on clustering algorithm of VANET environment", IEEE Conf. on Network Infrastructure and Digital Content, 2012, pp. 204–208.
[12] Qiong Yang; Lianfeng Shen, "A Multi-Hop Broadcast scheme for propagation of emergency messages in VANET", IEEE Conference on Communication Technology, 2010, pp. 1072–1075.