Fuzzy Systems and Soft Computing
ISSN : 1819-4362

A study on Discovering and Addressing Black Hole Threats in VANETs

Saruk Mallick[1], Jayanti Manjari Sahoo[2]
Raajdhani Engineering College, Bhubaneswar
[1]sarukmallick@rec.ac.in
[2]jayantimanjarisahoo@rec.ac.in

Abstract

Vehicular Ad hoc Networks (VANETs) combine ad hoc networking, wireless LAN, and cellular technology to enable intelligent Inter-Vehicle Communications (IVC) and Roadside-to-Vehicle Communications. Due to the open nature of the wireless medium, VANETs are susceptible to various potential attacks. Safety stands as a paramount concern for road users, and numerous safety applications such as traffic reports and accident notifications aim to support safety requirements. This research aims to identify attacks in VANETs and understand the attackers by categorizing attack classes. By managing attackers and their actions, lives can be saved. Additionally, an efficient solution is proposed for the Black hole attack, utilizing a redundancy elimination mechanism comprising a rate-decreasing algorithm and a state transition mechanism

.***Keywords:*** *VANET, Inter-Vehicle Communications, Vehicle-to-Vehicle Communications.*

1. Introduction

VANET is a subset of MANET. In VANET each node is a vehicle or RSU (Road Side Unit) which can move freely within the network range and stay connected. Every node communicates with other nodes in single hop or multi hop. VANET provides safe and non-safe services to the drivers [1]. VANET constitutes short-range radios installed in vehicles, Road Side Units (RSUs) and central authorities which are responsible for identity registration and management. Communication in VANET is Vehicle to Vehicle (V-V) and Vehicle to Infrastructure (V-I). However, it is critical for VANET to guard against misuse activities, the overall organization for VANET security architecture must be carefully designed especially when it is a worldwide implemented VANET.

2. Attacks on Vehicular Networks

Before designing any security solution for VANETs [2, 3], we should know different types of security threats, their capabilities, and the types of attackers also.

2.1 Classification of Attackers

Attackers can be classified according to scope, nature, and behavior of attacks [4,5]. Some types of attackers are discussed:

1. Some attackers eavesdrop only on the wireless channel to collect traffic information which may be passed onto other attackers. As these attackers do not participate in the communication process of the network, they are called passive attackers. On the other hand, some attackers either generate packets containing wrong

information or do not forward the received packets. These are called active attackers.

2. Attacker may be an authentic member of a VANET having authentic public keys and access to other members of the network. Such attackers are called insider. Outside attackers (outsider) are intruders and they can launch attacks of less diversity.

3. Some attackers are not personally benefited from the attack. Their aim is to harm other members of the network or disrupt the functionality of a VANET. These attackers are malicious. On the other hand, rational attacker seeks personal benefit and is more predictable in terms of type and target of the attack.

4. Local attacker launches an attack with a limited scope, that is, an attack is restricted to a particular area. An attack can be extended, where an attacker can control several entities distributed across the network.

2.2 Different Attacks on Vehicular Networks

Even if there are advances in VANET but still it has many challenges to be overcome. This challenge is attacks on VANET. Raya et al. [6] classifies attacker as having three dimensions: “insider versus outsider”, “malicious versus rational”, and “active versus passive”. Before designing any security solution for VANETs [7],[8], we should firstly know different types of security threats or attacks. There are different classes of attacks:

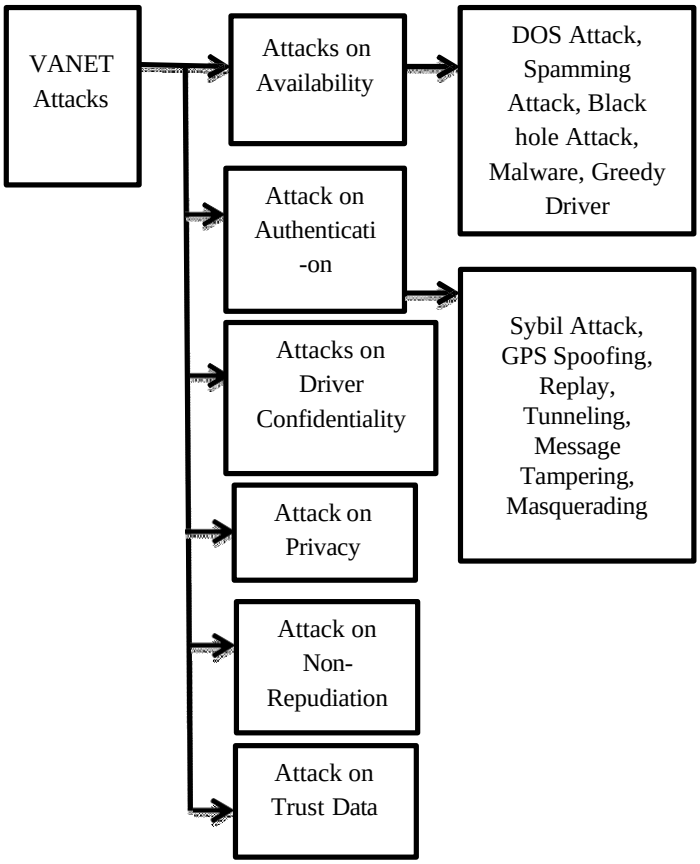


Figure1: Different type of classes of attacks

3. Proposed Algorithm

3.1 Description of Black Hole attack

Security is the major issue in VANET. Majority of the attacks were against Physical, MAC and few more layers which deals with routing mechanism of Vehicular ad hoc network. Primarily the attacks were classified based on the purpose (i.e) not forwarding the packets through routing mechanism, which affects sequence number and hop count. In the Black Hole attack malicious vehicle waits for the neighbors’ to initiate a RREQ packet. Since the receivable RREQ Packet reaches the vehicle, it will immediately send a false RREP packet with a modified higher sequence number. A malicious vehicle where there is a

attack which submerge all data packets of all objects and the packet will not be distributed further.

The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each vehicle of the network has to shares their routing tables among each other. Black-Hole attack involves some modification of the data stream or the creation of a false stream [9]. Figure2 below show a simple scenario of this attack with one malicious vehicle.

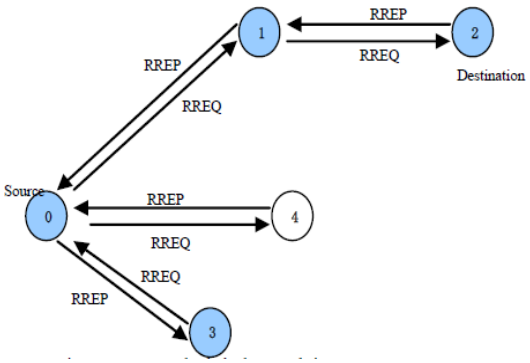


Figure 2: Black-hole attack in progress

The AODV protocol is vulnerable to the well-known black hole attack. AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes. In case of multiple routes, a vehicle selects the route with the highest sequence number. If multiple routes have the same sequence number, then the vehicle chooses the route with the shortest hop count. A malicious vehicle sends Route Reply (RREP) messages without checking its routing table for a fresh route to a destination. As shown in Figure2:above, source vehicle 0 broadcasts a Route Request (RREQ) message to discover a route for sending packets to destination vehicle 2. A RREQ broadcast from vehicle 0 is received by neighboring vehicles 1, 3 and 4. However, malicious vehicle 4 sends a RREP message immediately without even having a route to destination vehicle 2. A RREP message from a malicious vehicle is the first to arrive at a source vehicle. Hence, a source vehicle updates its routing table for the new route to the particular destination vehicle and discards any RREP message from other neighboring vehicles even from an actual destination vehicle. Once a source vehicle saves a route, it starts sending buffered data packets to a malicious vehicle hoping they will be forwarded to a destination vehicle. Nevertheless, a malicious vehicle (performing a black hole attack) drops all data packets rather than forwarding them on.

3.2 Recovery of Black hole

The proposed algorithm performs Efficient Routing in VANET, it detects and recovers the Black hole attack. Here, we modified the header of AODV by adding parent vehicle. The parent vehicle field in the packet is used to get the earlier source of packet. The alternative recovery approach is included in the proposed algorithm which offers the route redundancy to eliminate the need for route repair like link failure sessions.

3.3 Proposed Algorithm

Step-1: Source S wants to communicate with vehicle D. It broadcasts the request message RREQ. RREQ includes the level of security it requires and Did(D's id), a sequential number and Sid is the Source's id encrypted by Destination's public key and Trust Active. RREQ is like this :{ RREQ, seq_num,Sid, Did, T_A}. Where T_A Trust active is the time dependent trust value. Initially vehicle A have the trust value on vehicle B is at time t1; but after a certain period, vehicle B may travel to another zone which is out of radio range of vehicle A due to vehicles mobility in VANET. At time t2, vehicle B happens to back in vehicle A's range again. The trust value should decay during this time gap. Let ATB (t1) be the trust value of vehicle A to vehicle B at time t1 and ATB (t2) be the decayed value of the same at time t2. Then trust active is defined as follows,

$$(t_2) = {}_AT_B(t_1) * e^{-({}_AT_B\ n\ \Delta t)}\ (\ )^{2k}$$

Step-2: Vehicle A receives RREQ. It looks up its trust list for the trust values of the neighbors. And A will encrypt if own id with proper policy and append in the message. The message which will sent by A is

like this: {RREQ, seq_num, $P_b\ D[P_v|A[A_{id}], P_bD[Sid], Did, _B$ } where $P_v\ A$ is R^A

the private key of A. Where R^A (Vehicle proposal) is also used to identify the malicious behavior,

Evaluating the recommendation is given by R^A_B which is vehicle A's evaluation to vehicle B by collecting recommendations, $R^A_B = \frac{\sum_{v\in\gamma} V|A\rightarrow C| * V|C\rightarrow B|}{V|A\rightarrow C|}$

γ is a group of recommenders.

$V|A \rightarrow C|$ is trust vector of vehicle A to C.
$V|C \rightarrow B|$ is trust vector of vehicle C to B.

Step-3: D receives RREQ. It uses its private key and the public key of the intermediate vehicles to authenticate them. D checks if there are any bad vehicles. If they are all trusted, D generates a number for the flow Fid, and broadcasts the following message (suppose A and B are the intermediate vehicles): {RREP, Pb B[Fid , Pb A[F_{id} , Pb S[Pv D[F_{id}]]]]};

Table 1: Performance of various vehicles

No. Of nodes	Generated Packets	Received Packet	Packet Delivery Ratio	Total Dropped Packets	End-to-End Delay
10	20205	19956	98.7676	171	224.082
20	22308	22164	99.3545	97	237.122
30	20147	19897	98.7591	155	223.827
40	23372	23248	99.4695	70	247.197
50	23331	23210	99.4814	67	305.031

Step-4: Intermediate vehicle that receives the RREP uses its private key to decrypt the message and gets the flow id. Then it updates its route table with Fid designated to destination D;

Step-5: S receives RREP, uses its private key to decrypt the message and D's public key to identify the destination. Afterwards, it will send message with the vflow id Fid.

Step-6: Cluster Head maintains the Trust threshold value based on trust active and vehicle detect the attacks. If any vehicles below the Trust threshold value that vehicle is encountered by an attacks.

4. Results

Scenario of 10 Vehicles

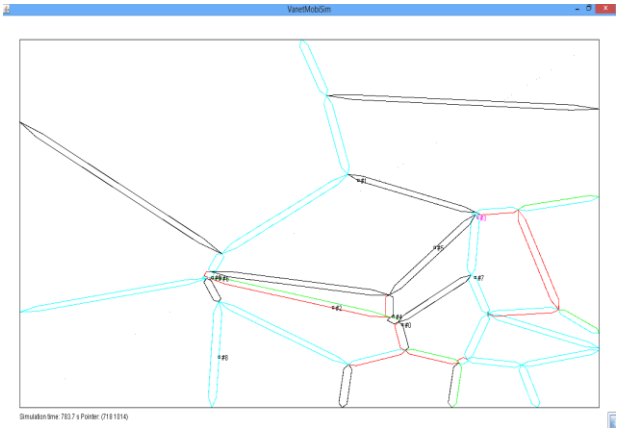
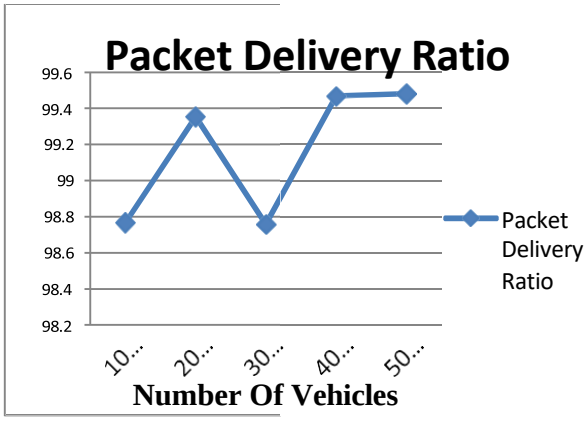


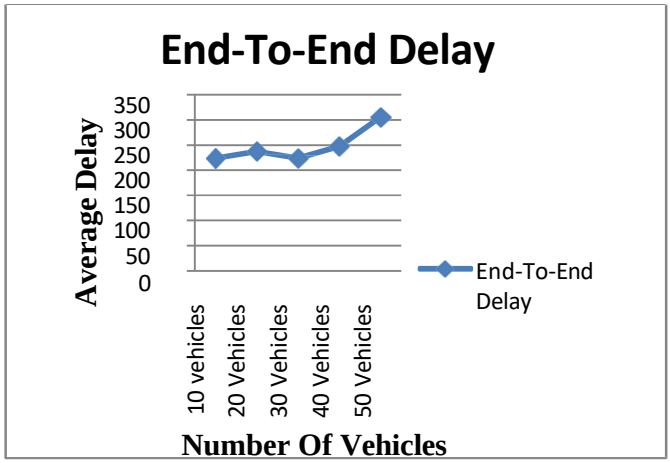
Figure 3: 10 Vehicles.

The above figure is showing the scenario of 10 vehicles.

Proposed algorithm used the 10 node scenario, also having the similar for 20,30,40,50 nodes



.



Figurer 5: End to End graph

Conclusion

VANETs are mainly used for improving efficiency and safety of (future) transportation. There are chances of a number of possible attacks in VANET due to open nature of wireless medium. VANET generally consist of On Board Unit (OBU) and Roadside Units (RSUs). OBUs enables short-range wireless adhoc network to be formed between vehicles. Each vehicle comprises of hardware unit for determining correct location information using GPS. Roadside Units (RSUs) are placed across the road for infrastructure communication. There is safety and non-safety messages are forwarded between the Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) on this communication medium. Cooperation between the vehicles is essential to communicate with each other because of the short range of wireless communication medium. The attacker generates problems in the network by getting full access of communication medium due to open nature of the medium. In the black hole attack, node is used to advertise a zero metric to all destinations, which become cause to all nodes around it in order to route data packets towards it. The AODV protocol is vulnerable to such kind of attack because of having network centric property, where each node of the network has to shares their routing tables among each other. By this research, Black hole attack is efficiently removed by the extended AODV technique. By using this technique black hole attack is easy to detect, manage and recover. Here packet delivery ratio is increased and end-to-end delay gets decreased.

References

[1] Bernsen, J. Manivannan, D., "Routing Protocols for Vehicular Ad Hoc Networks That Ensure Quality of Service" In the fourth international conference on Wireless and Mobile Communications., pp.1-6, Aug. 2008.

[2] T. Leinmuller, E. Schoch, and C. Maihofer, (2007) "Security requirements and solutions concepts in vehicular ad hoc networks". In Proceeding of Fourth Annual Conference on Wireless on Demand Network Systems and Services.

[3] P. Papadimitratos, V. Gligor, and J. P. Hubaux, (2006) "Securing vehicular communications—assumptions, requirements, and principles". In Proceedings of the Workshop on Embedded Security on Cars (ESCAR).

[4] M. Raya and J.-P.Hubaux,(2007)" Securing vehicular ad hoc networks". Journal of Computer Security, 15(1), 39–68.

[5] A. Aijaz, B. Bochow, F. Dtzer, A. Festag, M. Gerlach, R. Kroh, andT. Leinmuller, (2006) "Attacks on inter-vehicle communication systems—an analysis". In Proceedings of the 3rd international Workshop on Intelligent Transportation (WIT).

[6] Raya, M., &Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1–11), Alexandria, VA.

[7] T. Leinmuller, E. Schoch, and C. Maihofer, (2007) "Security requirements and solutions concepts in vehicular ad hoc networks". In Proceeding of Fourth Annual Conference on Wireless on Demand Network Systems and Services.

[8] P. Papadimitratos, V. Gligor, and J.-P. Hubaux,(2006) "Securing vehicular communications— assumptions, requirements, and principles". In Proceedings of the Workshop on Embedded Security on Cars (ESCAR).

[9] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin and Aamir Hassan (2012) Telecommunication System, Vol. 51, Issue 2&3.