ISSN 2278-9723
DOI:10.31838/ijccts/09.02.01

Research Article

Routing Attacks in Vanets

RANGISETTI RAJASEKHAR, K ANNAPURNA
Dept. of ECE, Vignan's Foundation for Science, Technology and Research (Deemed to be University)
Email: rplkrishna92@gmail.com[1], arya.anu85@gmail.com[2]

Received: 10.07.21, Revised: 12.08.21, Accepted: 08.09.21

ABSTRACT
Now-a-days many accidents are taking place due to inefficient drivers, traffic congestion, violation of traffic laws, inadequate road information, increased automobile usage, and due to lack of security assured infrastructure. With the help of intelligent road transportation system, researchers and industry people are enhancing the vehicular communication to reduce the number of accidents. VANET is a sub class of MANET, which is a very promising and latest technology. Security means protecting the privacy (confidentiality), availability, integrity and non-repudiation. Security implies the identification of potential attacks, threats and vulnerability of a certain system from unauthorized access, use, modification or destruction. A security attack is any action that compromises or bypasses the security of information illegally or in an unauthorized way. In this paper, the need for security, different possible attacks in VANETs and how to overcome them are presented.

keywords: V2V, V2I, VANET, Security, Availability, Privacy, Data Integrity, DSRC, Attacks, Challenges, preventive measures.

1. Introduction

A mobile ad-hoc network (MANET) is a type of wireless network, which configures its mobile nodes dynamically according to the position of nodes. It does not have any fixed infrastructure and contains any centralized coordinator for route establishment. As MANET nodes move randomly, topology of the network also varies frequently. Each node forwards data to other specified nodes and behaves like a router in the network. Each node in the network has a predefined distance range for data transmission. It is well suited for specific applications like battlefield environment, emergency response environment, sensor networks, vehicular networks, etcetera [1].

When compared to MANET, the VANET is more vulnerable to security threats because of its special characteristics such as dynamic topology and high mobility [2]. Security in VANETs is important as it contains safety messages, which are life-critical information. In addition to these messages if the priority [3][4][5] of vehicles is also informed then the high priority vehicles like ambulance will be provided clear route. In V2V communication, either fully connected or partially connected mesh network is used. As VANET is a wireless network it can easily be affected by different attacks such as wormhole, black hole, gray hole, Sybil attacks and so on.

2. Vanet Architecture

VANET is a subset of ad-hoc networks that consists of a vehicles, these vehicles can act as nodes. It contains three components namely On board units (OBUs) Road side units (RSUs) and trusted authority (TA). OBUs is placed inside the vehicles, which includes sensors, GPS and other devices. It acts as both transmitter and receiver. RSUs are placed besides the junctions, which collects the information from vehicles and broadcast that information to its nearest vehicles with in its range. TA is a third party which provides the security of authentic users. The main purpose of these networks is to send the safety related messages to drivers.

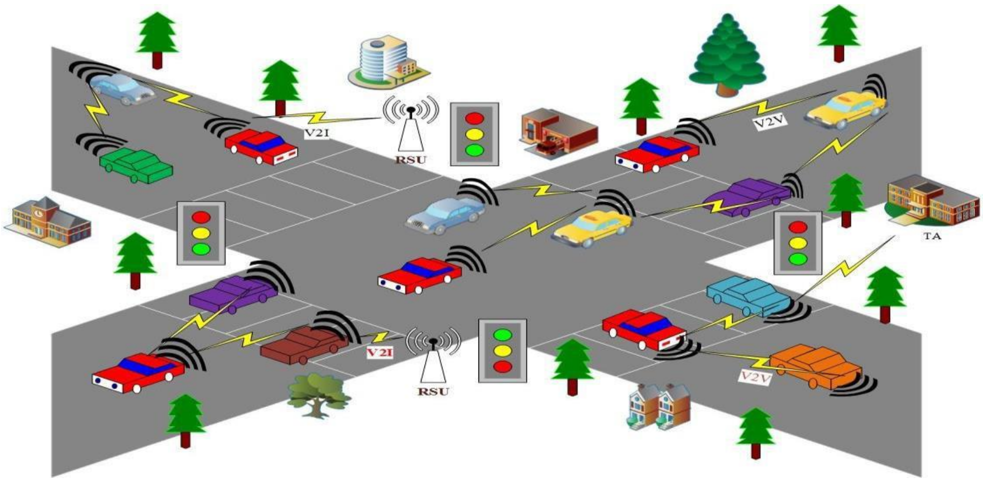

Fig.1: Vanet architecture

3. Security and privacy requirements in Vanets

Due to high mobility of VANETs they are easily prone to attacks. If any attacker succeeds in attacking then it leads to economical loss and sometimes life loss too. So it has to provide early warning messages about safety and comfort information like road conditions, road accidents history, nearby hotel and petrol station to drivers. All this information needs to be updated time to time. Security and privacy parameters to be considered for VANETs are discussed here.

Availability

It is a principle of security, which ensures that a resource /RSAP is available for authorized users only. But many attackers try to make the resources unavailable to the users. If the resources are unavailable, data cannot be transmitted and the utilization of resources will be reduced. So there is a need to address this attack.

Confidentiality

Confidentiality ensures that only the sender and receiver of the message get the contents of message and no other node should aware of data.

Authentication

Data authentication permits user or receiver to check whether the data was sent by the authorized user or not. In point to point communication, this mechanism is achieved through symmetric cryptography, in which the sender and the receiver share a secret key to encode/decode the information.

Data Integrity

Integrity ensures the information is received correctly without any alteration by attacker duringits transmission from source to destination.

Vehicle Privacy

The information shared should be readily accessible to authorized nodes and Road side access points (RSAPs). Such information must not be disclosed to unauthorized users to maintain privacy. Confidentiality among authorized users can guarantee the privacy of the information and hence network security.

Authorization

Authorization means giving the authority to authenticated users to access the all resources ofthe network.

Tracking of vehicle ID

Smart cars are equipped with modern hardware and software that helps to track and locate the vehicles. Modern GPS technology is used to the track the vehicles anywhere in the world. It is helpful for owners to protect the vehicles from dangerous situations.

Scalability

Without disrupting network efficiency, VANET should be able to allow number of additional vehicles. If the number of nodes increases, the complexity of the network increases and reduces the efficiency of the system.

Network Efficiency

Network efficiency means how efficiently it exchanges information to its neighbor nodes. By lowering overhead, reducing computation and delays, VANET efficiency can be increased.

Data Freshness

Messages should be updated at regular intervals of time to prevent the use of old messages, which may lead to wrong conclusions. For example, The first message is “Heavy traffic” and if the present status is “Road is free”. If one does not update the message, then he may think it is busy route and unnecessarily he will change the route.

4. Attacks on VANETS

This section classifies and introduces possible attacks against various routing protocols in the previous section. These attacks can be classified into two categories.

Routing-disruption attacks. In this kind of attacks, the attacker tries to act in such a way that seems actual data packets were directed in a dysfunctional path. Some examples of these attacks are mentioned as follows:

Blackhole

An attacker in a black hole attack distributes fake routing information to attract the traffic like, claiming falsified short distance information. This attacker then drops the data packets and hence full data is lost.

Gray hole

This attack is similar to the black hole attack, but the attacker drops the selective pacets instead of all packets.

Warmhole attack

warm hole attack is one of the major attacks in the MANET. The attackers gets a strong location in a network in a worm hole attack. Attacker in a worm hole attack make use of this location as a shortest path between nodes. Attacker advertises this node as a shortest path to all other nodes for transmitting data.

Rushing

The rushing attack, which result in denial of services when used against all previously published on-demand ad-hoc network routing protocol. When a node send a route request packet (RR packet) to another node in the wireless network, if there is an attacker then it will accept the RR packet and send to its neighbour with high transmission speed as compared to other nodes, which are present in the wireless network. Because of this high transmission speed, packet forwarded by the attacker will first reach the destination node. Destination node will accept this RR packet and discard other RRs (ROUTE REQUESTS).

Impact of rushing attacks

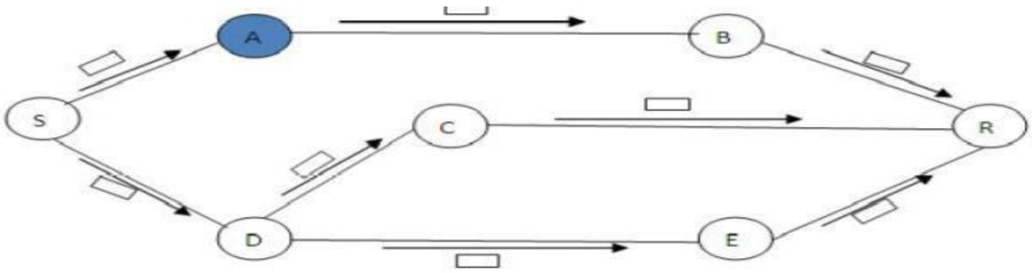

Fig.2:Attacker node nearer the sender

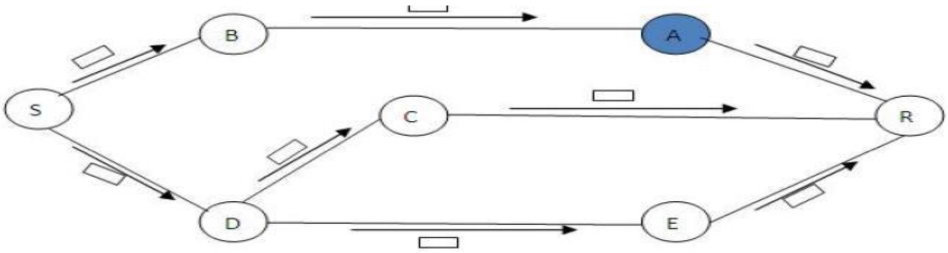

Fig.3: Attacker node nearer the receiver

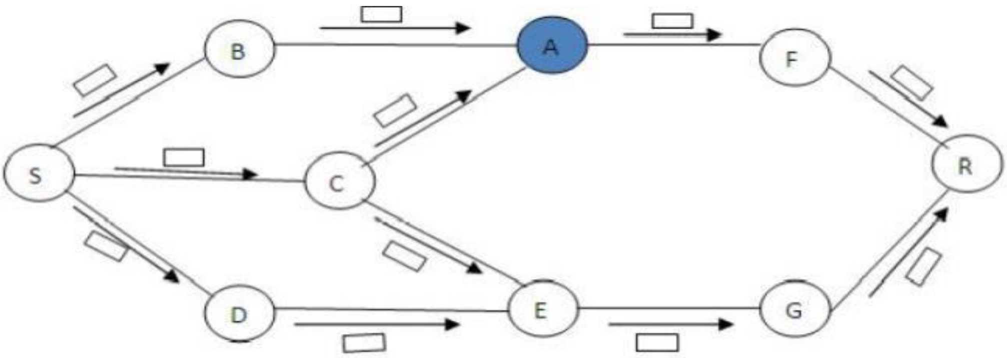

Fig.4: Attacker node at anywhere in the receiver

Resource-consumption attacks

In this category of attacks, the attacker adds extra packets into the network to waist essential network resources such as bandwidth, etc. Moreover, the attacker sometimes tries to consume the node resources such as memory or computation power.

Author	**Title**	**Attack**	**Preventive techniques**
Tyagi, and Dembl 2017.[6]	Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)	Black hol	In this paper ,author Usin pseudo reply packet(PRREP)
Chaudhary2020.[7]	A Fuzzy Logic-Based Contro System for Detection and Mitigation of Black hole Attac in Vehicular Ad Hoc Network https://doi.org/10.1007/978-981-15 0128-9_15163	Blackhole	Initially using trust based an after applying fuzzy logic
Mustikawati et al., 2017.[8]	Network Security Analysis in Vanet Against Black Hole an Jellyfish Attack with Intrusion Detection System Algorithm.	Blackhole jellyfish	In this approach the autho rejects the first RREP and wait second RREP (Route Reply).
Krzysztof Stepien et al., 2020.[9]	Security methods against Blac Hole attacks in Vehicular Ad-Hoc Network	Blackhole	In this approach the autho used SIN(connecting so-called intelligent nodes)algorithm with AODV routing protocol in that adde CRRT(coming route reply table).
Mahmood et al.,2020.[10	Review of Prevention schemes fo Replay Attack in Vehicular Ad ho Networks (VANETs)	Replay attack	Symmetric cryptography digital signature, has function, elliptical curv parameter and ID registration technique.

YING GAO and HONGRUI WU 2019.[11]	A Distributed Network Intrusio Detection System for Distributed Denial o Service Attacks in Vehicular Ad Hoc Network	DDOS	Spark-ML RF-Base algorithm.
Tanwar et al., 2018.[12]	A systematic review on securit issues in vehicular ad hoc network Security and Privacy.	Privacy	PublicKey, Symmetric and Hybrid, Certificat Revocation , ID-based Cryptography.

5. Conclusion

Because of special properties and requirements of mobile Ad-Hoc networks, it is very difficult to make them secure. In order to defend against existing attacks, many protocols are offered by researchers but still are many drawbacks. If one is able to predict [13] the attack based on history then there will be a chance of detecting the attacks easily. There is need to improve the detection techniques of those attacks.

References

1. Eze E., Zhang S. and Liu, E.(2014) "Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward", 2014 20thInternational Conference on Automation and Computing.
2. Jana B, Mitra S, Poray J.(2016) “An analysis of security threats and countermeasures in VANET”. Paper presented at: 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE); 2016:1-6.
3. Annapurna K., Seetha Ramanjaneyulu B. (2021) “Timeout- Aware Inter-Queuing for QoS provisioning of Real-Time secondary users in Cognitive Radio Networks”, Microelectronics, Electromagnetics and Telecommunications Lecture Notes in Electrical Engineering, vol. 655. Springer, Singapore., 693-700.
4. Seetha Ramanjaneyulu B., Annapurna K.(2021) “Supporting Real-Time Data Transmissions in Cognitive Radio Networks using Queue shifting mechanism”, International Journal of Embedded and Real-Time Communication Systems, 12(1), Jan- Mar 2021.
5. Satish Kumar K., Annapurna K., Seetha Ramanjaneyulu B.(2015) “ Supporting Real Time Traffic in Cognitive Radio Networks”, IEEE conference proceedings (SPACES-2015), KLU, pp:482-485.
6. Tyagi P. and Dembla D.(2017) “Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad- hoc network (VANET),” Egypt. Informatics J., vol. 18, no. 2, pp. 133–139, 2017.
7. Chaudhary A. (2020) “A Fuzzy Logic-Based Control System for Detection and Mitigation of Black hole Attack in Vehicular Ad Hoc Network”. https://doi.org/10.1007/978-981-15-0128- 9_15163.
8. Mustikawati E., Perdana D., and Negara R. M.(2017) “Network Security Analysis in Vanet Against Black Hole and Jellyfish Attack with Intrusion Detection System Algorithm”.
9. Krzysztof Stepien, Aneta Poniszewska-Maranda (2020) ” Security methods against Black Hole attacks in Vehicular Ad-Hoc Network”.
10. Mahmood A. et al.,(2020) “Review of Prevention schemes for Replay Attack in Vehicular Ad hoc Networks VANETs”.
11. YING GAO, HONGRUI WU (2019) ”A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network”.
12. Tanwar S, Vora J, Tyagi S, Kumar N, Obaidat MS.(2018)” A systematic review on security issues in vehicular ad hoc network”. Security and Privacy 2018;1:e39. https://doi.org/10.1002/spy2.39.
13. K.Annapurna, B.Seetha Ramanjaneyulu, C.Lakshmi Chaitanya, T.Hymavathi, “Spectrum Prediction in Cognitive Radio Networks using Neural Networks”, International Journal of Control Theory and Applications, vol.10, issue.28, May 2017.