Concordia Institute for Information System Engineering

(CIISE)

INSE 6120

Cryptographic Protocols and Network Security

Project Report

Submitted to:

Professor Dr. Ivan Pustogarov

Submitted By:

Student Name	Student ID
Dhruv Haribhakti	40172725
Dhrumil Sunil Chablani	40195291
Mohammed Rabith Tarapathi	40169519
Adnan Zuhaib	40185537
Amarvir Singh	40188944
Susmita Kar	40200023
Mahima Shukla	40206690
Varsha Anand	40188524
Jaimin Tejani	40198405
Oluwatomiwa Oluboba	40137501
Simran Kaur Gill	40205922

TABLE OF CONTENTS

1. Abstract

Today's cyber threats come from a wide array of potential attackers, which range from highly sophisticated state-sponsored adversaries to insiders helping external hackers or initiating their own incursions. In recent years, there has been massive evolution of automotive technology and with these new developments, modern vehicles are getting increasingly astute offering growing quantities of innovative applications that cover various functionalities that are controlled by hundreds of Electronic Control Units (ECUs). These features expose new attack surfaces that can be harnessed by attackers. Therefore, making them vulnerable to common threats such as malware injection can compromise the overall security of modern vehicles. In this project, we aim to provide an in-depth analysis of various security issues and vulnerabilities that impact vehicular systems and security in order to identify challenges and propose its security countermeasures. Furthermore, this report intends to become familiar with the crypto protocols used in the attacks with available defenses and how they can be applied to secure intelligent vehicles against emerging malware threats that can compromise the security of today's vehicles.

2. Introduction

2.1 Autonomous Vehicles

Autonomous vehicles can be defined as automobiles that are capable of sensing its surrounding environment and carry out operations with little to no human interaction. The Society of Automotive Engineers (SAE) has defined 6 levels of automotive vehicles.

Level	Description	Class
Level 0	Manual control. The human performs all driving tasks.	No Automation
Level 1	Vehicle features a single automated system.	Driver Assistance
Level 2	Vehicle can perform steering and acceleration. The human still monitors all tasks.	Partial Automation
Level 3	Environmental detection capabilities. The vehicle can perform most driving tasks, but human override is still required	Conditional Automation
Level 4	Vehicle performs all driving tasks under specific circumstances. Geofencing is required. Human override is still an option.	High Automation
Level 5	Vehicle performs all driving tasks under all conditions. No human interaction required.	Full Automation

Note: All the technologies and attacks set forth in this project operate on autonomous vehicles of level 2,3 and 4.

2.2 Vehicular Ad-hoc Network (VANET)

Vehicular Ad-hoc Network (VANET), which is the subclass of the Mobile Ad-hoc Network (MANET), the main objective of the is to create the Intelligent transportation system, which helps to reduce the traffic congestion and accidents on roads. Moreover, VANETs are also responsible for the communication between the moving vehicles in the certain range of area.

Vehicles can communicate with each other by vehicle-to-vehicle communication (V2V), or the vehicle can communicate with the entities like Road side unit (RSU) by Vehicle to Infrastructure (V2I). Main role of VANET is to create the communication environment between various moving vehicles in certain area without any central authority(hub) to handle the different difficult situations like road closure or accidents.[1]

2.3 Ad hoc On-Demand Distance Vector (AODV)

AODV is an on-demand distance vector routing protocol wherein the protocol uses distance or hop count as its primary metric for determining the best forwarding path. It is an on-demand protocol as the source node does not carry complete path to the destination, each node knows only its previous and next hop.

The Goals accomplished by AODV are:

- Minimized Broadcast
- Minimize transmission latency (when new routes are needed)

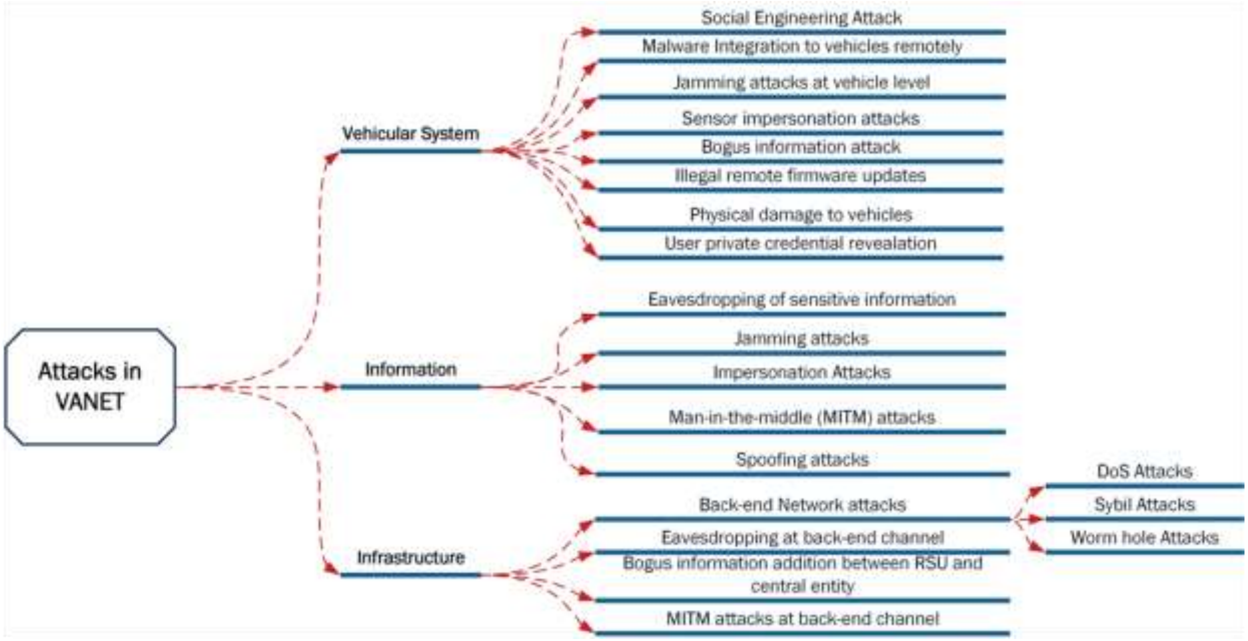
AODV has two main stages:

- Route Discovery: Route discovery process starts when a source node does not have routing information for a node to be communicated. Route discovery is initiated by broadcasting a RREQ message (<source_addr, source_seq_no, bcast_id, dest_addr, dest_seq_no, hop_cnt>). The route is established when a RREP message is received. A source node may receive multiple RREP messages with different routes, it chooses the route which has the least hop count.
  Reverse path setup: While transmitting RREQ messages through the network each node notes the reverse path to the source. When the destination node is found the RREP message will travel along this path, so no more broadcasts will be needed. For this purpose, the node on receiving RREQ packet from a neighbor records the address of this neighbor.
- Route Maintenance: When a node in an active route gets lost, a route error message (RERR) is generated to notify the other nodes on both sides of the link of the loss of this link.

3. Key Concepts (or Tools used)

Tools Used	Version	Description
Network Simulator (NS)	NS2: 2.35,2.28,2.24 NS3: 3.27,3.19,3.29	It is a discrete event simulator which depicts the dynamic nature of the network communications. It supports execution of different protocols over wired or wireless communications
NAM	1.15	It is the animator tool which is used by the simulators (NS) for viewing the network animation traces and real-world packet traces
NetSim	11.1	A Network simulator and emulator used for Wireless sensor Network
xgraph	12.2	It is used to show a graphical representation for parameters characteristics like throughput, drop, latency etc.
VEINS (using OMNETT++ and SUMO)	5.2	It is network-based simulator for executing the vehicular based project. It uses OMNETT++ and SUMO as a framework.

4. Background and Attacks


Attacks in VANET
Vehicular System
Social Engineering Attack
Malware Integration to vehicles remotely
Jamming attacks at vehicle level
Sensor impersonation attacks
Bogus information attack
Illegal remote firmware updates
Physical damage to vehicles
User private credential revealation
Information
Eavesdropping of sensitive information
Jamming attacks
Impersonation Attacks
Man-in-the-middle (MITM) attacks
Spoofing attacks
Infrastructure
Back-end Network attacks
Eavesdropping at back-end channel
Bogus information addition between RSU and central entity
MITM attacks at back-end channel
DoS Attacks
Sybil Attacks
Worm hole Attacks

Types of Attacks on VANET [2]

4.1 Blackhole

In blackhole attack, the malicious node in the routed network tries to attract some or all the network traffic by sending a route reply with the shortest route possible. After directing the packet from the real node towards the malicious node instead of directing it to the original destination, the malicious node drops the packet in between, thus preventing it from reaching the destination and blocking the ability to communicate with the destination which creates an effect like blackhole.

Problem caused by Blackhole on VANET:

In VANET, blackhole attack has two steps: the malicious node broadcasting to have shortest route to a node requesting for route; and, the malicious node dropping that packet received instead of relaying ahead. Basically, the malicious node will reply to routing control messages used to verify and maintain the connectivity to other nodes in the network, so that this attack is more difficult to detect as no route error messages are broadcasted which can signal a loss of connectivity.

Detection and Prevention of Blackhole on VANET:

We will be discussing the detection approaches for detecting the blackhole attack. We take into consideration 2 different approaches based on AODV routing protocol.

- Approach 1:
  The first approach is based on detecting blackhole attacks via neighbor awareness. "Neighborhood based blackhole detection" is the name given to it. Every node in this strategy will look out for their neighbors. The list of trusted and Non-trusted nodes is maintained by Neighbor. Individual node's incoming and outgoing traffic will be monitored by neighbor nodes. SEND PKT and RCV PKT are two counters that the neighbor node will keep track of. If the difference between two counter values exceeds a certain threshold value (Th), the node is classified as malicious. Initially, all nodes will be assumed to be Trusted Nodes, and entries in the Trusted Node list will be created. However, after it has been declared a malicious node, it will be removed from the trusted list and placed in the Non-Trusted List.

  Algorithm: In this section, we'll look at a neighborhood-based technique to blackhole discovery. We used SN for Source Node, DN for Destination Node, SN ID for Source Node ID, DN ID for Destination Node ID, MN for Malicious Node, MN ID for Malicious Node ID, SEND PKT for Number of packets sent by particular node, RCV PKT for Number of packets received by particular node, NN for Neighbour Node, EN for Each Node, MN ID for Mal List Trusted Node contains a list of trusted nodes, while List Non-Trusted Node has a list of non-trusted nodes. RSU stands for Roadside Unit. RREQ is for Route Request, and RREP stands for Route Reply. Block Node List is a list of nodes that RSU has blacklisted.

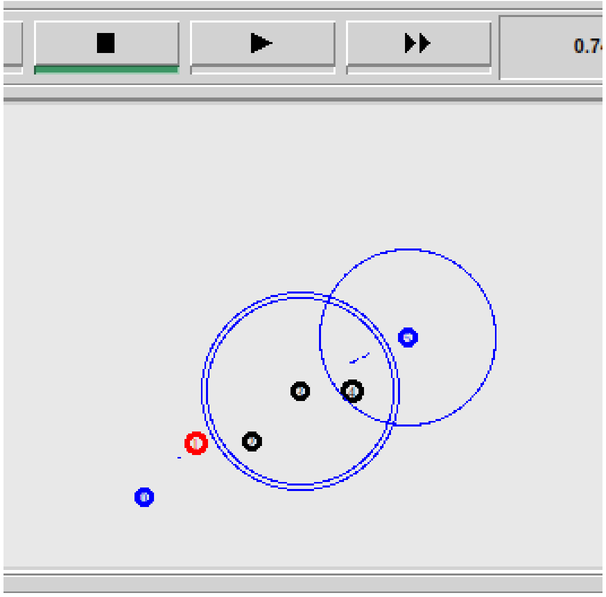
Step 1: At first, a source node that is unsure of the location of the destination node broadcasts a Route Request Message (RREQ). The source Node ID, Destination Node ID, Source Node Sequence No, and Broadcast ID are broadcasted with the Route Request.
Step 2: Different nodes receive the RREQ sent by Source Node and send Route Reply Message (RREP) to Source Node based on it.
Step 3: At first, all neighbor nodes will be treated as Trusted Nodes, and List Trusted Node will keep track of their Node Ids.
Step 4: Neighbors nodes will continuously check each node's in and out data transfer in order to detect malicious nodes. If the difference is greater than the threshold value (Th), the node will be identified as a malicious node. The threshold value will be determined depending on the network's current average drop rate.
Step5: Following the management of the trusted and non-trusted node lists, each node will submit its non-trusted node list to the appropriate RSU. RSU will get a list of all non-trusted node lists from each node within the range and create a block node list based on that information. This block node list will be sent to every node in RSU's range.
Step 6: Based on the updates provided by RSU, all nodes will update their trusted and non-trusted node lists.

- Approach 2:
  The second approach is based on the concept of identifying greater sequence numbers. "Sequence Number based blackhole detection" is the name of the technique. In this technique, each node will keep track of which nodes are trusted and which are not. If the source node receives a response from any node with the highest sequence number, it will be considered malicious. As described in Approach-1, all nodes will be treated as trusted nodes at first, and if a malicious node is discovered, it will be removed from the trusted node list and added to the non-trusted node list.
  The sequence number identification approach will be used to find blackholes in this algorithm. We used SN SEQ for Source Sequence Number, DN SEQ for Destination Sequence Number, and RT for Routing Table instead of approach.

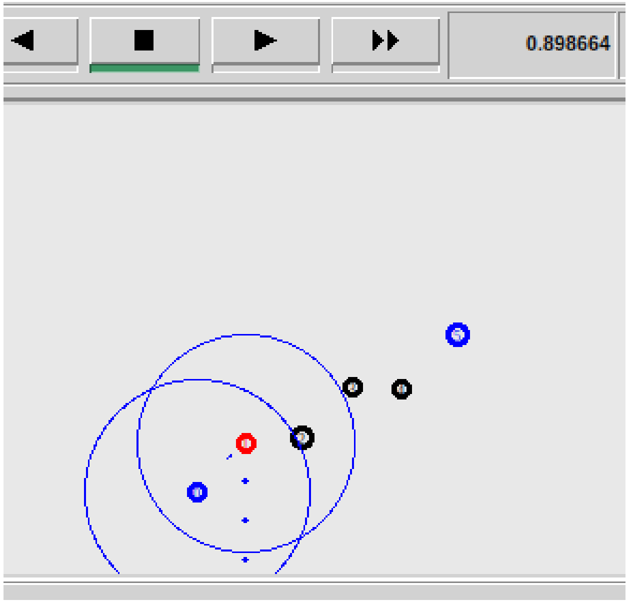
Step 1: At first, a source node that is unsure of the location of the destination node broadcasts a Route Request Message (RREQ).
Step 2: Different nodes receive the RREQ sent by Source Node and send Route Reply Message (RREP) to Source Node based on it.
Step 3: At first, all neighbor nodes will be treated as Trusted Nodes, and List Trusted Node will keep track of their Node Ids.
Step 4: If a source node returns a route response with an extremely big Sequence Number, that node is considered malicious.
Step 5: Once the list of trusted and non-trusted nodes has been managed, each node will communicate its non-trusted node list to the appropriate RSU. RSU will

get a list of all non-trusted node lists from each node within the range and create a block node list based on that information. This block node list will be sent to every node in RSU's range.

Step 6: Based on the updates provided by RSU, all nodes will update their trusted and non-trusted node lists.



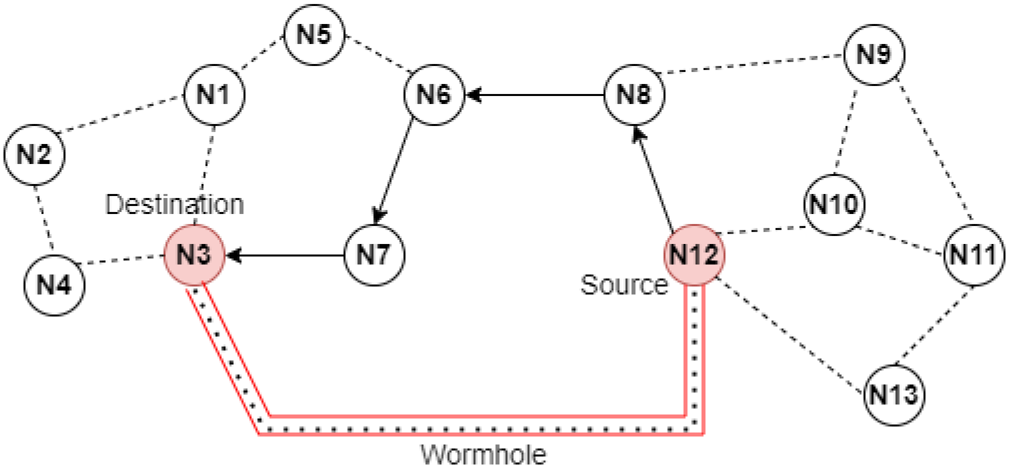
Non-malicious simulation of AODV



Malicious Node dropping packets

4.2 Wormhole

Wormhole attack is the most dangerous attacks on VANETs because of the variety post exploitation options. In this, the attacker may create 2-3 extra nodes which act as the part of any ad-hoc network to deploy the attack. The main idea is to create the communication tunnel between these malicious nodes (created by the attacker) and transfer the data from one destination to other through these nodes (a tunnel).



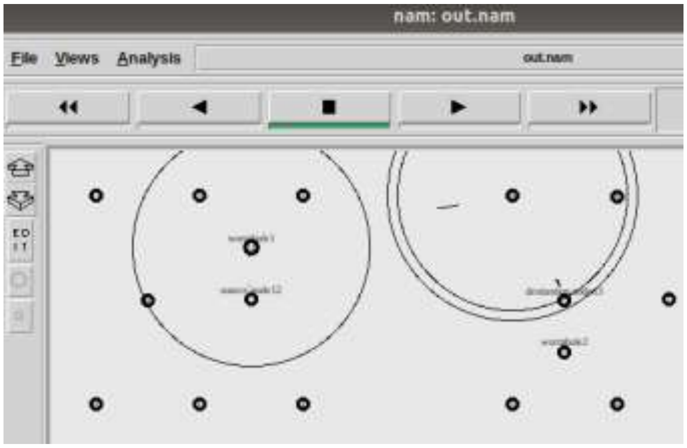
As in the above image the attacker creates the two malicious nodes N3 and N12 which is used to listen to the communication of the network for a while. To launch this attack, these nodes will publicize themselves to other legitimate nodes as the shortest path to transfer the data using the tunnel. The route introduced by the attacker nodes N3 and N12 is harder to predict as malicious route because it is not the part of real network. Fig, above shows where the node N10 wants to transfer the data to N1 node, as the N12 and N3 are the neighboring nodes of them and the tunnel is created and data is recorded at the N12 node end and after editing and tampering the data is transferred to the N3 node.[3]

Classification of Wormhole Attacks

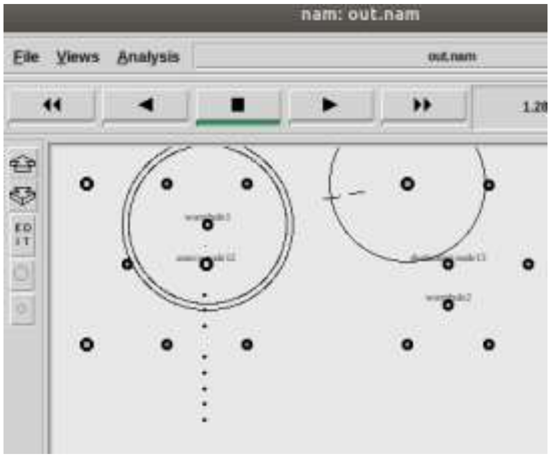
Based on implementation Process	Using packet encapsulation	In this attack the one legitimate source node sends some data to other legitimate node, firstly the source legitimate node broadcasts packets seeking the shortest path, the malicious node encapsulates the request and broadcast to colliding node and other malicious node rebroadcast the packets, which results in the legitimate node to select the malicious tunnel route as it has lesser number of hops and quickest in response as compared to other legitimate routes.
	Using out-of-band channel	In this mode, two malicious nodes are introduced that uses the direct wireless link or long range directional wireless link to forward the route request. This mode is hard to launch because it requires special hardware
	Using packet relay	In this mode, malicious node relay packets among two nodes that are far apart to convince them that they are neighbors.
Based on Communication Medium	Out of band Wormhole	In this type of attack the external communication medium is used to set the direct link between two end points and transfer the data.
	In band Wormhole	Here, the attacker makes an overlay tunnel over the actual wireless medium, and it does not use any external communication medium between two end points.

Prevention: The wormhole attacks can be prevented by registering each node which are include in the VANET communication over the network. In this way each node provided with unique id to maintain the record of each node participating in communication. The authenticated users or nodes decrease the possibility of the out-of- band channel wormhole attack as attackers would not be able to disrupt the route.

Each message or data transferred between two nodes should be hashed so if the attacker tries to change or modify the data then the hashing value also change to declare the attack happened on the network to avoid the formation of wormhole tunnel in the network.[4]



Non-Malicious Simulation of AD-Hoc Network



Malicious node dropping packets

4.3 Denial of Service (DOS)

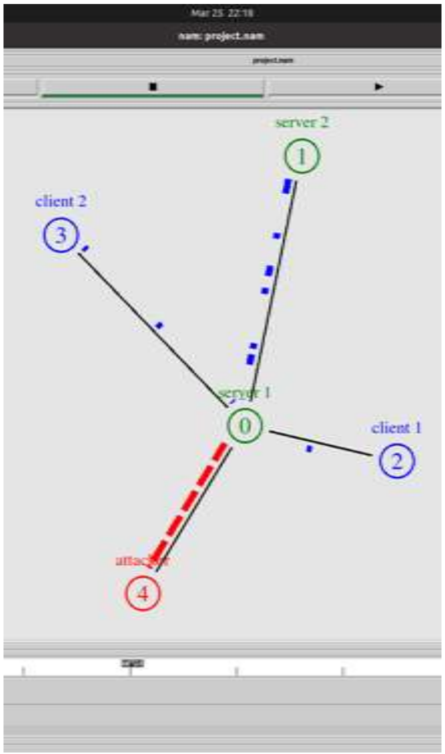
Vehicular ad hoc network is a sub-class of Mobile ad hoc network wherein the vehicles move freely and communicate with each other and with the roadside unit. These units are self-organized and freely mobile which makes them able to interact with any node which may or may not be trustworthy and is thus exposed to various attacks and threats. [5]

A DoS attack denies all the services of VANET. A DoS attack can be carried out on VANET in the following two modes:

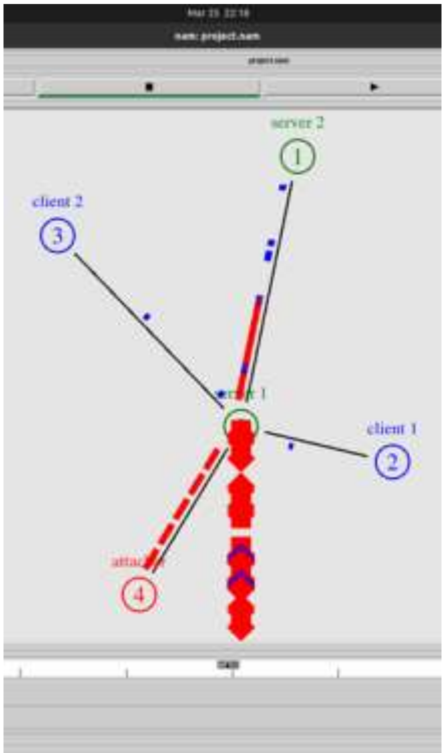
- Application Mode: In this mode, the attacker blocks the entire bandwidth and the data exchange between the nodes is completely jammed. A DoS Attack mainly poses a threat to the availability of the system. The main motive of a DoS Attack is to jam the network. The node stops receiving all the important messages such as, navigation and safety messages. This attack can promote a greater number of accidents and traffic jams.
- Network Mode: In this mode, the attacker broadcasts a wrong message to all the nodes and diverts messages to wrong paths by changing the headers of the frames as they are not encrypted. This attack also pose threat to the integrity of the system. The attacker may feed wrong messages and alerts to the particular group of nodes. This may lead the nodes to redirect to a new route and gather all-together to a common route, thus, leading to a traffic jam.

<u>Implementation:</u>

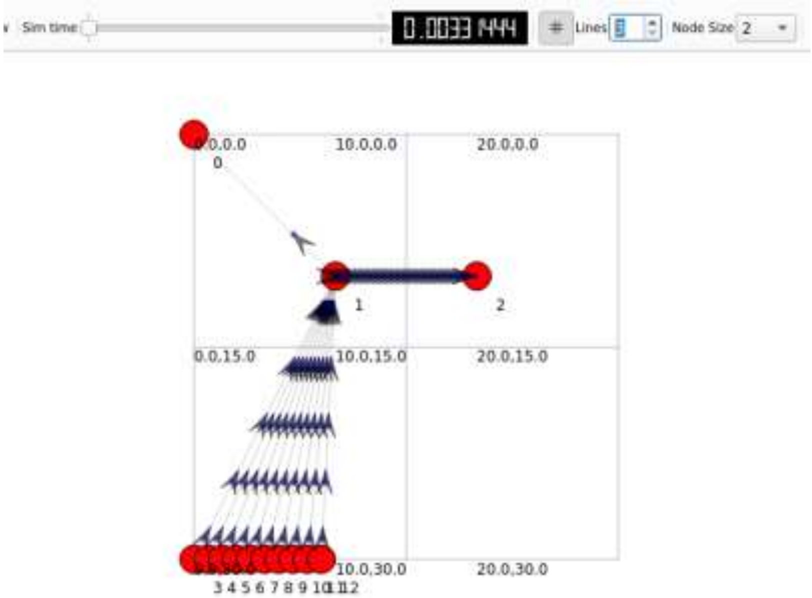
This attack was implemented in Network Simulator (ns2 and ns3). In this network, there are three types of nodes- Client (color blue), Server (color green) and the Attacker (color red). Server 1 is the public server that accepts requests and Server 2 is the server that processes the data received by Server 1. The two clients namely, Client 1 and Client 2 access services provided by the servers. When the attacker starts bombarding packets into Server 1, the server drops packets away.[6]



Non-malicious simulation (ns2)



Malicious packet drop (ns2)



Distributed Denial of Service Attack(ns3)

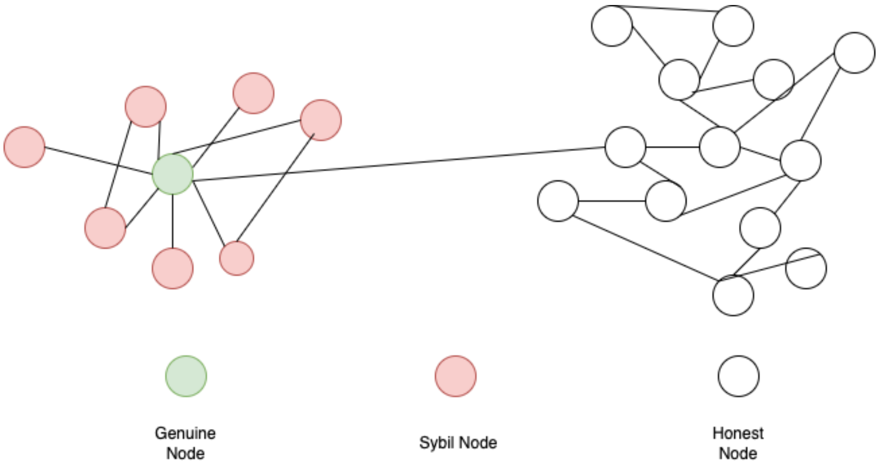
Mitigation:

- A DoS attack can be mitigated using message reception control thus preventing the flow of data that floods the network and allows the administrator to detect and stop the attack. If it is greater than the limit entered, the receiving node will ignore the message.

- Another way to mitigate DoS attacks is by including an authentication system (preferably signatures) to verify a valid user's information and thus prevents transmission of fake data messages.

4.4 Sybil

VANET is vulnerable to several attacks as it is infrastructure-less, one of the most common attack is Sybil attack. A Sybil Attack is a cyber-attack on the availability of the computer network. In such an attack an attacker creates multiple nodes and inserts them into the network. The attacker creates a very large number of fake identities (probably more than the number of honest nodes) such that they block the data transmission between the sender and the receiver nodes and creates a lot of traffic within the network which the server cannot handle.



In a sybil attack, an attacker tries to create false vehicles in order to dominate the whole network and infect false information to harm the legitimate user and degrade the network performance.

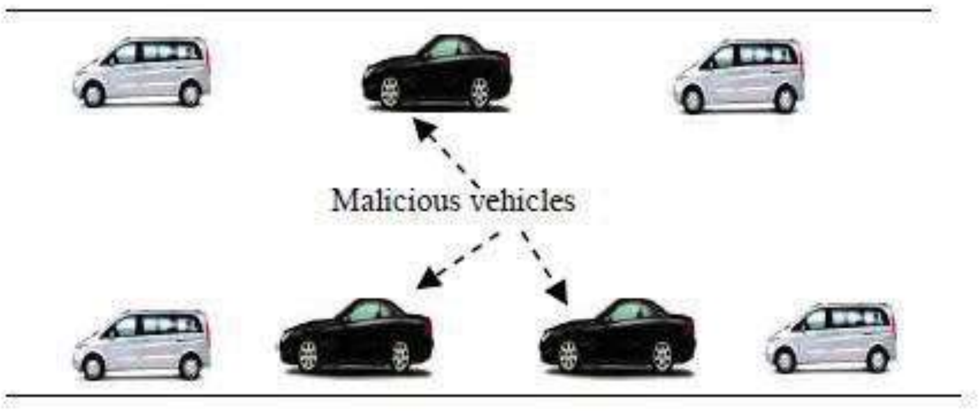


Fig 2. The basic overview of a Sybil attack on VANET network.

From Figure 2, the attacker tries to use the black malicious vehicles to create a dummy of multiple vehicles on the road, and from these other legitimate vehicles on the road realize that there is a heavy traffic. With this attack, an attacker can easily spoof the vehicles' identity and location and then implement any type of attack in the network and due to the fact that vehicles are highly mobile in nature, density of networks changes dynamically, network topology also changes dynamically so vehicles continue to communicate with each other in order to update their routing tables. By imposing Sybil attack, attacker takes over the control of network and may enact other attacks such as black hole attack, timing attack, denial of service attack, impersonation attack and others.[7]

Detection & Prevention of Sybil on VANET:

- Usually, in a network if there is a central authority in the network then it keeps the count of devices it is connected to. But, in the ad-hoc network there is no central authority as all the devices are connected in multi-hop (mesh) topology. Also, the nodes can come and go within the network and so the attacker can insert as many fake nodes he wants into the network.
- One way is to link one vehicle's ID to one position. So, if one ID has more than one positions then it can be identified as a Sybil node. The network can get the position of each vehicle by installing radars across the entire network. A tunable radar can be helpful for covering larger ranges.
- One of the most effective ways is to give roles to the vehicles which themselves can identify the Sybil node. The nodes in the network are given 3 different roles- Claimer, Witness and a Verifier. The claimer periodically sends its claimed position through a beacon signal. The Witness receives this beacon signal from the Claimer node and identifies its position by judging its signal strength and gets an estimated position of that claimer node. Now the Verifier gets both the claimed position and the estimated position form the Claimer and the Witness, respectively. The verifier then compares both the positions and if it finds the difference to be more than a threshold, then it identifies that node as a Sybil node.
- The Sybil nodes can also be detected using the RSUs. They are the actual witness to the vehicle's presence on the road. They can timestamp the signal received by the vehicle. In this way, if there are two different vehicles with the same timestamp then, surely one of them has to be a Sybil node. The RSU can also identify the vehicles using signatures, certificates and hashing using encryption and decryption techniques.[8]

4.5 Routing Replay Attack on VANET

In cryptographic terms, replay attacks are the attacks that capture one message transmission and then again send these captured messages. These attacks pose a threat to the authentication and integrity of the node. In VANET, this attack takes place when the attacker replays the transmission of earlier information to take advantage when a specific situation arises.

Problem caused by Replay Attacks on VANET:

VANET systems use 802.11 wireless transmission standard for V2V (Vehicle to Vehicle) transmission. However, 802.11 is designed in such a way that it has no protection against replay attacks. It does not use sequence numbers or timestamps. The keys can be reused to replay already stored messages with the exact same key to insert fraudulent messages in the system. To elaborate, an attacker could save a received message about a traffic event/accident which happened in the past then resend it in the future. In that case, other vehicles in VANET are deceived by fake alerts. The main motive of replay attacks could be to confuse the law enforcement authorities and prevent identification of vehicles (hit and run).

Detection & Prevention of Replay Attacks on VANET:

- Emphasis should be made to authenticate individual packages and not just encrypting them. This can be done by upgrading to the system where all the nodes can exchange different the messages with different keys. Also, the system can use hashed signatures for the authentication of the node.
- Individual packets must have timestamps. Timestamps will help the nodes to identify the uniqueness of the data and make sure that not a single message is being replayed a particular time.[9]

4.6 GPS Spoofing

GPS is a vehicle localization technique used in VANET. The GPS receiver fitted in the autonomous vehicle uses trilateration technique to calculate the location of the vehicle (It takes 3 satellite signals into consideration). GPS Spoofing is a type of attack in which the attacker copies the identity of any legitimate vehicle in VANET and becomes part of the network. This attack is also known as tunneling attack. Later on, it indulges in passing wrong location information.

Problems caused by GPS Spoofing Attack on VANET:

This attack poses a threat on confidentiality and integrity of the system. A GPS simulator is used to deceive the GPS receiver by sending false pseudo-random numbers. Spoofed GPS simulators uses stronger signals than the signals generated by genuine satellites. Spoofing attacks have high risks as they disrupt services like navigation, tracking and routing. The availability of low-cost spoofing tools has resulted into more incidents of GPS spoofing.

Detection & Prevention of GPS Spoofing Attack on VANET:

- RSU (Road Side Unit) based signal verification:
  As a control message, the encrypted content is transmitted over the RSU area. The control message is also signed digitally with RSU credentials. A private-public key pair is generated in the system, and the private key is distributed to all RSUs, while the public key is distributed to all cars. Any message that does not have a digital signature is rejected as a fraudulent message by the vehicle. Before

processing the control message from the RSU, the vehicle that receives it validates the signature.

- Proactive Defense against GPS Spoofing:
  This method involves learning the spatial and temporal characteristics of the attack. In VANET, one of the RSUs is assigned as the master.
  Each RSU classifies GPS signal and creates a feature vector stating each signal as authentic or spoofed. The feature vectors and their categories will be sent to the master RSU by each RSU. An SVM (Support Vector Machine) classifier is trained at the master RSU, and decision rules for classifying authenticated and spoofed signals are learned from the SVM using the method described in. Once a time period has passed, the learned decision rules are transmitted to each RSU and subsequently forwarded to each vehicle.

4.7 Eavesdropping:

In this attack, attackers monitor sensor readings and transmissions. Eavesdropping threatens location privacy, as each TPMS sensor has a sensor ID that remains fixed for the duration of its lifetime. It is possible to reach an eavesdropping range of up to 40 meters from a passing vehicle as mentioned in [11]. Further eavesdropping attacks on TPMSs are further facilitated because ECUs within TPMSs do not generally have authentication schemes in place to ensure that messages are coming from legitimate nodes.

Countermeasures: TPMSs should incorporate basic error checking, detect when conflicting information has been received, and filter out false activation signals. They also argue that the current packet structure is not conducive to proper encryption, and thus, a sequence number field and a cryptographic checksum should be added to TPMS packets. A Linear-Feedback Shift Register (LFSR)-based encryption method that would shield sensor IDs from attackers. Feedback loops are recruited to create 64-bit encryption keys, thus making it robust against brute force attacks. There are software for ECUs and suggest the use of static code analysis tools to identify and eliminate excess ambiguity in code design.

4.8 Node Impersonification

This Attack involves creating a malicious node which takes part in the data exchange between nodes. In VANET, each vehicle has their own IP address and identity, which is used during communication based on their range and functions. These unique identities become much more important during the time of an accident. The attacker tries to impersonate as a real node by stealing its identity and sending modified version of the message. Impersonation attacks does not really affect the communication, but the data integrity is breached by attacker which reduces the ability and quality of wireless communication.[10]

Problems caused by Node Impersonification on VANET:

- In 802.11 standard, currently, the hardware address of the nodes can easily be spoofed over the air by intercepting the packets.
- Node Cloning: It requires re-programming a node and give it the hardware address of an existing honest node from the network. This poses a threat to the authentication and integrity of the system.
- A false/cloned node in a VANET can confuse all the other nodes by passing on the wrong information into the network.
- This also increases the chances of having a Man in the Middle Attacks.

4.9 Cheating Sensor Information Attack:

The OBU and AU of a vehicle are targeted in these attacks, this causes the sensor information to be tampered with, allowing it to deceive authorities by changing factors like a position of vehicle.

4.10 Network Monitoring Attack:

In this attack, the attacker monitors the entire network and listens in on vehicle communication in order to send sensitive information to the beneficiaries. An attacker, for example, can alter the information of a patient sent by ambulance.

4.11 Man-in-the-Middle (MITM) Attack:

In MITM attacks represents an intermediary adversary node that can intercept and change communications as they go from the RSU to the cars and vice versa. These attacks have the potential to compromise the messages' integrity and confidentiality. To carry out these attacks, the attackers typically take advantage of the non-encrypted nature of messages sent across an insecure wireless communication channel. The primary goal of this adversary node is to intercept the message, change it, and send the bogus or updated message with incorrect information to other vehicles.

5. Results

Attack	Protocol	Property Compromised
Blackhole	AODV	Availability
Wormhole	AODV	Availability
Denial of Service	UDP	Availability
Sybil attack	AODV	Authentication
Routing Replay	AODV	Data Integrity
GPS Spoofing	NMEA	Authentication
Eavesdropping	TPMS (LF/UHF signal)	Confidentiality
Node Impersonification	AODV	Authentication, Availability
Cheating Sensor Information	NA	Integrity
Network Monitoring	NA	Confidentiality
Man In The Middle (MITM)	NMEA	Confidentiality

6. Conclusion

VANET is a significant and promising technology that attempts to improve road safety by allowing vehicles to communicate with one another. However, vehicles communicate via an insecure communication route, due to which various attackers try to interrupt communication or discard packets. VANET is vulnerable to a variety of threats and attacks which are explained in detail in the attack section. Many researchers worked for the provision of authentication to VANET, but not much work is done related to confidentiality and availability. So, there is a requirement to have more work-related VANET security as it has become the main requirement of users.

7. References

[1] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): Status, results, and challenges,” *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, Aug. 2012, doi: 10.1007/s11235-010-9400-5.

[2] F. Ahmad, A. Adnane, and V. N. L. Franqueira, “A Systematic Approach for Cyber Security in Vehicular Networks,” *Journal of Computer and Communications*, vol. 04, no. 16, pp. 38–62, 2016, doi: 10.4236/jcc.2016.416004.

[3] H. Kaur, S. Batish, and A. Kakaria, “An Approach To Detect The Wormhole Attack In Vehicular Adhoc Networks,” *International Journal of Smart Sensor and Adhoc Network.*, pp. 86–89, Oct. 2012, doi: 10.47893/ijssan.2012.1143.

[4] P. Kumar, S. Verma, and R. Singh Batth, “Implementation and Analysis of Detection of Wormhole Attack in VANET,” *Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org*, vol. 8, 2018, [Online]. Available: www.jncet.org

[5] K. Verma, H. Hasbullah, and A. Kumar, “Prevention of DoS attacks in VANET,” *Wireless Personal Communications*, vol. 73, no. 1, pp. 95–126, Nov. 2013, doi: 10.1007/s11277-013-1161-5.

[6] Institute of Electrical and Electronics Engineers., *2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE) : proceedings*. IEEE, 2012.

[7] A. A. Mane, “|| Volume, 06 || Issue,” 2016. [Online]. Available: www.ijceronline.com

[8] “Detecting Sybil Attacks in Vehicular Ad Hoc Networks.”

[9] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi, “Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs),” in *2020 3rd IEEE International Conference on Information Communication and Signal Processing, ICICSP 2020*, Sep. 2020, pp. 394–398. doi: 10.1109/ICICSP50920.2020.9232047.

[10] R. Regan and J. M. L. Manickam, “A Survey on Impersonation Attack in Wireless Networks,” *International Journal of Security and Its Applications*, vol. 11, no. 5, pp. 39–48, May 2017, doi: 10.14257/ijsia.2017.11.5.04.

[11] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, “Security and privacy vulnerabilities of incar wireless networks: A tire pressure monitoring system case study,” in Proc. 19th USENIX Conf. Security, Berkeley, CA, USA, 2010, pp. 21–21.

[12] https://github.com/tspradeepkumar/blackholeAttack_ns2

[13] https://www.youtube.com/watch?v=xHNcbq1g7CQ&t=1656s

[14] https://www.youtube.com/watch?v=FSJaf8VUCLk&t=1639s

[15] https://github.com/naman-gupta99/ns2-simulations