Presentation on

The Security Impact on Vehicular Ad-hoc Network

Course : INSE 6190 - Wireless Network Security

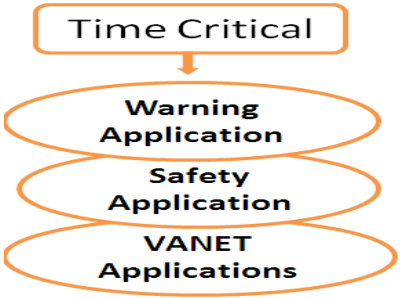
Submitted to Ayda Basyoun, PhD.

Student Name	Student ID
Jeyasuriya Ganesan Kanchana	40202287
Pranay Gulipilli	40185364
Vamsi Mohan Pavuluri	40165590
Ramya Gurumurthy	40218557
Sai Chandra Sekhar Reddy Dwarampudi	40189233
Sudeep Kumar Chamarthi	40184676

VANET Security:

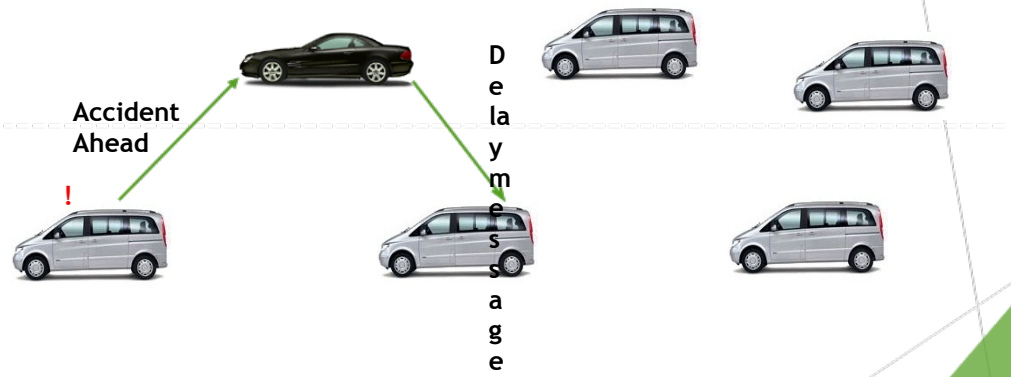
- The Vehicular Ad-hoc Network (VANET) is a promising and emerging technology that is utilized for traffic control, road safety, and entertainment systems.
- A VANET is a type of network in which nodes (vehicles) connect with each other on the road and with the network's infrastructure.
- Security and safeguarding the privacy of the owner has become a big challenge with VANETs.
- In order to provide greater security and retain privacy, one must first understand the various types of network assaults and how they behave.

Timing Attack:

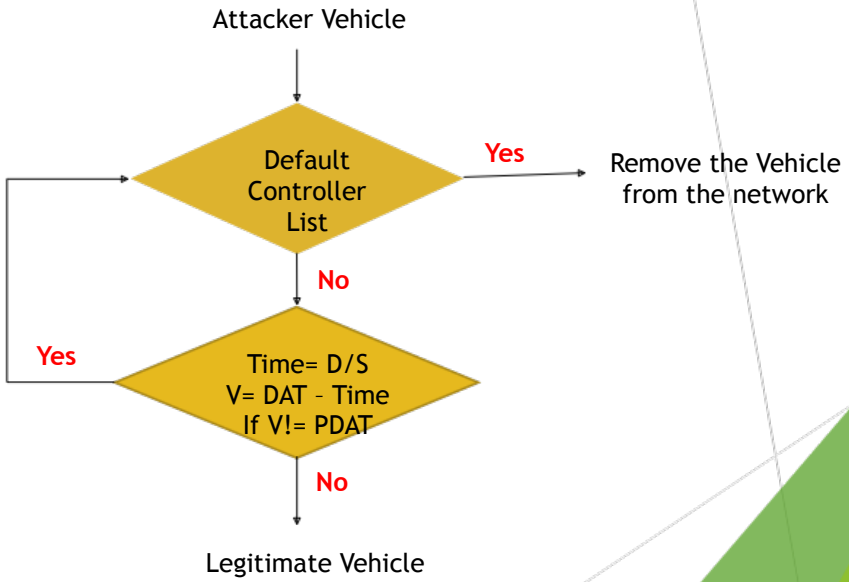


- In safety message, time and contents of the message are both important. Right information must be received the users in right time, this is basic requirement of the safety applications.
- Warning applications provide information about warning messages and these messages are time critical and its importance is also high for safety of human life.
- If an attacker creates delay in it, then it could result in very serious tragedy on the road and many accidents may occur due to this.

Timing attack Scenario:



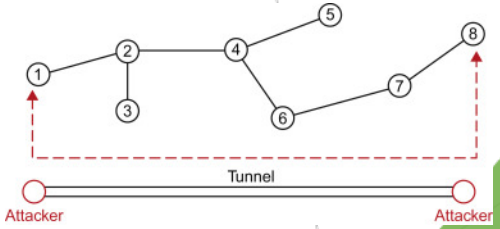
Timing Attack Prevention Protocol:



- Using this TAP Protocol, we can mitigate attackers from the network using Default Controller List and Software Defined Network.
- At First, we must find whether the data is coming from the attacker or not. This can be done by the Default controller list which contains the list of the previous attacker's Vehicle Id.
- If the vehicle is the new attacker, then we must calculate the time period using the Distance/ Speed calculation. And then minus the calculated time period from the Data Arrival Time.
- If the newly calculated time period is not equal to the Previous Data Arrival Time, then the Vehicle Id is found as an Attacker and sent to the Default Controller List. If the result matches the Warning message will be transmitted to the vehicle.
- This is how the TAP Protocol will detect and remove the attacker vehicle from the network.

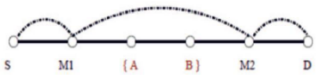
Wormhole Attack :

- Two or more malicious nodes are involved and it forms a tunnel from one end of malicious node to other end and data packets are broadcasted. The tunnel formed between these malicious nodes is called wormhole.
- It is a kind of DOS attack that it will mislead routing operations .The main plot of this attack is to forward the data from one compromised node to other end of the network over a tunnel .
- The routing mechanisms or Protocols can be disturbed when we are sending data packets . It can also changes the normal messages stream . This attack happens In network layer



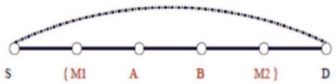
Classification of Wormhole Attack

- **Open Wormhole:** Data packets from the source are sent to wormhole which tunnels them to other wormhole and then pass on to the destination.



- **Half-open Wormhole** : Data packets are sent to a wormhole from the source and it will directly transfer them to destination.

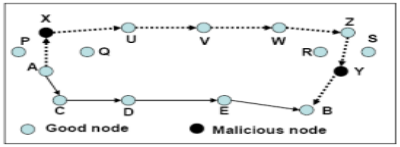
- **Close Wormhole** : Data packets will transfer directly from source to destination in a single hop.

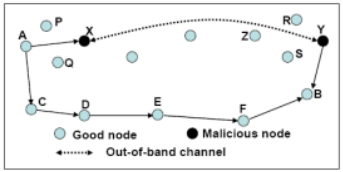


Different Modes

- **Wormhole using packet encaps**

Any routing protocol that uses tl
path to choose the best route is vul
mode of wormhole attack.





- **Wormhole using Out of band channel:**

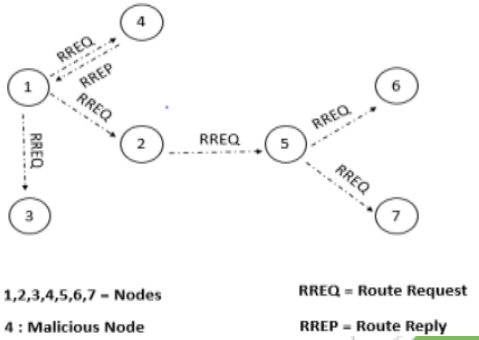
In this mode out of band channel is used to find the shortest path to perform the attack**.**

Black Hole Attack

- VANET is vulnerable to Black Hole attacks considering the transmission idea of the remote medium and an absence of security standards.
- An advanced technique is proposed to identify the malicious node which prevents the malicious node & removes that node completely without the scope of a future attack.
- In a Black hole attack, malicious node actively responds with the route reply though it doesn't have a course route.

Black hole attack Implementation

- The attack is implemented where the malicious node rapidly responds source node even though it doesn't have a course to its source node.
- Malicious node doesn’t check its routing table but this node is the first node to respond with a route reply (RREQ).
- Malicious node on the way of responding drops all the data packets which leads to the attack.



Detection of Black hole attack

- Two stages are involved in the detection of Black Hole Attack

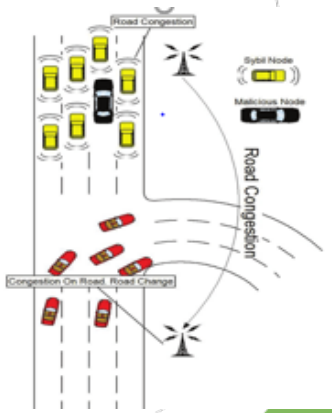
  Stage 1: - Prelim Stage

  Stage 2: - Secure Stage

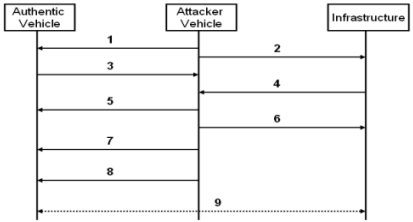
- In the prelim stage initially source node broadcasts the route request packets & accepts the RREP until the timer expires.
- RREPs are stored in a table called path response table in ascending order, this table is shared with RSU where RSU checks if there's any direct route available if it finds a direct path RSU allows the source node for communication otherwise it forwards it to the secure stage.
- In the secure stage RSU replaces the destination IP with unused IP and broadcast route response replies where if the response from the same node appears from the prelim stage RSU request the source node to broadcast for the entire network otherwise RSU allows the communication.

Sybil Attack

- The attacker creates multiple identities of the node and send false data to the other nodes in the network
- Implemented by the attacker to have clear roads in which he will travel.
- Attacker creates an illusion of high traffic in a path.
- The legitimate users to choose a different path.
- Path in which illusion of instances is created will be empty and the attacker can travel freely.
- Performed by an active attacker.
- The Identity the attacker uses is pre-fabricated identity.



Sybil Attack Process



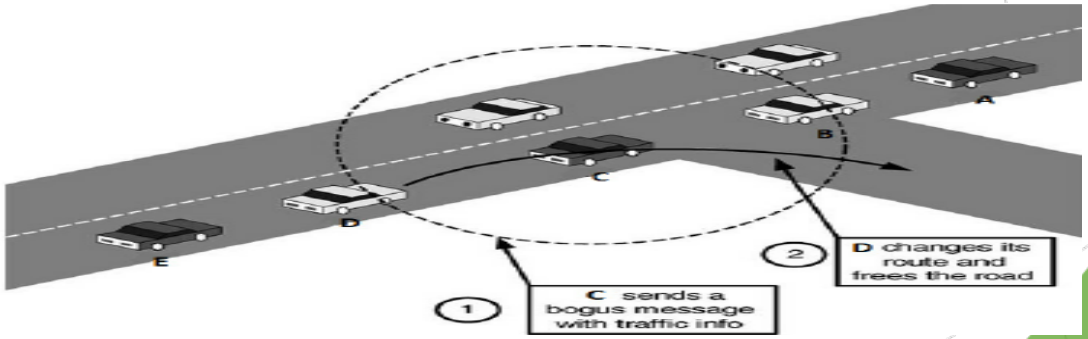
1. The attacker launches the Sybil attack to other genuine vehicle.
2. same attack is sent to the main infrastructure of the VANET.
3. The attacker vehicle receives the Safety messages from the other vehicles.
4. Infrastructure sends safety message to the attacker.
5. The attacker changes the content of the message and send it to the other vehicles.
6. Attacker vehicle sends wrong message to the infrastructure

Defense Mechanisms against Sybil attack

- **Recourse Testing** : Computational puzzles are used to test the computational resources of the node.
- **Usage of Public Key Cryptography** : Vehicle is provided with a public key to get authenticated and CPKI mechanisms are used
- **Pre-defined propagation model** : Node itself collects the data from the other nodes and any deviation is identified as an attacker.
- **Secure Positioning** : Signal and location of the transmitting peer node are verified by collaborating the trusted peers.
- **Distinguishability** : Multiple data are correlated and given a score, based on the score the higher score entities are accepted

Bogus Attack

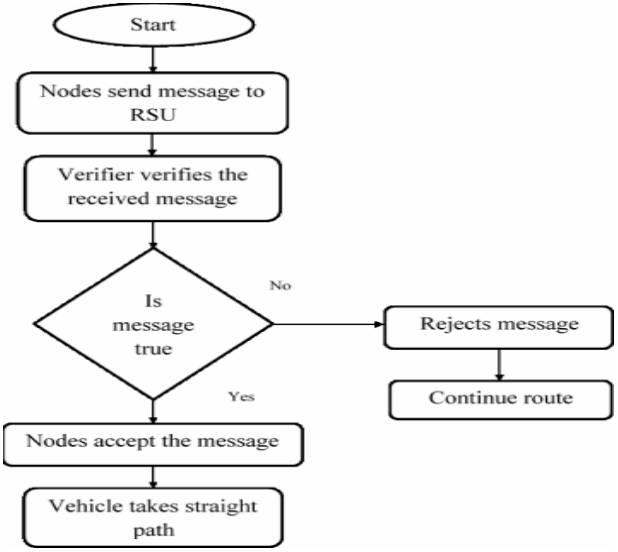
- Transmit fake information to other nodes in the network for personal gain or cause road accidents.
- Attacker can be an Insider or an Outsider.



Ways to Detect Attack

1. **Sender's Behaviour**: Compare the sender's behaviour pattern with the legitimate nodes to identify whether the information is false or not.
2. **Verification of the Position**: Greedy routing approaches and geographic routing approaches are the most common types of position-based routing for VANETs.
3. **Sensors**: Acceptance Range Threshold (ART) sensor, Proactive Exchange of Neighbour Tables and Reactive Position Requests sensor are deployed to identify the attack.

Detection and Prevention of Bogus Attack



GPS Spoofing attack

- The modification of location of an entity or an individual that could potentially cause fatal accidents. This attack can be performed in two methods:
  a. Signal Interference
  b. Fake Location Reporting
- This GPS tracking has been used in number of various applications such as shipment tracking, automated vehicles
- Based on strength of the spoofed signal, the GPS spoofing attack can be classified into three categories:
  a. Simplistic attack
  b. Intermediate attack
  c. Sophisticated attack

Behavioral Based detection

- This technique uses the gyroscope and accelerometer for tracking the individuals
- Consider a scenario of a person going a walking then the person will have to take different directions.
- Now, the movements, speed and angle of the device changes for each turn taken by the individual.

Prediction Based detection

- This is Recurrent Neural Network model involves Long Short-Term Memory(LSTM) model.
- It uses Comma2k19 dataset which contains the Global Navigation Satellite Systems(GNSS), Control Area Network(CAN), Inertia Measurement Unit(IMU).
- An error threshold is calculated from the predicted distance travelled with the GNSS positioning error and LSTM error.

Conclusion

- The Vehicular Ad-hoc Network (VANET) communications has to be securely transferred to avoid any unintended consequences
- Different kind of attack scenarios impact the VANET architecture in a fatal way.
- GPS spoofing attacks could implement countermeasures for the detected attack as future works.
- The threat to the VANET ecosystems increases as the new technologies come in existence
- As VANET is a heterogeneous architecture, every application involved must be audited for vulnerabilities in regular intervals.

Work Load Distribution

Team Members	Work Distribution
Pranay Gulipilli	Present different techniques involved in Black Hole Attacks and discuss the detection of black hole attacks.
Vamsi Mohan Pavuluri	Present the GPS spoofing attack and its impact on VANET security and conclude the impact of various attacks discussed.
Sudeep Kumar Chamarthi	Present various aspects involved in wormhole attack and its implementation.
Sai Chandra Sekhar Reddy Dwarampudi	Present the Sybil attack and its flow while creating sophisticated challenges for VANET.
Ramya Gurumurthy	Present the timing attack and the packet delay caused due to the attack.
Jeyasuriya Ganesan Kanchana	Present the bogus attack and discuss the flooding of the node with traffic.

References

- A. A. C. a. N. E. Elizabeth, "Verification Based Authentication Scheme for Bogus Attacks in VANETs for Secure Communication," 2018 International Conference on Communication and Signal Processing (ICCSP), pp. 0388-0392, 2018.
- R. A. R. A. Arsalan, "Prevention of Timing Attack in Software Defined Named Data Network with VANETs," 2018 International Conference on Frontiers of Information Technology (FIT), pp. 247-252, 2018.
- P. S. G. a. R. Shanmughasundaram, "Detection and Isolation of Black Hole in VANET," International Conference on Intelligent Computing,Instrumentation and Control Technologies , pp. 1534-1539, 2017
- P. A. N. U. a. D. J. Shah, " Attacks on Vanet Security," International Journal of Computer Engineering & Technology (IJCET)., vol. 9, no. 1, pp. 8-19, 2018.
- I. A. A. I. H. H. &. b. A. M. J.-l. Sumra, "Classes of attacks in VANET," Saudi International Electronics, Communications and Photonics Conference (SIECPC), pp. 1-5, 2011.
- G. G. a. B. Ducourthial, "On the Sybil attack detection in VANET," IEEE International Conference on Mobile Adhoc and Sensor Systems, pp. 1-6, 2007.
- F. M. V. R. P. E. V. C. E. R. S. A. a. S. U. D. Kreutz, "Software-Defined Networking: A Comprehensive Survey," Proceedings of the IEEE, vol. 103, pp. 14-76, 2015.
- O. A. A. Elahe Fazeldehkordi, "Wormhole Attack," Wormhole Attack, 2016.
- N. C. Priya Maidamwar, "A SURVEY ON SECURITY ISSUES TO DETECT," International Journal on AdHoc Networking Systems, vol. 2, no. ResearchGate, pp. 30-40, 2012.

References

- S. B. A. K. Harbir Kaur, "An Appr An Approach To Detect The W o Detect The Wormhole A ormhole Attack In V ttack In Vehicular Adhoc ehicular Adhoc," International Journal of Smart Sensor and Adhoc Network, vol. 2, no. 2, pp. 20-30, 2012.
- V. H. LA, "Security Attacks and Solutions in Vehicular Ad Hoc Networks," International Journal on AdHoc Networking Systems, vol. 4, pp. 1-20, 2014.
- J. Y. W. Z. J. &. Liu and C. Yang, "Detecting false messages in vehicular ad hoc networks based on a traffic flow model," International Journal of Distributed Sensor Networks, 2020.
- [Online]. Available: https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea .
- S. K. W. a. S. M. Yiu, "Location spoofing attack detection with pre-installed sensors in mobile devices," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol. 16, no. 4, pp. 16-30, December 2020.
- M. R. M. I. a. M. C. Sagar Dasgupta, "Prediction-based GNSS spoofing attack detection for autonomous vehicles," Transportation Research Board 100th Annual Meeting, 2021.
- S. T. Sunilkumar S. Manvi, "A survey on authentication schemes in VANETs for secured communication," vol. 9, pp. 19-30, 2017.

Thank You