

Insider Attack Mitigation Technique using Hybrid Security Framework on VANETs

Dhaval Patel¹ Dr. Vandana Rohokale² Mr. Gardas Naresh Kumar³

¹GTU PG School, GTU, Gandhinagar ^{2,3}CDAC ACTS, Pune

Abstract— Vehicular Ad Hoc Networks are create by apply the standards of mobile ad hoc networks (MANETs) the unconstrained creation of a wireless network for transmit and exchange data to the wireless node(vehicles). it is a main key component of intelligent transportation systems (ITS).Nowadays, Automation on vehicle and Transportation technology is broadly used by every people. But they have more concern about security. So that implementing security Is necessary in VANETs for This project work proposes detection technique for insider attack and mitigation using some hybrid security framework and ID-based and signature based authentication in between Roadside unit (RSUs) and vehicular node. So that it will reduce insider attack by applying this specific method or scheme based approach can be designed to mitigate attack. Also, it can provide attack classication which categorizes security threats to VANETs.Additionally, this work discusses countermeasures on attacks facing and mitigation techniques.

Key words: Application Unit; Intelligent transportation systems; Roadside unit; Vehicular Ad Hoc Networks; Vehicular Authentication security scheme

I. INTRODUCTION

Vehicular Ad Hoc Networks are create by apply the standards of mobile ad hoc networks (MANETs) the unconstrained creation of a wireless network for transmit and exchange data to the wireless node (vehicles). It is a main key component of intelligent transportation systems (ITS).

The Intrinsic people need for change on progress and mobility, comfort, security and safety are main things to the development of intelligent transportation systems. VANETs are the most dominant empowering innovation for ITS. They are constituted on node by vehicles with wireless communication. The taking part nodes in such networks (i.e. vehicle) associate and cooperate with each other by short-range direct communication, by trusting messages through vehicle (Vehicle-to-Vehicle) and road side unit (Vehicle-to-Infrastructure).

Generally, data about traffic on a road is just increased through inductive multiple time, camera, roadside sensors node or surveys of that. VANETs give settings to gathering real time data from on board sensors on vehicles and its expeditious broadcasting. The data collected through individual vehicles taking part in the ad- hoc network can be incorporated together to form a real time image of the road analysis. Numerous applications have been enabled by VANETs, however security and transportation operational efficient applications are the mainly essential driver for it.

Finally, in the part of Figure.1 we can see simple architecture of VANETs for communicating domain vehicles and the roadside unit. The vehicle node ITS services managed by the main ITS Server.

First Initial wireless ad hoc network where communicate vehicle to vehicle without any help of infrastructure.

Second is communicating between the road side units, a settled infrastructure, and vehicles. Each wireless node in VANET is furnished with two types of component i.e. On Board Unit and Application Unit (AU). OBU has the communication though AU executes the program making OBUs communication ability. An RSU can be appended to the main base system which is associated with the Internet. Since IPv6 security is applied between the nodes and the mobility and security server, represented by the unique Id. [6]

As per the figure 1 show that the Architecture of VANETs. Here all nodes are connected via ad hoc network.

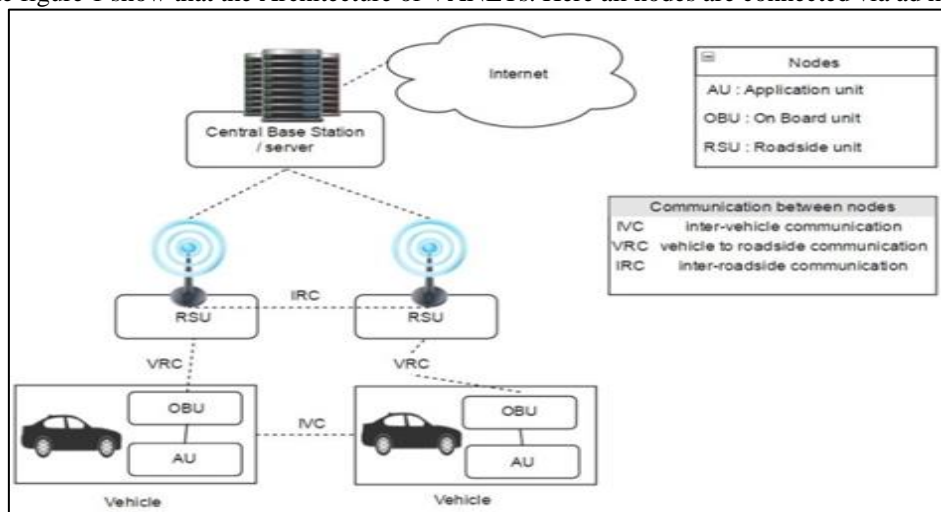


Fig. 1: Architecture of VANETs

II. CLASSIFICATION OF COMMON ATTACKS AND THEIR POSSIBLE SOLUTION OF VANETs

Attack type	Examples	Vulnerabilities
Passive attack	Brute force	Loss of node's identity
	Traffic analysis	Study of nodes activities by an attacker
Active attack	Sybil	Multiple instance of attacker
	Denial of Service	Channel jamming
	Sinkhole	Control of traffic by an attacker
Insider	Position attack	Position of nodes altered or cannot be known, bogus attack
	Misbehaving attack	dropping packets and injection of faulty data by faulty nodes
	Illusion attack	Creation of false traffic situation by malicious nodes.

Fig. 2: Common Attacks on VANETs

A. Main two type of Insider Attacks:

1) Misbehaving Attack:

This attack should be possible by intentional attackers or by faulty hardware, in which a node in VANET denies exchanging messages that it receives, wrongly information, make wasteful bandwidth utilization or inject bogus message or fake message. Figure 3 show that the how misbehaving vehicle broadcast wrong information.[5]

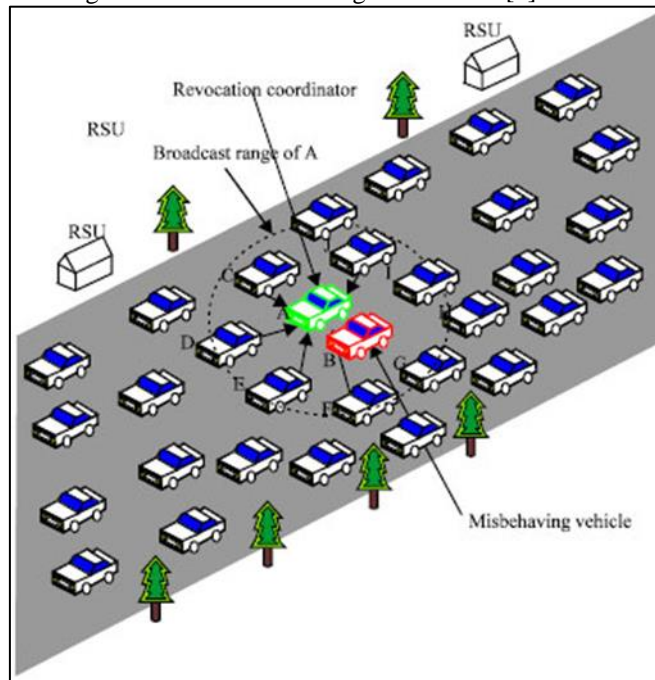


Fig. 3: Misbehaving Attack on VANETs

2) Illusion Attack:

This Attack is a nowadays security threat to VANETs. In this attack, the attacker Dissemination traffic warning messages in view of the road condition which yields an illusion to vehicles close by, bringing about a traffic jam, accidents and degraded overall VANET performance. Unfortunately, existing authentication protocols won't conflict with this attack since the attacker specifically controls and deceives the sensors (of its own car) to produce and Dissemination the wrong traffic information.[5]

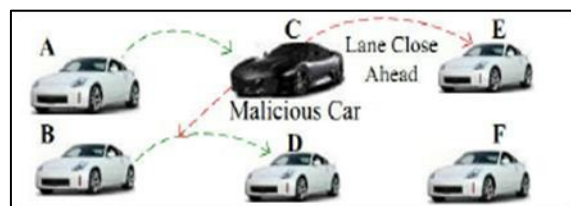


Fig. 4: Illusion Attack on VANETs

As per the figure 4 show that the attacker can generate the decoy on VANETs and after that it will send some wrong information through RSUs unit.to neighbour Vehicle.

III. SECURITY REQUIREMENTS IN VANETS

Security is an essential issues for ad hoc networks, particularly for security application. To build the security of an ad-hoc network, we have to consider criteria to measure security.[8]

A. Availability:

It deals with network services for all nodes involves of bandwidth and connectivity. Method utilizing group signature scheme has been acquainted with experiences the availability issues, prevention and detection. This plan concentrates on availability of transmitting the messages between vehicles and road side units. The proposed strategy still survives notwithstanding when the attack causes network unavailability because of interconnection utilizing public and private keys between RSUs and vehicles.

B. Confidentiality:

It ensures that unidentified substances can't have the access to the classified data information in the network .Confidential data information for example name, plate number and area can also be inhibited from unauthorized access. Pseudonyms, is the most well-known procedure, which is utilized to preserved privacy in vehicular networks. Numerous key sets with encryption will be given to every vehicle. Different pseudos' are utilized to encode messages and just important authority has access to it none of the vehicle node has been connected to it. When any pseudo expires, vehicles need to acquire new pseudo from RSUs.

C. Authentication:

It check the initials between vehicles and RSUs. Authentication is require because furthermore for the validate integrity of the data transmitted. It additionally guarantee that every one of the nodes are the authenticated vehicles to communicate within network. To establish connection between vehicles, RSUs and AS, public or private keys with certificate authority are proposed. Then again, as an authentication method, password is utilized to access to the RSUs and AS.

D. Integrity:

Data integrity is extremely crucial because it assures that the data got by nodes, RSUs and AS is like to the data and it has been created during the exchanges of the message. Digital signature which is incorporated with password access is utilized to secure the Integrity of the message.

E. Non-Repudiation:

To guarantee the sender and receiver so that later on it cannot deny sending and receiving the message for example some accident messages. Non-repudiation is also called audit ability in certain areas.

IV. PROPOSED SYSTEM

The architecture of the VANETs when modification can diminish the conceivable attacks on vehicular ad hoc networks so that as per the proposed solution Detection technique for insider attack and mitigate with using some hybrid security framework and ID-based and signature based authentication in between Roadside unit (RSUs) and vehicular node. So that it will reduce insider attack by applying this specific method or scheme based approach can be designed to mitigate attack.

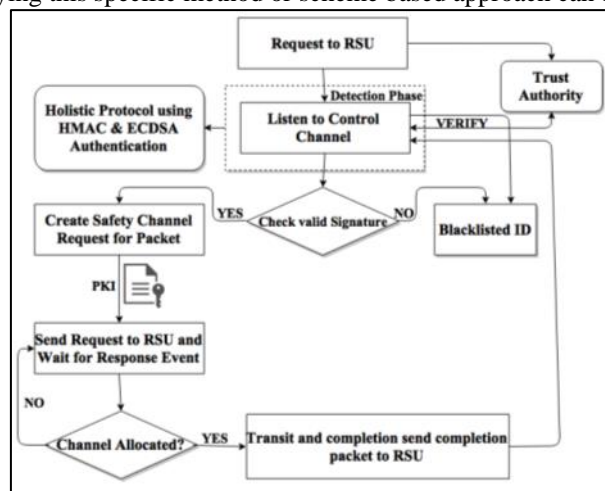


Fig. 5: Proposed model

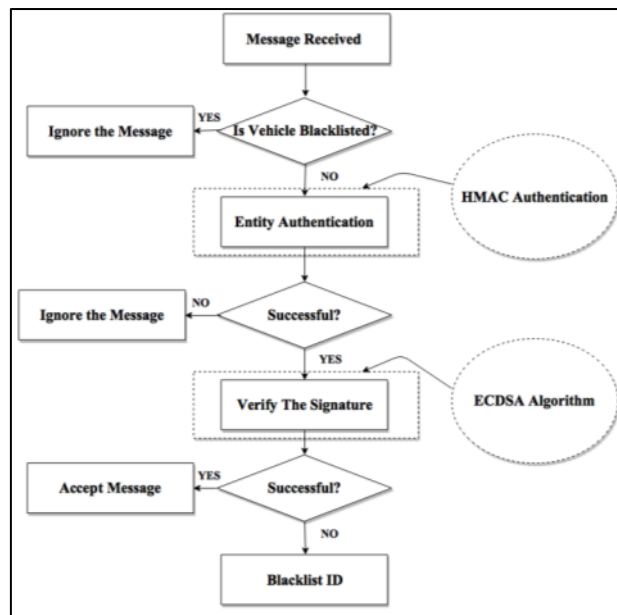


Fig. 6 : Detection phase

V. IMPLEMENTATION SCENARIO

Here is the secure communication scenario between RSU and vehicles.

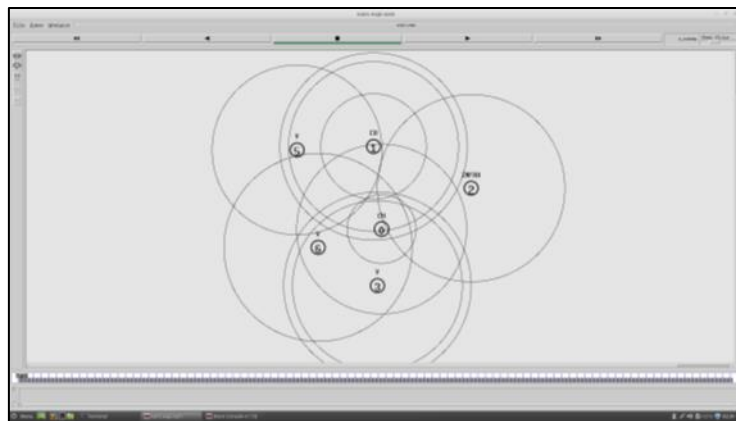


Fig. 7: Secure Communication

Here is the malicious node detection process.

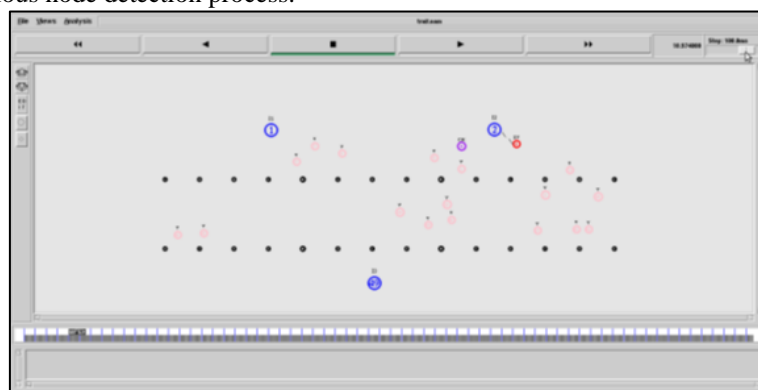


Fig. 8: detected malicious node by RSU

Here is the Alert generated by RSU and it will pass alert message to the valid nodes using secure channel.

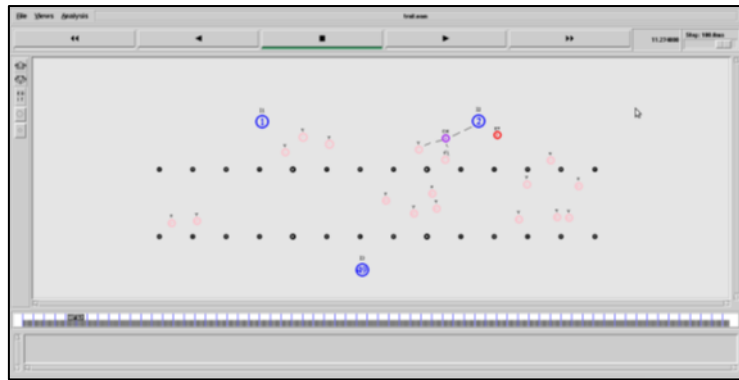


Fig. 9: Alert Message pass by RSU to Valid vehicles using secure channel

VI. CONCLUSION

Nowadays, Automation on vehicles and Transportation technology is broadly used by every people. But they have more concern about security on availability, privacy, confidentiality, authentication and non-repudiation. So that implementing security requests in VANETs and this literature survey will overview VANETs clarifying their security requirements and challenges. Also, it can provide attack classification which categorized security threats to VANETs. Additionally, we have discussed countermeasures on attacks facing and mitigation techniques.

REFERENCES

- [1] S. Dietzel, R. van der Heijden, J. Petit and F. Kargl, "Context-adaptive detection of insider attacks in VANET information dissemination schemes," Vehicular Networking Conference (VNC), 2015 IEEE, Kyoto, 2015, pp. 287-294.
- [2] T. Karimireddy and A. G. A. Bakshi, "A hybrid security framework for the vehicular communications in VANET," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 1929-1934.
- [3] Yongchan Kim, Jongkun Lee, "A secure analysis of vehicular authentication security scheme of RSUs in VANET," 2016 Springer Journal of Computer Virology and Hacking Techniques, August 2016, pp.145-150
- [4] Hongyu Jin and P. Papadimitratos, "Scaling VANET security through cooperative message verification," Vehicular Networking Conference (VNC), 2015 IEEE, Kyoto, 2015, pp. 275-278.
- [5] L. Bariah, D. Shehada, E. Salahat and C. Y. Yeun, "Recent Advances in VANET Security: A Survey," Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd, Boston, MA, 2015, pp. 1-7.
- [6] R. V. Alexandrescu, M. C. Surugiu and I. Petrescu, "Study on the implementation of protocols for providing security in average VANET intervehicular network communication systems," Electronics, Computers and Artificial Intelligence (ECAI), 2015 7th International Conference on, Bucharest, 2015, pp. WW-1-WW-6.
- [7] D. Tiwari, M. Bhushan, A. Yadav and S. Jain, "A Novel Secure Authentication Scheme for VANETs," 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, 2016, pp. 287-297.
- [8] E. A. M. Anita and J. Jenefa, "A survey on authentication schemes of VANETs", 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-7.