Security and Reliabilty Issues In Vehicular Ad Hoc Networks (Sr-Vanets)

Deeksha Hegde B[1] Chandrika C N[2]
[1,2]Asst. Prof , Dept Of CSE,
Sai Vidya Institute of Technology, Bangalore, India

Ramya K[3] Meghashri E M[4]
[3,4]Asst. Prof , Dept Of CSE,
Sai Vidya Institute Of Technology, Bangalore, India

***Abstract:-*Vehicular communication of prospect will have the possible to restrict some of the key troubles of road travel, namely, traffic congestions, collisions, emissions and fuel consumption. Vehicular ad-hoc networks (VANETs) as implemented, will build the biggest accomplishment of ad-hoc networks. It is observed that protection of VANETs is of vital importance, since the malicious attacks can jeopardize human being lives. Significant research is focused on improving the protection of such networks due to secure protocols developed for VANETs. This paper is to discuss the presented security protocols, focuses on the way to develop the cleverness of the decision system to improve reliability and security issues, with the aid of the physics of historical data and vehicle dynamics, which can be collected from different sensors like In-Vehicle Systems (IVS), Global Positioning System(GPS), and On-Road Assistance systems (ORA).**

KEYWORDS: Vanets, security, reliability, road side unit.

I.INTRODUCTION

A **vehicular ad hoc network** (**VANET**) uses the cars as the mobile nodes in a MANET to build a mobile network. A VANET makes every active car into a wireless node or router, allows the cars around 75 to 300 metres of one another to connect and, consecutively, construct a network with a broad range. When cars drop out of the network and fall out of the signal range, other cars will join in, connecting vehicles to each other therefore that a mobile Internet is produced. Vehicular Ad-Hoc Networks (VANETs) permit wireless information communication between vehicles and, wherever it is possible, between roadside equipment and vehicles. VANETs become an principal research field because of their use in road security and other viable applications. Necessity for research comes from the truth that comprehension of such network in the genuine world is a difficult task. Vehicles are constantly moving and making network topology very dynamic. Buildings, traffic signalization and other obstacles are disrupting wireless communication. On other side, vehicle movements are constrained by roads and traffic regulations, making mobility patterns that can be predicted to some extent. A lot of research has to be done to design VANET protocols that will overcome mentioned problems and take into account predictability to optimize communication and provide required functionality. In a VANET, vehicles will rely on the integrity of received data for deciding when to present alerts to drivers. Further in the future, this data may be used as the basis of control decisions for autonomous vehicles. If this information is corrupted, vehicles may present unnecessary or erroneous warnings to their drivers, and the results of control decisions based on this information could be even more disastrous. Information can be corrupted by two different mechanisms: malice and malfunction. Similarly, vehicles have two defense mechanisms: an internal filter and external reputation information. for example, obtain a less congested route for itself by overstating the number of vehicles on its desired roadway. As a Second example, a corrupted node could trigger erroneous driver warnings to be displayed in other vehicles by falsifying its position information. IEEE 1609.2, the trial-use standard concerning security services for vehicular environments, stipulates that vehicles will be authenticated using certificates issued by a Certificate Authority (CA) in a Public Key Infrastructure (PKI) setup [3]. Illegitimate vehicles should have these certificates revoked, and the identity of the revoked certificates (although ideally not the identity of the associated driver) should be published and distributed to legitimate vehicles. Whatever mechanism that is used for distributing this revocation information should distribute the info information securely, quickly, and broadly in order to limit the amount of damage illegitimate vehicles can do. Fig 1.1 shows the architecture of the Vehicular Ad-hoc Networks.

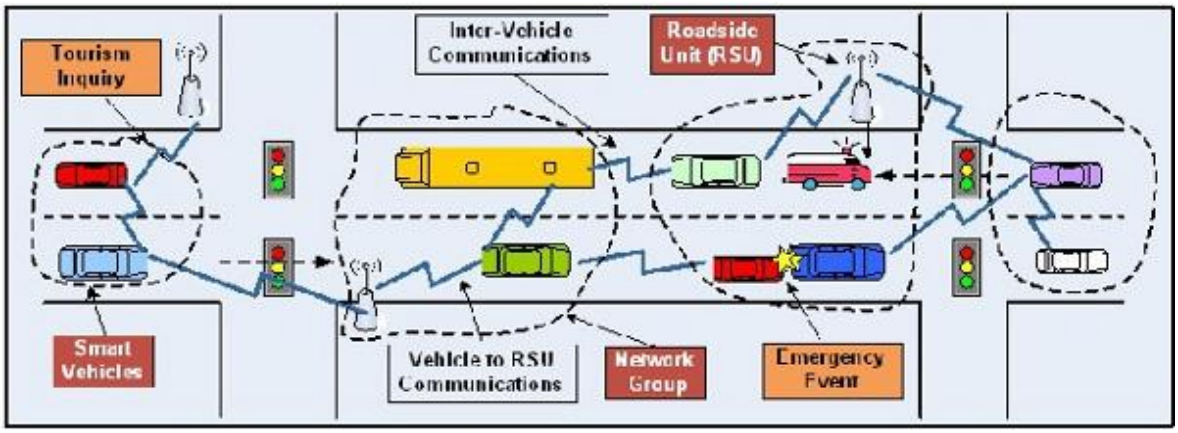

Fig 1.1 Vanet Architecture

II. VANET SECURITY ASPECTS

VANET experience from a variety of attacks. These attacks are explained in the following subsections:

A. *ATTACKS*

In this paper we are focused on attacks perpetrate against the message itself rather than the vehicle, as physical security is not in the scope of this paper.

1) Denial of Service attack

This attack occurs when the assailant makes control of a vehicle's jams or resources the communication route used by the Vehicular Network, thus it reduces the critical information from arriving. This attack in addition increases the threat to the driver, if it has to based on the application's information.

For example, if the nasty wants to create a substantial stack up on the highway, it can be able to create an disaster and utilize the Denial of Service attack to avoid the caution from reaching to the imminent vehicles [1], [5], [6], and [7].

Authors in [1] discussed a solution for DoS problem and saying that the existing solutions such as hopping do not completely solve the problem, the use of multiple radio transceivers, operating in disjoint frequency bands, can be a feasible approach but even this solution will require adding new and more equipments to the vehicles, and this will need more funds and more space in the vehicle. The authors in [12], planned a resolution by switching between even communication technologies (e.g., UTRA-TDD, DSRC, or Bluetooth for extremely short ranges) or replaying previous transmission, if they are obtainable, when one of them (classically DSRC) is bring down.

2) Message Suppression Attack

An attacker select the sinking packets from the network, these packets can stick dangerous information for the receiver, the attacker hide these packets and able to use them again in other times [5].

The aim of such an attacker can be to avoid registration and indemnity authorities from erudition about collisions involving his or her vehicle and/or to keep away from delivering the collision reports to the roadside approach points [17].

For example, an attacker could hide a congestion caution, and use it in a different time, thus vehicles will not receive the caution and mandatory to stay in the traffic.

3) *Fabrication Attack,*

An attacker can create this attack by sending fake information into the network, the information can be fake or the transmitter might declare that it is someone else.

This attack also includes warnings, fabricate messages, identities, certificates [5], [7] [17].

4) Alteration Attack,

This attack occurs when attacker signals an obtainable data, it consists of delaying the broadcast of the information, changing the genuine entry of the data sent or replaying prior transmission [5].

For example, an attacker able to modify a message informing the other vehicles that the present road is clear while the road is crammed [17].

5) Replay Attack,

This attack occurs when an attacker repeat the transmission of an former information to obtain advantage of the

circumstances of the message at the time of transmission[5]. Basic 802.11 security does not have any protection against replay. It does not contain timestamps or sequence numbers. Since the keys can be reused, it is likely to replay stored messages with the same key without detection to insert bogus messages into the system. Individual packets must be authenticated, not just encrypted. Packets must have timestamps.

The goal of such an attack would be to confuse the authorities and possibly prevent identification of vehicles in hit-and-run incidents [17].

5) *Sybil Attack,*

This attack happens when an attacker creates large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that there is jam ahead, and force them to take alternate route[5],[8].

Sybil attack based on how economically identities can be developed, the extent to which the system evaluate inputs from entities that does not contain a sequence of confidence connecting them to a confident entity, and whether the system treats all entities identically.

For instance an attacker can pretend and act like a hundred vehicle to convince the other vehicles in the road that there is congestion, go to another rout, so the road will be clear.

B.ATTACKERS

Selfish Driver

The general proposal for faith in Vehicular Network is that every vehicle should be trusted primarily, these vehicles are trusted to track the protocols mentioned by the application, few drivers attempt to maximize their gain from the network, despite the cost for the system by captivating advantage of the network resources dishonestly. The Selfish Driver be able tell new vehicles that there is blocking in the road, so they should choose a different route, thus the road will remain clear for it.

Malicious Attacker

This type of attacker attempts to trigger damage through the applications offered on the vehicular network. In several cases, malicious attackers will have certain targets, and attackers will contain access to the resources of the network.

For example, a terrorist can publish a deceleration caution, to build the road congested before explode a bomb.

]

III.SECURITY REQUIREMENTS

Authentication

In Vehicular Communication each message should be genuine, to make persuaded for its source and to control permission level of the vehicles, to accomplish this vehicles will allocate each message with their private key with its certificate at the recipient side, the recipient will receive the message and verify for the key and certificate once this is done, the recipient checks the message.

Availability

Vehicular network should be obtainable all the time, for various applications these networks will need real-time, these applications require quicker response from Ad Hoc Network or even sensor networks, a wait in seconds for few applications will create the message meaningless and perhaps the result will be destructive.

Attempt to convene real-time demands makes the system susceptible to the Denial of Service attack. In several messages, a wait in millisecond makes the message worthless. The problem is greatly larger, where the application layer is unpredictable, as the possible way to recuperate with unreliable communication is to store fractional messages in desire to be finished in next transmission.

Non-repudiation

Non-repudiation will assist the ability to recognize the attackers still after the attack occurs. This prevents traitors from controlling their crimes. Some information associated to the car like: the speed, trip rout, time, any infringement will be stored in the TPD, any bureaucrat side holding endorsement can recover this data.

Privacy

Holding the information of the drivers away from unconstitutional observers, This information like trip path, real identity, speed etc. The privacy can be succeeded by using anonymous keys, these keys will be altered regularly as every key can be used immediately for one time and expires after usage every the keys are stored in the TPD, and will be reloaded over again in next time that the vehicle makes an administrator checkup.

Integrity

Integrity for all messages should be protected to prevent attackers from altering them, and message contents to be trusted.

Confidentiality

The confidentiality of every driver must be protected; the messages should be enciphered to stop outsiders from obtaining the drivers information.

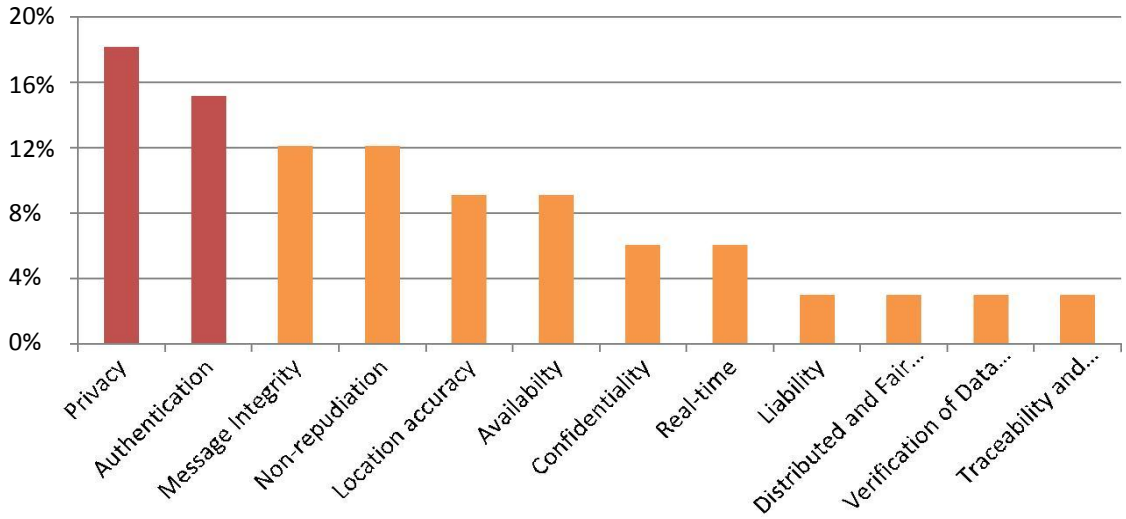

Figure 3.1. The important of security requirements in VANET

In Figure 3.1, privacy is the most important factor among other parameters. As a result, the main requirements of security are namely the authentication, non-repudiation and message integrity by 15%, 12% and 12% respectively

IV. CONCLUSION

The Need and importance of security for safety transportation, we focusing on security in SR-VANETS. We found some of the treats and challenges related to VANET security. Also, we obtain the requirements that are required for creating and designing a security model. These security issues make a potential stumbling block to deploy VANET .Vehicular Ad Hoc Networks is promising technology, which gives abundant chances for attackers, who will try to challenge the network with their malicious attacks. Therefore, it is necessary to develop a suitable framework which mitigates all these security problems; more research is required in this area. Moreover, the impact of trust on security in SR-VANETS is other objectives in future work.

REFERENCES

[1] Biswas, S., & Misic, J. (2013). "A Cross-layer Approach to Privacy-preserving Authentication in WAVE-enabled VANETs." Vehicular Technology, IEEE Transactions on 62(5): 2182 – 2192.

[2] Burmester, M., et al. (2008). "Strengthening privacy protection in VANETs. " Networking and Communications, 2008. WIMOB'08. IEEE International Conference on Wireless and Mobile Computing, IEEE.

[3] Chaudhuri, A., et al. (2012). "Identity Based Secure Algorithm for VANET." Procedia Engineering 38: 165-171.

[4] Chim, T. W., et al. (2011). "MLAS: multiple level authentication scheme for VANETs. " Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ACM.

[5] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.

[6] Dötzer, F. (2006). "Privacy issues in vehicular ad hoc networks. " Privacy enhancing technologies, Springer.

[7] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October 2006 .

[8] Grover, J., et al. (2013). "Trust Establishment Techniques in VANET." Wireless Networks and Security, Springer: 273-301.

[9] Isaac, J. T., et al. (2008). "A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks.", Computer Communications 31(10): 2478-2484.

[10]Kitchenham, B. (2004). "Procedures for performing systematic reviews.",Keele, UK, Keele University 33: 2004.

[11] Lee, S.-B., et al. (2007). "Secure incentives for commercial ad dissemination in vehicular networks." Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing, ACM.

[12] M Raya, J Pierre Hubaux, "The Security of Vehicular Ad Hoc Networks ", Proc. of the 3rd ACM workshop on Security of ad hoc and sensor networks, 2005.

[13]Leinmuller, T., et al. (2007). "Security requirements and solution concepts in vehicular ad hoc networks." Wireless on Demand Network Systems and Services, 2007. WONS'07. Fourth Annual Conference on, IEEE.

[14] Li, C.-T., et al. (2008). "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks." Computer Communications 31(12): 2803-2814.

[15] Lu, R., et al. (2008). "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications." INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, IEEE.

[16] Plößl, K. and H. Federrath (2008). "A privacy aware and efficient security infrastructure for vehicular ad hoc networks.", Computer Standards & Interfaces 30(6): 390-397.

[17] Prado, A., Ruj, S., & Nayak, A. (2013, June). "Enhanced privacy and reliability for secure geocasting in VANET." In Communications (ICC), 2013 IEEE International Conference on (pp. 1599-1603). IEEE.

[18] Pradweap, R. V., & Hansdah, R. C. (2013). A Novel RSU-Aided Hybrid Architecture for Anonymous Authentication (RAHAA) in VANET. In Information Systems Security (pp. 314-328). Springer Berlin Heidelberg.

[19] Raya, M., et al. (2006). "Securing vehicular communications.", Wireless Communications, IEEE 13(5): 8-15.

[20] Razzaque, M., et al. (2013). "Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead." Wireless Networks and Security, Springer: 107-132.