**Contemporary Engineering Sciences, Vol. 8, 2015, no. 5, 235 - 240**
**HIKARI Ltd, www.m-hikari.com**
**http://dx.doi.org/10.12988/ces.2015.5121**

# A Survey on Security Challenges and Malicious Vehicle Detection in Vehicular Ad Hoc Networks

**Neha Roy**

Department of Information Technology
Sathyabama University, Chennai, India

**Y. Bevish Jinila**

Department of Information Technology
Sathyabama University, Chennai, India



**Abstract**

In Vehicular Ad hoc Networks (VANETs), vehicles periodically broadcast messages for every 100 to 300 milli seconds. Such messages are used to report a safety or non-safety application. Authentication on such safety messages assures the end users in the network. However, a malicious vehicle can trace the messages and can launch varied types of malicious activity which leads to the compromise of personal privacy. Unfortunately, in VANETs many privacy preserving schemes are susceptible to Sybil attacks. This paper presents the security challenges faced by the network and analyzes the malicious Sybil activity. Schemes from existing literature are analyzed and a framework is proposed to overcome this malicious activity.

**Keywords**: Authentication, Security challenges, Sybil attack, VANET

## 1 Introduction

In a VANET vehicles communicate with each other in a multi hop manner. These communications can be monitored by fixed Road Side Units (RSU's). Each RSU has a fixed communication range. The vehicles within the communication range are monitored by the corresponding RSU's and these vehicles can also communicate with their respective RSU [1]. In turn, RSU can also communicate

with their nearby RSU. There is a Certificate Authority (CA) who is responsible for the registration and renewal of the vehicles in the network. Each vehicle new to the network should register itself to this trusted authority.

Even though this network offers safety and comfort to the public, there may be a situation where these safety measures can be compromised by malicious users. Security and privacy are the two most important concerns in a VANET which prevents the users in spreading malicious information across the network. In order to improve the safety message communication, all the messages communicated should be guaranteed even in the presence of persistent attacks.

The present day research in VANETs is mostly focused towards security. The challenges faced on security issues a lot. Out of the several challenges face by the network, Sybil attack weighs a lot. A malicious user capable of creating multiple fake identities is known as Sybil attack. For safety applications like traffic congestion warning a malicious user can host a Sybil node to create multiple fake identities thereby making the node to behave like multiple nodes. This paves way for a greater havoc in the network.

The rest of the paper is organized as follows. Section 2 discusses the system model. Section 3 discusses about the security challenges faced by authentication. Section 4 details about the various malicious vehicle detection schemes and section 5 concludes the work.

## 2 System Model

In vehicular ad hoc networks, each vehicle can communicate with other vehicle and they can also communicate with the fixed infrastructure, RSU. The figure 1 shows the system model and following are the major components in this model.

- On Board Unit (OBU)

Each vehicle is equipped with an On Board Unit which consists of a transceiver, GPS for positioning. A vehicle equipped with an OBU can communicate with other vehicles and the RSU's. A vehicle can be malicious if it is compromised to be an attacker.

- Road Side Unit (RSU)

These units are fixed infrastructures that can be deployed in any intersections or on the side of roads, street lights. All the vehicles within the communication range of the RSU can communicate with it. All the RSU's can communicate with each other and they are connected together to form a strong backbone network.

- Certificate Authority (CA)

This authority is responsible for the registration and renewal of the vehicles in this network. It is connected to the backbone RSU network. Once registered or renewed, vehicles don't keep direct interaction with this authority.

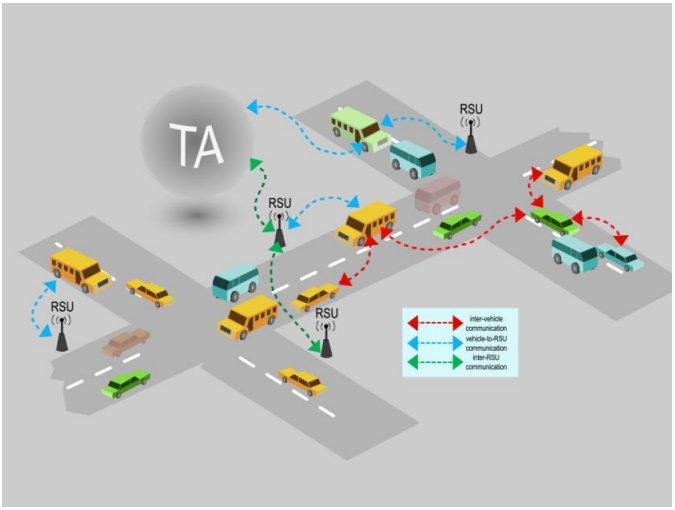


Fig.1. System Model

## 3 Security Challenges

Though there are several schemes available in the literature to secure VANETS, this network still suffers from varied security challenges. The malicious activity that occurs during authentication should be addressed to avoid greater havoc in the network. Such attacks reveal the ID of the vehicle thereby leads to leakage of privacy. The different attacks that affect authentication include Sybil attack, impersonation attack, spoofing, replay etc.

### III.1 Sybil Attack

An attacker tries to represent itself with multiple fake identities to accomplish a particular task. These multiple identities are generated from the pseudonyms set of their own OBU or they impersonate other vehicles identities to make it malicious. Such attacks lead to the privacy leakage thereby degrading the performance of the network.

## 4 Malicious Vehicle Detection

If the id of the vehicle is disclosed, there is a higher probability that the privacy of the user cannot be preserved. Certain authors have proposed the use of pseudonyms [2] – [4]. These are alternate identifiers generated by the certificate authority during vehicle registration or renewal. These can be used to hide a vehicles unique identity. So, when a vehicle needs to report an event, it randomly picks one pseudonym and signs it using public key cryptography. This makes a third party difficult to track the vehicle simply by observing the pseudonym it uses. Since the privacy preserved is user centric, it is susceptible to Sybil attacks

[5]. This is because a malicious user can misuse these pseudonyms and can generate multiple messages from a single entity and show as if is generated from different entities. To solve this problem [5] suggested that the vehicles can be preloaded with temporary pseudonyms, each having an expiry time. Vehicles are expected to obtain new set of pseudonyms from their nearby RSU's once when their pseudonyms are about to expire. This is also not successful because we cannot expect the vehicles to be near a particular RSU when its pseudonyms are about to expire.

A rather different approach was suggested by [6]. In this paper the author has suggested the use of directional antennas to identify the position or direction from which a message arrives. A vehicle that launches a Sybil attack is expected to be caught because all the messages are sending from the same position. However, if the network is dense, the localization errors lead to false positives. Another different approach suggested by [8] describes their scheme that when the vehicle speed is less than 30Km/hr it stops broadcasting messages and during this silent period pseudonyms are changed. By this method, we infer that several vehicles change their pseudonyms at the same time and same location. But, the use of silent periods is not advisable at all times where a certain time of silent period can cause a serious damage resulting in collision of vehicles.

The author [7] has proposed a technique called P2DAP for privacy preserving. In this paper a two stage hashing is used during the time of registration. A Pool of pseudonyms is generated, from which a coarse grained group of pseudonyms are selected to be used during a period of one year and hashed to a common value. From this coarse grained group, fine grained groups of pseudonyms are assigned to each vehicle. Even though this method can overcome Sybil attacks, it requires more computation in certificate authority, and if any mishap is found and if cannot be rectified by RSU it is directed to CA where CA becomes the sole responsibility to handle the issues. When there are more issues generated in a dense environment, it creates more delay for processing. Also, an attacker who has knowledge about the current scenario and traffic can compromise the RSU and can trace the vehicles.

Reza et.al. [9] has listed the drawbacks of [7] including the compromise of RSU and obtain its keys for Sybil attack detection and use them in low traffic road to correlate messages from vehicles. Another problem listed is the required time for communication between RSU and CA. As per the results the average time for communication is 45 seconds. But, if there are more attackers, the delay may move up to 100 seconds. To rectify this problem, [9] has suggested a Homomorphism Based Signature and Certificate Generation (HBSCG) scheme. In this scheme, the RSU's are semi trusted, where they know the real pseudonyms but not the exact relationship of a vehicles public and private keys. In [10], a cooperative detection method is proposed.

## 5 Conclusion

In this paper, various security challenges and malicious vehicle detection schemes are discussed. From the analysis it is evident that to face the security challenges new detection schemes are required.

**Acknowledgements.** We thank Sathyabama University for extending support for completion of this work.

## References

[1] Car-2-Car Communication Consortium. [Online]. Available: http://www.car-2-car.org/

[2] Dotzer, "Privacy issues in vehicular adhoc networks", Privacy Enhancing Technologies, 2006.

[3] M. Raya and J. P. Hubaux," The security of vehicular ad hoc networks", in SASN, Nov 2005. http://dx.doi.org/10.1145/1102219.1102223

[4] J.Y. Choi, M. Jakobsson and S. Wetzel, "Balancing auditability and privacy in vehicular networks", in Q2SWinet, 2005. http://dx.doi.org/10.1145/1089761.1089775

[5] B. Parno and A. Perrig, "Challenges in securing vehicular networks", HotNets – IV, 2005.

[6] P. Golle, D. Greene, and J. Staddon," Detecting and correcting malicious data in Vanets", in VANET Oct 2004. http://dx.doi.org/10.1145/1023875.1023881

[7] Tong Zhou, Romit Roy, Peng Ning, Krishnendu, " Sybil Attack Detection in Vehicular Ad Hoc Networks", IEEE Journal on selected areas in communications, vol. 29, no. 3, March 2011. http://dx.doi.org/10.1109/jsac.2011.110308

[8] Levente Buttyan, Tamas Holczer, Andre, William Whyte, "SLOW: A practical pseudonym changing scheme for location privacy in VANETS", Proc. of the IEEE Vehicular Networking Conference, Japan, Oct 28-29, 2009. http://dx.doi.org/10.1109/vnc.2009.5416380

[9] Reza, Maryam, "Distributed Sybil Attack Detection in VANET", International Journal of Computer Applications, Vol. 29, No. 12, Sept 2011. http://dx.doi.org/10.5120/3704-5192

[10] Bo Yu, Cheng Zhong Xu, Bin Xiao, "Detecting Sybil Attacks in VANETs", Journal of Parallel and Distributed Computing, Vol. 73, Issue 6, June 2013, pp. 746-756. http://dx.doi.org/10.1016/j.jpdc.2013.02.001

**Received: February 11, 2015; Published: March 5, 2015**