iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** II **Month of publication:** February 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

A Survey-Cryptography based Location Privacy in Vehicular Ad Hoc Networks

Allam Balaram[1], Gajula Rajender[2], M. Vijaya Laxmi[3]
[1, 2, 3]*Departmanet of Computer Science and Engineering, AAR Mahaveer Engineering College*

Abstract: ***Wireless Ad-hoc networks are more susceptible for large number of attacks due to its open medium and anomaly nature. Security is still a major issue in the vehicular Ad-hoc network. There are many security issues and one such issue is location privacy. Location privacy of a node (user) should be made as a mandatory property for wireless communication. Once the attacker has the knowledge of location of node, it can easily trace its activities. Location privacy is much necessary for vehicular Ad-hoc networks (VANETs) than mobile Ad-hoc networks (MANETs). A vehicular user gain access from vehicular network through wayside access box (WAB). During a long journey, a vehicular user is supposed to cross several WABs that belong to other network communities. Our proposal tries to prevent the unauthorized traceability of nodes to achieve the location privacy of vehicular user. Some of the smart attackers trace the nodes without accessing the packet content which cannot be easily detected. A node that has location privacy should carry transaction of message to another node which has location privacy. The nodes are given incentives for forwarding the packets. This work presents a proper mobility modeling for better understanding of privacy concept.***

Keywords: VANETs, Cryptography, Location Privacy System, Certificate Authority, Authentication

I. INTRODUCTION

Security in Vehicular Ad hoc Networks (VANETs) is an area of mounting theoretical and practical interest. In addition to the standard security requirements, VANET requires a special security requirement, that of location privacy. A brief discussion on history of VANET is suggested in [1] [2]. Location privacy can be informally defined as a user's belief that only authorized users should able to determine his/her current location. The major parts of communication in vehicular ad hoc networks are vehicles, Wayside Access Boxes (WAB), location servers and Certification Authorities (CAs). The vehicles and WAB can transmit data using the Dedicated Short Range Communications (DSRC). VANET offers two communication patterns, namely, Vehicle-to-Vehicle (V2V) interaction and Vehicle-to-infrastructure (V2I) interaction. In V2V interaction, there is no need for fixed infrastructure and is purely ad hoc in nature. On the other hand, in V2I interactions, a vehicle interacts with a fixed infrastructure like WAB. This infrastructure provides aggregation, key distribution to the vehicles. The major issue of this architecture is that the number of required WAB cannot be predicted. A location privacy of a vehicular user is a vital security requirement as the data sent by a vehicle may have important consequences like accident prevention. The nodes in the VANET move in and out of the network frequently as it has a greater dynamic mobility pattern. The dynamic nature of VANET makes it more vulnerable to attacks and has several security issues. The various forms of adversaries who attack the VANET system model are greedy drivers, insider attackers, pranksters, malicious attackers and snoops. By using advanced techniques in localization and tracking one can find the exact location of a vehicle. By doing so, it is possible to gain information about the past history of the vehicle it has visited. This information can be further used in an illegal manner by a stranger. Moreover, private information about a user can be gathered by identifying the Location Based Services (LBS) used by a vehicle. Generally, location privacy, ensuring schemes falls under the policy based [3] and anonymity based [4] [5] categories. Though there are many issues in VANET, this work is mainly concerned only with the location privacy and traceability of a VANET node.

A. Significance of Location Privacy

In VANET, it is easy to gather information about the speed, location, and trajectory of vehicles. By using these information, the malicious attackers can easily determines the user's living habits, social relationship and personality of driver. It is essential to verify a driver in the vehicle should be authenticated for communication. A selfish VANET node cannot transmit the safety messages to others and it creates accidents, forgery attacks in the network. A malicious attacker traces the user information from the WAB easily and it makes hazardous in the network. The location privacy preservation gives more attention in VANETs. It prevents the vehicles from accidents, and malicious attackers or intruders.

B. Potential Applications

Location privacy in the VANET provides a platform for different applications such as safety, driver assistance system, transportation regulation, and map location.

1) *Safety:* In safety ensuring applications, each vehicle is supposed to broadcast an authenticated safety message periodically enclosed with its verifiable identity, current location, acceleration, and speed. Though these safety messages to assist in preventing the accidents, they are vulnerable to unauthorized adversaries who can track and access the location of the vehicle. The location privacy prevention can reduce several types of attacks like spoofing, malicious attacks and crime.
2) *Transport regulation:* The WAB in VANET controls the traffic flow by distributing the traffic information to the vehicles within its communication range. The WAB can reduce the accident between vehicles using warning information. The civil engineers use the WAB information such as traffic flow, road topology and traffic observation, for constructing a new road.
3) *Map location:* In VANET, vehicle receives the location information using GPS receiver and it is used to trace the robbery vehicles. The sensors built on a vehicle is able to detect the car thefts, and find the threats and informs the remote end users via the internet.

II. LITERATURE SURVEY

A. Privacy Ensuring Techniques in VANET

SLOW (Silence at LOW speeds) ensures location privacy in VANETs in which the vehicles do not transmit heartbeat messages if their speed falls below a given threshold (silent period) [6]. The vehicles should change pseudonym during the silent period. This assures that vehicle waiting at traffic lights or moving slowly in traffic jam stop transmitting heartbeats and immediate change their pseudonyms at the same time and location. SLOW ensures silent periods and harmonized pseudonym changes with respect to time and location. SLOW does not depend on the cooperation between vehicles and any kind of infrastructure.

AMOEBA is an anonymity based location privacy ensuring scheme that makes use of group navigation of vehicles [7]. The idea of grouping the vehicles considerably mitigates the location tracking of any victim and also ensures robust anonymous access to prevent the profiling of LBS applications accessed by any target vehicle. Consequently, it randomly selects a silent period at the time of grouping for ensuring location privacy at appropriate places. Finally, it suggests a solution to balance the trade-off between safety and location privacy by exploiting the power control capability of vehicles. A density based location privacy (DLP) scheme provides location privacy that fixes a threshold to change the pseudonyms based on the density of the neighboring vehicle [8]. DLP scheme also derives the delay distribution and the expected delay of a vehicle within a given area. A cryptographic mechanism is used to strengthen the privacy in VANET and it provides trade off between the user's privacy and accountability of an adversary model [9]. Pairwise communication and group communication among vehicles along with the vehicle to infrastructure communication is considered. This cryptographic based approach is hybrid as it uses symmetric and public keys for data transfer authentication and encryption. Pseudonyms are varied only when it is needed and thus reduces overhead. The work in [10] suggests Efficient Privacy Preservation (EPP) protocol for VANET that uses the smart card system to authenticate users. It also exploits bilinear pairing scheme to issue the public and private key. The public key is related with the user's signature while the private key is related to the signature of the trust authority and WAB. This scheme enables users to verify signatures regardless of their corresponding certificates. Random Encryption Periods (REP) is a location privacy ensuring group communication protocol for VANET with a conditional stateless property [11]. A MobiCrowd scheme is introduced in [12]. In MobiCrowd scheme, the users have some location privacy information from the server and it passes the information to the location seeking neighbors without including the server. By hiding in the crowd, the user generates a hiding local query for determining their locations. The query receiving users, which already have some location information, replies to the query generators in terms of query reply. The users in MobiCrowd can preserve the location privacy of vehicles from unauthorized persons. Thus, the MobiCrowd scheme reduces the leakage of location privacy information. In [13], a novel Sybil attack detection scheme, Footprint is introduced to minimize the anonymity for preserving location privacy. The vehicle location is determined using the trajectory of vehicles. When a vehicle enters into the range of RSU, it receives an authorized message from the RSU for a proof of appearance time in the RSU. The collection of sequential authorized messages is used to generate the location hidden trajectory. A location hidden trajectory is generated from the vehicle for preserving location privacy. A privacy-preserving framework in [14] introduces an Anonymous Verification and Inference of Positions (A-VIP) for verifying the vehicle position based on location authority.

In [15], a Pseudonym Changing at Social spots (PCS) mechanism developed to anonymity set for achieving location privacy in VANETs. It proposed a Key-insulated Pseudonym Self-Delegation (KPSD) scheme to palliate the hazards due to vehicle theft. A scheme uses identity-based group signatures (IBGS) to split a large scale VANET into small groups for preserving location privacy [16].

B. Privacy and Security in VANET

The basic requirements regarding security and privacy between various communication devices in VANET are discussed in [17]. To meet these requirements, a secure and privacy defending protocol has been designed based on the Group Signature and Identity based Signature (GSIS) mechanism. GSIS approach does not offer only the security and privacy requirements, but also offers traceability of every vehicle's ID as it can be verified by certain authorities at dispute moment. Security issues are handled in two different aspects such as interaction between on- board units (OBUs) and interaction between OBU and road side unit (RSU). Group signature concept and ID based signature (cryptography) concept is used in the first and the second aspect respectively. The security issues in VANET have been discussed in a detailed manner in [18]. It also discusses about the current wireless standardization process for WAVE- wireless access in vehicular environment applications. It states that the two major issues in VANET are certificate revocation and conditional privacy preservation. It provides an effective measure for achieving the certificate revocation and conditional privacy preservation. The certificate revocation can be achieved by using either of these methods such as revocation using compressed certificate revocation lists, revocation of tamper proof device or distributed revocation protocol. The conditional privacy preservation can be achieved by using PKI. The basic security requirements in VANET have been addressed briefly in [19]. It provides a survey about the security issues and existing defense mechanisms to overcome these issues. It addresses all possible attacks and adversary models in VANET. It proposes some specific methods to achieve authentication, non-repudiation and privacy. The security and privacy have been assured in [20] using geographical secure path routing protocol. It mainly focuses on providing location authentication and location privacy of VANET. It also provides suggestions to reduce the location authentication overhead. In [21], a distributed Vehicular Public Key Infrastructure (VPKI) is proposed for providing security and location privacy preservation. It employs cryptographic tokens for determining hazardous vehicles.

C. Preserve Location Privacy in VANETs

To preserve the location privacy of vehicles, the work in [22] proposes an anonymous beacon generation mechanism. To provide high authentication messages by detecting the Sybil attack and compromised RSU, the work in [23] proposes an efficient authentication scheme and a secret maintenance mechanism. To detect Sybil attacker attack and a compromised RSU, the work in [24] supports a temporarily authorized certificate that includes the trusted certificate and secret key trajectories to the vehicles for communication.

III. GAP ANALYSIS

There are many location privacy schemes proposed for vehicular networks. These schemes identify various attackers affiliated with sharing the location information. The location of unauthorized VANET node not only detracts its own location privacy, while it also detracts the privacy of others. Location privacy is the major problem for providing security in a vehicular networking environment. The previous location privacy mechanisms provide security at average cost, while it fails to consider security in a large scale high mobility environment. By generating safety messages, several existing privacy preservation mechanisms provide security to the users. However, if a WAB is compromised, it can facilitate to the adversary produce fake legal trajectories. It is essential to develop cost-efficient techniques to determine the compromised WAB quickly. A framework adds dummy queries to the real query to confuse the adversary. The dummy query is need look like a real query, however an effective algorithm for designing dummy query is an open problem. A Mobi Crowd technique improves the location privacy of a user by hiding the real query from the server. However, it may often fail when the users have high mobility and the network size is very large.

IV. PROBLEM STATEMENT

The main problem associated with the VANET is the location privacy of users from the adversary. Privacy failures in VANET would be more serious. In case of privacy failures, the users may become the victim of adversaries who can collect and analyze users' communications. Many of the previous works focus on the location privacy of users. By adding dummy queries to the users real query can preserve the location privacy. However, it is not easy to generate dummy queries, as it is necessary to design look like a real query. When a node assigns long trip with greater mobility, obviously it has to cross several WAB's and it receives more authorities from different WAB's. The authorized user serves the location information to its neighboring nodes based on local query generation. The difficulty arises from the event of a user crossing from home, network domain and enters into another domain with roaming protocols. Consequently, both the home network domain and the other visited network domain during the trip may gain a lot of personal information about the node. For instance, the home network domain gains knowledge about the current location of the node and the other visited network domain may gain knowledge about the home domain network and unique identity.

Maintenance of location privacy is a serious issue when a node traverse within its home domain network and the problem becomes even more serious when it moves to other network domain. Moreover, it is essential to introduce new techniques for preserving the location privacy of a VANET node.

V. AIM AND OBJECTIVES

A. To preserve the location privacy of a user if it moves from one network to other network with higher mobility.
B. To strengthen the location privacy of the drivers in the presence of strong adversary that can observe globally and access all communications in VANET.
C. To provide guarantee the privacy of the current location of the user against the unauthorized users or observers.
D. To prevent any of the unauthorized users from predicting and accessing the future actions of the user.

VI. PROPOSED METHODOLOGY

A VANET node should preserve its private information, including the driver name, license plate, speed, location, and traveling routes. Effective location privacy mechanism aims at preserving the authorized user information in a critical manner. The Location Privacy System (LPS) provides security in a particular way to maintain the user's information secretly and improve the network throughput. The users queried to the LPS to provide the real-time security information associated with the current location and circumstances of the device. The LPS verifies each vehicle in an anonymous manner. The responsibility for location privacy system includes searching and discovering the real identity each vehicle, maintaining the location secrecy, and monitoring the vehicles are crossing the particular WAB.

Location privacy in VANET can only be protected for genuine users. The previous location privacy approach is classified into mix zone based, k-anonymity based, pseudonym based, and cryptographic based. The previous location privacy mechanisms only focused on location privacy. It is very difficult to achieve both location privacy and efficiency in VANET. The proposed methodology proposes both privacy and efficiency conflicting issues. In addition to, the proposed methodology focused on heuristic view of security in VANETs. The proposed methodology employs cryptographic and adversary revocation mechanisms for providing location privacy. The location privacy system in vehicular network is as shown in figure 1.The WABs are placed along the roadside and subordinated to the Certification Authority (CA). The CA can able to trace the real identity of a vehicle. Each WAB stores the real time information of all vehicles within the communication range.

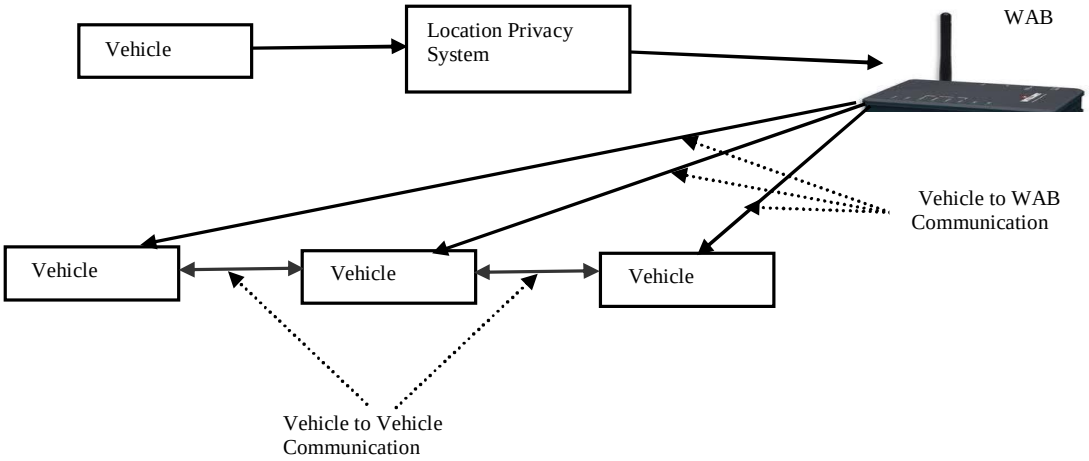


Figure.1 Location Privacy in Vehicular Ad Hoc Networks

The WABs are placed along the roadside and subordinated to the Certification Authority (CA). The CA can able to trace the real identity of a vehicle. Each WAB stores the real time information of all vehicles within the communication range. Each VANET node equipped with On Board Units (OBU) for making communications with WAB. A VANET node communicates to the WAB through LPS. The LPS preserves the private information about each vehicle. A vehicle whose real identity is already registered with the CA. The WAB distributes the safety message to the VANET node. The WAB verifies the real identity of a vehicle when the

vehicle enters its communication range. The WAB provides navigation services to the users and also provides the location privacy using cryptographic mechanism. If the WAB gets any invoked message from CA, the corresponding misbehaving vehicle is traced by the traffic police immediately. This leads to avoid the spoofing and eavesdropper in the network. Finally, the location privacy prevention improves the performance of overall VANET. The location privacy preservation is provided to the users at minimum cost and it should operate effectively in large scale network.

VII. EXPERIMENTAL REQUIREMENTS

Tool: Network simulator (NS-2)

Technology: There are two types of simulators required for simulating VANET such as traffic simulator and network simulator.

A. Traffic Simulator

A traffic simulator for generating traffic mobility files. The following MOVE (MObility generation for Vehicular Environment), VanetMobiSim, and TraNs (Traffic and Network Simulation Environment) simulators are satisfied the traffic mobility files. The MOVE is built on SUMO (Simulation of Urban MObility) with GUI (graphical user interface) and it has a good visualization tool which focuses on traffic level features. It provides all the configurable option of NS-2 TCL files. Unlike MOVE, TraNs, the VanetMobiSim are designed optimally for generating traffic mobility files.

B. Network Simulator

The main network simulator is NS-2 event driven, open source, and portable simulation tool. Several NS-2 simulator versions are evaluated in recent years. For an example NS-2.35 and NS-3. The input argument of NS-2 is TCL script. NS-2 employs two key languages. They are C++ and OTCL (Object oriented Tool Command Language). The NS-2 gives output files in the form of NAM or Trace files. Cygwin is used to run the NS-2 on windows based system.

C. Advantages of NS-2

The main advantages of NS-2 is as follows

1) It does not require any costly equipment
2) Complex scenarios can be easily tested
3) Results are updated rapidly
4) Modularity

VIII. PERFORMANCE METRICS

A. Vehicle density

The density of vehicles is defined as the number of vehicles within the communication range at a particular time period.

B. System Throughput

Throughput is defined as the number of vehicles delivered successfully to the destination per second.

C. Tracking Time Cost

It is defined as the total time taken to determine the adversary from the group of vehicles.

D. Location Privacy Gain (LPG)

It is defined as the number of vehicle's location can be preserved from the adversary.

E. Success Rate of Tracing

It is defined as the probability of successful tracking of a target vehicle by an adversary.

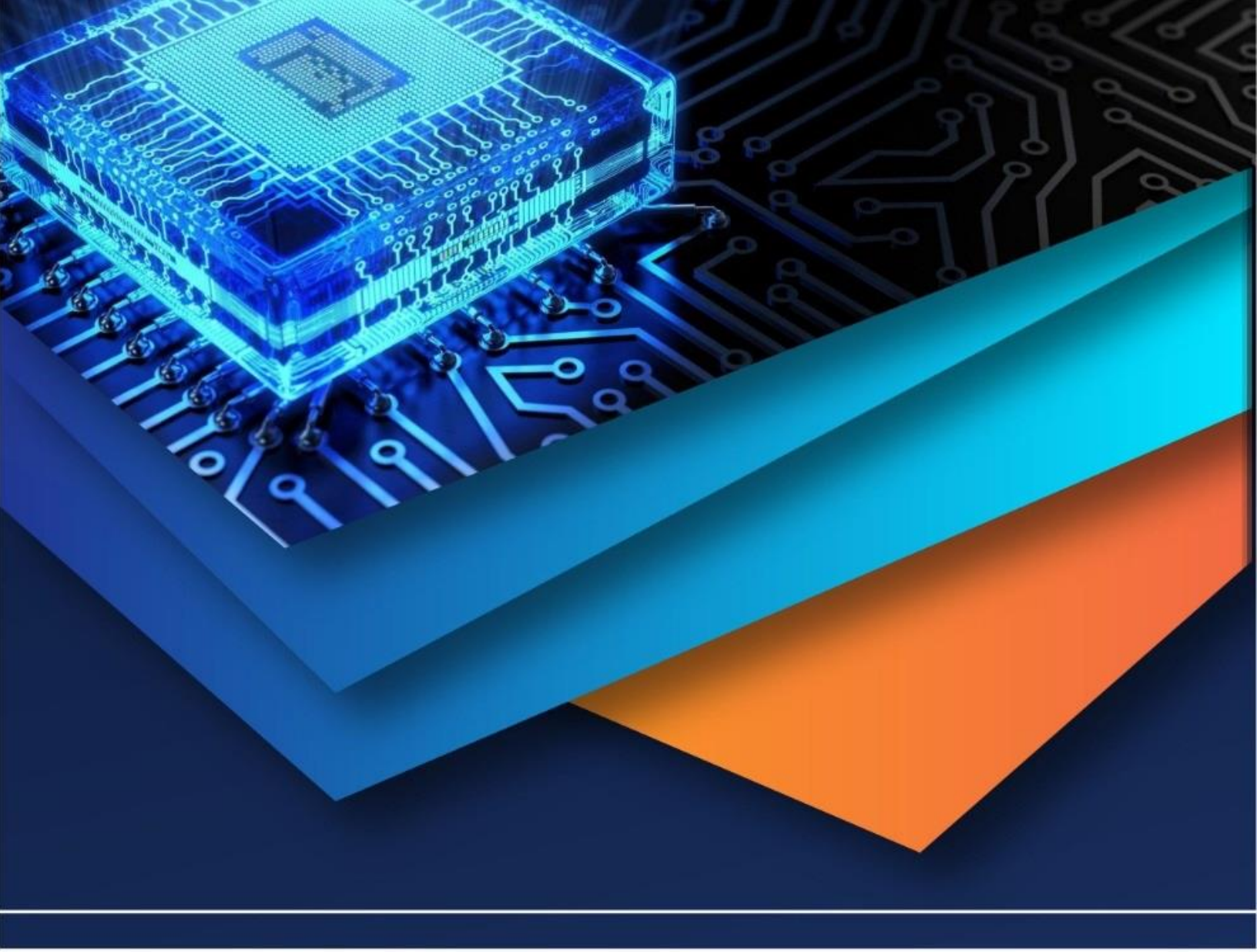
IX. CONCLUSION

This work presented an overview of location privacy preservation in vehicular ad hoc networks. The adversaries exploit the history of location information for several purposes, including advertisement and surveillance. The strengthening the location privacy of vehicles is more significant as the failure of privacy may thwart the development of the VANET communication technology. By

providing safety messages, the location privacy system prevents the users from the eavesdropping attackers. Though these safety messages to assist in preventing the accidents, they are vulnerable to unauthorized adversaries who can track and access the location of the vehicle. Moreover, the VANET needs cost-effective location privacy mechanisms for improving network performance.

REFERENCES

[1] Holger Füßler Sascha Schnaufer Matthias Transier Wolfgang Effelsberg, "Vehicular Ad-Hoc Networks: From Vision to Reality and Back", 4th Annual IEEE/IFIP Conference on Wireless on Demand Network Systems and Services (WONS), 2007
[2] Nathan Balon, "Introduction to Vehicular Ad Hoc Networks and the Broadcast Storm Problem", 2006
[3] G. Myles, A. Friday, and N. Davies, "Preserving privacy in environments with location-based applications", IEEE Pervasive Computing, Vol. 2, Issue 1, pp. 56– 64, 2003
[4] A. R. Beresford, "Location privacy in ubiquitous computing", 2004
[5] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period", in Process of the IEEE Wireless Communications and Networking Conference (WCNC), pp. 1187–1192, 2005
[6] Levente Buttyan Tamas Holczer, Andre Weimerskirch, and William Whyte "SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs", IEEE Vehicular Networking Conference (VNC), pp. 1-8, 2009.
[7] Krishna Sampigethaya, Mingyan Li, Leping Huang, and Radha Poovendran "AMOEBA: Robust Location Privacy Scheme for VANET", IEEE journal on selected areas in communications, Vol. 25, No. 8, pp. 1569- 1589, 2007.
[8] Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung "Wireless Location Privacy Protection in Vehicular Ad-Hoc Ne tworks", IEEE international conference on communications, pp. 1-6, 2009.
[9] Mike Burmester, Emmanouil Magkos and Vassilis Chrissikopoulos, "Strengthening Privacy Protection in VANETs", IEEE conference on wireless and mobile computing, pp. 508- 513, 2008.
[10] Bidi Ying, Dimitrios Makrakis, Hussein T. Mouftah, "Efficient Privacy Preservation Protocol Using Self-certified Signature for VANETS", Tech-Republic, 2011 .
[11] Albert Wasef, Xuemin (Sherman) Shen, "REP: Location Privacy for VANETs Using Random Encryption Periods", ACM journal on mobile networks and applications, Vol. 15, Issue 1, pp. 172- 185, 2010.
[12] Reza Shokri, George Theodora- kopoulos, Panos Papadimitratos, Ehsan Kazemi, andJean-Pierre Hubaux, "Hiding in the Mobile Crowd: Location Privacy through Collaboration", IEEE Transactions on Dependable and Secure Computing, Vol. 11, No. 3, pp. 266-279, 2014.
[13] Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, and Xuemin (Sherman) Shen, "Footprint: Detecting Sybil Attacks in Urban Vehicular Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 6, pp. 1103-1114, 2012.
[14] Francesco Malandrino, Carlo Borgiattino, Claudio Casetti, Carla-Fabiana Chiasserini, Marco Fiore, Member and Roberto S
[15] adao, "Verification and Inference of Positions in Vehicular Networks through Anonymous Beaconing", IEEE Transactions on Mobile Computing, 2013.Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang, and Xuemin Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs", IEEE Transactions on Vehicular Tech., Vol.61 , No.1 , pp. 86-96, 2012.
[16] Qin, Bo, Qianhong Wu, Josep Domingo-Ferrer, and Lei Zhang, "Preserving security and privacy in large-scale VANETs", In Information and Communications Security, pp. 121-135, 2011
[17] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen, "GSIS: A Secure & Privacy Preserving Protocol for Vehicular Communications", IEEE Transactions on Vehicular Tech., Vol. 56, No. 6, pp. 3442-3456, 2007.
[18] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin (Sherman) Shen, "Security in Vehicular Ad Hoc Networks", IEEE Communications Magazine, 2008.
[19] Maxim Raya and Jean-Pierre-Hubaux, "The Security of Vehicular Ad Hoc Networks", 2005.
[20] Vivek Pathak, Danfeng Yao, and Liviu Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing", IEEE international conference on Vehicular Electronics and Safety, pp. 3465- 353, 2008
[21] Alexiou, Nikolaos, Marcello Laganà, Stylianos Gisdakis, Mohammad Khodaei, and Panagiotis Papadimitratos. "Vespa:
[22] Vehicular security and privacy-preserving architecture" In Proceedings of the 2nd ACM workshop on Hot topics on
[23] wireless network security and privacy, pp. 19-24, 2013. Balaram, Allam and Pushpa, S., "Location Privacy using Anonymous Beacon in Vehicular Ad Hoc Networks", Research
[24] Journal of Applied Sciences, Engineering and Technology, Vol. 12, No. 4, pp. 407-414, 2016. Balaram, Allam and Pushpa, S., "Resilient Privacy Preservation Scheme to Detect Sybil Attacks in Vehicular Ad Hoc Networks", Indian Journal of Science and Technology, Vol. 9, No. 48, DOI: 10.17485/ ijst/ 2016/ v9i48 /99870, 2016.
[25] Balaram, Allam and Pushpa, S., "Sybil Attack Resistant Location Privacy in VANET", International Journal of Information and Communication Technology, Inder Science, ISSN: 1741-8070.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY