iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5440

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 V, May 2018- Available at www.ijraset.com

An Effective Location Privacy using SADLP in Vehicular Ad Hoc Networks

Manda Silparaj[1], Gajula Rajender[2], Allam Balaram[3]
[1]*Departmanet of Computer Science and Engineering, ACE Engineering College, Hyderabad.*
[2]*Departmanet of Computer Science and Engineering, AAR Mahaveer Engineering college, Hyderabad.*
[3]*Departmanet of Computer Science and Engineering, St.Peters University, Chennai*

Abstract: ***Vehicular Ad hoc Networks (VANETs) are more influence to a high number of attacks due to its open access and anomalous nature. Security is still a major issue in the VANET. Location privacy of the user should be made as a mandatory property for wireless communication. Once the attacker has the knowledge of the location of the node, it can easily trace its activities. During a long journey, a vehicular user is supposed to cross several Road Side Units (RSUs) that belong to other network communities. An attacker compromises an RSU and easily gets the real identity of a genuine vehicle. It impairs the location privacy of the user. Many of the existing works provides authentication certificates to the vehicles for providing location privacy. The existing works fail to reflect the location privacy, when RSU is compromised. This paper proposes a Sybil Attack Defendant Location Privacy (SADLP) for improving location privacy of the user. In order to provide the location privacy efficiently, a good authentication system is introduced in the proposed work. The SADLP employs a Location Privacy Unit (LPU) for providing good authentication system. The SADLP hides the real identity of a user and provides temporary key and trusted certificate to the users. The user provides the trusted certificate, including consecutive series of random numbers which is gotten from different RSUs for making V2V communication. By verifying the trusted certificate at the interference range of a genuine vehicle and an attacker, the SADLP determines the compromised RSU and thus it provides high location privacy. The simulation results show that compared to existing works, SADLP reduces the Sybil attack and provides high location privacy to the users in VANET.***

Keywords: VANET, Location privacy, Sybil attack, Authentication

I. INTRODUCTION

VANETs [1] [2] facilitate vehicles to communicate each other in also with the support of infrastructure. The span of VANET is too short as the network topology is dynamic in nature. The nodes in the VANET move in and out of the network frequently, as it has a greater dynamic mobility pattern. Moreover, the density of the network keeps on varying with respect to the traffic condition. The major parts of vehicular ad hoc networks are vehicles (entity or node), RSU, the Location Server (LS) and Trusted Certification Authority (TCA). The dynamic nature of VANET makes it more vulnerable to attacks and has several security issues. A privacy location of the vehicle user is much important as the data sent by a vehicle may have important consequences like accident prevention. The exact location of the vehicles is traced using advanced techniques in localization and tracking. Thus, 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 or details of the user can be gathered by identifying the LBS services used by a vehicle.

There are two approaches in VANET. One is vehicle-to-vehicle (V2V) interaction, and the other is vehicle-to-infrastructure (V2I) interaction. In V2V interaction, there is no need for fixed infrastructure or any RSUs, and it is purely ad hoc in nature. In V2V, a vehicle interacts only with another vehicle to estimate the traffic condition. On the other hand, in the case of V2I interactions, interactions are held between a vehicle and a fixed infrastructure like RSUs. This kind of infrastructure provides aggregation and key distribution to the vehicles. The major issue to be considered in this architecture is the number of required RSUs cannot be predicted. VANET has several security issues such as location privacy, traceability, availability, integrity, confidentiality, and authentication, non-repudiation, and non-frame ability. An efficiency of any system that provides a solution to above problems can be estimated using storage, efficiency in communication and computation efficiency [3].

In urban vehicular networks, location privacy preservation is very challenging. A malicious attacker can pretend to be multiple vehicles and disseminate false data in the network named as Sybil attack. Sybil attack is a significant concern as it impairs the performance of VANET. In Sybil attack, the attacker can design multiple identities, and it sends the identities to the other nodes to corroborate false data. It is simple to launch other attacks in the network at the presence of Sybil attack. The previous approaches

©IJRASET: All Rights are Reserved

develop several techniques to detect and reduce the Sybil attack and preserve the location privacy. However, an ingenious attacker compromises an RSU and collects the information of a genuine vehicle from the RSU. It is crucial to develop new approaches for preserving the user's location privacy. This paper proposes an SADLP to preserve the location privacy of a single user. The SADLP explained in two steps such as authentication system and TC verification system. The authentication system provides trusted certificate, temporary key and ID to the users for making secured V2V communication. The trusted certificate contains a random number series, which is received from different RSUs. The TC verification process identifies the false message by verifying the random number attached in the trusted certificate at the interference range of a genuine vehicle and an attacker. Moreover, it can identify the compromised RSUs which helps to the attacker for generating trusted certificates falsely.

A. Contribution

1) The primary objective of the proposed work is to preserve the location privacy of the user and reduce the Sybil attack in VANET. The SADLP scheme determines the compromised RSU and attacker using trusted certificate with random number series of the vehicle.

2) An authentication system provides a temporary trusted certificate, key and ID to vehicles using LPP unit. By providing good authentication system, the SADLP hides the users' real identity.

3) The TC verification system identifies the forgery trusted certificate of an attacker at the interference range of a genuine user and attacker. By using a random number series, the TC verification system distinguishes the forgery trusted certificates from real trusted certificate.

4) The performance of the SADLP is evaluated using Network Simulator-2 (NS-2). The simulation results demonstrate the performance of an SADLP. Compared to existing works, the SADLP provides better location privacy to the users.

II. RELATED WORKS

A. Security and privacy in VANET

The VANET users are greatly affected by threats over location privacy as they are not guaranteed privacy and the location of the vehicle can be traced out using their broadcast. To overcome this drawback [4] proposes an approach called CARAVAN. In considering the greater mobility, an approach was based on combining all neighbouring vehicles and formed into a group. This group formation significantly mitigates the number of broadcast times that the vehicle is used for V2I applications. This grouping mechanism helps in achieving extended silent period for each vehicle and thus anonymity gets improved. Additionally, an enhancement technique also suggested that considers the separation of RSUs and the ability of a vehicle to control its transmission power. Threats may arise for VANET users from the LBS application used by it, and it is effective in the global adversary model and over the safety application constraints. [5] Provides anonymity in which the vehicle updates its keys on direction changes, but using this system anonymity cannot be achieved in global adversary model.

The basic requirements regarding security and privacy between various communication devices in VANET are discussed in [6]. In order 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 RSU. Group signature concept and ID-based signature (cryptography) concept is used in the first and the second aspect respectively. The detailed description about privacy issues are addressed in [7]. This deals with privacy and security of vehicle-to-infrastructure interaction for providing safety, especially between vehicles and traffic light that act as an RSU. This system mainly aims at managing privacy rather than providing a complete anonymity or no privacy at all.

B. Privacy enhancing techniques in VANET

Privacy in VANET can be provided by varying the pseudonyms over a period of time. But that is not enough for maintaining the privacy and so [8] proposes a technique called mix contexts to enhance the privacy level for VANET users. The context information is used to trigger a change in pseudonym.

The VANET nodes cooperatively utilize the best opportunity to mix together with the number of vehicles and thus anonymity gets improved. The concepts of mix zones and mix nets are fused to form a new concept, mix contexts. The use of centralized mapping is well designed using approximate techniques.

©IJRASET: All Rights are Reserved

A cryptographic mechanism is used to strengthen the privacy in VANET, and it provides a trade-off between the user's privacy and accountability of an adversary model [9]. Pairwise communication and group communication among vehicles along with a 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.

To ensure privacy, a pseudonym is varied when it is needed and thus reduces overhead.

The idea of selecting the degree of privacy is left to the user in [10]. An adaptive privacy-preserving authentication mechanism has been suggested to achieve this requirement. It can provide a tradeoff between the degree of privacy and computation and communication overhead.

It also explains the major challenges regarding privacy and security. The adaptive privacy-preserving technique has been introduced mainly to reduce the computational and communication overhead. The value of communication overhead is calculated by the quantity of transmitting encrypted data.

The value of computational overhead is calculated by the number of authenticated common secrets distributed among all genuine users in addition to the amount of transmitted encrypted data. The number of messages that are to be delivered can be computed on the basis of VANET user's privacy requirements.

This value is then used to set the values of different parameters that are used in the privacy protection protocol. Thus, the degree of privacy can be related to the available resources. A user may assign to a lower degree of privacy when there is only limited resources and vice versa.

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 [11]. 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 [12].

Pairwise communication and group communication among vehicles along with a 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 when needed and thus reduces overhead. The work in [13] 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 a 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 RSU. 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 [14].

A MobiCrowd scheme is introduced in [15]. 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. Hiding from the crowd, the user generates a hiding local query for determining their locations.

The users who receiving the query 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.

A privacy-preserving framework in [16] introduces an Anonymous Verification and Inference of Positions (A-VIP) for verifying the vehicle position based on location authority. In [17], a Pseudonym Changing at Social spots (PCS) mechanism developed two 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 [18].

C. Location privacy and Sybil attack

In [19], 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 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. In [20], introduced a lightweight and scalable protocol to detect Sybil attack and to preserve the privacy. The RSUs overhears the distributed messages and determines the Sybil attacker.

©IJRASET: All Rights are Reserved

This protocol hides the real identity of vehicles at all times. Thus, the privacy is preserved. 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.

The work in [25] explains about survey about preserving location privacy of vehicle using cryptographic techniques.

III.OVERVIEW

A. Trusted certification authorities (TCAs)

TCA is a backbone of the security and privacy concerns in VANET. TCA is a unit that is mainly designed to establish trusts. TCA issues, personal certificates to RSUs, which in turn distributes them to vehicles. When a vehicle wants to communicate with other vehicles, it has to prove its identity issued by TCA.

TCA is also responsible for revoking certificates of malicious users. It has to meet the security requirements in its surrounding areas. The function of TCA is similar to the base station in MANET. It must also assure inter region's security as the vehicles keep on moving under different TCAs. TCA is the only unit that is trusted by all other units in VANET.

B. Road Side Unit (RSU)

RSU is a unit that participates in securing VANET users. It acts as an intermediate unit between TCAs and VANET users. TCA uses to guide or command RSU and give some specific task regarding security and privacy. This paper mainly concentrates on location privacy.

A TCA may have any number of RSU under its control within its transmission range. It should check the composition of the trusted certificate issued by TCA.

The mandatory fields in trust certificate are vehicle and owner's identity, public key of the vehicle, vehicle type (professional, personal, police, etc.), validity of trusted certificate, a unit that can identify the TCAs and together with these, it must contain the signature of the trusted certificate using the private key of trusted certificate authorities.

C. Transportation Administrative Office (TAO)

The TAO, which already has the real identity of all vehicles in the network. When the vehicle moves from its home network domain into other visited network, it registers to the TAO through RSU.

By registering to the TAO, each vehicle hides its real identity and gets a trusted certificate for other inter-communications. The vehicle can get temporary trusted certificate, key and ID using a trusted certificate.

D. Location Privacy Unit (LPU)

The LPU contains two parts such as key generator and local location server. The key generator generates temporary keys and IDs. The Location server is a part of the main server, and it provides the local location information to the users. The location server also stores the localized location information which is received from the RSU.

©IJRASET: All Rights are Reserved

IV. SYSTEM MODEL

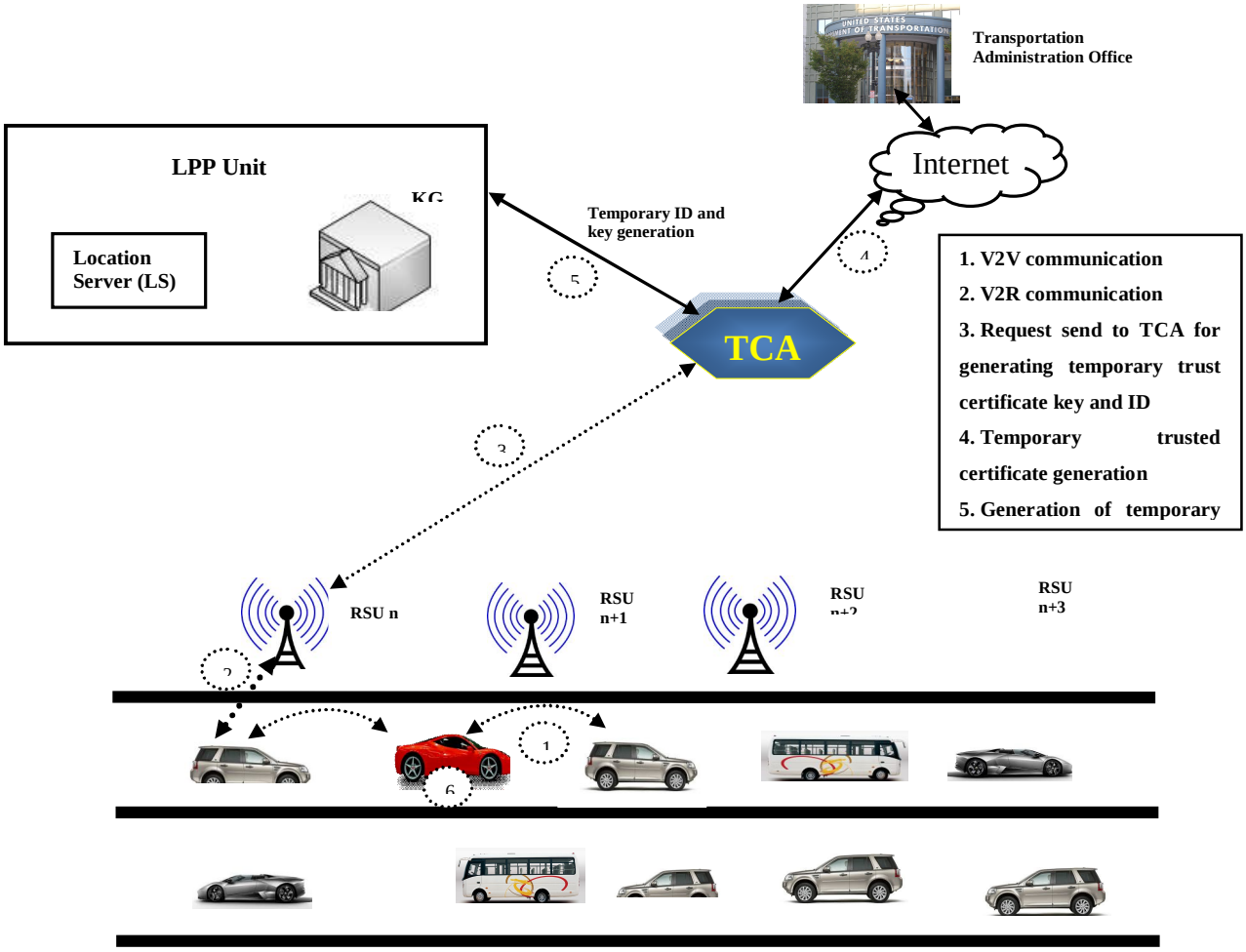


Figure.1 VANET hierarchy

The vehicle is equipped with OBU for enabling V2V and V2R communications. A GPU is a database unit, and it is attached to a vehicle for sensing the circumstance activities. A detailed view of system architecture is illustrated in figure.1. The architecture contains a number of vehicles, RSUs, LPU, TAO, and TCA. The number of vehicles is defined as V and the speed of a single vehicle v (v∈V) is S. The central part of the VANET structure is trusted certificate authority (TCA) and it has several RSUs in its control. A vehicle may contact TCA only through RSUs. TCA responds to the RSU's request by distributing the public key (K_{TA}^{pub}) and trusted certificate (TC_{VH}) which in turn distributes it to the vehicle to carry out the vehicle to vehicle communication. A vehicle will be under any one of the RSU's controls on its way. Moreover, the transmission range of a vehicle (TR_{VH}) will be larger when compared to the total width of the road and therefore, the position of a vehicle on the road does not influence the security and privacy. Each OBU/RSU is associated with temporary private/ public key pair that is generated by key generator. TCA issues trusted certificate to RSU in turn RSU distributes to vehicles under its control. This trusted certificate has a validity period after which it gets expired.

V. SYBIL ATTACK DEFENDANTS LOCATION PRIVACY (SADLP)

The proposed SADLP contains two processes such as authentication and TC verification. In SADLP, the authentication system hides the real identity and provides a temporary trust certificate and key to the users. When a vehicle cross first RSU, it receives the trusted certificate. In order to reduce overhead, the vehicle employs the same trusted certificate to cross the RSU group. Each RSU

©IJRASET: All Rights are Reserved

in the RSU group provides a random number to the vehicle and the vehicle stores the random number. When communication occurs between vehicles, the sender sends the trusted certificate, including random number series to receiver for authentication. The TC verification system verifies the trusted certificate at the interference range of the vehicle and attacker. If any falsely trusted certificate is determined by RSU, it informs to the TCA. Moreover, the SADLP provides high location privacy to the users.

A. Authentication

An adversary tries to prevent the privacy of either a vehicle or an RSU. The both vehicles or RSU components do not reveal their original identities and keys (public or private) during the communication instead they use temporary IDs and keys. These temporary IDs and temporarily trusted certificates are generated using a technique called public cryptography. An RSU keeps on broadcasting its temp_ID and temp_key within its transmission area. Whenever a vehicle enters its transmission range, it is supposed to receive RSUs broadcast and then involves associating itself and initiates the one-to-one authentication process. A vehicle requests the trusted certificate authorities to the RSU. Then, RSU forwards the vehicle's request to the corresponding TCA [20].TCA authenticates both the vehicle and RSU, and forwards the authentication information to RSU. TCA provides only partial authentication in order to reduce the computational overhead. RSU verifies the partial authentication of the vehicle and forwards it to the vehicle for RSU authentication [21]. The TCA issues a temporarily trusted certificate and temporary key, ID to carry out the communication between vehicles. The temporary key and ID are received from the LPP unit and trusted certificates are received from TAO. The entire process involves only one request-reply pair. The requesting object is a vehicle while the replying objects are TCA and RSU. The time taken for vehicle authentication falls under only in milliseconds.

The SADLP employs a good authentication system which can provide better privacy preservation. The proposed authentication system involves 4 steps. In the first step, the vehicle sends the request to the RSU for authentication of the vehicle. In the second step, the RSU forwards the request to TCA. The TCA sends the trusted certificates to the RSUs group in the third step. At the final step, the RSU responds to the vehicle. A diagrammatic representation of the authentication process is shown in figure 2.

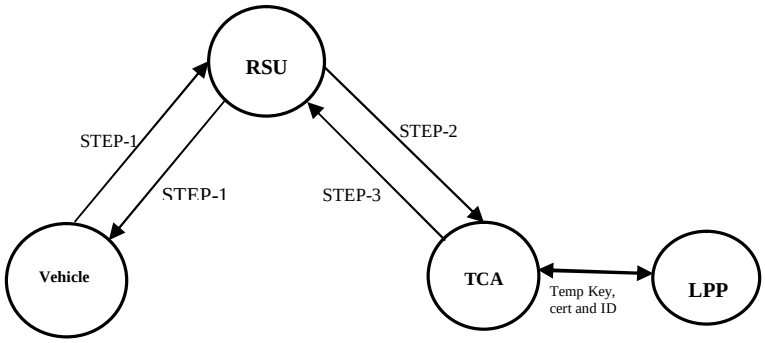


Figure 2: Flow of vehicle authentication

1) *Step 1: Vehicle (VH) communicates with RSU (VH/ RSU):* In the first step, the vehicle sends request to the RSU for authentication. A vehicle's request must contain the following information. Message type indicates the type of the message and it is a 1 byte field. The field payload indicates the position, direction, acceleration of the vehicle and it is generally 100 byte field. The TTL field indicates the time period or validity of the message that is allowed to remain in the VANET or in the transmission range of RSU group. RSU group ID is used to identify the group of the vehicle which it belongs to. The temporary ID of the vehicle represents the pseudo ID in order to conceal its original ID. SignVH field indicates the vehicle's signature on the previous six fields. The vehicle sends the authentication request to nth RSUn. The private key of the vehicle encrypts the time stamp and vehicle identity.
2) *Step 2: RSU communicates with TCA (RSU/ TCA):* In this step, RSU forwards the vehicle's request to the TCA. The RSU decrypts the timestamp value and vehicle's temporary identity of the vehicle and store it in a session until the TCA does not respond to the RSU request. After the decryption, the RSU forwards the encrypted packet (excluding the decrypted timestamp value and vehicle's temporary ID) to the TCA.The TCA then decrypts the RSU authentication request using its public key and verifies the vehicle and RSU.

©IJRASET: All Rights are Reserved

3) *Step 3: TCA communicates with RSU (TCA/ RSU):* As soon as the completion of the authentication process of vehicle and RSU, TCA will issue a trusted certificate (trusted_cert) with TTL to the vehicle through RSU. The trusted certificate is valid until the TTL value gets expired. The validity of the trusted certificate also depends on the duration of stay on the vehicle in an RSU moving at a high average speed. Therefore, different vehicles will have trusted certificates with different TTL values. Simultaneously, TCA will inform to all other RSUs in that particular group about the authentication of the vehicle. Finally, all the RSUs in a group have knowledge about the authentication of a particular vehicle. The RSU has to verify whether the encrypted packet is equal to CTA temp_ID_{VH} and TTL. If both values are the same, then the vehicle can authenticate RSU.
4) *Step 4: RSU communicates with VH (RSU/ VH):* This is the final step in the authentication process in which the RSU responds to the vehicle's request. The RSU attaches a random number in the trusted certificate. The RSU forwards the trusted certificates to the vehicle and at the same time the vehicle authenticate the RSU group. When the vehicle enters the communication range of other RSU, it verifies the certificate and get a random number of the RSU. The vehicle stores the random number series for authentication. The trusted certificate format is shown as follows, These are the steps to be followed at the time of authentication of the vehicle. Whenever a vehicle enters the other group of RSU, it has to re-authenticate. In addition, in the case of expiry of trusted certificate, the vehicle must re-authenticate using the 4 steps.

B. TC Verification

If the communication occurs between vehicles, a sender should attach the random numbers for previous four fields to the trusted certificate, and it submits the trusted certificate to the receiver. The receiver reaches the interference range, and it forwards the trusted certificate to the corresponding RSUs for verification. The RSUs verify the random number series of a receiver. If anyone RSU is compromised, the other genuine RSU determines the compromised RSU uses random number verification. The genuine RSU reports to the TCA to provide warning a message to the compromised RSU. The TCA maintains the key, trusted certificate and the real identity of an RSU and a vehicle. Using this information, the TCA verifies the concern is correct or not. If it is true, the TCA gives warning a message to the compromised RSU and provide a new temporary ID and a key to the compromised RSU. The TCA also provides invoked certificate to the attacker.

The TCA inspects the corresponding RSU for a particular time to improve the system performance. The attacker compromises an RSU n+1 and gets legal trusted certificates of other genuine vehicles. The attacker launch a Sybil attack on the network using legal trusted certificates. The genuine vehicle receives multiple trusted identities from the attacker. The trusted certificates are verified by RSUn and RSU n+1 at interference range. By verifying the trusted certificate with random number series, the RSUn determines the forged trusted certificate. The RSUn sends a compromised message to the TCA. A compromised RSU may blame the genuine RSU to launch the attack severely. The TCA verifies the compromised message, and it ensures RSU n+1 is compromised. The TCA sends a warning message to the compromised RSU n+1, and it provides new temporary key and ID RSU n+1. The TCA also provides an invoked certificate to the attacker. The TCA inspects the RSU n+1 for a particular time. Thus, the SADLP reduces the Sybil attack and protect the location privacy of the users efficiently.

VI. PERFORMANCE ANALYSIS

A. Simulation setup

The effectiveness of the proposed system is verified through simulation using the NS-2. The table 1 shows the simulation parameters. The entry of vehicles on the road is considered at random model in the area of 4 X 4 Km^2. The distance between two vehicles is assumed to be safety, and their communication range lies between 300m at the rate of 5 Mbps. Each simulation runs for a time period of 300 seconds. The proposed SADLP is compared with PCS scheme [17] for analyzing performance.

Parameter	Value
Vehicle generation	Random
Area	4 X 4 Km^2
Average high speed	60 Km/hr
Vehicle's communication range	300m
Data rate	5 Mbps
Packet size for vehicle message	480 bytes
Packet size for RSU message	380 bytes
Simulation time	300 s

Table 1: Simulation parameter

©IJRASET: All Rights are Reserved

B. Simulation Results

1) Expected Maximum Discovering Time

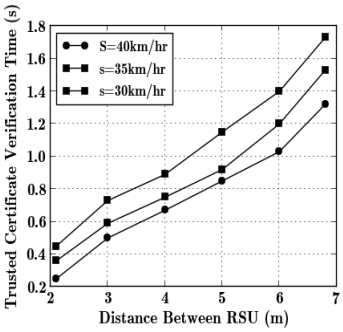


Figure.3 Distance vs. Expected Maximum Discovering Time

The EMVT is defined as the time taken by a vehicle to verify the trusted certificate after receiving it from another vehicle. It decreases with increasing the speed of the vehicle. The relationship between distance vs. EMVT is shown in figure.3. The simulations are performed for different speed values. The EMVT value is low to high-speed vehicles. For an example, a high-speed vehicle 60km/hr reach a distance 600m within 0.6 minutes and a low-speed vehicle 40km/hr reach a distance 600m within 0.9 minutes.

2) Location Privacy Accuracy (LPA)

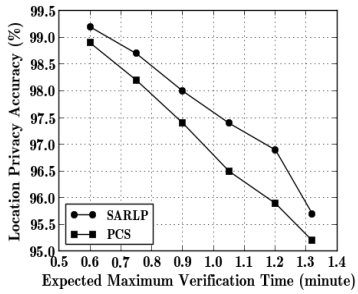


Figure.4 EMVT vs. LPA

It is the number of vehicle's location that can be preserved from the adversary to the total number of vehicles. In SADLP, a low EMVT vehicle achieves high location privacy, and a high EMVT vehicle achieves low location privacy compared to high EMVT vehicle. The relationship between EMVT and LPA is shown in figure.4. Compared to PCS technique, the SADLP achieves high location privacy by verifying the random number series within an EMVT period. In the figure. 4, a vehicle which has EMVT value 11s achieves 99.2% LPA and a vehicle have EMVT value 50s achieves 97% LPA.

3) Communication Overhead

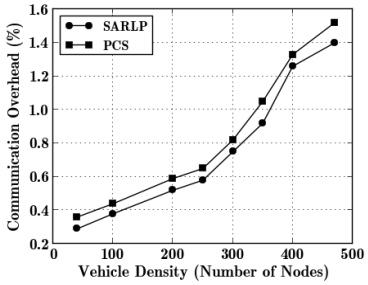


Figure.5 Vehicle density vs. communication overhead

©IJRASET: All Rights are Reserved

The relationship between vehicle density and communication overhead is shown in the figure 5. The communication overhead is the number of additional packets used in SADLP for providing location privacy. The additional packets are trusted certificates, temporary keys, compromised messages, warning messages and invoked certificates. In SADLP, the partial authentication of a trusted certificate reduces the communication overhead considerably. The communication overhead increases with increasing the vehicle density. The PCS scheme considers the location privacy of the user while it has not considered the impact on location privacy due to Sybil attack. The SADLP divides the RSUs into groups, and it provides a trusted certificate to the vehicle, at entering into the RSU group only. For an example, the PCS attains communication overhead 0.65 for 250 vehicles and SADLP attains the communication overhead 0.55 for 250 vehicles.

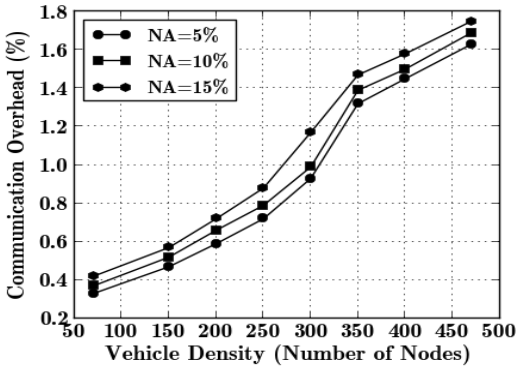


Figure.6 Vehicle density vs. communication overhead

The communication overhead for different number of attackers is shown in figure.6. When attacker presents in VANET, the TCA generates warning a message and invoked certificate. The communication overhead increases with increasing number of attackers. However, SADLP scheme attains at much lower overhead when compared to the existing PCS schemes.

4) Authentication Delay

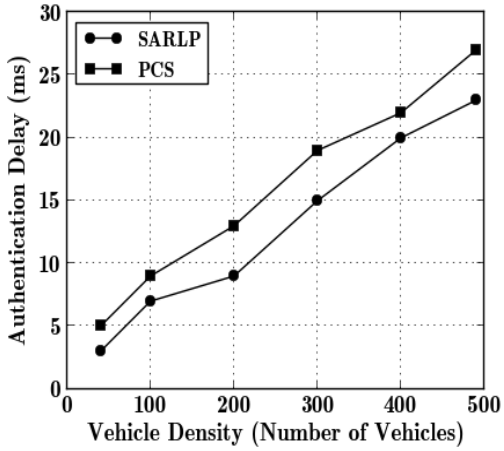


Figure.7 Vehicle Density vs. Authentication Delay

An authentication delay is defined as the time taken to deliver a temporarily trusted certificate to the user. The authentication delay increases with increasing vehicle density is shown in figure.7. When the network traffic is high, the vehicles are waiting in the queue. The trusted certificate authentication delay increases with increasing vehicle density in the urban area. In order to reduce the delay, the SADLP provides a less number of trusted certificates to each vehicle as the group formation of the RSU. For an example, in figure.8, SADLP attains 20ms authentication delay for 400 vehicles and PCS attain 23ms authentication delay for 400 vehicles.

©IJRASET: All Rights are Reserved

5) Effect of number of attackers

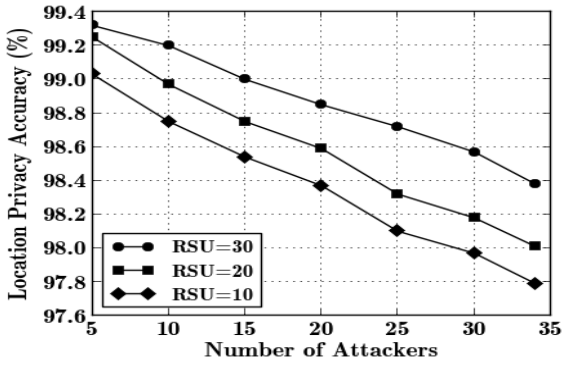


Figure.8 Number of attackers vs LPA

The relationship between the number of attackers versus location privacy is shown in figure. 8. The location privacy decreases with increasing number of attackers. It is varied for different number of RSUs. High number of RSUs detects and invokes the attackers quickly and thus improve the location privacy.

VII. CONCLUSION

This paper addresses the location privacy of a single user and proposes an SADLP scheme that ensures location privacy assures privacy of the VANET user. By verifying TC with random number series, the SADLP reduces the Sybil attack and improve location privacy. In SADLP, the TCA is responsible for trust verification for both vehicle and RSU, the RSUs load is significantly reduced. The SADLP involves only one pair of request-reply which reduces communication overhead and reduces authentication delay. When a traffic load is high, communication overhead increases substantially. Neighbouring RSUs are grouped to reduce the communication overhead. Authentication by neighbouring RSU using RSU group ID reduces this complexity. The proposed SADLP performance is simulated in the NS-2 simulator. The simulation results show that SADLP provides significant improvement in location privacy of the user. However, compared to existing works, the SADLP provides high location privacy to the user

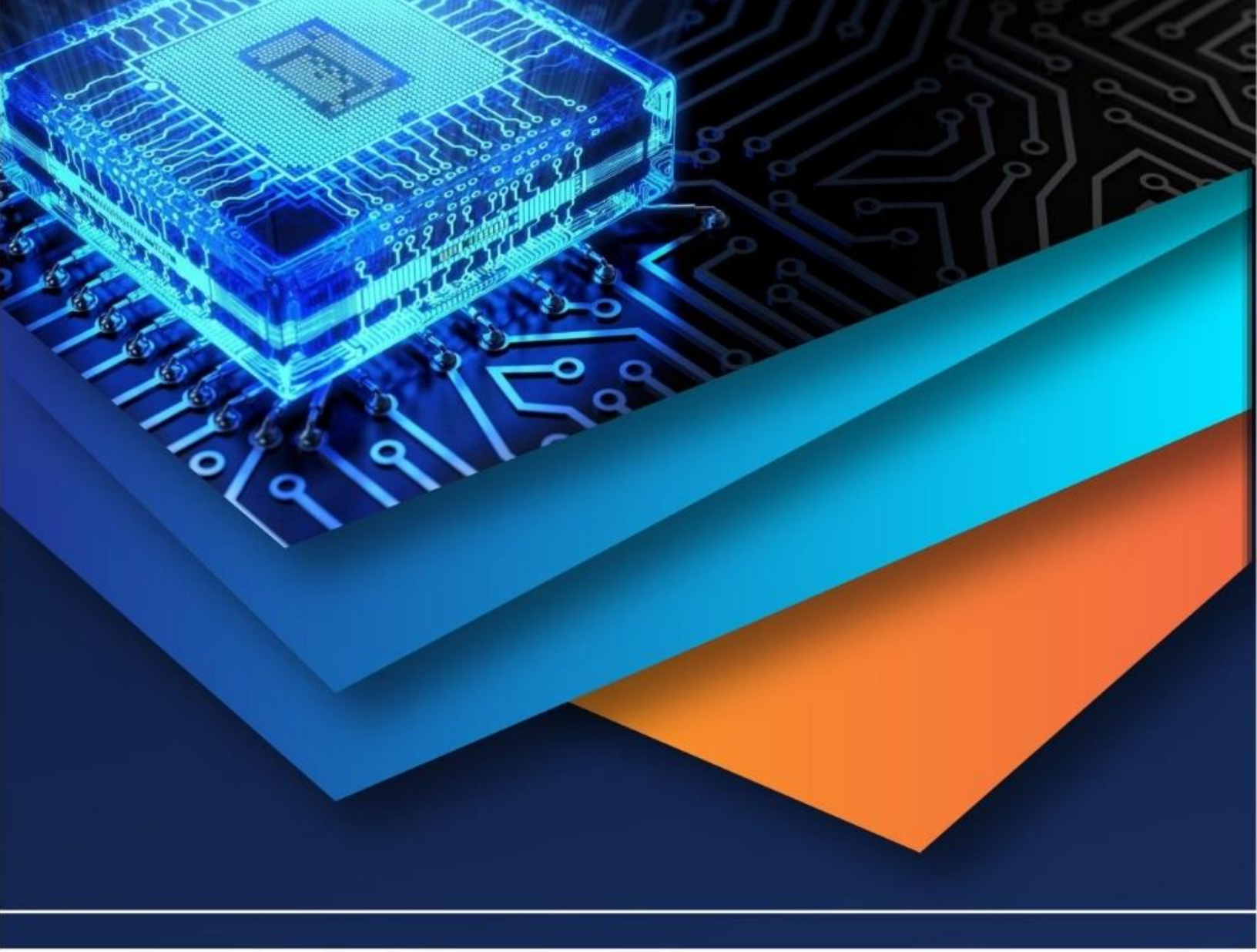
REFERENCE

[1] Holger Fubler, Sascha Schnaufer, Matthias Transier, and 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] Boukerche, Azzedine, Horacio ABF Oliveira, Eduardo F. Nakamura, and Antonio AF Loureiro, "Vehicular ad hoc networks: A new challenge for localization-based systems" Computer communications, Vol. 31, No. 12, pp. 2838-2849, 2008
[4] Krishna Sampigethaya, Leping Huangy, Mingyan Li, Radha Poovendran, Kanta Matsuuray, and Kaoru Sezaki “CARAVAN: Providing Location Privacy for VANET”, 2005
[5] Maxim Raya and Jean Pierre Hubaux “The Security of Vehicular Ad Hoc Networks” IOS transaction on computer science and networking and security, volume 15, pages 39- 68, 2007
[6] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen “GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications” IEEE transactions on vehicular technology, volume- 56, issue 6, 2007
[7] Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang “An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks” IEEE transactions on parallel and distributed systems, volume 21, issue 9, 2010
[8] Matthias Gerlach “Full Paper: Assessing and Improving Privacy in VANETs”, 2006
[9] Mike Burmester and Emmanouil Magkos and Vassilis Chrissikopoulos “Strengthening Privacy Protection in VANETs” IEEE international conference on wireless and mobile computing, pages 508- 513, 2008
[10] Kewei Sha, Yong Xi, Weisong Shi, Loren Schwiebert, and Tao Zhang “Adaptive Privacy-Preserving Authentication in Vehicular Networks” first IEEE international conference on communications and networking, pages 1- 8, 2006
[11] Joo-Han Song, Vincent W.S. Wong, and Victor C.M. Leung “Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks”, IEEE international conference on communications, pp. 1-6, 2009
[12] Mike Burmester, Emmanouil Magkos and Vassilis Chrissikopoulos, “Strengthening Privacy Protection in VANETs”, IEEE international conference on wireless and mobile computing, pp. 508- 513, 2008
[13] Bidi Ying, Dimitrios Makrakis, Hussein T. Mouftah, “Efficient Privacy Preservation Protocol Using Self-certified Signature for VANETS”, Tech-Republic, 2011

©IJRASET: All Rights are Reserved

[14] 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
[15] Reza Shokri, George Theodorakopoulos, 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
[16] Francesco Malandrino, Carlo Borgiattino, Claudio Casetti, Carla-Fabiana Chiasserini, Marco Fiore, Member and Roberto Sadao, "Verification and Inference of Positions in Vehicular Networks through Anonymous Beaconing", IEEE Transactions on Mobile Computing, 2014
[17] Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang, and Xuemin (Sherman) Shen, "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs", IEEE Transactions on Vehicular Technology, Vol.61 , No.1 , pp. 86-96, 2012
[18] 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
[19] 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
[20] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, Pin-Han Ho and Xuemin (Sherman) Shen "An Efficient Message Authentication Scheme for Vehicular Communications" IEEE transactions on vehicular technology, volume 57, issue 6, 2008
[21] Mohamed Salah Bouassida "Authentication vs. Privacy within Vehicular Ad Hoc Networks" International Journal of Network Security, Volume 13, issue 3, pages 121- 134, 201
[22] Balaram, Allam and Pushpa, S., "Location Privacy using Anonymous Beacon in Vehicular Ad Hoc Networks", Research Journal of Applied Sciences, Engineering and Technology, Vol. 12, No. 4, pp. 407-414, 2016.
[23] 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
[24] Balaram, Allam and Pushpa, S., "Sybil Attack Resistant Location Privacy in VANET", International Journal of Information and Communication Technology, Inder Science, ISSN: 1741-8070.
[25] Balaram, Allam, Rajender Gajula, and Vijayalaxmi, M., "A Survey-Cryptography based Location Privacy in Vehicular Ad Hoc Networks", International Journal for Research in Applied Science and Engineering Technology, Vol. 6, No. 2, 2018.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)