ISSN: 0975-766X
CODEN: IJPTFI
Available Online through Research Article
www.ijptonline.com

PERFORMANCE ANALYSIS OF LOCATION BASED PSEUDO IDS FOR PRIVACY PRESERVATION IN VEHICULAR NETWORKS

Y. Bevish Jinila
Assistant Professor, Department of Information Technology, Faculty of Computing,
Sathyabama University, Chennai, India.
Email: bevish.jinila@gmail.com

Received on: 10-03-2017 *Accepted on: 02-04-2017*

Abstract

Safety applications in vehicular networks should be handled with at most care such that no adversary should be allowed to intrude the privacy of the user. Replacement of IDs with pseudo IDs makes this possible. Generation of pseudo IDs play a major role. In this paper, we propose a novel approach, where pseudo IDs are generated on trip based on the location information and verified by the distributed Traffic Management Servers (TMS). Experimental analysis shows that this scheme provides better privacy and conditional traceability compared to existing approaches.

Keyword: Pseudo ID, Privacy, Vehicular Networks, Traffic Management Server.

Introduction

Vehicular Ad hoc Network (VANET) is an emerging intelligent network that provides safety and comfort to the public. This network includes a centralized Trusted Authority (TA), several Road Side Units (RSUs) and vehicles equipped with On Board Unit (OBU). Safety applications in VANET can be periodic or event driven. In case of event driven applications, a safety message is communicated by a specific vehicle that experiences the mishap or detects a mishap. The safety message includes the id of the vehicle, location, speed and events noticed. These messages are verified for their authenticity by the receivers. During this process, there is a chance where an adversary can reveal the id of the source vehicle by receiving the messages. This paves way for tracing a particular user on his/her travel or misuse of his/her ID where by invading their privacy. So, it is mandatory to preserve the privacy of the user involved in the communication. To do so, the source id of the vehicle should be replaced by some pseudo ID and should be changed frequently. Generating and maintaining pseudo IDs for a lifetime and revoking them requires a Revocation List (RL) to be retained. Each time an ID is verified for its validity this list should be consulted which becomes a serious issue. Also, the privacy provided to the vehicles should be conditional so that it can be traced if required by the trusted authority. This paper addresses pseudo ID generation on trip based on the location of the vehicle. When an event is reported by the vehicle, pseudo ID is generated and the message is communicated. In this system, we have included Traffic Management System (TMS) distributed across various zones and which is responsible for the verification of the events happened in the network. It is also responsible for taking necessary action. This scheme overcomes the problem of maintenance of revocation lists and storage of generated pseudo IDs in the Tamper Proof Device (TPD).

The rest of the paper is organized as follows. Section II presents the related work. Section III describes the system model, architecture and assumptions made. Section IV details the performance analysis of security and privacy provided by the system. Section V concludes our work and provides future directions.

Related Work

Several researchers have given their contribution in the area of privacy preserving authentication. Certain approaches provide conditional privacy to the user and certain don't. Subir Biswas [1] has proposed to use a common pseudo id for all the vehicles in a particular communication range. And, this pseudo id is selected from the most significant bits of the GPS (Geographical Positioning System) coordinates so that all vehicles within a communication range hold the same pseudo identity information. This method provides a complete privacy for the user, but doesn't provide any solution for conditional traceability.

The other most common approach used by several authors for pseudo id generation is the one proposed by Zhang [2]. This approach uses the real id to generate the pseudo ids. This scheme heavily relies upon the TPD (Tamper Proof Device) for storing all the pseudo ids generated by the trusted authority during vehicle registration. Though, it is proved to be conditionally traceable it is required to store the set of generated pseudo ids in the TPD and each time a message is send a different pseudo id is utilized.

Based on this method proposed by Zhang [2], the author [3] suggests a slightly different approach where the lifetime of the pseudo id is included. Based on the lifetime the pseudo ids are changed. And, similar to the other approach the pseudo ids generated are conditionally traceable and are stored in the vehicle's TPD.

Both these approaches completely rely on the TA (Trusted Authority) for traceability of the vehicles which makes the task of the TA overloaded. Also, Zhang [2] has included a driver authentication module where the driver has to provide the real id of the vehicle and the password for authentication but, it is not included in the process of pseudo id generation. Moreover, the entire task of traceability is done by the trusted authority.

Certain other authors have given different approaches for changing the pseudo IDs at certain intervals. Other has proposed that changing the pseudo IDs at fixed intervals makes the adversary to track the vehicle [4,5]. Other has proposed that the pseudo IDs can be changed at fixed locations called mix zones so that when all the vehicles in a mix zone changes their pseudo IDs at one point of time, it becomes impossible for the adversary to track the vehicle. Another author has proposed a more similar approach with changing pseudo ids at social spots.

Storing all generated pseudo ids in TPD and using them at regular intervals or changing it at fixed intervals or in mix zones becomes more hectic and even an adversary can trace the id of the vehicle when it is changed [6-8]. To overcome the limitations of all the previous approaches we have included the location information of the vehicle for pseudo id generation. On trip, the pseudo IDs are generated when an event is to be reported and it varies based on the travelling location. This scheme overcomes the limitation of storing multiple pseudo IDs in the TPD.

System Model

In this section, we propose a novel method of dynamic pseudo ID generation based on the location. In addition to TA (Trusted Authority), this scheme proposes the Traffic Management System (TMS) distributed across various zones. This TMS is responsible for taking necessary action in their respective zones when an event is reported. The notations used throughout this paper are listed in Table 1.

Table I: Notations Used in Our System.

Notations	Description
TA	Trusted Authority
TMS	Traffic Management Server
TPD	Tamper Proof Device
G	Cyclic Group
P	Generator of the cyclic group G
q	Prime order
Tpub	Public key of TA
m	Master secret of TA
d	Secret password assigned for a driver
Rid	Real Id of the Vehicle
Pid	Pseudo id of the vehicle
H	Hash function – SHA 1
f	A function

A. System Architecture

The system is equipped with a TA who is responsible for vehicle registration, password generation, stores the generated passwords and their corresponding real ids. In our system, we have introduced TMS distributed across various zones. This TMS is responsible for taking necessary action when an event is reported by the vehicles. Also, in case of any dispute, it forwards the message to the TA to trace the real ID of the vehicle involved. In addition, the user of each vehicle registered in the network, will be issued with a secret password which is used for driver authentication. On trip, when a vehicle needs to report an event it generates the pseudo ID immediately based on the current location and reports the event to the RSU available within in its communication range. These events related messages are collected by the RSU and are forwarded to the TMS to take necessary action. In case of any suspicious event report, the safety message is forwarded to the TA for retrieving the real ID of the vehicle. Knowing the real ID, the TMS takes the responsibility for endowing appropriate action on the vehicle involved in the dispute.

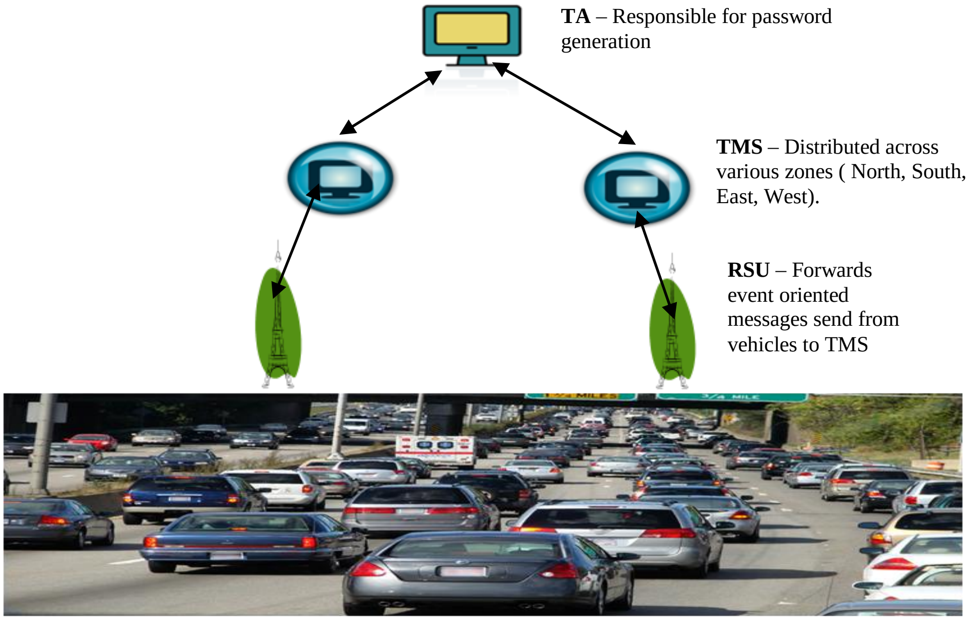
TA – Responsible for password generation
TMS – Distributed across various zones (North, South, East, West).
RSU – Forwards event oriented messages send from vehicles to TMS

Fig 1 : System Architecture.

As shown in figure 1, when an event is noticed by the vehicles nearby it sends a safety message to the RSU in its communication range regarding the events reported. The format of an unsigned safety message is shown in Table II. It includes the type ID, pseudo ID, location, speed and the ID of the event reported.

Table-II: Format of an Unsigned Safety Message.

Type ID	Pseudo id	Location	Speed	Event ID
2 bytes	2 bytes	4 bytes	2 bytes	2 bytes

B. Assumptions Made

- Trusted Authority (TA) stores a table of all the real ids and their corresponding secret passwords.
- The task of traceability is distributed to the Traffic Management Server (TMS) distributed across various zones.
- On dispute, the message is forwarded to the TA to find the real id.
- The TPD of all the vehicles are preloaded with the system parameters {G, p, q, Tpub, d,m}
- The pseudo IDs are generated by the vehicle on trip based on some public parameters, the location information and the master secret stored in the TPD.

C. Method

Let m be the master secret of the TA. The TA generates the secret password for driver authentication as follows and issues it to the driver to keep it secret. Let d be the secret password and is computed as,

$$d = m * Rid \tag{1}$$

The public key of the trusted authority is computed as

$$Tpub = m * p \tag{2}$$

Once when the authentication of the driver is confirmed, the pseudo ids are generated by the On Board Unit (OBU) of the vehicle on trip based on the location.

The pseudo id is computed as follows,

$$e = f\,(q*d,\ Tpub\ ,H(x,y)) \tag{3}$$

Where m is the master secret, d is the secret password, Tpub is the public key of the TA, x and y are the GPS coordinates. Finally the pseudo ID is,

$$Pid = d \oplus e \tag{4}$$

The pseudo ID generated is used in the safety messages for reporting the event.

Performance Analysis

A. Security Analysis

Conditional Traceability

The vehicles in the network should be traceable on condition (i.e.) in case of any dispute. Our system supports conditional traceability of vehicles by the TA. Given a pseudo ID Pid , the TA computes the function by using the public parameters q, Tpub , the secret password d and the location as,

$$n = f\,(q*d,\ Tpub\ ,H(x,y)) \qquad (5)$$

This computed value when XORed with the obtained pseudo ID returns the secret password issued to the vehicle user as,

$$n \oplus Pid = d \qquad (6)$$

The TA matches the ‘d’ value with the real ID stored in its database and forwards it to the TMS to take necessary action.

B. Privacy Analysis

Uncertainity

Let, ‘N’ be the total number of vehicles registered with the TA. It is shown in table 3, analysis is done for various categories of ‘N’ number of vehicles. Our analysis has restricted the total count of the vehicles registered to 65536 which requires a maximum of 16 bits (2 bytes) to represent the pseudo ID. Lower values of bits are negligible due to the smaller count of the registered vehicles. In our system, we have employed 16 bits to represent the pseudo ID.

Table IIII: Number of bits required to represent ‘N’ vehicles.

Total No. of Vehicles Registered: N	2	8	16	32	128	512	8192	32768	65536
No. of bits required : b	1	3	4	5	7	9	13	15	16

Let k be an event occurred near the RSU r. Let n be the number of vehicles that arrives near the event occurred in ‘r’ at time T= t. Let us assume that an adversary is stationary near ‘r’ monitoring the vehicles that arrive. The arrival rate of the vehicles near ‘r’ can be represented by a poisson distribution as,

$$P\ [X] = \ e^{-\lambda t}\,\frac{(\lambda t)^n}{n!} \qquad (7)$$

The expected number of vehicles that arrives in ’r’ is given by,

$$E\ [X] = \ \sum_{n=1}^{\infty} n\ P\ [X]$$

$$= \lambda t \qquad (8)$$

So, the number of messages captured by the adversary is λt, and hence the anonymity set size is λt. When an adversary obtains a pseudo ID, he/she should be uncertain about the real ID. The level of privacy provided by the system can be measured by a measure of uncertainty called entropy. This measure quantifies the expected value of the information contained in a message usually in units such as bits.

The entropy can be computed as follows,

$$\zeta = - \sum P\ (xi)\ \log b\ P(xi) \qquad (9)$$

Where P(xi) = 1/n

Here, ‘n’ represents the number of vehicles reporting the event. And, P(xi) represents the probability that one vehicle is selected for tracking. When, ζ is close to zero it means the system provides no privacy. When the value of ζ is close to maximum, it means the system provides better privacy.

Figure 2 shows the entropy measure for various N values. Since, we have employed 16 bits to represent the pseudo ID, the entropy obtained is 16 bits for ‘n’ number of vehicles.

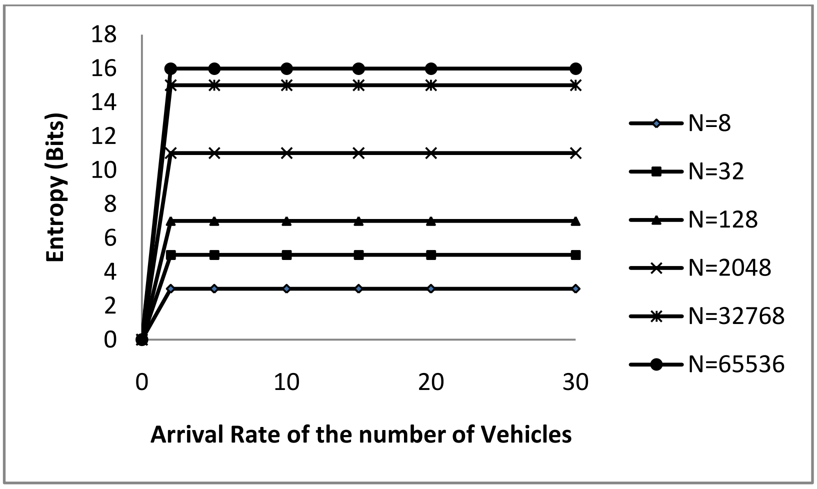

Fig. 2. Entropy measure based on the number of vehicles reporting the event.

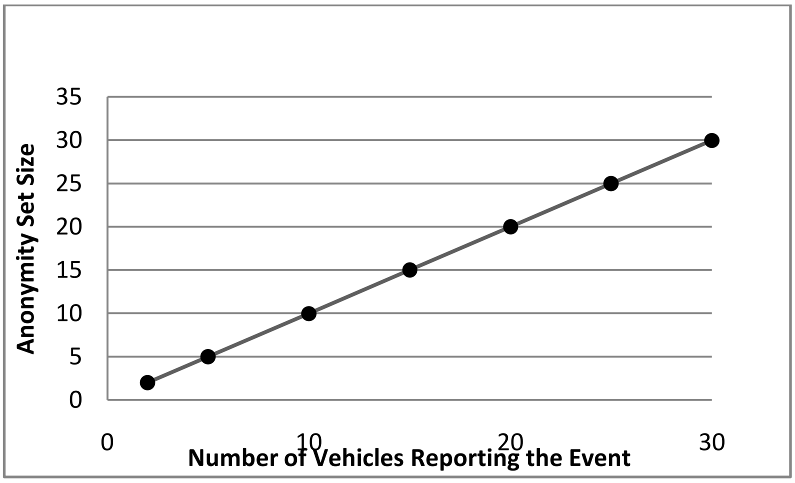

Fig. 3. Anonymity Set Size.

Unlinkability

Messages send from a particular vehicle should be unlinkable with each other so that it becomes difficult for the adversary to trace the ID of the vehicle. This feature of unlinkability should exist for messages communicated within a short period or a long period.

Assume, m1, m2,….mn be the set of messages send from a vehicle V. Message unlinkability can be expressed as the probability that an adversary can use the ID of the messages received to successfully determine whether a message captured in time t1, m(t1) and which is captured in time t2, m(t2) is send from the same vehicle. Let, m(t1) <-> m(t2) denotes that these two messages originated from the same vehicle.

Message unlinkability can be expressed as,

$$U= 1 - Pr(m(t1) \leftrightarrow m(t2)) \qquad (10)$$

The long term unlinkability for time threshold t can be expressed as,

$$U(t) = 1- Pr(m(t1) \leftrightarrow m(t2) \mid t2-t1 >= t \qquad (11)$$

Conclusion

In this paper, a novel method for generating pseudo IDs is introduced and investigated. The main advantage of our approach is the dynamic generation of pseudo IDs on trip based on the location when an event is reported. This scheme avoids the storage of multiple pseudo IDs in the Tamper Proof Device (TPD) there by reducing the size of it. Generation of pseudo IDs shows that it is unlinkable to the real ID and unlinkable with each other. Performance of the approach was analysed for its measure of privacy. The analysis showed that this method gives better privacy, unlinkability between the messages send and is conditionally traceable. In future, we will extend the usage of pseudo ID along with ID based signatures to design a better privacy preserving authentication protocol.

References

1. Subir Biswas and Jelena Misic, " A cross layer approach to privacy preserving authentication in WAVE enabled VANETs", IEEE Transactions on Vehicular Technology, Vol. 62, No. 5, June 2013.
2. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.
3. Y. Bevish Jinila , K. Komathy ," A privacy preserving authentication framework for safety messages in vanet", 4th International Conference on Sustainable Energy and Intelligent System (SEISCON 2013), December 12-14, 2013, pp. 456-461, IET.
4. Y. Bevish Jinila, K. Komathy, "Rough Set Based Fuzzy Scheme for Clustering and Cluster Head Selection in VANET", ELEKTRONIKA IR ELEKTROTECHNIKA, Vol.21, No.1, pp.54-59, ISSN : 1392-1215,2015.
5. Y. Bevish Jinila, "Anonymization based location privacy preservation in Vehicular ad hoc networks", Vol.8, No.1-4, pp.109-114, ISSN: 1313-6569,2015.

6. Rongxing Lu et. al., “Pseudonym changing at social spots: An effective strategy for location privacy in VANETs”, IEEE Transactions on Vehicular Technology, Vol. 61, No.1, Jan 2012.
7. Buttyan. L, Lolczer, Whyte.W, “SLOW: A practical pseudonym changing scheme for location privacy in VANETs”, International conference in vehicular networking, IEEE 2009.
8. Julien et. al, “Mix zones for location privacy in vehicular networks”, WIN – ITS 2007.