DISTRIBUTED AND SECURED DYNAMIC PSEUDO ID GENERATION FOR PRIVACY PRESERVATION IN VEHICULAR AD HOC NETWORKS

[1]Y. BEVISH JINILA,[2]K. KOMATHY

[1]Sathyabama University, Faculty of Computing, Research Scholar, Chennai, India

[2]Hindustan University, Department of CSE, Chennai, India

E-mail: [1]bevish.jinila@gmail.com, [2]gomes1960@gmail.com

ABSTRACT

Safety applications in Vehicular Ad hoc Networks (VANET) needs to be handled with at most care such that no adversary will be allowed to intrude the privacy of the user. Replacement of original IDs with pseudo IDs makes this possible. Generating and storing a set a pseudo IDs by the trusted authority in the tamper proof device of each vehicle and changing them at fixed intervals paves way for an adversary to trace the original ID of the vehicle. And, the space required for storing all the generated pseudo IDs in the tamper proof device of each vehicle is huge. In this paper, we propose a novel approach where pseudo IDs are generated dynamically based on the location information when an event is to be reported and verified by the distributed Traffic Management System (TMS). If a safety message send by a vehicle is detected to be malicious by the TMS, the safety message is forwarded to the Trusted Authority (TA) to map the original ID for the corresponding pseudo ID. The mapped original ID is forwarded to the TMS to take necessary action. Since pseudo ID generation is based on the password provided for driver authentication, in addition a distributed password preservation method is introduced, which preserves the password even when a TA is compromised. Experimental analysis shows that this scheme provides better privacy and conditional traceability compared to existing approaches.

Keywords: *Pseudo ID, Privacy, Trusted Authority, Password, Vehicular Ad hoc Network*

1. 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) [1]. 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 respective receivers. During this process, there is a chance where an adversary can reveal the ID of the source vehicle after receiving the messages. This paves a way for the adversary to trace a particular user on his/her travel or misuse of his/her ID there by invading their privacy. So, it is required to preserve the privacy of the user involved in the communication. To achieve this, the source id of the vehicle should be replaced by some suitable pseudo ID and needs to be changed frequently.

During the time of vehicle registration with the TA it generates and stores a collection of pseudo IDs in the Tamper Proof Device (TPD) of each vehicle's OBU so that the pseudo IDs can be changed at fixed intervals or in fixed locations. Storing a huge collection of pseudo IDs in the TPD occupies more storage space and changing the stored pseudo IDs at fixed intervals or in fixed locations makes an adversary's job of tracing an original ID easier. This invades the privacy of the vehicle user.

This paper addresses the dynamic pseudo ID generation based on the location information of the vehicle when an event is to be reported. In addition to TA and RSU, this scheme involves Traffic Management System (TMS) deployed across various zones which is responsible for the verification of the events occurred in the network. It is also responsible for taking necessary action when an event is reported and when a malicious event is detected. This scheme overcomes the problem of storing multiple pseudo IDs in the Tamper Proof Device (TPD) of each vehicle by dynamically generating the pseudo IDs when required. Also, when an event reported by a vehicle is detected to be malicious by the TMS, it is forwarded to the TA to map the original ID for the relevant pseudo ID and after receiving the original ID of the corresponding malicious vehicle, the TMS takes necessary action. In addition, since this proposed dynamic pseudo ID generation is based on the password provided to the user for driver authentication, a distributed password preservation scheme is introduced which enhances the security of the proposed scheme. Figure 1 shows the network model used by the proposed scheme.

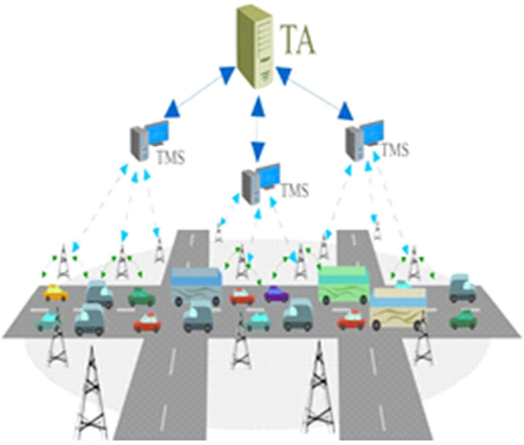

Figure 1: Network Model

The rest of the paper is organized as follows. Section II presents the related work. Section III describes the system architecture, assumptions made and the methodology employed in the proposed scheme. Section IV details the study and analysis of security and privacy provided by the proposed system. Section V concludes the proposed work and provides future directions.

2. RELATED WORK

Several researchers have contributed in the area of privacy preserving authentication. A detailed study on privacy preserving authentication is presented in [2] and a framework is proposed. Based on the framework proposed in [2], pseudo ID generation is considered for this work. Subir Biswas et. al. [3] 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 does not provide any solution for conditional traceability.

Zhang *et. al*. [4] uses an approach where original ID is used to generate the pseudo IDs. This scheme heavily relies upon the TPD 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. Kyung-Ah-Shim [5] has inducted the scheme of Zhang *et. al*. [4] and has included the lifetime for pseudo IDs. Based on the lifetime, the pseudo IDs are changed. This scheme is also proved to be conditionally traceable. The above schemes [3,4] heavily rely on the TPD to store all the generated pseudo IDs and these pseudo IDs are alive for a lifetime. Both [3,4] does not provide any solution for efficiently changing the pseudo IDs such that it becomes difficult for the adversary to trace the original ID of the vehicle.

Deciding where and when the pseudo IDs should be changed is a big task. The recent works [8,9] has proposed ways of changing pseudo IDs at fixed intervals or locations. Julien et al. [8] 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. Rongxing et. al [7] suggests that changing pseudo IDs at fixed intervals makes the adversary to trace the original ID of the vehicle and has proposed a more similar approach where the pseudo IDs are changed in social spots like traffic signals and parking lots where the quantity of vehicles arriving in such spots is quite high.

Gerlach *et.al* [9] considered the number of nodes in its proximity as a criteria to define the mix zones. When the neighbouring vehicles of a particular source have similar direction then such places are considered to be mix zones where the pseudo IDs are changed. These mix zones are said to be context mix zones. However, how the vehicles in the neighbourhood are detected and how the nearby vehicles are guaranteed to similarly react is not included in the paper. In addition to the criteria in [9], Stubbing [10] has considered the adversary's tracking capabilities as a measure for defining an appropriate time when a pseudo ID can be changed. Buttyan [11] proposed a scheme where the vehicles are allowed to change the pseudo IDs when the speed of the vehicle drops below 30 km/hr. This period is known as silent period where the vehicle does not transmit safety messages and just changes the pseudo ID. But, the occurrence of an emergency event in the silent period when not reported immediately may cause a serious issue.

Authors in [15, 16, 17] enforce group signatures to incorporate privacy in vehicular network communication. The limitation with this approach is that the member is anonymizable within a group but, a group leader can trace it.

To summarize, all the issues from existing works indicate that, 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 frantic and even an adversary can trace the ID of the vehicle when it is changed. To overcome the limitations of all the previous approaches, dynamically the pseudo IDs are generated based on the location information of the vehicle when an event is to be reported. This scheme overcomes the limitation of storing multiple pseudo IDs in the TPD. The TMS in our proposed scheme does the task of taking appropriate action when an event is reported and identifies the vehicle that reports the malicious event and forwards it to the TA to map the original ID of the corresponding vehicle and takes necessary action.

3. SYSTEM MODEL

This section, discusses the proposed method of distributed and secured dynamic pseudo ID generation scheme based on the location information.

Table 1: Notations Used

Notations	Description
TA	Trusted Authority
TMS	Traffic Management System
TPD	Tamper Proof Device
G	Cyclic Group
P	Generator of the cyclic group G
q	Prime order
T_{Pub}	Public key of TA
m	Master secret of TA
d	Password assigned for driver authentication
Q	Hashed password
R_{ID}	Original ID of the vehicle
P_{ID}	Pseudo ID of the vehicle
H( )	Hash function – SHA 1
f( )	A function

In this scheme, in addition to TA and RSUs the TMS is included and is distributed across three different zones namely north, south and central. The 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.

3.1 Assumptions Made

- The task of traceability is distributed to the Traffic Management Server (TMS) distributed across various zones (North, South, and Central).
- During registration, the TA generates passwords for driver authentication and issues it to the vehicle user.
- The generated passwords are splitted and stored in various zones.
- Trusted Authority (TA) stores a database of all the original IDs (R_{ID}) and their corresponding generalized range for the splitted passwords.
- On dispute, The TMS forwards the malicious events send by a vehicle to the TA.
- The method for detection of malicious events by TMS is out of the scope of this paper.
- The TPD of all the vehicles are preloaded with the system parameters $\{G, p, q, T_{pub}, d, m\}$.
- The pseudo IDs are generated by the vehicle, when an event is to be reported based on some public parameters, the location information and the master secret and the password stored in the TPD.

3.2 System Architecture

The system is equipped with a TA who is responsible for vehicle registration, password generation, stores the generated passwords and their corresponding original IDs. In addition, the TMS is 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 original ID of the vehicle involved. In addition, the user of each vehicle registered in the network, will be issued with a 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.

Table 2 shows the format of the unsigned safety message with 16 bits assigned for pseudo ID.

Table 2: Format of an Unsigned Safety Message

Type ID	Pseudo ID	Location & Time	Speed	Event ID
2 bytes	2 bytes	10 bytes	4 bytes	2bytes

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 original ID of the vehicle. Knowing the ID, the TMS takes the responsibility for endowing appropriate action on the vehicle involved in the dispute. Figure 2 shows the system architecture of the proposed scheme.

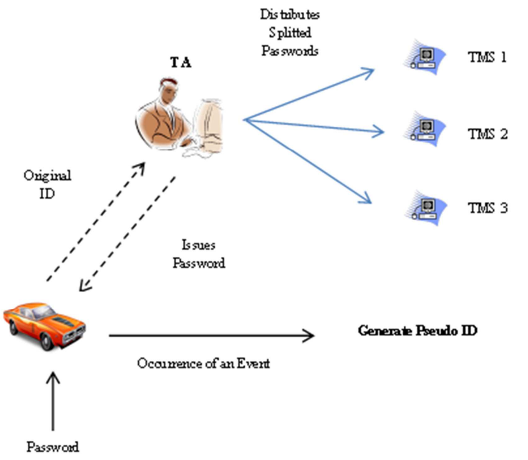

Figure 2: System Architecture of the Proposed Scheme

From figure 2, it is evident that once when a vehicle registers with the TA, it generates and issues password for driver authentication to the vehicle user, loads all the system parameters in the vehicles OBU and generates splitted passwords for the corresponding password and distributes to the TMS located in various zones. On trip, on occurrence of an event dynamically pseudo IDs are generated.

3.3 Methodology

This section focusses on the proposed schemes for distributed and secured dynamic pseudo ID generation. Since the pseudo ID generation is based on the password provided for authentication, in addition a distributed password preservation scheme is introduced which further enhances the security of the proposed scheme.

During the time of vehicle registration, the TPD of each vehicle is loaded with the public parameters, the master secret and the password given to the user for authentication.

3.3.1 Password generation and computation of system parameters

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 password and is computed as given in equation (1). The public key of the trusted authority is computed as given in equation (2).

$$d = m * R_{ID} \qquad (1)$$

$$T_{Pub} = m * P \qquad (2)$$

The master secret 'm' is hashed and stored in the TPD as shown in equation (3).

$$Q = H(m) \qquad (3)$$

The values obtained from equation (1) (2) and (3) along with parameters P and q are loaded in the TPD of the OBU.

3.3.2 Generation of splitted passwords

In this proposed scheme, instead of storing the passwords in the TA, splitted passwords are generated by adopting Shamir's secret sharing scheme [12] and distributed to the TMS located in various zones. The pseudo code of a simple algorithm for generation of splitted passwords is listed in Algorithm 1.

Algorithm 1: Pseudo code for generation of splitted passwords

```
Initialize
        A = password;
        K = No. of Splits;
for $i \in \{1,2,....K-1\}$ do
    $r(i)$ = rand ($i$);
end for
    for $j \in \{1,2,....K\}$ do
        $x(j)$ =rand($j$);
        for $i \in \{1,2,....K-1\}$ do
         $y(j) = A + r(i) * x(j) + r(i+1) * x(j)$;
        end for
    end for
for $j \in \{1,2,....K\}$ do
    for $t \in \{1,2,....K\}$ do
    $t(i) = y(j)$
    end for
end for
```

3.3.3 Dynamic pseudo ID generation

Once when the authentication of the driver is confirmed, the pseudo IDs are generated by the On Board Unit (OBU) of the vehicle dynamically based on the location when an event is to be reported. The pseudo code of a simple algorithm for dynamic pseudo ID generation is listed in Algorithm 2.

Algorithm 2: Pseudo code for dynamic pseudo ID generation

```
Initialize
        Event = NULL
for t  {1,2,…..n} do
    if Event ! = NULL then
        $l_1 = x$;
        $l_2 = y$;
        $k = H(l_1, l_2)$;
        $s = f(Q, T_{pub}, k)$;
        $P_{ID} = d \oplus s$;
    end if
end for
```

Whenever an event occurs the location is retrieved and hashed and a function is computed and the value obtained is XORed with the password to generate the pseudo ID.

4. PERFORMANCE ANALYSIS

The analysis of the level of security and privacy provided by this proposed system is required to show how the adversary is uncertain about the original ID of the vehicle, how two pseudo IDs generated from an original ID is unlinkable with each other and how the original ID of a malicious vehicle is traceable. This section, presents the security and privacy analysis of the proposed system. The performance of pseudo ID generation is tested under Pentium IV, 2 GHz and Windows 7 system on java platform.

4.1 Security Analysis of Pseudo ID

Even though, pseudo IDs are dynamically generated by the OBU of the vehicle itself, it is mandatory to trace the original ID of the vehicle when required so that the entire network can be secured from adversaries. This traceability of the original ID of the vehicle should be on condition and it should be done by the TA. This proposed system, supports the conditional traceability of the vehicles.

4.1.1 Conditional traceability

When a vehicle is identified as malicious, it is required to trace its original ID for taking necessary action. Once when a malicious event is identified by the TMS, it is forwarded to the TA for tracing the original ID. This is known as conditional traceability. Our system supports conditional traceability of a malicious vehicle by the TA. Given a pseudo ID, the TA computes the function by using the public parameters q, T , the secret password 'd' and the location as shown in equation (4). The equation (5) shows that, the computed value when XORed with the obtained pseudo ID returns the password issued to the vehicle user. After reconstructing the splitted passwords, this password is used to map the original ID from the database and the retrieved ID is send to TMS to take necessary action.

$$n = f(Q, T_{pub}, H(x,y)) \tag{4}$$

$$d = n \oplus P_{ID} \tag{5}$$

4.2 Privacy Analysis of Pseudo ID

The important factors used to measure the level of privacy provided include uncertainty and unlinkability. To measure these factors, in this system quantitative measure like anonymity set size, entropy and Pearson's correlation coefficient are used.

4.2.1 Uncertainty

When an adversary captures the pseudo ID of a vehicle or multiple vehicles, the amount of vagueness or randomness in the number of bits of the pseudo ID shows how much the ID is uncertain. This shows the level of privacy provided by the system.

Let, 'N' be the total number of vehicles registered with the TA. As shown in Table III, analysis is done for various 'N' number of vehicles. Our analysis restricted the total count of the vehicles registered to 2^{64}. Lower values of bits are negligible due to the smaller count of the registered vehicles.

The level of privacy provided by the system can be measured by a measure of uncertainty called entropy. Serjantov *et. al* [6] proposed the use of entropy to measure uncertainty. This measure quantifies the expected value of the information contained in a received pseudo ID usually in units such as bits. The entropy can be computed as shown in equation (6).

$$\zeta = - P(x_i) \log_b P(x_i) \tag{6}$$

where P (x_i) = 1/n. Here, 'n' represents the number of bits in the pseudo ID. And, P(x_i) represents the probability that pseudo ID of 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.

The proposed scheme of dynamic pseudo ID generation is compared with the static pseudo ID generation in [5]. According to the authors in [5], the pseudo IDs are generated statically during registration and loaded in the OBU so that the ID can be changed on frequent intervals. Figure 3 shows the comparative analysis of the dynamic and static pseudo IDs.

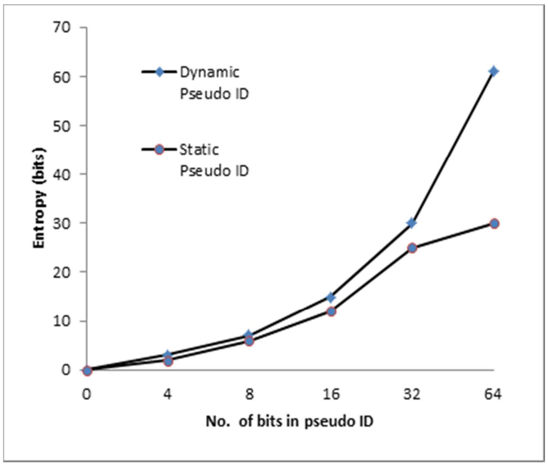

Figure 3: Entropy of the generated Pseudo IDs

For analysis, the number of bits in the pseudo ID is varied for different values from 4 to 64. From figure 3 it is evident that in the dynamic pseudo IDs, when the number of bits in the pseudo ID increases, the level of uncertainty also increases. When 64 bits are used to represent the pseudo ID, the adversary is uncertain of approximately 62 bits. This shows that, when the number of vehicles registered in the network increases, the number of bits used to represent the pseudo ID also increases and the level of uncertainty increases exponentially thereby making the adversary to be more uncertain on the received pseudo ID. However in the case of static pseudo IDs, when the number of bits in the pseudo IDs is increased, the uncertainty level remains stable.

4.2.2 Unlinkability

Making an adversary impossible to map two or more pseudo IDs received from the same vehicle to its original ID or a pseudo ID to its corresponding original ID is known as unlinkability. This feature of unlinkability should exist for pseudo IDs received within a short period or a long period. In this system, the IDs are represented using alphanumeric codes. For analysis, the ascii values of the corresponding alphanumeric codes is calculated and are represented using numeric values.

Case 1 :

Let r1,r2,….rn be the original IDs and p1,p2,…pn be their corresponding pseudo IDs. In this case, unlinkability can be expressed as the probability that an adversary can use the received pseudo IDs to successfully map their corresponding original IDs. Both these cases can be analysed with the Pearson's correlation coefficient.

Case 2 :

Let p1,p2 be the two pseudo IDs received from the same vehicle. In this case, unlinkability can be expressed as the probability that an adversary can use the received IDs to successfully determine whether an ID captured in time t1, and which is captured in time t2 is send from the same vehicle. Let, p1(t1) <-> p2(t2) denotes that these two messages originated from the same vehicle. The short period message unlinkability is expressed as given in equation (7) and long period unlinkability for a time threshold 't' is expressed as given in equation (8).

$$U(t)=1-Pr(p_1(t_1) <-> p_2(t_2)) \quad (7)$$

$$U(t)=1-Pr\ (p_1(t1) <-> p_2(t2))|\ t_2-t_1 \geq t \quad (8)$$

Pearson's Correlation Coefficient

Let R be a random variable that denotes the set of original IDs of vehicles $\{r_1, r_2, \dots. r_n\}$. Let P be another random variable that denotes the set of pseudo IDs generated for the corresponding original IDs. The correlation between these two random variables can be measured by the Pearson's correlation coefficient represented as shown in equation (9).

$$r = \frac{n\sum SP - \sum S \sum P}{\sqrt{n\sum S^2 - (\sum S)^2)(n\sum P^2 - (\sum P)^2)}} \quad (10)$$

When the value of r is close to zero, it means that the dispersion is more and the variables are uncorrelated. For our analysis, we have taken a sample set of data shown in Table 3.

For the given sample values, the correlation coefficient 'r' is 0.05 which is closer to zero. This ensures that the adversary finds it difficult to trace the original ID knowing its pseudo ID.

Let r_1 be the original ID of a vehicle and p_1, p_2,… be the corresponding pseudo IDs. Equation

(10) is used to show that the pseudo IDs are unlinkable with each other.

Table 3: Sample Data of Original and Pseudo IDs

Original ID	Pseudo ID
10	57
12	65
15	62
17	79
20	112

Table 4 shows the sample values of an original ID and their corresponding pseudo IDs.

Table 4: Sample Data of a set of Pseudo IDs for a single Original ID

R	P
20	61
	73
	87

The correlation between the pseudo IDs generated for a single original ID as shown in Table 4 is measured. The correlation coefficient 'r' is zero which shows that the pseudo IDs are unlinkable with each other. This shows that when an adversary captures two pseudo IDs generated from a single original ID, it becomes difficult for an adversary to link both pseudo IDs to map a original ID.

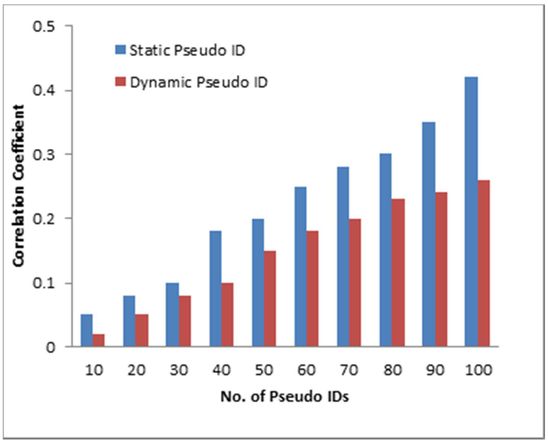

Figure 4: Correlation coefficient of the generated Pseudo IDs

For analysis, the number of pseudo IDs are varied 10 to 100 and the correlation coefficient is fixed to a probability value of 0 to 1. From figure 4 it is evident that the correlation coefficient for the dynamically generated pseudo IDs is comparatively less when compared to static pseudo IDs. As an average there is 10% difference in the correlation factor for dynamic and static pseudo IDs.

4.3 Security Analysis of the splitted passwords

Table 5 shows the sample original data set taken for evaluation. Initially, the data set is clustered based on the region of the vehicle owners.

From Table 5, it is evident that the sensitive attribute is the password. According to the proposed algorithm for splitted password generation, the password is splitted into k parts. Since it is assumed that the TMS is distributed in three different zones, we assume k=3 and we split the password into 3 parts and distribute each part to each TMS.

Table 5: Vehicle Owners Data Set

Name	ResNo.	Zip Code	Dob	Gender	Veh No.	Password
Anto	21	600020	03/04/1980	M	1340	1234
Eve	45	600119	12/26/1978	F	4567	3421
Ben	29	600101	09/09/1971	M	4456	5678
Jenn	49	600100	11/30/1979	M	4495	3232
Quin	35	600035	07/03/1965	F	6623	7891

Table 6 shows the sample of splitted password for the original ones. These splitted passwords are distributed to the TMS located in different zones.

Table 6: Splitted Passwords

Name	Password	P1	P2	P3
Anto	1234	1340	2410	3160
Eve	3421	3527	4597	5347
Ben	5678	5784	6854	7604
Jenn	3232	3338	4408	5158
Quin	7891	7997	9067	9817

In case of any dispute, the authority should be able to know the original password for mapping to the vehicle owner. The curve fitting method is applied and the original passwords are constructed from the splitted passwords.

4.3.1 Correlation

The level by which the sensitive attribute is preserved shows the level of security provided to the data set. For analysis, the Pearson correlation coefficient is used to measure the correlation between the original secret password and the preserved password.

Let S be a random variable that denotes the set of original secret passwords s_1, s_2,…s_n. Let P be a random variable that denotes the corresponding preserved passwords p_1,p_2,…p_n generated for the secret passwords. The correlation between these two random variables can be measured by the Pearson's correlation coefficient shown in equation (9).

The correlation between the two variables can be determined by the 'r' value. If 'r' value is closer to zero, it shows that there is less correlation and the correlation is positive maximum when the value is closer to +1 and negative maximum when the value is closer to -1.

The Pearson correlation coefficient is calculated for the sample values showed in Table 6. From the analysis, it is known that the 'r' value is -0.33 which is closer to zero and there is less correlation between the original password and the splitted passwords.

4.3.2 Splitted password reconstruction

The splitted passwords are distributed to the TMS located in different zones. For conditional traceability, the distributed password has to be reconstructed by the TA to trace the original ID of the vehicle. Since the password has been converted into a polynomial equation of a parabola, using the normal equations of parabola, the values of 0th,1st and 2nd derivative can be obtained and this gives the equation of a parabola by which the password can be obtained.

In this proposed scheme it is assumed, instead of storing the original passwords the TA applies the concept of anonymization [13] and stores the generalized value across each R_{ID}.

In this scheme, the curve fitting method [14] is adopted for reconstruction. The equations (10) (11) and (12) show the method for reconstruction of the sensitive attribute password. For the given data, $(x_1,y_1),(x_2,y_2),\ldots\ldots\ldots(x_n,y_n)$ can be fit to a parabola by solving the normal equations by the principle of least squares method.

$$y=na+bx+cx^2 \tag{10}$$

$$xy=ax+bx^2+cx^3 \tag{11}$$

$$x^2y=ax^2+bx^3+cx^4 \tag{12}$$

Solving equations (10),(11) and (12) the original password can be retrieved. It can matched with the computed password and the corresponding original ID of the vehicle can be retrieved.

5. CONCLUSION

In this paper, a novel method of distributed and secured dynamic pseudo ID generation is introduced and investigated. The main advantage of this proposed approach is the dynamic generation of pseudo IDs based on the location information, when an event is reported. This scheme avoids the storage of multiple pseudo IDs in the TPD there by reducing the size of it. Generation of pseudo IDs shows that it is unlinkable to the original 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 pseudo IDs and is conditionally traceable. In addition, the distributed password preservation scheme shows the security of the password issued. In future, this dynamic generation of pseudo ID will be combined with ID based signatures to design a better privacy preserving authentication protocol.

REFERENCES

[1] X. Lin,R. Lu, C. Zhang, H. Zhu, P. H. Ho and X. Shen, " Security in Vehicular Ad hoc Networks", *IEEE Communication Magazine.,* Vol. 46, No.4, pp. 88-95, Apr 2008.

[2] Y. Bevish Jinila, K. Komathy, " A privacy preserving authentication framework for safety messages in VANET", *Proceedings of IET Chennai 4th International conference on Sustainable Energy and intelligent System (SEISCON 2013)*, Dec 12-14, 2013.

[3] 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.

[4] C. Zhang, Rongxing Lu, Xiadong, Pin-Han, and Shen., " An efficient identity based batch verification scheme for vehicular sensor networks", *IEEE INFOCOM* 2008.

[5] Kyung-Ah Shim, "CPAS: An efficient conditional privacy preserving authentication scheme for vehicular sensor networks", *IEEE Transactions of Vehicular Technology*, Vol. 61, No. 4, May 2012.

[6] A. Serjantov et. al., "Towards an information theoretic metric for anonymity,", LNCS *2482*, pp 41-53, 2002.

[7] 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.

[8] Julien et. al, "Mix zones for location privacy in vehicular networks",*WIN – ITS* 2007.

[9] M. Gerlach and F. Guttler, " Privacy in VANETs using changing pseudonyms – Ideal and Original", in *Proceedings of the 65th IEEE Vehicular Technology Conference* VTC2007-Spring, April 2007, pp. 2521-2525.

[10] H. Stubing, " Multilayered security and privacy protection in car-to-X networks", *Springer* 2013.

[11] Buttyan. L, Lolczer, Whyte.W, "SLOW : A practical pseudonym changing scheme for location privacy in VANETs", *International conference in vehicular networking*, IEEE 2009.

[12] Dan Bogdanov, "Foundations and properties of Shamir's Secret Sharing Scheme", *Research seminar in cryptography*, University of Tartu, May 2007.

[13] Acar Tamersoy, Grigorios Loukides, Mehmet, Yucel, Bradley, "Anonymization of Longitudinal Electronic Medical Records", *IEEE Transactions on Information Technology* in Biomedicine, Vol. 16, No. 3, May 2012.

[14] Gurley, " Curve Fitting Techniques", CGN 3421- Computer Methods

[15] Yi Pin Liao, Chih-Ming Hsiao, "A novel multi server remote user authentication scheme using self-certified public keys for mobile clients", *Journal of future generation computer systems*, Apr 2012.

[16] T.W. Chim, S.M . Yiu, Lucas C.K. Hui and Victor O.K. Li, "SPECS: Secure and privacy enhancing communication schemes for VANETs", *Journal of Ad hoc Networks*, June 2010.

[17] Lei Zhang, Qianhong Wu, Agusti Solanas, Josep, " A Scalable Robust Authentication Protocol for Secure Vehicular Communications", *IEEE Transactions on Vehicular Technology*, volume 59, No. 4, May 2010.