An effective entropy based pseudonym management system for vehicular Ad hoc networks

T. Sivakumar¹, A.S. Nidhin²

¹Assistant Professor, ²Research Scholar, Department of Computer Science, SNGC, Chavadi, Coimbatore-641105, Tamilnadu, India
tsktiruppur@gmail.com¹, nidhiarackal@gmail.com²

Abstract

Objectives: The main objective of method is to optimize the utilization of pseudonym resources and improve the privacy in VANET.

Methods: There are different techniques based on pseudonyms used to improve privacy in VANET. One of such method utilizes minimum spanning tree algorithm and entropy based pseudonym shuffling process to improve the privacy with minimum transmission loss.

Findings: The anonymity through pseudonym techniques in VANET is one of the major responsibilities to degrade the transmission performance. The transmission cost of pseudonym is not considered during pseudonym distribution to Road Side Units (RSU). Therefore, an effective pseudonym management system is required for minimizing transmission cost of pseudonyms and increasing privacy.

Application/Improvements: To overcome transmission cost of pseudonyms, Esau-Williams (EW) algorithm and entropy based pseudonym shuffling process are introduced for anonymity.

Keywords: Vehicular Ad-hoc Network (VANET), Anonymity, Pseudonym Management System, Minimum spanning tree, Esau-Williams (EW) algorithm, Entropy.

1. Introduction

Based on the principles of Mobile Ad-hoc Network (MANET) [1], the Vehicular Ad-hoc Network (VANET) are developed which are spontaneous concern of wireless network for transmitting the information to the vehicle regions. In Intelligent Transportation Systems (ITS), the major component is VANETs. The most important objective of VANET is to increase the security, privacy and transportation efficiency in various applications like tragedy situations, adaptive speed control systems, track maintenance applications and supported braking.

The IEEE standard for VANET is 802.11p which offers the lesser amounts of limitations for MAC and PHY layers to cooperate the wireless services for vehicles [2]. The IEEE standards 1609 families are obtained for providing the limitations to high layers which offers the vehicles multiple channel capabilities to facilitate them for accessing infotainment facilities. These standards are also termed as Wireless Access for Vehicular Networks (WAVE). Specifically, vehicles are having ability to access six service channels (SCH) and control channels (CCH). The security data are forwarded on the CCH and non-security data are forwarded on the SCH by means of vehicles. Vehicles synchronously tune to CCH for 50ms to collect the whole cyclic and event-driven data after then switch to any one of the SCH for another 50ms.

The most important principle of vehicular protection functions is the condition for vehicles to broadcast the data including their locality, velocity and track information. But, the malicious data are agreed to track the persons without difficulty and perhaps blackmail them [3]. As a result, the uses of pseudonyms are established to conceal the vehicles from adversary and increase the privacy. Vehicles are employing these pseudonyms as source address for their beacon signals and make communications with other vehicles. Hence, the data does not bond to the vehicles so the privacy and security of users may remain secluded. Different approaches are developed in pseudonyms to improve the security and privacy in VANET.

In [4] developed pseudonymity to support anonymity in VANET. The several challenges in pseudonymity also its inclusion in vehicular networks were discussed. The various types like cross layer addressing technique, absolute locality facility, pseudonymity-improved packet transmitting methods and link layer call backs were established for finding the pseudonymity solutions.
In [5] investigated pseudonym scheme including with user-controlled anonymity (PUCA) for VANET. This method was developed for obtaining complete anonymity and utilized anonymous qualifications to validate with backend when the communication was leaving among vehicles and unmoved road side units. Here, the user privacy was achieved by cryptographic techniques. However, the computation power was more.

In [6] developed an efficient strategy for generating and changing pseudonym with privacy preservation in VANET. The location security issue in VANET was eliminated by the scheme named as pseudonym changing at proper location (PCP) provided to change the pseudonym. The self-delegated key generation were achieved by utilizing cyclic groups. However, attackers can track the vehicles easily in spatial-temporal method.

In [7] investigated about the probabilistic isolation of malicious vehicles in pseudonym changing. The bloom filters were provided for verifying dishonest and trusted nodes and also regularly transmitted these feedbacks so the receivers update their values. The tamper-proof device and honest majority were considered to carry the secure functions like signing and credit updating. The numerical method was introduced for evaluating the credit of the node itself by means of tamper-proof device. However, the performance was not better than other methods.

In [8] investigated about the changing pseudonyms in VANET for isolation security. The synchronous pseudonym change method was introduced for recovering privacy protection. This method was developed according to the vehicular status information and simultaneously changing pseudonym. The attacks on changing pseudonym were also described. This method was analyzed based on the comparison with position and similar status models. However, the optimization method for changing pseudonyms was required.

In [9] proposed an anonymity analysis based on the capacity finite social spots for pseudonym changing in VANETs. The suitable and authentic approach was introduced for changing pseudonyms at capacity finite social spots to improve the location protection. The location protection was achieved by considering anonymity set size as location protection metric. The privacy quality was computed by numerical method which is based on queuing theory. However, the probability of changing pseudonyms was not optimized.

In [10] developed two level privacy preserving pseudonyms authentication protocol in VANET. The pseudonym authentication protocol was developed including with conditional privacy preservation for improving the protection of VANET. This protocol was required honest-but-curious character from certification power. The mechanism was utilized to offer the user with two levels of pseudonyms for attaining conditional isolation. However, the optimization technique was required for pseudonyms.

In [11] developed location privacy through synchronously pseudonym changing in VANETs. An ID-based cryptosystem mechanism was proposed for achieving vehicles anonymity by means of pseudonyms. The pseudonyms synchronously change method was introduced to increase the anonymity. Furthermore, the simplified game theoretic scheme was adopted for evaluating the feasibility. However, the frequency of pseudonym changing was not optimized.

In [12] proposed protocol for changing pseudonyms in VANETs. The protocol was developed according to the periodic change of pseudonyms. Two different methods were introduced. The major aim of this protocol was to allow at least two vehicles for changing pseudonyms at similar time period. The bandwidth utilized by means of vehicles velocity was evaluated. This protocol was also according to the equidistant distribution of road side units and utilized the average velocity allowed on the road for computing lifetime of the pseudonyms and certificates. However, the bit error rate was not considered.

In [13] proposed an analytical framework for random changing pseudonym in VANET. The random changing pseudonym was described for evaluating the level of position privacy. This random changing pseudonym was compared with the uniform discrete distribution and age-based distribution to know about the effectiveness. The location privacy was provided by random changing pseudonym was improved. However, this method was limited to distributions which are used for pseudonym changing.

2. An effective entropy based pseudonym management system

2.1. System model

In this proposed model, a system of vehicles including an onboard unit (OBU) are considered which are equipped with wireless technology according to the IEEE 802.11p or WAVE standard and facilitating the vehicles for communicating with each other and road side units (RSU). The RSU are also equipped with similar technology having prearranged structure linked to all other and to the backbone network via wired links. OBU utilized IPv6 data services for communication with TA and used for communicating directly with all other, if within the communication area or utilize multiple hop transmission.
Let consider the existence of routing protocol and existence of Trusted Authority (TA) since high mobility and repeated disconnections which happens in VANET. The proposed model is considered that the TA is utilized for pseudonym management system [14]. TA is accountable for the generation of pool of pseudonyms which are used by vehicles. Also, the management of the pseudonyms distribution across RSU are controlled by TA.

2.2. Threat model

The treats are also vehicles system which may receive the information about their neighbors and if compromised they may distribute it with an adversary involved in tracking a certain vehicle. Due to the wireless nature of VANET, entire packets are sent by the vehicle are heard by all other nodes within its communication area. This develops other passive attacker composed of eavesdroppers which can control the communications of vehicles and may be interested in tracking the vehicles service channels. The passive adversary does not thwart in the system’s function and does not interrupt, adjust or introduce packets and so it is hardest for detecting. The RSU are also compromised for collaborating with an adversary or among all other for providing the information about the particular vehicle.

2.3. General architecture

In this system, TA is used to generate all offline pseudonyms and to distribute them to the RSU which receives the pool of pseudonyms whose ranges are constant with the level of their weights. Every RSU obtains the accountability of delivering the pseudonyms to vehicles which enter its communication area. Moreover, the RSU endures the shuffling process regularly by means of exchanging group of pseudonyms with all other. Therefore, the reuse of pseudonyms but not by the similar vehicles is facilitated. In addition, a lock or notify mechanism is introduced for avoiding any simultaneous utilization of pseudonyms by different vehicles therefore the uniqueness of the utilization of pseudonyms are ensured.

2.4. Addressing

The vehicles utilize the two addresses such as MAC address and IPv6 address. MAC address is 48-bit address which is used for uniquely identifying the node at the link layer and IPv6 address is 128-bit which is used for communications within the network. Therefore, using one false address on one layer of the protocol stack is not adequate as packets with similar address at another layer can be connected to the similar vehicle.

Cryptographically generated addresses (CGA) are IPv6 addresses which are generated by computing the hash function using public key and extra parameters. The OBU generates a group of pseudonyms combined with suitable certificates. The address generation characteristic of CGA and delegate the generation to the TA are exploited which generates the large amount of certificates and addresses offline from the initial master public key values given to the vehicles. Those addresses are shared to the vehicles via RSU. The CGA utilizes the 128-bit random number and public key for producing the interface identifier which is after combined with a subnet prefix for creating the IPv6 address. While vehicle receives IPv6 pseudonym, it can produce the MAC address by using hash value from SHA-1.

2.5. Pseudonym management

Assume that pseudonym pools which are controlled by Open Flow switches form the network as an undirected graph $G = G(V, E)$. The network of pseudonym pools contains $m$ nodes and $n$ node pairs [15]. The vertex is denoted by $V = \{i, ..., n\}$ and the set of edges are denoted by $E = \{(i, j) : i, j \in V, i \neq j\}$. Each vertex $i \in V \cup \{n\}$ is associated the non-negative weight $q_i$. Every edge $(i, j)$ is associated a cost or length $c_{ij}$. At time $t$, pseudonym pool $P_i$ possesses a certain number of residual pseudonym resources $R_i^t$. Each pseudonym pool generates pseudonyms at constant rate $\theta_i$. The average consuming rate of pseudonym resources of $P_i$ denoted as $\lambda_i^t$ in following time can be estimated from historical records by statistical methods. During time $T$, consider $r_i^T$ denotes the fraction between the number of required resources and the number of actual resources.

$$r(P_i) = \left| R_i^t + \theta_i T - \lambda_i^T \right|$$

(1)

The data packets of pseudonyms are transmitted between two connected pseudonym pools through wired path including low cost. In pseudonym’s data packets transmission, the data packet loss per distance is $l$. Then the weights of edges are computed by means of sum of pseudonym transmission loss between two connected pseudonym pools.

$$Transmissionloss, C = ld$$

(2)
In above equation, \( d \) denotes the distance between two connected pools. The link with minimum transmission loss between two pseudonym pools is computed by using Esau-Williams algorithm. The asymmetric matrix for vertex \( j \) and length of its gate \( g_j \) is given as,

\[
S = (s_{ij}) \text{where} s_{ij} = g_j - c_{ij}
\]  

(2)

The elements of matrix \( S \) such as \( s_{i,j}(i \neq j) \), represents the minimum transmission loss between pseudonym pools \( P_i \text{and} P_j \). Sometimes it may be rewritten as \( s(P_i, P_j) \). Consider set of vehicles, cost matrix \( \text{Cost}(i,j) \) and set of trees \( T_1, \ldots, T_k \) such that each vehicle belongs to each tree.

\[
\sum_{\text{trees}} \sum_{\text{links}} \text{Cost(\text{end}_1,\text{end}_2)} \text{is minimum.}
\]

Depending upon the transmission flow \( \lambda \), the RSU may acquire new group of pseudonyms for providing to vehicles passing through their communication area. To replace the exists group of pseudonyms in RSU, shuffling process is used. At each interval, RSU shuffle their pseudonyms with new pseudonyms and transmit to all other RSU. The objective of each RSU is to increase the percentage of pseudonyms received. This optimization problem can be defined as follows:

\[
\max \sum_{j=1}^{n} x_{ij} / \sum_{i=1}^{n} \sum_{j=1}^{n} x_{ij}
\]  

(3)

Such that

\[
\forall i \sum_{j=1}^{n} x_{ij} \leq N_{Si}
\]  

(4)

\[
\sum_{i=1}^{n} \sum_{j=1}^{n} x_{ij} = \sum_{i=1}^{n} \sum_{j=1}^{n} x_{ij}
\]  

(5)

\[
\forall i,j x_{ij} \geq 0
\]  

(6)

In above equations, (3) is the objective function which is used for increasing the proportion of received pseudonyms relative to the total in the network. (4) Refers the amount of transmitted pseudonyms groups which is less or equivalent to what the RSU has. (5) Denotes the total amount of transmit pseudonyms in the network is equivalent to the total received and (6) is the non-negativity condition.

To ensure location privacy, entropy based privacy preservation is proposed. Consider \( X_i(t) \) be the location of vehicle \( i \) at period \( t \). An adversary is interested to know about \( X_i(t) \) for \( i = 1, 2, \ldots, N \). Assume \( Y \) be the collection of observations available to the adversary. For vehicle \( i \) has accurate location privacy at period \( t \) respecting adversary \( A \), if and only if,

\[
\lim_{N \to \infty} I(X_i(t);Y) = 0
\]  

(7)

In equation (7), \( I(\cdot,\cdot) \) is the mutual information. The level of location privacy is measured as the uncertainty of the information which is related to the particular vehicle. The uncertainty is defined by privacy entropy \( H \).

\[
H_m = \log_2 (|S|)
\]  

(8)

In equation (8), \( |S| \) is denoted as the total amount of serviced vehicles which can be obtained the required pseudonyms. Thus the level of location privacy is improved based on the entropy.
2.6. Algorithm
Effective entropy based pseudonym management system

1. Each vehicle registers with TA and obtains public key, private key, and certificate.
2. Consider number of pseudonym pools to generate pseudonyms
3. Compute the amount of pseudonym resources
4. The pseudonyms are distributed to every RSU based on average transmission flow $\lambda$

//Minimize transmission loss
5. Consider group of vehicles and group of weights for each vehicle
6. Compute transmission loss by using equation (1)
7. Compute asymmetric matrix $S$ and cost matrix
8. Increase the pseudonym received by RSU

//Ensure location privacy
9. Find mutual information
   $$\lim_{N \to \infty} I(X_i(t); Y) = 0$$
10. Compute privacy entropy $H$
    $$H_m = \log_2(|S|)$$
11. Determine the level of location privacy

3. Results and Discussion

This section presents the experimental results that are performed to prove the proposed pseudonym management system achieves higher anonymity. The performance of the proposed effective pseudonym management system is evaluated in terms of degree of anonymity; effective anonymity set size, Pseudonym distribution traffic per RSU for low network activity, medium network activity and high network activity.

3.1. Degree of anonymity

Degree of anonymity is the probability associated with each vehicle by comparing entropy of the network.

$$d = 1 - \frac{H_m - H(X)}{H_m}$$

In above equation, $H(X)$ is the entropy of the entire network and $H_m$ is the maximum entropy of each vehicle in the network.
Figure 1 shows the degree of anonymity for different vehicle arrival rates, where it shows that greater anonymity is achieved in high network activity and with higher vehicle arrival rates. The figure shows that how higher vehicle arrival rates increasingly offset the low communication activity in the network.

### 3.2. Effective anonymity set size

It is defined as the variations in $H(X)$ and $H_M$. It is denoted as,

$$AS = H_M - H(X)$$

Figure 2 shows the effective anonymity set size for different vehicle speeds, where it shows that higher anonymity set is achieved in high network activity and with higher vehicle arrival rates. The figure shows that for a high activity network, the size of the anonymity can reach values up to 15 vehicles which will confuse the most sophisticated of tracking attackers.

### 3.3. Pseudonym distribution traffic per RSU

It is used for determining network overhead and computational cost of the system.

Figure 3 shows the growth of wireless overhead traffic per RSU in response to increasing both the average vehicle speed and wireless transmission range of vehicles. The figure shows that the pseudonym distribution per RSU is increased for high speed vehicles with higher transmission range.
4. Conclusion

This paper presented an efficient pseudonym management system for achieving high anonymity in VANET. The cost of pseudonyms during transmission is minimized by Esau-Williams graph cut clustering algorithm and the anonymity is improved by entropy based pseudonym shuffling process. The experimental results are proved that the proposed pseudonym management system has better anonymity. This performance results show that the ability of the system to maintain sufficiently large anonymity set which is intended to confuse the attacker.

5. References