COALITION FORMATION FOR PSEUDONYM SHARING USING GALE-SHAPLEY ALGORITHM IN VEHICULAR AD HOC

[1]G.Lavanya, [2]P.E.Prem, [3]S.Sinduja

[1]PG Scholar Department of Information Technology, Vivekanandha College of Engineering For Women (Autonomous) Thiruchengodu,India
[2,3]Assistant Professor Department of Information Technology, Vivekanandha College of Engineering For Women (Autonomous) Thiruchengodu,India

[1]glavanya9437@gmail.com [2]premchrprem@gmail.com [2]sindujanaga@gmail.com

Abstract: The primary goal of VANET is to provide road safety measures where information about vehicle's current speed, location coordinates passed with or without the development of infrastructure. This paper proposes an enhancement scheme of Pseudonym management with better privacy scheme. The pseudonym design focus on privacy among network participants. The major limitation of these vehicular ad hoc networks is packet delay. In order to improve the efficiency Gale - Shapley algorithm using vehicular ad hoc networks.

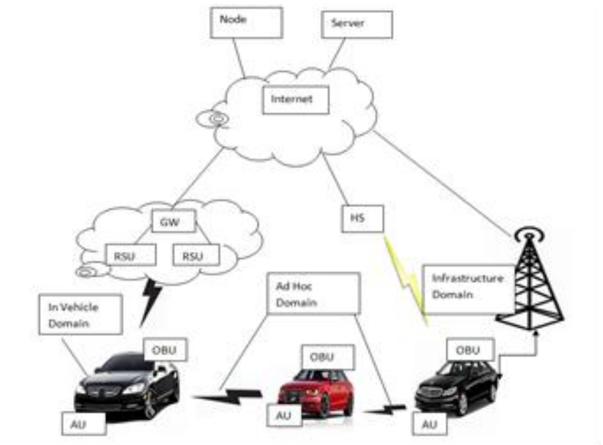
Index Terms: Vehicular Networks, Privacy, Anonymity, VANET, Gale-Shapley Algorithm.

1. INTRODUCTION

Vehicular Ad-Hoc Network is a technology that uses moves cars as nodes in a network to create a mobile network. The major problem regarding the increased use of private transport is the increasing number of losses that occur due to accidents on the roads; the expense and related dangers have been recognized as a serious problem being confronted by modern society. VANET provides a wireless communication between moving vehicles, using a dedicated short range communication (DSRC). DSRC is essentially IEEE 802.11a amended for low overhead operation to 802.11p; the IEEE then standardizes the whole communication stack by the 1609 family of standards referring to wireless access in vehicular environments (WAVE). Vehicle can communicate with other vehicles directly forming vehicle to vehicle communication (V2V) or communicate with fixed equipment next to the road, referred to as road side unit (RSU) forming vehicle to infrastructure communication (V2I). These types of communications allow vehicles to share different kinds of information, for example, safety information for the purpose of accident prevention, post-accident investigation or traffic jams. Other type of information can be disseminated such as traveller related information which is considered as non-safety information. The intention behind distributing and sharing this information is to provide a safety message to warn drivers about expected hazards in order to decrease the number of accidents and save people's lives. In this paper, we present a key document which can provide detailed information to researchers and developer so as to understand the main aspects and challenges related to VANET. It covers different issues such as network architecture, communication domains, challenges, applications and simulation tools.

1.1 VANET ARCHITECTURE

The communication between vehicles or between a vehicle and an RSU is achieved through a wireless medium called WAVE. The biggest problem regarding the increased use of private transport is the increasing number of fatalities that occur due to accidents on the roads; the expense and related dangers have been recognized as a serious problem being confronted by modern society. VANET provides a wireless communication between moving vehicles, using a dedicated short range communication (DSRC). DSRC is essentially IEEE 802.11a amended for low overhead operation to 802.11p; the IEEE then standardizes the whole communication stack by the 1609 family of standards referring to wireless access in vehicular environments (WAVE). Vehicle can communicate with other vehicles directly forming vehicle to vehicle communication (V2V) or communicate with fixed equipment next to the road, referred to as road side unit (RSU) forming vehicle to infrastructure communication (V2I).



This method of communication provides a wide range of information to drivers and travellers and enables safety application to enhance road safety and provides comfortable driving. The main system components are the application unit (AU), OBU and RSU.Typically the RSU hosts application that provides services and the OBU is a peer device that uses the services provided. The application may reside in the RSU or in the OBU.Each vehicle is equipped with an OBU and sensors to collect and process the information then send it on as a message to other vehicles through the wireless medium. The RSU can also connect to the internet or to another server which allows AU's from multiple vehicles to connect to the internet.

1.2 Wireless Technology in Vanet

There are numerous wireless access technologies available today, which can be used to provide the radio interface required by the vehicles in order to communicate with the each other, V2V communication, or to communicate with the RSUs, V2I communication. These communication technologies intended to improve road safety, traffic efficiency and to provide driver and passenger comfort by enabling a set of safety and non-safety applications. Some of these technologies relay on a centralized infrastructure to coordinate the communications between nodes. In this paper, we use the theory from stable matching well known gale-shapely algorithm for cooperation and hence coalition formation.

The remainder of this paper is organized as follows: section II overviews the related work. Section III gives a brief introduction to the system model. Section IV explains the proposed schemes in detail. Section V presents the performance analysis. And section VI covers the conclusion.

2. RELATED WORK

In this framework, the TA generates all pseudonyms offline and distributes them to the RSUs, which receive pools of pseudonyms whose sizes are consistent with the level of their demands. Each RSU takes the responsibility of delivering pseudonyms to cars that enter its transmission range.

In this framework, the TA generates all pseudonyms offline and distributes them to the RSUs, which receive pools of pseudonyms whose sizes are consistent with the level of their demands. Each RSU takes the responsibility of delivering pseudonyms to cars that enter its transmission range.

2.1 Pseudonym Management

In this we describe the distribution process of pseudonyms by both the TA and the RSUs, and then explain the shuffling of pseudonyms among the RSUs, before discussing the handling the periodic beacons and the unlinkabality property.

2.2 Distribution to the RSUs

Initially, each car registers its GID with the TA and gets its public key, private key, certificate, and initial pseudonym. This pseudonym will be used by the car to communicate with the first RSU and request a set of pseudonyms. The TA then sends the public keys of all registered cars to all the RSUs to be used for authenticating the cars.

2.3 Beaconing

Another challenge related to pseudonym changing is the fact that vehicular networks are wireless and vehicles send periodic beacons that include their addresses at the time. In our framework, the vehicle uses a different pseudonym for each ongoing session, meaning that the vehicle might have multiple addresses at the same time. It uses these addresses to receive packets from the ongoing sessions, to send packets to specific destinations and also to forward messages on the routing layer. Therefore, the vehicle has to beacon all the pseudonyms it is currently using. To exploit the simultaneous use of pseudonyms by the same vehicle as an additional dimension to the confusion of the attacker, the vehicle should send beacons for each address at the same time. Since this is physically impossible, it sends all beacons directly after each other. Due to the physical variables that affect a packet's reception, an attacker will not be able to discern if these messages were sent by the same vehicle but at very close times, or sent by another one at exactly the same time.

2.4 Unlikability

Now that the vehicle has a set of pseudonyms for use, it chooses a random one for each communication session with a peer. At the end of the session, the vehicle stops using the pseudonym and deletes it to save resources. This is not an issue since the car uses the SID to communicate with the RSU, hence, it does not need to send actual pseudonyms. In our system, unlinkability is the inability of the attacker to link two messages with different pseudonyms to the same source (i.e., same GID). Making the pseudonym change event unidentifiable avoids linking a pseudonym to a vehicle or linking an old pseudonym to a new one. As was mentioned before, all pseudonym changing algorithms aim at concealing the change by performing synchronous changes where at least two nodes change their pseudonyms at the same time [2]. Others extend the synchronicity algorithms to ensure that the simultaneously changing nodes have similar identifiers (speed, direction and position) as well [3][4]. Enhancing Unlinkability in Vehicular Ad Hoc Networks [10][11] we address the problem of movement tracking and enhance location privacy without affecting security and safety of vehicles. Performance evaluation and comparison showed that the SPCP provides significantly higher level of privacy over REP, AMOEBA and the silent period method.

2.5 System Effectiveness

To evaluate the efficiency of our system, we simulate a scenario using the network simulator ns3 that comprises a 10 km highway, with RSU's placed 500 m apart (consistent with [5] and [6]).We set the car flow rate to 3000 cars/hour and changed the average vehicle speed and transmission range, as they are the main contributors to the size of the anonymity set (see previous section). In the simulations, we choose a random vehicle as a target and calculate the anonymity set to be the number of vehicles that change pseudonyms simultaneously with the tracked vehicle. We divide our results to scenarios where vehicles use only one pseudonym at a time and other scenarios where vehicles are allowed the simultaneous use of multiple pseudonyms for each active session. On the age of pseudonyms in mobile ad hoc networks [8] developed a framework to analytically evaluate the age of pseudonyms. Our framework captures the mobility and interactions between nodes. With this model, we obtained critical conditions for the emergence of location privacy. An analytical model for random changing pseudonyms scheme in vanet [9], they analyze the level of location privacy under two special distributions, uniform discrete and age-based distributions. Mix Zones: User Privacy in Location-aware Services [12] we have refined the mix zone model, describing a quantifiable metric of location privacy from the point of view of the attacker. Analysis is computationally expensive and may require partial estimate of the problem–we have described a method of achieving this. As well, given fixed computational authority there exists a trade-off between the tractability of the problem and the accuracy in which the real world is modeled.

3. SYSTEM MODEL

Let us consider theory from stable matching well known gale-shapely algorithm for cooperation and hence coalition formation. We consider a system of vehicles each having an on board unit (OBU) equipped with wireless technology based on the IEEE 802.11p/WAVE standard, allowing them to communicate with each other and with road-side units (RSUs). The RSUs are equipped with the same technology and are fixed infrastructure connected to each other and to the backbone network through wired connections. OBUs communicate with each other directly, if within transmission range, or use multi-hop communication, where nodes collaborate to forward packets from source to destination. Due to high mobility and frequent disconnections that occur in VANETs, we assume the existence of a routing protocol that enables nodes to build optimal paths between source and destination nodes. We also assume the existence of a trusted authority (TA) that registers OBUs and RSUs by providing them with public and private keys. Each vehicle in the network performs spectrum using energy detection method in order to calculate the false alarm probability and received SNR from the primary user. This information is needed so that the SU users can calculate the utility while proposing to other SU users for forming coalitions. Each vehicle discovers neighbouring vehicles as well as information required to perform matching and eventually coalition formation. SUs need to also learn the probability of false alarm of their neighbours. After discovery phase and recovering all the information needed the users calculate the utility with all other user in the network for possible cooperation. The utility is calculated using the (13) based on the target probability of detection Pd'. The utility calculated from all the users is used to generate preference list PLi, where PLi is the utility of the ith user in the CRN. After the utility with each SU is calculated the SUs arrange the utility in an increasing order in the network, we can proceed to apply the matching algorithm to obtain the stable matching.

For a given network structure, during matching process, each coalition attempts to merge with other coalitions in its vicinity in a pair wise manner. The stable matching algorithm proceeds in several rounds until there is an identity matching where each coalition is matched to itself. The system model consists of different entities: Coalition Formation, Stable matching as illustrated in Fig: 2.

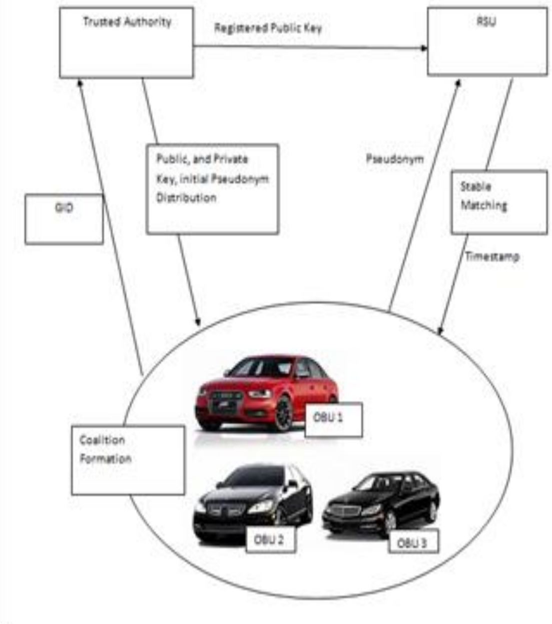


Figure 2: System Model

We consider a scenario where a RSU (licensed user) and there are multiple SUs (Vehicle) in the locality of the RSU. The CRN consists of n Vehicle pairs/links that can be connected in mesh topology. The RSU may operate over one or multiple channels. The RSU in the network is modeled as an ON/OFF source, where "ON" means that the RSU is actively transmitting.

3.1 Threat Model

In our threat model, both the data owner and authorized data users are considered as trusted. But the RSU is considered as "honest-but-curious" (i.e., semi trusted RSU). The RSU may predict and analyse the encrypted documents based on the information provided by the data owners and data users.

3.2 Design Goal

Where SNRi is the SNR between ith Vehicles transmit receive pair. When the Vehicles form a coalition then the coalition cannot transmit data until the local decision is combined at coalition head and the results are transmitted back to the coalition members. The coalition head waits for the local decisions from all the SUs to arrive in order to make final decision. As the number of SU in a coalition increases the final decision will be taken based on the stable match by using gale-Shapley algorithm. For a target detection probability the Vehicles may form coalitions to reduce their false alarm probability and therefore increase their average throughput.

4. PROPOSED SCHEME

This section describes the system initialization, Stable matching.

4.1 System Initialization

In this model Vehicles are registered their Vehicle id to Trusted Authority(TA) generate and distribute public key ,private key, initial pseudonym for all registered cars .TA will send all registered cars details to RSU. Stable matching is occurs between RSU and Vehicle.

4.2 STABLE MATCHING

According to Gale-Shapely algorithm [13] there exist stable Matching for any given preference lists. A mapping from the elements of one set to the elements of the other. A matching is stable when the following conditions are both false. An element (A) from the first set prefers an element (B) from the 2nd set over its currently matched pair. B also prefers A over its currently matched pair. Given n V1 and V2, where each person has an ordered preference of the opposite vehicle. Find a stable match for each person. The Gale-Shapely algorithm takes the V1 & the V2 sets V, RSU and preference lists of V1 & V2 sets PL (v1), PL (v2) as input and finds a stable matching in O (n2) time. Consider two disjoint sets of size n, the v1and the v2.

Associated with each person is a strictly ordered preference list containing all the members of the opposite side. Person RSU prefers v1 to v2, where v1 and v2 of the opposite side to RSU, if and only if v1 precedes v2 on RSUs preference list. A matching μ is a one-to one correspondence between the v1 and the v2. If Vehicle v1 and RSU1 are matched in μ, then V1 and RSU1 are called partners in μ, and we write m=RSUμ (V1), V1= RSUμ (V2); RSUμ (v2) is the μ-partner of v1, and RSUμ (v1) the μ-partner of v1. A matching for which there is at least one blocking pair is called unstable, and is otherwise stable.

4.3 GALE-SHAPELY ALGORITHM FOR COALITION FORMATION

The Gale-Shapley algorithm cannot be directly used for partition formation in the game hedonic game (N, $\geq_s$). The Gale-Shapley algorithm uses two different sets however in our Scenario we have only one set .i.e the SUs. We adapt Gale-Shapley algorithm to be used for single set of users and use it as a component of our coalition formation algorithm. In our algorithm the men and the women sets are both equal .i.e. that is *v1=v2*. We refer to set of men and women to as SUs users. Since we use same sets some elements of the sets can be matched to itself that is they don't prefer being matched to anyone in the set. Initial partition is a set of singletons Π ={{1},{2},….{n}}. Let Π = {s_1,…..,s_k} be the next obtained Partition. The preference list for a coalition $S_{i,}$ i=1,.k,defines relation $\geq s_i$ as:

Where s_{ij} ε Π, j=1,…k.

This equation represents that the SU appearing first on the list is the most preferred. Now the Gale-Shapley algorithm runs with the two identical sets Π and the same preference lists for both sets as input. Let the preference list of the set be denoted as PL (Π). Whole process repeats for new partition that are formed after

Applying first round of gale-shapely algorithm until the output Of the algorithm is stable matching of partition Π to itself. The Preference list is generated for each repetition using utility function v(s), as presented .If si and sj are coalition that are formed after application of first round of gale-shapely Algorithm then coalitions are joined and become a new Coalition Si U Sj if the stable matching allows otherwise they remain as independent coalition. Algorithm stops when Gale- Shapley algorithm gives an identity matching i.e., no more matching further is possible. Following is a pseudo-code of Our Coalition Formation (CF) algorithm. The algorithm takes the number of players n and a characteristic function v(s) as input and finds a partition of N = {1,2m…n}. Algorithm uses Gale-Shapley and Preference List (PL).

4.4 CF Algorithm

```
Input:   Set of players N ={1,2,…n}. Characteristic function    v(s);
Output:   Partition of the set N.
Repeat
    m=1
    Step 1:   Each SU (Coalition) discovers the other SUs (Coalition) in the network.
    Step 2 :  Each SU calculates utility function v(Si,j) with other SUs (Coalition) in the network to generate preference list.
V(S) ←{v(S1),v(S2),….,v(Sk)} ( utility of coalitions)
PL(Π) ← PL Algorithm (Π, Π,v(s)) (Preference list)
    Step 3:   The SUs (Coalitions) arrange the preference list in decreasing order.
    Step 4: The SUs (Coallitions) starts sending and receiving proposals for coalition formation which includes the potential utility if the form coalition.
    Step 5:  If v (Si) > v (Si,j)
                Match and form coalition
            Else
                No matching (.i.e. matches to itself)
            End
    Πm ← {S1, S2, .Sk} (New Partition)
Until
m ← m + 1
Πm-1 == Πm (Previous partition is similar to current partition)
```

Following is a pseudo-code of PL algorithm. The algorithm

takes a partition Π ={S1, S2,….Sk}and a characteristic function as input and returns preference list PL(Π) of Π.

4.4 Preference List Algorithm

```
Input: Partition $\Pi = \{S_1, S2,\ldots.S_k\}$.characteristic function v(s);
Output: Preference list PL ($\Pi$) of the partition $\Pi$.
for $i = 1$ to $k$
    for j =1 to k
        $v(S_{i,j}) \leftarrow v(_{Si\ U\ Sj})$ (Calculated from eq.(11))
    end
    $(v_{it1,}\ v_{it2,\ldots,}v_{itk}) \leftarrow$ Sort $(_{vit1,vit2},\ldots,v_{itk})$
    PL $(S_{i)} \leftarrow (v_{it1}$, vit2,..,$v_{itk})$
End
PL ($\Pi$) $\leftarrow$ (PL ($S_1$),…., PL($S_k$));
Return PL ($\Pi$)
```

5. PERFORMANCE ANALYSIS

We implement the proposed scheme using (Network Simulator) NS2. Although lot of research has been done on improving security of the IOT platform devices , They are failed to impress due to its adoptability and finite function i.e. the security code generated by the previous works are having end point so that guessing probability of attackers have been increased. Our proposed system mainly focuses to reduce the packet delay of transmission between RSU and Vehicle. The issues are solved by Gale-Shapley algorithm in Vehicular ad hoc networks.

5.1 Advantages

- Sender's Computational overhead

Average time for signature generation at sender side Reduces

- Receiver's Computational overhead

Average time for signature verification at receiver side Reduces

- Packet processing rate of a receiver

Increase in Ratio of message successively verified by total number of messages received

- Storage cost

Total amount of Bytes stored by Device Reduces

- Overall delay

Total authentication time taken to produce a message by sender to the time that is accepted by receiver Reduces.

- Packet Loss rate

Ratio of message successively received by total number of messages sent Reduces.

6. CONCLUSION

The proposed method used to increase the privacy using Gale-Shapley algorithm. We conclude that strong and verifiable confidentiality protection in vehicular ad hoc networks can be achieved. The goal is to study and analyze their performance for VANET based on performance metrics like Packet Delivery Ratio, Throughput and End to End Delay was achieved.

REFERENCES

[1] Hassan Artail, Senior Member, IEEE and Noor Abbani, "A Pseudonym Management System to Achieve Anonymity in Vehicular Ad Hoc Networks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 13, NO. 1, JANUARY/FEBRUARY 2016.

[2] M. Raya, J.P. Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security, 2007, 15(1), 39-68.

[3] E. Fonseca, A. Festag, R. Baldessari, R. Aguiar, "Support of anonymity in vanets-putting pseudonymity into practice", In IEEE Wireless Communications and Networking Conference, pp. 3400- 3405, 2007.

[4] H. Jayasree, A. Damodaram, "Anonymity and accountability in web-based transactions", Advanced Computing, 3(2).

[5] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, P. Papadimitratos, "Impact of pseudonym changes on geographic routing in vanets", In Security and Privacy in Ad-Hoc and Sensor Networks, Springer Berlin Heidelberg, pp. 43-57, 2006.

[6] A. Pfitzmann, M. Köhntopp, "Anonymity, unobservability, and pseudonymity - a proposal for terminology", In Designing privacy enhancing technologies, Springer Berlin Heidelberg, pp.1-9, 2001.

[7] L. Huang, K. Matsuura, H. Yamane, K. Sezaki, "Enhancing wireless location privacy using silent period", In IEEE Wireless Communications and Networking Conference, 2(2005), 1187-1192.

[8] M. Gerlach, F. Guttler, "Privacy in VANETs using changing pseudonyms - ideal and real", In IEEE Vehicular Technology Conference, 2521-2525, 2007.

[9] H. Weerasinghe, H. Fu, S. Leng, Y. Zhu, "Enhancing Unlinkability in Vehicular Ad Hoc Networks", In IEEE International Conference on Intelligence and Security Informatics, 161-166, 2011.

[10] Y. Yaffe, A. Leshem, and E. Zehavi, "Stable matching for channel access control in cognitive radio systems," in International Workshop on Cognitive Information Processing (CIP), Jun. 2010, pp. 470–475.

[11] E. Balamurugan, “Elliptic Curve Integrated Encryption Seceme Using Analysis Vehicular Ad Hoc Network”, International Journal of Innovations in Scientificand Engineering Research (IJISER), vol. 2, no. 5, pp. 47-50, 2016.

[12] S. Bayat, R. Louie, Z. Han, B. Vucetic, and Y. Li, “Physicallayer security in distributed wireless networks using matching theory,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 5, pp. 717–732, 2013.

[13] E Peh, YC Liang, Optimization for cooperative sensing in cognitive radio networks. Proceedings of IEEE Wireless Communications and Networking Conference (WCNC '07), March 2007, 27–32.