Cooperative Anonymity Authentication in Vehicular Networks

Jianmin Chen and Jie Wu
Department of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL 33431

***Abstract*— Data privacy in Vehicular Ad hoc NETworks(VANET) is a practical issue currently under the research and development. Privacy preserving anonymity authentication in network is a challenging topic combining anonymity, authentication, data privacy and network. Existing anonymity authentication in VANET are based on *k-anonymity* model, but *K-anonymity* model group selection may leak information due to absence of diversity in the sensitive attribute etc., and thus group selection is a problem left unresolved. In this paper, we would like to address anonymity authentication attack issues, how to improve efficiency and sustain anonymity service using cooperation instead of *zero* trust model, and flexibility of vehicular side group selection to adapt changing privacy-preserving concern. Therefore, we put together design of an anonymity authentication protocol with cooperation, data privacy, and privacy-preserving data publishing considerations. Through our extensive work, we demonstrated that privacy-preserving anonymity authentication in VANET could be extended with more efficiency and cooperation plays a key role.**

Keywords: Vehicular ad hoc network (VANET), anonymity, k-anonymity model, data privacy.

I. Introduction

With the rapid research and development of wireless communication technologies in recent years, more research has been done on the application of road-side vehicular communication in order to improve driver safety, traffic management, potential internet service, etc. With less expensive communication devices, vehicles can communicate with each other as well as the Road Site Units(RSUs). A network can be formed by connecting the vehicles and RSUs is called a *Vehicular Ad-hoc NETwork* (VANET).

In VANET, On Board Units (OBUs) (the communication devices registered with the vehicle) can communicate with RSUs and go through the authentication process to obtain services from RSUs, such as internet service. In addition, anonymity authentication protocols [1][2][3] are employed to preserve the privacy of OBUs.

Nevertheless, any malicious or naive behaviors of OBUs, such as DoS attack with time consuming public key encryption and transfer, could be fatal to an anonymity authentication service. RSUs should provide fairness to other normally behaving OBUs. Therefore, anonymity authentication protocols should be considered for RSU to sustain the service, provide fairness among different OBUs, and reduce OBU's verification time.

This paper tackles the problems of anonymity authentication in VANET from both sides, and provides a *cooperative* anonymity authentication protocol based on the *verifiable common secret encoding* [1]. The authors considered efficiency of selection of groups, diversification of groups, and interpretation of design parameters with a huge amount of data through a distributed application (e.g., corporate server (application server), server (RSU), and terminal client (OBU) which corresponds to the 3-tier application seen in Figure (1).

The contributions of this paper are as follows:

1) We address *anonymity authentication efficiency* problem and apply client puzzles and use RSU's anonymity group size advice among OBUs in anonymity authentication to VANET.
2) We discuss *DoS attack* and a solution using cryptographic solution client puzzle.
3) We consider *public data or privacy-preserving publishing* in VANET. We give some concrete ideas how to handle arise issues in authentication network protocol in VANET.
4) We define a *process how to form a group efficiently from large scale of group members*, customize a small anonymity set across Application Server-RSU-OBU 3-tier conceptually. All those work are based on cooperation among RSU and OBU, and we use fully trust model between RSU and OBU instead of zero trust model seen in previous work[3].
5) Anonymity related attack and anonymity measurement in VANET are still fuzzy terms, but we advise to *adapt anonymity models in data mining* to help analysis in wireless ad hoc network. As shown in previous work [1][3], RSU's *serve probing* attack is not efficient in VANET.

The remainder of this paper is organized as follows. Section II presents privacy-preservation authentication in VANET. Section III further explain protocols extension in VANET and value of the work. In Section IV, we evaluate the protocol basis and have comparison with previous similar work. Section V introduces related work. Finally, Section VI concludes this work and outlines future work.

II. Privacy-Preserving Authentication in VANET

The VANET here is a two-layer vehicular network model. The lower layer is composed of vehicles and RSUs. Each vehicle has its own public key and private key. The communication among them is based on the DSRC protocol and, in general,

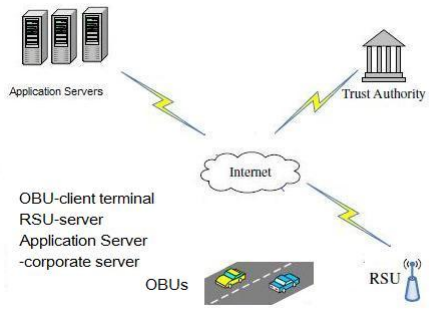

Fig. 1. The model of VANET, 3-tier application: Application Server - Server corporate version, RSU - Server, OBU - Client terminal

the top layer is a comprise of application servers, a *Trust Authority* (TA) and RSUs. The RSUs communicate with an *Application Server* (AS) using secure transmission protocols (different services may be provided by different servers), such as the wired *Transport Layer Security* (TLS) protocol. Figure 1 is the model of VANET.

A. Key Management and Group Formation

An AS manages group information. We choose to use a data structure like Java LinkedHashmap [4] to store group members information. We briefly describe the data structure that is used in group formation.

Group Linked Hash Map, G_{LHM}: Linked hash map is a hash table and a linked list implementation of the Map interface with predictable iteration order. The implementation maintains a double-linked list running through all of its entries. This linked list defines the iteration ordering, which is normally the order in which keys were inserted into the map(insertion-order).

Each group member (e.g. new vehicle) has a pair of public/private keys. We insert the group member information into a G_{LHM}. The key of hash map G_{LHM} is the member's public key which is unique. The value object of hash map G_{LHM} includes miscellaneous information: (1) the member insertion order (e.g. a counter starting from 0 increment by 1), (2) a group version, (3) time registered, (4) time revoked, (5) a bit validation information(e.g. if public key is revoked, value is false (0)), and (6) some registered information (e.g. public information to share with other OBUs).

After initialization, all the keys in the group are organized to a hash map, and a member's insertion order is kept as an index of group member. Each member (index j) can choose an index number inx and anonymity group size, g ($inx \leq j \leq inx + g$, if there is no revoked member yet), in the authentication process.

We assume that different APs may provide difference service, therefore the group size of different service may vary from hundred to million subscribers as OBUs in the future. Moreover, each OBU may only need to install portion of G_{LHM} if each OBU has to take restriction of maximum anonymity group size (e.g. 1000) to save computation cost. Another advantage for OBU is that the group data can be loaded into the memory and expedite the verification process compared with loading and searching data through static files in the hard disk.

We can also assume that the membership updating is not very often based on stolen vehicle statistics in US. If the member is revoked the entry of G_{LHM} is updated with bit of validation of public key. The order of G_{LHM} is not affected. When a new member joins the group, it will be put into the G_{LHM}, and insertion index increases one. It takes constant time to search a key value (e.g., here a public key is stored as a key value) in a hashmap. A linked list is used to avoid transferring a group of public keys, especially if the group size is big and group members stays together in a linked list: besides, members in the list could be selected based on criteria through huge size data using database efficient queries.

B. Protocol description

The protocol that we will describe is based on the previous work [1][2]. We consider privacy issues in VANET, and integrate it with anonymity models considering background knowledge attack, *t-closeness* attack, then we customize to add more features, (1) allow the OBU to form a group by randomized algorithm or prepare multiple groups depending on varied privacy needs using database queries, and (2) treat OBU and RSU rational players, (3) allow RSU adjust anonymity group level to avoid prisoner dilemma effect [5], (4) allow RSU give client puzzle [6] for suspicious anonymity request to prevent DoS attack.

It has 4 or 6 steps depending on the traffic of anonymity authentication.

(1): $RSU \rightarrow OBU : Cert(Pub_s, recGrpSize, timeout)$.

RSU broadcasts the message periodically with its certificate, recommended group size $recGrpSize$, and time out value $timeout$ for anonymity authentication request, in which Pub_s is a public key of RSU.

(2): version (a): $OBU \rightarrow RSU : Pub_s(true, inx, g, T_1, K_{session}, optional)$.

OBU constructs a message with a statically subset of the group, current time T_1, anonymity group member starting index inx, anonymity group size g, and a session key $K_{session}$. Then the OBU encrypts the message with the RSU's public key Pub_s to allow the RSU to decrypt the message. The parameter optional can be a probability value for an OBU to choose for probabilistic verification, if an OBU is a rational player, it may decide its probability before it chooses anonymity group size.

version (b): $OBU \rightarrow RSU : Pub_s(false, cusGroup, T_1, K_{session})$.

OBU customizes the subset by randomly choosing several members from the group using index number, therefore $cusGroup$ is a collection of $(inx_1, inx_2, ..., inx_n)$, in which one of them is the OBU's index value. As a special case, an OBU can choose authentication using its true identity, with *k-anonymity* group size k is 1.

(3) $RSU \rightarrow OBU : K_{session}(clientPuzzle, extInfo)$.

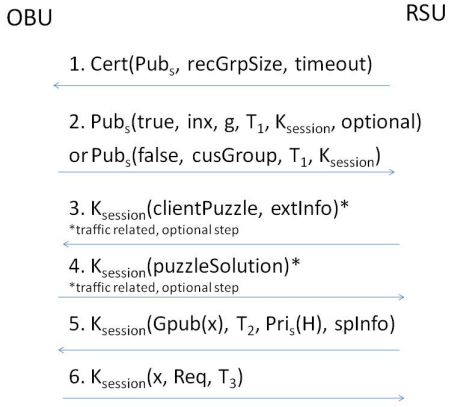

Fig. 2. Group-based authentication protocol in VANET.

When under a suspected DoS attack, RSU will attach a cryptographic puzzle to a suspected requester and require the solution to the puzzle to be attached in the reply before the RSU processes time consuming anonymity authentication *Verifiable Common Secret*(VCS). RSU can also send out a puzzle if the anonymity group is too big and not reasonable compared with its recommendation. $extInfo$ can be anything $(0, 1)$ in several categories related to busy traffic (0), anonymity group size too big (1).

(4) $OBU \rightarrow RSU : K_{session}(clientPuzzleSolution)$.

OBU sends out the client puzzle solution to RSU and waits for its anonymity authentication. Typically, solving a client puzzle requires a brute-force search in the solution space, while solution verification is trivial. Therefore, naive or adversary OBU cannot affect other normal OBU's anonymity authentication with its limited computation power compared with RSU.

(5) $RSU \rightarrow OBU : K_{session}(GPub(x), T_2, Pri_s(H), spInfo)$.

The fifth step is for RSU to give back a common shared secret encrypted with session key. RSU constructs the verifiable common secret for the group members with a random value x, its current time T_2, its current group version V_G, and the signature $Pri_s(H)$ obtained through encrypting the digest message (MAC) of $GPub$(x) using hash function H with its private key Pri_s, and *server probe* [3] information if a rational RSU using server probing tradeoff OBU probabilistic verification. (e.g., OBU can tolerate RSU server probing.)

(6) $OBU \rightarrow RSU : K_{session}(x, Req, T_3)$.

OBU decrypts x from the verifiable common secret and verifies its anonymity. Upon successful decryption and verification, it constructs a reply message with x, service request Req, and its current time T_3. The message is encrypted with the session key $K_{session}$.

Figure 2 shows group-based authentication protocol.

III. Anonymity Authentication Challenges and Solutions in VANET

In this section, we like to present anonymity authentication challenges and how we tackle problems through protocol design explanation and make contributions.

Cooperation in anonymity authentication: We consider the anonymity authentication as a service, the protocol is therefore not only an anonymity related protocol, but also a protocol to consider the cooperation. Previous anonymity authentication takes angle that OBU has *zero trust* to RSU, and RSU may pose threat to interrupt *verfiable common secret* (VCS) called *server probing*. To extend the protocol to VANET, we think that server probing attack is not practical and efficient if OBU flees away from authentication. Privacy is different from security, RSU will break privacy of OBUs as a group but still not affect individual OBU privacy concern. That is tough attack to prevent and which can be addressed by OBUs selection group smartly to avoid leak information as a group (e.g., an example in Section IV). Privacy is *extensive* concept in VANET to protect through all OBUs's work through anonymity authentication process.

Large scale group members: With less expensive CPU and other hardware, a vehicle can be equipped with a mobile device (e.g. OBU) like a laptop computer, and a lot of services can be sold to each vehicle with the OBU. First of problem arise in previous protocol is how to handle large scale of group efficiently. The members subscribed as OBU can be millions and data can be public available through an AS, how to address solution in anonymity authentication protocol level, which is not touched by original dynamic group protocol type [1].

Privacy measurement challenge: As more and more concerns from privacy and VANET privacy arise in the law in the future, all the applications to support the service including terminal client (e.g. installed on OBU), server application (e.g. installed on RSU), and corporate server (e.g. installed on AS) can be developed by service providers, and there must be privacy certification as some security certification to make sure the application can be fair to each subscriber and privacy is fairly considered. Previous protocol are solely based on *k-anonymity* model. As anonymity is more acceptable concept in VANET, different models in data privacy could be challenges to *k-anonymity* model but also complement it to cover its blinded areas. In protocol extension stage, how to make it adaptable to different models become a challenge and we show how we address that through several techniques.

A. AS-RSU-OBU 3-tier application configuration:

The protocol design is challenging if we like to extend to a real application like VANET. Big problem in previous design is that anonymity group size can be any number OBU chooses and even probabilistic verification still costs OBU, while RSU further suffers big computation time and transfer task. We propose a recommendation group size, and let OBU wisely takes size as needed. But how to implement in real application? This has to be addressed outside of protocol description.

Privacy preservation anonymity authentication is a 3-tier application client-server-corporation server privacy certification mandate, and it can be tested through several checkpoints using anonymity models. Moreover, the protocol is a small part of the feature in commercial application to comply with privacy act in short future, mostly likely the login process - authentication of commercial service with anonymity feature. Therefore, it is helpful to extend protocol to the application rather focusing on the protocol itself all the time.

Each OBU can have its terminal client application installed as a subscriber of service, and the application can boot up with default configuration and also have a configuration interface for a user to configure the settings. For instance, the anonymity group size. In order to save time to avoid user interaction, we can set (1) default anonymity group size as RSU's recommendation, (2) provide an option to set anonymity authentication with human interaction or automatically processing, (3) provide interface to allow the user to input anonymity group size accordingly, (4) provide an option to use static group or randomly formed group (seen in II (B) step 2(a), 2(b)). Usually, when client application boots up, it refreshes the group public keys and loads the data into the memory (e.g cache, sometimes it may be out of date and need to be reloaded) to do fast verification if the group size is a fit for size of memory assigned for the application.

Each RSU can have its server application installed to serve many OBUs. It also has its configuration, such as recommendation group size(e.g. default value, or user configurable), timeout setting, other settings related to client puzzle cryptographic primitive such as hash function configuration, abnormal case DoS attack related settings, etc. Each RSU may serve over hundreds to millions subscribed OBUs if the service gets cheap and become profitable in the future.

The AS acts as a corporate server, and it holds all subscribers and other public information. The AS can decide how to deploy the group keys to RSU or OBU economically, one RSU may provide anonymity authentication to partial subscribers, and further OBU can only need public key data matching up maximum group size.

B. Cooperation among OBUs and RSU

One of biggest concerns is cooperation among OBUs and RSU when the protocol [1] is extended to wireless ad hoc network (e.g. VANET). When comparing this protocol to previous work [2][3], RSU should provide fairness to all OBUs while sustaining anonymity authentication service, e.g., prevents DoS attack. we would like to address attack issue.

Dos attack in anonymity authentication process can be analyzed through several aspects. Since the computation cost of public key encryption is relatively expensive and one RSU will deal with many OBU, a malicious OBU can continuously send anonymity authentication request in limited time period and block RSU's service to other OBUs, similar to the TCP SYN flooding attack. Secondly, malicious or naive OBU can ask a big anonymity group for anonymity authentication, then RSU processes the request, which costs large amount of time because the amount of public key encryption operations of common value x time is the size of group, but OBU doesn't verify RSU's work and abandons RSU's response.

To avoid unnecessary computation cost, in our protocol design, RSU server application can set the upper limit group size, which can be determined by RSU's computer capability of processing public key operations and estimate a maximum number of authentication request in its wireless coverage area etc. Estimation can be based on facts and assumption. For example, RSU has limited wireless network coverage area while OBU has physical body width and length, and OBU moves as a vehicle does. There is a certain distance among vehicles. We assume that normal OBU keeps one session open with RSU at a time.

RSU can make an inference from authentication request and its location even though the requestor is anonymous, but OBU is in mobile status so that it is difficult to associate with one OBU with different positions. Hence, we evaluate cryptographic puzzle [6] to be used to tackle the DoS attack problem in the protocol.

C. Data privacy in VANET

How to interpret anonymity authentication in VANET is one of the biggest concerns to extend the protocol to VANET. First of all, there are numerous reasons why OBU chooses to use anonymity authentication to communicate with RSU, such as legal enforcement or insurance policy etc. Secondly, different users (OBUs) may have varying privacy needs in different contexts, and same user may require different levels of privacy in different times. Using location privacy threats as an example, an "RSU" may be an adversary obtaining OBU location information by authentication and drawing inferences from OBU time and frequency of passing certain "RSU"s. Thus, it may be necessary to develop personalized privacy protection protocol to help a user to find a comfortable balance between the extreme of fully disclosed and completely withheld driving history through anonymity authentication process.

As various anonymity models and algorithms [7] covers various privacy concern and complement each other, this protocol extension includes various anonymity models. From anonymity authentication in dynamic group [1] to VANET, protocol extension [2] is based on *k-anonymity* model, and OBU customizes its anonymity group size which is user-specific, also called *adaptive*. In further protocol extension [3], OBU can do *probabilistic* verification to save computation cost. However, previous protocols reflects privacy in VANET limited by the pitfall of *k-anonymity* model.

We should not ignore various anonymity models contribution to privacy integrity in this protocol extension. Various anonymity models are applicable in VANET at different levels. As an example of *m-invariant* model and location privacy in VANET [8], to control the number of alternative routes, a mobile user (OBU) would be difficult to maintain anonymous in situations where all k users are traveling along the same route segments pass through the same set of identifiable

RSUs, it passes *k-anonymity* model test but has low m value compared to value k.

D. Short review of anonymity models

In protocol extension to VANET, *k-anonymity* model was selected in protocol [2][3], OBU ensures that it forms a group with size k big enough for privacy concern. The extended protocol mainly focuses on RSU *server probing* attack, which is to break anonymity group size k. In this protocol, we extend the protocol in VANET considering that RSU can launch more efficient data analysis instead of *k-anonymity* group size as seen in all data privacy models analysis. Since more data are available to public or anonymity-preserving published in VANET, RSU can do more efficient attack besides *server probing* attack. Here we go through several models and discuss the techniques that can be extended in this protocol.

1) l-diversity model: The *k-anonymity* can create groups that leak information due to absence of diversity in the sensitive attribute. The *l-diversity* model is dealing with sensitive attributes diversity.

In order to avoid *l-diversity* model related problem, protocol description in last section doesn't provide, based on the prototype, we can provide a technique: OBU can use *l-diversity* model for each sensitive attribute to prepare a group. OBU can construct different queries through RSU from AS and build up a set of groups (seen in Table 1). Then, OBU can select a group from multiple groups depending on its current privacy concern.

2) t-closeness model : The *t-closeness*, as a privacy notion, requires that the distribution of a sensitive attribute in any equivalence class is close to the distribution of the attribute in the overall table (i.e., the distance between the two distribution should be no more than a threshold t).

3) Personalized privacy preservation model: The problem in anonymity design is that we may be offering insufficient protection to a subset of people, while applying excessive privacy control to another subset. The concept of *personalized anonymity* is a generalization framework.

4) Background knowledge attack model: Several anonymity models are related to background knowledge attack, inference attack. In VANET, RSU chooses *server probing* on *Verifiable Common Secret*(VCS), which is not effective in a way to break privacy, since RSU has more powerful computer than OBU, running machine learning algorithm to break privacy after anonymity authentication process may be more efficient. For example, intersection attack, from different OBUs requests, find the intersection of the set.

IV. Analysis and Evaluation

In this section we analyze the anonymity authentication protocols. Our test computer was a $2.0GHz$ Intel Core Duo CPU with $1.50GB$ of RAM running Windows Vista. Using Java platform standard edition 6.0's cryptography library RSA algorithm, the computer was able to complete 1698 public key encryption a second, in other words, spend $0.58ms$ to complete an RSA public key encryption.

A. Experiment with Client Puzzles

Client puzzles are a viable method for protecting SSL servers from SSL based DoS attack in a client puzzle extension to TLS protocol against DoS attack through the work showed in paper [9]; and that work showed that client puzzle can efficiently prevent the DoS attack if puzzle size is settled down properly. We believe that client puzzles in this anonymity authentication protocol should work out also to countermeasure against DoS attack in theory. As seen in work [9], we omit detail of client puzzle states enter/exit in this protocol and experiment of with/without client puzzle during the attack in this protocol.

In this protocol design, we have to roughly decide what RSU and OBU can configure properly in advance for client puzzle feature. Several things have to be considered: (1) hash function selection, (2) client puzzle size, (3) client puzzle other detail.

We choose to use hash function MD5 to evaluate the protocol related to client puzzles feature. For hash function $h(y)$, A client puzzle is the triple $(n, y', h(y))$, where y' is y with its n lowest bits set to 0. The solution to the puzzle is the full value of y. The best way for a client to generate y, is to exhaust the ways in the n lowest bits. This should take 2^{n-1} calculation of $h(y)$ on average. The test computer spends $629ms$ to complete 1 million calculation of MD5 hash function.

The RSU server,on the other hand, needs to generate a random block (for MD5, 512 bits) of data, and evaluate the hash function twice.

It takes test computer $629ms$ to complete 1 million MD5 hash function, between 2^{19} and 2^{20}, while 1000 RSA public key encryption requires a test computer $580ms$ to complete. If OBU unit sends out anonymity authentication with group size more than 100, RSU can give OBU dynamic size (e.g., range from 10 to 20 bits) puzzles before it commits the calculation of over 100 RSA public key encryption in order to prevent anonymous OBU wastes RSU time. Based on the fact that client puzzle size is linearly proportional to RSA group size, we argue that the client puzzles could stop attackers but will not disrupt OBU client operations if we allow RSU update puzzle size dynamically to find optimal value.

The protocol can also further be extended to allow OBU to bid for resources by tuning the difficulty of puzzles it solves called *Puzzle Auctions* [10].

B. Group Selection and Anonymity-preserving Publishing

The existing protocol design [2] uses a complete binary tree over the ordered list, in which the public keys are leaves in the tree and internal nodes are IDs to identify each subtrees. The group can be selected using a subtree root. The protocol did provide flexible subgroup organization, however, two nodes with far distance in the ordered list cannot stay in a group unless the group includes all the nodes in the connecting path.

We choose to keep the ordered list, but we also like to speed up the process to search a node through public key

with constant time. The double linked list of hashmap also provides quick search for customized group.

In VANET, corporate server may have subscribers with large scale of information across several tables like other commercial database (e.g., cellular phone customers). The subscriber's information may be public or anonymity-preserving published [11]. It is not practical for RSU/OBU to pre-install all members information and also get updated information with disabled members. We propose a solution to use off-line download group data information through queries on corporate database.

Example 1: An OBU is registered as Andy has access the following information:

TABLE I
PARTIAL PRIVACY-PRESERVING PUBLICATION OBU'S USER TABLE

public key	Age	Zip	Color	Model	Year	Seq
***	17	12k	white	Ford	1996	1
***	19	13k	blue	Ford	2008	2
***	20	14k	red	GM	2007	3
***	24	12k	green	Chrysler	2006	4
***	29	12k	black	Toyota	2003	5
***	34	12k	purple	Hyundai	2007	6
***	45	39k	white	Ford	2009	7

In this example, Andy has several preferences to choose from groups for his privacy concern. If he thinks that zip code is insensitive to him, he may chose a SQL statement "**Select** * **from** User **where** Zip = '12k' **order by** Auto Year **desc** " to query the table to get the same zip code (zip code is generalized to preserve privacy) with different public keys to prepare his group formation provided that zip code $12k$ meets *k-anonymity* ($k \geq 4$) property and also try to avoid old car which is sensitive for RSU to predict possible breakdown on the road. Result set in order is 6, 4, 5, 1 expressed in Seq column value, if *k-anonymity* group size is 3, then the first three 6, 4, 5 are selected (In the protocol, the node usually chooses $n-1$ node instead of n nodes and includes itself to form a *k-anonymity* group.) With a million records in the table, each OBU may customize multiple queries for its *diversified* privacy concerns to get hundreds record for group formation.

In terms of RSU searching a public key, the existing protocol design [2] has actually $O(n)$ computation cost, but our mechanism provides $O(1)$ time to do searching and also much more flexibility in group formation.

C. Random Selected Group Members and Various Anonymity Models

Basically, the database is a very good place to get sorted data using query based on index support. Hence, application server can respond to multiple queries from RSU, and those result data are sorted and efficiently searchable by a public key. Then, OBU gets data from RSU directly. RSU can generate different groups, where data privacy varies.

Computation cost with public key encryption/decryption is a major role to measure the cost. However, if application server has over million records of OBU, searching and maintaining computation cost is an important concern in group formation, especially for random selected group members. It takes a long time to search a member if the database is not prepared very well. Previous protocols doesn't address the problem, we like to prepare a solution in protocol design, we present hashmap instead of data structure of group which is low efficiency to support searching algorithms.

In our protocol, we use hashmap to provide constant time to search for a public key. Therefore, the time to form a random selected group is linear to the size of anonymity group. Since members are chosen with queries using customized criteria, we could consider different models include *l-diversity*, *t-closeness*, *(k,e)-anonymity*, *privacy skyline* and *δ-presence* avoiding shortcoming of *k-anonymity* model [7].

V. RELATED WORK

Anonymity authentication protocol designed in wireless ad hoc network is a challenge work. Different interpretation can lead to different extension of protocol. Related work areas are: (1) anonymity in network [12], (2) data privacy and models, (3) anonymity authentication, (4) wireless ad hoc network (e.g. VANET), (5) cryptographic protocol, (6) attacks and countermeasure, techniques etc. Even though our focus is still on VANET anonymity authentication. We believe that protocol should be extended to reflect privacy true nature instead of staying on *k-anonymity* model size of group.

Some anonymity authentication mechanism only works first k times authentication [13], which may be used to prevent user misbehavior such as DoS attack. Besides [2][3], *k-anonymity* for location privacy is in [14]. Ren proposed a privacy preserving authentication in [15] that uses blind signature and one-way hash chain cryptographic technique to keep privacy. Calandriello [16] proposed a pseudonym-based protocol which uses group signature as the mechanism for a vehicular to generate its own pseudonyms. Sun [17] used group signature and identity-based signature scheme guarantees security and anonymity. In detail, he applied group signature to vehicle-to-vehicle authentication and identity-based signature to vehicle-to-infrastructure authentication.

More general related work we also like to present here to reflect how to evaluate a protocol design, it is biased or game theory intelligent, or truly understanding anonymity difference among network, data mining, and data privacy broad areas. Here are some quick review of work.

Different models and algorithms in privacy-preserving data mining area [7] and anonymity in network [12] provides great resource related to anonymity, network, data privacy.

Probabilistic approach to anonymity [18] is very helpful to understand anonymity in network, e.g., especially posterior probability analysis can be related to a link analysis between observed event and possible input - an anonymity set.

K-anonymity model is widely used in anonymity network, e.g. DC-Net, Mix-Net. Different network schemes are related to implement k anonymity to hide sender-receiver, message-among-hops correlation. In order to reach target anonymity group size, techniques like delaying, flushing using time or

threshold of k message, dummy message used as noisy signal in traffic analysis etc.

Game theory knowledge [19][5] is helpful to evaluate the protocol design. RSU and OBU forms a 2-player game, with strategies from both sides. Cooperative issue in design should not be neglected while anonymity authentication allows a player hide him in a group. In anonymity authentication multiple extension, *adaptive* or *probabilistic* anonymity authentication in VANET could not settle down as a *saddle point* in game theory viewpoint, RSU responds with a strategy if RSU acts rationally for self-interest.

VI. Conclusion

In this paper, we demonstrate that anonymity authentication protocol design could be very interesting and challenging in VANET. Cooperation is necessary in multiple aspects. It takes RSU and normal behaving OBUs efforts to break DoS attacks, privacy-preserving could be OBUs's group cooperation efforts to reach through anonymity authentication even if it is single OBU's concern. Also, a privacy-preserving authentication protocol is proposed to enforce the cooperation in anonymity authentication in VANET, specifically against DoS attacks. The work demonstrated that anonymity authentication in VANET could reflect more anonymity model s in data privacy area and also it is a novel work in network protocol.

References

[1] S. Schecheter, T. Parnell, and A. Hartemink. Anonymous authentication of membership in dyanmic group. January 1999.

[2] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang. Adaptive privacy-preserving authentication in vehicular networks. In *Proceedings of IEEE International Workshop on Vehicle Communication and Applications, pp.1-8*, 2006.

[3] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang. Probabilistic adaptive anonymous authentication in vehicular networks. In *Journal of Computer Science and Technology*, Nov. 2008.

[4] http://java.sun.com/javase/index.jsp.

[5] V. Srinivasan, P. Nuggehalli, C. Chiasserini, and R. Rao. Cooperation in wireless ad hoc networks. 2003.

[6] A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In *6th NDSS*, 1999.

[7] C. Aggarwal and P. Yu. In *Privacy-Preserving Data Ming Models and Algorithms*, Springer LLC, 2008.

[8] L. Liu. From data privacy to location privacy: Models and algorithms. In *VLDB, pages 1429-1430. ACM.*, 2007.

[9] D. Dean and A. Stubblefield. Using clients puzzles to protect tls. In *Proceedings of 10th Annual USENIX Security Symposium*, 2001.

[10] X. Wang and M. Reiter. Defending against denial-of-service attacks with puzzle auctions. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy (SP'03)*, 2003.

[11] Y. Tao J. Li and X. Xiao. Preservation of proximity privacy in publishing numerical sensitive data. In *SIGMOD'08*, 2008.

[12] Free haven's selected papers in anonymity. In *http://www.freehaven.net/anonbib*.

[13] L. Nguyen and R. Safavi-Naini. Dynamic k-times anonymous authentication. In *ACNS, pages 318-333*, 2005.

[14] B. Gedik and L. liu. Location privacy in mobile systems: A personalized anonymization model. In *Proc. the 25th International Conference on Distributed Computing Systems*, 2005.

[15] Ren K etc al. A novel privacy preserving authentication and access control scheme for pervasive computing environments. In *IEEE Transaction on Vehicular Technology*, 2006.

[16] G. Calandriello, P. Papadimitratos, A. Lloy, and J. Hubaux. Efficient and robust pseudonymous authentication in vanet. In *Proc. the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, 2007.

[17] X. Sun, X. Lin, and P. Ho. Secure vehicular communications based on group signature and id-based signature scheme. 2007.

[18] K. Chatzikokolakis. Probabilistic and information-theoretic approaches to anonymity. In *Ph.D. thesis, Laboratoire d'Informatique (LIX)*, October 2007.

[19] Game Theory .net. http://www.gametheory.net/.