Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks

Yong Xi, Kewei Sha, Weisong Shi and Loren Schwiebert
Wayne State University
{yongxi,kewei,weisong,loren}@wayne.edu

Tao Zhang
Telcordia Technologies, Inc.
tao@research.telcordia.com

Abstract

Vehicular networks have attracted extensive attentions in recent years for their promises in improving safety and enabling other value-added services. Security and privacy are two integrated issues in the deployment of vehicular networks. Privacy-preserving authentication is a key technique in addressing these two issues. We propose a random key-set based authentication protocol that preserves user privacy under the zero-trust *policy, in which no central authority is trusted with the user privacy. We show that the protocol can efficiently authenticate users without compromising their privacy with theoretical analysis. Malicious user identification and key revocation are also described.*

1 Introduction

With the development of micro-electronic technologies and wireless communications, we envision that in the foreseeable future vehicles will be able to communicate with each other (V-to-V) or with roadside units (RSU) which serve as the gateway to the Internet (V-to-I). Several challenges need to be addressed in order to realize this vision. Current research in vehicular networks mainly focuses on issues related to vehicular communications. Significant progresses have been made in media access (MAC) layer protocols [8] and physical layer protocols [3]. However, issues about security and privacy, which will play a critical role in the acceptance of vehicular networks, have not been well studied. When we come to a point to consider deploying vehicular networks, security and privacy play an essential part in the deployment of the system. Recently, several works including [1, 7, 9] start to look at the problem of security and privacy in vehicular networks.

A vehicular network needs strong security guarantee. This is due to the fact that the main goal of deploying a vehicular network is to enable safety applications and to improve overall efficiency of the transportation network. In a safety application, the kinetic information obtained through sensors in a vehicle is shared to other vehicles. Thus it is important to guarantee the authenticity of this type of information. In those applications targeting improving the efficiency of the transportation network, the authenticity of the collected information can also help improving data accuracy. Thus, to provide strong security in vehicular networks, it is desirable to authenticate OBUs into the network.

However, authentication in this mobile environment poses a privacy risk to the users. Through authentication, the network can be aware of whereabout of a specific user at a specific time. To address the problem of authenticating users without compromising their privacy, previous approaches [1, 2] take partial trust policy [14], in which the privacy is explicitly protected by a designated central authority. A partial trust policy may not be enough since the central authority can track the user efficiently. To address the problem of providing privacy for authentications in a *zero-trust* policy, in which no central authority can be trusted with the user privacy, Sha *et al.* propose a group-based privacy-preserving authentication protocol for vehicular networks in [14]. However, this approach has considerable performance concerns because of the high overhead of asymmetric key encryption and decryption. Thus, in this paper, we propose to use symmetric random key-sets for privacy-preserving authentications in vehicular networks.

In the *zero-trust* policy, vehicles trust neither public nor private servers and networks. Users have to rely on OBUs to provide privacy. In our symmetric random key-set approach, each valid user is assigned a random key-set with k keys drawn without replacement from a central key pool. Each key drawn is shared by several users. A set of a keys are used for authentication to show the validity of the user. We analyze the security and privacy properties of our protocol, and the relationship between the privacy and several parameters, such as the size of the key pool, the number of keys in each vehicle, and the number of keys used for authentication. In addition, key management issues including key distribution and key revocation are also analyzed.

The contributions of this paper include three-fold. First, we introduce to apply symmetric random key-set for privacy-preserving authentication in vehicular networks. Second, we propose a privacy-preserving authentication protocol in a *zero-trust* environment. Third, we analyze the privacy and security properties of our protocol.

The rest of the paper is organized as follows. Problem statement and system description are denoted in Section 2. Symmetric random key-set based, privacy-preserved authentication protocol is proposed in Section 3. We analyze the privacy and security properties of the proposed protocol based of mathematical analysis in Section 4. Related work are discussed in Section 5. Finally, conclusion and future work are depicted in Section 6.

2 Problem Statement

A vehicular network consists of RSUs and OBUs. The communication happens between RSUs and OBUs or between different OBUs, depending on the application. Dedicated Short Range Communications (DSRC) is the designated wireless protocol for a vehicular network [3]. Usually, OBUs are assumed to be tamper-proof, where secrets (e.g., encryption keys) are stored and security protocols are executed.

Vehicular networks are developed to support a wide range of network applications, including transportation network operation support and safety applications.

Compared with wired and wireless networks, vehicular networks are characterized as highly dynamic. This poses a great challenge as to secure this network in such a highly dynamic environment. A universal authentication system is required not only for the purpose of providing necessary security, but also for the purpose of providing the desired pervasive service.

However, a universal authentication system, though technologically challenging, also poses a big threat to the user's privacy in the context of vehicular networks. DSRC is a short- to mid-range wireless protocol. This enables the network to pinpoint the user's approximate location without any additional mechanism besides the network accessing information. Also, various vehicular network applications propose using even higher precision location information. For example, in lane departure assistant applications, the location precision needs to be in centimeters.

Integrating location tracking ability into networks has been controversial during recent years. For example, the privacy in cellular phone E911 service has been extensively discussed. Even so, E911 service is based on GPS technology. The accurate location is managed by the cellular phone itself. This gives a user the flexibility to define how the location information should be managed. In a vehicular network, as discussed above, the location is essentially managed by the network. What makes the problem worse is that as the vehicular network becomes pervasive, the physical movement of an individual is under constant monitoring as in US people strongly rely on cars.

One way to protect users' privacy is through laws and policies. However, it is not enough just to rely on the laws and policies to protect users' privacy. For example, laws and policies involve social costs. If the costs exceed the benefits brought by such a system, the system is bounded to fail. Also, if a system provides the universal surveillance capability, it is bounded that this capability will be used. So, from the technical point of view, we should look at alternatives starting from the beginning.

An OBU will have contact with lots of RSUs during a user's trip. Essentially, to prevent a car from being possibly tracked, the privacy protection has to be provided at each OBU. Providing privacy protection at each OBU is also scalable since each RSU, which probably will be serving lots of OBUs, no longer has to provide privacy protection.

Preserving privacy while still enabling the authentication is a hard problem. A single identity enables the OBU being tracked. Using multiple identities at different RSUs is a natural extension. In this paper, we exploit this idea for preserving privacy while still allowing the authentication. The set of multiple identifiers has to be unique so that there is no two OBUs with the exactly same identity. However, we assume that this set member information is kept at the distribution center and not known by the RSUs.

Without identity information, multiple target tracking (MTT) [12] algorithms can be used to estimate the trajectory of a target based on some other measurements. For example, a single OBU might have a connection with a service provider across multiple RSUs, thus sending packets with the same destination. This problem can be solved by putting an anonymizer between the OBU and the service provider, which is complementary to our solution.

Different types of information can also be synthesized by an MTT algorithm to identify a car. For example, existing transponders on highways can detect the number of cars passed during a specific time. This can help an MTT algorithm to narrow down the candidate since the same car will be expected somewhere down the road. We do not expect to solve the tracking problem in this paper due to possibly a large range of inputs to an MTT algorithm. Instead, we argue that our approach can mitigate this problem and propose some extensions for this purpose.

Physical detection of cars is possible technologically. For example, scanning plates using cameras. If such technologies are deployed, a car can no longer prevent itself from being tracked. We call this type of privacy problem physical layer privacy problem. In fact, it is an independent problem not related with privacy protection in the communication network. In this paper, we do not address this problem, and assume that the privacy can only be violated through vehicle communications and other telematics applications.

Our approach intends to have the following properties. It is not possible for each RSU to tell exactly which OBU is authenticated. It is not possible for a sequence of RSUs to collectively identify an OBU without consulting with the key distribution center. During crime investigation and accidents forensics, a violating OBU can be identified with high probability with the help of the key distribution center.

3 Privacy Authentication by Symmetric Random Key-Set

Symmetric key approaches have been widely used for encrypting/decrypting purposes as they are more efficient than public key based approaches. Computation overhead of symmetric cryptography is much less than that of asymmetric cryptography under current implementations, which is a desired feature in real-time applications, such as vehicular networks.

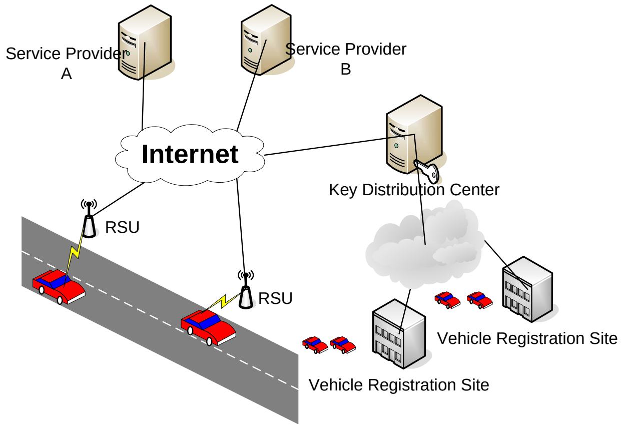
Symmetric random key-sets are sets of symmetric keys drawn from a shared key pool. It has been applied in wireless sensor networks to establish secure links between sensors because of the high probability of two key sets sharing a common key [4]. In this paper, we take advantage of the feature that one symmetric key is shared by several vehicles. We use symmetric key-sets for authenticating vehicles while preserving their privacy. Here, we first introduce the basic idea of symmetric random key-set. Then we provide the detail of the privacy-preserving authentication protocol.

In the symmetric random key-set approach, all valid keys form a key pool and each member will randomly draw a key set from the key pool. If the size of key pool and the size of the keys held in each member are properly chosen, there is a high probability that one key is shared by a set of members. In our approach, we take advantage of this feature, i.e., when the keys shared by a set of vehicles are provided to the RSU for the authentication purpose, the RSU cannot distinguish the vehicle that requests an authentication, because the same key may be provided by some other vehicles.

Symmetric random key-set has several advantages to be applied in an application, such as vehicular networks, which has strong real-time and privacy requirements. First, symmetric keys have much less time in encryption and decryption so that it is more suitable to be applied in vehicular network which has strong real-time requirement. Second, each key is shared by a set of vehicles, thus, privacy of the vehicle is well protected because the identity and the keys are not closely correlated. Third, each vehicle holding a set of keys is helpful to the key revocation, i.e., even some of the keys have been revoked, the rest of the vehicles can still have chances to be successfully authenticated. Forth, the whole key set or a majority of the keys in one vehicle can act as the identity of the vehicle, thus, if the whole set of the key can be caught by the third part, the identity of the vehicle can be revealed.

The whole set of the keys in each OBU is called its key ring. In the rest of the paper, we use key ring and full identity interchangeably.

The system architecture of VII is shown in Figure 1. It consists of key distribution center(s), service providers, vehicle registration sites, RSUs, and OBUs (i.e., cars). A key distribution center (KDC) serves as the central authority for administrating keys and assisting identifying a malicious user. RSUs actually authenticate vehicles. OBUs initialize authentications on behalf of users.



In our approach, key pre-distribution is done when the vehicle is sold and when the vehicle is registered at each state. The OBU will be installed a set of a symmetric keys randomly drawn from the key pool. These keys are used to upload data or download services. They are stored in some well protected parts, e.g., tamper-proof devices on vehicles. The keys are renewed every time the registration of the vehicle is renewed in state offices, e.g., DMV in New Jersey. Thus, the symmetric keys have a lifetime of at most one year if the period between the registration is one year. The expiration of keys can improve the security of the system. Key pre-distribution simplifies the classical problem of key distribution, which is especially difficult in such a large scale system.

We do not address the specific intrusion detection techniques. Instead, we provide a way to link the originating point of the attack to the attacker. This is due to the fact that access to the network requires authentication. Although we provide some anonymity, the KDC can still narrow down the range of candidates for the attacker, especially when other details about the attack is also provided, such as the physical location of the attack. We need to emphasize here that without the participation of the KDC, the privacy of an individual is protected.

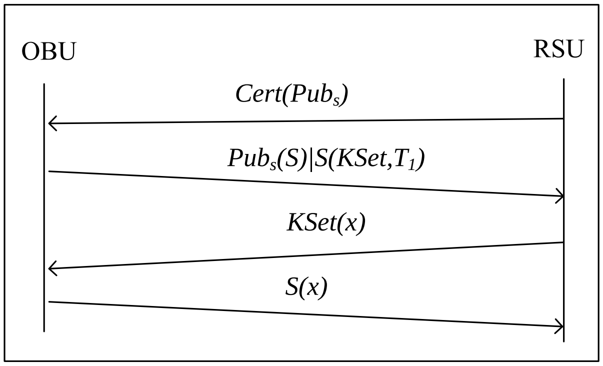
Our approach also possesses a nice feature on reducing the probability of attacking. Ideally, the attacker wants to use random key sets during the attack so that his physical trajectory won't be identified easily. However, the attacker has only a limited number of keys. Using different keys during the attack increases the probability of exposing his unique identity. This property does not contradict with the privacy protection provided for normal users. This is due to the fact that generally attackers only constitute a small part of the population, thus it is easier to identify an attacker.

Proper actions can be taken once the attacker is identified. If real-time response is required, the RSU can increase the number of keys required for authentication. This can effectively narrow down the range of possible attackers. The worst case is that normal users have to disclose full identities to access the network. We argue that this is an acceptable trade-off. It effectively falls back to the single identity authentication scheme. Even so, the network still can not know the individual corresponding to the identity. The best the network can do is to track a vehicle. However, the vehicle is aware of the change of the parameter. If a prolonged period of change of the parameter is detected, the vehicle can disconnect from the network to preserve its privacy.

For some type of network intrusion, the attack may only be detected after sometime the attack is already done. In this case, the proof can be collected and the identified attacker can be revoked. Stolen vehicles can be directly revoked or put into a special list for tracking. In such cases, the KDC distributes the full identity associated with such a vehicle. The RSU can match the candidates directly with those identities. To save space, the distributed list can be in a space-efficient form. For example, a Bloom filter can be used. Once a candidate is matched, the RSU can retrieve the actual list matching the candidate from the KDC. The number of revoked vehicles should only constitute a small part of all the vehicles. Thus a RSU rarely contacts the KDC.

We argue that identity privacy and location privacy are critical to the real deployment of this system when services are downloaded and data are reported. Referring to the privacy level described in [14], we intend to preserving privacy under *zero-trust*, in which the network and servers are not trusted to provide enough privacy protection. In our protocol, we take advantage of symmetric random key-set, in which every key is shared by a set of vehicles. Thus, when the key is used for authentication, a RSU cannot uniquely identify the OBU because the key may be provided by other vehicles who share the same key.

Our privacy-preserving authentication protocol consists of several steps as listed in Figure 2. First, the RSU announces its service by broadcasting certificated signed by the KDC. When a vehicle decides to access the service, it will send an authentication request together with a set of a key indices which were assigned from the key pool. $KSet$, which is denoted as $K_{k1}, K_{k2}, ..., K_{ka}, ...$, consists of a set of symmetric keys shared by the vehicle and the RSU. A time information T_1 is appended for message refreshness. All these information is encrypted by a session key S. The session key S is encrypted with the RSU's public key Pub_S. This encryption protects the message integrity and prevents the keys from being disclosed to an outside observer. A set of keys, instead of one key, are used for authentication, because there is a high probability for the OBU to have one key shared by a large amount of vehicles, which makes it difficult to identify a malicious vehicle if the key is reported as invalid, while there is only a much lower probability for a set of a keys being shared by a large number of vehicles so that it is much easier to catch a malicious vehicle.



After the RSU gets the authentication request from the vehicle, it creates a challenge message by encrypting a random secret with the set of keys indicated in the request. The encryption should use Cipher-block Chaining (CBC) mode with multiple encryption keys. The order to use the set of keys is the same as defined in the authentication request. If the road-side server detects some invalid keys or revoked keys, the authentication will fail immediately. Otherwise, the challenge is sent back to the vehicle to verify the actual possession of those keys by the vehicle. It is worth noting that a legitimate user may use some revoked keys for authentication due to the shared key pool. In this case, we show in Section 4.4 that the probability of all a keys being shared with a revoked user is very small. The RSU can thus detect that the key ring of the OBU should be updated. The RSU can then broadcast the revocation list to the OBU, which in turn updates its key ring and uses the updated key ring in future authentications without further problems. In this paper, we focus on the authentication protocol itself and omit the details of the revocation process, which is our future work.

Upon receiving the challenge, the vehicle decrypts the challenge with the chosen keys and creates a response by encrypting the random secret with the session key. The response is sent back to the RSU. RSU verifies the response by comparing the decrypted secret with its original secret. Upon successful verification, the RSU accepts the session key and

Parameters	Description
n	The total number of keys in the key pool
v	The total number of vehicles that registered in the system
k	The total number of keys in one vehicle
a	The number of keys that are sent for authentication
C_n^m	The total number of possible different combinations of choosing m different elements out of n different elements
$n!$	Factorial of N
$P\{a+\}$	The probability of two vehicles sharing at least a keys
$P\{a\}$	The probability of two vehicles sharing exactly a keys
$P\{a+\|A\}$	Given a keys, the probability of another vehicle sharing at least those a keys

the vehicle is authenticated.

Each vehicle defines a period in which a single key in its key ring is used only once. Other than that, the key set used for authentication is randomly selected from the key set the vehicle has. Thus, within one period, we can guarantee that every time the keys used for authentication are different, which improves the privacy of the protocol as discussed in Section 4. The session key has only a short lifetime. It is valid in a local area. The policy to manage the session key can be enforced by an OBU according to its privacy requirement. For example, a session key can be geo-bounded. The size of the area may be defined by the application.

4 Privacy Analysis

In the protocol described above, every time a vehicle enters some area it will send a set of symmetric keys to the road-side server to request an authentication. In this section, we analyze the anonymity provided by our protocol. The parameters we used in this paper are listed in Table 1.

Anonymity is the state of being not identifiable within a set of subjects, the anonymity set [10]. To analyze the anonymity provided by our protocol, we have to construct the corresponding anonymity set.

In this subsection, we construct the anonymity set out of the global set. We call this analysis static analysis since it does not consider any traffic scenario. And we call the anonymity under this scenario static anonymity. The static anonymity is the basic anonymity enjoyed by each vehicle. In a dynamic traffic scenario, the vehicle set is always a subset of the global set. The dynamic anonymity is less than the static anonymity. We analyze the dynamic anonymity in the next subsection. The meaning of this static anonymity is that when the network sees that the same set of keys is used for two different authentications, the network can not decide whether it is from the same vehicle or not.

Consider when multiple vehicles are accessing the same RSU. Assume that every vehicle has the same probability to be in the same area. Given a keys, the probability of two vehicles randomly picked out of the whole vehicle set sharing at least those a keys is: (please refer to the technical report version [15] for the formula deduction.)

$$P\{a+|A\} \approx \left(e^{-\frac{1}{2n}} e^{\frac{1}{2k}} \left(\frac{k-a}{n-a}\right)\right)^a$$

Assume that the combinations assigned to all vehicles are uniformly picked out of the whole combination space. The real static anonymity for each authentication is $P\{a+|A\}v$.

We designate the vehicle accessing the network as vehicle Bob. We also want the probability of Bob being tracked small. We assume that multiple vehicles are traveling on the same road. This is a reasonable assumption. If there is only Bob on the road, whatever keys he uses, he can still be tracked. Since RSUs do not know what keys are exactly stored in each vehicle, they can only make a combination of all possibilities. We show that anonymity is well preserved under this scenario.

To prevent correlation from being made, the OBU adopts an authentication reuse period concept. Within one period, for each authentication the OBU randomly picks up a keys which have not been used in the same period. So the average period of reusing each key is $c = \frac{k}{a}$ (in number of authentications). Assume that $T(c)$ other vehicles have been accessing the same set of OBUs during this time. The expected number of vehicles sharing a key with Bob is:

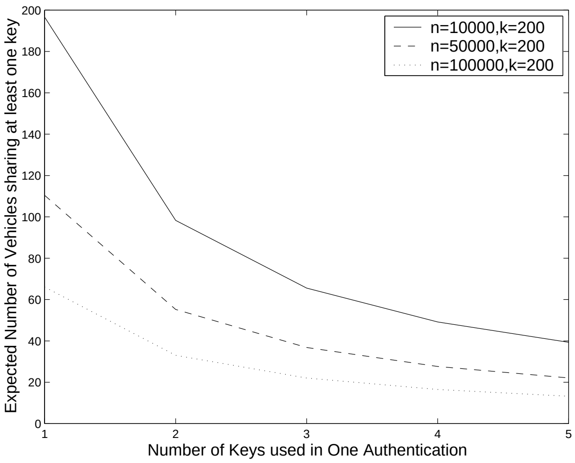
$$T(c) \times (1 - P\{0\}) \tag{1}$$

where $P\{0\}$ is the probability of two vehicles sharing no key. (Please refer to technical report for $P\{0\}$ [15].)

$$P\{0\} \approx e^{-\frac{2k^2}{n}}$$

It can be easily seen from the above equation that the expected number of vehicles increases as k increases. Since $P\{0\}$ is small, the number of vehicles is dominated by $T(c)$. This means that it can easily be increased by extending the period. Figure 3 shows the expected number of vehicles for different values of a. We assume that $T(c)$ is linear to $\frac{k}{a}$. This is a conservative assumption. It can easily be seen from the figure that the expected number of such vehicles is quite large.

Since those vehicles share a key with Bob and we use all keys in a period, it is guaranteed that those authentications



have common keys with Bob. This creates diversion if RSUs are trying to correlate the authentications with one common key. We need to point out that the authentications with a common key do not have to happen at the same RSU. Because we use different keys for each authentication within one period for each vehicle, the correlation can not be done for each vehicle within one period. Essentially, the tracking can only be done based on the whole key ring.

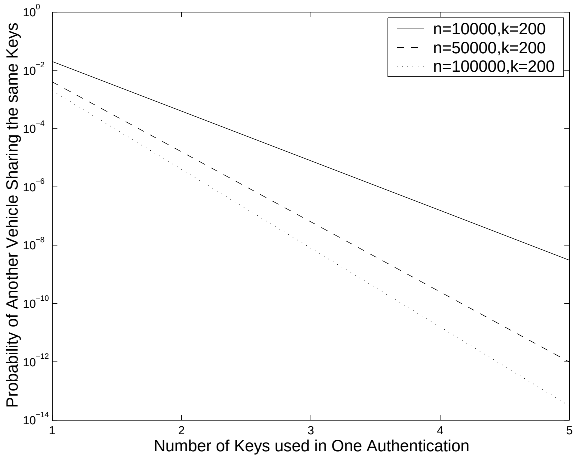
If RSUs are trying to correlate authentications with r common keys, where $1 < r \leq a$. The average time (in number of authentications) of the same r keys being reused for each vehicle can be shown as the following formula:

$$R = \frac{k!r!(a-r)!}{a!a!(k-a)!}$$

R is dominated by $\frac{k!}{a!(k-a)!}$ since r and a are small compared with k. This number is very big given a reasonable value for k. For example, for $k = 200$, $a = 5$ and $r = 3$, its value is $253, 565, 004$. It is easy to see that it is very unlikely that it will be repeated.

We also point out that it is very difficult for RSUs to correlate between individual authentications since authentications from the same vehicle does not have common keys within one period and authentications from a different vehicle does not have common keys either with high probability. It is very difficult to differentiate between them.

$P\{a+|A\}$ is also directly related with the probability with which a RSU can identify an attacker when the KPC is involved. Figure 4 shows this probability when a keys are being used during authentication. Apparently for $n \gg k$, $P\{a+|A\}$ is mainly decided by a. In Figure 4, we only show $P\{a+|A\}$ for different values of a. The figure was drawn with the exact form of $P\{a+|A\}$ in technical report version [15]. $P\{a+|A\}$ is shown in log-scale for clarity. It can be seen that the probability decreases sharply when the number of shared keys increases. This is a good property for differentiating an attacker from its immediate neighboring vehicles. For small values of a, the static anonymity is still quite large due to the large total number of vehicles. For larger values of a, we show in the next subsection that although a combination of a keys is unique, it is very unlikely that the combination will be reused again. Thus anonymity is still preserved.



a

We want our protocol possessing the following properties. It should enjoy a good static anonymity and it should be easy to identify the attacker when the KPC is involved. This can be done by choosing a reasonable $P\{a+|A\}$ and a large total number of vehicles.

Upon a vehicle being reported lost, its key ring may be revoked to prevent possible attacks from this vehicle. To disable possible access from this vehicle, all keys in its key ring will be revoked. This will affect other vehicles since the same key is shared by multiple vehicles. Revoking one key will also prevent legitimate vehicles from using the same key for authentication. However, in the following, we show that the effect is very limited.

The probability of two vehicles sharing exactly a keys is:

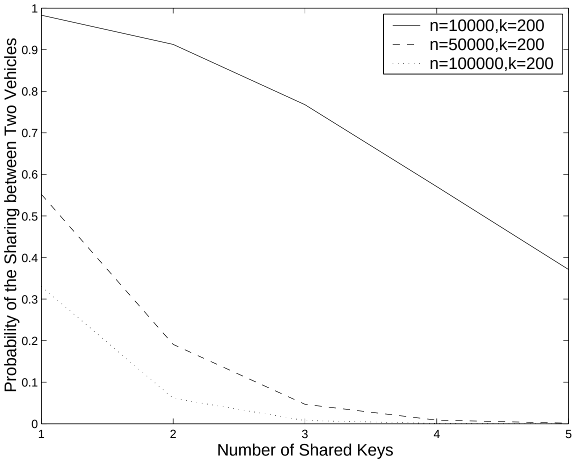
$$P\{a\} = \frac{C_k^a C_{n-k}^{k-a}}{C_n^k}$$

And the probability of two vehicles sharing at least a keys is:

$$P\{a+\} = \sum_{i=a}^{k} P\{i\}$$

Since a is small, we compute $P\{a+\}$ as:

$$P\{a+\} = 1 - \sum_{i=0}^{a-1} P\{i\}$$



The values of $P\{a+\}$ for different values of a are shown in Figure 5. It can be seen that for large values of n, the probability of two vehicles sharing more than three keys is very small. Thus revoking one vehicle will have minimum effect to other vehicles. If the KPC detects that another vehicle shares several keys with the vehicle being revoked, the KPC can invite the other vehicle to renew its key ring.

The choosing of parameters is complicated since it involves satisfying multiple constrains. However, we give some suggestions in this subsection. The essential privacy protection of our protocol is provided through a high probability of sharing one key between two random vehicles and a large key ring in each vehicle so that the number of combinations used for authentication is large. Consider that the number of combinations of choosing five keys out of a large key ring is already very large. For practical applications, we suggest that the number of keys used for each authentication is no greater than five. Also, we suggest that it should be at least three to make the number of combinations large enough.

Since the expected number of vehicles sharing common keys with a vehicle is mainly determined by $\frac{k}{a}$. The next step is to choose a proper size k for the key ring in each vehicle. The total key pool size n can always be decided afterwards. Delaying the decision for n can even give us one more benefit. The key pool does not have to be fixed at all time. It can grow over time to provide more flexibility. It can also purge expired keys over time. As long as we have a big enough window for all the vehicles, the desired anonymity can still be guaranteed.

5 Related Work and Discussions

Zarki *et al.* [16] address several security issues in vehicular networks focusing on system design, but lack in-depth analysis of privacy protection. Security and privacy of smart vehicles are studied in [7]. This work proposes to use electronic license plates and tamper-proof GPSes to preserve security and privacy, which can be used in our design to strengthen the security and privacy; so their work complements our protocol. Raya and Hubaux also explore the security issues in vehicular ad hoc networks [11]. They analyze attack models and some concrete attacks, then propose a set of security protocols for vehicular ad hoc networks. They also design a key changing algorithm to preserve anonymity and minimize the storage costs of the public keys. Different from their principle of using public keys, we choose symmetric key based random key-set approach to provide privacy, which is expected to be a lightweight authentication protocol. However, which one is better in terms of performance is not clear, and deserve further study.

In [6], the tracking problem in location-based systems is discussed. The general approach is to mix a car's path with other cars' path so that the precise path can not be determined. Our approach is similar. However, the mixing in our approach happens at the OBU, giving the privacy control back to the user. In [5], location privacy protection through k-anonymity approach is proposed. The authors mainly addressed the privacy problem in location-based services. This is different from the problem we are addressing. Our work can be complementary to their work by hiding the identity of the user. Also, our approach does not require any anonymization infrastructure.

In [2], the author propose to use pseudonyms to separate identity and service usage. The pseudonyms are distributed by a central authority. The relation between the pseudonyms and an identity is kept as a secret and only disclosed when attacks are being detected. Our approach can be viewed as a generalization of multiple identities. In fact, the symmetric keys in our approach can be readily substituted by certificates. We enhanced such multiple identities-based schemes through shared identities to provide limited anonymity. We also used combinations of multiple identities to further enhance the privacy. In [1], the authors also propose to use pseudonyms to preserve privacy in vehicular networks. The pseudonyms are generated through a time-dependent hash function. The system consists of two tiers: long term handles and short terms pseudonyms. The use of the two tiers obscures the vehicles' identities. Our approach provides comparable unlinkability as their approach. In addition, our approach provides a limited anonymity.

Preserving vehicle location privacy through unlinkability is addressed in [13]. The authors systematically discuses possible location privacy disclosure through communications between the mobile vehicle and the network. Random silent period and group formation are two basic mechanisms proposed to hide a single vehicle's path. Our approach instead focuses on the authentication problem and its associated privacy disclosure. Based on our approach, the above two mechanisms can be readily applied to further enhance the privacy protection of our protocol.

Sha *et al.* introduce the notion of adaptive privacy and propose a group-based authentication protocol, in which public key cryptography technique is used [14]. This work shares the same goal as theirs, however, we focus on symmetric key based approach, which has the potential of being a lightweight approach. Our next step will be evaluating the proposed approach in a comprehensive way and comparing its pros and cons with the approach proposed in [14].

6 Conclusion

In this paper, we propose to use random key-set for anonymously authenticating vehicles into vehicular networks. We take advantage of the shared keys between different random sets to achieve anonymity. The anonymity is further enhanced by using independent keys for authentications at neighboring RSUs. A corresponding system architecture and authentication protocol are described. Practical issues like identifying attackers and key revocation are also considered. Some possible optimizations which are useful for system deployment are discussed. The preliminary theoretical analysis of our protocol shows that it indeed has desirable properties of a practical privacy-preserving authentication protocol. Our next step will be systematically evaluating our proposal.

References

[1] J. Choi, M. Jakobsson, and S. Wetzel. Balancing auditability and privacy in vehicular networks. In *Proceedings of the 1st ACM international workshop on Quality of Service and Security in Wireless and Mobile Networks*, Oct. 2005.

[2] F. Dötzer. Privacy issues in vehicular ad hoc networks. In *Proc. of the 2nd ACM international workshop on Vehicular ad hoc networks*, Sept. 2005.

[3] Dedicated short range communications (dsrc). `http://grouper.ieee.org/groups/scc32/dsrc/`.

[4] L. Eschenauer and V. D. Gligor. A key management scheme for distributed sensor networks. In *Proceedings of ACM CCS'02*, Oct. 2002.

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

[6] B. Hoh and M. Gruteser. Protecting location privacy through path confusion. In *IEEE/CreateNet Intl. Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, Sept. 2005.

[7] J.Hubaux, S. Capkun, and J. Luo. The security and privacy of smart vehicles. *IEEE Security and Privacy*, 4(3):49–55, 2004.

[8] T. Mak, K. Laberteaux, and R. Sengupta. A multi-channel vanet providing concurrent safety and commercial services. In *Proc. of the 2nd ACM international workshop on Vehicular ad hoc networks*, Sept. 2005.

[9] B. Parno and A. Perrig. Challenges in securing vehicular networks. In *Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV)*, Nov. 2005.

[10] A. Pfitzmann and M. Kohntopp. *Anonymity, Unobservability and Pseudonymity – A Proposal for Terminology*. Springer-Verlag, 2001.

[11] M. Raya and J.-P. Hubaux. The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, Nov. 2005.

[12] D. B. Reid. An algorithm for tracking multiple targets. *IEEE Transactions on Automatic Control*, 24(6), 1979.

[13] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuuray, and K. Sezaki. Caravan: Providing location privacy for vanet. In *Embedded Security in Cars (ESCAR)*, Nov. 2005.

[14] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang. Adaptive privacy-preserving authentication in vehicular networks. In *Proceedings of the International Workshop on Vehicle Communication and Appliations*, Oct. 2006.

[15] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang. Enforcing privacy using symmetric random key-set in vehicular networks. Technical Report MIST-TR-2006-011, Wayne State University, Oct. 2006.

[16] M. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security issues in a future vehicular network. In *Proc. of EuroWireless 2002*, Feb. 2002.