A Survey on Conditional Privacy in Vehicular Adhoc Networks

Anitha Christy Angelin.P, John Moses

Abstract— Conditional Privacy preservation in VANETs (Vehicular Ad-hoc NETworks) must be achieved in the sense that the user related privacy information, including the driver's name, the license plate, speed, position, and travelling routes along with their relationships, has to be protected. The authorities should be able to reveal the identities of message senders in the event of a traffic dispute, such as a crime/car accident scene investigation. Therefore, it is critical to develop a conditional privacy preservation scheme in a VANET before it can be practically launched.

Index Terms—VANET, RSU, CA, ECPP, Pseudonym, OBU.

1 INTRODUCTION

Vehicular Networks (also known as VANETs) are the basis for the Intelligent Transportation Systems (ITS). It enables the vehicles to communicate with each other via Inter-Vehicle Communication (IVC) as well as with road-side base stations via Roadside-to-Vehicle Communication (RVC).By doing this they give an accurate information about the vehicles to the drivers and the authorities.The architecture is shown in Fig 1.Among the key issues in vehicular ad-hoc networks (VANET'S) ,security assurance and privacy preservation are two primary concerns. Without the security and privacy guarantee, serious attacks may jeopardize the benefits by the improved driving safety since an attacker could track the locations of the interested OBUs and obtain their moving patterns. Therefore, how to provide anonymous safety message authentication has become a fundamental design requirement in securing vehicular networks. However, anonymous message authentication in vehicular networks is a double-edge sword. A well-behaved OBU, due to the privacy protection mechanism, is willing to offer as much local information as possible to its neighbouring OBUs and RSUs to create a safer and more efficient driving environment. However, a maliciously-behaved OBU may abuse the privacy protection mechanism by damaging the regular driving environment. This particularly happens when a driver who is involved in a dispute event of safety messages may intend to escape from the investigation and responsibility. Therefore, the anonymous message authentication in vehicular networks should be conditional, such that a trusted authority can find a way to track a targeted OBU and collect the safety messages it has disseminated, even though the OBU is not traceable by the public.

Most of the existing security proposals for secure vehicular networks were simply for authentication with privacy preservation without an effective and efficient conditional tracking mechanism. To the best of our knowledge, only two reported schemes, which was based on a huge number of anonymous keys (denoted as HAB in the following context) and a pure group signature technique (denoted as GSB in the following context) , respectively, have targeted at the design of conditional privacy preservation. Although both HAB and GSB can provide an efficient tracking mechanism, they fall short in the aspects of requiring a huge storage for anonymous keys and safety message anonymous authentication. This problem becomes essentially fatal when the revocation list, which keeps all the revoked anonymous keys, is large. Note that when a signature is being verified, the validity of the public key should also be authenticated, which is, however, not as easy in the vehicular networks as that in wired networks.+

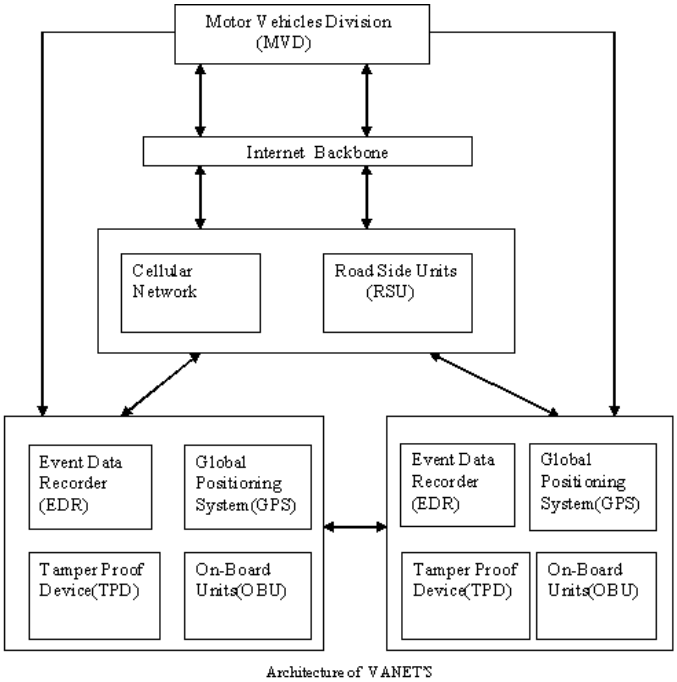

Fig (1)

- *Anitha Christy Angelin is currently working as an Assistant Professor in Karunya Univesity, Coimbatore, India, PH-9585248823. E-mail: anitha.angelin@yahoo.com*
- *John Moses is currently pursuing masters degree program in Network and Internet engineering in Karunya University, Coimbatore, India, PH-9486768698. E-mail: john.moses63@gmail.com*

2 EXISTING CONDITIONAL PRIVACY PRESERVATION PROTOCOLS

2.1 ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications

The Efficient conditional privacy preservation (ECPP) [1] protocol for secure vehicular communications can efficiently deal with the growing revocation list while achieving conditional traceability by the authorities. Instead of relying on a huge storage space at each OBU as most of the previously reported schemes did, the proposed protocol can keep the required anonymous key storage minimal without losing the security level. Meanwhile, the proposed protocol gains merits in the fast verification on safety messages and an efficient conditional privacy tracking mechanism, which can serve as an excellent candidate for the future VANETs.

2.2 Group Key Management Protocol (GKMP)

Roads are divided into cells that define groups, with the group leader being the vehicle closest to the cell In addition to the encrypted keys, the group leader includes hashes (e.g., *HA*) of the receivers' public keys to help the receivers identify which encrypted group key [2] to decrypt. A simple hash comparison suffices to achieve this When a vehicle leaves the cell, nothing needs to be done. Special attention needs to be paid to exchanges on cell boundaries when a vehicle switches from one group to another. In order to make this operation smooth, cell dimensions should be smaller than the diameter of the transmission range disk. For example, if the transmission range is 300 m, the disk diameter is 600 m, we can choose a cell size of 400 m. Hence, at the cell boundaries, a vehicle will receive messages from the leaders of both its previous and new groups.

2.3 Distributed Revocation Protocol (DRP)

The DRP protocol is used in the pure ad hoc mode where by vehicles accumulate accusations against misbehaving vehicles, evaluate them using a reputation system and, in case misbehaviour is detected, report them to the CA once a connection is available. Unlike RTPD and RCCRL, the revocation in DRP is triggered by the neighbors of a vehicle upon the detection of misbehaviour. The main principle of DRP is that the neighbours of the attacker vehicle take care of detecting and temporarily revoking it.

2.4 A Secure and Privacy-Preserving Protocol for Vehicular Communications

A secure and privacypreserving protocol for VANETs is introduced by integrating the techniques of **G**roup **S**ignature and **I**dentity (ID)-based **S**ignature called (GSIS) [4]. Security problems are divided into the following two aspects: security and privacy preservation between OBUs and OBUs [11], as well as that between the OBUs and the RSUs, in light of their different design requirements. In the first aspect, group signature is used to secure the communication between OBUs and OBUs, where messages can securely and anonymously be signed by the senders, while the identities of the senders can be recovered by the authorities. In the second aspect, a signature scheme using ID-based cryptography (IBC) is adopted in the RSUs to digitally sign each message launched by the RSUs to ensure its authenticity, where the signature overhead can greatly be reduced. OBUs that are installed in emergency vehicles will be treated in the same way as the RSUs, since it is unnecessary to protect the privacy of both the RSUs and the OBUs installed in emergency vehicles

2.5 VANET Authentication using Signatures and TESLA++ (VAST) protocol

VANET Authentication using Signatures and TESLA++ (VAST), which uses a combination of ECDSA signatures and TESLA++ to verify each packet. TESLA++ provides an efficient DoS resilient authentication mechanism to verify legitimate packets and filters out the majority of malicious or spurious messages. Under VAST, the digital signature is authenticated using TESLA++ before it is verified, preventing the majority of computational and memory-based DoS attacks. Authenticated signatures prevent attackers from broadcasting invalid signatures while posing as other VANET entities.

2.6 The Baseline Pseudonym approach (BP)

In Baseline Pseudonym approach, each node (vehicle) V is equipped with a set of pseudonyms, that is, public keys certified by the CA without any information identifying V. For the i-th pseudonym KiV for node V , the CA provides a certificate CertCA(KiV), which is simply a CA signature on the public key KiV .The private key kiV corresponding to the pseudonym KiV is used by the node to digitally sign messages. To enable message validation, the pseudonym and certificate of the signer are attached in each message.

2.7 Adversarial Parsimony approach

In short, parsimony assumes that an attack involving a few malicious nodes is more likely than an attack that requires collusion between a large number of nodes. Given this adversarial model, a node will always look for a way of restoring consistency based on the simplest possible explanation for the disagreement. This often resolves to assuming the smallest possible number of corrupt nodes, and hence, nodes often need to be able to tell at least some other nodes apart from one another. Without that ability, a malicious node can create additional ¯ctitious nodes to bolster its view of the VANET.

2.8 Trusted Component Approach (TC)

Implementing security for vehicular communications requires the vehicles to be equipped with a Trusted Component (TC). Many vehicles are already equipped with components, such as speed limiters, taco graphs, and event data recorders (EDRs), considered critical by manufacturers and legislators. We assume that nodes are equipped with a Trusted Component,i.e., tamper-resistant hardware and _rmware. The main role of the TC is to store sensitive cryptographic material (e.g., private keys) and to perform cryptographic operations using that ma-

terial. For this reason, the TC must have a processing unit, a memory module, and some non-volatile storage.

2.9 Mix Zone Approach

We consider a continuous part of a road network, such as a whole city or a district of a city. We assume that the adversary installed some radio receivers at certain points of the road network with which she can eavesdrop the communications of the vehicles, including their heart beat messages, in a limited range. On the other hand, outside the range of her radio receivers, the adversary cannot hear the communications of the vehicles. Thus, we divide the road network into two distinct regions: the observed zone and the unobserved zone. Physically, these zones may be scattered, possibly consisting of many observing spots and a large unobserved area, but logically, the scattered observing spots can be considered together as a single observed zone. There are various metrics to quantify the level of privacy provided by the mix zone [10] (and the fact that the vehicles continuously change pseudonyms). A natural metric in our model is the success probability of the adversary when making her decision as described above. If the success probability is large, then the mix zone and changing pseudonyms are ineffective. On the other hand, if the success probability of the adversary is small, then tracking is difficult and the system ensures location privacy.

2.10 Silent Period Approach

Random Silent Periods[9] are randomly chosen periods which vehicles are forced to remain silent. During silent periods, vehicles have no incoming or outgoing messages using VANET and cannot access location base servers. Silent periods should be placed after the process of updating pseudonyms and occur areas with heavier traffic. The disadvantages to this are vehicles can still be tracked due to time and space relations. If the silent period range longer that some x amount of feet could affect the safety and liability of drivers given there was an emergency that needed to be reported.

2 Discussions

TABLE 1 COMPARISON OF DIFFERENT CONDITIONAL PRIVACY SCHEMES

No.	Protocols used	Merits	Demerits
1	ECPP	The ECPP protocol gains merits in the fast verification on safety messages and an efficient conditional privacy tracking mechanism	It has high RSU latency and it takes longer time to search for revoked node.
2	GKMP	The attacker cannot alter the protocol function by changing the protocol itself..	It does not function properly at all times.
3	DRP	The revocation in DRP is triggered by the neighbours of a vehicle upon the detection of misbehaviour rather than the vehicles itself.	It is not a real re-vocation protocol but rather a warning system against attackers
4	Secure and privacy preserving protocols for vehicular communication.	The messages can securely and anonymously be signed by the senders, while the identities of the senders can be recovered by the authorities..	The Signature overhead is high.
5	VANET Authentication using Signatures and TESLA++ (VAST) protocol	Even under heavy loads VAST is able to authenticate 100% of the received messages within 107ms.	It is not flexible enough to meet all of the properties of VANET'S
6	The Baseline Pseudonym approach (BP)	They can generate their own pseudonyms without affecting the system security.	The size of CRL is much higher and there is a need for complex management
7	Adversarial Parsimony approach	If all the data agrees with the model (perhaps with high probability), the node accepts the validity of the data.	There is always a possibility for nodes to slightly spoof their locations and remain undetected.

8	Trusted Component Approach (TC)	Higher protection levels can be introduced.	The system may be subjected to tampering, which results in a large vulnerability window.
9	Mix Zone Approach	An adversary cannot track the vehicle with in the mixed zone.	The Vehicles cannot cross the border with in the mixed zone.
10	Silent Period Approach	It prevents attackers from linking transmission to a particular vehicle after an intersection.	In this approach privacy is little bit compromised for safety.

4 CONCLUSIONS

The survey helps in understanding the Conditional Privacy Preservation Protocols and approaches that are available for Preserving Privacy of Vehicles in VANET'S. With the numerous amounts of Privacy Preservation Protocols and approaches, a clear idea is provided for how the privacy is preserved for vehicles in VANET'S. The selection of Privacy Preservation Protocols and approaches depends on the Vehicle and the Road environment.

REFERENCES

[1] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc.* IEEE INFOCOM, Apr. 2008, pp. 1229–1237.

[2] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," J. Comput.Security, vol.15, no. 1, pp. 39–68, Jan. 2007.

[3] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing vehicular communications,"IEEE Wireless Commun., vol. 13, no. 5, pp. 8–15, Oct. 2006.

[4] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications,"IEEE Trans.Veh.Technol., vol.56, no.6, pp.344–345, Nov.2007.

[5] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *J. Commun. Netw.*, vol. 11, no. 6, pp. 574–588, 2009.

[6] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux Antonio Lioy, "Efficient and Robust Pseudonymous Authentication in VANET,"VANET'07, 10 September, (2007).

[7] P. Golle, D. Greene and J. Staddon, Detecting and correcting malicious data in VANETs, in: *Proceedings of VANET'04*, 2004, pp. 29–37.

[8] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, M. Raya "Architecture for Secure and Private Vehicular Communications''in Telecommunications, ITS, vol.5, no.6, pp.1-6 ,June/July 2007.

[9] L.Butty´an,T.Holczer,I.Vajda,"On the effectiveness of changing pseudonyms to provide location privacy in VANETs"In Proc.of Privacy in Ad hoc and Sensor Networks (ESAS 2007).

[10] Hang Dok, Huirong Fu, Ruben Echevarria, and Hesiri Werasinghe, "Privacy Issues of Vehicular Ad-Hoc Networks" in International Journal of Future Generation Communication and Networking Vol. 3, No. 1, March , 2010.

[11] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux," Secure vehicular communications: design and architecture", IEEE Communications Magazine, vol. 46, no. 11, pp. 100-109, November 2008.