Security and Privacy Enabling Lightweight Solution for Vehicular Networks

Upasana Singh
Computer Science and Engineering
NIT Hamirpur
Hamirpur, INDIA
upasananith@gmail.com

Pardeep Singh
Computer Science and Engineering
NIT Hamirpur
Hamirpur, INDIA
pardeep@nitham.ac.in

Abstract— Vehicular Ad-Hoc Network (VANET) is an emerging area of wireless networks which allows vehicles to communicate enabling Intelligent Transportation System (ITS). Immense amount of research is going on both by industry and academia. In vehicular communication there occurs frequent handover because of the high speed of vehicles and hence there is always a requirement of secure and fast authentication for a seamless handover to take place. In this paper we propose an authentication scheme that will not only provide security and privacy but also will reduce the storage and communication overhead increasing the efficiency.

Keywords— Vehicular Networks, Security, Privacy, Authentication, VANET.

I. INTRODUCTION

VANET is a very promising technology regarding the traffic safety and efficiency including several other applications like public services and infotainment. In present scenario vehicles are not only envisioned to communicate between each other, but also to get information from and send data to infrastructural units. Many R & D groups have shown enormous amount of interest in development of this technology. The CAR 2 CAR communication Consortium, SAFESPOT, eSAFETY, PReVENT, EASIS, SEVECOM are some of the European Initiatives. The vehicles and the Road Side Units (RSU) are equipped with On-Board processing and wireless communication modules. The vehicular communication could be Intra-Vehicular communication or Inter-Vehicle Communication. In Intra-Vehicular communication the On-Board Unit (OBU) communicates with several Electronic Control units (ECU). The Inter-Vehicular Communication could be Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. Since a rich set of tools are offered to drivers and authorities, but a formidable set of exploits and attacks becomes possible. Hence, the security of vehicular networks is indispensable, because these systems can make anti-social and criminal behavior easier, in ways that will actually jeopardize the benefits from their deployment [24]. Vehicular communication is vulnerable to several kind of attacks like Jamming in which the attacker purposely generates interfering transmissions that prevent communication; an attacker might forge and transmit false hazard which are taken up by all vehicles in both traffic streams; attackers can replay messages, impersonation where an attacker masquerade of an emergency vehicle to mislead other vehicles to slow down and yield or impersonate a roadside units, spoofing service advertisements or safety messages; the attacker may select to alter the data at their source, tampering with the on-board sensing and other hardware will be relatively simple. And hence there are various requirements that must be met in order to have secure vehicular communication:

-Message Authentication and Integrity.
-Message Non-Repudiation
-Entity Authentication
-Message Confidentiality
-Privacy and Anonymity

The paper is organized in the following way: Section II describes the related work. In Section III system model and problem statement are described. Our proposed solution is given in Section IV and security analysis in V. Finally section VI concludes the paper.

II. RELATED WORK

Security related problems have been discussed by many researchers. Blum and Eskandarian[8] propose a secure communications architecture based on a public key infrastructure (PKI) and a virtual network controlled by cluster-heads intended to counter the so-called "intelligent collisions", which are collisions intentionally caused by malicious vehicles. This approach produces a remarkable overhead and the use of cluster-heads can create bottlenecks. Gollan and Meinel [4] propose the use of digital signatures along with GPS technology to identify cars securely, improve the fleet management, and provide new applications for the private and the public sector. Considering the problem from a different point of view, Hubaux et al. [5] emphasize the importance of privacy and secure positioning, and propose the use of Electronic License Plates (ELP) to identify vehicles. Although they recognize the importance of conditional privacy, they do not provide any specific solution to the problem. To the best of our knowledge, there are few articles that consider both security and conditional privacy preservation in VANETs. In this line, Raya and Hubaux [3] gave a foundational proposal of using pseudonym based approach using anonymous certificates and the public key infrastructure (PKI).The anonymous

certificates are used to hide the real identities of users. This scheme required extra communication and had storage overhead. Also privacy could be invaded by logging the messages containing a given key and tracking the sender until her identity is disclosed. To avoid this attack, the authors proposed to use frequently updated anonymous public keys to fulfill the user's privacy requirements. However, this solution required storing large number of key pairs, hence making the secure distribution of keys, key management, and storage very complex; so this type of scheme should be avoided for the sake of practicality.

Lin et al. [6] presented GSIS, which is a conditional privacy-preserving scheme using group signatures [9], [10], and ID-based signatures [12]. In it a single membership manager is used to issues secret member keys to the vehicles. The conditional anonymity claimed applies only to the vehicles amongst the peer, with an assumption that the infrastructure points are trusted. Lu et al. [7] proposed an alternative way to overcome the limitation of pre-storing a large number of anonymous certificates while preserving conditional privacy. They proposed a group signature based scheme, making an assumption that vehicles and RSUs are able to collaborate actively. Every vehicle gets a short-time anonymous certificate from a RSU after running a Two-round protocol when passing by the RSU. In order to prevent link ability of the messages, the vehicle should change the anonymous certificate regularly by interacting with RSUs. These frequent interactions may affect the network's efficiency.

It is also worth mentioning the schemes in [13], [14], which also rely on RSUs. In [13], the method of mix-zones is used to enhance the anonymity of vehicles. However, this scheme still relies on pre-loading a large set of anonymous certificates in each vehicle. In [14], by exploiting a keyed hash message authentication code (HMAC), a scheme with low communication overhead is proposed for secure vehicle communication. This scheme requires a vehicle to obtain a symmetric key from an RSU using a key agreement protocol. In order to protect its privacy, the vehicle should use different public keys to communicate with the RSUs. Hence, the vehicle still needs to pre-load a certain number of anonymous certificates. As to robustness, the schemes in [13], [14] fully rely on RSUs. If an RSU collapses, then these schemes will not work any more.

Some other group signature based schemes are proposed in [15], [7], [16], where signer privacy is conditional on the group manager. They have the problem of identity escrow, i.e. the group manager could reveal the identity of any group member. The group based schemes could not be applied properly due to certain limitation as the difficulty in election of group leader due to the non-availability of a trusted entity among the peer vehicles; also there may be too few cars in the vicinity to create a group.

An ID-based security framework for VANETs is proposed by Kamat et al: [17], [18] to provide authentication, non-repudiation, and pseudonymity. However, their framework is limited by the strong dependence on the infrastructure for short-lived pseudonym generation, which renders the signaling overhead overwhelming. The proposed nonrepudiation scheme enables a single authority to retrieve the identity which may raise the concern on potential abuse. Schemes leveraging pseudonyms in VANETs can also be found in [19], [20] with the revocation feasible in limited settings, and in [21] where the certificate authority maintains mapping from an identity to the set of vehicle-generated pseudonyms.

By using ID-based cryptography [12] to avoid complicated certificate management, [14] designed an efficient conditional privacy-preserving protocol for vehicular communications. Their approach relies on tamperproof devices embedded in the vehicles. The system's master key is stored in those tamper-proof devices so that pseudoidentities can be generated locally. Storing the system's master key in each vehicle may expose the system to powerful attackers and unpredictable risks even if the storage devices are assumed to be tamper-proof. Those expensive tamperproof devices can prevent attackers from reading the secrets physically stored in them. However, since the system's master key will be involved in local computations, the attacker has the chance to measure the energy (or time) consumed by the computations, and the emitted electronic radiation, which contains information about the secret. With this information and by means of statistical methods, the attacker can launch powerful key extraction attacks such as side channel attack [22], [23], which are well-known in cryptography. Although the side channel attack may be expensive to regular users, it is attractive and practical to organized criminals since, once the master key is extracted, they have full control over the system [2].

In some more recent works the use of ECC (Elliptic Curve Cryptography) is seen like [2] bilinear map along with ECC is used and they focused on group based solution. Sun et al. [1] proposed solution based on ID-based cryptography in order to avoid the use of certificates. M. Raya pints out the drawbacks of asymmetric cryptography as; using ECC (Elliptic Curve Cryptography), the most compact public key cryptosystem so far, the estimated security overhead of the signature and certificate is around 140 bytes.

So it shows that asymmetric cryptography based solutions using certificates and signatures are secure but generate computational and storage overhead. Also group based schemes cannot be employed efficiently because of the reasons already discussed.

III. SYSTEM MODEL AND PROBLEM STATEMENT

A. System Model

Vehicular networks consist of several entities.

-TA: A Trusted Authority which could be a law enforcement authority (or a group of authorities) could trace and disclose the identity in case of accident or crime.

-AAA server: It is authentication, authorization and accounting server which authenticates the vehicle when it first enters the network and establishes the keys to be used.

-RSU: Road side units which ac as the access points or access routers.

-The OBUs are installed on vehicles, RSUs and AAA server. In order to have seamless mobility and support the infotainment applications the network is FMIPv6 based.

B. Problem Statement

1. The OBUS have less storage and computational power than the RSU.

2. Even though tamperproof OBUS could be used to secure the data stored and prevent the attacker from reading it but while communication the energy could be intercepted.

3. In asymmetric cryptography like ECC (Elliptic Curve Cryptography), the most compact public key cryptosystem so far, the estimated security overhead of the signature and certificate is around 140 bytes.

4. The vehicles are highly mobile and hence have very less time to connect to a new RSU. The time to complete the handover is dependent on the number of messages exchanged during the handover.

IV. OUR SOLUTION

In our solution we will be using terms vehicle and mobile node interchangeably similarly Access router (AR) and Road Side Unit (RSU) interchangeably. We have divided the Solution in three phases starting with mutual authentication and Key agreement phase, next verification phase and the handover phase.

Each vehicle is given a unique identity UID and password PSW by the TA. When the vehicle enters a network it enters UID and PSW in the OBU which generates a pseudoidentity ID_A as;

ID_A= (UID $\oplus$ PSW).

A. Mutual Authentication and Key agreement:

1. The AAA server chooses two large primes p and q and keeps them secret, it than computes $n = (p.q)$.
2. When the vehicle first enters the network it sends ID_A to the AAA server. AAA server than computes $J_A = f(ID_A)$ and sends J_A to the vehicle.
3. AAA chooses a secret s such that $1 \le s \le n-1$. Than

   Computes $v = (J_A.s)^2 \bmod n$ which is the Vehicles public **key.**
4. AAA selects and sends a shared secret 'g' to the vehicle.
5. Both AAA server and vehicle choose respective secret numbers a and b such that $1 \le a$ and $b \le g-2$ each co-prime to g-1. They respectively compute $a^{-1} \bmod g-1$ and $b^{-1} \bmod g-1$.
6. AAA server chooses a secret K such that $1 \le k \le g-1$, and computes $(k.a) \bmod g$ and sends to the vehicle.
7. Vehicle than multiplies the received value by b and sends it to AAA.
8. AAA than multiplies the received value by $a^{-1} \bmod g-1$ which undoes its previous multiplication and sends it back to the vehicle.
9. Vehicle than multiplies the received value by $b^{-1} \bmod g-1$ which results in $K \bmod g$.

   This $K \bmod g$ is the shared secret key between the AAA and the vehicle which is used as the Master key (MK). This key will not be used for any kind of encryption it will only be used for deriving handover encryption key.
10. The AAA computes handover encryption key (HEK) using the MK as $HEK = (MK||ID_{MN}||ID_{AR})$ and sends the HEK to the corresponding AR .

B. Verification Phase:

Before the vehicle attaches to the new RSU and disconnects from the previous one, previous RSU is responsible to send V's related authentication information to the new one. Whenever a vehicle enter the vicinity of an RSU and have to communicate its identity must be verified. Verification steps are as follows:

1. Vehicle sends ID_A and $x = (J_A.r)^2 \bmod n$ to the NAR(RSU) .
2. NAR than randomly select a challenge bit e=0 or 1 and send to vehicle.
3. The vehicle than compute $y=(ID_A.r) \bmod n$ if e=0 and if e=1 than $y = (ID_A.r.s) \bmod n$ and sends it to NAR.
4. NAR than computes J_A from ID_A using f and $y^2 = (x.v^e) \bmod n$. If both the values of y received and calculated are same than the verification is successful.

C. Handover Phase:

1. The MN sends RtSolPr request to the PAR to which it is already connected for the information of the available ARs.
2. The PAR than sends the information of the ARs to which the MN could attach via PrRtAdv.
3. When the MN selects NAR to which it wants to connect it sends;

Msg1= HEK(ID_{MN}, ID_{PAR}, ID_{NAR}, $Nonce_{MN}$), H(HEK, ID_{MN} || ID_{PAR} || ID_{NAR} || $Nonce_{MN}$) along with the verification request.

4. NAR on receiving Msg1 from MN firstly verifies the MN and than responds with
   Msg2= HEK(ID_{MN}, ID_{PAR}, ID_{NAR}, $Nonce_{MN}$, $Nonce_{NAR}$), H(HEK, ID_{MN} ||ID_{PAR} || ID_{NAR} || $Nonce_{MN}$ || $Nonce_{NAR}$) .
5. After exchanging message Msg1 and Msg2 the Handover key HK it be computed by the MN using a one way hash function;
   HK = (HEK, ID_{MN} || ID_{NAR} || $Nonce_{MN}$ || $Nonce_{NAR}$)
   which will be used further during Handover.
6. The MN will send FBU (Fast Binding update) message to the PAR along with some MAC (Message Authenticated Code) i.e. FBU, H(HK, NCoA, NonceNAR).
7. PAR than sends handover initiation HI message along with received MAC i.e. HI, H (HK, NCoA, NonceNAR).
8. On receiving the message NAR generates HK and verifies if what is received is same and if the verification is successful it sends Hack (Handover acknowledgement) to the PAR.
9. PAR responds with an FBack (Fast Binding Acknowledgement).
10. MN on attaching to the NAR transmits FNA (Fast Neighbor Advertisement) to the NAR to inform its presence.

V. SECURITY ANALYSIS

Our solution provides Identity privacy and anonymity via the use of pseudoidentity. Mutual authentication of MN and NAR is guaranteed via HK. Secrecy is achieved as Msg1 and Msg2 exchanged between MN and NAR are kept secret from an adversary. HK is only shared between MN and NAR. Neighbor ARs can not derive HK and the key is kept secret from the attackers.Msg1 and Msg2 exchanged between MN and NAR cannot be altered by the attacker and hence integrity is achieved.

Denial of Service attack: Our proposal suggests a secure binding update authentication scheme using a security association between AR and MN. The scheme provides not only mutual authentication between MN and ARs, but also guarantees secrecy between ARs.

Know-key Security: If the attacker have intercepted the previous session key, still he can't use them to derive new session keys as both vehicle and RSU both generates new nonce for every new session, and in addition protected by the secure hash function. Hence our solution is secure against any adversary known key attacks.

Passive attack: A passive attack is possible if the attacker tries to guess the session key based on the information available publically. Even if the attacker performs a passive attack, he can't succeed as after verification both vehicle and the RSU will compute their session keys based on their secret shared information and the attacker could not compute. Therefore the proposed protocol resists against the passive attack.

Man in middle attack: It is a kind of active attack. Since no information about the secret key is revealed so the solution is safe against the man in middle attack.

VI. CONCLUSION

Vehicular networks are the vital solution to secure and efficient transportation system proving different types of applications to the vehicles. In order to take full advantage of the vehicular networks the communication must be secured meeting all the security requirements. Our proposed solution provides security and privacy both using symmetric key cryptography reducing the computation and storage required. Also, it enables to reduce the handover latency by reducing the number of messages exchanged with AAA server to zero.

REFERENCES

[1] J. Sun, C. Zhang, Y. Zhang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks", *IEEE Trans. Parallel and Distributed System 2010*, Vol. 21, No. 9, p 1227-1239.

[2] L. Zhang, Q. Wu, A. Solanas, "A Scalable Robust Authentication Protocol for secure Vehicular Communication", *IEEE Trans. Vehicular Technology 2010*, Vol. 59, No. 4, p 1606-1617.

[3] M. Raya, J. Hubaux, 'Securing vehicular ad hoc networks', Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks 2007, Vol. 15, No. 1, p 39–68.

[4] L. Gollan, C. Meinel, "Digital Signatures for Automobiles", *Technical Report, Institute for Telematike 2004*, Vol. 6, No. 1,p 24-29.

[5] J. Hubaux, J. Luo, "The security and privacy of smart Vehicles", *IEEE Journal on Security and Privacy 2004*, Vol. 2, No. 3, p 49-55.

[6] X. Lin, X. Sun, P. Ho, "GSIS: A secure and privacy preserving protocol for vehicular communications", *IEEE Trans. Vehicular Technology 2007*, Vol. 56, No. 6, p 3442-3456.

[7] R. Lu, X. Lin, X. Zhu, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications", *IEEE INFOCOM 2008*, pp. 1229-1237.

[8] J. Blum, A. Eskandarian, "The threat of intelligent collisions".

[9] D. Boneh, M. Franklin,"Identity-based encryption from the Weil pairing", *Journal on Advances in Cryptology-CRYPTO 2001, Lecture Notes in Computer Science*, Vol. 2139, p 213-229.

[10] D. Chaum, E. Van Heijst, "Group signatures", Advances in Cryptology 1991, *Lecture Notes in Computer Scienc*e, Vol. 576, p 257-265.

[11] T. W. Chim et al, 'SPEC: Secure and Privacy enhancing communications schemes for VANETs", *Journal on Ad Hoc Networks (2010)*, doi: 10.1016/j.adhoc.2010.05.005.

[12] A. Shamir, "Identity based cryptosystems and signature schemes", *Lecture Notes in Computer Science 1984*, Vol. 196, p 47-53.

[13] J. Freudiger, M. Raya, M. Feleghhazi, "Mix zones for location privacy in vehicular networks", *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), 2007*.

[14] C. Zhang, R. Lu, X. Lin, An efficient identity based batch verification scheme for vehicular sensor networks, in *Journal IEEE INFOCOM 2008*, p 246-250.

[15] X. Lin, X. Sun, P. Ho, "GSIS: A secure and privacy-preserving protocol for vehicular communications", *IEEE Trans. Vehicular Tech. 2007*, Vol. 56, No. 6, p 3442–3456.

[16] A. Studer, E. Shi, F. Bai, "TACKing together efficient authentication, revocation, and privacy in VANETs", Proc. 6th Annual IEEE SECON Conference (SECON'09), 2009.

[17] P. Kamat, A. Baliga, W. Trappe, "An identity-based security framework for VANETs", *Proc. 3rd ACM Int'l Workshop on Vehicular Ad Hoc Networks, VANET'06*, p 94–95.

[18] P. Kamat, A. Baliga, W. Trappe, "Secure, pseudonymous, and auditable communication in Vehicular Ad Hoc Networks", *Journal on Security and Communication Networks* 2008, Vol. 1, No. 3, p 233–244.

[19] J. Sun, C. Zhang, Y. Fang, "An id-based framework achieving privacy and non-repudiation", vehicular ad hoc networks in *Proc IEEE Military Communications Conf. 2007*, p 1–7.

[20] J. Sun, Y. Fang, "Defense against misbehaviour in anonymous vehicular ad hoc networks", *Journal on Ad Hoc Networks 2009*, Vol. 7, No. 8, p 1515–1525.

[21] G. Calandriello, P. Papadimitratos, J. Hubaux, "Efficient and robust pseudonymous authentication in VANET", *Proc. 4th ACM Int'l Workshop on Vehicular Ad Hoc Networks, VANET'07*, p 19–28.

[22] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems", in *Lecture Notes in Computer Science 1996*, Vol. 1109, p 104-113.

[23] F. Standaert, T. Malkin, M. Yung, "A unified framework for the analysis of side-channel key recovery attacks", in Lecture Notes in Computer Science 2009,Vol. 5479, p 443-461.

[24] M. Raya, P. Papadimitratos, J. Hubaux, "Securing Vehicular Networks".

[25] P. Papadimitratos, V. Gligor, J. Hubaux, "Securing Vehicular Communications - Assumptions, Requirements, and Principles".

[26] E. Schoch, F. Kargl, M. Weber, "Communication Patterns in VANETs", *IEEE Communications Magazine 2008*, p 119-125.