Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks

Surabhi Mahajan
Dept of Computer Enginnering
PEC University of technology
Chandigarh, India

Prof. Alka Jindal
Dept of I.T
PEC University of technology
Chandigarh, India

ABSTRACT
Since the last few years VANET have received increased attention as the potential technology to enhance active and preventive safety on the road, as well as travel comfort. Security and privacy are indispensable in vehicular communications for successful acceptance and deployment of such a technology. Generally, attacks cause anomalies to the network functionality. A secure VANET system, while exchanging information should protect the system against unauthorized message injection, message alteration, eavesdropping. In this paper, various security and privacy issues and challenges are discussed. The various authentication schemes in wireless LAN, VANETS are discussed. Out of various authentication schemes that are used to reduce the overhead in authentication, when roaming - *proxy re-encryption* scheme and new proxy re encryption scheme is reviewed in detail. A comparison between the two schemes is done, which shows that the privacy can be maintained better by using new proxy re encryption.

Categories and Subject Descriptors
Security necessities, privacy challenges, authentication schemes.

General Terms
Authentication using Proxy re-encryption

Keywords
Non- frame ability, Identity privacy**,** Location Privacy**,** delegators

1. INTRODUCTION
Vehicular ad hoc network (VANET) can offer various services and benefits to VANET users and thus deserves deployment effort. VANETs with interconnected vehicles and numerous services promise superb integration of digital infrastructure into many aspects of our lives, from vehicle-to-vehicle, roadside devices, base stations, traffic lights, and so forth. A network of a huge number of mobile and high-speed vehicles through wireless communication connections has become electronically and technically feasible and been developed for extending traditional traffic controls to brand new traffic services that offer large traffic-related applications. Safety information exchange enables life-critical applications, such as the alerting functionality during intersection traversing and lane merging, and thus plays a key role in VANET applications. The attractive features of VANETs inevitably incur higher risks if such networks do not take security into account prior to deployment. For instance, if the safety messages are modified, discarded, or delayed either intentionally or due to hardware malfunctioning, serious consequences such as injuries and even deaths may occur. Unlike traditionally wired networks are protected by several lines of defense such as firewalls and gateways, security attacks on such wireless networks may come from any direction and target all nodes. Therefore, VANETs are susceptible to intruders ranging from passive eavesdropping to active spamming, tampering, and interfering due to the absence of basic infrastructure and centralized administration. Moreover, the main challenge facing vehicular ad hoc networks is user privacy. Whenever vehicular nodes attempt to access some services from roadside infrastructure nodes, they want to maintain the necessary privacy without being tracked down for whoever they are, wherever they are and whatever they are doing. It is considered as one of the important security requirements that should be paid more attention for secure VANET schemes, especially in privacy-vital environment. A number of security threats to vehicular ad hoc networks have been addressed [2, 13, and 6]. In [7], Ray et al. introduced three kinds of security threats in VANETs, including attacks on safety-related applications, attacks on payment-based applications, and attacks on privacy.

2. RELATED WORK
Before proceeding to the details of the paper, we are first giving some details regarding security in VANET which is given below:

2.1 VANET Security Necessities
The security design of VANET should guarantee following:

1. Message Authentication, i.e. the message must be protected from any alteration.
2. Data integrity does not necessarily imply identification of the sender.
3. Entity Authentication, so that the receiver is not only ensured that sender generated a message, in addition has evidence of the liveness of the sender.
4. Conditional Privacy must be achieved in the sense that the user related information, including the driver's name, the license plate, speed, and position and traveling routes.
5. In some specific application scenarios, Confidentiality, to protect the network against unauthorized message injection, message alteration, and eavesdropping, respectively.

An important feature of VANET security is the Digital Signature as a building block [4]. Whether in inter-vehicle communications or communications through infrastructure,

authentication (using signatures) is a fundamental security requirement since only messages from legitimate senders will be considered. Signatures can also be used to guarantee data integrity (i.e., the message being sent is not modified). While fundamental to secure communications in many other networks, message confidentiality remains an option in VANETs depending on the specific. For instance, safety-related messages do not contain sensitive information and thus encryption is not needed [4].

2.2 Security aspects restricted to VANET

1. Position verification techniques to thwart position spoofing attacks.
2. Traceability by trusted network authorities (e.g., network administrator) for privilege revocation once misbehavior is detected.
3. Identity and location privacy preserving mechanisms against unlawful tracing and user profiling.
4. Non-frameability of an honest user who cannot be falsely accused of having misbehaved, 5. Detecting and correcting malicious data to ensure data consistency.
6. The system must have light overheads in terms of computational costs and high efficiency.
7. Preventing impersonation attacks, that is, no one can impersonate another authorized member to cause service abuse problems and to damage the security of VANETs.
8. Preventing eavesdropping, in other words, an intruder cannot discover some valuable information from communications between members in VANETs.

Generally, attacks cause anomalies to the network functionality. A lot of previous studies have investigated security vulnerabilities of routing protocols for wireless networks. Also, there are attacks in which malicious nodes advertise fake locations to their neighbor nodes. Malicious attackers may damage the network by announcing fake node locations. Such attacks are even more difficult to mitigate.

2.2.1 The Case of Vehicular Networks

The unique properties of vehicular networks (like Geographically Constrained Topology, Partitioning and Large Scale, Predictable Mobility, Power Consumption, Node Reliability) given in [3], have an impact on attack effectiveness. First of all, attacks that target in exhausting the node battery are not applicable here. Vehicles have the ability of constantly charging their batteries. Moreover, the vehicle's power supply is more than enough to support energy-demanding computational systems. As a result, authentication processes do not have to be light-weight.

However, vehicular networks could suffer from other types of attacks. Specifically, in [9] Dousse et al. proves that the probability of end-to-end connectivity decreases with distance, for one-dimensional network topologies. This implies that it now becomes much easier for a malicious attacker to partition the network. This effect can potentially be addressed by maintaining multiple forwarding nodes for each packet. Hence, if we only have one or a few malicious nodes, the rest of them could potentially maintain the node reliability. However, a synchronized attack by multiple compromised vehicles would be disastrous. This, together with the unreliability of single vehicles, is ideal for applying even simple attacks.

2.3 Privacy Challenges

During a long-distance trip in high speed, a vehicular user could roam across multiple APs either belonging to their home wireless domain or to domains owned by different authorities including various service providers. This poses challenges on privacy and network performance to the current public wireless networks access protocols. The privacy challenge comes from traffic logging at AP's and at home domain in current public wireless LAN roaming protocols. As a result, both home and visited networks can acquire many personal information, e.g., the home network knows the current location of a mobile user, the visited network knows the mobile user's identity and its home domain. Privacy in vehicular networks has to deal with threats that try to correlate received identifiers, or to correlate them to real-world identity, or to have position-identifier pairs. The performance challenge originates from the exchange of authentication messages between a user and its home domain when roaming. Mobile wireless communication has introduced new ***Location Privacy*** issue. Location Privacy is defined as an identity not being associated with a location, or a series of locations.

2.4 Authentication in WLAN

Many researches has addressed authentication in the interdomain roaming for WLANs. RADIUS based roaming and AAA architecture has been widely used for inter-operation between WLAN networks [10, 11] and also for inter-operation between a cellular network and WLANs [12, 5].

Further investigations show that the procedure impacts performance by introducing delays ranging from 2 to 7 seconds depending on roaming scenarios and network security configuration. While all these work addresses issues relating to roaming and security for multiple system domains, few has addressed privacy in authentication and none has discussed how to reduce the latency during the authentication procedure. The issues of privacy and latency are common for roaming within a domain or cross a domain.

The handoff in roaming architecture deals with authentication, authorization and accounting (AAA). In current authentication architecture, for intra-domain roaming, APs will send authentication messages back to the RADIUS server of the domain [14]. For inter-domain roaming, visited networks need to send authentication messages back to home networks [12, 5]. These authentication procedures suffer from overhead and delay in message transmissions and privacy problems.

3. AUTHENTICATION SCHEME IN VANET

The scenario for VANET communication we consider in this paper includes communicating entities of the service providers (SP), the cars, and the access points (AP) operated on behalf of service providers. The SPs and the APs can communicate with each other by some application-layer proprietary protocols via Internet. The APs are deployed along the roadside with reasonable wireless coverage to facilitate communication. A car typically belongs to one wireless network service provider, and communicates with the APs for accessing the internet along the road it travels through. When it travels, it also roams into wireless coverage that provide by other authorities.

To make the authentication process time-efficient, traditional solutions using centralized authentication server (AS) is not

preferable because of the large amount of messages exchanged among the car, the APs and the ASes. If the overlay network interconnecting the APs and the ASes is based on Internet, the delay for exchanging authentication messages could be prohibitive given the shortness of communication duration between the fast moving car and an individual AP. Thus the authentication protocols are devised such that after the car initiates communication requests until the communication session is established, the protocol should involve as less parties as possible besides the car and the AP, and as less on-demand communication over Internet as possible besides the wireless link between the communicating two parties. In addition, the number of messages exchanged in order for authentication should be controlled.

In our design, the user authentication will be performed at the APs, i.e., the user will prove to the AP that it is a legitimate one. A more strict security will require the AP to prove it is a legitimate one as well, so to have mutual authentication.

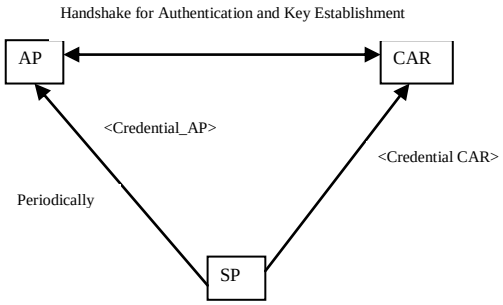

Figure1. General Authentication Process

During the authentication, the two parties will negotiate a secret session key for the communication afterwards. The session keys could be established in a way that synchronizes the update at both the car and the AP so to allow location privacy countermeasures as reviewed in the previous section. The general authentication process is shown in figure 1.

3.1 Proxy Re-encryption (PRA) in Authentication

Proxy re-encryption is a concept introduced by Blaze et al [15] in that allows a semi-trusted entity called the "proxy" to convert cipher texts addressed to an entity B called the "delegator" to another entity C called the "delegate", while maintaining that the proxy cannot learn anything about the underlying plaintext, and C cannot learn anything about the underlying plaintext without co-operation from the proxy. B does this delegation by providing a special piece of information, called the "rekey", to the proxy. Proxy re-encryption has found various applications like secure email forwarding, etc.

The basic concept of proxy re encryption[8] says that, a cipher text for Alice that is encrypted by Alice's public key can be transformed by a proxy to a cipher text for Bob that can be decrypted by Bob's private key. The proxy however cannot read the cipher text. In this procedure, Alice delegates her decryption right to Bob. The key that the proxy uses to do the transformation is called re-encryption key $rk_{a \to b}$.

In VANET, a car first needs to subscribe from a service provider SP. The car is assigned a pair of public and private keys at signup. For each time slot the SP has a public key PK_{SP} (ti).According to the subscription contract, the SP assign a series of re-encryption keys $ReKey_{CAR}$ (ti) corresponding to the time slots in subscription duration, by which the car can re-encrypt a message originally encrypted by the SP's public key to generate a cipher text encrypted by its own public key.

The authentication process is depicted in figure 2. For the first step, the car sends an authentication request to the AP detected in its range. The request message just contains the time of request t and a random number n1: <t1,n1 >. After the AP receives this message, it compares the time t1 provided by the car to its own clock. If the time is considered to be within normal deviation, the access point sends a message back to the car. The message constitutes a new random number n2 encrypted by the public key of the service provider of the time slot corresponding to t1: < (n2) PK_{SP} (t1) >.

After the car receives the reply, it uses the re-encryption key corresponding to t1 to re-encrypt the message. The outcome is thus available for it to decrypt using its own private key, and the n2 is revealed. It then takes n1 and n2, combines them by some cryptographic algorithm E known to both parties to generate E (n1, n2), and uses it as a symmetric key to encrypt a success tag as the authentication proof.

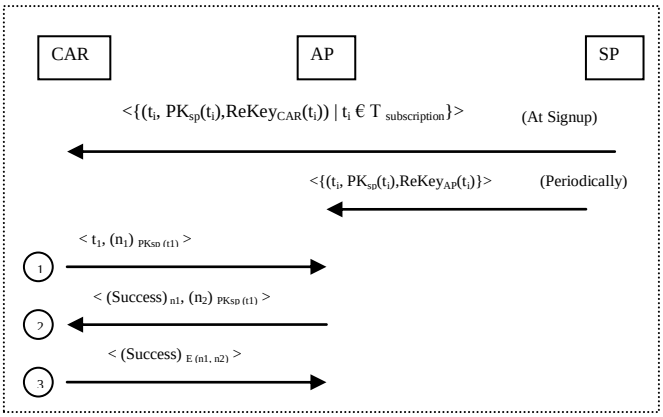

Figure 2. Authentication using Proxy Re- encryption

The encrypted message is sent back to the AP separately, or the car can also choose to immediately start sending data packets, with the authentication proof piggybacked to the first data packet. After the AP verifies the message by decrypting it using E (n1, n2), a secure and trusted connection is established. The session key E (n1, n2) is used to secure the following data transmission.

For the AP to show itself as authorized, it needs to answer a challenge just as it posts to the car. For this purpose the AP needs to get time-related re-encryption keys along with the SP's public keys from the SP in a periodic fashion. When the car initiates authentication request, besides the timestamp, the nonce n1 is encrypted by the current public key of the SP as a challenge. After the AP receives the request, it can use re-encryption to resolve the challenge. In the response message, besides the challenge message to the car, it includes the proof of re-encryption capability by a success tag encrypted using n1

as a symmetric key. The car can then use n1 to reveal the success tag and validate the AP.

4. ATTACKS IN PROXY RE-ENCRYPTION

Besides having advantages of the proxy re-encryption method for authentication, there are still some attacks that can be possible in above stated authentication methods. These are explained as follows:

1. Denial of Service (DoS) attack:

Attackers may seek to initiate excessive authentication requests in order to exhaust the resources of the AP. A general solution would be to limit the number of authentication requests which can be processed in a unit of time period. This method can guarantee that the server is not overwhelmed by DoS. But this could also delay a request. The implementation of the schemes must take such tradeoffs into consideration.

2. Eavesdropping:

Since the session key is calculated based on the nonce's contributed by the car and the AP respectively. Both of the car's nonce and the AP's nonce are encrypted by the public key of the SP during transmission. The attacker can reveal the session key, if he/she got the SP's private key, or an appropriate re- encryption key/private key pair.

3. Masquerade attack:

An unauthorized car which did not subscribe service from the SP may overhear the authentication messages on the air and try to have itself authenticated to the AP by replaying them. The attacker can get the car's public key and certificate and replay the car's authentication request. If the nonce n1 (randomly chosen) by the AP, matches with the one chosen earlier then the attacker can decrypt the response message from the AP which is encrypted by the car's public key.

4. Key bootstrapping and rekeying:

Anonymous keys are preloaded by the transportation authority or the manufacturer, but with different consequences. Moreover, while ELPs (Electronic License Plate) are fixed and should accompany the vehicle for a long duration (potentially its life cycle), anonymous key sets have to be periodically renewed after all the keys have been used or their lifetimes have expired. This renewal can be done during the periodic vehicle checkup (typically yearly) or by similar procedures. In addition to the ELP and anonymous keys, each vehicle should be preloaded with the CA's public key.

5. Tamper-proof device:

The use of secret information such as private keys incurs the need for a tamper-proof device in each vehicle. In addition to storing the secret information, this device will be also responsible for signing outgoing messages [16]. To reduce the risk of its compromise by attackers, the device should have its own battery, which can be recharged from the vehicle, and clock, which can be securely resynchronized, when passing by a trusted roadside base station. The access to this, device should be restricted to authorized people. For example, cryptographic keys can be renewed at the periodic technical checkup of the vehicle.

6. The measurements, like the time of arrival (a measurement of the round trip time between vehicle and AP), the angle of arrival (for radio signals) or the received signal strength, may be vulnerable to some amount of tampering as nodes (vehicles) may reduce (or, at higher cost, increase) the strength of their signal.

5. PROPOSED NEW PROXY RE-ENCRYPTION METHOD:

Because of the attacks in Proxy re-encryption method. We have proposed a new proxy re-encryption method which comprises all the features of earlier method with the only change that the public key of car for encryption of AP message is replaced by the private key.

Since an unauthorized car which did not subscribe service from the SP may overhear the authentication messages on the air and try to have itself authenticated to the AP by replaying them. If the proxy re-encryption method is taken into consideration, then the attacker can get the car's public key and certificate and replay the car's authentication request. Thus the attacker will be successful in getting the secure message of the vehicle.

To remove this attack, the new proxy re-encryption method will provide the car, a private(secret) key that is known only to the AP and to the car and also cannot be replayed by the attacker. In this manner the message can be securely transmitted between vehicles after authentication.

Since the private key is preserved and the attacker cannot be able to get it anyhow, the attacks such as DoS, Eavesdropping can never arise in case of new proxy re-encryption method for authentication, security and privacy in fast roaming networks.

This can be explained as follows:

1. Denial of Service (DoS) attack:

Because of the private key shared between the AP and car only, the attacker can never be able to exhaust the resource of the AP. Hence the delay in the request could also be prevented which usually occur in case of proxy-re encryption method of authentication.

2. Eavesdropping:

In case of earlier method the session key can be obtained, since the cars and AP's nonce are encrypted by the SP's public key. But if secret key is maintained between car and AP then even after the encryption, the attacker can never be able to reveal the re- encryption key. Hence privacy and security is maintained in new proxy- re encryption method.

However the issues like recharging of the batteries, maintaining ELP's, clock time management, received signal strength etc. donot have any impact with the change of the key. So, these remain same approximately as in the case of proxy re-encryption method.

6. CONCLUSION

In this paper the problems of Security, Privacy in VANET are discussed. The authentication scheme- *proxy re-encryption* is reviewed which helps in reducing authentication overheads in rapid roaming networks with the use of public key assigned to the "delegate" and private key assigned to the "delegator". Further the new proxy re-encryption scheme is presented in which the public key is replaced by the private key so as to get better result for authenticity and privacy in rapidly changing networks. The private keys are assigned to both delegator and delegate, which will prove secure email forwarding with less overhead in the information transmission. It is observed that the new proxy re-encryption scheme is better than the earlier one on the basis of the privacy; security and authentication and reduce overheads while roaming networks.

7. REFERENCES

[1] T. Leinmu ¨ ller, C. Maiho ¨ fer, E. Schoch, F. Kargl, "Improved security in geographic ad hoc routing through autonomous position verification", in: Proceedings of the 3rd International Workshop on Vehicular Ad Hoc Networks, Los Angeles, USA, 2006, pp. 57–66.

[2] T. Leinmu ¨ ller, E. Schoch, F. Karql, "Position verification approaches for vehicular ad hoc networks", IEEE Wireless Communications 13 (5) (2006) 16–21.

[3] Review Article- "Routing in Vehicular Networks: Feasibility,Modeling, and Security" Ioannis Broustis andMichalis Faloutsos Department of Computer Science and Engineering, University of California -Riverside, Riverside, CA 92521, USA Correspondence should be addressed to Broustis Ioannis, broustis@cs.ucr.edu Received 11 July 2007; Accepted 19 March 2008

[4] M. Raya, J.-P. Hubaux, "Securing vehicular ad hoc networks", Journal of Computer Security 15 (1) (2007) 39–68. Special issue on Security of Ad Hoc and Sensor Networks

[5] J.-S. Leu, R.-H. Lai, H.-I. Lin, and W.-K. Shih. "Running cellular/PWLAN services: practical considerations for cellular/PWLAN architecture supporting interoperator roaming". IEEE Communications Magazine, 44(2):73–84, 2006

[6] K. Plossl, T. Nowey, C. Mletzko, "Towards a security architecture for vehicular ad hoc networks", in: The First International Conference on Availability, Reliability and Security, 2006.

[7] M. Raya, J.P. Hubaux, "Security aspects of inter-vehicle communications", in: Proceedings of the 5th Swiss Transport Research Conference (STRC 2005), Ascona, Switzerland, 2005

[8] Ran Cantee , Susan Honenberger "Chosen Ciphertext secure Proxy "reencryption in CCS'07, October 29–November 2, 2007, Alexandria, Virginia, USA. Copyright 2007 ACM 978-1-59593-703-2/07/0010

[9] O. Dousse, P. Thiran, and M. Hasler, "Connectivity in ad hoc and hybrid networks," in Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '02), vol. 2, pp. 1079–1088, New York, NY, USA, June 2002.

[10] W. Wang and I. Akyildiz." A New Signaling Protocol for Intersystem Roaming in Next-Generation Wireless Systems". IEEE Journal on Selected Areas in Communications (JSAC), 19(10):2040–2052, October 2001.

[11]F. Bari and J.-L. Bouthemy. "An aaa based service customization framework for public wlans". In WCNC, 2005.

[12] G. Association. "WLAN Roaming Guidelines". Official DocumentIR.61,http://www.gsmworld.com/documents/wlan/ir61.pd Aug. 2004.

[13] S. Eichler, F. Dotzer, C. Schwingenschlogl, F.J.F. Caro, J. Eberspacher, "Secure routing in a vehicular ad hoc network", in: IEEE 60th Vehicular Technology Conference, 2004, pp. 3339–3343.

[14] C. Rigney, S. Willens, A. Rubens, and W. Simpson. "Remote authentication dial in user service (radius)", 2000.

[15] Matt Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography" . In Eurocrypt 1998, LNCS 1403, pp 127- 144, 1998.

[16] Xiaonan Liu, Zhiyi Fang, Lijun Shi. "Securing Vehicular Ad Hoc Networks", School of Computer Science and Technology, Jilin University Changchun, 130012, P.R China Lxn6O2@sina. com, zyfang@public. ccjl. Cn

[17] Jun Liu, Xiaoyan Hong, Qunwei Zheng, Lei Tang "Privacy-Preserving Quick Authentication in Fast Roaming Networks" Department of Computer Science, University of Alabama, Tuscaloosa, AL 35487 {jliu,hxy,qzheng,ltang}@cs.ua.edu