Privacy-Preserving Quick Authentication in Fast Roaming Networks

Jun Liu, Xiaoyan Hong, Qunwei Zheng, Lei Tang
Department of Computer Science, University of Alabama, Tuscaloosa, AL 35487
{jliu,hxy,qzheng,ltang}@cs.ua.edu

Abstract

Vehicular networks will become an important component for information accesses in one's daily life. A vehicular network provides a vehicular user not only chances to communicate with peer vehicles but also to use Internet through roadside access points (APs). During a trip a vehicular user could roam across multiple APs either belong to their home wireless domain or to domains owned by different authorities. This poses challenges on privacy and network performance to the current public wireless network access protocols. In this paper we explore an idea that shifts the paradigm of authentication that goes back to home networks to a paradigm of authentication that performs at the APs. We propose three authentication schemes in realizing the idea. These schemes are designed for preserving user's identity and location privacy. They also greatly reduce response time for authentication when roaming. The paper then analyzes the security and privacy properties of these schemes as well as the efficiency of them.

1 Introduction

It's expected that the vehicular network will become an important component for information accesses in one's daily life given the amount of time people spend on wheels. A vehicular network provides a vehicular user not only chances to communicate with peer vehicles but also to use Internet through roadside access points (APs). 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 APs 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. Although a few countermeasures have been proposed for location privacy [13] [27], a fast roaming user makes it difficult to fully benefit from the schemes and more data could be logged to help correlation.

The performance challenge originates from the exchange of authentication messages between a user and its home domain when roaming. The measurements [1] show that running security protocols used for various roaming scenarios take 2-7 seconds in delay, with the longest time accounting for the strongest security policy which ensures mutual authentication, confidentiality, integrity and non-repudiation. On the other hand, [23] reports that a connection from a car to a roadside access point takes 1/3 of total time period in high loss when entering the coverage area and another 1/3 period exiting the area. For a car driving at a speed of 100km/h through an AP with 200m range, a total connection only lasts for 15 seconds! Not much time leaves for a good quality of network usage. Clearly, long delay in roaming handoff could greatly impact the vehicular communication performance.

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 [26]. For inter-domain roaming, visited networks need to send authentication messages back to home networks [2, 20]. These authentication procedures suffer from overhead and delay in message transmissions and privacy problems.

In this paper we explore an idea that shifts the paradigm of authentication that goes back to home networks to a paradigm of authentication that performs at the APs. This shift is based on more security requirements at APs or local network access control severs behind APs. In realizing the idea we propose three authentication schemes. The three schemes only incur message exchanges between a vehicle and an AP through a three way handshake. Each of them uses different security primitives, namely, digital certificate, pairing [9] [6], and proxy re-encryption [3]. These security schemes are designed for preserving user's identity and location privacy. And they greatly reduce the number of messages for authentication, leading to quick response time when roaming, and thus making them suitable for applications such as military networks that require strong survivability and seamless handoff. In the paper, we further discuss the security properties of these schemes. The potential threats to the system are the untrusted APs, untrusted users and external eavesdroppers. The schemes proposed here, share the same security guarantees as supposed to traditional AAA architecture with strengthened privacy and reduced authentication time.

The paper is organized as follows. Section 2 briefly surveys related work on authentication in roaming, location privacy and vehicular networks. Section 3 describes our protocols in detail. Section 4 gives analysis on system security and privacy properties. Section 5 concludes the paper. For easy presentation, the paper is presented based on a vehicular user. However, the schemes and their benefits apply to mobile users using other wireless mobile networks.

2 Related Work

2.1 Authentication and Privacy in WLAN

Many research has addressed authentication in the inter-domain roaming for WLANs. RADIUS based roaming and AAA architecture has been widely used for inter-operation between WLAN networks [29, 5] and also for inter-operation between a cellular network and WLANs [2, 20]. In general, with either a web-based or a SIM-based AAA procedure, the number of message exchanges will count to 14 to 17, which involve AP point, RADIUS client and server at the visited network and at the home networks. 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 [1, 21]. Efstathiou et al [11] propose organizing WLAN domains to a peer-to-peer wireless network for a ubiquitous Internet access in wider area coverage. In the scheme, distributed and self-organizing agents are exploited to eliminate administrative overhead. They also use tunnel, pseudonyms, and mix-network mechanism to protect identity and location privacy.

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. Our work fits for both scenarios.

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*. Approaches such as *mix zones* [7], *disposable interface identifiers* [14], *blind signature* [15, 16] and *silent period* [17] are proposed to de-correlate identities to the locations. Our study differs from these studies in that we address the location privacy during the handoff procedure when roaming between two domains. These related work can be used to further enhance privacy after the handoff finishes.

2.2 Security and Privacy in Vehicular Networks

In vehicular networks, sender authentication and message integrity are critical security problems. To solve the problems, digital signatures on messages and timestamps are suggested using Public Key Infrastructure (PKI) by Zarki [30], Raya [25], Hubaux [18] and Parno [24]. An architecture for authentication and authorization has also been proposed using the Kerberos model by Moustafa [22].

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. In the aforementioned literature, Parno has demanded "anonymization service" to be one primitive. Hubaux suggests vehicle's privacy be protected by frequently changing pseudonyms. And Raya proposes to use a large pool of anonymous public/private key pairs and associated certificates with the electronic license plate at each vehicle. In addition, Dotzer [10] suggests geo-bounded pseudonyms. And Sampigethaya [28] uses a combination of a few aforementioned techniques and grouped transmission behaviors to thwart both temporal and spatial correlation analysis.

In all, these schemes are proposed to address the security and privacy issues within the vehicular networks. In the paper, we study the security and privacy issues when the vehicular networks roam across public wireless LANs.

3 Privacy-Preserving Quick Authentication

3.1 Network Scenarios

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 coverages that provide by other authorities. Our scenario envisions that when a car roams, it should be allowed for Internet access. This will need service agreement among SPs, but that is beyond the scope of this paper. The business model of a public wireless access network does not charge in term of the service time, but in a periodical subscription fashion. As long as a user is authenticated and authorized, the use of Internet is for free. This business model fits nicely into the authentication architecture presented here, which excludes accounting functionality.

Generally, a car has an initial service subscription with the SP. As for the security requirement needed for this work, we assume that the SP will take extra steps in authenticating the user at its sign-up. These steps are to establish initial secret with the car. The details of the initial secret will be discussed in the later subsections. In some of the proposed schemes, the SP and its APs also share the credential materials. Since the widely deployed APs are prone to attacks, the SP would monitor the behaviors of the APs' operation from time to time. In addition, in order to avoid secret weakening over time, we assume that these secret shares are periodically refreshed.

We consider two types of possible adversaries to the car. The first type is *external adversary*. These attackers don't possess any cryptographic materials issued by the SP and used by the car and the AP to conduct authentication. They just passively listen to the communication on the air, trying to get valuable information for malicious purposes. The second type is called *insider adversary*: untrustworthy APs logging and tracing the mobility pattern of a car, or untrustworthy users that abuse the cryptographic materials and status information stored in the car. Measures must be taken in order to control the damage once it happens.

3.2 Design Goals

Apparently, authentication schemes for VANET must be designed taking the characteristics of VANETs(i.e. high mobility and relatively short session time, etc.) into consideration. The primary goals are to achieve security and privacy and to reduce authentication overhead in terms of latency.

(i) Privacy: The privacy concerned in this paper includes identity privacy and location privacy. To external adversaries, identity leakage may allow tracing a mobile track. To insider adversaries, untrustworthy APs can also use revealed identity to trace the car. Besides identity divulgence, location privacy can also be compromised through improper use of cryptographic mechanisms. E.g., a same digital certificate used for a long period of time leading to temporal correlation. In terms of privacy protection, the SP is usually not a spontaneous cooperator. Depending on how authentication schemes are implemented, the SP may or may not be capable of assisting attacks on privacy. We will address the possibilities regarding to this issue in the discussion of the schemes proposed in later sections.

(ii) Reduced authentication overhead: 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 we manage to design authentication protocols 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.

3.3 Overview

In RADIUS architecture, when a car enters into the coverage of a new AP, the authentication will be conducted on a RADIUS server, which belongs to either the same domain or a different domain. 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. 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 details are out of the scope of this paper.

We present three different yet related authentication schemes. The first scheme utilizes certificates and general public key operations. The second one uses a cryptographic mechanism called proxy-reencryption, and the third one exploits the pairing theory. The schemes can be used to implement mutual authentication through handshake protocols. The architecture is shown in figure 1. We assume each AP is coupled with a local processing unit as a server. The thin lines indicate initial security establishment and possible periodical updates for mutual authentications. The thick line is the authentication protocols introduced in this paper. In our architecture, we depict the need for updating secret share to reduce security risk. As reflected in the protocols, we use time-stamps to indicate current updating time zone. This time-stamp mechanism is not our major focus here, and can be substituted using other methods.

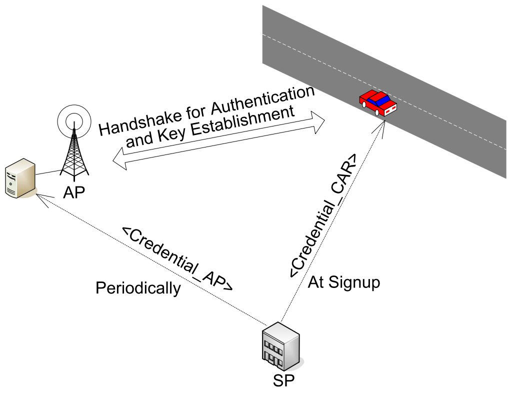

Figure 1: General Authentication Process

The three schemes are described in detail in the following subsections. To clearly characterize the schemes, we only describe one-way authentication(car to the AP) for each scheme at first. We then discuss the authentication of the AP to the car for all of the three schemes, consummating full specification of mutual-authentication.

3.4 Authentication Using Digital Certificate(DCA)

We now use traditional digital certificate to conduct the car-to-AP authentication. The SP partitions the service duration into time slots. When the car signs up at the SP, SP assigns a series of the car's public keys $PK_{CAR}(t_i)$ and their digital certificates $Cert_{CAR}(t_i)$ to the car. Only one specific public key and digital certificate pair can be used in the corresponding time slot during subscription. For each time slot during the SP's service, the SP has a corresponding public key. The SP also sends its own time-related public keys $PK_{SP}(t_i)$ to the car.

The SP administrates a large number of distributed APs and monitors the behavior of them. The SP distributes its time-related public keys to the APs periodically for the upcoming time slots.

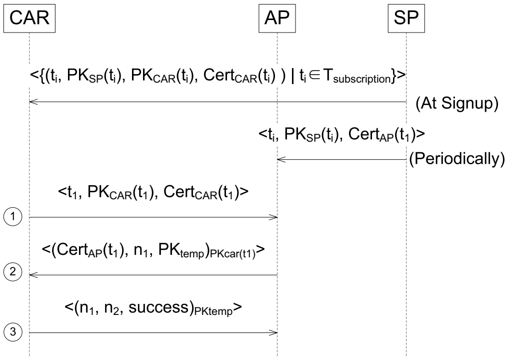
CAR
AP
SP
$<\{(t_i, PK_{SP}(t_i), PK_{CAR}(t_i), Cert_{CAR}(t_i)\ ) \mid t_i \in T_{subscription}\}>$
(At Signup)
$<t_i, PK_{SP}(t_i), Cert_{AP}(t_1)>$
(Periodically)
$<t_1, PK_{CAR}(t_1), Cert_{CAR}(t_1)>$
1
$<(Cert_{AP}(t_1), n_1, PK_{temp})_{PKcar(t1)}>$
2
$<(n_1, n_2, success)_{PKtemp}>$
3

Figure 2: Authentication Using Digital Certificate

As shown in figure 2, the authentication request is initiated by the car. According to its clock, it gets the time t_1 and the corresponding public key $PK_{CAR}(t_1)$ and certificate $Cert_{CAR}(t_1)$ issued by SP. The car sends a message consisting of the three data fields $< t_1, PK_{CAR}(t_1), Cert_{CAR}(t_1) >$ to the AP. After the AP receives this messages, it checks t_1. If it considers t_1 unacceptable with regard to a deviation threshold, it can either simply disregard the request, or send a time-correction message to the car in order for it to have it's clock adjusted. After the time adjusting, the car can initiate the authentication request again. If the time is validated, the AP tries to verify the certificate of the car's public key carried in the authentication request message by the SP's public key corresponding to t_1. If the verification is successful, it randomly chooses a nonce n_1 and generates a temporary public key PK_{temp}. After encrypting them by the $PK_{CAR}(t_1)$ provided in the request, the AP sends the message back to the car. The car can decrypt the message and get n_1. After generating another nonce n_2, it can send a verification to the AP consisting n_1, n_2 and a success tag encrypted altogether using PK_{temp}. The AP can decrypt the message and get n_2. Both parties can use some method E to generate session secret key from n_1 and n_2. The session key $E(n_1, n_2)$ is used for the data communication. The last verification message can be also piggybacked to the first data packet sent by the car.

3.5 Authentication Using Pairing(PA)

Pairing mechanism can also be used for authentication between the car and the AP. The basic idea of pairing mechanism is that a security authority(SA) can issue pseudonym/secret point pairs based on a master secret. Without the knowledge the master secret, any two parties who possesses a pseudonym/secret point pair can present pseudonyms to each other and a common secret key can be established.

The major construct of pairing is based on bilinear map. Consider two groups G_1, G_2 with the same prime order q with G_1 viewed as an additive group and G_2 as a multiplicative group. A cryptographic bilinear map is a mapping $e : G_1 \times G_1 \rightarrow G_2$ which satisfies the following properties: (1) Bilinearity: $\forall P, Q \in G_1, \forall x, y \in Z_q^*, e(xP, yQ) = e(P, Q)^{xy}$; (2) Non-degeneracy: If P is a generator of G_1, then $P \neq 0$ and $e(P, P) \neq 1$; (3) Computability: $\forall P, Q \in G_1, e(P, Q)$ is efficiently computable.

Examples of cryptographic bilinear maps include Modified Weil Pairing [9] and Tate Pairing [6] [12]. The security relies on the assumption that the BDHP(Bilinear Diffie-Hellman Problem) is hard, i.e., given $< P, wP, xP, yP >$ for $P \in G_1$ and $w, x, y \in Z_q^*$ which are the secrets of three parties, it is hard to compute $e(P, P)^{wxy}$.

To initialize, the SA comes up with two groups G_1 and G_2, as well as a bilinear function e. The SA also determines a master secret key $g \in Z_q^*$. The communicating parties are equipped with knowledge of G_1, G_2, e and a hash function $H_p : \{0, 1\}^* \rightarrow G_1$. The SA assigns random pseudonyms PN for users. The corresponding secret point is calculated as $S = gH_p(PN)$. Suppose we have two parties Alice and Bob. After Alice sends its pseudonym PN_A to Bob, Bob computes a hash value of this pseudonym: $P_A = H_p(PN_A)$. Then he can come up with a secret key $K_B = e(P_A, S_B)$, where S_B is a secret point possessed by Bob. Bob replies to Alice the pseudonym PN_B corresponding to S_B. Now Alice can also compute a secret key $K_A = e(P_B, S_A)$ where $P_B = H_p(PN_B)$ and S_A is the secret point corresponding to PN_A. Since $S_A = gP_A$, we have $K_A = e(P_B, gP_A) = e(P_B, P_A)^g$. Similarly we can also compute $K_B = e(P_B, P_A)^g$. So $K_A = K_B$ and the key negotiation completes.

This key-negotiation process using pairing is external-attack proof. Any third party who overhears both of the pseudonyms can not learn what the negotiated secret key is. Also, with the knowledge of any pseudonym/secret point pairs, a node can not recover the master secret g, due to the problem of discrete logarithm(DLP) being considered hard. Thus the adversaries can not generate new pseudonym/secret point pairs and the security is ensured.

During sign-up stage, when the car subscribes service from the SP, a series of pseudonym/secret point pairs are assigned to the car, with each pair being used in a time slot of subscription. The number of pairs is determined by the subscription length. The APs also get these pseudonym and secret point pairs, but in a periodic way similar to that of DCA. The SP stops assigning these pairs to an AP if the AP's found misbehaving.

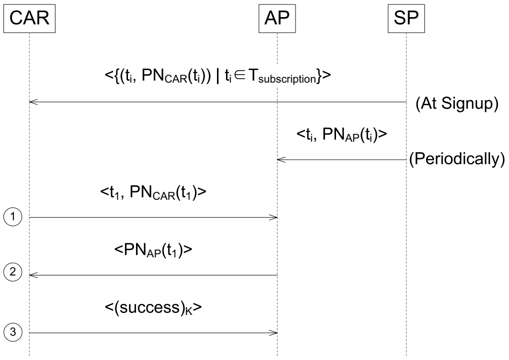
CAR
AP
SP
<{(t$_i$, PN$_{CAR}$(t$_i$)) | t$_i$ ∈ T$_{subscription}$}>
(At Signup)
<t$_i$, PN$_{AP}$(t$_i$)>
(Periodically)
<t$_1$, PN$_{CAR}$(t$_1$)>
1
<PN$_{AP}$(t$_1$)>
2
<(success)$_K$>
3

Figure 3: Authentication Using Pairing

The authentication message exchange still involves a three-way handshake. As shown in figure 3, the car initiates an authentication by sending a request message to the AP: $< t_1, PN_{CAR}(t_1) >$. The message contains a timestamp t_1 and the car's pseudonym $PN_{CAR}(t_1)$ bounded to that timestamp. If the time provided by the car is within normal deviation, the service provider picks one of its secret point corresponding the time provided by the car and computes a shared secret key *K*, otherwise it can initiate time synchronization with the car as mentioned before. It then replies the car with a message containing the pseudonym just used to generate the secret key *K*: $< PN_{AP}(t_1) >$. After the car receives the message, it can calculate the same secret key *K* based on the pseudonym provided by the AP. The car then encrypts a tag indicating successful authentication with the common secret key *K* and sends the message to the AP. After the AP confirms the message, the trust relationship between the car and the AP is established.

3.6 Authentication Using Proxy Re-encryption(PRA)

We can also utilize proxy re-encryption mechanism for authentication. Proxy re-encryption was first proposed in [8]. The most recent study of proxy re-encryption can be found in [4]. Distributed implementations of proxy re-encryption were proposed in [19] and [31]. The basic concept of *proxy re-encryption* 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* $rk_{a\to b}$.

We briefly introduce an implementation of proxy re-encryption here [8]. This scheme uses ElGamal encryption with some modification. To encrypt a message m for Alice, the sender computes and sends

$$\begin{aligned} c_1 &= mg^k \bmod p \\ c_2 &= (g^a)^k \bmod p \end{aligned}$$

where p is a prime of the form $2q + 1$ for prime q, g is a generator in $\mathbf{Z}_p^*$, a is Alice's secret key, g^a is her public key, k is a random number. Alice, who knows a^{-1}, can recover m by computing

$$c_1((c_2^{(a^{-1})})^{-1}) \bmod p$$

Let the re-encryption key be $\pi_{a\to b} = a^{-1}b$, where b is Bob's secret key. Then by computing $c_2^{\pi_{a\to b}}$, proxy transforms the cipher text for Alice to a cipher text for Bob. Notice that in this procedure, proxy has no way to read m.

In the most recent implementation [4], the re-encryption key is generated from Alice's private key and Bob's public key; Bob's private key is not needed.

A car first needs to subscribe from a service provider. The car is assigned a pair of public and private keys at signup. For each time slot the SP has a public key $PK_{SP}(t_i)$. According to the subscription contract, the SP assigns a series of re-encryption keys $ReKey_{CAR}(t_i)$ 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 ciphertext encrypted by its own public key.

The SP distributes its public keys $PK_{SP}(t_i)$ for the current time slots t_i to the APs periodically. If the service provider detects misbehavior of any APs, it simply stops updating its public keys to them.

The authentication process is depicted as in figure 4. 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 n_1: $< t_1, n_1 >$. After the AP receives this message, it compares the time t_1 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 n_2 encrypted by the public key of the service provider of the time slot corresponding to t_1: $< (n_2)_{PK_{SP}(t_1)} >$. After the car receives the reply, it uses the re-encryption key corresponding to t_1 to re-encrypt the message. The outcome is thus available for itself to decrypt using its own private key, and the n_2 is revealed. It then takes n_1 and n_2, combines them by some cryptographic algorithm *E* known to both parties to generate $E(n_1, n_2)$, and uses it as a symmetric key to encrypt a success tag as the authentication proof. 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 $E(n_1, n_2)$, a secure and trusted connection is established. The session key $E(n_1, n_2)$ is used to secure the following data transmission.

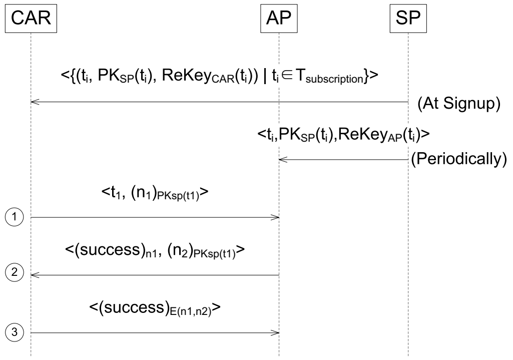
CAR
AP
SP
$<\{(t_i, PK_{SP}(t_i), ReKey_{CAR}(t_i)) \mid t_i \in T_{subscription}\}>$
(At Signup)
$<t_i, PK_{SP}(t_i), ReKey_{AP}(t_i)>$
(Periodically)
$<t_1, (n_1)_{PKsp(t1)}>$
1
$<(success)_{n1}, (n_2)_{PKsp(t1)}>$
2
$<(success)_{E(n1,n2)}>$
3

Figure 4: Authentication Using Proxy Re-encryption

3.7 Authentication of the APs

We just described procedures to authenticate the car to the AP. As the three schemes we propose achieve mutual authentication, now we present how the AP could be authenticated to the car. Authentication of the AP does not incur much additional overhead for the schemes we propose.

For DCA, The AP only needs to provide to the car with certificates that are issued by the SP periodically along with the public keys of the SP. These certificates are also time-related, with each one used for a specific time slot. It can be included in the AP's reply message answering the car's authentication request. The certificate can be encrypted together with the nonce n_1 and the temporary public key PK_{temp} by the public key $PK_{CAR}(t_1)$ provided by the car.

For PA, the authentication of the AP to the car is already implied without need for extra messages. If the AP is authentic, it should be equipped with valid pseudonym/secret point pairs. As long as the AP can provide a pseudonym, and it can come up with a secret key according to the pseudonyms including the car provided one, it should be capable of decrypting encrypted data packets coming from the car by the negotiated secret key. If it fails to do such decryption, it's not an authentic AP and the data transmitted from the car to it is always kept secret.

For PRA, 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 n_1 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 n_1 as a symmetric key. The car can then use n_1 to reveal the success tag and validate the AP.

4 Scheme Analysis

The three schemes we propose all implement authentication between the car and the AP. We now analyze these three schemes and discuss the impacts brought by their different authentication approaches in terms of our design goals.

4.1 Minimum Communication Party Involvement at Realtime

Unlike traditional authentication schemes like RADIUS [26] which is based on a client-server architecture, the three schemes do not require interaction with any remote backend authentication servers at the time of authentication, i.e., no other communicating parties than the car and the AP are involved. The initial phase has pre-prepared some steps that otherwise will be needed in realtime authentication. These initial steps include: the SP is responsible for issuing credentials for the purpose of authentication. The car is preloaded with a set of credentials at the signup stage, and the AP is sent such credentials periodically. For DCA, the credentials are the time-related digital certificates. For PA, the credentials are the time-related pseudonym/secret point pairs. For PRA, the credentials are the time-related re-encryption keys. Without real-time assistance from any third party, these cryptographic materials distributed to the cars and the APs already satisfy the authentication requirements.

4.2 Security in Authentication

All of the three authentication schemes achieve certain level of security. In order to clearly demonstrate their strength of security and privacy protection, we enumerate some attack scenarios and discuss the impacts brought by them.

4.2.1 *Eavesdropping*

An external eavesdropper can not guess the final session key based on the exchanged authentication messages. For DCA, the nonces which later form session keys are randomly chosen by the AP and the car, and encrypted by the car's public key and a temporary public key provided by the AP respectively. Knowing the ciphertext and the public key does not help to uncover the encrypted content which contains the nonces. For PA the session key is calculated independently at the AP and the car using the pseudonyms exchanged. An external attacker can not compute the session key, since she does not know any of the secret points associated with the pseudonyms. For PRA, the session key is calculated based on the nonces 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. Without the knowledge of the SP's private key, or an appropriate re-encryption key/private key pair which is only assigned to a valid customer, the attacker can not reveal the session key.

4.2.2 *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. DCA is immune to this attack. Although the attacker can get the car's public key and certificate and replay the car's authentication request, it can not decrypt the response message from the AP which is encrypted by the car's public key. Since the nonce n_1 is randomly chosen by the AP, the response message differs every time whenever the same authentication request is received repeatedly. Thus the authentication can not proceed. For PRA, the situation is similar. The AP uses random nonce n_2 in the second authentication message, making the attacker unable to respond with an appropriate confirmation and effectively preventing the attacker from being authorized. For PA, the attacker may reply with the authentication request comprising the car's pseudonym. If the AP only has one pseudonym for a particular time slot, it will always respond with the same pseudonym. The attacker can then use the previously overheard confirmation to complete the authentication. However, even if the authentication process successfully completes, since the attacker does not have the secret point corresponding to the pseudonym it overhears, it can not come up with a valid session key with the AP, thus the subsequent data transmission can not proceed.

4.2.3 *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.

4.3 Privacy in Authentication

Privacy achieved by the three schemes is different. First of all, none of the schemes use explicit identification information for authentication. They all use a series of cryptographic materials in the handshake procedure. Besides these, all of the following communication messages exchanged are encrypted using the session keys. Moreover, a distinguished feature of PRA is the higher level of anonymity it achieves. In PRA, the cryptographic material(re-encryption key) is not included in any of the authentication messages exchanged. Instead, the car only uses the re-encryption key to respond to the challenge from the AP. The authentication request message only contains a timestamp and a randomly chosen nonce, which could be different for each request initiated.

Attackers may independently or collaboratively collect and analyze authentication messages sent along the road. They typically try to find the motion pattern of a car through traffic analysis. There could be external attackers, or insider attackers such as the APs themselves. In the proxy-reencryption based authentication scheme PRA, no cryptographic material is presented repeatedly. The random nonce leaves no trace of which user is authenticating. Thus it achieves a high level of untraceability. Nevertheless, when the traffic on the road is sparse enough, even if there are no repeated messages on the air, the attackers can still link authentication messages together based on estimated speed and distance apart the APs. An intuitive countermeasure is to maintain a silent period randomly during which the car stops authenticating with APs [17]. This method can effectively thwart traffic analysis in such scenario, but at the cost of reduced data communication efficiency. The tradeoffs between anonymity and data transmission performance always exist.

4.4 Revocation for Misbehaving APs

In case the SP finds out that an AP is misbehaving, it can always revoke the authentication privilege by suspending the periodic credential update. For DCA, the suspended AP can no longer provide valid time-related certificate to the car. For PA, suspended AP can not use stale pseudonym/secret point pairs to negotiate common session keys with the car. For PRA, the suspended AP can no longer answer the challenge without updated re-encryption keys. This passive revocation approach fits our authentication scenario perfectly, for it never requires interaction between the SP and the car in order to transfer revocation information. Also, suspension of a particular AP does not involve interaction with any other APs.

4.5 Authentication Efficiency

When time bound is a concern, the authentication delay can be further reduced by piggyback. For DCA, the third authentication message can be piggybacked to the first data packet from the car to the AP. While for PA and PRA, after the second authentication message, the two communicating parties already possess all materials in order to construct the session secret key. Therefore the data communication can start immediately after the first two authentication messages. With these mechanisms all three schemes achieve better performance in authentication efficiency.

5 Conclusion

We address the privacy and the long latency problems in the authentication procedure incurred when a vehicular network user roams across APs and different domains. We propose to shift the paradigm of authentication that goes back to home networks to a paradigm of authentication that performs at the APs. This shift is based on more security requirements at APs or local network access control severs behind APs. We propose three authentication schemes all realizing the idea. The schemes use different security primitives, namely, digital certificate, key paring, and proxy re-encryption. They are designed for preserving user's privacy and they greatly reduce the number of messages for authentication so to improve performance. We further discuss the security and privacy properties when there are untrusted APs, untrusted users, external eavesdroppers and traffic analysis attack. The schemes proposed here, share the same security guarantees as supposed to traditional AAA architecture with strengthened privacy and reduced authentication time.

References

[1] A. K. Agarwal and W. Wang. An Experimental Study of Cross-Layer Wireless Security in Public Access Wireless Networks. Technical Report TR02-NeTWIS-04, Dept of Electrical and Computer Engineering, North Carolina State Univ., 2004.

[2] G. Association. "WLAN Roaming Guidelines". Official Document IR.61, `http://www.gsmworld.com/documents/wlan/ir61.pdf`, Aug. 2004.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *Proc. of the 12th Annual Network and Distributed System Security Symposium (NDSS)*, 2005.

[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Trans. Inf. Syst. Secur.*, 9(1):1–30, 2006.

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

[6] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In *CRYPTO '02: Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology*, 2002.

[7] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. *IEEE Pervasive Computing*, 2(1):46–55, 2003.

[8] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In *Eurocrypt'98, LNCS 1403*, 1998.

[9] D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, 2001.

[10] F. Dotzer. Privacy Issues in Vehicular Ad Hoc Networks. In *Workshop on Privacy Enhancing Technologies (PET)*, 2005.

[11] E. Efstathiou and G. Polyzos. A peer-to-peer approach to wireless lan roaming. In *ACM Int'l Workshop on Mobile Applications and Services on WLAN Hotspots,*, Sept. 2003.

[12] S. D. Galbraith, K. Harrison, and D. Soldera. Implementing the tate pairing. In *ANTS-V: Proceedings of the 5th International Symposium on Algorithmic Number Theory*, 2002.

[13] M. Gruteser and D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking. In *MobiSys03*, 2003.

[14] M. Gruteser and D. Grunwald. Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: A Quantitative Analysis. In *WMASH'03*, 2003.

[15] Q. He, D. Wu, and P. Khosla. Quest for Personal Control over Mobile Location Privacy. *IEEE Communications Magazine*, 42(5):130–136, 2004.

[16] Y.-C. Hu and H. J. Wang. A Framework for Location Privacy in Wireless Networks. In *Proceedings of the ACM SIGCOMM Asia Workshop*, Beijing, China, April 2005.

[17] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki. Enhancing Wireless Location Privacy Using Silent Period. In *IEEE WCNC*, 2005.

[18] J.-P. Hubaux, S. Capkun, and J. Luo. The Security and Privacy of Smart Vehicles. *IEEE Security & Privacy Magazine*, (3):49–55, May-June 2004.

[19] M. Jakobsson. On quorum controlled asymmetric proxy re-encryption. In *PKC '99: Proceedings of the Second International Workshop on Practice and Theory in Public Key Cryptography*, 1999.

[20] 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.

[21] W. Liang and W. Wang. On Performance Analysis of Challenge/Response Authentication in Wireless Networks. *Journal of Computer Networks (Elsevier Science)*, 48(2), June 2005.

[22] H. Moustafa, G. Boudron, , and Y. Gourhand. AAA in Vehicular Communication on Highways with Ad Hoc Networking Support: A Proposed Architecture. In *VANET'05*, Cologne Germany, September 2005.

[23] J. Ott and D. Kutscher. Drive-thru internet: Ieee 802.11b for.

[24] B. Parno and A. Perrig. Challenges in Securing Vehicular Networks. In *Workshop on Hot Topics in Networks (HotNets-IV)*, MD, Movember 2005.

[25] M. Raya and J.-P. Hubaux. The Security of Vehicular AdHoc Networks. In *In SASN'05*, Movember 2005.

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

[27] D. Samfat, R. Molva, and N. Asokan. Untraceability in Mobile Networks. In *ACM MOBICOM*, pages 26–36, 1995.

[28] R. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: Providing Location Privacy for VANET. In *in Proceedings of Embedded Security in Cars (ESCAR)*, November 2005.

[29] 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.

[30] M. E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian. Security Issues in a Future Vehicular Network. In *EuroWireless*, February 2002.

[31] L. Zhou, M. A. Marsh, F. B. Schneider, and A. Redz. Distributed blinding for distributed elgamal re-encryption. In *ICDCS '05: Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, pages 824–824, 2005.