Entropy **2014**, *16*, 6152-6165; doi:10.3390/e16116152

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Improving the Authentication Scheme and Access Control Protocol for VANETs

Wei-Chen Wu [1,2,*] and Yi-Ming Chen [2]

[1] Computer Center, Hsin Sheng Junior College of Medical Care and Management, No. 418, Kaoping Village, Lungtan Township, Taoyuan County 32544, Taiwan

[2] Department of Information Management, National Central University, No. 300, Jhongda Rd., Jhongli City, Taoyuan County 32001, Taiwan; E-Mail: cym@cc.ncu.edu.tw

[*] Author to whom correspondence should be addressed; E-Mail: wwu@hsc.edu.tw; Tel.:+886-3-4117578 (ext. 260); Fax: +886-3-4117600.

External Editor: James J. Park

Received: 10 August 2014; in revised form: 25 September 2014 / Accepted: 4 November 2014 / Published: 19 November 2014

Abstract: Privacy and security are very important in vehicular *ad hoc* networks (VANETs). VANETs are negatively affected by any malicious user's behaviors, such as bogus information and replay attacks on the disseminated messages. Among various security threats, privacy preservation is one of the new challenges of protecting users' private information. Existing authentication protocols to secure VANETs raise challenges, such as certificate distribution and reduction of the strong reliance on tamper-proof devices. In 2011, Yeh *et al.* proposed a PAACP: a portable privacy-preserving authentication and access control protocol in vehicular *ad hoc* networks. However, PAACP in the authorization phase is breakable and cannot maintain privacy in VANETs. In this paper, we present a cryptanalysis of an attachable blind signature and demonstrate that the PAACP's authorized credential (AC) is not secure and private, even if the AC is secretly stored in a tamper-proof device. An eavesdropper can construct an AC from an intercepted blind document. Any eavesdropper can determine who has which access privileges to access which service. For this reason, this paper copes with these challenges and proposes an efficient scheme. We conclude that an improving authentication scheme and access control protocol for VANETs not only resolves the problems that have appeared, but also is more secure and efficient.

Keywords: vehicular *ad hoc* networks (VANETs); cryptanalysis; privacy; authentication; access control

1. Introduction

VANETs are a special case of mobile *ad hoc* networks (MANETs) that aim to enhance the safety and efficiency of road traffic [1–4]. A number of distinguishing features and limitations are related to the very nature of wireless communications in VANETs and the rapid movement of the vehicles involved in those communications. Compared to wired or other wireless networks, VANETs are very dynamic and their communications are volatile. In these networks, nodes are vehicles equipped with communication devices, known as on-board units (OBUs), and, depending on the applications, OBUs are used to establish communications with other vehicles or roadside units (RSUs), such as traffic lights or traffic signs.

In recent years, several research works on VANETs have been conducted by academics and various industries. Recently, some of these works addressed the security issues. As an instance of MANET, VANETs might suffer from any malicious user behaviors, such as bogus information and replay attacks on the disseminated messages. Among various security threats, privacy preservation in VANETs is one of the new challenges of protecting users' private information. For instance, Chen and Wei proposed a safe, distance-based location privacy scheme called SafeAnon [5,6]. By simulating vehicular mobility in a cropped Manhattan map, they evaluated the performance of the SafeAnon scheme under various conditions to show that it could simultaneously achieve location privacy, as well as traffic safety. However, as Chen and Wei focused on the issues of the vehicles' location privacy, little emphasis was put on the initial authentication phase of communications among vehicles.

In 2005, Raya *et al.* [7] first proposed a solution that mentioned both the security and privacy issues of safety-related applications. Wang and others reviewed Raya and Hubaux's communication scheme in 2008 [8] and argued that Raya and Hubaux paid a great deal of attention to safety-related applications, such as emergency warnings, lane changing assistance, intersection coordination, traffic-sign violation warnings and road-condition warnings [9], but non-safety-related applications were neglected. In Raya and Hubaux's communication scheme, Safety messages do not contain any sensitive information. However, VANETs also provide non-safety applications that offer maps [10,11], advertisements and entertainment information [12].

Similar to safety applications, non-safety applications in VANETs have to take both security and privacy issues into consideration. In addition, designing a practical non-safety application for VANETs should take the following requirements into consideration [13,14]:

Mutual authentication: providing mutual authentication between the two communicating parties, such as a vehicle-to-roadside communication device.

Context privacy: allowing mobile vehicles to anonymously interact with roadside devices to access services.

Lower computational cost: a system must have light overhead in terms of computational costs and high efficiency.

Session key agreement: generating dynamic session keys to secure the communication between nodes in VANETs.

Differentiated service access control: providing several services with different levels of access privileges for different users' requirements.

Confidentiality and integrity: providing data confidentiality and integrity in applications of communications.

Preventing eavesdropping: an intruder cannot be allowed to discover valuable information from communications between members in VANETs.

Scalability: coping with the large-scale and dynamic environment presented by VANETs.

In 2008, Li *et al.* proposed a secure and efficient communication scheme named SECSPP [14] that employs authenticated key establishment for non-safety applications in VANETs. SECSPP is the first security scheme with explicit authentication procedures for non-safety applications. However, the speed of a vehicle can be extremely high in SECSPP. It is possible that the response sent from the service provider (SP) has not yet arrived, but the requesting vehicle has passed the RSUs' transmission range. Moreover, all requests made by non-safety applications must first be verified by the proper SP, which will become a bottleneck of SECSPP. The scalability issue rises in a popular SP if a large number of requests are made.

In 2011, Yeh *et al.* [13] proposed a PAACP: a portable privacy-preserving authentication and access control protocol for vehicular *ad hoc* networks. However, in the authorization phase, a PAACP is breakable and cannot maintain privacy in VANETs. Recently, Wu *et al.* [15] presented a cryptanalysis of an attachable blind signature and demonstrate that the PAACP's authorized credential (AC) is not secure and private, even if the AC is secretly stored in a tamper-proof device. This is because an eavesdropper is able to construct an AC from an intercepted blind document. Consequently, PAACP in the authorization phase is breakable and cannot maintain privacy in VANETs. Any outsiders can determine who has which access privileges to access which service. In addition, this paper efficiently copes with these challenges and proposes an efficient scheme. We conclude that improving an authentication scheme and access control protocol for VANETs will not only resolve the problems that have appeared, but will also be secure and efficient.

The remainder of this paper is organized as follows. Section 2 reviews the cryptanalysis of a PAACP. Section 3 introduces an improved scheme. In Section 4, we compare the performance of our schemes with PAACP and SECSPP and analyze various aspects of the security of our scheme. Finally, we conclude this paper and indicate some directions for future research in Section 5.

2. Cryptanalysis of A PAACP

In 2011, Yeh *et al.* [13] proposed a novel portable privacy-preserving authentication and access control protocol for vehicular *ad hoc* networks. To eliminate the communication with service providers, they proposed a novel portable access control method to store a portable service right list (SRL) into each vehicle, instead of keeping the SRLs with the service providers. In order to assure the validity and privacy of an SRL and prevent privilege elevation attacks, an attachable blind signature is used by PPACP. Recently, Wu *et al.* [15] proposed a cryptanalysis of an attachable blind signature and demonstrated that the PAACP's authorized credential (AC) is not secure and private, even if the AC is secretly stored in a tamper-proof device. Their analysis showed that in PAACP, an eavesdropper can construct the AC from an intercepted blind document. As a result, PAACP in the authorization phase is breakable, and as any outsider can determine who has which access privileges to access which service, the privacy of users in PAACP's scheme is jeopardized. Wu *et al.* presented Cryptanalysis 1, which shows that m' cannot keep privacy, and Cryptanalysis 2 shows that an intruder can use public key PK_{S_t} of the S_t to compute authorized credential $AC_i^{S_t}$. The notation used throughout the remainder of this paper is shown in Table 1.

Table 1. Notation used in the remainder of the paper.

Notation	Description
V_i	the i-th vehicle
VID_i	i-th vehicular node's real identification
S_t	the t-th service provider
SID_t	t-th service provider's real identification
$SVID_k$	k-th service's identification
AR_k	the access privilege of $SVID_k$
AC_i	authorized credential for vehicle V_i
$AC_i^{S_t}, AC_i^{V_i}$	authorized credential made by S_t and V_i, respectively
AC_i^*	portable authorized credential for vehicle V_i
SRL^{S_t}, SRL^{V_i}	service right list made by S_t and V_i, respectively
$D_k()$	a corresponding symmetric cryptosystem that uses the secret key k for decryption
$E_k()$	a secure symmetric cryptosystem that uses the secret key k for encryption
N_i	fresh nonce, randomly generated by VID_i
N_s	fresh nonce, randomly generated by the service provider
$h()$	a collision-free and public one-way hash function
$\|\|$	a string concatenation
$X \rightarrow Y : Z$	a sender X sends a message Z to receiver Y

Cryptanalysis 1. *To acquire a message m', an intruder can eavesdrop on the two blind documents BD_1, BD_2 in the $(User \rightarrow Signer)$ channel and also eavesdrop on BD_1', BD_2' in the*

$(Signer \rightarrow User)$ channel. After stealing BD_1, BD_2, BD'_1 and BD'_2, the intruder can use public key e of the signer to compute the following equation:

$$\frac{(BD'_1BD'_2)^e}{(BD_1BD_2)} = m'$$

Cryptanalysis 2. *Similarly, to acquire authorized credential $AC_i^{V_i}$ and $AC_i^{S_t}$, an intruder can eavesdrop on the two blind documents $BD1_i, BD2_i$ in the $(Vehicle \rightarrow Service\ Provider)$ channel and also eavesdrop on $BD1'_i, BD2'_i$ in the $(Service\ Provider \rightarrow Vehicle)$ channel. After stealing $BD1_i, BD2_i, BD1'_i$ and $BD2'_i$, the intruder can use public key PK_{S_t} of the Service Provider to compute the following equation:*

$$\frac{(BD1'_iBD2'_i)^{PK_{S_t}}}{(BD1_iBD2_i)} = AC_i^{S_t}$$

Finally, according to $\sqrt{(AC_i^*)^{PK_{S_t}}} = AC_i^{V_i} = AC_i^{S_t}$, $AC_i^{S_t}$ is equal to $AC_i^{V_i}$, where AC_i^* consists of both $AC_i^{V_i}$ and $AC_i^{S_t}$. Yeh *et al.* [13] claimed that an attachable blind signature can keep privacy; no one could comprehend the access privileges in $AC_i^{V_i}$, and no one can realize who is accessing those services. On the basis of our cryptanalysis, $AC_i^{S_t} = \{SID_t \| T_{expired} \| SRL_i^{S_t}\}$ and $AC_i^{V_i} = \{SID_t \| T_{expired} \| SRL_i^{V_i}\}$ could be comprehended by outsiders who could then decode the service right lists $SRL_i^{S_t}$ and $SRL_i^{V_i}$, respectively. In a previous description, the service right list is as the following equation:

$$SRL_i^{V_i} = \{SVID_1 \| AR_1 \| SVID_2 \| AR_2 \| \ldots \| SVID_k \| AR_k\}$$

where $SVID_k$ denotes the index of the k-th service and AR_k represents the granted access privileges of $SVID_k$. Hence, anyone can determine who has which access privileges to access which service even if AC_i^* is secretly stored in a tamper-proof device.

3. Improved Scheme

In this section, we propose an improved scheme and offer an efficient authentication and access control protocol for VANETs. The security of this scheme depends on a secure one-way hash function, not the use of an attachable blind signature. This scheme consists of three phases: the registration phase, the authentication phase and the access phase. We demonstrate our scheme as follows.

3.1. The Registration Phase

A vehicle V_i creates a service right list $SRL_i^{V_i}$ and an authorized credential $AC_i^{V_i}$, just as Yeh *et al.* proposed. Let x be a secret key maintained by the service provider S_t, and let $h()$ be a secure one-way hash function with a fixed-length output. The registration phase is performed over a secure channel.

- $V_i \rightarrow S_t : VID_i, AC_i^{V_i}$
  A V_i, who submits his/her identity VID_i and his/her $AC_i^{V_i}$ to the S_t for registration.

- $S_t \rightarrow V_i : h(), e_i$

  The S_t also creates $SRL_i^{S_t}$ and $AC_i^{S_t}$ as Yeh *et al.* proposed. The S_t then computes V_i's secret information $y_i = h(VID_i, x)$ and $e_i = y_i \oplus AC_i^{S_t} \oplus AC_i^{V_i}$ and writes $h()$ and e_i into the smart card of on-board units (OBUs) and issues the card to V_i.

- $S_t \rightarrow R_j : y_i, AC_i^{S_t}$

  The S_t also performs a multicast to send messages y_i and $AC_i^{S_t}$ to their road side units (RSUs) R_j.

3.2. The Authentication Phase

After V_i sends an authentication request message to the S_t, the S_t and V_i will execute a mutual authentication between the vehicle and the service provider. First, let $E_k(\cdot)/D_k(\cdot)$ be a symmetric encryption/decryption function with secret k, respectively.

- $V_i \rightarrow S_t : VID_i, C, N_i$

  When V_i wishes to access services provided by S_t, V_i generates a nonce N_i, where N_i is a random and fresh number. Then, V_i computes $C = h(e_i \oplus AC_i^{V_i}, N_i)$ and sends an authentication request message (VID_i, C, N_i) to the S_t.

- $S_t \rightarrow V_i : M$

  After receiving the authentication request message (VID_i, C, N_i), the S_t and V_i execute the following steps to facilitate a mutual authentication between the vehicle and the service provider. The S_t performs the following operations:

  - Verifies that VID_i is a valid vehicle identity. If not, the authentication request is rejected.
  - Computes $y_i' = h(VID_i, x)$ and verifies whether $y_i = y_i'$. If the verification fails, the request is rejected.
  - Checks whether it received $C = h(y_i' \oplus AC_i^{S_t}, N_i)$. If not, the request is rejected; otherwise, the request proceeds to the next step.
  - Generates a nonce N_s, where N_s is a random and fresh number.
  - Encrypts the message $M = E_{y_i \oplus AC_i^{S_t}}\{N_s, N_i, AC_i^{S_t}\}$ and sends it back.
  - After V_i receives the message M, V_i will decrypt the message $D_{e_i \oplus AC_i^{V_i}}\{M\}$ to derive $(N_i', N_s', AC_i^{S_t\prime})$ and verify whether $N_i' = N_i$. If the answer is yes, the mutual authentication is done. The portable authorized credential is $AC_i = AC_i^{V_i} \oplus AC_i^{S_t}$, and we propose that $AC_i^{V_i}$ is not equal to $AC_i^{S_t}$. Either S_t may reduce access privileges for some reason (for example, not paying before the deadline or breaking a contract) or V_i may disable access privileges himself/herself for some reason (for example, privacy issue or lower communication costs). Therefore, AC_i is $AC_i^{V_i}$ and performs an exclusive operation with $AC_i^{S_t}$ that is reasonable and makes sense.

3.3. The Access Phase

This phase is based on the key exchange protocol proposed by Diffie *et al.* [16]. It is used to encrypt an individual conversation with a session key. The lifespan of a session key is the period of a particular communication session. A new session phase involves two public parameters, q and α, where q is a large prime number and α is a primitive element $mod\ q$. After V_i sends a service request to its neighboring R_j, R_j will verify the authorized credential AC_i by itself without further communication with S_t. According to the access privileges stored in the authorized credential $AC_i^{S_t}$, R_j could decide whether V_i's request is accepted or not. Furthermore, R_j could detect whether V_i is launching an elevation of privilege (EoP) attack.

- $V_i \rightarrow R_j : W_i$
  V_i computes $W_i = \alpha^{r_{v_i}} mod\ q$ and sends W_i to R_j, where r_{v_i} is a random number.

- $Rj \rightarrow Vi : S_i$
  Similarly, R_j computes $S_i = \alpha^{r_{R_j}} mod\ q$ and sends S_i to V_i, where r_{R_i} is a random number. V_i computes $K_V = (S_i)^{r_{v_i}} mod\ q$, and R_j computes $K_R = (W_i)^{r_{R_j}} mod\ q$. Then, both of them check whether $K_V = K_R$. If yes, a new session will be created. This is because:

$$\begin{aligned} Session\ key &= (S_i)^{r_{v_i}} mod\ q = (\alpha^{r_{R_j}} mod\ q)^{r_{v_i}} mod\ q = (\alpha^{r_{R_j} r_{v_i}}) mod\ q \\ &= (\alpha^{r_{v_i}} mod\ q)^{r_{R_j}} mod\ q = (W_i)^{r_{R_j}} mod\ q \end{aligned}$$

- $V_i \rightarrow R_j : (Service\ request\ message)$
  If V_i wants to access service, it encrypts $E_{K_V}(SVID_1 \parallel AC_i)$ with K_V as the service request message and sends it to R_j. After R_j receives the message, R_j will decrypt the message:

$$D_{K_R}(E_{K_V}(SVID_1 \parallel AC_i))$$

  with K_R to gain $(SVID_1 \parallel AC_i)$ and then derive AC_i and $SVID_1$, because of $K_V = K_R$. When R_j derives AC_i, R_j verifies it and is then convinced that V_i is a legal user.

- $V_i \rightarrow R_j : (Service\ request\ message)_{nth}$
  When V_i continues to access the n-th service, it encrypts the n-th service request message $E_{K_V+n}(SVID_n \parallel AC_i)$ with $K_V + n$ and sends it to R_j. After R_j receives the n-th service request message, R_j will decrypt the message:

$$D_{K_R+n}(E_{K_V+n}(SVID_n \parallel AC_i))$$

  with $K_R + n$ to derive AC_i and $SVID_n$. R_j examines whether SID_t, as well as $SVID_n$ are included in $AC_i^{S_t}$ and checks the validity of the authorized credential by $T_{expired}$. If the verification succeeds, AC_i is legitimate and V_i is authorized; otherwise, R_j terminates this session.

4. Analysis of the New Scheme

In this section, we roughly compare the security properties and performance of the related mechanisms discussed. The security properties comparisons between PAACP, SECSPP and our scheme in the authentication phase and access phase are shown in Table 1. The performance comparisons are shown in Table 2.

4.1. Comparison

Table 1 lists important security properties in VANETs based on Yeh *et al.*'s proposals. As mentioned, with PAACP, an attachable blind signature, is breakable and cannot maintain privacy, and the PAACP's AC is not secure, even if the AC is secretly stored in a tamper-proof device. An eavesdropper is able to construct the AC from an intercepted blind document. Any outsiders in VANETs can know who has which access privileges to access which service. Consequently, PAACP cannot still satisfy context privacy properly.

Table 2. Comparison of security features.

Requirements	Our Scheme	PAACP	SECSPP
Mutual Authentication	Yes	Yes	Yes
Context Privacy	Yes	No	Yes
Session Key Agreement	Yes	Yes	Partially Yes
Differentiated Service Access Control	Yes	Yes	No
Confidentiality and Integrity	Yes	Yes	N/A
Preventing Eavesdropping	Yes	No	Yes
Scalability	Fully Distributed	Fully Distributed	Bottleneck at Service
Lower Communication and Computational Cost	Low	High	Extremely High

a: In PAACP, authorized credential (AC) is not secure and private; b: In SECSPP, the session key TSK is determined by V and S, not V and R.

4.2. Performance

Since the computational load of the PKI (Public Key Infrastructure) cryptosystem is a heavy burden for all communicating nodes in the PPACP and SECSPP, we propose an efficient version without PKI cryptosystems. Furthermore, the speed of encryption/decryption with symmetric encryption schemes is faster than with asymmetric ones, namely PKI cryptosystems. For instance, it is known that DES (Data Encryption Standard) is 100-times faster than RSA in software and 1000-times faster in hardware [17]. Consequently, we treat the computational load of a PKI operation as that of 100 symmetric operations. As listed in Table 3, the PPACP needs nearly 702 symmetric operations and SECSPP needs 740 symmetric operations in the related work, while it requires about 124 symmetric operations in our scheme. Moreover, it takes 0.0005 s to complete a one-way hash operation and 0.0087 s to finish a symmetric en-/de-cryption. We hence ignore the computational load of the one-way hash function, since it is quite lighter than that of a symmetric en-/de-cryption [18]. As a result, computational loads can be reduced to 1.0788 s in our scheme.

Table 3. Comparison of efficiency.

	Our Scheme	PAACP	SECSPP
Authorization Phase	$2T_{sym} + 2T_{hash} + 5T_{xor}$	$4T_{asym} + T_{hash}$	$2T_{asym} + 2T_{exp} + 3T_{hash} + 4T_{xor}$
Access Service Phase	$2T_{sym} + 2T_{exp} + 3T_{xor}$	$3T_{asym} + 2T_{sym} + T_{hash}$	$3T_{asym} + 2T_{exp} + 6T_{hash} + 5T_{xor}$
Computational Costs	$\approx 124T_{sym}$	$\approx 702T_{sym}$	$\approx 740T_{sym}$
Rounds	4	3	5
Authorization ($T_{Authorization}$)	$\approx 0.0174s$	$\approx 3.48s$	$\approx 2.784s$
Access Service ($T_{Accss\ verification}$)	$\approx 1.0614s$	$\approx 2.6274s$	$\approx 3.654s$
Total Costs	$\approx 1.0788s$	$\approx 6.1074s$	$\approx 6.438s$

T_{hash}: Computational cost of one-way function; T_{xor}: Computational cost of Exclusive-OR operation; T_{sym}: Computational cost of symmetric encryption; T_{asym}: Computational cost of asymmetric operation; T_{exp}: Computational cost of modular exponentiation

The following is based on the computation method in PAACP. Assume that n vehicles in the VANET request the services of the same services provider at the same time and the locations where these service requests are invoked are uniformly distributed within m RSUs. The transmission delay $T_{trans-delay}$ is the time in seconds to deliver a message from a vehicle, which is forwarded to the service provider by an RSU. The waiting time $T_{waiting}$ consists of the round-trip transmission delay and the time spent on verification by the service provider. In SECSPP, the average waiting time $T_{waiting}$ for a requesting vehicle can be estimated as:

$$T_{waiting} = 2 \times T_{trans-delay} + \frac{(n+1)}{2} * T_{Accss\ verification}$$

In PAACP and our scheme, the average waiting time $T_{waiting}$ for a requesting vehicle can be estimated as:

$$T_{waiting} = \begin{cases} \frac{(n/m+1)}{2} \times T_{Accss\ verification}, & \text{if } n > m \\ T_{Accss\ verification}, & \text{otherwise} \end{cases}$$

In a uniform distribution of locations, the average number of requests pending in each RSU will be $\frac{n}{m}$. Therefore, the average time spent for request verification in an RSU is $\frac{(n/m+1)}{2} \times T_{Accss\ verification}$. Figure 1 shows that when m is equal to 10, the average waiting time $T_{waiting}$ for a service request from vehicle n increases from 1 to 50. Figures 2, 3 and 4 show that the average waiting time $T_{waiting}$ for a service request from vehicle n increases from 1 to 100 when m is equal to 10, 30 and 50, respectively. As Figure 2 shows, when 100 vehicles are requesting the desired services, the average waiting time $T_{waiting}$ to finish the authentication in PAACP is 14.32 s. In our scheme, the average waiting time $T_{waiting}$ is about 5.73 s. Similarly, as shown in Figure 3, our scheme takes about 2.28 s, compared to about 5.65 s for PAACP. Finally, our scheme takes about 1.59 s, compared to PAACP's average of about 3.94 s, as shown in Figure 4. In summary, the average waiting time $T_{waiting}$ decreases when RSU increases.

Figure 1. Average waiting time when m is equal to 10.

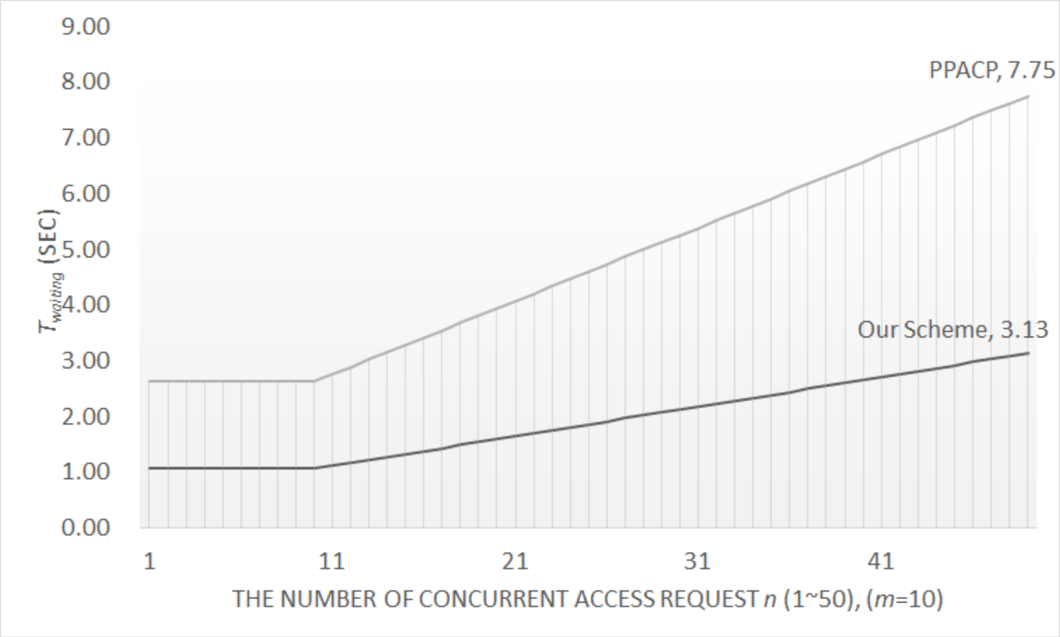


Figure 2. Average waiting time when m is equal to 10.

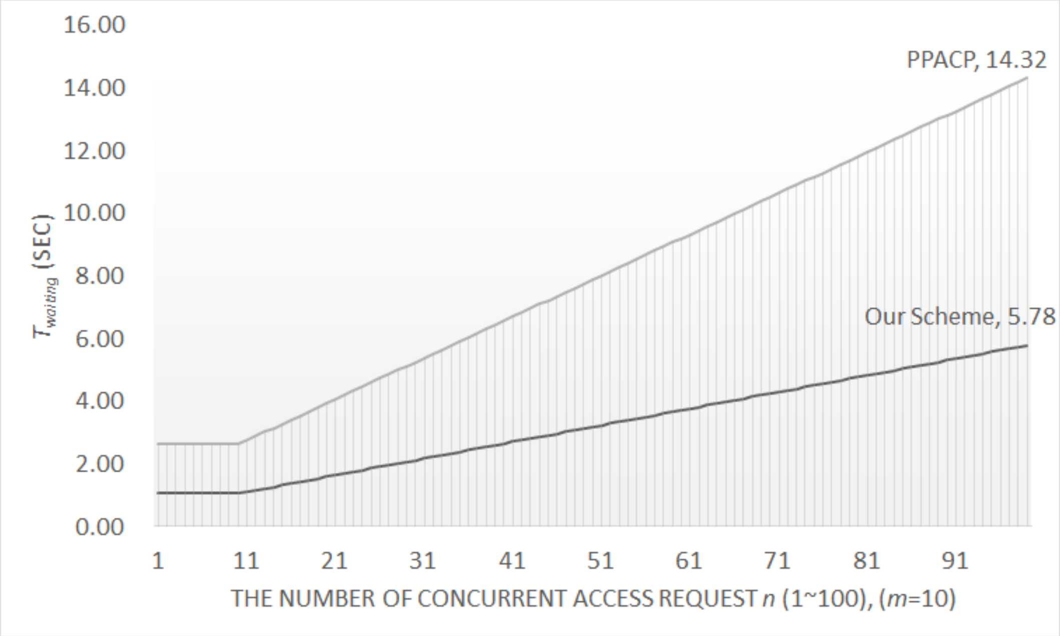


Figure 3. Average waiting time when m is equal to 30.

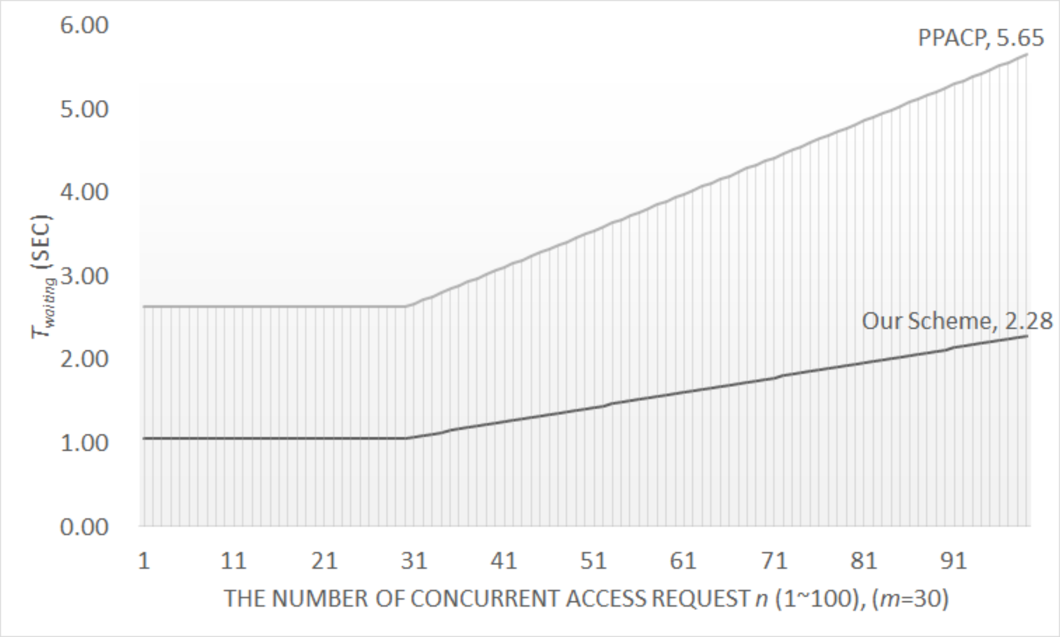
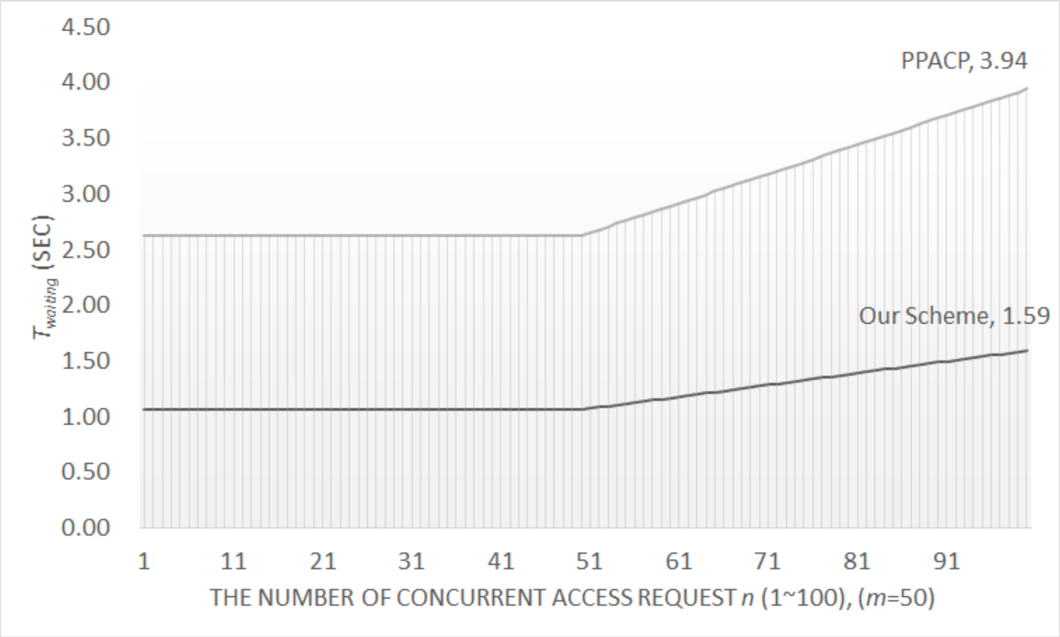


Figure 4. Average waiting time when m is equal to 50.



4.3. Security Analysis

The other security features of our new scheme are also discussed below:

Forward secrecy: This security means that before a V_i wants to access the $(n+1)$-th service, he/she cannot decrypt the service request message that existed prior to his/her session key $K_V + n$. Our scheme can attain forward secrecy because, if a V_i requests next $(Service\ request\ message)_{(n+1)-th}$, then a new $K_V + (n+1)$ will be generated by the $(n+1)$-th service.

Backward secrecy: After a user logs out of the server, he/she cannot receive any services belonging to the left server. After a V_i accesses the n-th service, he/she cannot decrypt the service request message that existed posterior to his/her session key $K_V + (n+1)$. Our scheme can attain backward secrecy, because after a V_i requests next $(Service\ request\ message)_{(n+1)-th}$, the session key $K_V + (n+1)$ will be generated, and the $K_V + (n)$ will be invalid.

Authentication: A V_i must submit his or her authentication request message (VID_i, C, N_i) to the service provider S_t, and then, the S_t acknowledges the V_i. After receiving the authentication request message, the S_t encrypts the message $M = E_{y_i \oplus AC_i^{S_t}}\{N_s, N_i, AC_i^{S_t}\}$ to facilitate a mutual authentication between the vehicle and the service provider.

Authorization: In the registration phase, the service provider creates a service right list by the following equation:

$$SRL_i^{V_i} = \{SVID_1 \| AR_1 \| SVID_2 \| AR_2 \| \ldots \| SVID_k \| AR_k\}$$

where $SVID_k$ denotes the index of the k-th service and AR_k represents the granted access privileges of $SVID_k$. Hence, anyone can determine who has which access privileges to access which service. Only valid V_i can encrypt $E_{K_V}(SVID_1 \parallel AC_i)$ with K_V. After R_j receives $E_{K_V}(SVID_1 \parallel AC_i)$, R_j will decrypt the message:$D_{K_R}(E_{K_V}(SVID_1 \parallel AC_i))$ with K_R to gain $(SVID_1 \parallel AC_i)$ and then derive AC_i and $SVID_1$, because of $K_V = K_R$.

Replay attack: In the registration phase, a V_i submits his/her registration information over a secure channel, so there are not any replay attack issues. In the authorization phase, an old message was eavesdropped by an attacker. He/she may try to replay the old message (VID_i, C, N_i). It may fail because it is not always the same, and the nonce N_i is a random number that is generated and has a value that has not been used before, to avoid replay attack and the serious time synchronization problem.

5. Conclusion

In this paper, we review a cryptanalysis of an attachable blind signature and demonstrate that the PAACP's AC is not secure and private, even if the AC is secretly stored in a tamper-proof device. An eavesdropper can construct the AC from an intercepted blind document. Consequently, during the authorization phase, PAACP is breakable and cannot maintain privacy in VANETs. Consequently, any outsiders can determine who has which access privileges to access which service.

Furthermore, this paper efficiently copes with these challenges and proposes an efficient scheme. We conclude that an improved authentication scheme and access control protocol for VANETs not only resolves the documented problems, but also is secure and efficient. Compared with PAACP and SECSPP, our scheme achieves more functionality and satisfies the security features required by VANETs. Future research can focus on the many commercial applications [19–23].

Author Contributions

Wei-Chen Wu was responsible for planning, design, analysis and writing the manuscript. Yi-Ming Chen reviewed the manuscript. Both authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Chung, Y.; Choi, S.; Won, D. Lightweight anonymous authentication scheme with unlinkability in global mobility networks. *J. Converg.* **2013**, *4*, 23–29.
2. Taysi, Z.C.; Yavuz, A.G. ETSI compliant GeoNetworking protocol layer implementation for IVC simulations. *Hum.-Centric Comput. Inf. Sci.* **2013**, *3*, 1–12.
3. Singh, R.; Singh, P.; Duhan, M. An effective implementation of security based algorithmic approach in mobile adhoc networks. *Hum.-Centric Comput. Inf. Sci.* **2014**, *4*, 1–14.
4. Peng, K. A secure network for mobile wireless service. *J. Inf. Process. Syst.* **2013**, *9*, 247–258.
5. Chen, Y.M.; Wei, Y.C. SafeAnon: A safe location privacy scheme for vehicular networks. *Telecommun. Syst.* **2012**, *50*, 339–354.
6. Wei, Y.C.; Chen, Y.M. Safe distance based location privacy in vehicular networks. In Proceedings of the 2010 IEEE 71st Vehicular Technology Conference (VTC 2010-Spring), Taipei, Taiwan, 16–19 May 2010; pp. 1–5.
7. Raya, M.; Hubaux, J. The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM Workshop on Security of Ad hoc and Sensor Networks, Alexandria, VA, USA, 7–10 November 2005.
8. Wang, N.; Huang, Y.; Chen, W. A novel secure communication scheme in vehicular ad hoc networks. *Comput. Commun.* **2008**, *31*, 2827–2837.
9. Wischhof, L.; Ebner, A.; Rohling, H. Information dissemination in self-organizing intervehicle networks. *IEEE Trans. Intell. Transp. Syst.* **2005**, *6*, 90–101.
10. Isaac, J.; Camara, J.; Zeadally, S.; Marquez, J. A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks. *Comput. Commun.* **2008**, *31*, 2478–2484.
11. Yousefi, S.; Mousavi, M.; Fathy, M. Vehicular ad hoc networks (VANETs): Challenges and perspectives. In Proceedings of the 6th International Conference on ITS Telecommunications, Chengdu, China, 21–23 June 2006; pp. 761–766.
12. Zhang, C.; Lin, X.; Lu, R.; Ho, P.; Shen, X. An efficient message authentication scheme for vehicular communications. *IEEE Trans. Veh. Tech.* **2008**, *57*, 3357–3368.
13. Yeh, L.; Chen, Y.; Huang, J. PAACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks. *Comput. Commun.* **2011**, *34*, 447–456.
14. Li, C.; Hwang, M.; Chu, Y. A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks. *Comput. Commun.* **2008**, *31*, 2803–2814.
15. Wu, W.; Chen, Y. Cryptanalysis of a PAACP: A portable privacy-preserving authentication and access control protocol in Vehicular Ad Hoc Networks. *Appl. Math. Inf. Sci.* **2012**, *6*, 463S–469S.
16. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654.

17. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed.; John Wiley & Sons: New York, NY, USA, 1996.
18. Chen, H.B.; Hsueh, S.C. Light-weight authentication and billing in mobile communications. In Proceedings of the IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, Taipei, Taiwan, 4–16 October 2003; pp. 245–252.
19. Kim, H.I.; Kim, Y.K.; Chang, J.W. A grid-based cloaking area creation scheme for continuous LBS queries in distributed systems. *J. Converg.* **2013**, *4*, 23–30.
20. Oh, J.S.; Park, C.U.; Lee, S.B. NFC-based mobile payment service adoption and diffusion. *J. Converg.* **2014**, *5*, 8–14.
21. Følstad, A.; Hornbæk, K.; Ulleberg, P. Social design feedback: Evaluations with users in online ad-hoc groups. *Hum.-Centric Comput. Inf. Sci.* **2013**, *3*, 1–27.
22. Park, S.W.; Lee, I.Y. Anonymous authentication scheme based on NTRU for the protection of payment information in NFC mobile environment. *J. Inf. Process. Syst.* **2013**, *9*, 461–476.
23. Gohar, M.; Koh, S.J. A network-based handover scheme in HIP-based mobile metworks. *J. Inf. Process. Syst.* **2013**, *9*, 651–659.