Expert Systems with Applications 41 (2014) 2559–2564

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

Improvements on an authentication scheme for vehicular sensor networks

Joseph K. Liu [a,*], Tsz Hon Yuen [b], Man Ho Au [c], Willy Susilo [c]

[a] Institute for Infocomm Research, Singapore
[b] University of Hong Kong, Hong Kong
[c] Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, Australia

ARTICLE INFO

Keywords:
Authentication
Vehicular sensor networks

ABSTRACT

In a recent paper, Shim (2012) presented a very interesting authentication scheme for vehicular sensor networks. Shim claimed that the scheme is secure against the highest adopted level of attack, namely the chosen-message attack (CID-CMA). Nevertheless, we find that the proof in Shim's paper *does not* actually prove that the scheme is secure in this level. Instead, it can only ensure that the scheme is secure in a strictly weaker level of attack, the adaptive chosen-identity and *no-message* attack (CID-NMA). In this paper, first we show that there exist some security risks in vehicular networks if a scheme, which is only secure against CID-NMA but not CID-CMA, is deployed. Hence, having the proof that the scheme is only CID-NMA is insufficient for the aforementioned application. That is, Shim *did not* prove that the proposed scheme can resist these kinds of attack. Here, we use a different approach to prove the scheme for security against CID-CMA. We note that this proof is essential to ensure that the scheme can indeed be used for the aforementioned scenario. In addition, we also show that the batch verification of the scheme, proposed in the same paper, may have non-negligible error. Two invalid signatures may give a positive result. We further improve the batch verification part so that the error rate can be reduced to negligible level.

1. Introduction

With the advancement of mobile technology, wireless networks have become widely available. Car manufactures and telecommunication industries have started to equip vehicles with wireless devices for interconnection. Cars can communicate with other cars or the roadside infrastructure to improve driving safety or exchange traffic information. These types of vehicular communication networks are usually referred as vehicular ad hoc networks (VANETs). Within the infrastructure of VANETs, privacy and security are the two major challenges. No driver wants to broadcast his/her real identity and current location while in contrast, authentication is required at the same time. Otherwise, one may send some wrong messages or pretend others to send messages. There are many schemes in the literature (such as Sun, Lu, Lin, Shen, & Su, 2010; Huang, Yeh, & Chien, 2011; Huang, Misra, Verma, & Xue, 2011; Sun, Feng, Hu, & Su, 2012) that deal with these two seeming contradictory requirements.

Recently, Shim (2012) proposed a conditional privacy-preserving authentication scheme for vehicular sensor networks. It is based on an Identity-based Signature (IBS) scheme proposed in the same paper. Shim adopted the security definition and model of the IBS schemes in Shim (2010). The security model is the normal existential unforgeable against adaptive chosen-identity and chosen-message attack (CID-CMA), which is considered to be the strongest security notion of IBS scheme. Under this notion, the adversary is allowed to query an extraction oracle and a signing oracle. When it submits an identity to the extraction oracle, it returns a private key corresponding to this identity. When it submits a message and an identity to the signing oracle, it returns a valid signature corresponding to this message and identity. After adaptively querying these oracles, the adversary outputs a challenged identity, a challenged message and a valid signature corresponding to this identity and message. The restriction is that: the adversary is not allowed to query the challenged identity to the extraction oracle and the challenged identity-message pair to the signing oracle. However, it is allowed to query the signing oracle for the challenged identity with other messages.

On the other side, in an adaptive chosen-identity and *no-message* attack (CID-NMA), it is similar to CID-CMA except that no signing oracle is provided. In other words, the adversary is not allowed to see any signature corresponding to the challenged identity. If it happens to see a signature (of any message) from this

[*] Corresponding author. Tel.: +65 82117031.
E-mail addresses: ksliu@i2r.a-star.edu.sg (J.K. Liu), thyuen@cs.hku.hk (T.H. Yuen), aau@uow.edu.au (M.H. Au), wsusilo@uow.edu.au (W. Susilo).

0957-4174/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.eswa.2013.10.003

identity, it may produce some forged signatures or pretend to be this identity to sign some messages. It is a strictly weaker security notion for IBS scheme. If a scheme can only achieve CID-NMA security, it should not be used in general except in the case that the identity can only produce one signature in the whole life time (e.g. one-time signature Bicakci, Tsudik, & Tung, 2003; Mohassel, 2010).

This Work. The contribution of this paper can be categorized as follow:

1. We find that there is a flaw in the proof of the IBS in Shim (2012). Although it is claimed to be CID-CMA, we show that the proof of the corresponding theorem cannot attend the claimed security. Instead, only a strictly weaker security, the CID-NMA can be achieved.
2. We describe a list of security risks in VANETs for deploying an authentication scheme which is only CID-NMA secure. In other words, if the scheme in Shim (2012) is used, it cannot prove that it can resist such kinds of attacks.
3. We attempt to provide the correct proof for Shim's IBS using a completely different approach. In our proof, we show that the IBS scheme in Shim (2012) is CID-CMA secure.
4. In addition, Shim also deployed a batch verification on the signature scheme. We demonstrate that the false acceptance rate is non-negligible: we can easily construct two invalid signatures such that when they are batched together for verification, they become valid signatures. That is, they can pass through the batch verification equation. We further modify the batch verification part to reduce this false acceptance to a negligible level, which is our final contribution in this paper.

2. Related works

We discuss some of the related works here and explain why our improved version has some advancement over existing works.

In the area of security and privacy of Vehicular Ad Hoc Networks (VANETs), a number of research works have been done on anonymous authentication to ensure security and privacy. A majority of these schemes make use of pseudonyms (e.g. Calandriello, Papadimitratos, Hubaux, & Lioy, 2007; Sun et al., 2010; Huang, Misra, et al., 2011) or anonymous credentials (e.g. Chim, Yiu, Hui, & Li, 2011; Gonzalez-Tablas, Alcaide, de Fuentes, & Montero, 2013). A recent approach is to use signature-based technique (e.g. Kounga, Walter, & Lachmund, 2009; Chen, Ng, & Wang, 2011) to achieve anonymous authentication. All these schemes are suitable for authorization. However, these pseudonym-based authentication schemes are prone to generate a huge revocation list, as pointed out in Shim (2012). Another approcah is to deploy group signature (e.g. Lin, Sun, Ho, & Shen, 2007; Lin, Sun, Ho, & Shen, 2008; Sun, Zhang, Zhang, & Fang, 2010) to achieve anonymous authentication. But the verification cost in group-signature-based schemes is too expensive for devices in VANETs which may require very fast verification time. Similar to a group signature, a ring signature (Chaurasia & Verma, 2011; Yuen, Liu, Au, Susilo, & Zhou, 2013; Au, Liu, Susilo, & Yuen, 2013) can also be used to provide privacy preserving capability. By removing the need for a group manager and allowing a signer to create an ad hoc group membership, a ring signature scheme can be used for in applications with the competing requirements of message authenticity and signer privacy. However, facing the same obstacle as group signature, the verification of ring signature is not efficient enough. On the other side, identity-based schemes (e.g. Zhang, Lu, Lin, Ho, & Shen, 2008; Shim, 2012) allow fast or batch verification that is particularly suitable for vehicular communications. Nevertheless, the scheme in Zhang et al. (2008) required the long-term system master key preloaded into *all* tamper-proof devices and the security rely on it. In practice, these tamper-proof devices may be subjected to side-channel attacks. The compromised of one device results in the leakage of the master secret key which is a serious security flaw in the whole system. The scheme in Shim (2012) does not contain this risk, though there is a flaw in their security proof and their batch verification is not always sound, as we mentioned in the last section.

We summarize the comparison among these cryptographic primitives in Table 2.

3. Security risks in VANETs for deploying an insecure scheme

In this section, we present some concrete security risks in VANETS if an insecure scheme (or not secure enough in an acceptable level) is deployed as the underlying security primitive.

3.1. Deploying a scheme which is only CID-NMA secure – message forgery

We first demonstrate that by incorporating an Identity-based Signature (IBS) scheme, which is only CID-NMA secure, in VANETs, then some practical security risks in the whole system may be presented.

In the following, we consider the same scenario as in Shim (2012). There are some communications between the road side unit (RSU) and vehicles. When the RSU sends an authenticated message to vehicles, it uses the underlying IBS scheme to sign a message. Upon receiving the message, the vehicle verifies the signature corresponding to the RSU. If the scheme is only CID-NMA secure but not CID-CMA secure, the vehicle cannot ensure that the received signature is really signed by the RSU. This is because an adversary can pretend to be the RSU to generate a valid message (once it has seen a valid signature by the RSU), and hence, the authenticity is lost.

Additionally, when a vehicle sends an authenticated message to the RSU, it signs the message with his/her pseudo-identity. When an adversary obtains this signature from this pseudo-identity, it can produce another valid signature for this pseudo-identity within the valid time period although it does not have its private key. This may result in a message forgery. The adversary can then deliberately send false and harmful messages using this pseudo-identity as it is no longer accountable to the adversary but the pseudo-identity of the victim. This results in the security breakdown of the whole system.

3.2. False acceptance on batch verification

In a batch verification, the whole batch would be dropped or rejected, even if there is just one false signature in the batch. It should be a deterministic process with no exception. Otherwise, a harmful message may get through the batch verification process (that is, the authentication gateway) to jeopardize the safety of the traffic system. An adversary may take advantage of this loophole by injecting some harmful messages in each authentication cycle. This attack may bring fatal traffic consequences for a VANET-based traffic system.

Roadmap. In the next section, we will show that the proof for the IBS in Shim (2012) only shows that the scheme is secure against CID-NMA but not CID-CMA. That is, Shim (2012) did not prove that the proposed authentication scheme can resist against the attack mentioned above. Due to the lack of this proof, then the scheme in Shim (2012) may not be able to be adopted in the VANET scenario mentioned in the original paper. Fortunately, in Section 5, we are able to provide the correct proof so that the scheme achieves CID-CMA.