Comments on "Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks"

Jiannan Wei, Guomin Yang, *Member, IEEE*, and Yi Mu, *Senior Member, IEEE*

***Abstract*—In a recent paper (IEEE Trans. Wireless Commun., vol. 14, no. 1, 2015), He *et al.* proposed an accountable and privacy-enhanced access control (APAC) protocol, which aimed to provide privacy for honest users against network owners and accountability against misbehaving users without the involvement of any trusted third party. However, the level of trust on the network owner has not been clearly defined in He *et al.*'s paper, and we demonstrate in this letter that in the case where the network owners cannot be trusted to correctly generate the system parameters, then the APAC protocol cannot ensure user privacy.**

***Index Terms*—Access control, wireless sensor network, user privacy, accountability.**

I. Introduction

WIRLESS sensor networks (WSNs) are widely used in many practical applications, in which user privacy is an important criterion in the design of a wireless communication protocol. In a recent work [3], He et al. proposed an accountable and privacy-enhanced access control (APAC) protocol for WSNs under the goal of providing privacy for honest users against the network owners and accountability against dishonest/misbehaving users. However, we found that the trust model given in [3] (Section III-B) is not clearly defined in terms of the capability and behavior of the potential adversaries such as the network owners. In this letter, we demonstrate that in the case where the network owner cannot be trusted to correctly generate the system parameters, then the APAC protocol cannot ensure user privacy.

II. The Security Issue of APAC

A. A High-Level Description of The Problem

The APAC protocol proposed in [3] is based on a cryptographic primitive named Group Signature [2], [4], which allows a group user to anonymously generate a signature on behalf of the whole group. A signature verifier can only tell that the signature is generated by one of the group members, and only a trusted group manager can reveal the identity of the real signer. One basic security condition of group signature is that *the system parameters must be honestly generated by a fully trusted party (e.g., the group manager)*.

Group signature is used as the main building block in the design of the APAC protocol [3]. However, in order to eliminate the need of a fully trusted party, the APAC protocol employed the separation of duties principle to split the fully trusted party into two different entities, namely a Law Authority and a Network Owner. That is, in the APAC protocol, the Law Authority and the Network Owner will generate the system parameters, which is originally done by a fully trusted party in group signature.

It is easy to see that if either the law authority or network owner is not trusted (i.e., one of them does not generate the system parameters honestly), then the basic security condition of group signature highlighted above will be violated even if the two parties don't collude. As a result, the security properties of a group signature cannot be maintained, which in turn will directly affect the security of the APAC protocol. In APAC, the network owner is considered as an adversary against user privacy which is achieved by the anonymity of group signature. If the network owner does not generate the system parameters honestly, then the anonymity of the group signature cannot be preserved, and in turn the network owner can break the user privacy of APAC easily.

In the rest of this section, we demonstrate the security problem of APAC described above using the concrete APAC protocol presented in [3]. We must stress that the underlying group signature [2] itself has no security issue under the condition that the system parameters are honestly generated by a trusted party. We should also note that changing the underlying group signature scheme cannot solve the problem since the condition is required by all the group signature schemes. Therefore, the APAC protocol can achieve its original goals only under the assumption that the network owner and the law authority are trusted in generating the system parameters. Although [3] makes some assumptions on how much the network owner and the law authority can be trusted, it does not specify their level of reliability in generating the scheme parameters in a clear way.

B. A Concrete APAC Protocol [3]

There are three types of entities in the system, including a law authority, the network owners and the network users. Below we review the APAC protocol which includes *System setup phase*, *User joining phase*, *User query phase*, and *Receiver verification phase*.

System setup phase: The law authority is responsible for the generation of the partial group private key and partial group public key of the whole network. The law authority proceeds as follows. (1) Randomly select an l_Q-bit prime Q and an

Manuscript received April 16, 2015; revised June 29, 2015, September 10, 2015, and November 25, 2015; accepted November 27, 2015. Date of publication December 9, 2015; date of current version April 7, 2016. The associate editor coordinating the review of this paper and approving it for publication was C.-F. Chiasserini.

The authors are with the Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong, N.S.W. 2522, Australia (e-mail: jw903@uowmail.edu.au; gyang@uow.edu.au; ymu@uow.edu.au).

Digital Object Identifier 10.1109/TWC.2015.2507124

l_P-bit prime P such that $Q|P-1$. Let F be an element of order Q in $\mathbb{Z}_P^*$. (2) Randomly choose $X_G, X_H \in \mathbb{Z}_Q$ and set $G = F^{X_G} \bmod P$, $H = F^{X_H} \bmod P$. (3) Send partial group public key $\{Q, P, F, G, H\}$ to network owners, possibly via an open wireless channel, and keep partial group private key X_G secretly.

Additionally, each network owner prepares the full group public key and partial group private key as follows. (1) Choose an l_n-bit RSA modulus $n = pq$ as a product of two safe primes p and q. Select at random $a, g, h, w \in QR_n$. QR_n denotes the set of all quadratic residues of $\mathbb{Z}_n^*$. (2) Keep the partial group private key (p, q) secretly. The group public key is $gpk = \{n, a, g, h, w, Q, P, F, G, H\}$ and the group private key $gsk = \{X_G, p, q\}$. Notice that neither the network owner nor the law authority knows the full gsk. The group public key gpk is distributed to all the users.

New user joining phase: In order to join a group managed by a network owner, the user performs the following steps. (1) Select a random number $x_i \in \mathbb{Z}_Q$ and compute $Y_i = G^{x_i} \bmod P$. (2) Form a commitment to x_i, which is $g^{x_i} h^{r'_i} \bmod n$ with $r'_i \in \mathbb{Z}_n$, and prove the knowledge of x_i, r'_i. The partial member secret key is $\{x_i, r'_i\}$. (3) Send $(Y_i, g^{x_i} h^{r'_i} \bmod n)$ and the proof to owner j via a secure channel.

Upon receipt of the message, owner j prepares the other partial member secret key of user i as follows. (1) Choose a random l_e-bit number e_i such that $E_i = 2^{l_E} + e_i$ is prime. (2) Compute $\omega_i = \omega^{E_i^{-1}} \bmod n$ based on the knowledge of (p, q). (3) Choose a random number $r''_i \in \mathbb{Z}_e$ and set $y_i = (a g^{x_i} h^{r'_i + r''_i})^{E_i^{-1}} \bmod n$. (4) Transmit $\{grp_j, \omega_i, y_i, E_i, r''_i\}$ back to user i via a secure channel, where grp_j indicates the identity of the group. Finally, user i sets his/her member secret key $msk_i = \{gpk, \omega_i, x_i, r_i, y_i, e_i\}$ where $r_i = r'_i + r''_i$.

User query generation phase: User i generates a query request req and also a group signature on $h(req||grp_j)$ using his/her member secret key msk_i as follows, where $h(\cdot)$ denotes a hash function. (1) Select a random number $r \in \{0,1\}^{l_n/2}$ and $R \in \mathbb{Z}_Q$. (2) Compute $u = h^r y_i \omega_i \bmod n$, $U_1 = F^R \bmod P$, $U_2 = G^{R+x_i} \bmod P = G^R Y_i \bmod P$, $U_3 = H^{R+e_i} \bmod P$. (3) Choose $r_x \in \{0,1\}^{l_Q+l_c+l_s}$, $r_r \in \{0,1\}^{l_n/2+l_c+l_s}$, $r_e \in \{0,1\}^{l_e+l_c+l_s}$ and $R_R \in \mathbb{Z}_Q$ and compute $v = u^{r_e} g^{-r_x} h^{r_r} \bmod n$, $V_1 = F^{R_R} \bmod P$, $V_2 = G^{R_R+r_x} \bmod P$, $V_3 = H^{R_R+r_e} \bmod P$. (4) Generate a challenge $c = h(gpk, u, v, U_1, U_2, U_3, V_1, V_2, V_3, h(req||grp_j))$ and set $z_x = r_x + cx_i$, $z_r = r_r + c(-r_i - rE_i)$, $z_e = r_e + ce_i$ and $Z_R = R_R + cR$. The group signature σ is $(c, u, U_1, U_2, U_3, z_x, z_r, z_e, Z_R)$.

Receiver verification phase: The following steps are used to verify a group signature σ generated by a user. (1) Check that $z_e \in \{0,1\}^{l_e+l_c+l_s}$ and $z_x \in \{0,1\}^{l_Q+l_c+l_s}$. (2) Set $v = (a\omega)^{-c} g^{-z_x} h^{z_r} u^{c*2^{l_E}+z_e} \bmod n$, $V_1 = U_1^{-c} F^{Z_R} \bmod P$, $V_2 = U_2^{-c} G^{Z_R+z_x} \bmod P$, $V_3 = U_3^{-c} H^{Z_R+z_e} \bmod P$. (3) Check if the challenge c is correct: $c \overset{?}{=} h(gpk, u, v, U_1, U_2, U_3, V_1, V_2, V_3, h(req||grp_j))$.
The group signature is accepted if and only if the equation holds.

C. The User Privacy Issue in the Concrete Protocol

One of the security goals of the APAC protocol is to achieve privacy of an honest user against the network owner. However, below we show that a dishonest network owner who does not generate the system parameters honestly can locate the identity of a network user *without being detected*.

We first review some background knowledge on groups.

Definition 1 (Sub-group Decision Problem [1]): Given a group $\mathbb{G}$ of composite order $n = pq$ where p and q are distinct (unknown) primes, a generator g_p of the subgroup $\mathbb{G}_p$ with order p and a generator g of the whole group $\mathbb{G}$, it is computationally infeasible to decide whether an element T is a random element of the subgroup $\mathbb{G}_p$ or a random element of the group $\mathbb{G}$.

In the APAC protocol, the group QR_n is a group of order $p'q'$ where $p' = (p-1)/2$ and $q' = (q-1)/2$ are both primes since p, q are safe primes. Suppose that the network owner is dishonest, then it could perform the following steps to break the user privacy. (1) During the *System setup phase*, after generating p, q, n where $n = pq$, $p = 2p'+1$, $q = 2q'+1$, instead of choosing $a, g, \omega, h \in QR_n$, the network owner selects $a, g, \omega \in QR_n$ and $h \in \mathbb{G}_{p'}$ where $\mathbb{G}_{p'}$ is the subgroup of QR_n with order p'. Due to the difficulty of the *sub-group decision problem*, no one can detect such a modification in the system parameters. (2) In the *User joining phase*, after generating $(\omega_i, y_i, E_i, r''_i)$ for user i, the network owner also saves $\zeta_i = (y_i\omega_i)^{p'} \bmod n$ in its database. Notice that since a, g, ω are randomly chosen from QR_n, the probability that they fall in the subgroup $\mathbb{G}_{p'}$ is $1/q'$ which is negligible. Hence, with overwhelming probability, $\zeta_i \neq 1$. Also, since the values of x_i and E_i are different for different users, the probability of a collision (i.e., $\zeta_i = \zeta_j$) is also negligible. Also notice that since E_i is chosen by the network owner, it can always regenerate a new E_i if the value ζ_i has appeared before. (3) In the *User query generation phase*, given a group signature $\sigma = (c, u, U_1, U_2, U_3, z_x, z_r, z_e, Z_R)$, the network owner computes $\zeta^* = u^{p'} = (h^r y_i \omega_i)^{p'} = (y_i\omega_i)^{p'} \bmod n$ and searches its database to find $\zeta_i = \zeta^*$, which reveals the identity of the signer.

III. Conclusion

In this letter, we revisited an accountable and privacy-enhanced access control (APAC) scheme [3] for wireless sensor networks, and showed that there is a security issue in the scheme. We also demonstrated this issue using a concrete APAC scheme given in [3]. Our conclusion is that the problem cannot be fixed without introducing an assumption in the trust model.

Acknowledgment

We thank Dr. Carla-Fabiana Chiasserini and the anonymous reviewers for their helpful comments and suggestions.

References

[1] D. Boneh, A. Sahai, and B. Waters, "Fully collusion resistant traitor tracing with short ciphertexts and private keys," in *Proc. Adv. Cryptol.—EUROCRYPT*, 2006, pp. 573–592.

[2] J. Camenisch and J. Groth, "Group signatures: Better efficiency and new theoretical aspects," in *Security in Communication Networks*, New York, NY, USA: Springer, 2005, pp. 120–133.

[3] D. He, S. Chan, and M. Guizani, "Accountable and privacy-enhanced access control in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 389–398, Jan. 2015.

[4] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. Adv. Cryptol.—CRYPTO*, 2004, pp. 41–55.

Jiannan Wei received the M.S. degree from Zhengzhou University, China, in 2012. She is currently pursuing the Ph.D. degree in computer science and software engineering at the University of Wollongong, Wollongong, N.S.W., Australia. Her research interests include public key cryptography, privacy-preserving digital signatures, and wireless network security.

Guomin Yang (M'13) received the Ph.D. degree in computer science from the City University of Hong Kong, Hong Kong, in 2009. He worked as a Research Scientist with the Temasek Laboratories, National University of Singapore (NUS), Singapore, from September 2009 to May 2012. He is currently a Senior Lecturer and an ARC DECRA Fellow with the School of Computing and Information Technology, University of Wollongong, Wollongong, N.S.W., Australia. His research interests include applied cryptography and network security.

Yi Mu (M'03–SM'03) received the Ph.D. degree from the Australian National University, Canberra, A.C.T., Australia, in 1994. He is currently a Professor and the Co-Director of the Centre for Computer and Information Security Research with the University of Wollongong, Wollongong, N.S.W., Australia. His research interests include information security and cryptography. He is a member of the IACR. He is the Editor-in-Chief of the *International Journal of Applied Cryptography* and serves as an Associate Editor for 10 other international journals.