International Journal of Multimedia and Ubiquitous Engineering
Vol.9, No.1 (2014), pp.361-368
http://dx.doi.org/10.14257/ijmue.2014.9.1.33

Anonymous Electronic Voting Protocol with Deniable Authentication for Mobile Ad Hoc Networks

Maede Ashouri-Talouki[1] and Ahmad Baraani-Dastjerdi[2]

[1]*Department of Information Technology Engineering,*
[2]*Department of Computer Engineering,*
Faculty of Engineering, The University of Isfahan, Isfahan, Iran

{[1]ashoori,[2]ahmadb}@eng.ui.ac.ir

Abstract

This paper analyzes Chun et al.'s e-voting protocol for mobile ad-hoc network and modifies it based on blind signature technique to support anonymous voting property. Based on this property the trusted node cannot learn who has voted for whom. As the previous protocol, the modified protocol does not need any centralized administration. We analyze security and computation cost of the proposed protocol and show that it is well suited for mobile environments.

Keywords: *E-Voting, Anonymous Voting, Mobile ad hoc networks, Blind Signature, Cryptography*

1. Introduction

Electronic voting is an important topic in the field of group decision. There are a huge number of protocols to provide e-voting in wired or wireless environments [1-12]. In 2008 Chun *et al.*, [1] proposed an e-voting scheme for mobile ad hoc network that provides deniable authentication property [1]. In deniable authentication encryption scheme, the receiver could verify the integrity of a message, but could not prove the source of a message to any third party, even if he/she cooperates with the third party.
We analyze this protocol and modify it to support anonymous voting property. The structure of the paper is as follows. Section 2 reviews Chun *et al.*'s electronic voting protocol. We explain anonymity problem of Chun *et al.*'s protocol in Section 3. Section 4 describes our solution to this problem. We analyze our protocol in Section 5 and conclude it in Section 6.

2. Chun *et al.*'s Protocol

Chun *et al.*'s e-voting protocol has two phases: authentication phase and voting phase that describe bellow [1].

2.1. Authentication phase

In this phase, each voter is authenticated by the chosen group leader (System) during the following steps:

First: System (S) generates a unique tag number $(tag\#)$ for a vote, selects a random number $a \in GP(p)$ to compute $X = g^a$ and forms message Msg_S^1 through equation (1); then broadcasts message Msg_S^1 to all voters, where σ_S^1 is the S's signature on Msg_S^1, ID_S is S's

ISSN: 1975-0080 IJMUE

identifier, N_S is a nonce chosen by S and m is a blank ballot.

$$(Msg_S^1 = \{tag\#, ID_S, N_S, X, m\}, \sigma_S^1) \quad (1)$$

Second: Each voter verifies the validity of message Msg_S^1 through equation (2). If it holds, the voter selects a random number $b \in GP(p)$ and computes $Y = g^b$ and forms message Msg_{V_i} through equation (3); otherwise stops.

$$VA_{pk_s}(Msg_S^1, \sigma_S^1) \stackrel{?}{=} 1 \quad (2)$$

$$(Msg_{V_i} = \{tag\#, ID_S, N_S, ID_{V_i}, N_{V_i}, Y\}, \sigma_{Vi}) \quad (3)$$

Then the voter sends message Msg_{V_i} to S.

Third: S verifies the validity of voter (V_i) and the validity of message Msg_{V_i}. If both are hold, S computes $V_{S,V_i} = Y^a = g^{ab}$ and stores $(ID_{V_i}, N_{V_i}, V_{S,V_i})$ in his database; otherwise stops.

Forth: After receiving all the replies from all voters, S generates Msg_S^2, and broadcasts it to all voters. s

$$(Msg_S^2 = \{tag\#, ID_S, N_S, H(ID_{V_i}, N_{V_i}, V_{S,V_i})\}, \sigma_S^2) \quad (4)$$

Fifth: Finally each voter verifies the validity of message Msg_S^2 through equation (2). If it holds, each voter V_i computes $V'_{S,V_i} = X^b = g^{ab} = Y^a$.Then the voters checks whether $H(ID_{V_i}, N_{V_i}, V'_{S,V_i})$ is equal to $H(ID_{V_i}, N_{V_i}, V_{S,V_i})$ or not. If the equation holds, the voter V_i and the System have a common and unique vote $(ID_{V_i}, N_{V_i}, V_{S,V_i})$.

2.2. Voting phase

In this phase, each voter starts to vote by the following steps:

First: Each voter V_i selects his vote m_i , challenge e_i and computes $SK_S^{V_i} = Y_S^{xv_i} = g^{xsxv_i} = Y_{V_i}^{xs} = SK_{V_i}^S$, where $SK_S^{V_i}$ is a static shared key between S and V_i. Notice that $(Y_S = g^{sx}, sx)$ is the public/private key of S and $(Y_{V_i} = g^{xv_i}, xv_i)$ is the public/private key of the voter V_i. Then V_i computes message $Msg_{V_i}^2$ and sends it to S, where E_{pk_s} is the encryption of a message with S's public key:

$$(Msg_{V_i}^2 = \{tag\#, ID_S, N_S, E_{pk_s}(ID_{V_i}, N_{V_i}, m_i, challenge_i, H(ID_{V_i}, N_{V_i}, V'_{S,V_i}, m_i, SK_{V_i}^S))\} \quad (5)$$

Second: S verifies the validity of the $tag\#$, then S uses its private key to decrypt the message and gets the parameters. Afterward, S computes $SK_S^{V_i} = Y_{v_i}^{xs} = g^{xsxv_i} = Y_S^{xv_i}$ and verifies equation (6):

$$H(ID_{V_i}, N_{V_i}, V_{S,V_i}, m_i, SK_S^{V_i}) \stackrel{?}{=} H(ID_{V_i}, N_{V_i}, V'_{S,V_i}, m_i, SK_{V_i}^S) \quad (6)$$

If it holds, the vote m_i is counted and $(ID_{V_i}, N_{V_i}, V_{S,V_i})$ is marked as non-fresh; otherwise

stops.

Third: To prove the correctness of the results, S sends $E_{SK_S^{V_i}}[challenge_i + 1]$ to each V_i. Then V_i recovers $challeng_{ei}$ and is convinced that his vote has been counted.

3. Anonymity Problem of Chun *et al.*'s Protocol

The structure of Chun *et al.*'s protocol allows S to learn which vote belongs to whom. In other word, the votes are not anonymous for the System point of view. S would simply learn the voters' votes through decrypting $Msg_{V_i}^2$; the message $Msg_{V_i}^2$ contains voter's ID $\left(ID_{V_i}\right)$ and his vote $\left(m_i\right)$. This is not desirable for voters because they prefer to keep their votes secret even from the election community staffs (i.e., form the election administer S).

To alleviate this drawback, we modify Chun et al.'s protocol to support votes' anonymity even from the S. To achieve this goal, we apply blind signature protocol [12] for generating a blind token to anonymously authenticate voters to the System.

Blind signature protocol, proposed by Chaum [12], is used for anonymous applications such as untraceable payment and electronic voting. In this protocol a message is blinded by the sender and sent to a signer. Then, the signer signs the blinded message without any clue about its content, and then the sender could obtain the signed original message by unblinding the signed blind message. Further, if the signer sees her signature on the original message, she cannot link it to the corresponding signed blind message.

In the next section we describe how the blind signature protocol can be feed into the Chun *et al.*'s protocol to support vote anonymity.

4. Modification of Chun *et al.*'s Protocol

We introduce an anonymous token to authenticate each voter to the System without revealing voter's identity. Applying blind signature scheme, the anonymous token ensures that the System cannot link the anonymous token to the user identity, while the token provides some means to ensure user validity [12]. In authentication phase, each voter V_i would obtain his anonymous token by revealing his ID_{V_i} to the S. Then, in the voting phase, V_i uses this token to anonymously authenticate himself to the S, without revealing his identity ID_{V_i}. In the following, the detail of each phase is described.

4.1. Authentication phase

Getting the anonymous token, each voter tries the following steps:

First: System (S) generates a unique tag number $\left(tag\#\right)$ for a vote, computes $X = g^a$ $\left(a \in GP(p)\right)$ and forms message Msg_S^1 through equation (1) and broadcasts it to all voters. Note that S's signature on Msg_S^1 $\left(\sigma_S^1\right)$, and its identifier is included in the message Msg_S^1.

Second: After validation of message Msg_S^1 through verifying S's signature, the voter V_i selects a random number $q \in GP(p)$ and computes $c(q)$, where c is a computing function only known to V_i that acts as a blinding factor and blinds its content. Then, V_i forms message Msg_{V_i} through equation (7).

$$Msg_{V_i} = (\{tag\#, ID_S, N_S, ID_{V_i}, N_{V_i}, Y, c(q)\}, \sigma_{Vi}) \quad (7)$$

The V_i sends Msg_{V_i} to S.

Third: S verifies the validity of V_i and its message Msg_{V_i} through verifying V_i's signature, as before. Then, S signs the blind message $c(q)$, forms the message $Msg_S^2 = \{\sigma_S(c(q))\}$ and sends it to V_i.

Forth: Finally, V_i verifies the validity of S's signature on $c(q)$ by checking $VA(\sigma_S(c(q)), c(q)) \stackrel{?}{=} 1$; if it holds, V_i extracts S's signature on the original message q $(\sigma_S(q))$ by computing $c'(\sigma_S(c(q)))$, where c' (unblinding factor) is the inverse function of c only known to V_i [12].

Now, $\sigma_S(q)$ is the anonymous token for the voter V_i; no one can generate V_i's anonymous token because, only V_i knows c' and can compute $c'(\sigma_S(c(q)))$ [12]. Also, in the voting phase, this anonymous token ensures the System that the holder of $\sigma_S(q)$ is an authenticated voter.

Thus, without any further interaction, the voter obtains his anonymous token and can start the voting phase to cast his vote.

4.2. Voting phase

In this phase, V_i casts his vote while authentication will be done through the anonymous token:

First: The voter V_i selects his vote m_i, and generates $\left(Msg_{V_i}^2 = \{E_{pk_s}(\sigma_S(q), m_i, q)\}\right)$ which is the encryption of V_i's anonymous token $(\sigma_S(q))$, his vote and q, under the System's public key E_{pk_s}. Then, V_i sends the message $Msg_{V_i}^2$ to S.

Second: After receiving $Msg_{V_i}^2$, S decrypts it using its private key and recovers $\sigma_S(q)$, m_i and q. Then S verifies the correctness of the anonymous token by checking $VA(\sigma_S(q), q) \stackrel{?}{=} 1$. If this equation holds, it shows that the holder of the anonymous token is a valid user without revealing his identity, thus his vote m_i is valid and is counted. Further, the anonymous token $\sigma_S(q)$ is appended to the non-fresh-tokens list; otherwise stops.

This list contains all the tokens that have been used successfully and no longer can be used. The System controls the freshness of the tokens; if this check returns true, the token is non-fresh and the System rejects the message.

To control the length of the list, S can periodically change his signature key, so the list can simply turns to be clean and all the pre-issued token would be invalid.

Third: To prove the correctness of the results, S computes $\sigma_S(q+1)$ and sends it back to the voter. Thus, V_i recovers $q+1$ and is convinced that his vote has been counted.

5. Discussion

In this section, we first compare Chun *et al.*'s protocol with its modified version in terms of e-voting general requirements. Then a security analysis and performance comparison of the modified Chun et al.'s protocol and its original version is presented.

5.1. Requirements comparison

The modified Chun *et al.*'s protocol meets all the requirements of e-voting protocol and it also provides anonymous voting requirement, shown in Table 1.

Table 1. Requirement Comparisons

Requirements	Chun *et al.*'s protocol	Modified Chun *et al.*'s protocol
Completeness	✓	✓
Uniqueness	✓	✓
Privacy	✓	✓
Eligibility	✓	✓
Fairness	✓	✓
Verifiability	✓	✓
Mobility	✓	✓
Uncoercibility	✓	✓
deniable authentication	✓	✓
Anonymous Voting	×	✓

The modified version of Chun *et al.*'s protocol meets the following requirements:

Completeness: if the attacker wants to fake a vote in our proposed protocol, he must know c and c' functions of the voter which are kept secret from the attacker. In addition, as the same with Chun *et al.*'s protocol, if S be a trusted node, no one can add an invalid vote to the final results and our protocol provides completeness property.

Uniqueness (Unreusability): Blind signature scheme [12] and the anonymous token avoid double voting problem. The anonymous token becomes invalid after one successful use and only legal voter could generate this token, so no one can use this token to vote more than once.

Privacy: Using public key technique, an attacker cannot obtain any knowledge from the ballots.

Eligibility: Using blind signature scheme and public key scheme, only legal voters can obtain anonymous token in the modified version of Chun *et al.*'s protocol.

Fairness: Decrypting the ballot messages requires the knowledge of S's private key, thus an attacker cannot obtain the partial result of the election.

Verifiability: To support this requirement, the modified protocol sends a response to each voter, if his vote is counted.

Similar to Chun *et al.*'s protocol, the modified protocol meets mobility, uncoercibility and deniable authentication requirements [1], because the protocols do not differ in this way.

5.2. Security Analysis

To analyze the security of the modified Chun et al.'s protocol, we investigate the resistance of the protocol against the following attacks:

Man-In-The-Middle attack: To modify Msg_S^1 and Msg_{V_i} in authentication phase, an attacker should have the knowledge of S's private key or V_i's private key, and because these information is secret the attacker would fail. In addition, if the attacker wants to fake the ballot message in voting phase, he should have the knowledge of function c' to produce $\sigma_S(q)$, but because he does not have this information, the attack would fail.

Impersonation attack: Due to the fact that the attacker does not know a voter's private key, he is unable to impersonate a legal voter. Also, eavesdropping the transmitted messages cannot help the attacker to generate the anonymous token, because only legal voters have the knowledge of functions c and c' .

Replay attack: Using random nonce makes the protocol resistant against replay attack. Furthermore, the un-reusability of the anonymous token makes this attack to be failed.

Eavesdropping: Using cryptography techniques in all messages, the eavesdropper cannot obtain any useful information; the attack would fail.

5.3. Performance Comparison

To compare the performance of the modified Chun *et al.*'s protocol with its original version, we analyze the computation and communication cost of these two protocols.

According to the performance analysis presented in [1], in the original Chun et al.'s protocol, the total time taken by System (or a voter) is $3T_{Exp}+2T_{En}+2T_{De}+2T_{Ha}+1T_{Sym}$ where T_{Sym} is the time taken by a symmetric encryption/decryption operation; notice that the time of a signing (verifying a signature) operation is assumed to be the same as an encryption (decryption) operation. As it is clear, the total time taken by a voter and the total time of the System is equal.

Table 2 shows the total time taken by each voter and the System for each phase of the modified version of Chun *et al.*'s protocol.

Table 2. Computation Cost of the modified version of the Chun *et al.*'s protocol

Phase	Voter V_i	System S
Authentication	$1T_{Blind}+1T_{En}+2T_{De}+1T_{Unblind}$	$1T_{Exp}+2T_{En}+1T_{De}$
Voting	$1T_{En}+1T_{De}$	$1T_{En}+2T_{De}$

The blinding operation or unblinding operation takes one exponentiation in RSA blind signature. According to [1], an encryption (decryption) operation can be roughly estimated as $2T_{Exp}+1T_{Ha}$ ($1T_{Exp}+1T_{Ha}$). Based on the above discussion, the computation comparison of the two protocols is presented in Table 3.

Table 3. Computation comparison of the two protocols

Protocol	Voter V_i	System S
Original Chun *et al.*'s protocol	$9T_{Exp}+6T_{Ha}+1T_{Sym}$	$9T_{Exp}+6T_{Ha}+1T_{Sym}$
Modified version of Chun *et al.*'s protocol	$9T_{Exp}+5T_{Ha}$	$10T_{Exp}+6T_{Ha}$

Table 3 shows that the modified Chun *et al.*'s protocol provides the vote anonymity requirement with a low additional cost at *S*; moreover, the computation cost of voters is decreased.

Further, the modified Chun *et al.*'s protocol includes shorter messages than the original Chun *et al.*'s protocol; the length of messages Msg_S^2 and $Msg_{V_i}^2$ in modified protocol, is shorter than the original protocol. Thus, the communication cost is decreased in the modified version and makes it more suitable for the mobile environments.

6. Conclusion

In this paper, we analyze one recently proposed e-voting protocol and add a useful property to it to support anonymous voting property which is an important property in every election. We use blind signature to provide the mentioned property. Then we discuss the features of our proposed protocol; perform the security analysis, computation and communication cost analysis. As a result, our proposed e-voting protocol is well suited for mobile environments because of its low computation cost; also it supports anonymous voting property.

References

[1] C. T. Li, M. S. Hwang and C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile ad hoc networks", Computer Communications, vol. 31, **(2008)**.
[2] D. Chaum, "Untraceable electronic mail", Communications of the ACM, vol. 24, no. 2, **(1981)** February.
[3] Y. Aumann and M. Rabin, "Efficient deniable authentication of long messages", in International Conference on Teoretical Computer Science in Honor of Professor Manuel Blum's 60th Birthday, **(1998)** Hong Kong,China.
[4] F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi and A. Vaccarelli, "Seas, a secure e-voting protocol: design and implementation", Computers & Security, vol. 24, no. 8, **(2005)** November.
[5] A. Boukerche, K. El-Khatib, L. Xu and L. Korba, "An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks", Computer Communications, vol. 28, no. 10, **(2005)** June.
[6] C. C. Chang and J. S. Lee, "An anonymous voting mechanism based on the key exchange protocol", Computers & Security, vol. 25, no. 4, **(2006)**.
[7] Y. Y. Chen, J. K. Jan and C. L. Chen, "The design of a secure anonymous Internet voting system", Computers & Security, vol. 23, no. 4, **(2004)**.
[8] I. Chlamtac, M. Conti and J. J. N. Liu, "Mobile ad hoc networking: imperatives and challenges", Ad Hoc Networks, vol. 1, no. 1, **(2003)**.
[9] L. Cranor and R. Cytron, "Sensus: a security-conscious electronic polling system for the Internet", in: Proceedings of the International Conference on System Sciences, **(1997)**, Hawaii, pp. 561–570.
[10] X. Deng, C. H. Lee and H. Zhu, "Deniable authentication protocols", IEE Proceedings Computers and Digital Techniques, vol. 148, no. 2, **(2001)**.
[11] W. Diffie and M. E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory IT, vol. 22, no. 6, **(1976)**.
[12] D. Chaum, "Blind Signatures for Untraceable Payments", Proceeding of Crypto, **(1998)**, Santa Barbara, pp. 199-203.
[13] M. A. Talouki, "Mobile Database Security Assessment against Location Detection Attacks Using Blind Signature", Mcs. Thesis, Isfahan University, Iran, **(2007)**.
[14] H. Pietilainen, "Elliptic curve cryptography on smart cards", MSc. Thesis, Helsinki University of Technology, **(2000)**.