AN ID-BASED MULTI-RECEIVER SIGNCRYPTION SCHEME IN MANET

[1, 2]Lei Wu
[1]School of Information Science and Engineering, Shandong Normal University, Jinan 250014, Shandong, China
[2]Shandong Provincial Key Laboratory for Distributed Computer Software, Jinan 250014, Shandong, China

ABSTRACT

In Mobile Ad hoc network (Manet), to solve the problems of the message receiver privacy exposure and signcryption (decryption) unfairness in existing signcryption schemes, a new ID- based multi-receiver signcryption scheme based on bilinear pairings is proposed. We also analyzed its security and efficiency. The result shows that the new scheme is provable secure in the random oracle model. It is significantly efficient and with low computation cost and is very suitable for secure communication in Manet. Then, the scheme can avoid the destruction of the malicious nodes. This scheme can satisfy the requirement of security and efficiency in real network environment, it is more propitious to applications in practice.

Keywords: *Multi-receiver Signcryption, Manet, Bilinear Pairing*

1. INTRODUCTION

Mobile Ad hoc network (Manet)[1] is a wireless technique that the nodes in the network could move randomly, topology changes highly dynamic and there is no beforehand support of network infrastructure. Manet has the characteristics of temporarily network, rapidly deploy, no control center and survivability, so it can provide flexible and convenient communication, broaden the field of mobile communications applications. Therefore, there has a wide range of applications for Manet early, such as tactical military communications network and personal radio. In recent years, the technology is rapidly expanding to the civilian system, such as wireless local area networks, personal area networks, sensor networks, etc., they have broad application prospects. In a major natural disaster occurred due to leaving the fixed telecommunications network facilities were destroyed or not working correctly, or in remote, wild areas of work can not rely on fixed facilities ore the default network access, Manet which has the ability to separate network and self-organizing capacity of communication in these situations is the only or the best option, especially for military applications is of great significance. As Manet has its own characteristics, from a security point of view, the security of Manet is more worthy of attention compared with traditional networks. How to deal with the malicious nodes becomes a hotspot of research, we need to design special secure algorithm to solve this problem.

In 1997, Zheng introduced the concept of public key signcryption[2]. This kind of primitive simultaneously performs encryption and signature in a single logical step in order to obtain confidentiality, integrity, authentication and non-repudiation more efficiently than the sign-then-encrypt approach. Many efficient signcryption schemes[4-7] have been proposed since then. In 2002, Malone-Lee first proposed an ID-based signcryption scheme[8]. Since then, many ID-based signcryption schemes[9-12] have been proposed. In these schemes, when broadcasting a message to $n(n>1)$ users who are jointly working on the same project to communicate with one another in a secure and authenticated manner, a sender has to signcrypt the message for every receiver and transmit different ciphertext to the corresponding receiver using above signcryption schemes. This trivial solution will lead to drastically high computational costs and communication overheads. To avoid this, multi-receiver signcryption was proposed. It can simultaneously provide confidentiality and authenticity for multiple receivers in a single logical step, achieving higher efficiency than signcrypting a message for each receiver. To deal with the malicious nodes in Manet, we need to simultaneously send a message to several receivers and insure the security and authenticity of the message. So a new ID-based multi-receiver signcryption scheme is proposed to increase the security and efficiency of Manet.

2. PRELIMINARIES

2.1 Security Notions

An ID-based multi-receiver signcryption scheme is made of 4 algorithms: (1) Setup; (2) Keygen; (3) Signcrypt; (4) Unsigncrypt. Paper[2] defined secure notions of an ID-based multi-receiver signcryption scheme as following:

***Definition* 1** We say that an identity based signcryption scheme (IDSC) has the indistinguishability against adaptive chosen ciphertext attacks property (IND-IDSC-CCA) if no polynomial bounded adversary has a non-negligible advantage in the following game.

1. The challenger runs the Setup algorithm and sends the system parameters to the adversary.

2. The adversary A performs a polynomially bounded number of requests:

- Signcryption request: A produces two identities ID_i , ID_j and a plaintext M . The challenger computes d_{ID_i} = $Keygen(ID_i)$ and then $Signcrypt(m, d_{ID_i}, ID_j)$ and sends the result to A .

- Unsigncryption request: A produces two identities ID_i and ID_j , a ciphertext σ . The challenger generates the private key d_{ID_i} = $Keygen(ID_i)$ and sends the result of $Unsigncrypt(\sigma, d_{ID_j}, ID_i)$ to A (this result can be the $\perp$ symbol if σ is an invalid ciphertext).

- Key extraction request: A produces an identity ID and receives the extracted private key $d_{ID} = Keygen(ID)$.

A can present its requests adaptively: every request may depend on the answer to the previous ones.

3. A chooses two plaintexts $M_0, M_1 \in M$ and two identities ID_A and ID_B on which he wishes to be challenged. He can't have asked the private key corresponding to ID_A nor ID_B in the first stage.

4. The challenger takes a bit $b \in_R \{0,1\}$ and computes

$C = Signcrypt(M_b, d_{ID_A}, ID_B)$ which is sent to A .

5. A asks again a polynomially bounded number of requests just like in the first stage. This time, he cannot make a key extraction request on ID_A nor ID_B and he cannot ask the plaintext corresponding to C .

6. Finally, A produces a bit b' and wins the game if $b' = b$.

The adversary's advantage is defined to be $Adv(A) := \left|2P[b' = b] - 1\right|$

***Definition* 2** An identity based signcryption scheme (IDSC) is said to be secure against an existential forgery for adaptive chosen messages attacks (EF-IDSC-ACMA) if no polynomially bounded adversary has a non-negligible advantage in the following game.

1. The challenger runs the Setup algorithm with a security parameter k and gives the system parameters to the adversary.

2. The adversary A performs a polynomially bounded number of requests just like in the previous definition.

3. Finally, A produces a new triple (σ^*, ID_A, ID_B) (i.e. a triple that was not produced by the signcryption oracle), where the private key of ID_A was not asked to the key extraction oracle and wins the game if the result of $Unsigncrypt(\sigma^*, d_{ID_B}, ID_A)$ is not the $\perp$ symbol.

The adversary's advantage is simply its probability of victory.

2.2 Bilinear Pairings

Let G_1 be a cyclic additive group generated by P , whose order is a prime q , and G_2 be a cyclic multiplicative group of the same order q , $a, b, c \in Z_q^*$. A bilinear pairing is a map $e : G_1 \times G_1 \to G_2$ with the following properties:

Bilinear: $\forall P, Q, R \in G_1$,

$$e(P, Q + R) = e(P, Q)e(P, R)$$
$$e(P + Q, R) = e(P, R)e(Q, R)$$
$$e(aP, bP) = e(P, Q)^{ab} ;$$

Non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$;

Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

3. ID-BASED MULTI-RECEIVER SIGN CRYPTION SCHEME

In this section, we propose an ID-based multi-receiver signcryption scheme which consists of the following 4 algorithms.

Setup

Given security parameters k and l , the PKG chooses two group G_1 and G_2 of the same prime order $q > 2^k$, P is the generator of goup G_1 ,

$e: G_1 \times G_1 \to G_2$ is a pairing map. The PKG selects cryptogaphic hash functions $H_1: \{0,1\}^* \times G_1 \to G_1$; $H_2: G_2 \to \{0,1\}^l$; $H_3: \{0,1\}^* \times G_1 \to Z_q^l$, and picks a romdom s as the master key and computes the public key $P_{pub} = sP$. PKG keeps s secret and publishes the system parameters parms: $\{k, l, G_1, G_2, P, P_{pub}, H_1, H_2, H_3\}$

Keygen

For convenience , we will denote a sender and $n(n>1)$ receivers by S and R_i ($i = 1,2,...,n$) with the ID of ID_s and ID_i ($i = 1,2,...,n$). S chooses $r_S \in Z_q^*$, computes $P_S = r_S P$, then sends (ID_S, P_S) to PKG. PKG computes $Q_S = H(ID_S, P_S)$, $t_S = sQ_S$, and send (Q_S, t_S) to S.

S can verify the validity of t_S by $e(t_S, P) = e(Q_S, P_{pub})$, if the equation holds, S accepts t_S as computes $V_S = rQ_S + t_S$ and keeps it as his private key, P_s as his public key. The receiver R_i gets the public/private key (P_i, V_i) through the same way.

Signcrypt

The sender S sends message m to n receivers with the ID $(ID_1, ID_2, ..., ID_n)$ by following steps:

① S chooses $c \in Z_q^*$, computes $U = cP$;

② S computes $X_i = e(P_i + P_{pub}, Q_i)^c$, $i = 1,2,...,n$;

③S computes $d_i = H_2(X_i) \oplus m$, $i = 1,2,...,n$;

④ S computes $W = c^{-1} H_3(m,U) V_S$

⑤ S outputs the ciphertext $\sigma = (U, W, d_1, ..., d_n)$

Unsigncrypt

If R_i receives σ,

① R_i computes $X_i' = e(U, V_i)$;

② R_i recovers $m = d_i \oplus H_2(X_i')$;

R_i verifies $e(U,W) = e\left(P_S + P_{pub}, Q_S\right)^{H_3(m,U)}$ holds or not, if the above equation holds, accept the signcryption. At the same time, the public key of the sender S is also authenticated.

4. ANALYSIS OF THE SCHEME

4.1 Correctness

If the message sender is honest, the scheme can recover the correct secret.

Proof.

$$X_i' = e(U, V_i) = e(U, r_i Q_i + t_i) = e\left((r_i + s)P, Q_i\right)^c$$
$$= e\left(P_i + P_{pub}, Q_i\right)^c = X_i$$

$$e(U,W) = e\left(cP, c^{-1} H_3(m,U) V_S\right)$$
$$= e\left(P, H_3(m,U)(r_S + s) Q_S\right)$$
$$= e\left((r_S + s)P, Q_S\right)^{H_3(m,U)}$$
$$= e\left(P_S + P_{pub}, Q_S\right)^{H_3(m,U)}$$

4.2 Confidentiality and Forward Security

Theorem 1. In the random oracle model, if there is an IND-IDSC-CCA adversary A against our scheme with an advantage ε when running in a time t and asking at most q_{H_i} ($i = 1,2,3$) H_i queries, q_E keygen queries, q_S signcrypt queries and q_U unsigncrypt queries, there exists an algorithm B that can solve the MCBDH problem with an advantage $\varepsilon' > \frac{n\varepsilon}{q_{H_1}} \left(1 - q_S \frac{q_S + q_{H_3}}{2^k}\right) \left(1 - \frac{2q_U}{2^k}\right)$, within a time $t' \le t + \left(q_{H_1} + q_E + 3q_S\right) t_{sm} + \left(q_S + 2q_U\right) t_{pr}$.

Proof. At the challenge phase, A outputs messages (m_0, m_1) and identities $(ID_s, ID_1, ..., ID_n)$ and he has never obtained the private keys of identities $ID_1, ..., ID_n$. If $(ID_1, ..., ID_n) \ne (ID_1^*, ..., ID_n^*)$, B stops. Otherwise, B chooses a random bit $b \in \{0,1\}$ and signcrypts m_b . To do so, B sets $U^* = cP$, and chooses $V^* \in G_1$, $C^* \in \{0,1\}^*$ randomly and $N_1^*, ..., N_n^* \in \{0,1\}^l$, then returns the challenge ciphertext $\sigma^* \le C^*, U^*, V^*, N_1^*, ..., N_n^*$ to A . A can not recognize that σ^* is not a proper ciphertext unless it asks for a hash value

$$H_2\left(ID_i, U^*, e\left(P_{pub}, H_1\left(ID_i^*\right)\right)^c\right)$$

for some $i \in \{1,2,...,n\}$.

Along the guess stage, A's view is simulated as before and its eventual output is ignored. At last, B looks into the list H_2^{list} for a tuple of the form $H_2\left(ID_i, U^*, e\left(P_{pub}, H_1\left(ID_i^*\right)\right)^c\right)$ for some $t \in \{1,2,...,n\}$. B outputs “failure” if there isn’t such a tuple exists. Otherwise, B has to make a solution to the MBCDHP.

Let E_1 be the event that A does not choose to be challenged on $\left(ID_1^*,...,ID_n^*\right)$, E_2 the event that key extract queries are made on $\left(ID_1^*,...,ID_n^*\right)$, E_3 the event that B aborts in a signcrypt query because of a collision on H_3, and E_4 the event that B rejects a valid ciphertext in an unsigncrypt query. Obviously, there is $\Pr[\neg E_1] = n / q_{H_1}$, where the event $\neg E_1$ means $\neg E_2$.

There are

$\Pr[\neg E_3] \le q_S\left(q_S + q_{H_3}\right)/2^k$; $\Pr[\neg E_4] \le 2q_U / 2^k$.

$$\Pr[\neg E_1 \neg E_3 \neg E_4] \ge \frac{n}{q_{H_1}}\left(1 - q_S\frac{q_S + q_{H_3}}{2^k}\right)\left(1 - \frac{2q_U}{2^k}\right).$$

B's advantage is

$$\varepsilon' > \frac{n\varepsilon}{q_{H_1}}\left(1 - q_S\frac{q_S + q_{H_3}}{2^k}\right)\left(1 - \frac{2q_U}{2^k}\right).$$

The bound on B's computation time is

$$t' \le t + \left(q_{H_1} + q_E + 3q_S\right)t_{sm} + \left(q_S + 2q_U\right)t_{pr}.$$

4.3 Unforgeability

Our scheme is unforgeable. Any adversary without the sender's private key can not forge a signcrypted message on behalf of the sender.

4.4 Public Verifiability

To prove to a trusted 3rd party T that a sender with an identity ID_S actually signcrypted a message m, receiver R_i only need to send (U,W,m) to T.

T verifies $e(U,W) = e\left(P_S + P_{pub}, Q_S\right)^{H_3(m,U)}$ holds or not, if the above equation holds, the signcryption is valid.

4.5 Efficiency

We compare our scheme with Li's scheme[12] and Chow's scheme[10] when signcrypting a message for n receivers in Table 1. Here, M denotes the cost of computing a multiplication in G_1, E denotes the cost of computing an exponentiation in G_2, P denotes the cost of computing a bilinear pairing. From table 1, our scheme is more efficient.

Table 1: Efficiency Comparison Of 3 Schemes

Scheme	Computational cost	Ciphertext size
Li[12]	$3nM + 3nE + 2nP$	$2n\lvert G_1\rvert + n\lvert m\rvert$
Chow[10]	$3nM + 6nP$	$n\lvert G_1\rvert + n\lvert M\rvert + n\lvert q\rvert$
Ours	$M + cnE + nP$	$2n\lvert G_1\rvert + n\lvert m\rvert$

4.5 Dealing With Malicious Nodes In Manet

In Manet, every node has the probability of being destroyed or captured. To resist the inner attack of captive nodes, we do the following job: Assume that every node has some surveillance mechanism. If one node A detect that its neighbour node B has malicious behavior, then send warning message $Warning < ID_B >$ and broadcasts the warning message to the whole Manet. The receivers are ID_1 ,…, ID_n , computes $\sigma = Signcrypt\left(m, V_A, ID_1,...,ID_n\right)$. When each receiver R_i receives the ciphertext, computes $Unsigncrypt\left(\sigma, ID_A, V_i\right)$ and gets the warning message. Then R_i checks if the node B has malicious behavior or not. If "no", rejects the warning message, if "yes", adds the node B to the complaint index. If one node's complaints increases to the threshold value, the node is marked "malicious". In this way , our scheme can be used to deal with malicious nodes in Manet.

5. CONCLUSION

A new ID- based multi-receiver signcryption scheme based on bilinear pairings is proposed. We also analyzed its security and efficiency. The result shows that the new scheme is provable secure in the random oracle model. It is significantly efficient and with low computation cost. The scheme can avoid the destruction of the malicious nodes. It is very suitable for secure communication in Manet.

ACKNOWLEDGEMENTS

This work is supported by Shandong Provincial Natural Science Foundation (No. ZR2011FQ032) and Project of Shandong Province Higher Educational Science and Technology Program (No. J11LG33).

REFERENCES:

[1] Zhou Li-dong, Hass Z J, "Securing Ad hoc networks", *IEEE Network Magazine*, Vol. 13, No.6, 1999, pp. 24-30.

[2] Libert B, Quisquater J, "A new identity based signcryption schemes from pairings", 2003 *IEEE information theory workshop Paris*, IEEE press, 2003, pp. 155-158.

[3] Zheng Yuliang, "Digital Signcryption or How to Achieve Cost(Signature&Encryption)<< Cost (Signature)+Cost(Encryption)", *LNCS: Advances in Cryptology-CRYPTO'97*, Berlin: Springer-Verlag Press, 1997, pp. 165-179.

[4] Yum B H,Lee P J, "New Signcryption Schemes Based on KCDSA", *LNCS: Proc of ICISC'01*, Berlin: Springer Verlag Press, 2001, pp. 305-317.

[5] Libert B,Quisquater J J, "Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups", *PKC 2004*. Berlin: Springer-Verlag Press, 2004, pp. 187-200.

[6] Libert B,Quisquater J J,"Improved Signcryption from Diffie-Hellman Problems", *LNCS: Security Communication Networks-SCN04*. Berlin:Springer-Verlag Press, 2005, pp.220-234.

[7] MA Chang-she, "Efficient Short Signcryption Scheme with Public Verifiability", *LNCS: Inscrypt 2006*. Berlin:Springer-Verlag Press, 2006, pp.118-129.

[8] Malone-Lee J, "Identity based signcryption", Cryptology ePrintArchive, 2002 http://eprint. iacr.org/2002/098.pdf.

[9] Boyen X, "Multipurpose Identity-Based Sign--cryption: a Swiss Army Knife for Identity-based Cryptography", *LNCS: Advances in Cryptology-Crypto2003*, Berlin: Springer-Verlag Press, 2003, pp.383-399.

[10]Chow S S M, Yiu S M, Lucas C K, et al, "Efficient Forward and Provably Secure ID-based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity", *LNCS: information Security ande Cryptology-ICISC'03*, Berlin:Springer-Verlag Press, , 2004, pp.352-269.

[11]Chen L,Malone-Lee J,"Improved Identity-based Signcryption", *LNCS:PKC'05*, Berlin: Springer-Verlag Press, 2005, pp.362-379.

[12]LI Fa-gen, HU yu-pu, LI Gang, "An efficient identity-based signcryption scheme", Chinese Journal of Computers, Vol. 29, No. 6, 2006, pp:1641-1647.