A Identification and Key Establishment Scheme based on Self-Certified Public Key for MANETs

Dongwei Zhang¹², Yi Sun¹²*, Yuanyan Luo¹
¹Information Science and Technology Institute, Zhengzhou, China
²Henan Provincial Key Laboratory of Information Security, Zhengzhou, China

*Corresponding author e-mail: sunyi-1001@163.com

Abstract: Due to the mobility of nodes, lack of infrastructure and limited computing and storage resources in mobile ad hoc networks (MANETs), this scheme uses the self-certification public key, combined with the interactive zero-knowledge proof and KEA+ key exchange method in the GPS identity authentication protocol, uses four interactions to complete the two-way identity authentication and key exchange of both parties, and which security is analyzed subsequently. The scheme effectively reduces the leakage of the claimant’s secret knowledge in the identity authentication process, and enhances the reliability of the identity authentication and key exchange process.

1. Introduction

In recent years, MANETs (Mobile Ad Hoc Networks) is omnipresent emerges in the social construction and military applications. MANETs have the characteristics such as no fixed infrastructure, node mobility, dynamic topology and limited resources. In addition to routing security, authentication and key establishment schemes between nodes are also important. Research areas[1-3]. The original idea of self-certifying public keys comes from Girault's self-certifying public key scheme[4], which eliminates the generation and storage of certificates compared to certificate-based authentication, which avoids the user private key generated by the registry compared to identity-based authentication. The interactive proof system (IP) and zero-knowledge proof were originally proposed by Galdwasser, Micali and Rackoff, and an interactive Turing machine (ITM) computational model was given[5]. When the self-certifying public key is combined with the interactive zero-knowledge proof for identity authentication, it can have the advantages of no public key certificate publishing and storage, no need to absolutely trust the certificate center, large amount of calculations are completed offline and small information leakage during interactive authentication. The security of the key establishment process can be improved when combining the establishment of the session key with the two-way identity authentication.

G. Poupard and O. Baudron et al. constructed an identification scheme GPS[6-7] for low-cost computing environments such as smart cards. The online identity authentication in this scheme is based on the interactive zero-knowledge identification in Girault's self-certified public key scheme. The scheme was officially accepted as the only identification pre-selection scheme by NESSIE(New European Schemes for Signatures, Integrity and Encryption). However, the GPS solution adopts one-way authentication, and the identity authentication does not perform negotiation and exchange of session keys. KEA+[8] proposed by K.Lauter and A.Mityagin has improved the security of KEA...
proposed by the National Security Agency (NSA). During the key exchange process, both parties have added temporary secret random numbers, and combine long-term secrets with temporary secrets to ensure each session key is different, and the identity information of both parties is also added to the negotiation of the session key. However, the KEA+ scheme uses a symmetric crypto mechanism for identity authentication.

The group key negotiation scheme [9-11] is also an important category in key management in MANETs. This scheme combines Girault's self-certified public key idea, GPS interactive zero-knowledge proof and KEA+ enhanced key exchange scheme. It is designed from the user registration phase and two-way authentication and key exchange phase to complete the session key negotiation while implementing the two-way identity authentication.

2. Our scheme

Due to space limitations, the GPS identity authentication scheme and the KEA+ key exchange scheme are no longer stated. Our scheme consists of two phases. One is the user registration phase, and the registration authority RA adopts the Schnorr signature scheme proposed by H. Petersen and P. Horster[12] to generate its public-private key pair in cooperation with the user, and the RA cannot know the user's private key, and also avoids the absolute trust of the RA. The second is the authentication phase. The registered users complete the two-way identity authentication and session key exchange through four passes based on the interactive knowledge proof and the KEA+ key exchange method.

2.1 User registration phase

The first step, RA Registration Authority generates the public parameters.

I. Selects large prime numbers \( p, q \), to satisfy: \( q \mid (p - 1), q \geq 2^{160}, p \geq 2^{1024} \).

II. Selects \( \alpha \in Z_p^* \) and \( \text{ord}_p(\alpha) = q \), which is \( \alpha^q \equiv 1 \mod p \), \( \alpha \neq 1 \).

III. According to the application environment, a security parameter \( t \) is selected. Generally, \( t \geq 80 \), the probability that the fake authenticator can succeed is less than \( 2^{-t} \).

IV. Selects a safe one-way hash function \( h : \{0,1\}^* \to Z_q \).

V. Randomly chooses \( x_z \in Z_p^* \), calculates \( y_z = \alpha^{x_z} \mod p \), \( x_z \) is the RA’s private key, \( y_z \) is the RA’s public key.

VI. Publish public parameters \( (p, q, \alpha, y_z) \) and Hash \( h() \). Keep private key \( x_z \) confidential.

In the second step, the user registers to generate a public-private key pair. The information that user Alice interacts with the registry RA is:

\[
RA \to Alice : \quad \tilde{r}_A
\]

(1)

\[
Alice \to RA : \quad r_A, ID_A
\]

(2)

\[
RA \to Alice : \quad \tilde{s}_A
\]

(3)

\[
Alice \to RA : \quad y_A
\]

(4)

I. RA randomly chooses \( k_A \in Z_q^* \), calculates \( \tilde{r}_A = \alpha^{k_A} \mod p \). The message (1) is then sent to Alice.

II. Alice randomly chooses \( a \in Z_q^* \), calculates \( r_A = \tilde{r}_A \cdot \alpha^a \mod p \). The message (2) is then sent to RA.

III. RA calculates \( \tilde{s}_A = x_z \cdot h(r_A, ID_A) + k_A \mod q \), message (3) is then sent to Alice.

IV. Alice calculates the private key \( x_A = \tilde{s}_A + a \mod q \), \( y_A = \alpha^{x_A} \mod p \). The message (4) is then sent to RA.
Finally, RA validates \( y_A = y_z^{h(r_A, ID_A)} \cdot r_A \mod p \) is established. If it is established, it will accept Alice's registration, otherwise it will terminate the registration.

This stage, Alice’s private key \( x_A \) and public information \((y_A, r_A, ID_A)\) are generated.

2.2 User performs two-way authentication and key exchange phase

Alice and Bob have completed the legal identity registration, the corresponding parameters are: Alice\((x_A, y_A, r_A, ID_A)\) and Bob\((x_B, y_B, r_B, ID_B)\), and have securely obtained the RA’s public key \( y_z \). Two-way authentication online interaction information:

- Alice to Bob: ID_A, r_A, t_A, h(y_A)
- Bob to Alice: ID_B, r_B, t_B, h(y_B), c_B
- Alice to Bob: w_A, z_A, c_A
- Bob to Alice: w_B, z_B

Step 1: Alice randomly chooses \( u_A \in \mathbb{Z}_q \) as a secret promise, calculates \( t_A = \alpha^{u_A} \mod p \) as a public evidence, using a hash function to protect the public key integrity. The message (1) is then sent to Bob.

Step 2: After receiving the message (1), Bob first uses the RA’s public key \( y_z \) to calculate \( y'_A = y_z^{h(r_A, ID_A)} \cdot r_A \mod p \), and verifies \( h(y'_A) = h(y_A) \) is true. If it is not established, this phase will be aborted, otherwise it will be sure that \((y_A, r_A, ID_A)\) is legal. Then randomly choose \( c_B \) \((0 < c_B < 2^t)\) as the challenge data. And choose \( u_b \in \mathbb{Z}_q \) as a secret promise, the calculation \( t_B = \alpha^{c_B} \mod p \) is used as public evidence for the integrity protection of the public key. The message (2) is then sent to Alice.

Step 3: When receiving the message (2), Alice first verifies the legitimacy of \((y_B, r_B, ID_B)\) by calculating \( y'_B = y_z^{h(r_B, ID_B)} \cdot r_B \mod p \) and determining if \( h(y'_B) = h(y_B) \) is true. If it is illegal, this phase will be aborted. If it is legal, \( w_A = u_A + x_A c_B \) will be calculated as a response message. Then randomly chooses a challenge data \( c_A \) \((0 < c_A < 2^t)\) for Bob and a random number \( n_A \in \mathbb{Z}_q \), calculates \( z_A = \alpha^{n_A} \mod p \). The message (3) is then sent to Bob.

Step 4: After receiving the message (3), Bob first verifies \( t_A = \alpha^{w_A} \cdot y_A^{-c_A} \mod p \) is true. If it is not established, this phase will be aborted. Otherwise, it knows that Alice already has the secret of the private key \( x_A \) corresponding to its public key \( y_A \) and accepts Alice’s identity. Then calculate \( w_B = u_B + x_B c_A \) as a response to Alice, generate a random number \( n_B \in \mathbb{Z}_q \), and calculate \( z_B = \alpha^{n_B} \mod p \). The message (4) is then sent to Alice. The session key \( k_{AB} = h(y_A^{n_A}, z_A^{n_B}, ID_A, ID_B) \) is then calculated.

Step 5: After receiving the message (4), Alice first verifies \( t_B = \alpha^{w_B} \cdot y_B^{-c_B} \mod p \) is true. If it is not established, this phase will be aborted. Otherwise, it knows that Bob already has the private key \( x_B \) corresponding to its public key \( y_B \) and accepts Bob's identity. Then calculates \( k_{AB} = h(x_A^{n_A}, y_B^{n_B}, ID_A, ID_B) \) as a session key and complete the key exchange with authentication.

The key of this phase is steps 4 and 5, which generate and exchange session keys while completing identity authentication through interactive zero-knowledge proof.
3. Security analysis

Conclusion 3.1: It is not feasible in calculation for an attacker to guess the user's private key only when he knows the public key and public parameters.

Proof: During the user registration phase, the security of the user's private key is based on the discrete logarithm problem in the $\mathbb{Z}_p^*$. Obviously, under the condition that the discrete logarithm problem is difficult, it is not feasible in calculation for the registration authority RA and other users to calculate the corresponding private key by only using user's public key.

Conclusion 3.2: The user's public key satisfies verifiability.

Proof: In the user registration phase, the user's private key is generated by the random number generated by the user, the random number generated by the RA, the user identity ID, and the private key of the RA. If the RA falsifies the user's public key, it is obviously easy to be discovered by the registered user. Similarly, the user cannot separately generate the public-private key pair. Otherwise, the RA can be easily detected. Since the RA participates in the generation of the user's private and public keys, all registered users can easily restore and verify each other's public keys.

For example, the RA's signature on the user's Alice public key $(r_A, ID_A)$, all registered users can restore and verify the validity of Alice's public key through the RA's public key $y$ by verifying $y = y_z^{l(r_l, ID_l)} \cdot r_l \mod p$ is true. That is, the consistency of the triples $(y_z, r_l, ID_l)$.

Conclusion 3.3: Two-way authentication and key exchange satisfy the completeness of interactive knowledge proof.

Proof: In the two-way authentication and key exchange phase, for the honest protocol subject, both parties can identify the authenticity of each other's identity in accordance with the agreement.

\[
\begin{align*}
\alpha^{x} \cdot y^{c_A} &\equiv \alpha^{(u_A + x_B c_B)} \cdot \alpha^{-x_B c_B} \equiv \alpha^{u_A} \equiv t_A \mod p \\
\alpha^{w} \cdot y^{c_B} &\equiv \alpha^{(u_B + x_A c_A)} \cdot \alpha^{-x_A c_A} \equiv \alpha^{u_B} \equiv t_B \mod p
\end{align*}
\]

Conclusion 3.4: Two-way authentication and key exchange satisfy the rationality of interactive knowledge proof.

Proof: In the two-way authentication and key exchange phase, the protocol uses interactive knowledge proof. Challenge data $c_A$ and $c_B$ meet $1 < c_A, c_B < 2^t$. $t$ is a system security parameter whose value depends on the application environment. In this scheme that if the impersonator guesses the challenge data, the probability of the verifier's success is $(2^{-t})^2$ [13], that is, the probability of successful execution of the protocol is $2^{-80}$.

Conclusion 3.5: The session key $k_{AB}$ satisfies forward security

Proof: $k_{AB} = h(z^{c_A}, y^{c_B}, ID_A, ID_B) = h(\alpha^{x_A}, \alpha^{x_B}, ID_A, ID_B) = h(y^{c_A}, z^{c_B}, ID_A, ID_B)$

$k_{AB}$ is calculated by a secure hash function which is composed of two temporary random numbers $n_A$ and $n_B$ which generated by the authentication process, two long-term user private keys $x_A$ and $x_B$, and the user's identity information $ID_A$ and $ID_B$. The session key $k_{AB}$ is composed of the user's long-term secret and the temporary secret at the time of authentication, which ensures the randomness of each session key. If the adversary obtains the session key for a communication, it will not affect the security of the previous session.

4. conclusion

This paper proposes an effective identity authentication and key exchange scheme for MANETs. The scheme avoids the user's absolute trust in the certificate center, reduces the calculation amount and storage capacity of the certificate, and also effectively reduces the knowledge leakage in the identity authentication process, and improves the security and effectiveness of the identity authentication and key exchange process. How to choose key parameters, reduce the time complexity of solution implementation, and further improve the security of two-way identity authentication is the focus of further research.
Acknowledgments

This work was financially supported by National Natural Science Foundation of China (61702550) fund.

References

[1] A.O. Durahim, E. Savas, A 2-make: an efficient anonymous and accountable mutual authentication and key agreement protocol for wmmns, Ad Hoc Network. 9 (7) (2011) 1202–1220.

[2] R. Amin, S.H. Islam, Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks, Comput. Network. 101 (2016) 42–62.

[3] A.M. Hegland, E. Winjum, S.F. Mjolsnes, A survey of key management in ad hoc networks, IEEE Commun. Surv. Tut. 8 (3) (2006) 48–66.

[4] M. Girault, Self-Certified Public Keys, In Eurocrypt ’91, LNCS547. Springer-Verlag, 1992, 490-497.

[5] S. Goldwasser, S. Micali, and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems, In Proceedings of the 17th STOC, ACM Press, 1985, 291-304.

[6] G. Poupard and J. Stern, Security analysis of a practical ‘on the fly’ authentication and signature generation, Advances in cryptology – Eurocrypt’98, Lecture Notes in Computer Science 1403, Springer-Verlag, 422-436.

[7] O. Baudron, F. Boudot, P. et al. DCSST Crypto Lab. GPS- an asymmetric identification scheme for on the fly authentication of low cost smart cards. A proposal to NESSIE, https://www.cosic.esat.kuleuven.ac.be/nessie/ 2003.

[8] Kristin Lauter, Anton Mityagin. Security Analysis of KEA Authenticated Key Exchange Protocol. PKC 2006 (LNCS 3958). April, 2006,378-394.

[9] Chan Yeob Yeun, Kyusuk Han, Secure authenticated group key agreement protocol in the MANET environment, information security technical report 13 (2008) 158–164.

[10] Dijiang Huang, Deep Medhi, A secure group key management scheme for hierarchical mobile ad hoc networks, Ad Hoc Networks 6 (2008) 560–577.

[11] Orhan Ermi, Serif Bahtiyar, A secure and efficient group key agreement approach for mobile ad hoc networks, Ad Hoc Networks 67 (2017) 24–39.

[12] H. Petersen, P. Horster. Self-certified keys-concepts and applications. In Proc. Conference on Communications and Multimedia Security’97, Chapman & Hall, 1997:102-116.

[13] A. Menezes, Pvan Oorschot, and S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.415-416.