International Journal of Future Generation Communication and Networking
Vol. 8, No. 6 (2015), pp. 135-140
http://dx.doi.org/10.14257/ijfgcn.2015.8.6.13

A Pairing-Free Identity-Based Authenticated Key Agreement Protocol for MANET

Shaheena Khatoon

School of Studied In Mathematics, Pt. Ravishankar Shukla University, India
shaheenataj.28@gmail.com

Abstract

Providing a suitable authenticated key establishment protocol in MANETs is challenging due to all the characteristics of networks, such as communication capability, computation capability and storage resources. This paper presents an efficient and flexible authenticated key agreement protocol without bilinear pairings for MANET. Our proposed protocol not only provides mutual authentication between users and servers but also supports session key agreement. In addition, in our protocol the user does not need to perform the expansive bilinear operations, so it reduces the computation loads.

Keywords: *Elliptic curve cryptography, identity-based cryptosystem; session key agreement; pairing-free technique*

1. Introduction

The idea of identity based cryptography (IBC) was first given by Shamir in the year 1984 [1], IBC is not only simple to use but also more efficient as compare to traditional public key cryptography (PKC). But a fully functional identity-based scheme was proposed recently in 2001 by Boneh and Franklin [3], they designed practical ID-based encryption scheme using bilinear pairing on elliptic curves with security proof in a random oracle. Since then, a large number of identity-based authenticated key agreement (ID-AK) protocols based on the pairing idea have been proposed [4-7].In the year 2002 Smart [8] proposed the first ID-AK protocol using Weil pairings in the same year Chen and kudla [6] proposed some more ID-AK protocol by modifying Smart's protocol. Since then many other authors proposed many identity-based protocols with or without key escrow property. But most of them used pairing which is time consuming as well as costly. Recently, Zhu [11] and Cao. [12, 13] proposed paring free identity-based authenticated key agreement protocols which are computationally efficient and secure.

Therefore, this paper presents a pairing free efficient identity-based authenticated key agreement (ID-AK) protocol without key escrow mode and having all the security attributes as defined by Blake-Wilson. [2] with minimum computational cost.

2. Preliminaries

In this section, we first introduce the basics concept of elliptic curve cryptography (ECC) and Identity-based cryptosystem (IBC), and some of the computationally hard problems on `the elliptic curve group.

2.1. Elliptic Curve Cryptography

Let E_P (a, b) be a set of elliptic curve points over the prime field F_P, defined by the non-singular elliptic curve equation:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \text{ with } a, b \in F_P \text{ and } (4a^3 + 27b_2) \bmod P \neq 0.$$

The additive elliptic curve group defined as $G_P = f(x, y) = \{(x, y): x, y \in F_P\}$ and $(x, y) \in E_p(a, b) \cup \{0\}$, where the point 0 is known as point at infinity. The scalar multiplication on the cyclic group G_P defined as k.P = P +P +…………….. + P(k times). The elliptic curve cryptosystem was initially proposed by Koblitz (1987) [15] and Miller (1985) [14] to design public key cryptosystem and presently it is widely used in several cryptographic schemes to provide desired level of security and computational efficiency. Details of elliptic curve group properties are given in [16].

2.2. Identity Based Cryptography

The identity based cryptosystem (IBC) is a public-key cryptosystem proposed by Shamir [1] in 1984. The basic concept of IBC is that the user can choose arbitrary string, for example, the email address, any online identifiers, etc., as their public key and the corresponding private key is generated by binding the identity of the user with a master-key of a trusted authority, called private key generator (PKG). In 2001, Boneh and Franklin [3] gave the full functional solution for IBC, called IBE using bilinear pairing over the elliptic curve.

2.3. Computational Problems

Elliptic curve discrete logarithm problem (ECDLP). Given $(P, Q) \in Gp$, find an integer $k \in [1, n - 1]$ such that $Q = kP$.

Computational Diffie-Hellman problem (CDHP). Given $(P, aP, bP) \in Gp$ for any as, $b \in [1, n -1]$, computation of abP is hard to the group Gp.

3. Proposed Scheme

The protocol consists of three phases, the set-up, key generation and key agreement phases.

3.1. Set Up

The PKG takes the secret parameter k and a master key s and performs the following:

1. Choose a k-bit prime p and determine the tuple $\{F_q, E/F_q, Gp, P\}$.

2. Choose the master secret key $s \in Z^*_q$ and compute the system public key $P_{pub} = sP$.

3. Choose two cryptographic secure hash functions $H_1:\{0,1\}^* \longrightarrow Z_q^*$ and $H_2:\{0,1\}^* \longrightarrow \{0,1\}^k$.

4. Then PKG publishes public system parameters $\{ F_q, E/F_q, Gp, P, H_1, H_2\}$ and keeps the master secret s secret.

3.2. Key Generation

The PKG takes as input the system parameters, master key and users identifier, carries out the computations and then returns the users ID-based long-term private key. For a user, A, with a particular online identifier, e.g. ID_A, the PKG by using the key generation algorithm, works as follows:

1. Map a user's online identifier ID_A to an integer elements, e.g. $H_1:\{ID_A\} \longrightarrow a \in Z_q$.

2. Compute A's public key as $A_{pub} = (a + s) P$ and A's private key as $A_{pri} = (a + s)^{-1}P$.

3. In a similar manner, the algorithm generates B's pair of public and private keys as $B_{pub} = (b + s) P$ and $B_{pri} = (b + s)^{-1}P$, respectively.

3.3. Key Agreement

Entity A and entity B run the following algorithm to establish a securely shared session key.

STEP 1: A initiates a session with B as follows:

1. Entity A chooses a random ephemeral key, $x \in Z^*_q$, and calculates $T_A = xP$ and signature $S_A = xA_{pri} + H(ID_A||T_A) A_{pri}$.
2. Then A sends, ID_A, T_A and S_A to B.

STEP 2: Upon receipt of A's message, B does the following.

1. Check the validity of the received message, ID_A, T_A, S_A from A and then verify the authenticity by using the signature part, S_A as follows: B confirms if $S_A A_{pub} = T_A P + H(ID_A||T_A)P^2$ using A's public key. This verification authenticates both the message and its source. The hash computation, $H(ID_A||T_A)$, also ensures the integrity of the ephemeral key, $x \in Z^*_q$, in T_A, used for key agreement as follows:
2. If the verification holds, B, chooses a random ephemeral key, $y \in Z^*q$, and calculates $T_B = yP$ and the signature part, $S_B = xB_{pri}+H(ID_B||T_B)B_{pri}$.
3. B first calculates $K_{BA} = yT_A$ and then computes the session key as $SK = H_2 (ID_A||ID_B||T_A||T_B||K_{AB})$.
4. B then sends, ID_B,T_B,S_B and MAC_{SK} to A , where $MAC_{SK} = H_1(T_A||T_B||SK)$

STEP 3: Upon receipt of B's message A does the following:

1. Check the authenticity of the message by confirming if $S_B B_{pub} = T_B P+H(ID_B||T_B)P^2$, otherwise B quits the session.
2. Upon correct verification results, A computes $K_{AB} = xT_B$, and then computes the session key as, $SK = H_2(ID_A||ID_B||T_A||T_B||K_{BA})$ and the authentication token $MAC^*_{SK} = H_1(T_A||T_B||SK)$. Then, A checks the condition $MAC^*_{SK} = MAC_{SK}$. If it holds, A accept the session key SK, otherwise sends an authentication failed message to B.

4. Security Analysis

The proposed protocol satisfies all the security properties as defined by Blake-Wilson. [2] and we are now going to discuss them.

4.1. Known Session Specific Temporary Attack

User A and B computes the session key as $SK = H_2 (ID_A||ID_B||T_A||T_B||K_{AB})$, security of which is depends on the secrecy of $K_{AB} = xyP$. However, if the session ephemeral secrets x and y are exposed to an adversary, but he cannot computes the session key SK. He can generate the session key if he knows xyP. However, knowing the pair $(T_A, T_B) = (xP, yP)$ from which computation of xyP is impossible due to difficulties of solving the CDHP problem. Therefore, the known-session specific temporary information attack is not possible.

4.2. Key Off Set Attack

In our protocol, user A sends the message (ID_A, T_A, S_A) to B. Suppose that the adversary E modifies it to (ID_A,T^*_A, S_A) where $T^*_A = aT_A$.Now B computes the session key $SK =H_2(ID_A||ID_B||T_A||T_B||K^*_{AB})$,where $K^*_{BA} = yT^*_A = axyP$ and returns themessage $(ID_B, T_B, S_B,MAC^*_{SK})$ to A. Again, the adversary E modifies T_B to $T^*B = aTB$, but does not change the $MAC^*_{S K}$, because he has no ability to compute it without B's secret. Now the user A computes $K^*_{AB} = xT^*_B$ and the session key $SK^{**} = H_2(ID_A||ID_B||T_A||T_B||K^*_{AB})$, AB), and the authentication token $MAC^{**}_{SK} = H_1(T_A||T^*_B|| SK^{**})$ and then compares it with received MAC^*_{SK}. However, $MAC^*_{SK} \neq MAC^{**}_{SK}$, and therefore, user A rejects the session key agreement and sends an authentication-failed message to B. Thus, the key off-set attack is not possible.

4.3. Known Key Security

Even if one session key is compromised, still more other session keys apart from the compromised ones remain secure. This is simply because every session key is unique due to the randomly chosen ephemeral key for each protocol run. Therefore, an attacker would not know any other session key from the knowledge of a compromised one because the session key computation depends on the random ephemeral keys, which is given by $SK = H_2 (ID_A||ID_B||T_A||T_B||K_{AB})$

4.4. Key Compromise Impersonation Attack

Assume that A's secret key is exposed to an adversary, and then he tries to impersonate B to A for obtaining the resulting session key. This security attribute is well satisfied in the protocol because any sender of a message endorses its authenticity by sending a verifiable signature component, $S_A = xA_{pri} + H (ID_A||T_A) A_{pri}$, that proves the ownership of the ID and corresponding public key. Therefore, without knowledge of the private key, $B_{pri} = (b+s)^{-1}P$ for B, (as an entity to be impersonated), no adversary can form a verifiable signature component S_B. Therefore, the proposed protocol secures against key-compromise impersonation attack.

4.5. No Key Control

In our scheme, both participants A and B have an input into the session key neither participant can force the full session key to be a preselected value. The session key in our protocol is determined jointly by both participants A and B. Thus $SK=H_2(ID_A||ID_B||T_A||T_B||K_{AB})$,depends on $T_A = xP$ and $T_B = yP$, and these are generated by A and B respectively. Therefore, any single user cannot control the outcome of the session keys or enforce others.

4.6. Perfect Forward Security and PKG Forward Security

If the secret keys of A and B are compromised, it does not allow an adversary to recover any past session keys. The adversary may compute the session key SK if he knows $K_{AB} = xyP$ T_A and T_B. Suppose T_A and T_B are disclosed to adversary, he cannot compute K_{AB} due to hardness of CDHP problem. From this discussion one can see that, if the secret key of PKG is disclosed, the secret key of all participants are compromised, but the current or past session keys are still secured. Thus, the perfect forward security and PKG forward security are preserved in our protocol.

5. Efficiency Analysis

In this section we compare our protocol with other existing protocol in terms of pairing, scalar multiplication, exponentiation and group addition. From the table 1 it is shown that proposed protocol is more computational efficient than others. The proposed protocol does not involve pairing or exponentiation, where as protocols [8] and [10] includes pairing and exponentiation which increases the cost. The protocols [11, 12 and 13] do not involve pairing or exponentiation, but their computational cost is overweighed by more number of scalar multiplication and group addition. Therefore proposed protocol is computational more efficient.

Table 1. Efficiency Comparison

Operation protocol	Pairing	exponentiation	Scalar multiplication	Group addition
Smart [8]	2	-	2	-
Wang. [10]	2	4	-	-
Zhu. [11]	-	-	12	-
Cao. [12,13]	-	-	10	4
Proposed	-	-	4	2

6. Conclusion

This paper presented an efficient ID-based key agreement protocol that is pairing and escrow-free. The protocol achieves all the desirable security attributes with minimum computational cost based on the ECDLP and CDHP problems. In addition to the security properties of no key control, unknown key share resilience and known key security, the proposed protocol also provides KCI resilience and PFS, which are properties lacking in many other ID-based key agreement protocols. The proposed protocol integrates a signature component in the message flow for common key computations, which ensures message integrity and the authenticity of the source of the message. The merit of the protocol is that it achieves security at a very low computational cost, making it ideal for applications adhoc devices like MANET.

Acknowledgments

We would like to thank the anonymous reviewers for their valuable comments and suggestions.

References

[1] A. Shamir, "Identity-based cryptosystems and signature protocols", Proceedings of CRYPTO84 on Advances in cryptology, Springer- Verlag, New York, USA, **(1984)**, pp.47-53.

[2] S. Blake-Wilson, D. Johnson and A. Menezes, "Key agreement protocols and their security analysis", Proc. of the 6th IMA International Conference on Cryptography and Coding, LNCS, Springer-Verlag, **(1997)**.

[3] N. McCullagh and P.S.L.M. Barreto, "A new two-party identity-based authenticated key agreement", Proc. of the topics in Cryptology-CT-RSA, **(2005)**, pp.262-274.

[4] M. Hou and Q. Xu, "A Secure ID-Based Explicit Authenticated Key Agreement Protocol Without Key Escrow", IAS09, fifth International Conference, vol. 1, **(2009)**, pp. 487-490.

[5] L.Chen and C.Kudla, "Identity based key agreement protocols from pairings", Proc. of the 16th IEEE Computer Security Foundations Workshop, **(2002)**, pp.219-233.

[6] S. Chow, "Removing Escrow from Identity-Based Encryption", New Security Notions and Key management Techniques, 12th International Conference on Pratice and Theory in Public Key Cryptography, **(2009)**, pp. 256-272.

[7] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", Lecture Notes in Computer Science, vol. 2139, **(2001)**, pp. 213-229.

[8] N. P. Smart, "Identity-based authenticated key agreement protocol based on Weil pairing, IEE Electronics Letters, vol. 38, no. 13, **(2002)**, pp. 630-632.

[9] K. Shim, "Efficient ID-based authenticated key agreement protocol based on Weil pairing", IEE Electronics Letters, vol. 39, no. 8, **(2003)**, pp. 653-65.

[10] S. Wang, Z.Cao and K-K.R. Choo, "Provably Secure ID-Based Authenticated Key Agreement without Random Oracles", Cryptology ePrint Archive, **(2006)**.

[11] R.W. Zhu, G. Yang and D.S. Wong, "An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices", Theoretical Computer Science, **(2007)**, pp.198-207.

[12] X. Cao, W. Kou, Y. Yu and R. Sun, "Identity-based authentication key agreement protocols without bilinear pairings", IEICE Transaction on Fundamentals, **(2008)**, pp.3833-3836.

[13] X. Cao, W. Kou and X. Du, “A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges”, Information Sciences, **(2010)**, pp.2895-2903.

[14] V.S. Miller, “Use of elliptic curves in cryptography”, In: Proceeding on Advances in cryptology-CRYPTO85, Springer-Verlag, New York, **(1985)**, pp.417-426.

[15] N. Koblitz, “Elliptic curve cryptosystem”, Journal of Mathematics of Computation, **(1987)**, pp.203-209.

[16] S. Hankerson, A. Menezes and S. Vanstone, “Guide to elliptic curve cryptography”, Springer-Verlag, New York, USA, **(2004)**.

Author

Shaheena Khatoon received the B.Sc., M.Sc. and MPhildegree in Mathematics form Pt. Ravishankar Shukla University, Raipur. Chhattisgarh, India in 2005, 2007 and 2009. She joined School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, India for her research work.