Indian J.Sci.Res. 17(2): 19 - 23, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

ONE ROUND TWO-PARTY KEY AGREEMENT PROTOCOL FOR MANETS USING PAIRINGS

[1]Ch. Asha Jyothi, [2]G. Narsimha
[1]Department. of Information Technology, JNTUH College of Engineering Jagtial, Nachupally, Kondagattu, Jagtial, Telangana, India.
[2]Department. of Computer Science and Engineering, JNTUH College of Engineering Sultanpur, Pulkal, Sangareddy,Telangana, India.

Abstract - In MANET environment, the network entities are free to move independently of each other. Hence these networks have dynamically changing network topology. This causes complexity in maintaining a centralized trusted authority say Certification Authority CA or Key Generation Center KCG. Security is indeed one of the most difficult problems to be solved in these networks due to lack of centralized network management. In addition most of cryptographic techniques need a key to be shared between the two communicating entities. So to establish a secret key in MANET environment, we propose a one round two-party key agreement protocol that does not take the support of central authority and secure against passive attacks. This uses mathematical function called pairings or bilinear maps. Our protocol is based on Joux's, a one round pairing-based three-party key agreement protocol which in turn is the generalization of Diffie-Hellman protocol. If Joux protocol is directly extended to two-party, it is vulnerable to release of message contents attack. Hence this paper proposes a minor modification to prevent such a passive attack.

Keywords- Pairing-based cryptography, Bilinear Maps, Mobile Ad hoc Networks, Key Agreement Protocol.

I. Introduction

Mobile ad hoc networks [20] are a special type of wireless networks. A Mobile Ad hoc NETwork (MANET) [21] is one that comes into practice as and when needed, without the support of existing fixed infrastructure. MANET is an autonomous system of mobile hosts (also serves as routers), connected by wireless links. In a MANET, no infrastructure exists and the network topology may dynamically change in an unpredictable manner since nodes are free to move. The important characteristics of MANETs [21] are Dynamic Topology, Energy-constrained operation, Limited bandwidth, Security Threats. These networks enable the deployment of communication networks at a low cost i.e., they allow the installation of networks where the nodes are setup in an instant, with very little human intervention and at a lower cost, to initiate communication and to exchange information. However, they have a disadvantage compared with classic networks: vulnerability to attacks.

Wireless transmissions are easier to intercept than those transmissions over fiber or wire-line connections. So, Ad hoc networks are particularly prone to malicious behavior. In the absence of any fixed entity [20], it becomes difficult to setup a traditional public key infrastructure and establish a centralized certification authority. Lack of any central administration makes these dynamically changing wireless structures extremely susceptible to penetration, eavesdropping, interference, and so on. Security [21] is indeed one of the most difficult problems to be solved in these networks due to lack of centralized network management. Security (cryptographic) mechanisms are used to counter these security problems. Most of the security mechanisms essentially require a secret key or session key or master key to be shared between the two communicating entities. So there is a need to share a key between the sender and receiver without the use of centralized network management or certification authority.

Key agreement [21] is one of the basic essentials of the cryptographic mechanisms. This is needed in cases where two or more users want to communicate securely among themselves. The first two-party key distribution protocol was introduced by Diffie-Hellman in 1976. Since its discovery, the Diffie-Hellman protocol [1] has become one of the most famous and largely used cryptographic primitive. In its basic version, it is a competent solution to the problem of establishing a common secret between two participants. Our protocol is based on Joux's tripartite key agreement protocol [1] which in turn is the generalization of Diffie-Hellman two-party key agreement protocol. Joux protocol uses pairings whereas Diffie-Hellman protocol uses discrete logarithm concept. Like Joux's tripartite key agreement protocol [1], our protocol also uses pairings but ours is a two-party key agreement protocol.

One round tripartite key agreement Joux's protocol [1] especially uses Weil and Tate Pairings and the idea of Diffie-Hellman [23]. These pairings were first used in cryptography as cryptanalytic tools to reduce the complexity of the discrete logarithm problem on some "weak" elliptic curves, but they are also used today to build cryptographic systems. In this paper, we present a

[1]Corresponding Author

one round two-party key agreement protocol using pairingsl for MANET environment. This model extends popularly known Joux's three-party key agreement protocol to two-party with minor modifications.

The paper is organized as: Section II discusses on the background essentials needed to understand the proposed model. Section III discusses on the related work done to share a key between two entities using pairings. Section IV talk about the detailed description of the proposed model. Section V gives the software implementation of the proposed model and Section VI confers the conclusion and future enhancements that can be done to improve the model.

II. Preliminaries

A. Bilinear Maps

The bilinear map [22] was proposed initially as a tool for breaking elliptical curve cryptography by reducing the problem of discrete logarithm on an elliptical curve to the problem of discrete logarithm in a finite field, thereby reducing its complexity. However, this method has been used recently as an encryption tool for information protection, instead of an attacking tool. Bilinear pairing is equivalent to a bilinear map.

Let A and B be abelian groups written additively with identity element 0. Suppose C is a cyclic group written multiplicatively with identity element 1. A pairing [2][17] is a non-degenerate, bilinear map

$$e : A \times B \to C,$$

Non-degenerate: for every $A_1 \in A$ there exists a $B_1 \in B$ such that $e(A_1, B_1) \neq 1$.

Bilinear: for $A_1, A_2 \in A$, $B_1, B_2 \in B$ we have

$e(A_1 + A_2, B_1) = e(A_1, B_1)\, e(A_2, B_1)$,

$e(A_1, B_1 + B_2) = e(A_1, B_1)\, e(A_1, B_2)$.

This can be restated in the following way:

$$e(aA_1, bB_1) = e(A_1, B_1)^{ab} = e(bA_1, aB_1).$$

Computable : There exists an efficient algorithm to compute $e(A_1, B_1)$ for all $A_1 \in A$ and $B_1 \in B$.

Properties of Bilinear Pairings: For $A_1 \in A$ and $B_1 \in B$, the following equations hold:

$e(A_1, O) = e(O, B_1) = 1$ where O is the point at Infinity.

$e(-A_1, B_1) = e(A_1, B_1)^{-1} = e(A_1, -B_1)$

$e(aA_1, B_1) = e(A_1, B_1)^a = e(A_1, aB_1) \quad \forall\, a \in Z$

$e(aA_1, bB_1) = e(A_1, B_1)^{ab} \quad \forall\, a, b \in Z$

Weil Pairing [11] and Tate Pairing [5] are certain examples of cryptographic bilinear maps. Pairings in elliptic curve cryptography are functions which map a pair of elliptic curve points to an element of the multiplicative group of a finite field.

There are two types of pairings commonly used in the cryptography literature. The first type of pairings are of the form $e : A \times A \to C$, where A and C are cyclic groups of prime order p. Such pairings are called symmetric pairings. The second type of pairings called Asymmetric Pairings are of the form $e : A \times B \to C$, where A, B and C are cyclic groups of prime order p. The first form is just the special case with B = A. Asymmetric Pairings are further divided into two types and hence leading to totally three types of Pairings [18]:

Type 1: A = B;

Type 2: $A \neq B$ but there is an efficiently computable homomorphism, $\psi : B \to A$;

Type 3: $A \neq B$ and there are no efficiently computable homomorphism's between A and B.

III. Literature Review

Initially pairings are used as cryptanalysis tool for reducing the discrete logarithm problem on some elliptic curves to the discrete logarithm problem in a finite field. One of the first applications of pairings with positive motive was a tripartite key agreement protocol given by Joux [1]. This requires one-round of communication but is vulnerable to man-in-the-middle attack MITMA. There are many key agreement protocols based on bilinear maps, and later most of them have been broken. Even though this key agreement does not authenticate the users, it was a noteworthy step in the advance of pairing based cryptography. This scheme does not use identity-based cryptography.

Many key agreements from bilinear maps and identity based cryptography have been since proposed. Scott [7], Smart [8], and Chen and Kudla [6] have proposed two-party key agreement protocols, all of which have been broken. All of these schemes require that all parties involved in the key agreement are clients of the same Key Generation Centre (KGC). Nalla proposes a tripartite identity-based key agreement in [9], and Nalla and Reddy propose a scheme in [10], but both have been broken [12, 13]. Shim presents two key agreements [14, 15], but both these schemes have been broken by Sun and Hsieh [16]. Another authenticated tripartite key agreement proposed by Al-Riyami and Patterson [3] was broken by Shim [4].

Our proposed model is based on Joux's Protocol. It uses bilinear maps (Pairings) and does not uses Identity based cryptography(IDC) because IDC needs the use of Key Generation Centre (KCG), a centralized controller and which is infeasible in MANETs environment.

A. Joux's Protocol

This protocol allows three users to share a common key. It is secure against passive attacks but vulnerable to active attacks like man-in-the middle attack.

Protocol Description [1]

Consider three parties A, B, C with secret keys a, b, c $\in Z_q^*$ respectively chosen at random. Also consider the Symmetric Pairing e: $A_1 \times A_1 \rightarrow C_1$ and P is the generator of the cyclic group A_1. The Protocol works as follows:

1. A sends aP to both B,C
2. B sends bP to both A,C
3. C sends cP to both A,B
4. A computes $K_A = e(bP, cP)^a$
5. B computes $K_B = e(aP, cP)^b$
6. C computes $K_C = e(aP, bP)^c$

Common agreed key of A, B, C is $K_{ABC} = K_A = K_B = K_C = e(P, P)^{abc}$.

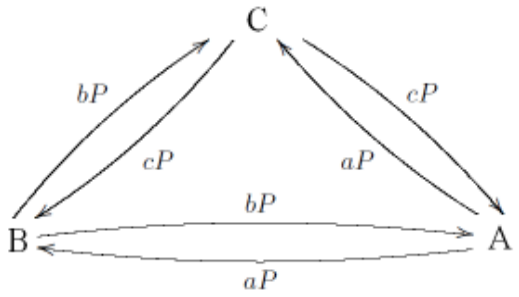

Fig1. Joux's Tripartite Key Agreement

This protocol assumes that Bilinear Diffie-Hellman (BDH) problem [sec. 3.2.] is hard to resolve. It is secure against passive attacks. It requires only one round of communication i.e., all the transmissions of Fig.1. takes place simultaneously. It is more efficient in computation because from steps 1, 2, and 3 it requires three scalar multiplications and from steps 4, 5, and 6 it requires three pairing computations and three exponentiations.

B. Diffie-Hellman Assumption

In this subsection we specify only the version of the Diffie-Hellman problem which we will require. Consider the triplet $< A, C, e >$ where A, C are two cyclic subgroups of a large prime order p and $e : A \times A \rightarrow C$ is a cryptographic bilinear map. We consider A as an additive group and C as a multiplicative group.

Bilinear Diffie-Hellman (BDH) Problem:

The security strength of the proposed model and Joux's protocol is based on the Bilinear Diffie-Helman (BDH) assumption [2]. Let P be the generator of A and a, b, c $\in Z_q^*$. The BDH assumption considers the computation of $e(P, P)^{abc}$ given <P, aP, bP, cP> to be hard.

IV. Proposed Model

One of the applications of Joux's protocol for MANETs is to share a master key between two communicating parties and one central authority say certification Authority CA or Public Key Generator PKG or among group of three users. MANET environment lacks central management and hence there is need for two-party key agreement protocol without central administration. We propose such a protocol that is based on Joux's Protocol and makes use of Pairings (or Bilinear Maps). This serves the same purpose as Diffie-Hellman but uses pairings alike Joux. Let A and B be the two communicating parties want to share a secret or session key. Let A, B respectively select secrets at random a, b □ Z_q^*. If Joux's protocol is directly extended to two-party, it appears as follows and shown in Fig 2:

1. A □ B : aP
2. B □ A : bP
3. A computes $K = e(P,bP)^a = e(P,P)^{ab}$.
4. B computes $K = e(aP,P)^b = e(P,P)^{ab}$.

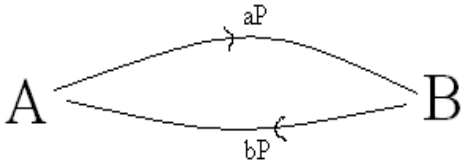

Fig 2. Extension of Joux's protocol to two-party key agreement.

But with this scheme the adversary can easily compute the key as $e(aP,bP) = e(P,P)^{ab}$ by just intercepting aP and bP during steps 1 and 2.

To counter this we slightly modify the process so that adversary is unable to generate the secret key K. Let the initiator say A selects two random values a, c □ Z_q^* and the other communicating entity B selects one random value b □ Z_q^*. The sequence of steps of our model is as follows and shown in Fig 3.

1. A □ B : aP, cP
2. B □ A : bP
3. A computes $K = e(aP,bP)^c = e(P,P)^{abc}$.
4. B computes $K = e(aP,cP)^b = e(P,P)^{abc}$.

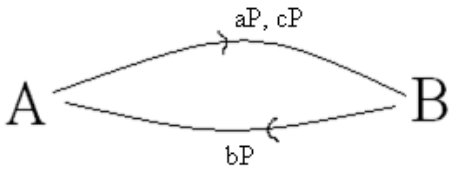

Fig 3. Proposed model for two-party key agreement

Even though adversary can intercept aP, bP and cP, but cannot compute the key K because to find the key K, he has to compute Bilinear Diffie-Hellman problem which is hard to compute. Like Joux's this model is a one-round protocol because the two exchanged messages are independent of each other. Like Joux's protocol the strength of our proposed model also depends on the hardness of BDH problem. Like Joux's our model is only resistant to passive attacks and needs at least one additional round of communications in order to resist from active attacks.

V. Implementation

Two-party key agreement protocol is implemented in software using the Pairing-Based Cryptography Library (PBC) [19]. The Elliptic curve chosen and the results of our proposed model are as follows:

The Elliptic curve is chosen as: $y^2 = x^3 + x$, with x, y elements of a Field F_q; q is a prime number. A is a subgroup of $E(F_q)$. C is a subgroup of F_q^2. There are q+1 points on the ECC curve, i.e. $\#E(F_q) = q+1$.

q = 3 modulus 4.

r = order of A = prime factor of q+1.

h = cofactor = $\#E(F_q) / r$.

The following are the sample values chosen and executed:

q=87807107996633125224377819847540498158068831994142082110286533992664756308802229570786251794226622214231558587695823174592777133673174813249251299982247 91.

r=730750818665451621361119245571504901405976559617

h=120160122648911460793888213667405342048029544012513118229196151310472072893597045311028448021839065377867 76

GeneratorP=
(764213932795790385166146156484628185710738246136731223594607305863197148904107335230752866953232919510098156557991388877251113225844051396939078151410688 4,
841053126166803064145349163706237513167951671763744795990943027230354098248702951019958048685849729494818612964151563063433969126677448023463 4049031935396)

a=321231739573260508064943282038854866624801566274

c=33279005974745643182951119871411467384390110439 5

b=59106961775923294833451653834113368400396396754 1

K=e(aP,bP)^c=e(aP,cP)^b=
(411874021818983935494518378468671897765968395058497750231537284872046634607045530820852050427874577949368791925702115715036551400857093954220214517925062 6,
792272713616191570585463230096947246676587164343554480144379956667402825333387256294430771484207666103108581680992251414596583914923441539968 1428439428268)

VI. Conclusion and Future Scope

In this article, we described a generalization of the Diffie-Hellman protocol and Joux Protocol to two-parties. Our model also does not assume a centralized trusted authority, which is difficult to establish in MANET environment. Therefore, this new protocol seems quite promising as a new building block to construct new and efficient cryptographic protocols. On the other hand, there is a future scope to ensure the integrity of the data exchanged between the two communicating parties and secure against active attacks like man-in-the-middle attack. This model has all the strengths and weaknesses of Joux's protocol except that it is applicable to two-party key agreement rather than to three-party key agreement.

References

[1] Antoine Joux, "A One Round Protocol for Tripartite Diffie-Hellman," LNCS 1838, pp. 385-393, Springer-Verlag Berlin Heidelberg 2000.

[2] Ian F. Blake, Gadiel Seroussi, Nigel P. Smart, "Advances in Elliptic Curve Cryptography," London Mathematical Society Lecture Note Series, Cambridge University Press 2005.

[3] S. S. Al-Riyami, K. G. Paterson, "Tripartite authenticated key agreement protocols from pairings," IMA Conference on Cryptography and Coding, volume 2898 of Lecture Notes in Computer Science, pages 332–359, Springer-Verlag, 2003.

[4] K. Shim, "Cryptanalysis of Al-Riyami-Paterson's authenticated three party key agreement protocols," IACR Cryptology ePrint Archive, 2003.

[5] P. S. L. M. Berreto, H. Y. Kim and M. Scott, "Efficient algorithms for pairing-based cryptosystems," Advances in Cryptology – Crypto'2002, LNCS 2442, Springer-Verlag 2002, pp. 354-368.

[6] L. Chen and C. Kudla, "Identity based authenticated key agreement from pairings," Commun. Korean Math. Soc. 20 (2005), No. 4, pp. 849–859, 2005.

[7] M. Scott, "Authenticated ID-based key exchange and remote log-in with insecure token and PIN number," IACR Cryptology ePrint Archive, 2002.

[8] N. P. Smart, "An identity based authenticated key agreement protocol based on the Weil pairing," Electronics Letters, 38:630–632, IEEE, 2002.

[9] D. Nalla, "ID-based tripartite key agreement with signatures," Cryptology ePrint Archive, 2003.

[10] D. Nalla and K. C. Reddy, "ID-based tripartite authenticated key agreement protocols from pairings," IACR Cryptology ePrint Archive, 2003.

[11] D. Boneh, M. Franklin, "Identity Based Encryption from the Weil Pairing," In Advances in Cryptology - Crypto '2001, LNCS 2139, Springer-Verlag (2001), pp. 213-229.

[12] Z. Chen, "Security analysis on Nalla-Reddy's ID-based tripartite authenticated key agreement protocols," IACR Cryptology ePrint Archive, 2003.

[13] K. Shim, "Cryptanalysis of ID-based tripartite authenticated key agreement protocols," IACR Cryptology ePrint Archive, 2003.

[14] K. Shim, "Efficient ID-based authenticated key agreement protocol based on Weil pairing," Electronics Letters, 39(8):653–654, 2003.

[15] K. Shim, "Efficient one round tripartite authenticated key agreement protocol from Weil pairing," Electronics Letters, Vol. 39, Iss. 2, pp. 1-2, 2003.

[16] H.-M. Sun and B.-T. Hsieh, "Security analysis of Shim's authenticated key agreement protocols from pairings," IACR Cryptology ePrint Archive, 2003.

[17] Rana Barua, Ratna Dutta, and Palash Sarkar, "Extending Joux's Protocol to Multi Party Key Agreement," INDOCRYPT 2003, LNCS 2904, pp. 205–217, Springer-Verlag Berlin Heidelberg 2003.

[18] Steven D. Galbraith, Kenneth G. Paterson, Nigel P. Smart, "Pairings for cryptographers," Discrete Applied Mathematics, Volume 156, Issue 16, pp. 3113-3121, Elsevier, 2008

[19] Pairing Based Cryptography Library - http://crypto.stanford.edu/pbc/

[20] Hakima Chaouchi, Maryline Laurent-Maknavicius, "Wireless and Mobile Network Security - Security Basics, Security in On-the-shelf and Emerging Technologies," ISTE Ltd and John Wiley & Sons, Inc. 2009.

[21] Carlos de Morais Cordeiro, Dharma Prakash Agrawal, "Ad Hoc and Sensor Networks - Theory and Applications," World Scientific Publishing Co. Pvt. Ltd. 2006.

[22] James J. Jong Hyuk Park, Leonard Barolli, Fatos Xhafa, "Information Technology Convergence: Security, Robotics, Automations and Communication," Springer Science & Business Media – 2013.

[23] Erdal Cayirci, Chunming Rong, "Security in Wireless Ad Hoc and Sensor Networks," John Wiley & Sons Ltd., pp. 149, 2009.