Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Two-Party Threshold Key Agreement Protocol for Manets using Pairings

Ch. Asha Jyothi[1], G. Narsimha[2], J. Prathap[3] and Gorti VNKV Subba Rao[4]

[1] JNTUH College of Engineering Jagtial

Received: 13 February 2015 Accepted: 3 March 2015 Published: 15 March 2015

Abstract

In MANET environment, the nodes are mobile i.e., nodes move in and out dynamically. This causes difficulty in maintaining a central trusted authority say Certification Authority CA or Key Generation Centre KCG. In addition most of cryptographic techniques need a key to be shared between the two communicating entities. So to introduce security in MANET environment, there is a basic need of sharing a key between the two communicating entities without the use of central trusted authority. So we present a decentralized two-party key agreement protocol using pairings and threshold cryptography ideas. Our model is based on Joux?s three-party key agreement protocol which does not authenticate the users and hence is vulnerable to man-in-the-middle attack. This model protects from man-in-the-middle attack using threshold cryptography.

Index terms— pairing-based cryptography, threshold cryptography, bilinear maps, mobile ad hoc networks, key agreement protocol.

Introduction and so on. Security [22] is considered to be the major "barrier" in the commercial use of this technology. Security is indeed one of the most difficult problems to be solved in these networks due to lack of centralized network management. 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 is one of the basic cryptographic essentials. This is needed in cases where two or more users want to communicate securely among themselves. The first two-party key sharing protocol was introduced by Diffie-Hellman. Since its detection in 1976, the Diffie-Hellman protocol [1] has become one of the most well-known and mostly used cryptographic primitive. In its basic version, it is an efficient solution to the problem of creating a common secret between two participants. Since this protocol is also used as a building block in many complex cryptographic protocols, finding a generalization of Diffie-Hellman would give a new tool and might lead to new and more efficient protocols. But this is an unauthenticated protocol in the sense that an adversary who has control over the communication channel can use the man-in-the-middle attack to share two separate keys with the two users, without the users being aware of this. In this paper, we present a secure two-party key agreement protocol that protects from man-in-themiddle attack. Our protocol is based on Joux's protocol [1] which in turn is the generalization of Diffie-Hellman protocol.

One round tripartite key agreement Joux's protocol [1] uses Weil and Tate Pairings and the idea of Diffie-Hellman. These pairings were first used in cryptology as cryptanalysis tools to decrease 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 secure two-party key agreement protocol for MANET environment. This model extends the popular known Joux's tripartite key agreement protocol [1] to two-partite with minor modifications. Similar to Joux model [1], this model uses pairings or bilinear maps, unlike Joux this model uses threshold cryptography.

1 Recently

Pairing-based ireless technology [22] is suitable of communicating virtually every location on the plane of the earth. Most of the people exchange information every day using pagers, cellular telephones, laptops, several types of personal digital assistants (PDAs) and other wireless communication products. A Mobile Ad hoc NETwork (MANET) is one that comes into practice as needed, without the support of existing infrastructure or any other kind of fixed stations. MANET is an independent system of mobile hosts (also serving 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 natural characteristics of MANETs [22] include frequently changing Topology, Lack of Central Administration, Battery Power supply or Restricted Energy, Restricted bandwidth, Physical Security fear.

Ad hoc networks are particularly prone to malicious behavior. Lack of any centralized network management or certification authority makes these dynamically changing wireless structures extremely vulnerable to penetration, eavesdropping, interference, W Year 2015 cryptography in the form of Identity-based cryptography has become a highly working research issue.

The paper is organized as: Section II discusses on the background fundamentals needed to understand the proposed model. Section III discusses on the previous 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.

2 II.

3 Preliminaries a) Bilinear Maps

The bilinear map was proposed originally as a tool for attacking elliptical curve encryption by reducing the problem of discrete algebra on an elliptical curve to the problem of discrete algebra 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.

Consider two additively written abelian groups A1 and A2; the identity element being 0. Also consider a multiplicatively written cyclic group C; the identity element being 1. A pairing [2][17] on A , A and C is a non-degenerate, bilinear map A bilinear pairing e is a function which maps a pair of points on an elliptic curve E, defined over fields A1 and A2, to an element of the multiplicative group of a finite extension field C. This mapping is said to be pairing as it maps a pair of elliptic curve points. The pairing e has the following characteristics: Non-degenerate: Given a point the re e xis ts a point s uch tha t e ; Whe re is the p oint at infinity on the elliptic curve over the finite field A1.

4 Bilinear: for all points

This can be redefined in the following way:

Computable: There exists a computationally efficient algorithm to find e(X, Y) for all X Laws of Bilinear Pairings: The following equations holds good for the bilinear pairing e. Consider X is the p oint a t Infinity.

where and C are cyclic groups of prime order p written additively and multiplicatively respectively.

The second type of pairing called Asymmetric Pairings are of the form The first form is just the special case with A2= A1. Asymmetric Pairings are further divided into two types and hence leading to totally three types of Pairings [19] Type 1:A 1 = A 2 Symmetric Pairing; Type 2 :

As ymmetric Pa iring but there is a n efficiently computable homomorphism function Type 3 :

Asymmetric Pairing and there are no efficiently computable homomorphism functions between A 1 and A 2 .

5 b) Threshold Cryptography

Let t and n be positive integers, t threshold scheme [25] is a method of sharing a secret K among a set of n participants in such a way that any t participants can compute the value of the secret, but no group of t?1 or fewer can do so.

Let the set of participants be denoted by E. The value of the secret K is chosen by the dealer, denoted D, who is a special participant not in E. When D wants to share the secret K among the participants in E, D gives each participant some partial information, called a share. The shares are distributed secretly, so no participant knows any other participant's share.

At a later time, when some qualified subset of participants F ? E want to compute the secret K, they will then pool their shares together. The most famous construction of a (t, n)-threshold scheme, called the Shamir Threshold Scheme [18][21], is invented in 1979. Therefore, a (t, n) threshold secret sharing scheme can protect the secret against an adversary who can intercept at most t ? 1 paths. In t he proposed model D don't want to share the secret K among several participants in E, but D wants to share the key with the other end of communication say G, with whom he wants a secure communication. So D sends the shares of thee : A 1 × A 2 ? C. 1 2 O ? X ? A 1 Y ? A 2 Y ? A 2 O X, X 1 , X 2 ? A 1 , and Y, Y 1 , Y 2 ? A 2 and u, v ? Z we have e(X 1 + X 2 , Y 1)

= e(X 1 , Y 1) e(X 2 , Y 1), e(X 1 , Y 1 + Y 2) = e(X 1 , Y 1) e(X 1 , Y 2). e([u]X, [v]Y) = e(X, Y) uv = e([v]X, [u]Y;.

where [u]X = X + X +..+ X (u times)? A 1 and Y ? A 2 .

?A 1 , and Y ? [11] and Tate Pairing [5]. 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.A 2 and u, v ? Z and O e(X, O) = e(O, Y) = 1 e(-X, Y) = e(X, Y) -1 = e(X, -Y) e([u]X, Y) = e(X, Y) u = e(X, [u]Y) e([u]X, [v]Y) = e(X, Y) uv e : A 1 × A 1 ? C, A 1 A 1 ? A 2 ? : A 2 ? A 1 ; A 1 ? A 2

There are two types of pairings commonly used in the cryptography literature. The first type of pairing called Symmetric Pairings are of the form secret key K through n independent paths [24] to G. When G receives at least t shares, he can recover the secret and there by a key is shared between D and E.

Year 2015 e : A 1 × A 2 ? C, where A1, A2 are additively written cyclic groups of prime order p and C is a multiplicatively written cyclic group of prime order p.

The opponent is facing the challenge of getting at least t shares by intercepting t paths at the same time, unless until he cannot recover the secret key.

6 III.

7 Related Work

There are many key agreement protocols based on bilinear maps, and later most of them have been broken. One of the first applications of pairing based cryptography was a tripartite key agreement protocol given by Joux [1]. This key agreement protocol does not authenticate the users, and thus is subject to the attack namely man-in-the-middle. Of course, it was an important step in the advancement of pairing based cryptography. This protocol only uses pairings especially Tate pairing but 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, none 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 recommends a tripartite identity-based key agreement in [9], and Nalla and Reddy recommends a authenticated tripartite identity-based key agreement scheme in [10], but both have been broken down [12,13]. Shim presents two key agreement protocols [14,15], but both of these schemes have been broken by Sun and Hsieh [16]. Another authenticated tripartite key agreement protocol recommended by Al-Riyami and Patterson [3] was broken by Shim [4]. Cullagh and Barreto recommend a two-party identity based authenticated key agreement. Most of the above protocols are based on identity-based cryptography.

Our proposed model is based on Joux's Protocol [1]

8 b) Diffie-Hellman Assumption

In this subsection we specify the version of the Diffie-Hellman problem which we will require. Consider the triple < A , C, e > where A , C are two cyclic subgroups of a large prime order q and e : A1 x A ? C is a cryptographic bilinear map. We take A as an additive group and C as a multiplicative group.

9 Bilinear Diffie-Hellman BDH Problem

The strength of Joux's protocol is based on the Bilinear Diffie-Helman (BDH) [2] assumption. Let P be the generator of A1 and a, b, c are positive integers . The BDH assumption considers the computation of e(P, P) given <P, aP , bP, cP> to be hard. When A and B receives at least t shares of Si and Ri respectively, they can reconstruct S and R as Hence unless the adversary intercepts at least t shares of Ri and Si, he cannot reconstruct R and S and therefore the key. Also the key is the session key that has small life time i.e., over a single session; hence the time scope for adversary to reconstruct the key is small, thereby protecting the protocol from man-in-the-middle attack.

10 c) Man-in-the-middle Attack

V.

11 Implementation

The proposed key agreement protocol is implemented in software using the Pairing-Based Cryptography Library (PBC) **??**20]. The results are as follows: The Elliptic curve is chosen as: y2 = x3 + x, with x, y elements of a Field Fq; q is a prime number. A1 is a subgroup of E(Fq). C is a subgroup of Fq2. There Year 2015

To counter this we apply the concept of threshold cryptography for steps 1 and 2; steps 3 and 4 remain the same. The secrets 'u' and 'v' are split into n shares each using Shamir's secret sharing mechanism [21] to get u i and n, whe re n is the numbe r of multiple independent paths that exist between sender and receiver. The shares of the products [u] P and [v]P are then calculated as R i = [u i]P and S i = [v i]P. These shares are then exchanged through n independent paths with the other party as shown in

12 Conclusion and Future Scope

In this article, we described a generalization of the Diffie-Hellman protocol and Joux Protocol to twoparties. Our two-party key agreement protocol uses the pairings and threshold cryptography concepts. 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 complex cryptographic protocols. On the other hand, there is a scope to ensure the integrity of the secret shares. Additionally, there is scope to use this shared secret key in pairing based cryptography for encryption and decryption of messages, there by secret transmission of messages between the two communicating parties. [1]

1

Figure 1: 1 2E

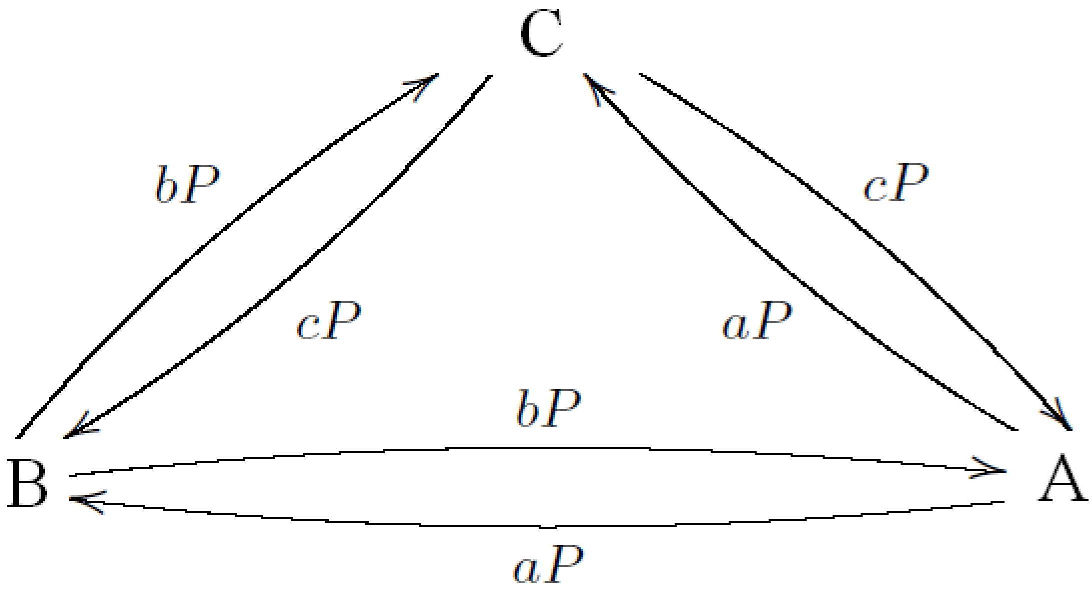
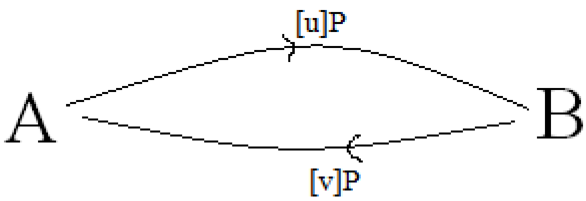


Figure 2:

Figure 3:

1

Figure 4: 1 × A 1 ?



1

Figure 5: Figure 1 :

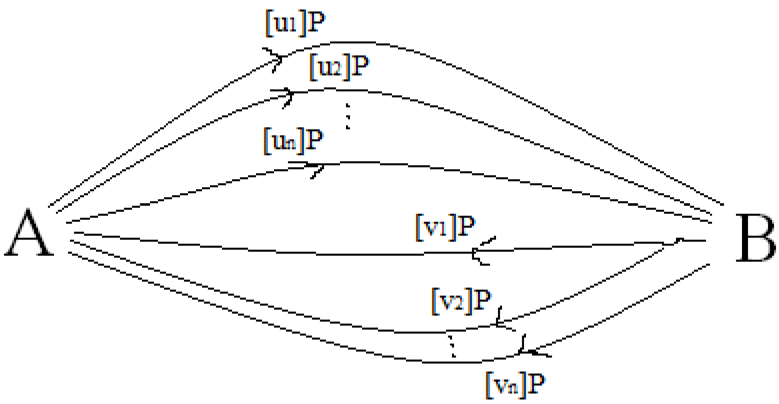


Figure 6:

231 

Figure 7: Figure 2 :Figure 3 : 1 4

Figure 8:

[Cryptology Eprint ()] , Archive Cryptology Eprint . http://eprint.iacr.org/ 2003/103, 2003. 2003/103. (Report)

[Maggie Xiaoyan Cheng Li (ed.) (2008)] *Advances in Wireless Ad Hoc and Sensor Networks -Springer Science & Business Media*, Deying Maggie Xiaoyan Cheng, Li (ed.) Dec-2008. 15.

[Gorti et al. ()] 'An Efficient Secure Message Transmission in Mobile Ad Hoc Networks using Enhanced Homomorphic Encryption Scheme -Global'. Vnkv Subba Gorti , & Rao , Dr , Garimella Uma . *Journal of Computer Science and Technology* 2013. 13. (Issue 9 Version 1.0 Year)

[Smart ()] 'An identity based authenticated key agreement protocol based on the Weil pairing'. N P Smart . *Electronics Letters* 2002. 38 p. .

[Scott ()] *Authenticated ID-based key exchange and remote log-in with insecure token and PIN number*, M Scott . http://eprint.iacr.org/2002/164/ 2002/164, 2002. (Report) (Cryptology ePrint Archive)

[Blake et al. ()] Ian F Blake , Gadiel Seroussi , Nigel P Smart . *Advances in Elliptic Curve Cryptography*, London Mathematical Society Lecture Note Series 2005. Cambridge University Press. 317.

[Shim ()] *Cryptanalysis of Al-Riyami-Paterson's authenticated three party key agreement protocols. Cryptology ePrint Archive*, K Shim . http://eprint.iacr.org/2003/122 2003/122, 2003. (Report)

[Shim ()] 'Cryptanalysis of ID-based tripartite authenticated key agreement protocols'. K Shim . http://eprint.iacr.org/2003/115 *Cryptology ePrint Archive* 2003/115, 2003. (Report)

[De and Cordeiro] Carlos De , Morais Cordeiro . *AD HOC AND SENSOR NETWORKS Theory and Applications -Copyright © 2006 by*, World Scientific Publishing Co. Pte. Ltd.

[Berreto et al. ()] 'Efficient algorithms for pairing-based cryptosystems'. P S L M Berreto , H Y Kim , M Scott . *Advances in Cryptology -Crypto '2002*, 2002. Springer-Verlag. 2442 p. .

[Shim ()] 'Efficient ID-based authenticated key agreement protocol based on Weil pairing'. K Shim . *Electronics Letters* 2003. 39 (8) p. .

[Shim ()] *Efficient one round tripartite authenticated key agreement protocol from Weil pairing*, K Shim . 2003.

[Barua et al. ()] 'Extending Joux's Protocol to Multi Party Key Agreement'. Rana Barua , Ratna Dutta , Palash Sarkar . *INDOCRYPT 2003*, LNCS 2904 (Berlin Heidelberg) 2003. Springer-Verlag. p. .

[Shamir ()] 'How to share a secret'. A Shamir . *Communications of the ACM* 1979. 22 (11) p. .

[Nalla and Reddy ()] *ID-based tripartite authenticated key agreement protocols from pairings. Cryptology ePrint Archive*, D Nalla , K C Reddy . http://eprint.iacr.org/2003/004 2003/004, 2003. (Report)

[Nalla ()] *ID-based tripartite key agreement with signatures. Cryptology ePrint Archive*, D Nalla . http://eprint.iacr.org/2003/144 2003/144, 2003. (Report)

[Chen and Kudla ()] 'Identity based authenticated key agreement from pairings'. L Chen , C Kudla . http://eprint.iacr.org/2002/184 *Cryptology ePrint Archive* 2002/184, 2002. (Report)

[Boneh and Franklin ()] 'Identity Based Encryption from the Weil Pairing'. D Boneh , M Franklin . *Advances in Cryptology -Crypto '2001*, 2001. Springer-Verlag. 2139 p. .

[Iftene] Sorin Iftene . *Secret Sharing Schemes with Applications in Security Protocols. Thesis submitted to the*, University of Iasi for the degree of Doctor of Philosophy in Computer Science

[Joux ()] Antoine Joux . *One Round Protocol for Tripartite Diffie-Hellman. LNCS 1838*, (Berlin Heidelberg) 2000. Springer-Verlag. p. .

[Mccullagh and Barreto] Noel Mccullagh , Paulo S L M Barreto . *A New Two-Party Identity-Based Authenticated Key Agreement -Topics in Cryptology-CT-RSA 2005*, Springer.

[Sun and Hsieh ()] *Security analysis of Shim's authenticated key agreement protocols from pairings. Cryptology ePrint Archive*, H.-M Sun , B.-T Hsieh . http://eprint.iacr.org/2003/113 2003/113, 2003. (Report)

[Chen ()] *Security analysis on Nalla-Reddy's IDbased tripartite authenticated key agreement Year*, Z Chen . 2015.

[Steven et al. ()] D Steven , Kenneth G Galbraith , Nigel P Paterson , Smart . 10.1016/j.dam.2007.12.010. *Pairings for cryptographers*, 2008. Elsevier. 20. PBC (Pairing-Based Cryptography) Library

[Al-Riyami and Paterson ()] 'Tripartite authenticated key agreement protocols from pairings'. S S Al-Riyami , K G Paterson . *IMA Conference on Cryptography and Coding* 2003. Springer-Verlag. 2898 p. .