Modified Authentication Protocol Using Elliptic Curve Cryptosystem for Virtual Subnets on Mobile Adhoc Networks

Ankush A. Vilhekar and C.D. Jaidhar

ABV-Indian Institute of Information Technology and Management, Gwalior
Morena Link Road, Gwalior India-474010
mtis_200904@students.iiitm.ac.in, cdjaidhar@rediffmail.com

Abstract. In 2010, an efficient authentication protocol has been proposed for virtual subnets on Mobile Adhoc Networks (MANET). It uses virtual subnet and each node in the subnet is authenticated using certificate. Further, it is claimed that protocol is robust, more efficient and practical. However, it is not suitable for devices have low computation power like mobile, PDAs, smart cards because number of computations are more in RSA based cryptosystem. In order to reduce the number of computation with same level of security, this paper proposes the same scheme using Elliptic Curve Cryptography (ECC) (modified scheme). Our scheme uses ECC in place of RSA to reduce number of computations with shorter key size.

Keywords: Mutual authentication, Mobile Ad-hoc Networks, Elliptic Curve Cryptography.

1 Introduction

A Mobile Ad-hoc Network (MANET)[1,6] is infrastructure-less communication network which is created on demand without support from central servers. It is an autonomous system of mobile nodes connected by wireless links. Each mobile node communicates with other nodes within its transmission range by radio waves and relays on other nodes to communicate with mobile nodes outside its transmission range. MANETs have some special characteristic such as topology changes dynamically, open medium, absence of fixed central structure, constrained capability, limited bandwidth, battery, lifetime and computation power of nodes etc. Due these characteristics, MANETs are vulnerable to various types of attacks such as impersonation, denial-of-service, passive and active attacks. Mobile phones, palm computers etc., got vide popularity in today's world because they are portable in nature. People can uses these portable devices at anytime and anywhere to do business over an Internet such as Internet banking, pay TV channel (dish TV, big TV), on-line shopping etc. Security is utmost important when user secrete information is transmitted over insecure communication channel. MANET needs to divide into sub domains or groups in order to provide security services and efficient

P. Sénac, M. Ott, and A. Seneviratne (Eds.): ICWCA 2011, LNICST 72, pp. 426–432, 2012.

communication. MANET architecture for single subnet is as shown in figure 1. Due to this, only legitimate node can access information and it also reduces redundant transmission. Despite the fact that there is no centralized device in MANET to construct the groups or virtual subnet [2, 3]. To provide secure group communication in virtual subnet to resist possible attacks from malicious nodes, authentication is the primary requirement. Public Key Cryptosystem (PKC) based authentication scheme has been proposed [4,5, 10,11]. Number of computations is more in PKC because of discrete logarithm problem. Mobile nodes in MANET have constraints on bandwidth, processor, memory and power. As the number of computation increases power consumption also increases. Hence, PKC is not suitable for MANET. In order to reduce the number of computations with same level of security, this paper propose modified scheme using Elliptic Curve Cryptosystem. Security of the ECC is based upon difficulty of Elliptic Curve Discrete Logarithm Problem (ECDLP) and Elliptic Curve Deffie-Hellman problem (ECDHP)[7,8,9]. Compared with PKC, ECC offers a better performance because it achieves the same security with smaller key size.

The rest of our paper is organized as follows. Section 2 provides review of the authentication protocol for virtual subnets on MANET. Proposed authentication scheme described in section 3. Security analysis discussed in section 4. Finally, conclusion given in section 5.

2 Review of Authentication Protocol for Virtual Subnet on Mobile Ad-Hoc Networks (MANET)[13]

Node authentication for virtual subnet has been proposed [13]. It consists of three phases named as Key Generation phase, Certificate Generation phase and Certificate Authentication phase. The process of assigning the key pair before deployment is as follows. All the nodes in virtual subnet elect a node called a leader node whose sole responsibility is to generate common shared key and individual private key for every node.

This section is providing the details of previous scheme [13] including three phases and they are as follows.

2.1 Key Generation

Step 1. Leader node generates two large prime number 'p' and 'q', then computes $N = p*q$: randomly selects g such that $g \in Z^*_N$ where $Z^*_N = \{g \mid 1 \leq g \leq N-1, gcd(g, N) = 1\}$.

Step 2. Leader node generates $a_1, a_2, \ldots\ldots, a_k$. k is number of nodes in virtual subnet, where $gcd(a_i, a_j) = 1$, $gcd(a_i, \phi(N)) = 1$, , $1 \leq i, j \leq k$ and $i \neq j$.

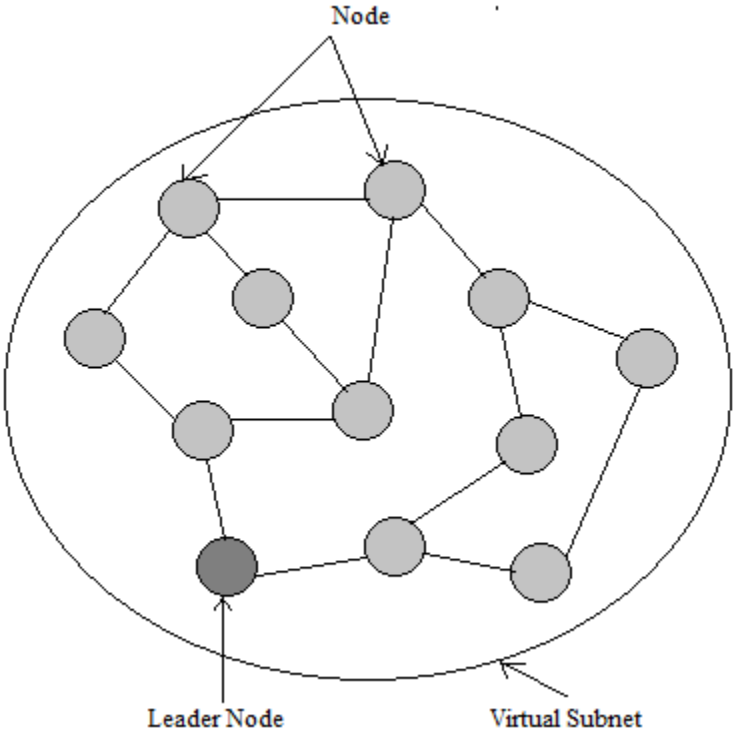

Fig. 1. MANET Architecture of single subnet

Step 3. Leader node calculate private key $s_i = {}_g\Pi^k_{j=1, j\neq I}\ a_j \bmod N$ *for node I,* $1 \leq i \leq k$.

Step 4. Leader node calculate common shared key $v = 1 /\ {}_g\ \Pi^k_{j=1, j\neq I}\ a_j \bmod N$.

Step 5. Leader node sends (s_i, a_i) to node i, where $1 \leq i \leq k$.
Leader node is no longer valid after the completion of key generation.

2.2 Certificate Generation

Step 1. Node i randomly select r *such that* $r \in Z^*_N$ where $1 \leq i \leq k$.

Step 2. Node i generate $x = r^{ai} \bmod N$.

Step 3. Node i calculates $\alpha = h(a_i, x)$, and $y = r * s_i^{\alpha} \bmod N$, certificate of node i is $cert\ i = (ID_i, a_i, \alpha, y)$ *where* ID_i is identity of node i and $h()$ is strong oneway hash function.

The source node broadcasts a virtual subnet join request packet as an advertisement which includes certificate.

2.3 Certificate Authentication

Step 1. Any node in a subnet can authenticate the other nodes in the same subnet using certificate of node i. Using public key *v and cert i = (ID_i, a_i, α, y)* node in the subnet computes $x' = y^{ai} * v^{\alpha} \bmod N$.

Step 2. *x'* is used to generate $\alpha' = h(a_i, x')$. If $\alpha = \alpha'$, then the node is legitimate one and belongs to the same group otherwise, discard certificated node.

3 Proposed Authentication Protocol Using Elliptic Curve Cryptosystem

Authentication scheme proposed in this paper is based on ECC and it is a modified version of scheme [13]. Elliptic Curve is cubic equation of basic form

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

where *a, b, c, d* and *e* are real numbers. In ECC over prime finite field F_p, the Elliptic Curve equation is standardized in the form of

$$y^2 = (x^3 + ax + b) \bmod p$$

and equation is denoted as $E_p(a, b)$. where $a, \ b \in F_p$, $p > 3$ and $4a^3 = 27b^2 \neq 0 \ (mod \ p)$. Given an integer $s \in F_p^*$ and a point $B \in E_p(a, b)$, the point multiplication $s \ . \ B$ over $E_p(a, b)$ can be defined as $s \ . \ B = (B + B + \ldots\ldots + B)_{s \ times}$. Security of the ECC totally depends on the difficulties of following problems as defined in [8].

Problem 1- Given two points *A* and *B* over $E_p(a, b)$, the Elliptic Curve Discrete Logarithm Problem(ECDLP) is to find an integer $s \in F_p^*$ such that $B = s \ . \ A$.

Problem 2- Given three points A, $s \ . \ A$ and $t \ . \ A$ over $E_p(a, b)$ for $s, t \in F_p^*$, Elliptic Curve Diffie- Hellman Problem (ECDHP) is to find the point $(s \ . \ t) \ . \ A$ over $E_p(a, b)$.

Problem 3- Given two points *A* and $B = s \ . \ A + t \ . \ A$ over $E_p(a, b)$ for $s, t \in F_p^*$, Elliptic Curve Factorization Problem (ECFP) is to find two points $s \ . \ A$ and $t \ .A$ over $E_p(a, b)$.

Proposed scheme consists of three phases namely Key Generation phase, Certificate Generation phase and Node Authentication phase. Prior to key generation, all nodes elect a node called as leader node. Its function is to generate and distribute common shared key and individual private key for all the nodes. The key generation steps are as follows.

3.1 Key Generation

Step 1. Leader node chooses Elliptic Curve $E_p(a, b)$ in which p is prime number used for modulo operation and a, b are the values of coefficient in equation $y^2 = x^3 + ax + b$.

Step 2. Leader node generates $a_1, a_2, \ldots\ldots\ldots\ldots, a_i$. k is number of nodes in the group where $1 \leq i \leq k$.

Step 3. Then leader node calculates private key X_i for node i, $1 \leq i \leq k$, $X_i = B \,.\, \Pi^k_{j=1} a_j \bmod p$ where B is base point on elliptic curve.

Step 4. Leader node computes common shared key $s = (B. \Pi^k_{j=1} a_j \bmod p)^{-1}$

Step 5. Finally, leader node sends the parameters (X_i, s, a_i) to node i where $1 \leq i \leq k$.

After the generation and distribution of private key and common shared key, leader node no longer valid in other words leader node is temporary. This is to ensure that a leader node does not maintain private key and common shared key of other nodes. Key generation phase is executed whenever there is a change in the subnet. Therefore, private key and common shared key are refreshed to provide forward secrecy and backward secrecy.

After the distribution of parameter to all the nodes of virtual subnet, they deploy over specified region and communication can be initiated randomly. Each node needs to generate its own certificate to provide authentication in virtual subnet. Certificate generation steps are as follows.

3.2 Certificate Generation

Step 1. Node i randomly selects r, r belongs to Z_p^* where $1 \leq i \leq k$.

Step 2. Node i generates $q = r \,.\, a_i \bmod p$.

Step 3. Then node i calculates $C = h(a_i, q)$, $g = r \,.\, x_i \,.\, C \bmod p$. Certificate of node i is Cert $i = (ID, a_i, C, g)$ where IDi is the identity of node i, h() is a strong one way hash function.

The source node broadcasts a virtual subnet join request packet as an advertisement in which certificate parameters are included. All other nodes in the same virtual subnet receive the join request packet and process them to authenticate the node in the subnet. The authentication procedure is as follows

3.3 Certificate Authentication

Step 1. Any node in a virtual subnet can to authenticate the other node i in the same subnet using public key s and node 'i' certificate parameters $Cert_i = (ID, a_i, C, g)$ to calculate $q' = g \,.\, a_i \,.\, s \,.\, C^{-1} \bmod p$.

$q' = r \,.\, x_i \,.\, C \,.\, a_i \,.\, x_i^{-1} \,.\, C^{-1} \bmod p$
$q' = r \,.\, a_i \bmod p$
$q' = q$

Step 2. Then it uses q' to compute $C' = h(a_i, q')$ to verify whether $C = C'$, If they are equal then node is authenticated else drop the received certificate.

4 Security Analysis

4.1 Replay Attack

In the proposed scheme, the replay attack fails because the private key and shared key is refreshed whenever there is a change in the membership. Role of leader node is only for short span of time and no longer exists once the key generation and distribution phase is completes. This is to ensure that node cannot obtain private key of other nodes.

4.2 Outsider Attack

Attacker is unable to derive private key of the node 'i' from the intercepted certificate *Cert i= (ID, a_i, C, g).* To obtain private key X_i of node 'i' generated by leader node, attacker needs to compute x_i and r. This is infeasible because of ECDLP and ECFP. As per the previous research, still there is no algorithm is able to solve these problems. Hence, proposed scheme withstands outsider attack.

4.3 Stolen Verifier Attack

Nodes in virtual subnet do not store any verification table. Hence, proposed scheme resists stolen-verifier attacks. When a new node is added in the virtual subnet, other nodes need not to keep private or shared secrete in the storage space. Whenever there is a change in change in the membership both the keys are refreshed which ensure the Therefore, the proposed scheme can resist stolen-verifier attacks and provides high scalability for the user addition such that it is very practical for the applications with large number of users.

5 Conclusion

Authentication protocol for virtual subnets on Mobile Adhoc Networks has been proposed using RSA based Public Key Cryptosystem. It has more computation cost because of RSA Public Key Crypto system. In order to reduce the number of computations with same level of security, this paper proposes the same scheme using Elliptic Curve Cryptosystem. Our scheme provides the same level of security with shorter key size. Further, security analysis shows that proposed scheme is highly secure.

References

1. Aziz, B., Nourdine, E., Mohamed, E.-K.: A Recent Survey on Key Management Schemes in MANET. In: ICTTA 2008, pp. 1–6 (2008)
2. Perkins, C.: Ad Hoc Networks. Addison-Wesley, Reading (2001)
3. Rajaravivarma, V.: Virtual Local area Network Technology and Applications. In: Proceeding of the Twenty-Ninth Southeastern Symposium, March 9-11, pp. 49–52 (1997)
4. wieselthier, J.E., Nguyen, G.D., Ephremides, A.: Algorithms for Energy-Efficient Multi-casting in Static Ad Hoc Wireless Network. In: Mobile Networks and Applications (MONET), June 2001, 6-3, pp. 251–263 (2001)
5. Li, F., Xin, X., Hu, Y.: Identity Based Broadcast Signcryption. Computer Standard and Interfaces 30, 89–94 (2008)
6. Capkum, S., Buttya, L., Hubaux, P.: Self-Organized Public Key Management for Mobile Ad Hoc Networks. IEEE Trans. Mobile Computing 2(1), 52–64 (2003)
7. Miller, V.S.: Use of Elliptic Curves in Cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986)
8. Koblitz, N.: Elliptic Curve Cryptosystem. Mathematics of Computation 48, 203–209 (1987)
9. Forouzan, B.A.: Cryptography and Network Security, special Indian edition. Tata McGraw Hill (2007)
10. Chiang, T.-C., Yeh, C.-H., Huang, Y.M.: A Virtual Subnet Protocol for Mobile Ad Hoc Networks Using Forwarding Cache Scheme. International Journal of Computer Science and Network Security 6(1), 108–115 (2006)
11. Huang, Y.M., Yeh, C.H., Wang, T.I., Chao, H.C.: Constructing Secure Group Communication over Wireless Ad Hoc Networks based on a Virtual Subnet Model. IEEE Wireless Communications 14(5), 70–75 (2007)
12. Guillou, L.C., Quisquater, J.-J.: A “Paradoxical” Identity-Based Signature Scheme Resulting from Zero-Knowledge. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 216–231. Springer, Heidelberg (1990)
13. Chang, C.-W., Yeh, C.-H., Tsai, C.-D.: An Efficient Authentication Protocol for Virtual Subnets on Mobile Ad Hoc Networks. In: International Symposium on Computer, Communication, Control and Automation, 3CA2010, pp. 67–70 (2010)
14. Kavak, N.: Data Communications in ATM Networks. IEEE Network 9(3) (May/June 1995)