International Journal of Networked and Distributed Computing, Vol. 2, No. 2 (April 2014), 70-77

Fully distributed certificate authority based on polynomial over elliptic curve for MANET

Ahmad Alomari
Faculty of Mathematics and Computer Science, University of Bucharest
Bucharest, Romania
alomari.jordan@gmail.com

Abstract

A mobile ad hoc network (MANET) is a wireless communication network, which does not rely on any centralized management or a pre-existing infrastructure. Various certificate authorities (CAs) distributed over the network, each with a periodically updated share of the secrete key, is usually adopted. Elliptic Curve Cryptography (ECC) is a cryptographic technique prominent suited for small devices, like those used in wireless communications, and is gaining momentum. The main advantage of ECC versus RSA is that for the same level of security it requires a much sorter key length. The purpose of this work is to design and implement a fully certificate authority based on polynomial over elliptic curve, based on trust graphs and threshold cryptography, which though has better cryptography in nature. The security is based on the elliptic curve discrete logarithm problem.

Keywords: MANET; certificate authorities; certificate revocation; elliptic curve cryptography.

1. Introduction

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration. People and vehicles can thus be Internet worked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with each other within their radio range; if the nodes are not in the direct communication range they use the intermediate nodes to communicate with each other. In these two situations, the network is formed when all the nodes participated in the communication automatically, therefore this kind of wireless network can be known as mobile ad hoc network. Mobile ad hoc networks (MANETs) have become one of the fastest growing areas for the researchers, with the propagation of cheaper, smaller, and more powerful mobile devices. Due to self-organize and rapidly deployment, MANET can be applied to different applications including emergency relief scenarios, battlefield communications, public meeting, law enforcement, also the ad hoc self-organization makes them suitable for virtual conferences, where setting up a traditional network infrastructure is a time-consuming high-cost task. Among all the research issues of ad hoc network, the nature of communication and lack of infrastructure support make the security particularly more challenging. A number of security mechanisms has been developed and proposed, but it is still hard to ensure that whole network is free from any malicious attack.

Providing security services including authentication, integrity confidentiality, availability, and anonymity to the mobile user is the main goal of the security solutions for MANET. To achieve this goal, the security solution should supply complete protection spanning the entire protocol stack. The traditional Internet style key distribution protocols, like Kerberos, relying on online trusted third parties (TTP) to distribute session keys to nodes are infeasible for ad hoc networks because the TTP may be out of range or not available to all of the nodes or during certain times for a number of

Published by Atlantis Press

reasons. These include communication range limitations, network dynamics, node movements and unknown network topology prior to deployment. There are a number of researches and proposals for ad hoc networks, which try to increase the availability of the key distribution service by repeating the online key server to a subset of nodes arranged arbitrarily or hierarchically. Nevertheless, the performances of these schemes, in terms of efficiency and scalability, are still not reassuring. In addition, these schemes still need TTP; compromising the TTP compromises all the keys it issues.

This work focuses on peer-to-peer key management in fully self-organized mobile ad hoc networks. A fully self-organized MANET means any user with the appropriate equipment (and software) can join and leave at random, and we can call this network as an "open" network; there is no form of access control. Such a network will therefore not find application in, for example, hostile military environments, but rather in commercial, community-based environments. Present approaches for authentication services depend on centralized management approaches by either certificate authorities (CA) or key distribution centers. A centralized approach may be acceptable in cases where a specific node can be protected and is accessible by other nodes of the network. However, for the wireless ad hoc networks that we visualize for our targeted applications, a centralized approach will suffer from a single-point of service denial and may be unreachable by network nodes requiring CA services. Thus a more robust CA approach must be used. This need for wireless ad hoc networks is presently a very active research area. Providing CA functionality in an ad hoc network is to assign a single node to be the CA. The success of this scheme depends on that single CA node. Since failure of one node breaks the system, this approach is not fault tolerant. Similarly this approach is highly vulnerable, since an adversary needs only to compromise one node to acquire the secret key. Finally, given the unpredictability and expected mobility of ad hoc networks, it may be possible that nodes will not be able to reach the CA in due course, making availability greatly unpredictable. Thus, a single CA cannot effectively service a whole ad hoc network.

In this paper we proposed a dynamic fully distributed certificate authority scheme based on a polynomial over elliptic curve for Mobile Ad Hoc Networks, which though has better cryptography in nature. The security is based on the elliptic curve discrete logarithm problem, but the participants' keys are distributed by a trusty center, which takes a lot of inconvenient in practical applications. This article offers a sharing scheme based on a polynomial over elliptic curve, in these scheme participants will hold optional sub-secret keys.

2. Related Work

Major H One of the first approaches to solve the key management problem in MANETs is Partially Distributed Certificate Authority Approaches published in Securing Ad Hoc Networks [1]. The authors Zhou and Z. J. Haas, proposed a distributed public key management service for asynchronous ad hoc networks, where the trust is distributed between a set of nodes by allowing the nodes share the system secret. The distributed certificate authority (DCA), illustrated in Figure (1) [1], consists of n server nodes which, as a whole, have a public/private key pair K/k. The public key K is known to all nodes in the network, whereas the private key k is divided into n shares (s_1, s_2, s_3, . . . , s_n), one for each server.

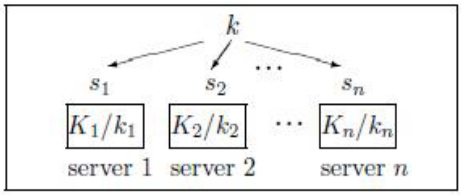

Figure (1): Key management service K/k configuration

The distributed certificate authority (DCA) signs a certificate by producing a threshold group signature as shown in Figure (2) [1]. Each node generates a partial signature using its private key share and submits the partial signature to a combiner C. The combiner can be any node and requires at least t + 1 shares to successfully reconstruct the digital signature.

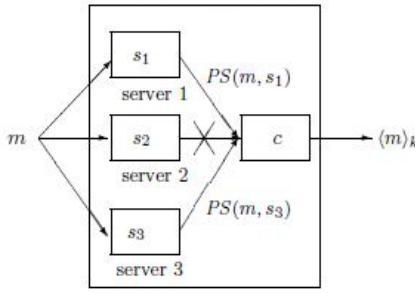

Figure (2): Threshold signature K/k generation

Fully Distributed Certificate Authority Approaches, this solution is first described by Luo and Lu in [2]. It uses a (k, n) threshold scheme to distribute an RSA certificate signing key to all nodes in the network. It

also uses verifiable and proactive secret sharing mechanisms to compromise the certificate signing key and protect against denial of service attacks.

This solution is aimed across planned, long-term ad hoc networks with nodes capable of public key encryption. However, since the service is distributed among all the nodes when they join the network, there is no need to choose or elect any specialized server nodes. Their solution also uses an (n, k) threshold signature scheme to form a distributed certificate authority (DCA). They enhance the availability feature of Practical PKI (public key infrastructure) for Ad Hoc Wireless Networks [3] by choosing n to be all the nodes in the network. The private key SK of the DCA is thus shared among all the nodes in the network and enables a node requiring the service of the DCA to contact any k one-hop neighbor nodes. In contrast to Practical PKI for Ad Hoc Wireless Networks no differentiation is made between server and client nodes with respect to certification services. The solution includes a share update mechanism to prevent more powerful attackers from compromising the certification service.

Implementing a fully distributed certificate authority in an Optimal Link State Routing (OLSR) MANET was proposed D. Dhillon, T. S. Randhawa, M. Wang, L. Lamont [4]. They present their approach to integrate a fully distributed CA in a proactive ad hoc routing protocol named OLSR. IETF's MANET working group has identified OLSR as one of the four base routing protocols for use in ad hoc networks. The other three are AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) and TBRPF (Topology Broadcast Based on Reverse-Path Forwarding) routing protocols. Their approach addresses the concerns of control traffic overload by tightly coupling the operations of a fully distributed CA at the network layer level. The existing OLSR specific packet types, identified in the IETF's draft proposal on OLSR, are used, as much as possible, to also support the proposed PKI. A real test-bed has been constructed in which the existing implementation of OLSRv4 [5] was utilized and a fully distributed CA was introduced. This is to their knowledge the first attempt to address the security issues of OLSR. The paper thus provides valuable insight by detailing the implementation and evaluation of the proposed approach.

3. Preliminaries

As we mentioned earlier, our approach is based on a polynomial over elliptic curve for Mobile Ad Hoc Networks, so, in this section we will review some preliminary concerning these technique Elliptic Curve Cryptography (ECC) [6]. An elliptic curve E over a finite field F_q consists of all the points consists of all the points $(x; y) \in F_q \times F_q$

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6;$$

With $a_i \in F_q$, whose discriminate is non null, along with the point at infinity. There is a point addition operation whose neutral element is the point at infinity. This set of points under this operation is an Abelian group.

Therefore, a point $Q \in E$ (F_q) can be multiplied by a scalar:

$$eQ = \underbrace{Q + \ldots + Q}_{e \text{ times}} = P$$

The inverse problem (i.e., given P and Q, find an e such that P = eQ), called the Elliptic Curve Discrete Logarithm Problem (ECDLP), appears to be computationally hard to solve. There are several cryptosystems, whose security is based on the intractability of the ECDLP problem. The main concern of the ECDLP, compared to the ordinary DLP for multiplicative groups, is that there are sub-exponential algorithms such as the index calculus to solve the DLP on multiplicative groups, but they cannot be used to solve the ECDLP. Hence, it turns to be a harder problem. Under a practical point of view, it appears that shorter keys can be used in the ECDLP while offering the same security as DLP.

4. Distributed certificate authority based on polynomial over elliptic curve

We consider an ad hoc wireless network with m mobile nodes. Nodes communicate with each other with the bandwidth constrained, and insecure channel. The m nodes may be dynamically changing as mobile nodes join, leave, or fail over time. Besides, m is not constrained; there may be a large number of networking nodes. The network provides neither logical infrastructure support nor physical [7], [8]. We have the following assumptions. (1) The public key PK for certificate verification is well known to each node in the network (2) Communication between multi-hop communications is considered less reliable compared with one-hop neighboring nodes. (3) Every node has at least k one-hop valid neighboring nodes. (4) To identify

misbehaving nodes among its one-hop neighborhood, every node is equipped with some local detection mechanism.

Assume that there is a certification authority (CA) an m participant node in the mobile ad hoc network (MANET). CA will dispense a secret key to every participant node in the network, the secret key SK_{CA} can be resumed if and only if the number of participants is not less than t. The CA holds a pair of keys (PK_{CA}, SK_{CA}), PK_{CA} is the public key known by every one, Skis the private key with external confidentiality. IN our design we make extensive use of the polynomial secret sharing and fully distributed CA is based on an approaches described by Shamir[1] and Luo and Lu [2] respectively, and we implement our fully distributed over elliptic curve.

A secret, specifically the exponent of the certificate-signing key SK_{CA}, is shared among all nodes in the network according to a random polynomial of order t-1. A coalition of t nodes with t polynomial shares can potentially recover SK by Lagrange interpolation, while any coalition up to t-1 nodes yields any information about SK_{CA}.

4.1. *Initialization of proposed scheme:*

In this scheme we choose a secure elliptic curve E(F_q) over the finite fields F_q (q is a prime number) :-

$$y^2 = x^3 + ax + b \qquad q > 3$$

Which a,b$\in F_q$ and satisfy the equation $4a^3 - 27b^2 \neq 0$.

G is a point over the elliptic curve, with a big prime number order n whose binary-length is at least 160 bits. CA will choose a r-power polynomial g(x); Which could be decompounded as follows:-

$$(g(x)) = g_1(x)\, g_2(x) \ldots\ldots g_k(x)$$

$g_i(x)$ is r_i-power polynomial which could not be decompounded, the number of polynomials which prime with g(x) over F_q is :-

$$\phi_n(g(x)) = n^r \prod_{i=1}^{k} \left(1 - \frac{1}{n^{ri}}\right)$$

We change the coordinates of G, G is appoint on elliptic curve whose order is large value n, to polynomial formal:- $G = \langle h(x), h'(x) \rangle_{g(x)}$; $G = \langle h(x), h'(x) \rangle_{g(x)}$ means both polynomials h(x), $h'(x)$will modulo the polynomial g(x). H (x) is a one-way hash function without collision. The coalition of nodes whose response of CA publishes the public parameters (E, G, g(x), $\phi_n(g(x))$, H (x)).

4.2 *A fully distributed CA by using polynomial over elliptic curve*

In our proposed fully distributed CA is passed on an approach described by Lau and Lu in Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks [2]. We apply the CA in mobile ad hoc network over elliptic curve cryptography (ECC) key pair with public key PK_{CA}, private key SK_{CA}, and modulus g(x). First the dealer initialized t nodes and then these t nodes initialized the rest of the network, in the fully distributed, SK_{CA} is distributed by using Shamir's secret sharing method by embedded SK_{CA} as the root of polynomial over the Elliptic Curve E(F_q), the dealer randomly chooses a point r and at-t power polynomial over the elliptic curve E(F_q), and also the dealer determine the domain parameters T = (p, a, b, G, n, h), which do not be kept secret.

$$F(x) = a_\circ + a_1 x^1 + a_2 x^2 + \ldots\ldots\ldots + a_{t-1} x^{t-1}$$

Where $a_\circ = SK_{CA}$, $a_k \in [1, \phi_n(g(x))]$, (k = 0, 1, 2, …..,t-1) , $f(0) = SK_{CA}$

Each shareholder node with a unique non-zero identity receives a share $s_i = f(i) \bmod g(x)$, where i = 1,2, ….,m . With knowledge of at least t shares the polynomial can be evaluate by calculating:-

$$F(x) = \sum_{i=1}^{t} s_i . l_i \ (x) \bmod n$$

Where l_i (x) is the Lagrange coefficient defines as

$$l_i(x) = \prod_{i=1, j\neq i}^{t} \frac{x-i}{i-j}$$

f(x) s kept secret, and then the dealer do the following work:

Order r $p_i = (x_i, y_i) \bmod n$

Compute $y_i = f(x_i) \bmod n$ (i= 1, 2… m)

R= r G mod n

For CA the dealer or coalition nodes in the

network publishes the point R and the parameters y_i, in order to check the validity of the secret sharing of the secret key (SK), CA will compute and publish the parameters $H_i = H(r\, p_i)$, (i= 1, 2… m)

Participant nodes have two proceeding to do here, the first, each node in the network selects private key P_{riv} over the elliptic curve and after that computes the public key $P_{Ki} = P_{riv} \times G \bmod p$, P_{Ki} is a public key of node I for encryption and verification, P_{riv} is a private key of decryption and signing. The nodes uses this keys for encryption and decryption the data packets. A challenge and response protocol can be followed to prove the knowledge of the private key P_{riv} and a certificate proves the association. The second, the participant nodes in the network compute

$p_i = s_i G = \langle h(x), h'(x) \rangle_{g(x)}$, i = 1,2, ….,m, this parameter use for verification for the partial certificate when the node i sign his certificate by s_i.

A. *Self-Initialization*

Secure wireless networks used in our targeted applications are comprised of mobile nodes that may result in nodes joins and leave the network. As we said previously, the dealer initialized k nodes and then these k nodes initialized the rest of the network; when a new node enters the network and does not have access to a dealer, an alternative method is necessary for this node to join the coalition of nodes able to provide secret shares. This alternative method is necessary to securely provide the node, the ability to generate dynamically new secret shares that are compatible with other coalition nodes already in the network. Luo and Lu [2] propose a distributed self initialization algorithm to address this problem. In particular, they use a coalition of members already in the network. The coalition communicates interactively to generate partial-secret shares that can be combined to generate the secret share for the new node.

Every node starts to broadcast the certificate request (Creq) to every neighbour in the radio range, which will re-broadcast the message until it reaches the destination. So, intermediate nodes are used to deliver the message if the destination node is not in the range as shown in the figure 3.

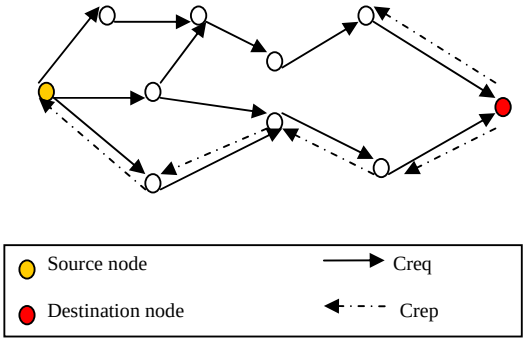

Figure 3: the diagram for distributed scheme

The generation of a secret share for a new node that joins the network is constructed by a coalition SK, of t nodes currently in the network. When a new node wants to join to the network, a new node broadcasts an initialization request to the neighbors nodes and when the all coalition receive this request they generate the parameter $p_{i+1} = s_{i+1} G \pmod n$ which is encrypted by the public key of the new node. Also they compute two parameters $r\, p_{i+1}, y_{i+1}$ and opened y_{i+1}:

$$r\, p_{i+1} = (x_{i+1}, y_{i+1}) \bmod n$$

$$y_{i+1} = f(x_{i+1}) \bmod n$$

Each participant communicates privately with every node in S by exchanging secret information. Each node $j \in SK$, subsequently returns a shuffled version of its secret share s_i to the new node. A shuffled version is used to protect the value of its secret share s_i

$$s_i^{'} \leftarrow shuffle(s_i, Sk)$$

The value s_i depends on its interaction with the other participants in SK and the current size of the network. Once the new node has obtained the shuffled shares it may construct its secret share s_{n+1} by,

$$s_{t+1} \leftarrow unsuffle_{k,t}(s_i^{'}, ..., s_k^{'})$$

B. *Certificate Renewal*

Since certificates are only valid for a limited time they need to be renewed before they expire. When a node p has to renew its certificate, cert requests a certificate renewal from a coalition of k neighbor nodes. Each node in this coalition checks that the old certificate

has not already expired and that it has not been revoked. If it has been revoked, then the nodes ignore the request, otherwise the request is granted; each of these k server nodes generates a partial certificate with a new expiration date and returns it to node p. Node p then combines the k partial certificates to obtain its updated certificate cert-updated. If any of the nodes are compromised they may generate an invalid partial certificate, which they then send to the combiner. The certificate produced by the combiner will then also be invalid. The node will need to update its certificate with the new public key. If the node changes its private and public keys, this is accomplished in a similar way as the renewal of the certificate.

C. *Certificate Revocation*

Users can revoke any issued certificate to other users in the instance of suspicion in the public key/identity binding. Similarly, users can also revoke their own certificate if they know that their private key has been compromised. The certificate revocation mechanism is based on the assumption that all nodes monitor the behavior of their one-hop neighbors and maintain their own certificate revocation lists. If a node discovers that one of its neighbors is misbehaving, it adds its certificate to the CRL (certificate revocation list) and broadcast an accusation against the node to the neighbor nodes. Any node receiving this broadcast accusation first checks its CRL to verify that the accusation did not originate from a node whose certificate has been revoked. If the accuser certificate has been revoked the accusation is ignored. Otherwise, the accusation originated from a valid node, the accused node is accepted and the changes are made to the CRL.

4.2 *Comparison between our scheme and another distributed system.*

We compare our scheme with two methods: first one - self organized public key management; one of the certificate-based authentication methods proposed by Capkun, Buttyan and Hubaux is by formation of certificate graphs [9]. The suggested approach is similar to PGP certificates [10], apart from the fact that in PGP a central certificate server is used. A certificate graph is defined as a directed graph G (V, E) where V and E stand for the set of vertices and the set of edges, respectively. The vertices of the certificate graph represent public keys, and the edges represent certificates. The second method: an enhanced distributed certificate authority scheme for authentication in mobile ad-hoc networks [11]; the proposed scheme uses Shamir's secret sharing scheme along with a redundancy technique to support certificate renewal and revocation. The malicious nodes are detected by the trusting mechanism by monitoring the behavior hop by hop. By simulation results, we show that the proposed scheme achieves more packet delivery ratio while attaining less delay and overhead, compared with the previous existing scheme. Their scheme is contributed with three components, monitoring routing cum forwarding (RCF) behavior, certificate revival and certificate revocation (see table 1).

It is obvious from this table that our scheme is the most secure and authenticated because if we use the same key length it is very hard for any attacker to discover the key because it depends on the discrete algorithm problem for elliptic curves (ECDLP), so the key in our scheme is more efficient and more secure.

5. Security Analysis

The CA for this solution requires an organizational/administrative infrastructure to provide the registration and initialization services. The main benefits of this scheme are its availability and that its polynomial over the elliptic curve.

The security of our scheme depends on the Intractability of Elliptic Curve Discrete Logarithm Problem (ECDLP). Consider the equation $Q = k\,p$ where $Q, p \in E(F_q)$, and $k < p$ it is relatively easy to calculate Q given k and p, but it is relatively hard to determine k given Q and p. This is called the discrete algorithm problem for elliptic curves (ECDLP). This technique makes the certificate authority more robust against some kinds of attacks.

The security of ECC depends on how difficult it is to determine k given $k\,p$ and p. This is referred to the elliptic curve logarithm problem, if we make a comparison between the RSA and ECC algorithms by comparable key sizes in terms of computational effort for cryptanalysis. Considerably smaller key size can be used for ECC compared to RSA. Thus, there is a computational advantage to using ECC with a shorter key length than a comparably secure RSA.

Since all nodes are part of the CA service, it is adequate that a requesting node has t one-hop neighbors for the CA service to be available. The amount of network wide traffic is also limited.

The cost of achieving this availability is a set of rather complex maintenance protocols, e.g. the share initialization and the share update protocols. A larger number of shares are also displayed to compromise since each node has its own share as compared to only

the specialized server nodes in the partially distributed solution. The parameter *t* therefore may need to be chosen larger since an attacker may be able to compromise a larger number of shares between each share update. This in turn affects the availability of the service. The solution must also provide a synchronization mechanism in the case of network segmentations.

Conclusion

In our scheme we proposed a fully distributed certificate authority based on polynomial over elliptic curve, and based on trust graphs and threshold cryptography, this scheme provides a robust and more secure distributed CA over the MANET, which though has better cryptography in nature. The security is based on the elliptic curve discrete logarithm problem.

□

Table 1: Comparison of Certificate-distribution systems

Requirements	*Self Organized Public Key Management - Capkun*	*An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Ad-hoc Networks*	*Our proposal*
(1) Resource awareness	Each node maintains two certificate repositories, which incurs a high overhead.	The generation and distribution of keys using complex polynomial functions based on finite field.	The generation and distribution of keys using complex polynomial functions over elliptic curve.
(2) a. Creation	Self–signed certificates, and hence more robust than a shared key based mechanism	Requires at least k neighbors, The certificate comprises of 3 basic fields: Node ID (NID), Initiation Time (IT) and Expiry Time (ET).	Requires at least k neighbors which might be a bottleneck
(2) b. Revocation	Explicit revocation causes delay between far-away nodes in the network.	System Trust Counter Table (NTT), stored at each node and hence memory intensive.	System CRL table stored at each node and hence memory intensive.
(3) Security and the key	Same long key normal security	Same long key normal security	Same long key more security

References

1. L. Zhou and Z. J. Haas, *Securing Ad Hoc Networks. IEEE Networks*, Volume 13, Issue 6 1999.

2. H. Luo and S. Lu, *.Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks.*, Technical Report200030, UCLA Computer Science Department 2000[5] J-P. Hubaux, L. Buttyán and S. Capkun.

3. S. Yi and R. Kravets, "*Practical PKI for Ad Hoc Wireless Networks*," Department of Computer Science, University of Illinois, Technical Report UIUCDCS-R-2002-2273, UILU-ENG-2002-1717, August 2001.

4. D. Dhillon,T. S. Randhawa, M. Wang, L. Lamont, *Implementing a Fully Distributed Certificate Authority in an OLSR MANET*, wireless communication and networking conference, 2004. WCNC. 2004 IEEE.

5. L. Christensen and G. Hansen, "*OLSR Routing Protoco*l", http://hipercom.inria.fr/olsr/, September 2003.

6. V. S. Miller, "*Use of Elliptic Curves in Cryptography*", Proc. CRYPTO'85, Springer-Verlag, New York, pp. 417-426, 1986.

7. Y. Dong, A.-F. Sui, S. Yiu, V. O. Li, and L. C. Hui. *Providing distributed certificate authority service in cluster-based mobile ad hoc networks.* Elsevier, Computer Communications, May 2007.

8. Yuan Yangtao, Liu Quan, Li Fen, *A Design of Certificate Authority Based on Elliptic Curve Cryptography*, 2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.

9. S. Capkun, L. Buttyan and J-P Hubaux. "*Self-Organized Public-Key Management for Mobile Ad Hoc Networks* ", *IEEE Transactions on Mobile Computing, Vol. 2, No. 1*, Jan-Mar 2003, pp. 52-64.

10. P. Zimmerman. The Official PGP Users guide, MIT Press, 1995, ISBN 0-262-74017-6.

11. Rajaram Ayyasamy1 and Palaniswami Subramani. "*An Enhanced Distributed Certificate Authority Scheme* for Authentication in Mobile Ad-hoc Networks", The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.