# Certificate Path Discovery by Constructing Virtual Hierarchy to Administer Trust Relationship using Peer to Peer PKI in MANETs

Sushma Nayak and Ramakrishna M

*Abstract*—**Due to unreliable wireless media and lack of infrastructure in MANETs, providing certificate path is a big challenge and also faces a big security problem [1]. MANETs are dynamic Peer-to-Peer PKIs and certification path can be built in case any part of the infrastructure that is temporarily not reachable. Hence efficient path discovery is very important. Path discovery is difficult since trust relationship is bidirectional. Certification paths are easy to find in case of hierarchical PKI since there is only one path among two entities. To obtain resilience and efficient path discovery among Peer- to –Peer trusted PKI' s for issuing entities we use a tool to address these problems by overlying a virtual hierarchical architecture. Since it is executed for short time in a dynamic atmosphere this is suitable in case of MANETs. Proposed technique to establish a virtual hierarchy in a Peer-to-Peer PKI, based on the trustworthiness of the participating neighbors. The upward approach is used to build the hierarchical structure i.e. from the leaves to the root. The main importance is given for the multi-rooted approach in case of building a hierarchy, depending upon the possibility. In addition the protocol does not require to issue new certificates among PKI entities, facilitates the certification path discovery process and the maximum path length can be adapted to the characteristics of the users with limited processing and Storage capacity.**

*Index Terms*—**PKI, MANET, peer-to-peer trust model, hierarchical trust model, multi-rooted hierarchical trust model.**

## I. Introduction

A Mobile Ad-hoc Network (MANET) is a Peer-to-Peer network, with one of the self organized wireless network without any pre-existing infrastructure. Due to absence of backbone network such as Central administration system, stable connection and control over network principals and so on, there is a lack of fixed infrastructure. Security issues are drawn to a greater attention in case of MANET. All network functionalities are supported by mobile end systems which are expected to act co-operatively.

As considering the functionalities such as traffic routing and adaptation to highly dynamic state of network links. Such functionalities can be extended over any services such as security. Since mobile devices are capable of forming network at a fly all the fixed security infrastructure which is existing in case of wired network fails and hence demands for a dynamic security consideration, assuming the possibility of the nature of network.

In case of connectivity, it is not easy to maintain in ad-hoc networks which was assumed to be good in case of previous PKI solutions, hence maintaining connectivity is one of the main challenges as the infrastructure-less nature of ad-hoc networks which guarantees any kind of connectivity. One of the problems present in ad-hoc networks is increased physical vulnerability among the nodes themselves [2]. The possibility of compromising of nodes is higher in a hostile environment in wired network with any stationary host, but they can recover and store the sensitive information relying upon the infrastructure for detection of compromised nodes. But the ad-hoc node is deprived of such conveniences since there are no stable entities in the ad-hoc network.

PKI defined in [3] is as ―The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke public key certificates based on public key cryptography.

In online economy, PKI and Digital certificates are developing as one of the foundation to the new era of the emerging technology. Set of security services specialized in case of public- key cryptography and X.509 certificates through the protocols which supports strong authentication, encryption of data, digital certificates and access controlled functions in case of MANETs. For any client of the Public Key Infrastructure, the term principal is commonly used, whether be any human, client or any server [4]. The term principal is anything that needs to be authenticated by any other principal or to authenticate itself. Hence Public Key Certificates play an important role in authentication. Public Key Certificates have become an accepted method for securely binding the identity of an individual or device to a public key, in order to support Public Key Cryptographic operation such as digital signature verification and public key-based encryption. PKI is considered as one of the most effective and efficient tool in providing security for dynamic network. Since its increased popularity in MANETs, it is drawing a greater attention towards security issues [1].

Trust models provide a framework to create and manage trust relationships among the different entities of a Public Key Infrastructure (PKI). These trust relationships are verified through the certification path validation process, which involves: path discovery, signature verification and revocation status checking. When trust relationships are bidirectional, multiple paths can exist between two entities, which increase the runtime of the path discovery process. In addition, validation of long paths can be difficult, especially when storage and processing capacities of the verifier are

Manuscript received December 01, 2011; revised January 30, 2012.

The authors are with the Department of Information and Communication Technology, Manipal Institute Technology, Manipal, INDIA 576104 (e-mail: sushma.ait@gmail.com; ramakrishna.m@manipal.edu)).

limited.

PKI supports data integrity, confidentiality, strong authentication and non repudiation, wherein any users of a particular domain who is responsible cannot deny the charges [5]. Trusted Third Parties (TTP's) are used in case of PKI called as Certification Authorities (CAs) to digitally sign the certificates called Public Key Certificates (PKCs), describing that particular public key belongs to a particular Users. The certificate users can verify to confirm the validity and integrity of a certificate by checking the issuing CA's digital signatures in the certificate on demand. Since integrity is the one of the most important service for the certificates, as there should not be any alterations of the contents in the certificates by unauthorized means. The entity can build a chain of certificates known as Certificate paths as the certificates allow establishing different trust relationship among the entities, i.e. from its trusted CA to other entities and verify the validity of the certificates.

By decentralizing CA functionalities, single point of failure is overcome using distributing the functionality of a single CA to a set of nodes by secret sharing and threshold cryptography [6]. Later, management of multiple trusted relationships among the PKI entities that are taken into consideration, as the nodes are dynamic and bidirectional trust relationships are created among them. In order to reach to a target entity, discovering the path towards it becomes a very difficult task due to the multiple paths among different entities. Obtaining the required resources, storing and verifying the certificates has become tedious as in case of mobile nodes which has limited interoperability and capacities due to the complicated and complex mathematical calculation in public key algorithms, hence validation of long path is difficult.

The main purpose of this protocol is to find an efficient path discovery process which is offered in case of hierarchical PKIs, where the trust relationships are unidirectional and paths are easy to find.

## II. Background

Basic three configurations of the traditional PKI/Certificate architectures are (i) A Single CA model, (ii) A hierarchical model and (iii) A Peer-to-Peer model. Each of these have been defined and determined by fundamental attributes of PKI and number of CAs in the PKI where trust relationships between CA's and multi- CA's PKI plays a very important role among the users so as to place their trust in them.

A CA is considered as trustworthy if a certification domain has been defined in the organizational or geographical boundaries, hence all the domain of certification consider this authority as their trust anchor. A trust anchor is the CA verification key used by the client application as the starting point for all certification validation [7].

### A. Single CA Model

This is the most basic PKI architecture, and provides PKI services for all the users of the PKI. In this architecture all the users trusts this single CA itself [4]. Hence every certification path will begin with the CA's public key. This model is easy to deploy but to a certain extent due to sudden changes in the CA public key, since all the architecture must be reconfigured. Hence this model is not suitable for very large community of users.

### B. Hierarchical Model

This configuration, [5] all users trust the same root CA (RCA) i.e. all the users of a hierarchical PKI begin their certification paths with the RCA's public key. The root CA does not issue certificates to users but only issues certificates to subordinate CAs. If it is permitted by the certification policies, each subordinate CA may issue certificates to users or another level of subordinate CAs. In case of hierarchical PKI, trust relationships are unidirectional. Hierarchical PKI's are scalable. Certification paths are easy to develop since they are unidirectional and the longest path is equal to the depth of the tree less than one, since root CA's certificate is not considered as it is known by all the authorities. Moreover, it will be easy for the users to know the applications of the certificate implicitly which is based on the position of the CA.

The drawback of this model is the dependence on the single trust point. Compromise of the entire PKI is due to compromise of RCA's private key. Trust relationship and path discovery is difficult to achieve across companies or geographical boundaries due to top down approach, since user has to trust the root CA which has multiple path to reach the RCA due to vulnerable attack [1].If the user does not trust the root CA, then it should use upward approach through the 3 hierarchy for a trusted CA that has certified the public key of the CA in question [5].

### C. Multi-rooted Hierarchical Model

The end entity certificates are validated using the same approach as with any hierarchical PKI. The difference is that a certificate will be accepted if it can be verified back to any of the set of trusted roots. Popular web browsers use this approach, and are shipped with trusted CA lists containing dozens of CAs. While this approach simplifies the implementation of a limited form of certificate verification [8].A multi-rooted hierarchy overcomes many of the problems of a strict hierarchy listed above. It removes the problem of the Root CA being a single point of failure for the enterprise. It also simplifies certificate and key lifetime management, since the local CA's keys and certificates can be decoupled from that of the root. In general, therefore, the multi-rooted approach is to be preferred over the strict hierarchy for many situations. In our protocol, the root CA's will be cross-certified to avoid the MITM (Man In The Middle) attack.

### D. Peer-to-Peer Model

It is also known as mesh or cross-certificate architecture. Here, the user's trust anchor is its local CA and all the CAs can be trust points because they are autonomous [5]. Autonomy refers to the CA which is not a superior CA in a hierarchy. Peer-to-Peer cross-certification can be performed among different autonomous CAs. Thus, a pair of certificates describes their bidirectional trust relationship. Limitations of the trust in case of a CA will have to specify the limitations in the certificates issued to its peers. All certificates validation, by clients within an autonomous CA,

starts with the local CA's self-signed certificate. There is no single point of failure in case of Peer-to-peer PKI as it counts on different trust points, which can easily incorporate a new community of users and the management cost is high. They can have multiple paths between two users. From a set of isolated CAs a peer-to-peer PKI can easily be constructed, since users do not need to change their trust points. This model serves to represent the dynamic changes of the organizational structures or environments where communicating entities are not related hierarchically.

The number of trust relationships is directly proportional to the number of CAs (n), that is, the number of trust relationships is equal to n*(n - 1), which is a cause for scalability problems. In addition, this model requires larger certificates because the users must determine which applications a certificate may be used for based on the content of the certificates [1]. Thus, certificates have more extensions and the validation process is more complex. The maximum length of a certification path in a peer-to-peer PKI is the number of CAs in the infrastructure.

## III. Cross Certification

The term cross-certification refers to two operations [7]:

- The first operation, which is generally executed infrequently, is the establishment of a Trust relationship between two CAs through the signing of another CA's public key in a certificate referred to as a "cross-certificate".
- The second operation, executed frequently by the client application, involves verifying the trustworthiness of a user's certificate signed by a CA within your PKI network. The operation is often referred to as "walking a chain of trust". The "chain" refers to a list of cross-certificate validations that are "walked" (or traced) from the root CA key or ―trust anchor ‖ of the verifying user to the CA key required to validate the other user's certificate.

## IV. Simplifying the Certification Path Discovery by Establishing A Virtual Hierarchy

This protocol establishes a virtual hierarchy in a peer-to-peer PKI, based on the trustworthiness of the participating neighbors. The upward approach is used to build the hierarchical structure i.e. from the leaves to the root. This approach is easy for the certification path discovery and can be adapted to users with the limited capacities [9].

The main importance is given for multi-rooted approach in case of building a hierarchy i.e. only when such possibility arises. This can be shown in case of two phases which the protocol is divided so as to understand the better working of the protocol.

- Ordering the entities with respect to Trustworthiness: In this phase, the neighboring entities of the demanding neighbor are arranged from less trustworthy to the most trustworthy.
- Constructing the hierarchy: In this phase, considering the Peer- to-Peer entities where the order is considered, it establishes a Hierarchical trust relationship.

TABLE I: Notation in Protocol

| Notation | Meaning |
|---|---|
| Ei | Entity i |
| Li | Number of certificates from the leaves to entity i. |
| INi | Number of entities which Ei trusts (received certificates) |
| OUTi | Number of entities that trust Ei (issued certificates). |
| E0 | Current entity. |
| N0 | Number of participant neighbors of E0. |
| Order [N0+1] | Array that contains E0 and its participant neighbors ordered from the less trustworthy. |

### A. Ordering the Entities with Respect to Trustworthiness

In first phase each entity is put in order according to its neighbors, from less trustworthy to most trustworthy by determining which of its neighbors are less trustworthy and more trustworthy than itself i.e. by issuing a certificate to E0 or to entities that E0 issued a certificate to other participant neighbors. Based on its processing and storage capacity, E0 proposes a max certification path length (LMAX). Containing this value entity E0 sends a request message wherein whichever message is sent among the entities along the protocol must be authenticated by the receiver. Any of the neighbors can accept or reject to collaborate in establishment of virtual hierarchy, where in acceptance or rejection messages are sent to demanding entity.

Once entity E0 receives the responses from all its neighbors, it determines the number of entities that want to be part of the hierarchy and a certificate is issued to E0 i.e. (INi), and as the number of entities that want to participate in the hierarchy receives a certificate from E0 i.e. (OUT0) [1]. Then, E0 sends these values to its participant neighbors as an information message and these neighbors send to E0 with their own parameters INi and OUTi. Later, E0 compares OUT0 with the received OUTi values and puts them in order from the lowest to the highest. The entity with the lowest OUTi is the less trustworthy, that is, the neighbor that less the other participants trust. If there are two or more entities with the same OUTi, they are arranged in accordance with the INi value from the lowest to the highest too. After ordering in this manner if the most trustworthy neighbor i.e. nth neighbor and (n-1)th neighbors OUTi are same as well as their INi are same, then they both form a trusted anchor(Root nodes), where multi-rooted hierarchy comes into picture. Hence each entity put in order its neighbors, from the less trustworthy to the most trustworthy, determining which of its neighbors are less trustworthy and more trustworthy than itself. At the beginning of the protocol, Li = 0 for all the entities.

### B. Constructing the Hierarchy

In this second phase the order is set in case of first phase among the participant neighboring entities from the less trustworthy to the most trustworthy [1]. Therefore, the less trustworthy entity in the neighborhood acts first and the

other entities must wait for the intervention of their less trustworthy neighbors. Each entity chooses a superior CA among the participant neighbors that issued it a certificate (trusted neighbors). Thus, when an entity E0 acts, it looks for the most trustworthy entity of its trusted neighbors, based on the trustworthiness order established at the first phase of the protocol, and chooses this neighbor like superior CA. If L0 is higher than Li of the superior CA and (L0 + 1) is less than or equal to (LMAX - 1), Li of superior CA takes the value of (L0 + 1). In case that (L0 + 1) is higher than (LMAX - 1), the chosen superior CA is not appropriate and E0 must choose the next trusted neighbor like superior CA provided that this neighbor is more trustworthy than E0. E0 checks again if L0 is higher than Li of the new superior CA and so on until E0 finds a suitable superior CA. Nevertheless, it can be possible that none of the trusted neighbors that are more trustworthy than E0 can be used like superior CA. If there are entities which have same level of trustworthiness among multiple CAs, i.e. most trustworthy CAs then all the CAs (CAs having same level i.e. only most trust worthier) is considered as superior CAs. Thus, when E0 concludes this procedure, it sends an association message to its neighbors informing the identity of its superior CA or a failure message indicating that it was not possible to choose a superior CA.

## V. Conclusion

In this paper we describe our protocol which establishes a virtual hierarchy in Peer-to-Peer PKI based on the trustworthiness of the participating neighbors. Two parameters play a very important role in determining the level of trustworthiness i.e. INi (Number of received certificates) and OUTi (Number of issued certificates).Advantage of our protocol is the formation of the trust relationship among the existing relationship to establish the hierarchy and hence not necessary to issue new certificates or to adjust the trust points.

The upward approach is used to build the hierarchical structure i.e. from the leaves to the root. The main importance is given for the multi-rooted approach in case of building a hierarchy, depending upon the possibility. The entities in multi-rooted CA cross-certify among each other, in order to form trust among each other. In addition the protocol does not require to issue new certificates among PKI entities, facilitates the certification path discovery process and the maximum path length can be adapted to the characteristics of the users with limited processing and Storage capacity.

The effectiveness of the proposed technique has been analyzed theoretically; same is being implemented to obtain the efficient results in practical conditions.

## References


[1] Cristina Satizábal, Juan Hernández-Serrano, Jordi Forné and Josep Pegueroles ,Department of Telematics Engineering, Technical University of Catalonia, Jordi Girona 1-3 C3, 08034 Barcelona, Spain Department of Engineering and Architecture, Pamplona University, Km 1 via Bucaramanga, Pamplona, Colombia Received 25 July 2006; revised 17 December 2006; accepted 29 December 2006.

[2] S. Yi, R. Kravets, MOCA: Mobile certificate authority for wireless ad-hoc networks, Proceedings of 2nd Annual PKI Research Workshop (PKI03), 2003.

[3] Arsenault, A., Turner, S., Internet X.509 Public Key Infrastructure, draft-ietf-pkix-roadmap-06.txt, Internet Society, November 2000.

[4] R. Perlman, An overview of PKI trust models, IEEE Network 13 (1999) 38–43.

[5] C. Satizabal, R. Paez, and J. Forne. PKI Trust Relationships: From Hybrid Architecture to a Hierarchical Model. 2006.

[6] Y. Dong, H.W. Go, A.F. Sui, V.O.K. Li, L.C.K. Hui, S.M. Yiu, Providing distributed certificate authority service in mobile ad hoc networks, Proceedings of First International Conference on Security and Privacy for Emerging Areas in Communications Networks 2005 (SecureComm 2005) 2005, pp. 149–156.

[7] Jim Timbull, Cross-Certification and PKI Policy Networking, Entrust: Securing Digital Identities and Information.

[8] M. Cooper, Y. Dzambasow, P. Hesse, S.Joseph, R.Nicholas, Internet X.509 Public Key Infrastructure: Certification Path Building, RFC 4158.

[9] Y. Elley, A. Anderson, S. Hanna, S. Mullan, R. Perlman, S. Proctor, Building certification paths: Forward vs. reverse, Proceedings of Network and Distributed System Security Symposium (NDSS 2001), 2001.


**Sushma Nayak** received her degree in Electrical and Electronics Engineering from Visweswaraya Technological University, Belgaum (India) in 2006. She received M.Tech degree in 2010 from Manipal University, Manipal and currently she is working as an Assistant Professor in Moodlakatte Institute of Technology, Kundapura. Her research interest includes PKI and Network Security.

**Ramakrishna M**. received his degree in Computer Science and Engineering from Visweswaraya Technological University, Belgaum (India) in 2008. He received M.Tech degree in 2010 from Manipal University, Manipal and currently he is working as an Assistant Professor in Manipal Institute of Technology, Manipal. His research interest includes Routing, PKI and Network Security.