January 2012

An Improved Protocol for Proxy Based Certification Authority for MANETs

Bibhudendu Panda

Department of Computer Science and Engineering, NIT, Rourkela, India, bibhu_panda25@rediffmail.com

Pabitra Mohan Khilar

Department of Computer Science and Engineering, NIT, Rourkela, India, pmkhilar@nitrkl.ac.in

Follow this and additional works at: <https://www.interscience.in/ijssan>

Part of the [Digital Communications and Networking Commons](#), and the [Electrical and Computer Engineering Commons](#)

Recommended Citation

Panda, Bibhudendu and Khilar, Pabitra Mohan (2012) "An Improved Protocol for Proxy Based Certification Authority for MANETs," *International Journal of Smart Sensor and Adhoc Network*: Vol. 1 : Iss. 3 , Article 9. DOI: 10.47893/IJSSAN.2012.1058

Available at: <https://www.interscience.in/ijssan/vol1/iss3/9>

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Smart Sensor and Adhoc Network by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

An Improved Protocol for Proxy Based Certification Authority for MANETs

Bibhudendu Panda & Pabitra Mohan Khilar

Department of Computer Science and Engineering, NIT, Rourkela, India
E-mail : bibhu_panda25@rediffmail.com, pmkhilar@nitrrkl.ac.in

Abstract - This paper includes developing framework for proxy based certificate Authority for MANET. Key management is a central aspect for security in mobile ad hoc networks. In mobile ad hoc networks, the computational load and complexity for key management is strongly subject to restriction of the node's available resources and the dynamic nature of the topology. PKI has been recognized as one of the most effective tools for providing security for dynamic networks. However, providing such an infrastructure in MANETs is a challenging task due to their infrastructure-less nature. In this paper we have considered such challenges in detail, identify the requirements for such solutions, and propose a practical PKI service for MANETs. We used threshold cryptography to distribute the CA functionality. To reduce the overhead research work employs a proxy and a timer during multicasting to achieve certification service. Results from simulation establish the effectiveness and the efficiency of the approach.

Keywords- PKI,MANET,AODV,CA

I. INTRODUCTION

In the past few years, more attention has been drawn to the security of mobile ad hoc network (MANET)[1][2]. Due to its glorious success in securing Internet computing, the Internet de facto standard public key cryptography including encryption and digital signature becomes natural choice as a fundamental building block to secure MANET. However, since MANET is significantly different from the Internet, a salient issue is how to adopt the technology to the new environment. As we know, successful application of PKI relies on the ubiquitous capability of verifying the binding between a public key and the owner principal. In the internet, mainstream solution is to have a third party centrally trusted entity, called certificate Authority(CA); vouch for the authenticity of the binding by issuing digital certificates, which in essence is a statement of the binding digitally signed by the CA. In practice, CAs and digital certificates are organized and maintained by PKI.[3][4]. It is questionable yet if PKI can be implemented in MANET because PKI requires well protected CAs and constant connectivity between users and CAs. However, MANET is composed of a group of mobile devices communicating with each other through a wireless link without a backbone or infrastructure. In such an environment, all devices are exposed to hacking to the same extent and no device can be assumed to be significantly more secure than the others. Moreover, devices roam around, run out of

power or just stop functioning, which lead to volatile connectivity among them and CAs. Research proposals have been seen in[5][6][7] etc. , to address the two issues by distributing the CA's functionality across a set of network nodes and use threshold signature[8] to achieve tolerance up to the threshold number of faulty nodes. These methods are suitable for small MANETs with a single CA. This is partially due to inherent high communication cost. A more fundamental reason is that it is difficult if not feasible for a CA to get familiar with all other principals. Some researchers take another approach based on the concept of "web of trust" first appearing inPGP [9]. In these methods each principal is it's own CA[10][7] and keeps a certificate directory. To authenticate a certificate signed by another principal,a principal has to find a certificate path between them but this lead to difficulty of finding such a path without incurring a lot of broadcasting cost or forcing each principal to save a large number of certificates in it's local directory.

II. RELATED WORK

In [11], a secure and efficient key management framework(SEKM) for mobile ad hoc networks is proposed. SEKM builds PKI by applying a secret sharing scheme and an underlying multicast server group. In SEKM, the server group creates view of the certification authority(CA) and provides certificate update service for all nodes, including the server

themselves. A ticket scheme is introduced for efficient certificate service. In addition, an efficient server group updating scheme is proposed.

In [12], a locality driven key management architecture that achieves robust key authentication and facilitates timely and efficient establishment of distributed trust is proposed. The architecture reflects application oriented view of MANET and is based on threshold cryptography to achieve high fault tolerance against network partition and malicious nodes. On top of it, distributed trust protocols are designed to help set up trust relations on the fly. In [13], a practical PKI service for ad hoc networks is proposed. Threshold cryptography is employed to distribute the CA functionality over specially selected nodes based on the security and the physical characteristics of nodes. The selected nodes that collectively provide PKI functionality are called MOCAs, an efficient and effective communication protocol for correspondence with MOCAs for certification services is presented.

Pathak et al proposed in [14] a voting based scheme for both public key authentication and group membership control. In this method, the decision of trust is made collectively by a group of n principals via voting. The system achieves high fault tolerance when it satisfies Byzantine condition. Compared to the above threshold based CA solutions, the method does not require a shared trusted principal (the dealer) and therefore does not have any single point of failure. However, the group [18] does not own a single signing key. Consequently each individual principal has to know all public keys of the n voters and perform n signature verifications to authenticate one public key. In section II we have discussed various proposed scheme for proxy based authentication. In section III proposed proxy based certificate authority scheme has been discussed. In section IV cost and effectiveness of our proposed scheme through simulation we have shown and finally we have concluded with future work in section V.

III. PROXY BASE CERTIFICATE AUTHORITY FOR MANETS

In this part of the research, Proxy Based Certificate Authority (PBCA) is proposed. In this frame work, all the N nodes in the network provide CA (Certificate Authority). Using threshold cryptography, any r nodes can reconstruct the full CA key. Threshold cryptography is an application of secret sharing that was first proposed by Shamir [15]. The basic idea of secret sharing is that it is mathematically possible to divide up a secret to n pieces in such way that anybody who requires the full secret can collect any k piece out of those n to reconstruct the full secret. k becomes the threshold needed to reconstruct the secret. Threshold cryptography

applies this technique to the keys for cryptographic operations. Frankel and Desmedt [16] proposed to use secret sharing for the private key of public key cryptography and Shoup proposed a way to generate a digital signature from key pieces without reconstructing the full key at any point.

In the Fig 1.1, we assume that there are 6 nodes, a proxy node in the network. A new node is joining in the network and sending a request to proxy, in turn multicast the request to all the other nodes in network. Let us assume that the minimum number of nodes need to reply be 2.

Figure 1.1: New Node sending request to proxy and proxy multicast to other nodes in the network

In Fig 1.2, it can be observed that proxy receives reply with their corresponding key share from only 3 nodes in network. As the threshold condition is satisfied, the proxy reconstructs the full signature and sends to the new node.

Any client requiring a certificate service must contact all the nodes in network with its request. This request is sent to the nodes in the network via a proxy node. So, a new client unicast the request message to the proxy and then the request message is multicast then the timer is specified which indicates that the node need to reply within the time limit or else need no reply. When the timer expires, the nodes need not reply. This technique reduces the overhead cost. The nodes which send reply will generate a partial signature over the received data. The client needs to collect at least r such partial signatures to reconstruct the full signature and successfully receive the certificate service. The reconstruction of the full signature is done by proxy node and is sent to the client. This process reduces the cost without implementing in every new client.

Maintaining information on revoked certificates is one of the key tasks of the CA and this topic has got much of the attention in recent years [17]. In our

approach, the certificate can be revoked only upon the agreement of minimum r nodes in the network. So, when r nodes come to an agreement to revoke the certificate, each node generates the revocation certificate with its partial key. This revoke certificate is then sent to the proxy node. This proxy upon receiving r revoke certificates, it reconstructs the full revocation certificate. This avoids false revocation. The threshold value r must be chosen carefully, such

Figure 1.2: New nodes receiving request from proxy and proxy receiving reply from some of the nodes in the network

that overhead does not increase or decrease security. In this protocol, the chance of not receiving the reply from the nodes and possibility of failure in reconstructing the full signature is very less because the request message is sent to all the nodes in the network unlike the MOCA.

The request and reply message are similar to the Route Request (RREQ) and Route Reply (RREP) message in on-demand ad hoc routing protocol like AODV and DSR. The management of routing information is also similar to these protocols. As a request packet passes through a node, the reverse path to the sender is established. If no reply is returned within the time-out period, the reverse path entry in the routing table expires and is purged. If a reply traverses back through the previously setup reverse path to the sender, the routing table entries are refreshed and the bidirectional path remains in the routing table for potential reuse. This similarity to on-demand routing presents a potential for our certification protocol and the existing on-demand routing protocols to benefit from each other by sharing routing information. In our protocol, there is requirement of unicast-based optimization as the request is sent to all the nodes in the network. When any client leaves the network, then the proxy sends a request message to revoke the existing

certification and to build the new certificate. Then the nodes reply back with revoke certificate with their key share. The nodes include the key share also in the revoke certificate. When proxy receives minimum of r replies from the nodes, the certificate is revoked and new certificate is generated and the respective key shares are multicast to all the nodes in the network.

IV. RESULTS

The focus of our evaluation of the PBCA framework is effectiveness and efficiency (or cost). Effectiveness is measured using the success ratio of certification requests.

$$\text{Success ratio} = \frac{\text{number of successful certification request}}{\text{Number of total certification request}}$$

The cost of a certification protocol can be evaluated using the two metrics.

1. Packet overhead
2. Additional communication delay caused by the certification process.

Certification delay: The most frequent use of a certification service is to acquire the communicating peer's public key certificate. The delay to get the certification service is added to the start up latency of any secure communication relying on PKI

Figure 1.3: The distribution of arrival times of CREP packets.

It can be observed that the no of replies received is more with the proposed protocol when compared to MOCA. This is because the request is sent to all the nodes in the network but not only to selected nodes. The limitation might be the slight overhead in multicasting. The comparison of MOCA and PBCA in terms of success ratio is shown in Fig 1.4. The success ratio is more in PBCA.

Fig 1.4: Success ratio of MOCA with respect to PBCA

The minimum no of replies is considered as 20% of the total requests. Success ratio depends on the minimum of replies required to reconstruct the full certificate.

Fig 1.5: Comparison of Success ratio with varying r for PBCA

When we vary the minimum number of required replies r , the success ratio varies. When r is increased then success ratio decreases and vice versa. This variation is shown in Fig 1.6 for PBCA.

V.CONCLUSIONS

In this paper we have introduced a key management framework for ad hoc wireless network and proposed proxy based certificate authority protocol. The PKI framework has many problems to be implemented in ad hoc networks. These problems are resolved using the proposed framework. The need of unicast-based optimization is eliminated. The overhead of the system is reduced by using a proxy node and the timer to receive the replies from the nodes with their key share. Once the timer is expired, it is implied to the nodes no more replies are accepted. If any node replies, it becomes an invalid data. Efficient and effective communication protocols are developed which are

similar to AODV and DSR. These communication protocols give the reserved reversible path for destination to the sender. The simulation results obtained in this paper establishes that the proposed protocol is better when compared to the legacy system. Developing PKI infrastructure solutions for MANETs is not easy and this paper made an attempt to study the issues of PKI and proposed a method based on proxy certificate with permissible delay. However, extending this solution to other networks would be an interesting problem of research. Also, studying about faulty nodes vs proxy certificates would be another future work. The proposed model can be implemented using Elliptic Curve Cryptography (ECC) to minimize the mobile node's resource utilization.

VI. REFERENCES

- [1] C.E. Perkins, E. Royer, and S.R D," AODV routing", In 2nd IEEE workshop on mobile Computing Systems and Application (WMCSA'99), 1999.
- [2] Y.C Hu, A Perig, and D.B Johnson Ariadne, " a secure on demand routing protocol for ad hoc networks", in the proceedings of the 8th annual ACM/IEEE International conference on mobile computing and Networking (Mobicom) 2002.
- [3] S.Berkovits, S. Chokhani, J furlong, J.geiter, and J.Guild, public key infrastructure study final report. MITRE report, 1994.
- [4] K.Drira, H.Sebe, H.Kheddouci, "ECGK: An efficient clustering scheme for group key management in MANETs", computer communication 33(2010) 1094-1107.
- [5] L. Zhou and Z.J Haas, " securing ad hoc networks", In IEEE networks, volume 13(6).1999.
- [6] J.kong, P. Zerfos, H.Luo, S.Lu, and L.Zhang," providing robust and ubiquitous security support for mobile ad hoc networks", in proceedings of ICNP '01.
- [7] S. Yi and R Kravets.Moca: ," Mobile Certificate Authority for wireless adhoc networks", in the proceeding of the 10th IEEE International Conference on Networks protocols (ICNP'02), 2002.
- [8] V. Shoup. Practical threshold signatures, theory and Application of Cryptographic Techniques 2000.
- [9] P.Zimmermann, The official PGP user's guide, MIT Press,1995.

- [10] T.Aura and S.M"aki", " Towards a survivable security architecture for ad hoc networks. In Security protocols", 9th International workshop, Cambridge,UK, april 2001, Volume 2467 of Lecture notes in computer science. Springer-verlag, Berlin. Springer- verlag Berlin Heidelberg 2002.
- [11] Capkun, S., Hubaux, J., and Buttyan, I.2006. " mobility helps peer-to-peer security". IEEE Trans. Mobile Comput. 5, 1, 43-51..
- [12] Hao yang, HaiyunLuo, fan Ye, Songwu Lu, and Lixia Zhang, " security in mobile Ad hoc networks- Challenges and solutions, " IEEE Transactions on wireless communications , Vol 11, no.1, pp. 38-47, 2004.
- [13] S. Yi and R Kravets.Moca: ," Mobile Certificate Authority for wireless adhoc networks" , in the proceeding of the 2nd annual PKI research workshop(PKI'03),2003.
- [14] V.Pathak and L. Iftode, "Byzantine fault tolerant authentication ", technical report, Dept of Computer science, Rutgers University , 2003
- [15] A.Shamir," How to share a secret", Communication of the ACM, 1979.
- [16] Y.Frankel and Y.G desmedt," parallel Reliable Threshold Multisignature" technical report Tr 94-04-02, University of Wisconsin Theory . IT-28:714-720.
- [17] The Network Simulator- NS-2. Available at <http://www.isi.edu/nsnam/ns/>
- [18] A.Renuka, and K.C Shet, " Cluster based Group key Management in Mobile Ad hoc Networks," IJCSNS International journal of Computer Science and Networks, Vol . 9, no. , pp., 42-49,2009.