International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 7, July 2014 ISSN 2319 - 4847

Self-Organized key management based on fidelity relationship list and dynamic path

Himadri Nath Saha[1], Dr. Debika Bhattacharyya[2], Sulagna Mukherjee[3*], Bipasha Banerjee[4], Rohit Singh[5] and Debopam Ghosh[6]

[1] Institute of Engg & Management, Department of Computer Science,
Y-12, Block -EP, Sector-V, Salt Lake Electronics Complex
Kolkata - 700 091, West Bengal, India

[2]Institute of Engg & Management, Department of Computer Science,
Y-12, Block -EP, Sector-V, Salt Lake Electronics Complex
Kolkata - 700 091, West Bengal, India

[3*]Institute of Engg & Management, Department of Computer Science,
Y-12, Block -EP, Sector-V, Salt Lake Electronics Complex
Kolkata - 700 091, West Bengal, India.
Corresponding author.

[4]Institute of Engg & Management, Department of Computer Science,
Y-12, Block -EP, Sector-V, Salt Lake Electronics Complex
Kolkata - 700 091, West Bengal, India

[5]Institute of Engg & Management, Department of Computer Science,
Y-12, Block -EP, Sector-V, Salt Lake Electronics Complex
Kolkata - 700 091, West Bengal, India

[6]Institute of Engg & Management, Department of Computer Science,
Y-12, Block -EP, Sector-V, Salt Lake Electronics Complex
Kolkata - 700 091, West Bengal, India

Abstract

MANET or mobile ad hoc network, unlike the conventional networks does not allow trusted centralized servers or authorities. Hence, self-organized key management technique is used to provide certification for the various nodes in the network. There are several self-organized key management protocols but most of them take up huge time and space to collect and maintain the certificates. We propose an effective self-organized key management system which takes up much lesser space to store the collected certificates. We use a fidelity relationship list based on which certificates are collected by source node for a path(selected previously on basis of a fidelity parameter in the network).

Keywords – certification, fidelity, fidelity relationship list, MANET, Self-organizing key management.

1. Introduction

Mobile ad hoc networks (MANETs) are autonomous collection of mobile nodes which communicate over relatively bandwidth constrained wireless links. A mobile ad hoc network, by definition [3][6] does not rely on any fixed infrastructure instead the nodes perform the networking functions by themselves in a self-organizing manner.

There are 2 ways of introducing security keys in a MANET system:

1) By a centralized single authority domain
2) By full self-organization (Without any central authority)

The main problem of any public-key based security system is to make each user's public key available to others in such a way that its authenticity is verifiable. In mobile ad hoc networks, this problem becomes even more difficult to solve because of the absence of centralized services and possible network partitions. The best known approach to the public-key management problem is based on public key certificates [4]. A public-key certificate is a data structure in which a public key is bound to an identity (and possibly to some other attributes) by the digital signature of the issuer of the certificate. Public key Infrastructure is not fully flexible because of difficulty in introduction, high cost, and necessity of network environment enabling connection between each user and CA (Certificate Authority). Hence, in our system, like in PGP [5], users' public and private keys are created by the users themselves. We use a modified web of trust[2] approach such that less frequent communications and lesser memory are used. All the other node's public key certificates are not stored by all nodes. Instead only a fidelity relationship list is maintained by each node and a model similar to that in [1] is followed thereafter.

THE PROPOSED METHOD

When a probable and trusted path has been established between a source node S and a target node T, it is assumed that every node in the path has been selected based on some fidelity factor. Certification request is generated for verification of each node along the path before data can be securely transferred. Each node generates a pair of secret and public keys. If a node (*A*) trusts other node (*B*) by its own means, *A* gives digital signature for B's public key certificate using *A*'s own secret key and issues the certificate for *B*'s public key. Each node manages only those certificates that were generated for its own public key.

2.1 Building the Fidelity Relationship List

In a probable path from source S to target T, S gives certificate for its next hop neighbor node N's public key and N certifies its next node and so on till the target node T is reached. Once a node verifies another node, it unicasts the fidelity information, i.e. the addresses of the verified and verifier nodes, to the source. Each node in the path of the unicast adds the information onto their fidelity relationship list. This procedure is repeated till the list completed for the path, i.e. the node T is added as verified node. The fidelity relationship list is checked for each transmission. If the path required for the transmission is present in the fidelity list, it sends the data along the verified path. If the source is changed or node next to the source is changed, the entire list is deleted, and the message is broadcasted to all the nodes of the path (they delete their fidelity list entries) and new certification request phase starts. If a part of the previously verified path is unchanged till a node, say N, the certification procedure starts from N onwards till the destination is verified. The fidelity list is updated accordingly by deleting the entries which are no longer required and inserting newly created (verifier, verified) tuples.

3. CERTIFICATE REVOCATION

Each user can revoke a certificate she issued if she believes that the user key binding expressed in that certificate is no longer valid. Moreover, if a user believes that her own private key is compromised, she can revoke its corresponding public key. There are cases where certificate must be revoked even though it is in valid duration because of secret key leakage and other reasons. If user notices her secret key leakage, she must distribute revocation information signed by her own secret key to the network. Users who receive the revocation information must delete all the tuples having that revoked user as its member from her list

4. AUTHENTICATION PROCEDURE

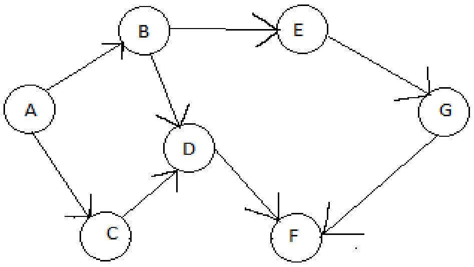

Figure 1: Fidelity Relationship Model

Table.1: Fidelity Relationship List

Fidelity Relationship Information
A→B
A→C
B→E
B→D
C→D
D→F
E→G
G→F

A source user consults its fidelity relationship list to check if a verifiable path can be found to the target node. For the path A-> C-> D-> F, A assumes it can directly trust node F. Just before real communication, A asks for the public key certificates of D and F and collects them. The certificates are verified as described in [1] and direct fidelity relationship is established between source and target users and data transfer begins.

5. COMPARISON WITH OTHER SIMILAR SELF-ORGANIZED KEY MANAGEMENT SCHEMES

Basic problem with the primary web of trust method is overhead. This method requires long time to collect all the certificates in the network, because repository must be exchanged among moving users periodically. Capkun [7] described that it takes approximately 10000 seconds for one node to collect all the repositories in case repositories are exchanged every 60 seconds for the ad hoc network which consists of 100 nodes and 600 certificates. The amount of communications at a time for exchanging repository periodically increases as the number of the certificates stored in repository increases. In order to manage all the certificates, large memory size is required. The validity of each certificate has to be checked periodically.The next modification of self-organized key management based on trust relationship list[1] took up a different approach of storing only the certificates certifying the public key of a node at that node. This helped reduce the overhead to a large extent. This method built up a web of trust in the network where certificate about a target node is collected on need basis. It maintains a trust relationship list at every node where the (verifier-> verified) pairs have their addresses stored. For our method, the key management is focused on only a selected path at time. The path is assumed to be built on basis of some fidelity factor (taking the battery, reliability of a node to transfer data, etc. together) and hence somewhat secure. This verification process gives them further security against spoofing[8] and other identity threats prevalent in MANET[9]. The fidelity relationship list cannot be stored longer than a paths longevity (the duration for which it actively transfers data) because the fidelity values for each node is a dynamic variable. It changes continuously based on the node’s performance. Hence, a set of trusting nodes with one certifying the other may not remain that way from the next time interval. So storing stale certificates for non-existent path is not an option. Also due to shorter lifetime, the periodic validity check is not necessary. Our method reduces the storage space needed from [1] because it considers only paths in the full network and not a larger sub network other than the path. For a path a smaller list is needed to store the necessary information and lesser number of certificates are collected.

6. CONCLUSION

In this paper we proposed a different approach of self-organized key management in ad hoc networks. It is proposed as a general method that will work well with algorithms which use a fidelity parameter to rank the behavior of the nodes involved in the network. It does not rely on any trusted authorities throughout its lifetime. The amount of memory used to store the fidelity relationship list is reduced since at a time only a single path is considered from the network. As we consider only the smallest possible part of the network for a limited period of time, it renders security to the communication involved. For future work, we will try and implement this proposal on a model in a network simulator and calculate numerically the actual amount of communication needed.

REFERENCES

[1.] Hideaki Kawabata, Yoshiko Sueda, Osamu Mizuno, Hiroaki Nishikawa And Hiroshi Ishii,” Self-Organized Key Management based on Trust Relationship List.”

[2.] Hisham Dahshan, James Irvine”Key Management in Web of Trust for Mobile Ad Hoc Networks”,*International* ***Conference on Advanced Information Networking and Applications***, 2009, IEEE Computer Society.

[3.] D.B. Johnson, “Routing in Ad Hoc Networks of Mobile Hosts,” *Proc. IEEE Workshop Mobile Computing Systems and Applications,Dec.* 1994.

[4.] L.M. Kornfelder, “***Toward a Practical Public-Key Cryptosystem***,”bachelor’s thesis, Dept. Electrical Eng., Massachusetts Inst. Of Technology, Cambridge, 1978.

[5.] P. Zimmermann,*The Official PGP User’s Guide.* MIT Press, 1995.

[6.] J. Jubin and J.D. Turnow, “The DARPA Packet Radio Project”*Proc. IEEE*,1987.

[7.] Srdjan Capkun,Levente Buttyan,and Jean-Pierre Hubaux,“Self-Organized Public-Key Management for Mobile Ad Hoc Networks , ”***IEEE Transactions on Mobile Computing***, vol.2, No.2, pp52-64, Jan-Mar 2003.

[8.] Paul Ferguson and Daniel Senie, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, RFC 2827, IETF Tools.

[9.] Djamel Djenouri, Nadjib Badache “A Survey on Security Issues in Mobile Ad hoc Networks”

Prof Himadri Nath Saha :Prof. Saha is graduated from Jadavpur University.He did his post graduate degree from Bengal Engineering and Science university.He is Assistant Professor of Institute of Engg and Management .His research interest is security in MANET

Prof.(Dr)Debika Bhattacharyya:
Prof.Bhattacharyya did Phd. from Jadavpur University in the dept. of ETCE. She is HOD in the Dept of CSE.Her research Interest is security in MANET

Sulagna Mukherjee: She is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. Her research Interest is MANET

Bipasha Banerjee: She is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. Her research Interest is MANET

Rohit Singh: He is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. His research Interest is MANET

Debopam Ghosh: He is a student of Institute of Engineering and Management and is currently pursuing B.Tech in Computer Science. His research Interest is MANET