SELF-ORGANIZED PUBLIC-KEY MANAGEMENT FOR MOBILE AD-HOC NETWORKS

Ch.B.V.Durga*

K.Hima Bindu*

B.Lalitha Rajeswari*

S. Satish Kumar*

Abstract

Ad-hoc networks are the networks do not rely on fixed infrastructure. In such network all the networking functions are performed by the nodes in a self organized manner. Due to infrastructure less architecture security in communication is of a major concern. Ad-hoc networks are the evolving technology in wireless networks. In such network all the networking functions are performed by the nodes in a self organized manner. The main objective is to develop a fully self-organized public-key management system for Ad-hoc networks aims to realize a public-key cryptographic method to perform authentication regardless of the network partitions and without any centralized services. The Security method to be realized is based on self organization among network nodes by updating information.

Keywords: Ad-hoc networks, authentication, public-key cryptographic, centralized services

* LBR College of Engineering, Mylavaram, India.

INTRODUCTION

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. There is no fixed infrastructure such as base stations for mobile switching. Nodes within each other's. There are two different types of wireless networks

- The easiest network topology is where each node is able to reach all the other nodes with a traditional radio relay system with a big range. There is no use of routing protocols with this kind of network because all nodes "can see" the others.
- The second kind uses also the radio relay system but each node has a smaller range, therefore one node has to use neighboring nodes to reach another node that is not within its transmission range. Then, the intermediate nodes are the routers.

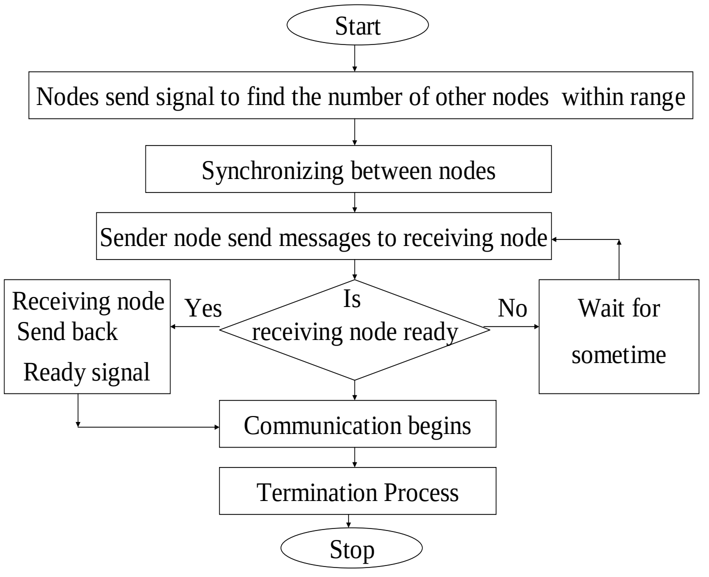
Start
Nodes send signal to find the number of other nodes within range
Synchronizing between nodes
Sender node send messages to receiving node
Receiving node Send back Ready signal
Yes
Is receiving node ready
No
Wait for sometime
Communication begins
Termination Process
Stop

Figure 1: Working of a general Ad-Hoc Network

There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment they are

- *Confidentiality*: Protection of any information from being exposed to unintended entities. In ad-hoc networks this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed.
- *Availability:* Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack. On physical and media access control layer

attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g. key management service.

- *Authentication*: Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.
- *Integrity*: Message being transmitted is never altered
- *Non-repudiation:* Ensures that sending and receiving parties can never deny ever sending or receiving the message.

Authentication

Authentication is the basis of any secure communication.

Without a robust authentication mechanism security goals are not achievable. Authentication assures that the origin of communication is what it claims to be or from.

Without this an attacker would pretend to be another node and may gain unauthorized access to resource and secure information.

Methods of authentication

- Several methods of authentication have been proposed for ad hoc networks.
- The threshold cryptographic method is found to be the most commonly used current method

RELEATED WORK

Threshold Cryptographic Method

The Network authenticate the data transfer based on a centralized node key exchange

- The centralized node is decided based on the node coverage Probability.
- The node with maximum number of nodes as its neighbor is declared as the head.
- All the member nodes transfer their public key to the centralized node.
- The keys are requested and recovered from this node on request.

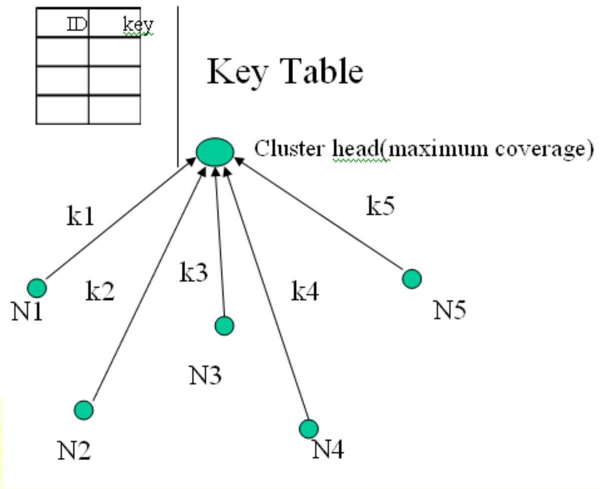

Figure 2 Threshold cryptography

N1, N2, N3… Member nodes K1, K2, K3… Corresponding Keys

Limitations:

- Threshold based cryptography method is based on the centralized node for monitoring the keys.
- The key distribution and Authentication is completely relied on centralized node.
- Any failure in key generation may result in wrong authentication.
- All nodes depend on the centralized node for authentication.
- Due to key Request the communication results in delayed packet transfer rate.

Self organized cryptography

Each node distributes its public key to their one hop neighbor during the broadcast period. Each node acknowledge back to the node back with the certificate for the received node key. The Exchanged certificates are saved as repository tables in each node. The exchanged certificate gives the authentication of the key received by presenting the key of node-m's key which it received with its own key. The authentication of the key is done by the node by checking the second field of the certificate i.e it's own as received by node-n

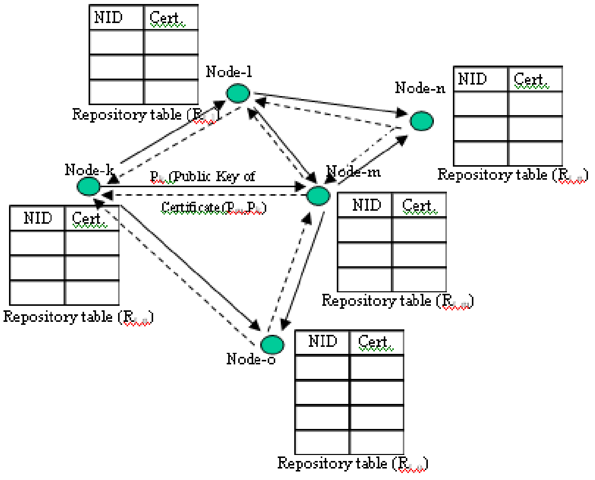

Figure 3: Self organized cryptography

Repository Updating

After every beacon period the network update the repository entry with the new certificates as updated entry and previous entry as Backup repository.

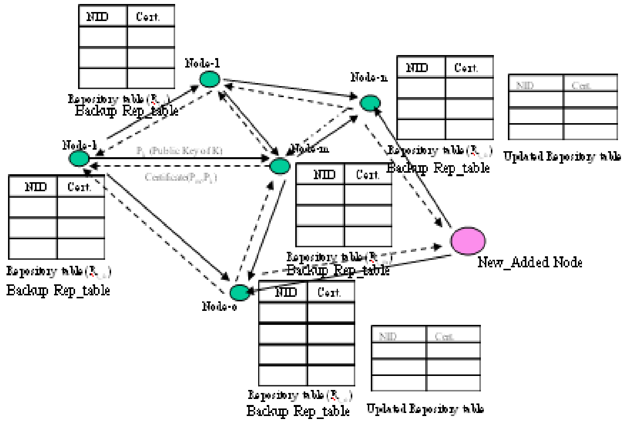

Figure 4: Repository Updating

Advantages:

The proposed self-organized public key management system is completely independent in operation. Does not rely on any centralized node for key. The method performs certificate exchange so the authentication is most secure. The repetitive certificates are kept as backup so the trustiness of the key is evaluated. As the updated repository table holds only the new keys entered the resource required is very less. Each Node maintains a key table hence the key request time is completely avoided, making the communication delay minimum.

Implementation

We will consider randomly distributed nodes and create nodes and keys.

In this implementation using mat lab, we will compare the threshold cryptography method with the self organized cryptography method and calculate and plot Propagation delay, Average Packet Delivery, Repository Updating.

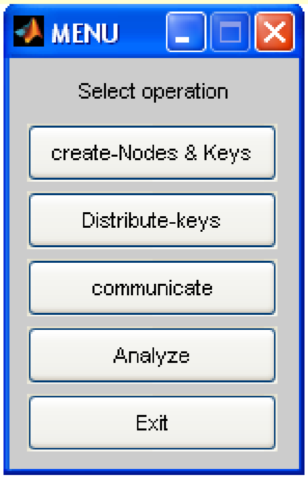

Figure 5: select operation

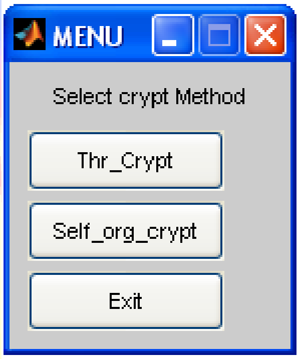

Figure 6: selecting cryptography method

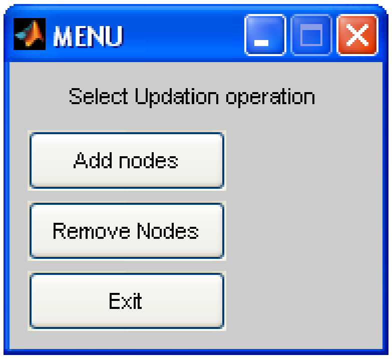

Figure 7 : Adding or removing nodes and updating

Results

Considered Network

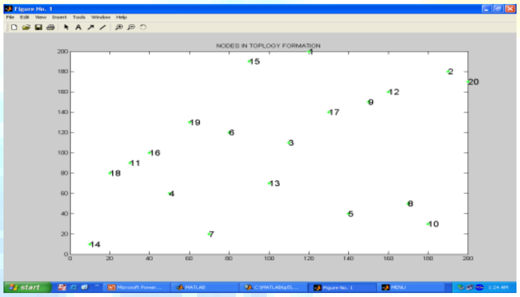

Figure 8 Randomly distributed Nodes

Case 1: With No Add-on nodes

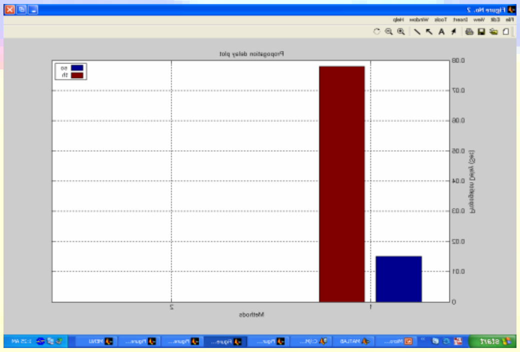

Figure 9: Propagation delay plot

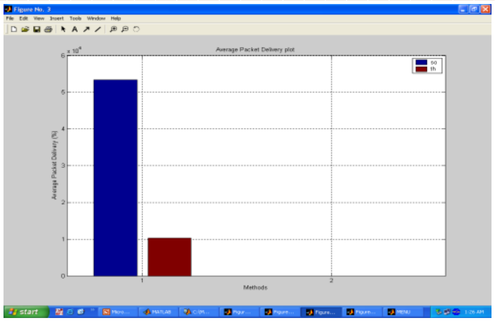

Figure 10: Average Packet Delivery plot

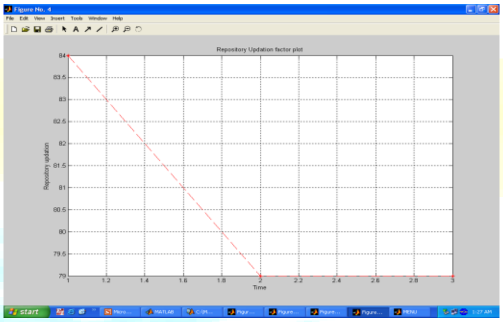

Figure 11: Repository Updating plot

Case 2: With 2 Add-on nodes

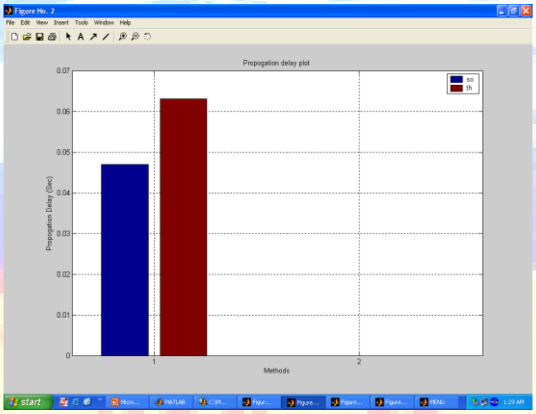

Figure 12: Propagation delay plot

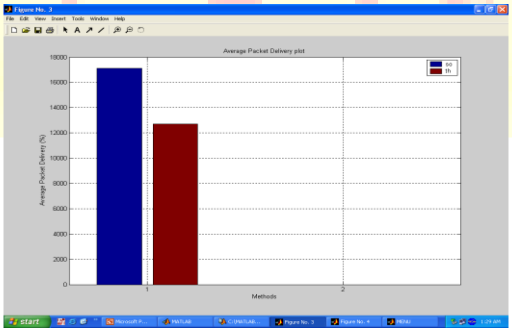

Figure 13: Average Packet Delivery plot

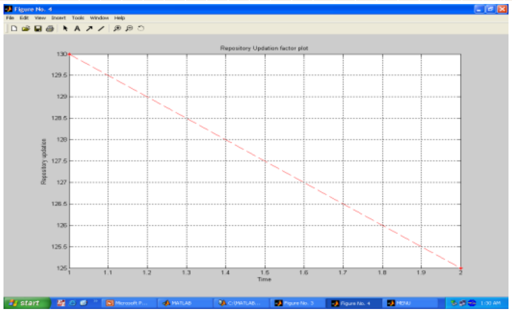

Figure 14: Repository Updating plot

Case 3: With 2 Add-on nodes, 1-remove-Node

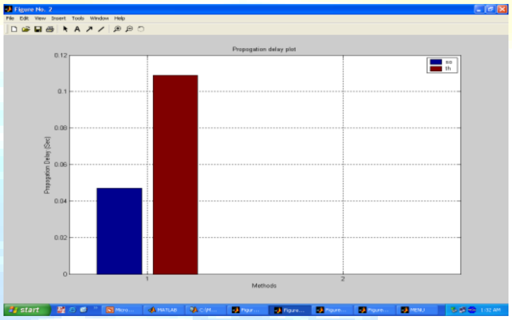

Figure 15: Propagation delay plot

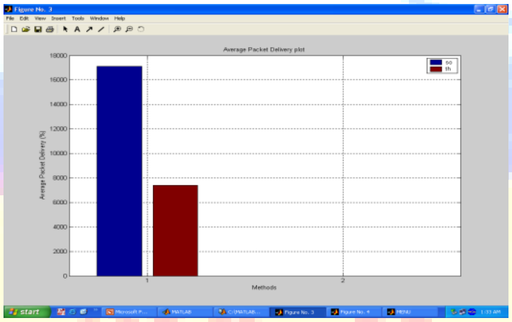

Figure 16: Average Packet Delivery plot

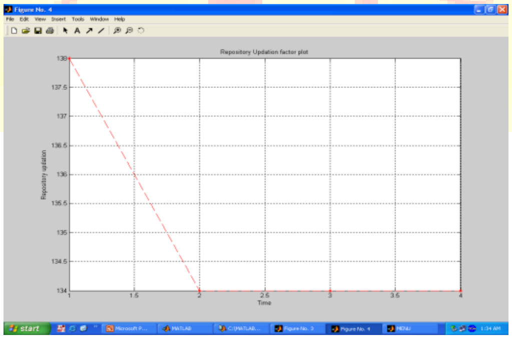

Figure 17: Repository Updating plot

CONCLUSION

A self organized key distribution mechanism is developed for ad Hoc network. The proposed self key management scheme outperforms the performance of the existing threshold based cryptography. The repository updating factor is observed to be reduced down with more number of users; hence the proposed scheme is optimal under resource constraint systems. The packet delay is found to be less in self organized cryptography as compared to Threshold based cryptography.

REFERENCES

[1] C. E. Perkins, *Ad Hoc Networking*, Addison Wesley Professional, Dec. 2000.

[2] D. B. Johnson, “Routing in Ad Hoc Networks of Mobile Hosts,” in *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications*, December 2001.

[3] S. Garfinkel, “PGP: Pretty Good Privacy,” *O’Reilly & Associates Inc.*, USA, 2005

[4] “PKI practices and policy framework,” *ANSI X9.79*, American National Standards Institute, 2000.

[5] L. Gong, “Increasing availability and security of an authentication service,” *IEEE Journal on Selected Areas in Communications*, Vol.11, No.5, Jun. 2001.

[6] Y. Frankel, P. Gemmell, P. Mackenzie and M. Yung, “Proactive RSA,” *CRYPTO*, 1999

[7] 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 the 9th International Conference on Network Protocols (ICNP), November 2001.

[8] J. Douceur, “The Sybil Attack,” in Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS), 2002.

[9] G. Montenegro and C. Castelluccia, “Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses,” in Proceedings of the 9th Annual Network and Distributed System Security Symposium (NDSS), 2002.

[10] G. O’Shea and M. Roe, “Child-proof Authentication for MIPv6 (CAM),” ACM Computer Communications Review, April 2001.

[11] J.-P. Hubaux, Th. Gross, J.-Y. Le Boudec, and M. Vetterli, “Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project,” IEEE Communications Magazine, January 2001.

[12] L. Blazevi ˇ c, L. Butty ´ an, S. ´ Capkun, S. Giordano, J.-P. Hubaux, and J.-Y. Le Boudec, “Self-Organization in Mobile Ad Hoc Networks:The Approach of Terminodes,” IEEE Communications Magazine, June 2001.

[13] J.-P. Hubaux, L. Buttyan, and S. ´ Capkun, “The Quest for Security in Mobile Ad Hoc Networks,” in ˇ Proceedings of the ACM Symposiumon Mobile Ad Hoc Networking and Computing (MobiHoc), 2001.

[14] Srdjan Capkun, Levente Buttyan, and Jean-Pierre Hubaux, “Small Worlds in Security Systems: an Analysis of the PGP Certificate Graph,” in ACM New Security Paradigm Workshop (NSPW), 2002.

[15] L. Buttyan and J.-P. Hubaux, “Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks,” ´ To appear in ACM/Kluwe Mobile Networks and Applications (MONET), vol. 8, no. 5, October 2003.

[16] F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks,” in Proceedings of the 7th International Workshop on Security Protocols, 1999.

[17] Frank Stajano, Security for Ubiquitous Computing, John Wiley and Sons, Feb. 2002.

[18] R. Anderson and M. Kuhn, “Tamper Resistance - a Cautionary Note,” in Proceedings of the Second Usenix Workshop on Electronic Commerce, 1996.