Secure Key Exchange ThroughElgamal Cryptosystem In Adhoc Networks

Sai Vikas Gunti
Computer science department, K.L University
Vaddeswaram, Guntur dist. Andhrapradesh
vikasgunti15@gmail.com

Abstract— Establishment of secure key exchange system in the ad hoc networks is a difficult procedure due to the special characteristics of ad hoc networks. Security in the ad hoc networks is very important as they use common radio channel for the entire nodes and security can be attained using the cryptographic techniques. Key management in ad hoc networks is difficult as there is no centralized system for the this type of networks to answer these problems , In this paper it is proposed that secure key exchange can be performed through the use of ELGAMAL CRYPTOSYSTMS in a group of nodes which are formed by using the binary tree formation method.

Index Terms—. Ad hoc network, binary tree, cryptography, decryption, encryption, group formation, key exchange,

1 INTRODUCTION

Cryptography is the most common and reliable means to ensure security. Cryptography is not specific to ad hoc wireless networks. It can be applied to any type of communication network. Cryptography is the study of principles, techniques, and algorithms by which information is transformed into disguised version which no unauthorized person can read, but can be recovered in its original form by an intended recipient. In cryptography, original message is called as plain text and the coded message is called cipher text. The process of converting the plain text in to cipher text is called as encryption or enciphering, restoring the plain text from the cipher text is called as decryption or deciphering. The process of encryption and decryption are governed by the keys which are small amount of information used by the cryptographic algorithms. When the key is to be kept secret to ensure security of a system it is called a secret key. The secure administration of cryptographic keys is called key management. Effective key management is goal of any cryptographic key management. Providing a key management service in any network is challenging, but in an ad hoc network it is particularly difficult. Centralized servers cannot be relied on in an ad hoc network. There are three distinct approaches to key management for ad hoc networks pursued in the literature: Key Exchange, Key Agreement and Public Key Infrastructure. In this paper we are going to discuss on key exchange though ELGAMAL CRYPTOSYSYTEM in group of nodes which are formed through binary tree formation method.

1.2 Key exchange

Key exchange is the most primitive form of key management. Alice and Bob wishing to communicate over an insecure channel exchange a-priori a cryptographic key. This key can be exchange by physical contact as suggested or over a secure side channel expands this idea and suggests the use of public key exchange. Thus the side channel need only be secure against a 'man in the middle' attack [MIMwikipedia] but can tolerate eavesdropping, as the information exchanged is public. A'man in the middle' (MIM) can be detected/avoided by using a short range Infrared or radio channel. A 'man in the middle' (MIM) can be detected/avoided by using a short range Infrared or radio channel. These principles are quite old. The use of physical key exchange must be the earliest form of key management, if it can be described as key management at all. The key exchange is usually an inconvenient way for key exchange but in the ad hoc wireless networks it may not be that much inconvenient

1.3 Group key management in ad hoc networks

Group keying allows multiparty secure communications, and hence provides group level authentication and security. The main goal of a group key management protocol is to securely provide group members with an up-to-date security association (SA), which contains the needed information for securing group Communication (i.e., the group data). We call this SA the Data SA. In ad hoc wireless networks, there is a common radio channel for all the nodes, so the data transferred can be visible to all the nodes which are sharing the same radio channel, but all nodes which are utilizing the same radio channel doesn't belong to same groups, so the key must be managed properly that it must not be known to other nodes except for the nodes which belong to a group. To secure group communication, nodes share a single symmetric key for encrypting and decrypting messages in existing systems. In the traditional group key exchange mechanism, if a new node joins or leaves, then the group key must be globally updated and distributed among the nodes in the group. This is called as group re keying, this requires a centralized mechanism for the re issue of the key it takes more time and also consumes more battery power of ad hoc wireless nodes.To avoid this disadvantage we go for the key exchange between the groups of authenticated nodes. Whenever there is a change in set of authenticated neighbors, a node must compute a new key and send this new key to all its authenticated neighbors. Now the keys are exchanged only in the neighbor nodes the time taking also become less and authentication increases. Ad hoc networks consist of frequently changing nodes, so the key exchange must be secure and must be fast. Here the key exchange can be done using RSA algorithm, every time a node change occurred it would be easier to exchange the key through a single message.

International Journal of Scientific & Engineering Research Volume 5, Issue 4, April-2014
ISSN 2229-5518

2 NEED FOR CRYPTOGRAPIC SECURITY IN ADHOC NETWORK

Due to the unique characteristics of the ad hoc wireless networks, such networks are more vulnerable to security attacks compared to wired or infrastructure based networks. These features and properties also bring many security management challenges to wireless ad hoc networks. The main characteristics of wireless ad hoc networks include dynamic topology, high link breakage and data loss, constrained energy, limited bandwidth and transmission range, poor physical protection, distributed cooperation for multiple hop communication and no central authority. With these challenging characteristics, wireless ad hoc networks are at risk from security breaches. In ad hoc wireless networks node are free to move about their limitations. This type of highly dynamic topology need to loss of mutual trust among nodes in ad hoc networks. The mobility of nodes may also cause frequent link breakage and data loss, since the nodes may join and leave the networks without any notice. So the connections among the nodes will not be guaranteed all the time. This intermittent transmission environment has great impact on information communication in wireless ad hoc networks, which will affect all applications including security implementation. Limited communication bandwidth may also be a target for malicious attacks, such as Denial of Service (DoS) attack. To implement such attack, the malicious node may send vicious queries flooding to target nodes to consume the bandwidth and occupy the shared wireless media, which make the network service unavailable to other nodes. More over security is important for any type of network the users want the privacy for their data. As such, end-to-end security may often be required. In fact we rely on the fact that our data can be overheard by nearby nodes so that it can be transmitted through the network. Clearly with more nodes having greater access to the data sent in the network the need to secure that data by cryptographic means increases. Finally, an ad hoc network may consist of hundreds or even thousands of nodes, Security mechanisms should be scalable to handle such a large network. So there is a high need of cryptographic security for the ad hoc networks.

3 ELGAMAL CRYPTOSYSTEM

In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described byTaher Elgamal in 1985. ElGamal is an encryption scheme that, like RSA, depends on computational assumptions to guarantee security. Unlike the RSA assumption, however, ElGamal depends on type of assumption called the Discrete-Logarithm assumption. Roughly, this assumption claims that it is hard in some groups to find x given gx mod n.The name comes from the fact that

x log(g) mod n = log(gx) mod n

and division is easy to compute in a group, so x is easy to compute given log(gx) mod n

3.1 Algorithm

3.1 .1 Key generation

Take global elements: q is prime number

z is z<q and z is a primitive root of q

1. Generate a random integer XA , such that 1 < XA < q – 1.
2. Compute YA = a^XA mod q
3. A's private key is XA, A's pubic key is {q, a, YA}

3.1.2 Encryption using public key

1. Select Plaintext: M < q
2. Select random integer k where k< *q*
3. Calculate K K= (YA) ^k mod q
4. Calculate *C*1 *C*1 = z^k mod q
5. Calculate *C*2 *C*2 = KM mod q
6. Cipher text is: (*C*1, *C*2)

3.1.3 Decryption using private key

1. Cipher text is: (*C*1, *C*2)
2. Calculate K K= (*C*1) ^XA mod q
3. Plaintext is: M = (C2K^–1) mod q

4 IMPLEMENTATION-A THEORETICAL APPROCACH

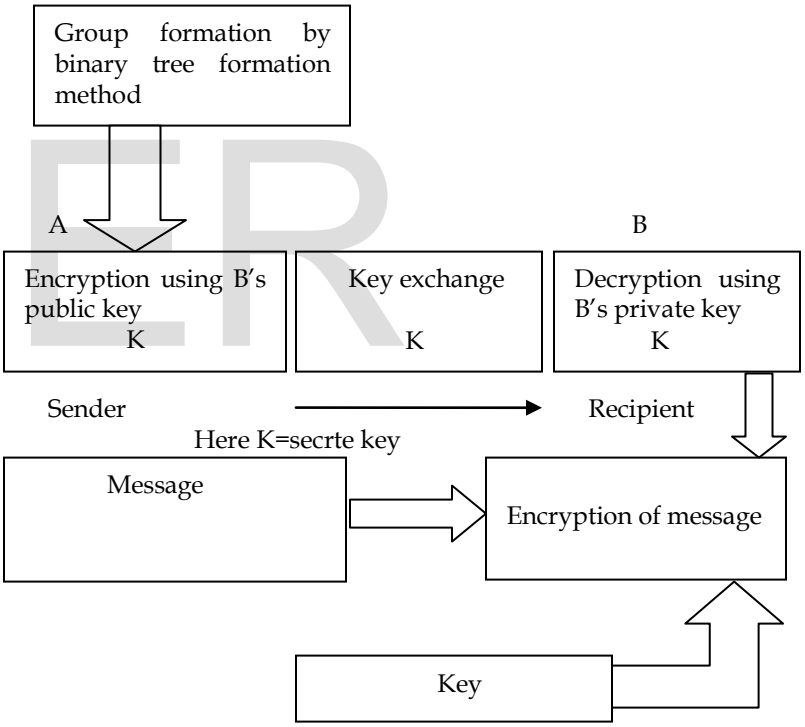

Figure1: Total proposed system

4.1 Group fromation

For the group formation of ad hoc network nodes, we follow the binary tree formation. Whenever the nodes want to join the group, they are joined in the network by using binary tree node insertion method. Whenever the node gets detached from the group the network topology uses the binary tree node deletion method. Initially there is no connection between the nodes in the network range of an ad hoc network. Then any one node in range can take initiation and sends a special HELLO message to its neighbors stating that it wants to initiate a tree-based trust relationship with them. Naturally, as

International Journal of Scientific & Engineering Research Volume 5, Issue 4, April-2014
ISSN 2229-5518

there is no pre-established trust among any network nodes in a typical ad hoc network, the adjacent nodes can accept the invitation or simply reject it. Accepting such an invitation from a given node means that the invited node is willing to proceed with a mutual-certification process with the initiator. The purpose of the protocol is to form a binary tree of trust between all network entities. So, each node can provide certificates to a maximum of two neighboring nodes.Group formation is depicted in figure(2) here intailly all the nodes are in the signal range and doesn't have any connection between them, so node A intiated the call for other nodes and forms a group based on binary tree formation method.In this binary tree foemation method , the node which on top from all the nodes will be called as root node in figure (2) A is root node ,also A will be called as parent node to node B , C where B, C are called as child nodes to the node A and the node which doesn't have any child node is called leaf node.

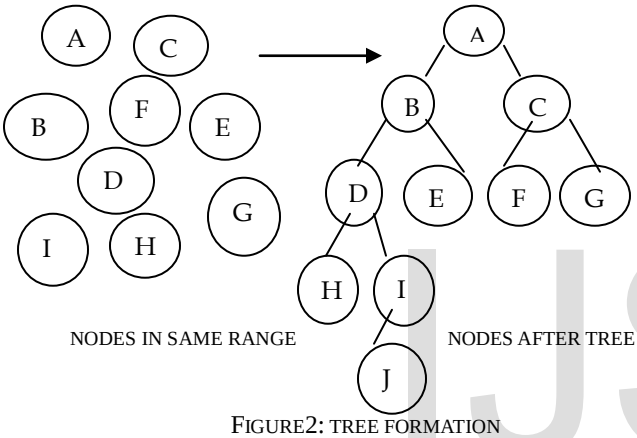

FIGURE2: TREE FORMATION

4.2 group leaving

As ad hoc network is most dynamic network some of the node in the range of network leaves the group, depending on some conditions. In this system the detachment of a node from network is straight forward.If a node has no child nodes then the node will be detached directly, if node to be detached will have the one child node then that child node is attached to its grandparent. If the node to be detached will have two child nodes then the node which is at the far most end in left sub tree or right sub tree to the detaching node can take that position.Here in figure(3) the leaf node i.e;anode with out having any child node will be detached dirctely. In figure (4) a node with one child node I want to detach from group then the chils node J will be attached to the grandparent D. In figure(5) when a node having two child nodes A want to leave the group then there may be a chance for J or H or F to become the root node, here in node F became the root node.

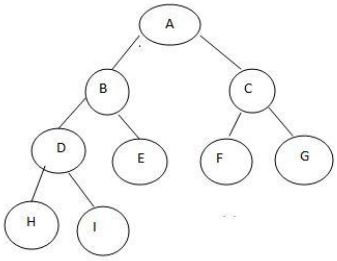

Figure3: Detachment of leaf node with one child node

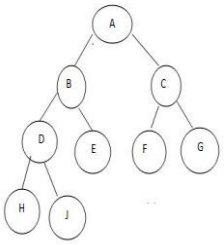

Figure4: Detachment of node

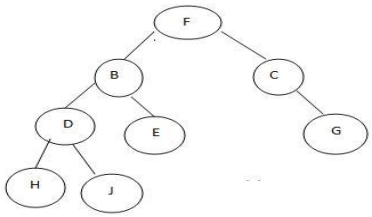

FIGURE3: DTEACHMENT OF NODE WITH TWO NODES

4.3 Key exchange

All nodes have a {public, private} key pair created locally by using ELGAMAL CRYPTO SYSTEM, so for every node pair each part signs the public key of the other using its private key and sends the result towards the other part. This node detection scheme is identity-free and is carried over through a handshake process between any pair of neighbors. Handshaking procedure is basically carried over for key exchanges between a given node and its new detected neighbors. After the handshake procedure, each pair of nodes shares a chain of secret keys. Secret keys are exchanged securely by encrypting the secret key with the intended recipient's public key. Only the intended recipient can decrypt the secret key because it requires the use of the recipient's private key. Therefore, a third party who intercepts the encrypted, shared secret key cannot decrypt and use it. HELLO messages are periodically sent to the nodes in the group. To forward the information the RREQ and RREP messages are used by each intermediate node to establish the route between the source and the destination nodes in the network. Here K = secerete key.

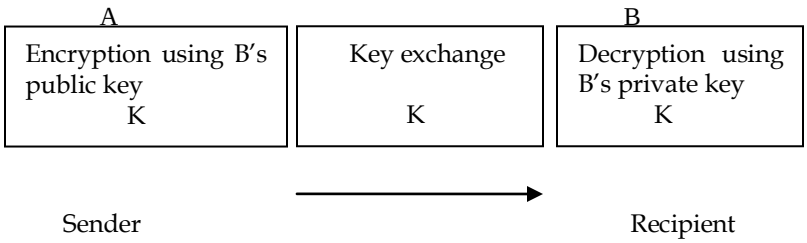

Figure 4: key exchange scenario

International Journal of Scientific & Engineering Research Volume 5, Issue 4, April-2014
ISSN 2229-5518

5 CONCLUSION AND FUTURE ADVANCEMENTS

This paper proposes the secure key exchange using the elgamal cryptosystems, as the ad hoc networks are highly dynamic in nature it will be quite difficult for the communication and it is difficult to form the groups which are having secured way for exchanging keys .These two problems will be solved by this proposal by stating the group formation using the binary tree formation method and key exchange through the elgamal cryptosystems. This proposal assures security and reduces the overhead of key distribution centers for the secure key exchange and also avoids the rekeying issues. This can be utilized ever it required for secure group communication in ad hoc networks. The future advancements for this proposed system may be inclusion of futures such as detachment of malicious behaving nodes at any time, key storage at nodes.

REFERENCES

[1] C.S.Ram Murthy, B.S.Manoj, "ad hoc wireless Networks: Architectures and protocol", 2nd Edition.2005. pageno.483 (9.11)

[2] Shared RSA Key Generation In A Mobile Ad Hoc Network
B.Lehane and L.Doyle, D.O'Mahony MILCOM'03 Proceedings of the 2003 IEEE conference on Military communications - Volume II

[3] Securing Wireless Ad Hoc Networks: Towards A Mobile Agent Security Architecture Li Xia and Jill Slay the 2nd Australian Information Security Management …, 2004 – Citeseer

[4] Elgamal wikipedia

[5] Cryptography and network security principles and practice by willam stallings 5th ed. Pearson publications pageno 307 (10.2)

[6] Binary Tree Based Public-Key Management for
Mobile Ad Hoc Networks
Georgios Kambourakis, Elisavet Konstantinou and Stefanos Gritzalis

[7] Security Issues in Mobile Ad Hoc Networks
- A Survey
Wenjia Li and Anupam Joshi

[8] Secure key exchange & encryption mechanism for group communication in wireless ad hoc networks S. Sumathy and B.Upendra Kumar

[9] Encrypted key exchange password –based protocols secure against dictionary attacks stven m bellovin michale merit

[10] Key aggrement in adhoc networks N. Asokan, Philp Ginzborg