ISSN: 2321-7782 (Online)
Volume 2, Issue 3, March 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Key Management Scheme for Broadcast and Multicast Service

G. Visalaxi
Assistant Professor
Apollo Engineering College
Chennai – India

Abstract: ***The Purpose of Key Management is to provide secure procedures for handling cryptographic keying material to be used in symmetric (or) asymmetric cryptographic mechanisms. Key Management Schemes generally depend on the type of keys to be handled, on the given facilities & on the specific application. Key Management Scheme focus on the reduction of transmission overhead caused by distribution of associated key material over broadcast and interact channel. In Multicast it is important to update security keys when a user joins or leaves the multicast group. The main aim is to reduce the number of keying messages & to update the key at a reduced cost. The group key needs to be securely conveyed to the group members every time the group key is changed. In this work, we investigate how to secure route discovery of the MAODV protocol of wireless network. Here, we propose a secure route discovery of MAODV based on attacks (black hole) & two-way hash function.***

Keywords: key management; multicast ad-hoc on demand distance Vector; black hole attack; multicast; communication system security; Hash function.

I. INTRODUCTION

Key management scheme for broadcast & Multicast service [1] are typically based on 4 layer key management.

- Layer -1 client server mutual authentication and session key (SK) establishment.
- Layer-2 responsible for provisioning of group management key (GMK) to a client that is authorized to access selected multicast broadcast service.
- Layer-3 In charge of distributing traffic encryption key (TEK) under GMK.
- Layer-4 delivers TEK encrypted.

Multicast is communication between a single sender & multiple receivers on a network. Otherwise it transmits a single message to a selected group of recipients. Multicast is used in streaming video in which many megabytes of data are sent over the network. Single packets copied by the network are sent to a specific subset of network address. These addresses are specified in the destination addresses. It greatly reduces the transmission cost when sending the same packets to multiple recipients [2].

Instead of using multiple uncast transmissions it is advantageous to use multicast in order to save bandwidth & resources .Since a single message can be delivered to multiple receivers simultaneously [3]. In the existing system dynamic rekeying [4 - 6] KTS Scheme is used in broadcast & multicast service. Logical key hierarchy (LKH) with dynamic rekeying can reduce the cost in multicast [5].Without dynamic rekeying, when the number of users increases, the rekeying cost will increases rapidly.

© 2014, IJARCSMS All Rights Reserved

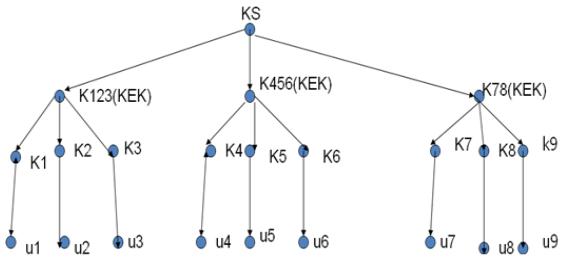

Fig. 1 Pictorial representation of user Joins & Leaves the key tree

It is a tree with single root and two parameters, (i) height h, which is the longest path from a leaf to the root, (ii) degree d, which is the maximum number of outgoing edges of a node in the tree. The tree is called key tree. Each leaf in the key tree represents a unique user. Every user owns three key

(1) Individual key which is shared with the key server (KS).

(2) Group key which is shared with the KS & all other users in the multicast group.

(3) Auxiliary key which is stored in an intermediate node, the user and the KS.

II. PROPOSED SYSTEM

A. Two – Way hash Chain (2HCS)

Cryptographic hash functions have been widely used in a various security application such as integrity protection & authentication. Huang and Medhi [7] introduced the importance of using hash chaining for many-to-many secure group communication. Dutta et al [8] extended their approach by utilizing bi-directional hash chains for secure communication in wireless network.

a. Operation

In Two way hash chain (2HCS), Group Management Key is represented by the key seed pair(KSP). KSP is a 2-tuple {KS1,KS2}, where KS1, KS2 are random key seeds generated & distributed by the key management server over an interaction channel.

TEKs are no longer transferred over a broadcast channel but generated from a KSP both by a client & server.

1) Cryptographic hash function is applied n times to KS1 producing a sequence of hash values {Si} which is called forward hash chain (FHC).

$Si=hash(Si-1)$, for $i=(2,....,n)$, given $Si=hash(KS1)$ ---- (1)

2) Cryptographic hash function is applied n times to KS2 producing a sequence of hash values {Mj}, which is called reverse hash chain (RHC).

$Mj-1=hash(Mj)$, for $j=(1,...n-1)$, given $Mn=hash(KS2)$ ----(2)

3) After computing FHC & RHC, n TEKs are derived as

$TEK_k=S_k \oplus M_k$ for $K=(1,...n)$

© 2014, IJARCSMS All Rights Reserved

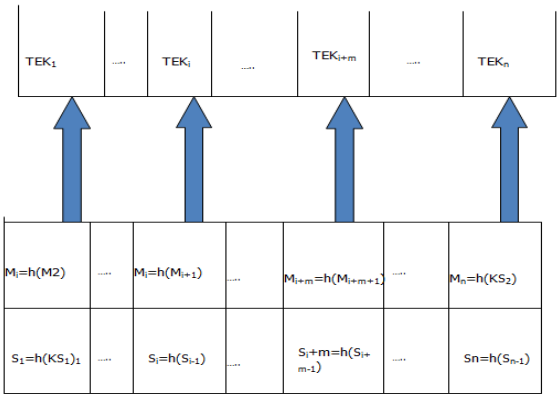

Fig. 2 Pictorial representation of 2HCS Key Generation Mechanism

III. RELATED WORK

In order to protect confidentiality and integrity of the information, the nodes should be securely associated with the neighbouring nodes (via) encrypted data link. Therefore key management plays a critical role in establishing secure communication in wireless network.

A. Study of Group wise key Distribution Scheme

Security requirements for group wise key distribution scheme include [9]

Group confidentiality: Nodes that are not part of the group should not have access to any key that can decrypt any data broadcasted to the group.

Forward Secrecy: Nodes that detach from the group should not have access to any future keys, which ensures that a detached node cannot decrypt further data.

Backward Secrecy: A new node that attaches to the secession should not have access to any old keys, which ensures that a node cannot decrypt data sent before it attaches to the group.

Collusion Freedom: Any set of fraudulent nodes should not be able to deduce the current active TEK.

Hence, it is required to offer a reliable rekeying process with minimum number of rekeying messages. The rekey scheme should also require neither a large number of storage keys nor high computation overhead at the GKM (or) the nodes in the group.

B. Hash chain

A hash function Hash takes a binary string of arbitrary length as input, and outputs a binary string of fixed length.

C. Proposed System Architecture

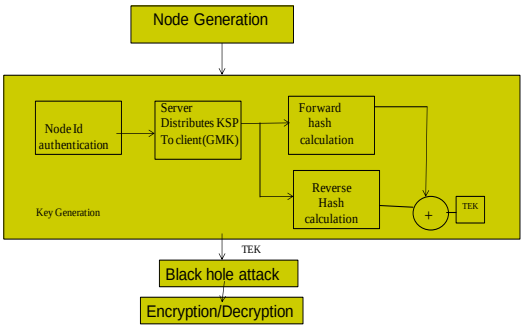

Fig. 3 Proposed Work

© 2014, IJARCSMS All Rights Reserved

a. Nodes Generation

It is connection point, redistribution point (or) end point for data transmission. Nodes have a programmed capability to recognize & process forward transmission to other nodes. Each node has its own attributes each node is the key value store, unique ID used to identity that node.

b. Generation of TEK

Forward hash chain: S1=h(KS1), S2 = h(S1)... Si=h(Si-1), Sn=h(Sn-1)

Reverse hash chain: M1=h(M2)..Mi=h(Mi+1).. MN=h(KS2)

TEK=S1 $\oplus$ M1

Hash methodology using sha -1.

c. Key Generation

Client performs mutual authentication with the server that results in establishment of unique session between client & server [10].Client sends a service request to join a selected multicast broadcast group. If the service request is validated and processed successfully, the server provision key seed pair to the client. After receiving the key seed pair from the server the client calculates the granted number of traffic encryption

d. Black Hole Attack

A packet drop attack or black hole attack is a type of denial-of-service attack accomplished by dropping packets. Black hole refers to places in the network where incoming traffic is silently discarded (or) dropped without informing the source that the data did not reach its intended recipients[11,12].

e. Encryption /Decryption

Plain text to be encrypted must be 64 bits in length and key-56 bit in length 16 rounds. Data Encryption Standard Algorithm

1. Permutation (reshuffling)
2. Divide blocks-left, right
3. Process right block(32 bits)
    - Expand (48 bits)
    - XOR with Re key
    - Substitution (32 bits)
    - Permutation
4. XOR the left block with the processed right block.
5. Repeat the above steps for 16 rounds.

IV. IMPLEMENTATION OF SECURE MAODV

The multicast Ad-hoc on demand distance vector (MAODV) routing protocol [13] constructs a shared multicast tree, which connects the group members. MAODV helps the group members to get connected to the multicast tree through the forwarding nodes. Members can join or leave the group at any time. The multicast sequence number is used to check the freshness of the multicast group. An unauthorized node should not be able to participate in the MAODV routing. Non-group member node should not be able to act as a group member.

© 2014, IJARCSMS All Rights Reserved

A. Group Member

Every group member has the privilege to initiate a route request to join a multicast tree. Group member justifies that it belongs to a particular multicast group.

B. Node Validation

Group members or non group member in the network have a validation called the node validation. Only node possessing node validation is eligible to participate in routing.

C. Multicast Tree Member

It generates and securely distributes the tree key to the entire multicast tree members. A node that has the valid key tree will reply the route request.

D. Secure Route Discovery

Source node broadcasts the route request and then it receives a route reply. RREQ (Route request) the request ID is used to check the freshness of the request.

Case (i): If a group member 'i' wants to join a multicast group, then it prepares the RREQ packets & broadcasts it to all its one hop neighbors. It the receiver is a multicast tree node, then it apply validation of the source and send a reply to the sender by checking its routing table. The routing table contains the control information of the destination. The nodes of the tree maintain a dynamic request table.

Case (ii): If a group member 'i' wants to send data to a destination group by creating the multicast tree with valid group members of that session, then it prepares the RREQ and replaces the join request field by creating a multicast tree. RREQ If a node 'i' does not receive a RREP message then it rebroadcast the request 'm' times. Then the node 'i' declares itself as the group by sending group of packets.

V. EXPERIMENTAL RESULTS

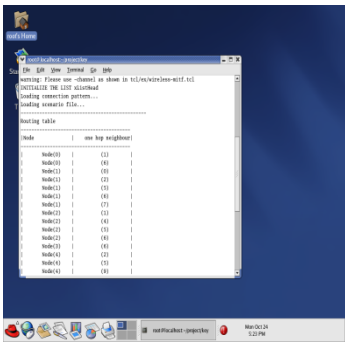

Fig. 4 Routing Request Table

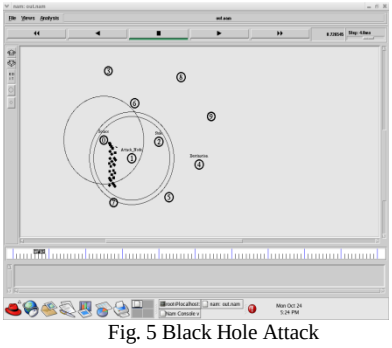

Fig. 5 Black Hole Attack

© 2014, IJARCSMS All Rights Reserved

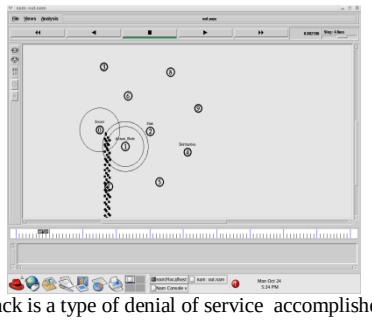

Fig. 6 Packets drop attack is a type of denial of service accomplished by dropping packets

VI. CONCLUSION

In this work, we have reduced the group membership. We have introduced a request table which stores the next help & previous hop IPS. It validates nodes with node id and secret sharing key. This two way hash chain scheme provides effective combination of key generation methods & service.

References

1. Security of broadcast / multicast service (M\BMS) release 7, 3GPPTS 33.246, Dec 2007.
2. Elizabeth Royer and C-K Toh, A Review of current routing protocols for Ad-hoc mobile wireless networks, IEEE personal communication magazine, April 1999.
3. Oscar F. Gonzalez, Godwin Ansa, Michael Howarth & George Pavlou, Detection & Accusation of packet forwarding misbehavior in mobile Ad-hoc network, Journal of Internet Engineering, Vol. 2, No.1, June 2008 PP 181-192.
4. C.K. Wong, M. Gouda, and S.S. Lam, Secure Group Communications using key graphs, IEEE/ACM Trans. Networking, Vol. 8, pp. 16-31, Feb 2000.
5. D.M. Wallner, E.J. Harder and R.C Agee, Key management for multicast: issues & architectures, IETF RFC 2627, June 1999.
6. B. Briscoe, MARKS : Zero side effect multicast key management using arbitrarily revealed key sequences, in proc. International workshop on Networked group communication (NGC), Pisa, Italy, pp. 17-20, Nov. 1999.
7. D.J. Huang and D. Medhi, A key chain based keying scheme for many-to-many secure group communication, ACM Trans. Inf. system security, Vol. 7, No.4, pp. 423-552, Nov 2004.
8. R. Dutta, E.C. Chang and S. Mukhopadhyay, Efficient Self-healing key distribution with revocation for wireless sensor networks using key chains. ACM Trans. Inf. System security Vol. 7, No.4, pp. 423-552.
9. Y. Challal & H. Seba, Group key management protocols: A novel Taxonomy, Int'I Info Tech. Vol. 2, pp. 105-119, 2005.
10. Service & content protection for mobile broadcast services, OMA TSBCAST SVC cnt protection V1.0, Dec 2008.
11. Yih-chun Hu, Adrian Perrig, David B. Johnson, Rushing Attacks & Defense in wireless Ad-hoc Network routing protocols, San Diego, California, USA, pp. 30-40, wise 2003, Sep 19, 2003.
12. Shennu Sharma Dr. Roopam Gupta, Simulation Study of Black hole attack in mobile Ad-hoc Network, International conference on network applications, protocols and services 2008 (NetApps 2008), pp. 1-6, Nov 2008.
13. E.M. Royer & C.E. Perkins, Multicast operation of the Ad-hoc on-demand distance vector routing protocol, 5th Annual ACM/IEEE International conference on mobile computing & Networking Mobicom '99, pp. 207-218, 1999.

AUTHOR(S) PROFILE

Mrs G.visalaxi, is currently working as Assistant Professor in the Department of Computer science & Engineering of Apollo Engineering College, chennai having an experience of 1.1 years. This college has been affiliated to Anna University, Tamil Nadu, India. The M.E Degree is awarded to her by the Anna University during December 2012. Her area of interest includes Data Mining, image processing, Networking

© 2014, IJARCSMS All Rights Reserved