Generation of Shorter Length Keys for Broadcast and Multicast Services Using 2-way Hash Chain Schemes

Shweta M. Kulkarni, Shubhada S. Kulkarni

Abstract: ***Broadcasting is the distribution of message to dispersed audience via communicating channels. Whereas,* multicasting *refers to sending of message to a selected group. Key management for multicast and broadcast services has difficulty to find an appropriate security mechanism because, a very high number of users consume data simultaneously. Thus our project is focused on new Key Management Scheme, called 2-way Hash Chains Scheme (2HCS), that focus on the reduction of transmission overhead caused above and thus, effectively reduces the number and the size of keying messages.***

Keywords: Communication system security, multimedia systems, security, hash function.

I. INTRODUCTION

Broadcasting is the distribution of audio and video content to a dispersed audience via any audio or visual mass communication medium, but usually one using electromagnetic radiation (radio waves). Broadcasting has been used for purposes of private recreation, non-commercial exchange of messages, self-learning and emergency communication such as amateur (ham) radio and amateur television (ATV) in addition to commercial purposes like popular radio or TV stations with advertisements.

Multicasts transmit a single message to a selected group of recipients. A simple example of the multicasting is sending an e-mail message to a mailing list, teleconferencing and video conferencing also uses multicasting, but it require more robust protocols and networks.

Thus, multicasting refers to sending a message to a selected group whereas broadcasting refers to sending a message to everyone connected to a network.

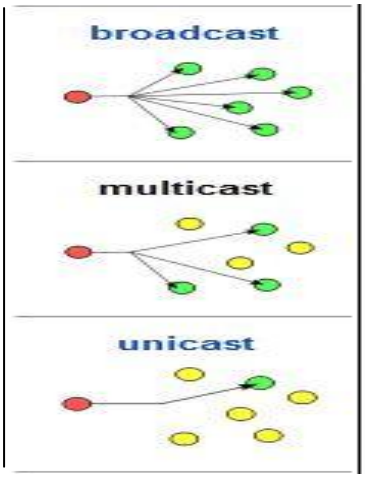

Fig.1.1 Multicast and Broadcast architecture

Manuscript received September, 2013.

Ms. Shweta M. Kulkarni, M Tech IV SEM Gogte Institute of Technology Belgaum-590008, Karnataka, India.

Shubhada S. Kulkarni, Gogte Institute of Technology, Belgaum-590008, Karnataka, India.

II. KEY MANAGEMENT SCHEME

KEY management schemes for mobile Broadcast and Multicast Services (BMS) such as those standardized in 3GPP (3rd Generation Partnership Project) MBMS (Multimedia Broadcast/Multicast Services), DVB-H (Digital Video Broadcasting) and ETSI [1] are typically based on 4-layer key management architecture illustrated in Fig. 2.1:

- Layer 1 provides client-server mutual authentication and session key (SK) establishment.
- Layer 2 is responsible for provisioning of group management key (GMK) to a client that is authorized to access selected multicast broadcast service (i.e. to every member of an associated multicast broadcast group).
- Layer 3 is in charge of distributing traffic encryption keys (TEKs) under GMK, and
- Layer 4 delivers TEK encrypted content.

From a performance perspective, operation of layer 2 and layer 3 induce significant amount of key management messages to pass over interaction (unicast) and broadcast channels. Each time a user (client) joins or leaves a multicast broadcast service, the server typically generates and unicasts new GMK to each connected group member.

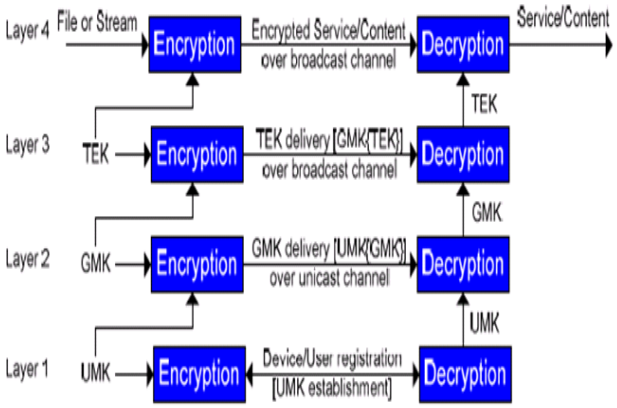

Figure 2.1. Mobile broadcasting security architecture.

In addition, the server updates TEK periodically or occasionally. While GMK lifetime may largely depend on a client's average session time, TEK lifetime should be in order of seconds to ensure fine granularity of access control to the encrypted content.

Recent studies have focused on reducing the number and the size of messages carrying GMKs and TEKs over interaction and broadcast channels. However, present solutions often fail to handle transmission overhead by sacrificing required security level or loosely address the case of group key updates caused by client's leaving its multicast group.

III. MOTIVATION AND PROBLEM DEFENITION

Motivation:

Recent studies have focused on reducing the number and the size of messages carrying GMKs and TEKs over interaction and broadcast channels. However, present solutions often fail to handle transmission overhead by sacrificing required security level or loosely address the case of group key updates caused by client's leaving its multicast group.

The basic motive is to propose a framework that introduces a novel 2-way Hash Chains Scheme (2HCS) that constitutes key generation and management scheme based on cryptographic hash functions and aims to address above issues efficiently and also to provide an outline of the security properties of 2HCS.

Problem Definition / Objective:

- To propose new approach to key management, called 2-way Hash Chains Scheme (2HCS), which effectively reduces the number and the size of keying messages and shows considerable performance improvement over its predecessors.
- To avoid potential misuse of the access credentials. In addition, the 2HCS as well as any of the current key distribution solutions should be accompanied by strong key wrapping algorithms.
- To propose a flexible and powerful key management scheme for mobile broadcast and multicast service which provides high security level and shows outstanding performance among its peer solutions.

IV. PROPOSED TECHNOLOGY

2-Way Hash Chains Based Kms

Cryptographic hash functions have been widely used in a various security applications such as integrity protection and authentication. Below shows, how to use two hash chains to reduce key management overhead in BMS.

Operation

In 2HCS, GMK is represented by the Key Seed Pair (KSP). KSP is a 2-tuple {□□1,2}, where □□1 and □□2 are random key seeds generated and 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 and the server [2].

The operation of 2HCS is based on the below TEK generation mechanism and the BCAST service provisioning model:

- The client performs mutual authentication with the server that results in the establishment of unique SK between client and server.
- The client sends a service request (protected under SK) to join a selected multicast broadcast group.
- If the service requested is validated and processed successfully, the server provisions associated KSP to the client.
- After receiving the KSP from the server, the client calculates granted number of TEKs and is ready to consume multicast broadcast contents.

Note that, in a service with long operational time, the server will periodically provision new KSP to each connected client. If a client would like to connect to a service that has already started or to get access to shorter service interval, then the server will only provision a pair of intermediate hash values, called Access Value Pair (AVP), to the client. AVP is a 2-tuple {□□,+□}, where □ equals the index of the TEK used for encryption when the client connects to a service, and □ is the length of the access interval (in the number of associated TEKs).

Algorithm of proposed Technology: To generate Traffic Encryption Key (TEK) :

Step 1: KSP is a 2-tuple {ks1, ks2} – random key seeds.

Step 2: Design hash function H() [SHA2].

Step 3: Apply H() , n times to KS1 to produce {Si}

i.e., Forward Hash Chain (FHC)

S1 = H(KS1)

For i=2 to n

Si = H(Si-1)

Step 4: Apply step 2 for KS2 to produce {Hj}

i.e., Reverse Hash Chain (RHC)

Mn = H(KS2)

For j = n…..2

Mj-1 = H(Mj)

Step 5: TEK, are derived as-

TEKk = Sk xor Mk for K= 1….

V. RESULTS AND ANALYSIS

GRAPHS

Graph 1: Figure 5.1 depicts the Multicast output graph showing the time taken by the server to transmit messages of various lengths.

Analysis: Figure 5.1 shows that as the message length of the message increases then the time taken by the server to send that message to all the other clients of selected group will also increases.

ID	mesg_type	mesg_len	timetaken
58	g1	1	2
59	g1	1	23
60	g1	9	31
61	g1	18	52
62	g1	27	58
63	g1	36	89
64	g1	45	104

Table 5.1: multicast message length v/s Time taken

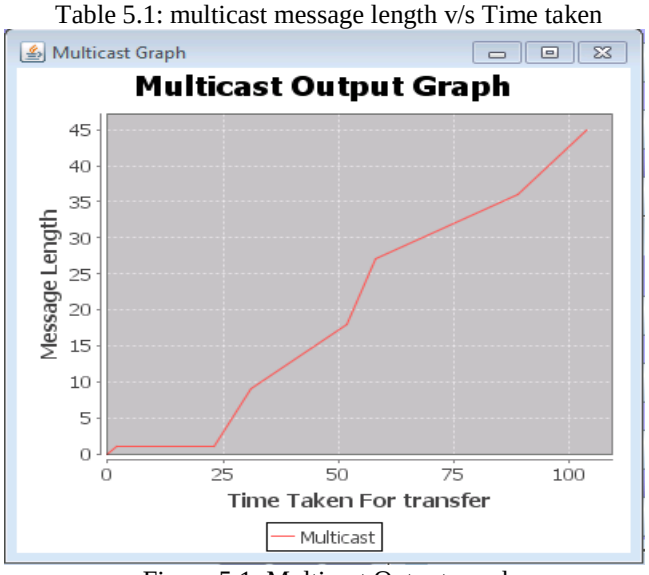

Figure 5.1: Multicast Output graph

Graph 2: Figure 5.2 depicts the Broadcast Output graph showing the time taken by the server to transmit messages of various lengths.

Analysis: Figure 5.2 shows that as the message length of the message increases then the time taken by the server to send that message to all the other clients connected to the server will also increases.

ID	mesg_type	mesg_len	timetaken	Add New Field
65	b	1	9	
66	b	7	25	
67	b	13	35	
68	b	19	56	
69	b	25	69	

Table 5.2: Broadcast message length v/s Time taken

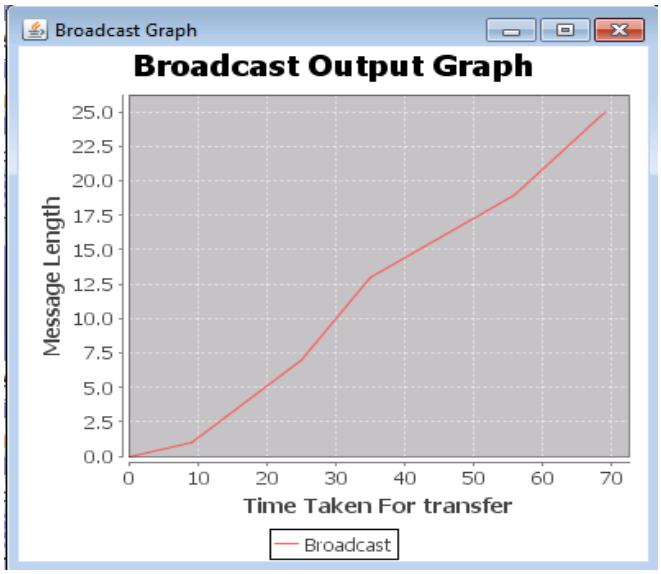

Figure 5.2: Broadcast output graph

VI. CONCLUSION

This thesis proposes a flexible and powerful key management scheme called 2-way Hash Chains Scheme (2HCS) for mobile broadcast and multicast services which effectively reduces the number and the size of keying messages and shows considerable performance improvement over its predecessors and it also provides high security level and shows outstanding performance among its peer solutions.

Even the transmission overhead caused by distribution of associated key material over broadcast and interaction channels is reduced.

REFFERENCES

[1] 3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS), Release 7, 3GPP TS 33.246, Dec. 2007.

[2] Digital Video Broadcasting (DVB): Transmission System for Handheld Terminals (DVB-H), ETSI EN 302 304, Nov. 2004.

[3] Service and Content Protection for Mobile Broadcast Services, OMA TS BCAST SvcCntProtection v1.0, Dec. 2008.

[4] D. J. Huang and D. Medhi, "A key-chain-based keying scheme for many-to- many secure group communication," ACM Trans. Inf. Syst. Security, vol. 7, no. 4, pp. 423-552, Nov. 2004.

[5] R. Dutta, E. C. Chang, and S. Mukhopadhyay, "Efficient self-healing key distribution with revocation for wireless sensor networks using one-way key chains," ACM Trans. Inf. Syst. Security, vol. 7, no. 4, pp. 423-552, Nov. 2004.

[6] H. Lu, "A novel high-order tree for secure multicast key management," IEEE Trans. Comput., vol. 54, no. 2, pp. 214-224, Feb. 2005.

[7] C. K. Cheng, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," IEEE/ACM Trans. Networking, vol. 8, no. 1, pp. 16-30, Sep. 2000.

[8] S. M. Cheng, W. R. Lai, P. Lin, and K. C. Chen, "Key management for UMTS MBMS," IEEE Trans. Wireless Commun., vol. 7, pp. 3619-3628, Sep. 2008.