Reusable Key Management Technique for Secured Wireless Computer Communication

S.Afrin Banu

Anna University Tirunelveli.
Nagercoil-3, K.K Dist Tamilnadu,India.

afrinbanu1986@gmail.com

***Abstract*- Wireless communication is used to transfer information over short distances that is a few meters as in television remote control or long distances for thousands or millions of kilometers for radio communications. It includes GPS units, garage door openers and or garage doors, wireless computer mice, keyboards and headsets, satellite television and cordless telephones. Wireless communication in computers is an effective approach for disseminating data to a number of users. To provide secure access to data in wireless broadcast services, symmetric-key based encryption is used. symmetric-key based encryption is used to ensure that only users who own the valid keys can decrypt the data With regard to various subscriptions as the efficient key management for distributing and changing keys is in great demand for access control in computer broadcasting services . The proposed system uses the efficient key management scheme, called key tree reuse (KTR), to handle the key distribution with regard to complex subscription options and user activities. KTR has many advantages as it is scalable, efficient and secure as it lets multiple programs to share a single tree. So that the users subscribing these programs can use only minimum number of keys**

Keywords- Wireless broadcast, key management, key hierarchy, secure group communication, key distribution

I. INTRODUCTION

In computer communication services, the basic data unit is a data item. The data items are grouped in to programs, and the user specifies the required program to perform the specific task. A user may subscribe to one or more programs and the set of subscribed programs are called the user's subscription. The users can communicate through the Internet or uplink channels to specify the programs that they are interested in receiving. Wireless data broadcast services have mainly focused on performance issues such as reducing data access latency and conserving the battery power of mobile devices but the critical security requirements of this type of broadcast services have not yet been addressed as the service providers need to ensure backward and forward secrecy, with respect to membership dynamics.

In the wireless broadcast environment, any user can monitor the broadcast channel and record the broadcast data. If the data is not encrypted, the content is open to the public, and anyone can access the data . In addition, a user may only subscribe to a few programs. If data in other programs are not encrypted, the user can obtain data beyond his subscription privilege. Subscription is a messaging pattern in which the senders of messages do not program the messages to be sent directly to specific receivers or subscribers. The basic wireless data broadcasting system is shown in figure-1.

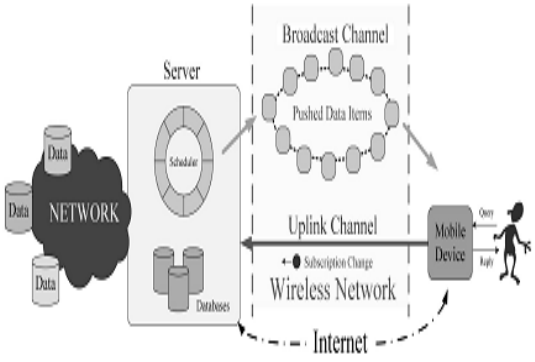

Fig.1.A wireless data broadcast system.

The published messages are characterized into classes and the access control should been forced by encrypting the data in a proper ways such that only subscribing users can access the broadcast data, and subscribing users can only access the data to which they subscribe.

II. LITERATURE SURVEY

Logical Key Hierarchy (LKH) uses a key tree for each group of users who subscribe the same program. The root (top node) of the tree is the data encryption key (DEK) of the program. Each leaf(bottom node) in the tree represents the individual key (IDK) of a user that is only shared between the system and the user. This

operation is called rekey, and the broadcast message of new keys is called rekey message. Kimetal [6] proposed a combination of key tree and Diffie-Hellman key exchange to provide a simple fault-tolerant key agreement for collaborative groups. The working [2] reduces the number of rekey messages, while [9] and [2] improve the reliability of rekey management. Balanced and unbalanced key trees are discussed in [5] and[2]. Periodic group rekeying is studied in[7] and [8] to reduce the rekey cost for groups with frequent joins and leaves. Issues on how a key tree is maintained and how encrypted keys are efficiently placed in multicast rekey packets are studied in [8] and [2] Moreover, the performance of LKH is thoroughly studied [3],[8]. In broadcast Encryption, there are some key management schemes in the literature for multicast and broadcast services. Briscoe [2] used arbitrarily revealed key sequences to do scalable multicast key management without any over head on joins leaves. Wool[8] proposed two schemes that insert an index head in to packets for decryption. Lubyand Staddon[7] proposed a scheme for yield in gmaximal resilience again starbitrary coalition so for on privileged users. However, the size(entropy) of its broadcast key messages large, at least a zero-message scheme [7], [8] which does not require the broadcast server to disseminate any message in order to generate a common key.

III. Proposed System

In the proposed system, the communication mechanism includes wireless broadcast channels and (optional) uplink channels. In the broadcast channels, the main mechanism for data dissemination is that users can recover lost or missed data items. The uplink channels, which have limited bandwidth, are reserved for occasional uses to dynamically change subscriptions. the ever-growing popularity of smart mobile devices ,along with the rapid advent of wireless technology, there has been an increasing interest in wireless data services among both industrial and academic communities in recent years .Among various approaches, broadcast allow save efficient usage of the scarce wireless bandwidth, because it allows simultaneous access by an arbitrary number of mobile clients. Wireless data broadcast services have been available as commercial products for many years. It includes, the following,

A. Key Forest

In order to address scalability and flexibility in key management, an intuitive solution is to use a key tree for each program.LKH[7] is used as the basis of our scheme., but when the user u1 subscribes to two programs simultaneously, he needs to manage two sets of keys in both trees, which is not very efficient , hence, SKT is proposed to reduce this cost in key management. We let the two programs share the same sub key tree, so that users subscribing to both programs only need to manage the keys in the gray triangle.

The advantage of SKT is that any user subscribing to both g1 and g2 only needs to manage one set of keys for both programs. Moreover, when a user joins or leaves a tree shared by multiple programs the encryption and communication cost for rekey operations can be significantly less than conventional LKH approaches fig 2. In order to ensure that a user will not pay for subscribed programs multiple times; the key forest obviously should have the following properties, which are guaranteed in any directed acyclic graph which is an abstract representation of a set of objects where some pairs of the objects are connected by links.

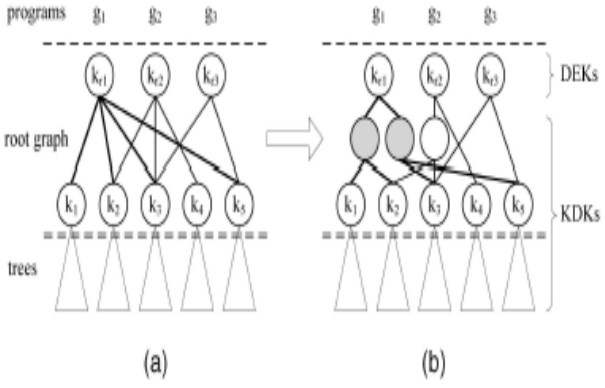

Fig. 2. Multilayer root graph.

B. Rekey Operations

The user activities of joining or leaving or shifting among trees instead of joining or quitting or changing among programs is the mapping between the tree-oriented operations and the corresponding program-oriented user events. When a user us shifts from tr4 to tr6 and when us was in tr4, us subscribed g1 and g2, he shifts to tr6, he subscribes g1, g2, and g3, the shift, in fact, means that the user adds g3 into his current subscription. This has the ability to change a lock so that a different key may operate it.

IV. Performance Evaluation

This is the process of obtaining, analyzing, and recording information about the relative worth of the system. It is the analysis of successes and failures and suitability for further improvement. The performance of KTR at the server side and the client side, respectively are analyzed.

A. Server Side Analysis

This is the analysis done on a computer program running as a service, to serve the needs or requests of other programs which may or may not be running on the same computer. Since a server is generally abundant in energy and memory, its computation capacity becomes the main factor that affects the performance of the whole system. If the processing time for each event is large, this would delay a user's request. We measured the management cost of a server by two metrics which is the total number of keys to be managed and the number of keys to be inspected and updated per rekey event.

1) *Simulation1*

The simulations can be done on a server which is a computer with a 2-GHz CPU and a 2-Gbyte RAM running Linux but on the average, the server uses tens of milliseconds for one rekey operation in the KTR scheme in which the simulation results for two services with 10,000 users. The first row is a small service that provides only 5 programs and 31 valid trees, and each tree is shared by 2.5 programs on the average. The second row is a large service that provides 50 programs and 300 valid trees, and each tree is shared by 12 programs on the average.

A. Client Side Analysis

There are some main performance metrics that are to be measured. They are , the average rekey message size per event, average number of decryption per event per user, and maximum number of keys to be stored which can well capture the overhead of KTR on resource-limited mobile devices in terms of communication, storage, power consumption, and computation. Based onthe metrics, we can infer other metrics that are more directly related to the mobile devices. We can obtain metrics such as the communication overhead in the rekey messages.

1) Simulation2

In the simulation, we compare KTR with three other representative schemes. They are SKT, eLKH, LKH. SKT is the approach in where only SKT is applied. That is its average number of decryption per event per user is the smallest which requires least storage in mobile devices because a mobile receiver generally has limited resources so that they can have a longer working duration and more computation capacity to process broadcast data.

V. ADVANTAGES

The simulation shows that KTR can save about 45 percent of communication overhead in the broadcast channel and also 50 percent of decryption cost for each user as compared with the traditional LKH approach. This approach is also applicable to other LKH-based approaches to reduce the rekey cost as in KTR. And also eLKH is an approach where only a critical key is applied to enhance LKH. Neither SKT nor a critical key is adopted in LKH. If SKT is adopted, key management is based on the key forest. A key tree is created for each program, and a user is assigned to all trees corresponding to the programs that the subscribes. If critical key is used, a key in an enroll path is changed if and only if it is a critical key.

To solve this, we use a multilayer structure to connect the DEK with the roots of the shared trees. As in Fig. 3, kg1 is connected with kr1 , kr2; kr3 , and kr5 via two intermediate key nodes . Such a multilayer structure inherently exploits the advantages of LKH. For different programs, the number of intermediate nodes and the number of layers may be different, which is obviously determined by the number of trees to which the program is connected.

KTR combines the advantages of both SKT and critical key. This scheme has a light communication overhead which incurs less computation and power consumption on mobile devices rather than the other schemes.

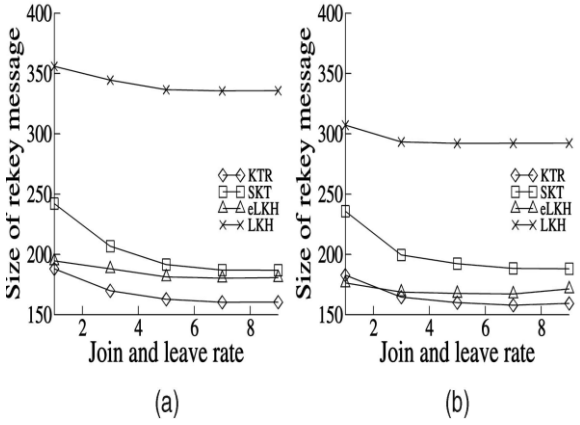

Fig. 3. Average rekey message size per event.
(a) Case 1 , (b)Case 2.

group key management should satisfy four security properties

1. Non-group confidentiality,
2. Collusion freedom,
3. Future confidentiality (forward secrecy), and. past confidentiality (backward secrecy).

VI. CONCLUSION AND FUTURE WORKS

The issues of key management in support of secure wireless broadcast services. We proposed the KTR as a scalable, efficient, and secure key management approach in the broadcast system. We used the key forest to

exploit the overlapping nature between users and programs in broadcast services. KTR lets multiple programs share a single tree so that the users subscribing these programs can hold fewer keys. In addition, we proposed a novel shared key management approach to further reduce rekey cost by identifying the minimum set of keys that must be changed to ensure broadcast security. This approach is also applicable to other LKH-based approaches to reduce the rekey cost as in KTR.

REFERENCES

[1] J. Xu, D. Lee, Q. Hu, and W.-C. Lee, "Data Broadcast," Handbookof Wireless Networks and Mobile Computing, I. Stojmenovic, ed.,John Wiley & Sons, pp. 243-265, 2002.

[2] D. Wallner, E. Harder, and R. Agee, Key Management for Multicast: Issues and Architectures, IETF RFC 2627, 1999.

[3] J. Snoeyink, S. Suri, and G. Varghese, "A Lower Bound forMulticast Key Distribution," Proc. IEEE INFOCOM '01, vol. 1.

[4] LeinHarn and ChangluLin "Authenticated Group Key Transfer Protocol Based On SecretSharing " IEEE Transactions On Computers, Vol. 59, No. 6, June 2010

[5] Xingyu Li and H,Vicky Zhao "An Efficient Key Management Scheme For Live Streaming" IEEE Communications Society,IEEE "Globecom" 2009

[6] Ohtake,Goichiro Hanaoka, and Kazuto Ogawa "An Efficient Provider Authentication ForBidirectional Broadcasting Service" IEEE Transactions On Broadcasting,January2009

[7] Xiaoguang Niu , Yanmin Zhu , Li Cui , Lionel M. Ni "FKM: A Fingerprint-based KeyManagement Protocol for SoC-based Sensor Networks"IEEE Communications Society, IEEE 2009

[8] Xukai Zou Elisa Berti Yuan-Shun Dai "A Practical and Flexible Key Management Mechanism For Trusted Collaborative Computing" IEEE Communications Society, IEEE "Globecom" 2009