ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Survey on Wireless Broadcast Services

G. Surender[*1], N.SriHariRao[2]
[*1,2] CMR Institute of Technology, Hyderabad, Andhra Pradesh, India

Abstract

In a mobile wireless communication network, broadcast signaling can be transmitted to multiple (two or more) receivers simultaneously. In networking, a distinction is made between broadcasting and multicasting. Broadcasting sends a message to everyone on the network whereas multicasting sends a message to a select list of recipients. In this paper we mainly focus on different techniques and algorithms that are already known.

Keywords: Cellular Network, Broadcasting and Multicasting.

Introduction

Broadcasting is that the distribution of audio and video content to a distributed audience via any audio or visual mass communications medium, However sometimes one using electromagnetic radiation. The receiving parties may include the general public or a comparatively large subset thereof. Broadcasting has been used for purposes of private recreation, non-commercial exchange of messages, experimentation, self-training, and emergency communication such as amateur radio and amateur television in addition to commercial purposes like popular radio or TV stations with advertisements.With 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 allows a very 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. In particular, the announcement of the MSN Direct Service has further highlighted the industrial interest in and feasibility of utilizing broadcast for wireless data services.

A wireless data broadcast system consists of three components as depicted in Figure 1: (1) the broadcast server; (2) the mobile devices; and (3) the communication mechanism. The server broadcasts data on air.

A user's mobile device receives the broadcast information, and filters the subscribed data according to user's queries and privileges. The specialty of the broadcast system is that (a) the server determines the schedule to broadcast all data on air, and (b) users' mobile devices listen to the broadcast channel but only retrieve data (filter data out) based on users' queries. The communication mechanism includes wireless broadcast channels and (optional) uplink channels. Broadcast channel is the main mechanism for datadissemination.

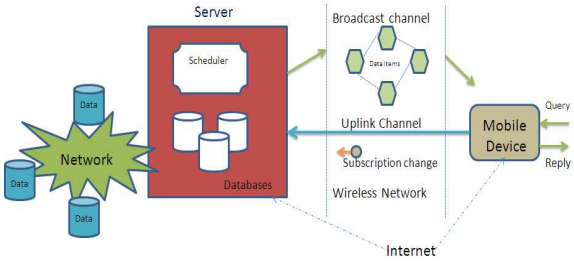

Figure1. A Wireless Data Broadcast server

Data is broadcast periodically so 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. In broadcast services, the basic data unit is data item, such as a piece of news or a stock price. Data items are grouped into programsand a user specifies which programs he would like to access. Typical programs could be weather, news, stock quotes, etc. For simplicity, we assume that each program covers a set of data items, and programs are exclusively complete. A user may subscribe to one or more programs. The set of subscribed programs is called the user's subscription. Users can subscribe via Internet or uplink channels to specify the programs that they are interested in receiving.

Wireless Communication Networks:

In a mobile environment, wireless communication networks are needed to attach to the stationary host and establish communication with the central database server. A variety of wireless communication networks is described in detail as follows:

Cellular Network

Cellular network evolves from generation to generation. The first generation of cellular network (1G) is predicted on analog technology. The voice is transmitted using Frequency Modulation (FM). This technology includes Advance Mobile Phone System (AMPS), Total Access Communication System (TACS), and Nordic Mobile Telephone (NMT).The second generation (2G) includes Time Division Multiple Access (TDMA), and Code Division Multiple Access (CDMA), Global System for Mobile Communications (GSM), and Personal Digital Cellular (PDC). The transmission rate ranges from 9-14 Kbps. The third technology (3G) provides transmission rates from 144 Kbps to 2000 Kbps. This includes Universal Mobile Telecommunication System (UMTS), the Code Division Multiple Access 2000, and the NTT DoCoMo of Japan [7] [9].

Radio Network

Radio Network can be classified into two classes namely, Public Packet Data Network, and Private Packet Data Network. This type of network only provides data transmission and utilizes base stations, network control, Centre's, and switches infrastructure for data transmission .Examples of Public Packet Data Network include Ericsson's Enhanced Digital Access Communication Systems (EDACS), and so on (Sharma, 2001). The average data rate for this network is between 4800 bps and 19.2Kbps.The Private Packet Data Network is a private organization or company that established the network for its own use [8].

Wireless LAN Network

Currently, of all the networks, Wireless LAN network provides the highest speed in communication. However, WLANs is not designed to support true quality is additional involved with providing a wireless interface or bridge to the wired networks.The institute of Electrical and Electronics Engineers (IEEE) 802.11 standard for wireless LANs focuses on medium-range but high data rate applications .IEEE802.11 is presently the dominant approach utilized in providing an Ethernet-like wireless networking environment [7] [9] [10].

Satellite

Satellite technology ordinarily provides long latency, wide-range, and high cost. However, it has a limited quality voice or data.The long latency is due to the long distance that incorporates propagation delay for data transmission [8].

Literature Survey

Jack Snoeyink et al. [1] analyzed a lower bound is additionally necessary for a general category of key distribution schemes. Whereas key distribution schemes will trade addition value for deletion cost, for any scheme there is a sequence of 2n insertion and deletions whose total cost is $\Omega(n \log n)$. Thus, any key distribution scheme contains a worst-case value of $\Omega(\log n)$ either for adding or for deleting a user. The thought of broadcasting extends to a network of point-to-point links, such as the web. For instance, source S can send a message to the group $N1 \ldots N4$, by sending a single copy of the message to the router, which might then built 3 copies of the message, one for the link to $N1$,$N2$ respectively and one for the broadcast link to which $N3$ and $N4$ are connected. Thus, messages are sent on a "Steiner tree," with routers creating multiple copies of messages at branching pointswithin the tree. This provides a bandwidth reduction from 4 to 1 on the common link from S to the router. It might be better if deletion from a group of size n should be accomplished in one message, then keys must bemaintained for all subsets of size $n - 1$.Multicast key can be a broadcast channel that permits a sender to communicate with every user which will hear the channel employing a single broadcast message. A satellite link includes a news source to broadcast to any or all users in the shadow of the satellite, cable TV, microwave, and therefore the LAN.

Melekonen et al. [2] described to reorganize the Logical Key Hierarchy (LKH) scheme by on an individual basis regrouping members supported their membership duration aiming at conserving members with long duration membership from the impact of rekeying operations caused by arrivals or departures of transient members and used an easy definition of loyalty wherever one willclassify members with regards to their membership duration.So as to assure high reliability for members staying in group, firstly restructure the key tree and split the tree into two different groups with regards to members' membership duration. The reliability assurance for members of every total different set can increase proportionally with the membership duration of the corresponding members.During this LKH scheme, due to the inherent strong dependency between keys of different subsequent intervals, all members suffer from rekey packet losses regardless of their membership duration.

Dalit Naor et al. [3] developed a framework referred to as Subset-Cover framework that abstracts a spread of revocation schemes together with the matter of a center sending a message to a group of users such that some subset of the users is considered revoked and will not be able to acquire the content of the message. During this technique subset cover algorithm has been used particularly for suitable stateless receivers where the performance of the second technique is considerably higher than any broadcast encryption algorithms. The

main improvements of this algorithm over previous ones are (1) reducing themessage length to O(r) regardless of the coalition size while maintaining a single decryption at the user's end (2) offer a seamless integration between the revocation and tracing so that the tracing mechanisms does not need any change to the revocation algorithm.

Avishai Wool [4] mentioned broadcast applications wherever the transmissions got to be encrypted, like direct broadcast digital TV networks or Internet multicasts. Hera a user who buys a package should be able to view every program belonging to that package, however nothing else. A flexible scheme must allow for packages of varied sizes to be offered, from a single program up to any or all the programs. So we use a set-top terminals (STT) contains a secure chip, either directly or on a smart-card, which has a secure memory for the entitlements. This memory ought to be non-volatile, writable and tamper-resistant so as to use the number of programs say 20,000 or more, additional number of keys to be managed throughout broadcast and try to achieve flexibility and security.

Chung Kei Wong et al.[5] planneda completely uniqueresolution to the scalability problem of group/multicast key management like teleconference, information services, distributed interactive simulation, and collaborative work. Currentlyallow us to consider for a group of members, distributing the group key securely to all members requires 'n' messages encrypted with individual keys. Every such message is also sent separately via unicast. Instead, the messages are also sent as a combined message to all group members via multicast. Either way, there is a communication cost proportional to group size 'n'. Observe that for a point-to-point session, the costs of session establishment and key distribution are incurred just once, at the beginning of the session. A group session, on the other hand, may persist for a relatively long time with members joining and leaving the session. Consequently, the group key should be changed frequently. To achieve a high level of security, the group key should be changed after every *join* and *leave* in order that a former group member has no access to current communications and a replacement member has no access to previous communications.

Xiaozhou Steve Li et al. [6] approach is to use of periodic batch rekeyingwhich might improve efficiency and alleviate the out-of-sync problem. In batch rekeying, the key server collects join and leave requests in a period of time and rekeys once a batch has been collected. We devise a marking algorithm to process a batch of requests.Once the size of a batch is not large i.e., roughly, when the number of joins is less than half of current group size, and the number of leaves is less than a quarter of current group size, four is that the best key tree degree; otherwise, key star outperforms small-degree key trees.

Conclusion

To provide secure access to data in wireless broadcast services, several techniques have been mentioned above as a literature survey. In order to overcome the problems, we are coming up with a new concept called an Efficient Key Management Scheme for Secure Data Access Control in Wireless Broadcast Services.

References

[1] J. Snoeyink, S. Suri, and G. Varghese, "A lower bound for multicast keydistribution," in *IEEE Infocom*, vol. 1, 2001, pp. 422–431.

[2] M. Onen and R. Molva, "Reliable group rekeying with a customer perspective," in *IEEE GLOBECOM*, vol. 4, 2004, pp. 2072–2076.

[3] Dalit Naor, MoniNaor, and JeLotspiech, "Revocation and Tracing Schemes for StatelessReceivers", Advances in Cryptology — CRYPTO 2001Lecture Notes in Computer Science Volume 2139, 2001, pp 41-62

[4] A.Wool, "Key management for encrypted broadcast," *ACM Transactions on Information and System Security*, vol. 3, no. 2, pp. 107–134, 2000.

[5] C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communicationsusing key graphs," in *ACM SIGCOMM*, 1998, pp. 68–79.

[6] Y. R. Yang, X. S. Li, X. B. Zhang, and S. S. Lam, "Reliable grouprekeying: a performance analysis," in *ACM SIGCOMM*, 2001, pp. 27–38.

[7] Sharma C., "Wireless Internet Enterprise Applications", John Wiley & Sons Inc., U.S.A., 2001.

[8] Zaslavsky A., and Tari S., "Mobile Computing: Overview and Current Status", Australian Computer Journal, 30(2): 42-52, 1998.

[9] Pitoura E. and Samaras G., "Data Management for Mobile Computing", Kluwer Academic Publishers, London, 1998.

[10] Vaughan-Nichols J. S., "Bull Market for IEEE 802.11 WLAN Chipsets", Computer Magazine, Vol.35, No.11, pp. 17-19, November, 2002.