Efficient Multicast Packet Authentication using Digital Signature

J.Sridevi,
Lecturer, Dept. of IT
College of Engg & Tech,
Pagalavadi, Trichy-621014.
Tamil Nadu,India

R.Mangaiyarkarasi
Asst.Professor, Dept of .CSE Jayaram
Jayaram College of Engg & Tech,
Pagalavadi, Trichy-621014
Tamil Nadu,India

ABSTRACT
Existing digital signature schemes are computationally expensive; the ideal approach of signing and verifying each packet independently raises a serious challenge to resource-constrained devices. In order to reduce computation overhead, conventional schemes use efficient signature algorithms and are vulnerable to packet injection by malicious Here, MABS can achieve perfect resilience to packet loss in lossy channels in the sense that no matter how many packets are lost, the already-received packets can still be authenticated by receivers. Basic scheme MABS-B is efficient in terms of latency, computation and communication overhead. An enhanced scheme called MABS-E combines the basic scheme MABS-B and a packet filtering mechanism to tolerate packet injection.

Keywords
Multicast, authentication, signature

1. INTRODUCTION
The efficient method to deliver multimedia content from a sender to a group of receivers is multicasting. It has several applications such as real time stock quotes, interactive games, video conference, live video broadcast, or video on demand. Multicast authentication may provide three security services such as data integrity, data origin authentication, Non repudiation. The sender generates a signature for each packet with its private key, which is called signing, and each receiver checks the validity of the signature with the sender's public key, which is called verifying. If the verification succeeds, the receiver knows the packet is authentic.

There are following issues in real world challenging the design. First, efficiency needs to be considered, especially for receivers. Compared with the multicast sender, which could be a powerful server, receivers can have different capabilities and resources.. Second, packet loss is inevitable. In the Internet, congestion at routers is a major reason causing packet loss. Constant service interruptions may be caused due to packet losses.

Though TCP provides a certain retransmission capability, multicast content is mainly transmitted over UDP, which does not provide any loss recovery support. In mobile environments, the situation is even worse. The instability of wireless channel can cause packet loss very frequently. Moreover, the smaller data rate of wireless channel increases the congestion possibility. This is not desirable for applications like real-time online streaming or stock quotes delivering. End users

Existing digital signature algorithms are computationally expensive; the ideal approach of signing and verifying each packet independently raises a serious challenge to resource-constrained devices. In order to reduce computation overhead, conventional schemes use efficient signature algorithms and are vulnerable to packet injection by malicious attackers. An attacker may compromise a multicast system by intentionally injecting forged packets to consume receivers' resource, leading to Denial of Service (DoS). Compared with the efficiency requirement and packet loss problems, the DoS attack is not common, but it is still important in hostile environments.

A novel multicast authentication protocol called MABS (in short for Multicast Authentication based on Batch Signature) is used. MABS includes two schemes. The basic scheme (called MABS-B hereafter) utilizes an efficient asymmetric cryptographic primitive called batch signature which supports the authentication of any number of packets simultaneously with one signature verification, to address the efficiency and packet loss problems in general environments. The enhanced scheme (called MABS-E hereafter) combines MABS-B with packet filtering to alleviate the DoS impact in hostile environments. MABS provides data integrity, origin authentication, and non-repudiation, specialized application; it is often constructed with the aid of general-purpose grid software libraries and middleware.

2. BASIC SCHEME
The goal is to authenticate multicast streams from a sender to multiple receivers. Generally, the sender is a powerful multicast server managed by a central authority and can be trustful. The sender signs each packet with a signature and transmits it to multiple receivers through a multicast routing protocol. Each receiver needs to assure that the received packets are really from the sender (authenticity) and the sender cannot deny the signing operation by verifying the corresponding signatures. Ideally, authenticating a multicast stream can be achieved by signing and verifying each packet. However, the per-packet signature design has been criticized for its high computation cost, and therefore, most previous schemes incorporate a block-based design.

They do reduce the computation cost, but also introduce new problems. The block design builds up correlation among packets and makes them vulnerable to packet loss, which is inherent in the Internet and wireless networks. Received packets may not be authenticated because some correlated packets are lost. Also, the heterogeneity of receivers means that the buffer resource at each receiver is different and can vary over the time depending on the overall load at the receiver. In the block design, the required

block size, which is chosen by the sender, may not be satisfied by each receiver.

Third, the correlation among packets can incur additional latency. Consider the high layer application needs new data from the low layer authentication module in order to render a smooth video stream to the client user. It is desirable that the lower layer authentication module delivers authenticated packets to the high layer application at the time when the high layer application needs new data. In the per-packet signature design it is not a problem, since each packet can be independently verifiable at any time. In the block design, however, it is possible that the packets buffered at the low layer authentication module are not verifiable because the correlated packets, especially the block signatures, have not been received. Therefore, the high layer application has to either wait, which leads to additional latency, or return with a no-available-packets exception, which could be interpreted as that the buffered packets are "lost." This latency, which is incurred at the high layer when the high layer application waits for the buffered packets to become verifiable, is different from the buffering latency, which is required for the low layer authentication protocol to buffer received packets.

In view of the problems regarding the sender-favoured block-based approach, receiver-oriented approaches by taking into account the heterogeneity of the receivers. As receiving devices have different computation and communication capabilities, some could be powerful desktop computers, while the others could be cheap handsets with limited buffers and low-end CPUs. Mixed with various channel loss rates, this heterogeneity poses a demand on the capability of adjusting the buffer size and authenticating buffered packets any time when the high layer application requires at each receiver.

The computation complexity of BatchVerify() comes with the fact that there are some additional cost on processing multiple packets.. Batch size is chosen by each receiver, which can optimize its own batch size, so that the batch size will not be unmanageably large. Batch BLS Signature

Here, we propose a batch signature scheme based on the BLS signature.

2.1.1 BLS

1. Key generation

The key generation algorithm selects a random integer x in the interval [0, r − 1]. The private key is x. The holder of the private key publishes the public key, g_x.

2. Signing

Given the private key x, and some message m, we compute the signature by hashing the bitstring m, as h = H(m). We output the signature $\sigma = h_x$.

3. Verification

Given a signature σ and a public key g_x, we verify that $e(\sigma,g) = e(H(m),g_x)$.

2.1.2 Batch BLS

- Based on BLS, we propose our batch BLS scheme here.
- Given n packets {mi, σ i},i=1,…n,
  1. Compute hi=h(mi),i=1,…n
  2. Check whether $e(\Pi^{n}_{i=1} \sigma,g) = e(\Pi^{n}_{i=1} H(m),g_x)$.

3. ENHANCED SCHEME

The basic scheme MABS-B has perfect resilience to packet loss irrespective of the type of losses In such situations, an attacker can inject forged packets into a batch of packets to disrupt the batch signature verification, leading to DoS. An approach to defeat the DoS attack is to divide the batch into multiple smaller batches and perform batch verification over each smaller batch, and this divide-and-conquer approach can be recursively carried out for each smaller batch In the worst case, the attacker can inject forged packets at very high frequency and expect that each receiver stops the batch operation and recovers the basic per-packet signature verification, which may not be viable at resource-constrained receiver devices.

An enhanced scheme called MABS-E combines the basic scheme MABS-B and a packet filtering mechanism to tolerate packet injection. In particular, the sender attaches each packet with a mark, which is unique to the packet and cannot be spoofed. At each receiver, the multicast stream is classified into disjoint sets based on marks. Each set of packets comes from either the real sender or the attacker. The mark design ensures that a packet from the real sender never falls into any set of packets from the attacker, and vice versa. Next, each receiver only needs to perform BatchVerify() over each set. If the result is True, the set of packets is authentic. If not, the set of packets is from the attacker, and the receiver simply drops them and does not need to divide the set into smaller subsets for further batch verification. Therefore, a strong resilience to DoS due to injected packets can be provided.

4. EXISTING SYSTEM

Existing block-based multicast authentication schemes overlook the heterogeneity of receivers by letting the sender

1. To choose the block size
2. To divide a multicast stream into blocks
3. Associate each block with a signature and

Spread the effect of the signature across all the packets in the block through hash graphs or coding algorithms.

There are some problems in existing digital signature algorithms. They are computationally expensive. There is also possibility of packet loss, packet forgery by attackers leading to Denial of Service. The approach of signing and verifying each block independently raises a serious challenge to resource-constrained devices. Compared with the efficiency requirement and packet loss problems, the DoS attack is not common, but it is still important in hostile environments.

4.1 Problems in Existing System

- The correlation among packets makes them vulnerable to packet loss, which is inherent in the Internet and wireless networks.
- The lack of Denial of Service (DoS) resilience renders most of them vulnerable to packet injection in hostile environments

5. PROPOSED SYSTEM

Using a batch signature all packets are verified simultaneously. A novel multicast authentication protocol, namely MABS, includes two schemes.

5.1 Basic Scheme (MABS-B)

The basic scheme (MABS-B) eliminates the correlation among packet and thus provides the perfect solution to packet loss. It is also efficient in terms of latency, computation, and communication overhead due to an efficient cryptographic primitive called batch signature, which supports the authentication of any number of packets simultaneously.

5.2 Enhanced scheme (MABS-E)

The Enhanced scheme MABS-E combines the basic scheme with a packet filtering mechanism to avoid the DoS impact

6. SYSTEM ARCHITECTURE

In the network, the messages are split into packets. Every signed message from the sender goes to the receiver via the router. The router contacts the administrator which acts as the arbiter and subjects the message and its signature to a number of tests to check its origin and content. The message is then dated and sent to the receiver with an indication that it has been verified to the satisfaction of the administrator. When the packets are multicasted, the router verifies the signature with the help of signatures available in database. No information is shared among the parties before communication, preventing alliances to defraud. No incorrectly dated message can be sent. The content of the message from the sender to receiver is secret from administrator and anyone else.

An enhanced scheme called MABS-E, which combines the basic scheme MABS-B and a packet filtering mechanism to tolerate packet injection. In particular, the sender attaches each packet with a mark, which is unique to the packet and cannot be spoofed. At each receiver, the multicast stream is classified into disjoint sets based on marks. Each set of packets comes from either the real sender or the attacker. The mark design ensures that a packet from the real sender never falls into any set of packets from the attacker, and vice versa. Next, each receiver only needs to perform BatchVerify() over each set. If the result is True, the set of packets is authentic. If not, the set of packets is from the attacker, and the receiver simply drops them and does not need to divide the set into smaller subsets for further batch verification. Therefore, a strong resilience to DoS due to injected packets can be provided.

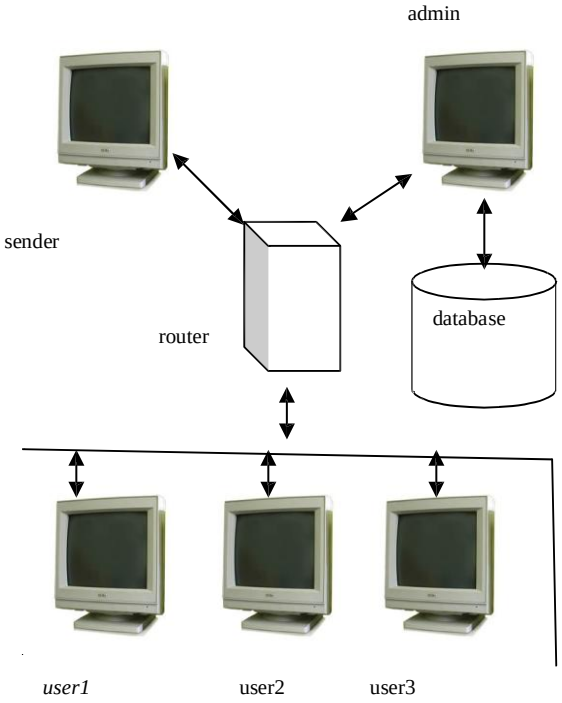

Fig.1 Architecture diagram

7. CONCLUSION

While transmitting data in a network, existing system faces some problems like signature verification, congestion, computing block size, vulnerability to packet loss and lack of resilience to denial of service (DoS) attack. To overcome these problems related research papers have been studied.. A novel authentication scheme called MABS is used in the proposed system. MABS will be a perfect solution to packet loss due to the elimination of the correlation among packets and can effectively deal with DoS attack. Moreover, the use of batch signature can achieve the efficiency comparable with the conventional schemes. Finally, further two new batch signature schemes based on BLS and DSA are developed which are more efficient than the batch RSA signature scheme. RSA algorithm can only be applied for text files. So a new and efficient algorithm called Elliptic Curve Cryptography(ECC) which can also applied for other files like ppt,pdf files,etc can be used. Finally, Batch BLS implemented over ECC is used.

8. REFERENCES

[1] Challal. Y, Bettahar. H, and Bouabdallah.. A.,"A Taxonomy of Multicast Data Origin Authentication: Issues and Solutions," IEEE Comm. Surveys & Tutorials,vol. 6,no. 3, pp. 34-57, Oct. 2004.

[2] Challal. Y, Bettahar.H, and Bouabdallah.A., "A^2Cast: An Adaptive Source Authentication Protocol for Multicast Streams," Proc. Ninth Int'l Symp. Computers and Comm. (ISCC '04), vol. 1, pp. 363-368, June 2004.

[3] Choi S., "Denial-of-Service ResistantMulticast Authentication Protocol with Prediction Hashing and One-Way Key Chain," Proc.. Seventh IEEE Int'l Symp. Multimedia (ISM '05), Dec. 2005.

[4] Judge. P and Ammar. M, "Security Issues and Solutions in Mulicast Content Distribution: A Survey," IEEE Network Magazine, vol. 17, no. 1, pp.30-36, Jan./Feb. 2003.

[5] Karlof. C, Sastry. N, Li. Y, Perrig. A, and Tygar. J. D, "Distillation Codes and Applications to DoS Resistant Multicast Authentication," Proc.. 11th Ann. Network and Distributed System Security Symp. (NDSS '04), Feb.2004

[6] Perrig. A,Canetti. R, Tygar. J D. and Song. D, "EfficientAuthenticationand Signing of Multicast Streams over Lossy Channels," Proc.. IEEE Symp. Security and Privacy (SP '00), pp. 56-75, Feb.2004.

[7] Pannetrat. A and Molva. R, "Efficient Multicast Packet Authentication," Proc..10th Ann. Network and Distributed System SecuritySymp.(NDSS'03),Feb2003

[8] Wong. C.K. and Lam. S.S., "Digital Signatures for Flows and Multicasts," IEEE/ACM Trans. Networking, vol. 7, no. 4, pp. 502- 513, Aug.1999.

[9] Zhou. Y and Fang. Y.,"BABRA: Batch-Based Broadcast Authentication in Wireless Sensor Networks," Proc. IEEE GLOBECOM, Nov. 2006.

[10] Zhou. Y and Fang. Y., "Multimedia Broadcast Authentication Based on Batch Signature," IEEE Comm. Magazine, vol. 45, no. 8, pp. 72- 77, Aug. 2007.