A Survey on Authentication Techniqes in focus of Batch Signatures in multicasting

1. M.Vazralu **2.C.Sushma**

Abstract:

Data delivery is we termed casting in generally in network environment. Unicasting will forward the pockets one site at a time while multicasting is used to send the data pockets to multiple destinations at the same time. These casting technics are well equipped and implemented but during the casting data pocket must be authenticated. Authentication must be implemented to multiple pockets at the same time called batch signatures. We are focusing the batch signatures in the paper. The authentication of any number of packets simultaneously with one signature verification, to address the efficiency and packet loss problems in general environments. The authentication consist two methods first one is Basic method it eliminates the correlation among packets and thus provides the perfect resilience to packet loss. Next method is enhanced one which combines the basic scheme with a packet filtering mechanism The enhanced scheme MABS-E combines and MABS-B with packet filtering.

INTRODUCTION

What Is Multicasting?

Multicasting is a technical term that means that you can send a piece of data (a *packet*) to multiple sites at the same time. (How big a packet is depends on the protocols involved-it may range from a few bytes to a few thousand.) The usual way of moving information around the Internet is by using *unicast* protocols -- tools that send packets to one site at a time.

You can think of multicasting as the Internet's version of broadcasting. A site that multicasts information is similar in many ways to a television station that broadcasts its signal. The signal originates from one source, but it can reach everyone in the station's signal area. The signal takes up some of the finite available bandwidth, and anyone who has the right equipment can tune in. The information passes on by those who don't want to catch the signal or don't have the right equipment.

On a multicast network, you can send a single packet of information from one computer for distribution to several other computers, instead of having to send that packet once for every destination. Because 5, 10, or 100 machines can receive the same packet, bandwidth is conserved. Also, when you use multicasting to send a packet, you don't need to know the address of everyone who wants to receive the multicast; instead, you simply "broadcast" it for anyone who is interested. (In addition, you can find out who is receiving the multicast -- something television executives undoubtedly wish they had the capability to do.)

Multicast is an efficient method to deliver multimedia content from a sender to a group of receivers and is gaining popular applications such as real-time stock quotes, interactive games, video conference, live video broadcast, or video on demand. Authentication is one of the critical topics in securing multicast in an environment attractive to malicious attacks.

Basically, multicast authentication may provide the following security services:

1. Data integrity: Each receiver should be able to assure that received packets have not been modified during transmissions.

2. Data origin authentication: Each receiver should be able to assure that each received packet comes from the real sender as it claims.

3. Non-repudiation: The sender of a packet should not be able to deny sending the packet to receivers in case there is a dispute between the sender and receivers. All the three services can be supported by an asymmetric key technique called signature. In an ideal case, 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.

Existing work

Authentication is one of the critical topics in securing multicast in an environment attractive to malicious attacks. An overloaded router drops buffered packets according to its preset control policy. TCP provides a certain retransmission capability; multicast content is mainly transmitted over UDP, which does not provide any loss recovery support. The instability of wireless channel can cause packet loss very frequently. 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 of online streaming will start to complain if they experience constant service interruptions due to packet loss, and missing critical stock quotes can cause severe capital loss of service subscribers. Therefore for applications the quality of service is critical to end users.

Drawbacks

- Authentication is critical for securing multicast environment.
- The smaller data rate of channel increases the congestion possibility in network.
- Does not provide any loss recovery support.

Proposed Approach

The proposed system overcomes the above mentioned drawbacks. MABS (Multicast Authentication based on Batch Signature) 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 combines MABS with packet filtering to alleviate the DoS impact in hostile environments. MABS provides data integrity, origin authentication and nonrepudiation as previous asymmetric key based protocols. 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.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

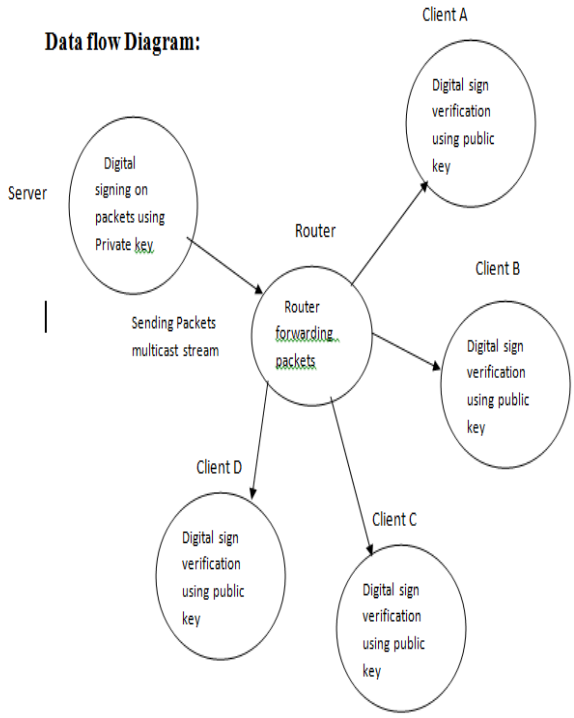
Modules:

1. Network model.

2. DSA key generation.

3. Digital Signature (sending packets)

4. Signature Verification (receiving packets).



Approaches

1. Network model.

Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.

2. DSA key generation:

Key generation has two phases. The first phase is a choice of algorithm parameters which may be shared between different users of the system:

Choose an approved cryptographic hash function H. In the original DSS, H was always SHA-1, but the stronger SHA-2 hash functions are approved for use in the current DSS. The hash output may be truncated to the size of a key pair.

Decide on a key length L and N. This is the primary measure of the cryptographic strength of the key. The original DSS constrained L to be a multiple of 64 between 512 and 1024 (inclusive). Recommends lengths of 2048 (or 3072) for keys with security lifetimes extending beyond 2010 (or 2030), using correspondingly longer N.[3] specifies L and N length pairs of (1024,160), (2048,224), (2048,256), and (3072,256).

3. Digital Signature (sending packets)

Digital signatures employ a type of asymmetric cryptography. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional

handwritten signatures in many respects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes in the sense used here are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless.

4. Signature Verification (receiving packets)

Signature verification may be performed by any party (i.e., the signatory, the intended recipient or any other party) using the signatory's public key. A signatory may wish to verify that the computed signature is correct, perhaps before sending the signed message to the intended recipient.

The intended recipient (or any other party) verifies the signature to determine its authenticity.

Prior to verifying the signature of a signed message, the domain parameters, and the claimed signatory's public key and identity shall be made available to the verifier in an authenticated manner.

The public key may, for example, be obtained in the form of a certificate signed by a trusted entity (e.g., a Certification Authority) or in a face-to-face meeting with the public key owner.

CONCLUSION

To reduce the signature verification overheads in the secure multimedia multicasting, block-based authentication schemes have been proposed. Unfortunately, most previous schemes have many problems such as vulnerability to packet loss and lack of resilience to denial of service (DoS)

attack. To overcome these problems, we develop a novel authentication scheme MABS. We have demonstrated that MABS is perfectly resilient to packet loss due to the elimination of the correlation among packets and can

effectively deal with DoS attack. Moreover, we also show that the use of batch signature can achieve the efficiency less than or comparable with the conventional schemes. Finally, we further develop two new batch signature schemes based on BLS and DSA, which are more efficient than the batch RSA signature scheme.

REFERENCES:

[1] S.E. Deering, "Multicast Routing in Internetworks and Extended
LANs," Proc. ACM SIGCOMM Symp. Comm. Architectures and
Protocols, pp. 55-64, Aug. 1988.
[2] T. Ballardie and J. Crowcroft, "Multicast-Specific Security Threats
and Counter-Measures," Proc. Second Ann. Network and Distributed
System Security Symp. (NDSS '95), pp. 2-16, Feb. 1995.
[3] P. Judge and M. Ammar, "Security Issues and Solutions in
Mulicast Content Distribution: A Survey," IEEE Network Magazine,
vol. 17, no. 1, pp. 30-36, Jan./Feb. 2003.
[4] Y. Challal, H. Bettahar, and A. Bouabdallah, "A Taxonomy of

Multicast Data Origin Authentication: Issues and Solutions," IEEE
Comm. Surveys & Tutorials, vol. 6, no. 3, pp. 34-57, Oct. 2004.
[5] Y. Zhou and Y. Fang, "BABRA: Batch-Based Broadcast Authentication
in Wireless Sensor Networks," Proc. IEEE GLOBECOM,
Nov. 2006.
[6] Y. Zhou and Y. Fang, "Multimedia Broadcast Authentication
Based on Batch Signature," IEEE Comm. Magazine, vol. 45, no. 8,
pp. 72-77, Aug. 2007.
[7] K. Ren, K. Zeng, W. Lou, and P.J. Moran, "On Broadcast
Authentication in Wireless Sensor Networks," Proc. First Ann. Int'l
Conf. Wireless Algorithms, Systems, and Applications (WASA '06),
Aug. 2006.
[8] S. Even, O. Goldreich, and S. Micali, "On-Line/Offline Digital
Signatures," J. Cryptology, vol. 9, pp. 35-67, 1996.
[9] P. Rohatgi, "A Compact and Fast Hybrid Signature Scheme for
Multicast Packet," Proc. Sixth ACM Conf. Computer and Comm.
Security (CCS '99), Nov. 1999.
[10] C.K. Wong and S.S. Lam, "Digital Signatures for Flows and
Multicasts," Proc. Sixth Int'l Conf. Network Protocols (ICNP '98),
pp. 198-209, Oct. 1998.
[11] C.K. Wong and S.S. Lam, "Digital Signatures for Flows and
Multicasts," IEEE/ACM Trans. Networking, vol. 7, no. 4, pp. 502-
513, Aug. 1999.
[12] R. Gennaro and P. Rohatgi, "How to Sign Digital Streams,"
Information and Computation, vol. 165, no. 1, pp. 100-116, Feb. 2001.
[13] R. Gennaro and P. Rohatgi, "How to Sign Digital Streams," Proc.
17th Ann. Cryptology Conf. Advances in Cryptology (CRYPTO '97),
Aug. 1997.
[14] A. Perrig, R. Canetti, J.D. Tygar, and D. Song, "Efficient
Authentication and Signing of Multicast Streams over Lossy
Channels," Proc. IEEE Symp. Security and Privacy (SP '00), pp. 56-
75, May 2000.
[15] Y. Challal, H. Bettahar, and A. Bouabdallah, "A2Cast: 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.
[16] S. Miner and J. Staddon, "Graph-Based Authentication of Digital
Streams," Proc. IEEE Symp. Security and Privacy (SP '01), pp. 232-
246, May 2001.
[17] Z. Zhang, Q. Sun, W-C Wong, J. Apostolopoulos, and S. Wee, "A
Content-Aware Stream Authentication Scheme Optimized for
Distortion and Overhead," Proc. IEEE Int'l Conf. Multimedia and
Expo (ICME '06), pp. 541-544, July 2006.
[18] P. Golle and N. Modadugu, "Authenticating Streamed Data in the
Presence of Random Packet Loss," Proc. Eighth Ann. Network and
Distributed System Security Symp. (NDSS '01), Feb. 2001.
[19] Z. Zhang, Q. Sun, and W-C Wong, "A Proposal of Butterfly-
Graphy Based Stream Authentication over Lossy Networks," Proc.
IEEE Int'l Conf. Multimedia and Expo (ICME '05), July 2005.
[20] S. Ueda, N. Kawaguchi, H. Shigeno, and K. Okada, "Stream
Authentication Scheme for the Use over the IP Telephony," Proc.
18th Int'l Conf. Advanced Information Networking and Application
(AINA '04), vol. 2, pp. 164-169, Mar. 2004.

Authors Profiles

M.Vazralu
M.Tech
Asst. Professor, CSE department
MALLA REDDY COLLEGE OF
ENGINEERING &TECHNOLOGY

C.Sushma
M.Tech student,
MALLA REDDY COLLEGE OF
ENGINEERING &TECHNOLOGY