Multicast Authentication Based on Batch DSA

K. Rajarajan
Department of CSE
Anna University, India

T. M. Thiyagu
Department of CSE
Anna University, India

S. Chandrasekar
Department of CSE
UCET, India

Abstract

A conventional block-based multicast authentication scheme overlooks the heterogeneity of receivers, by letting the sender choose the block size and also divides a multicast stream into blocks. It associates each block with a signature, and spreads the effect of the signature across all the packets in the block through hash graphs or coding algorithms. The correlation among packets makes them vulnerable to packet loss, which is inherent in the Internet and wireless networks. Moreover, the lack of Denial of Service (DoS) flexibility provides most of them vulnerable to packet injection in hostile environments. An efficient method to overcome this vulnerability is to make use of multicast authentication protocol called MABS. MABS helps to overcome this issue by creating batch signature for the packets being multi-casted. This project is aimed to deliver an extended MABS protocol that does packet filtering along with creating batch signature. The batch signature is created using batch DSA which is more efficient than batch RSA.

1. Introduction

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 or video on demand. Multicast enables efficient large-scale content distribution by providing an efficient transport mechanism to communicate between one-to-many and many-to-many communications. Over the years, multicast has been the topic of many research. Today, applications that are of multicast nature have increased (for example: video conferencing, distance learning, pay per view TV, financial stock quote distribution, etc). One of the important tasks for the use of multicast communication is the authenticity.

1.1. Authenticity

Authenticity means that the receiver must be able to verify the identity of the data's source. First level of functionality is for the receiver to be able to verify that the data is from a group member. The next level of functionality is for the receiver to be able to verify that it is from an authorized sender. The most precise functionality is for the receiver to be able to determine the exact identity of the sender.

In case of multicast communication, authentication is a difficult problem, since it requires that a large number of Authentication is one of the critical topics in securing broadcast in mobile computing, an open environment attractive to malicious attacks.

Multicast authentication may provide the following security services like Data integrity, Data origin authentication and Non repudiation of the data to be transmitted .Designing a broadcast authentication protocol needs to consider the requirements like Resilience to packet loss, resilience to denial of service (DoS) attacks and efficiency.

1.2. Designing Multicast Authentication

Designing a multicast authentication protocol is not an easy task. Generally, 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. The receiver heterogeneity requires that the multicast authentication protocol be able to execute on not only powerful desktop computers but also resource-constrained mobile handsets. In particular, latency, computation, and communication overhead are major issues to be considered.

Packet loss is inevitable. In the Internet, congestion at routers is a major reason causing packet loss. An overloaded router drops buffered packets according to its preset control policy. 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 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 where the quality of service is critical to end users, a multicast authentication protocol should provide a certain level of resilience to packet loss .Specifically, the impact of packet loss on the authenticity of the already-received packets should be as small as possible.

In multicast, a single copy of packets is sent by the sender and routed to each receiver within the multicast group via multicast-enabled router. For a wide range of applications, multicast is an efficient and natural way of communicating information .However, multicast services lack support for traffic management, accounting and billing, reliability, and security. There are three distinct problem areas to consider in providing multicast security services.

First and most important, in secure multicast group members must be able to verify that the data received is indeed sent by an authorized sender. This is called origin authentication, includes group authentication and source authentication. Group authentication is the property that guarantees only that a message was sent (or last modified) by a member of the group. Since a MAC (Message Authentication Code) can be used for group authentication, it is rather inexpensive to authenticate even streaming data in real time. But in most applications the receivers must be able to establish the source of the data, at least for themselves. In other words, source authentication is more and more needed in multicast applications.

Moreover, a stronger version of the above property, referred to as non-repudiation, which enables each receiver to prove the origin of data to any impartial third party. Unfortunately, multicast source authentication is a difficult problem. The simplest solution is to digitally sign each packet, but signing each packet is computationally expensive, and introduces excessive per packet communication overhead.

Several solutions have been documented that amortize the cost of digital signatures over multiple packets, such as hashing tree and hashing chain. However, neither of them is efficient for all kind of multicast applications.

1.3. Signature Generation

The services of multicast authentication 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.

Efficiency and packet loss resilience can hardly be supported simultaneously by conventional multicast schemes. As is well known that 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.

2. Related Works

J.Sridevi et.al.,[1] have proposed the approach of signing and verifying each Packet independently raises a serious challenge to resource- constrained devices. 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.

Adrian Perrig et.al., [2] have proposed several substantial modifications and improvements to TESLA. One modification allows receivers to authenticate most packets as soon as they arrive (whereas TESLA requires buffering packets at the receiver side, and provides delayed authentication only). Other modifications improve the scalability of the scheme, reduce the space overhead for multiple instances, increase its resistance to denial-of-service attacks, and more.

Lei Zhang et.al.,[3] have proposed aggregate signatures that allow an efficient algorithm to aggregate n signatures of n distinct messages from n different users into one single signature. The scheme is proven existentially unforgeable against adaptive chosen-message attacks under the standard computational Diffie–Hellman assumption. The scheme is also very efficient in both communication and computation and the Proposal is practical for many-to-one authentication.

M.V.Vijaya saradhi et.al.,[4] have proposed emphasis protocol which provides a scope for the dynamic group operations like join the group, leave the group, merge without the need of central mechanisms. An important component for protecting group secrecy is re-keying. With the combination of strong public and private key algorithms this would become a better serve to the multicast security.

Anna Lisa Ferrara et.al.,[5] have proposed RSA signatures satisfy the latter condition, but are generally thousands of bits in length. The first constructions for batching group signatures, Which answers an open problem of Camenisch et al. It experimentally verify that the theoretical results of Camenisch et al. and this work, indeed, provide an efficient, effective approach to verifying multiple signatures from (possibly) different signers.

Qiyan Wang et.al.,[6] have proposed authentication to time critical multicast data, where low end-to-end delay is of crucial importance. The TV-HORS has perfect tolerance to packet loss and strong robustness against malicious attacks.The communication overhead of TV-HORS is much smaller than Regular OTS schemes, and even smaller than RSA signature. The Only drawback of TV-HORS is a relatively large public key of size 8KB to 10KB, depending on parameters.

Qinghua Li et.al.,[7] have proposed Multicast has been envisioned to be useful in many Smart Grid applications such as demand-response, wide area protection, in-substation protection, and various operation and control. This scheme is more appropriate for Smart Grid applications where the receivers have limited storage (e.g., home appliances and field devices) or where data communication is frequent and short (e.g., phasor data). These gains are at the cost of increased computations in signature generation and/or verification, and fortunately our scheme can flexibly allocate the computations between the sender and receiver based on their computing resources. It formulate the computation allocation as a nonlinear integer programming problem to minimize the signing cost under a certain verification cost, and propose a heuristic solution to solve it.

Christophe Tartary et.al.,[8] have proposed a hybrid scheme based on Tartary and Wang’s approach and Merkle hash trees. The construction exhibits a smaller overhead and a much faster processing at the receiver making it even more suitable for multicast than the earlier approach. As Tartary and Wang’s protocol, the construction is provably secure and allows the total recovery of the data stream despite erasures and injections occurred during transmission.

Heba K.Aslan et.al.,[9] have proposed multicast communication, authentication is a challenging problem, since it requires a large number of recipients to verify the data originator. Many of multicast applications are running over IP networks, in which several packet losses could occur. The proposed scheme has a low delay at the sender side and no delay at the receiver side, assuming no loss occurs. Finally, its latency equals to zero, assuming no loss occurs.

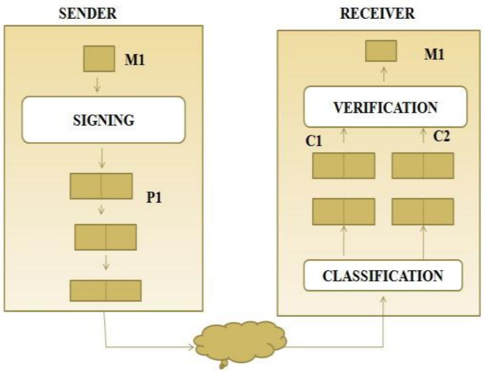
3. System Architecture

3.1. Overall Architecture

The early approach to multicast authentication is Conventional broadcast authentication protocols use a block-based approach to reduce the number of signature verification operations at each receiver. In particular, the sender divides a broadcast stream into blocks, associates each block with a signature, and spreads the effect of the signature across all the packets in the block through some data structures. The proposed system is Multicast Authentication based on Batch dsa 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.

Figure 1. Architecture of proposed system

The system provides data integrity, origin authentication, and non repudiation as previous asymmetric key based protocols. By using batch dsa signatures, our design can eliminate the authentication latency in the sense that each receiver can verify the authenticity of any number of packets in its buffer simultaneously whenever high-layer applications require. This is a significant improvement in the quality of real time applications compared to



conventional block-based protocols. In view of the problems regarding the sender favoured block-based approach, we conceive a receiver-oriented approach by taking into account the heterogeneity of the receivers in mobile communications. As mobile devices have different computation and communication capabilities some could be powerful mobile vehicles or portable laptops, while others could be PDAs or handsets with constrained memory resource and low-end CPUs. This poses a demand on the capability to authenticate any number of packets simultaneously on request by the high-layer applications at each receiver. The services of multicast authentication 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. Efficiency and packet loss resilience can hardly be supported simultaneously by conventional multicast schemes. As is well known that 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 multicasting, to avoid the vulnerability that is caused by the relevance between the packets, batch signature is used. This project suggests providing batch signature along with packet filtering technique. This packet filtering technique enables the sensible data to be protected. Batch dsa signatures are provided by RSA I general. However there are various issues with respect to the RSA algorithm. Hence, a batch signature using DSA is suggested to provide an efficient and improvised algorithm.

3.1. Digital Signature Algorithm (DSA)

DSA is a variant integrated Schnorr and ElGamal signature algorithm. Parameters in DSA are defined as follows.

p: a large prime with bit length between 512 to1024 of the multiple of 64.
q: a large prime divisor of p – 1, and the bit length equal to 160.
g: an element in Z_p of order q.
x: a secret key belongs to $Z_{q.}$
y: a public key $y=g^x$ mod p.
H(•): a secure hash algorithm,.
m: a message.
DSA's signing and verifying processes are as follows.

3.1.1. Signing process

Step 1: The signer chooses a random number k belongs to Z_q.

Step 2: The signer creates signature according to the following formulas:

$r=(g^k \bmod p)\bmod q$
$s=(k^{-1}(H(m)+xr))\bmod q$

The signature pair (r, s) of message m will be sent to the verifier.

3.1.2. Verifying process

To verify the received signature pair (r, s), the verifier computes the following formulas:

$W=s^{-1}\bmod q$
$U1=(H(m)*w)\bmod q$
$U2=(rw)\bmod q$
$V=((g^{u1}y^{u2})\bmod p)\bmod q$

If the equality v = r establishes, then the signature is correct.

4. Experimental Evaluation

4.1. Multicast Establishment

Multicast is an efficient method to deliver multimedia content from a sender to a group of receivers and is gaining popular applications. Here there is a sender and a group of receivers are established. The receiver requests the sender to join in that group to collect the data.

4.2. Signature Generation

The sender generates a signature using Batch DSA algorithm. Then it sends the public key and generator to the client who is all joined in its group.

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.

4.3. Data Broadcasting

During data broadcasting the sender signs each and every packet with its signature generated and it broadcasts the data to its clients. The clients those who are receiving the data verify the signature for a batch of n packets. If sign is verified then the data is loaded to client.

5. References

[1] J.Sridevi, R.Mangaiyarkarasi,” Efficient Multicast Packet Authentication using Digital Signature”, International Conference on Emerging Technology Trends(ICETT),2011.

[2] Adrian Perrig, Ran Canetti, Dawn Song, J.D. Tygar,” Efficient and Secure Source Authentication for Multicast”, EURASIP Journal on Wireless Communications and Networking Volume 2011.

[3] Lei Zhang, Bo Qin,Qianhong Wu, Futai Zhang,” Efficient many-to-one authentication with certificateless aggregate signatures”,The International Journal of Computer and Telecommunications Networking Volume 54 Issue 14,October,2010.

[4] M .V.Vijaya saradhi, BH.Ravi Krishna ,“a group key management approach for multicast cryptosystems”, Journal of Theoretical and Applied Information Technology,2009.

[5] Anna Lisa Ferrara, Matthew Green, Michael ostergaard Pedersen,” Practical Short Signature Batch Verification”, CT-RSA '09 Proceedings of the The Cryptographers' Track at the RSA Conference 2009 on Topics in Cryptology,2009.

[6] Qiyan Wang, Himanshu Khurana, Ying Huang, Klara Nahrstedt,” Time Valid One-Time Signature for Time-Critical Multicast Data Authentication”, IEEE INFOCOM 2009 The 28th Conference on Computer Communications ,2009.

[7] Qinghua Li, Guohong Cao,” Multicast Authentication in Smart Grid With One-Time Signature”, IEEE INFOCOM 2009 The 28th Conference on Computer Communications, 2009.

[8] Christophe Tartary, Huaxiong Wang, and Josef Pieprzyk,” An Hybrid Approach for Efficient Multicast Stream Authentication over Unsecured Channels”, ProvSec'07 Proceedings of the 1st international conference on Provable security 2007.

[9] Heba K. Aslan,” A hybrid scheme for multicast authentication over lossy networks”, Military Communications Conference 2007 MILCOM 2007 IEEE ,2007.

[10] Seema Patil, Sahana Hanumantagouda Patil,” Authentication of Packets using Batch RSA and Batch DSA for Multicast Environment”, IEEE Communications Magazine ,August 2007.