Multicast Authentication Based on Batch Signature (MABS) in Network Security

Srikanth Bethu¹*, Asrar Ahmed M. D.², Jesurun Prem Kumar Dasari³, Soujanya S.⁴ and Kanthi Kumar K.⁵

¹,⁴Department of Computer Science and Engineering, HITS College, JNTU Hyderabad, A.P., India.
²Department of Computer Science and Engineering, Osmania University, Hyderabad, A.P., India.
³MS Information Systems, University of Ballarat, Melbourne, Australia.
⁵Department of Electronics and Communication Engineering, JNTUK Kakinada, A.P., India.
e-mail: ¹srikanthbethu@gmail.com

Abstract. 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. Multicast authentication may provide the following Security services: Data Integrity, Data Origin Authentication, Non-repudiation. 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. 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. Second, 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

*Corresponding author.

K. R. Venugopal and L. M. Patnaik (Eds.) ICCN 2013, pp. 180–188. © Elsevier Publications 2013.
Multicast Authentication Based on Batch Signature (MABS) in Network Security

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. 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 algorithms amortize one signature over a block of packets. 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. MABS-B is efficient in terms of less latency, computation, and communication overhead. Though MABS-E is less efficient than MABS-B since it includes the DoS defense, its overhead is still at the same level as previous schemes.

Keywords: data integrity, data origin authentication, MABS, MABS-B, MABS-E non-repudiation.

1. Introduction

Security issues in multicast communication have rarely been touched upon to date. We believe that wide-area multicast communication is at a substantially increased risk from specific security threats, compared with the same threats in unicast. This arises both from the lack of any form of effective group access control, and from the fact that multicast traffic traverses potentially many more communication links than does a single uni-cast communication, thereby creating more opportunity for a link attack. We discuss specific threats that are relevant to multicast, and explain why they are so. We propose security mechanisms specifically for multicast groups requiring safeguards that afford protection against some of these threats. More precisely, we propose a version of the IGMP protocol that can reliably enforce subnet-level group access control. We also describe a scalable mechanism to control multicast traffic in transit that can, for example, prevent a misbehaving source from causing undue congestion over the wide-area.

Multicast enables efficient large-scale content distribution by providing an efficient transport mechanism for one-to-many and many-to-many communication. The very rare properties that make multicast attractive, however, also make it a challenging environment in which to provide content security. We show how the fundamental properties of the multicast paradigm cause security issues and vulnerabilities. We focus on four areas of research in security for multicast content distribution: receiver access control, group key management, multicast source authentication, and multicast fingerprinting. For each we explain the vulnerabilities, discuss the objectives of solutions, and survey work in the area. Also, we briefly highlight other security issues in multicast content distribution including source access control, secure multicast routing, and group policy specification. We then outline several future research directions.

1.1 Properties of multicast

The definition of the host group model provides a summary of the key properties of multicast: a host group is a set of network entities sharing a common identifying multicast address, all receiving any data packets addressed to this multicast address by senders (sources) that may or may not be
members of the same group and have no knowledge of the groups membership. This definition highlights the three main properties of multicast:

- All members receive all packets sent to the address: Multicast routing delivers all packets sent to the multicast address to all members of the multicast group.
- Open group membership: Multicast provides an open group model and allows group membership to be transparent to the source.

1.2 Multicast routing protocol

Multicast routers execute a multicast routing protocol to define delivery paths that enable the forwarding of multicast data grams across an internetwork. The Distance Vector Multicast Routing Protocol (DVMRP) is a distance-vector routing protocol, and Multicast OSPF (MOSPF) is an extension to the OSPF link-state unicast routing protocol.

1.3 Multicast routing protocol

These properties of multicast lead to security issues and vulnerabilities because of two reasons: the issues are multicast-specific or the issues also exist in unicast, but the unicast solutions do not apply, the three multicast properties leads to vulnerabilities and the areas of research that provide solutions to these issues. The multicast model delivers any traffic sent to the multicast address to the entire group. This means that any host can send data to the multicast group. This leads to two problems. First, group members need to be able to verify that messages received are from the intended source. Multicast source authentication solutions have been proposed to provide this functionality. Second, there should be mechanisms to restrict unauthorized sources from sending data to multicast groups due to the potential for denial-of-service attacks. Multicast sender access control solutions are necessary to defend against this threat.

2. Related Work

We introduce and exemplify the new concept of ON-LINE/OFF-LINE digital signature schemes. In these schemes the signing of a message is broken into two phases. The first phase is off-line. Though it requires a moderate amount of computation, it presents the advantage that it can be performed leisurely, before the message to be signed is even known. The second phase is on-line. It starts after the message becomes known, it utilizes the precomputation of the first phase and is much faster. A general construction which transforms any (ordinary) digital signature scheme to an on-line/off-line signature scheme is presented, entailing a small overhead. For each message to be signed the time required for the off-line phase is essentially the same as in the underlying signature scheme; the time required for the on-line phase is essentially negligible. The time required for the verification is essentially the same as in the underlying signature scheme. In a practical implementation of our general construction; we use a variant of Rabin’s signature scheme (based on factoring) and DES. In the on-line phase, all we use is a moderate amount of DES computation. This implementation is ideally suited for electronic wallets or smart cards. On-line/Off-line digital schemes may also become useful in case substantial progress is made on, say, factoring. In this case, the length of the composite numbers used in signature schemes may need to
be increased and signing may become impractical even for the legitimate user. In our scheme, all costly computations are performed in the off-line stage while the time for the on-line stage remains essentially unchanged. An additional advantage of our method is that in some cases the transformed signature scheme is invulnerable to chosen message attack even if the underlying (ordinary) digital signature scheme is not. In particular, it allows us to prove that the existence of signature schemes which are unforgeable by known message attack is a (necessary and) sufficient condition for the existence of signature schemes which are unforgeable by chosen message attack.

2.1 Basic scheme

Our target 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 is a less powerful device with resource constraints and may be managed by a non trustworthy person. Each receiver needs to assure that the received packets are really from the sender (authenticity) and the sender cannot deny the signing operation (non repudiation) 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. 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. Next, we present three implementations. In addition to the one based on RSA, we propose two new batch signature schemes based on BLS and DSA, which are more efficient than batch RSA. We must point
out and will show later that MABS is independent from these signature algorithms. This independence brings the freedom to optimize MABS for a particular physical system or platform as much as possible.

2.2 Basic scheme

The BLS signature scheme uses a cryptographic primitive called pairing, which can be defined as a map over two cyclic groups. One merit of the BLS signature is that it can generate a very short signature. It has been shown in that an \( n \)-bit BLS signature can provide a security level equivalent to solving a Discrete Log Problem (DLP), over a finite field of size approximately \( 2^{6n} \). Therefore, a 171-bit BLS signature provides the same level of security as a 1,024-bit DLP-based signature scheme such as DSA. This is a very nice choice in the scenario where communication overhead is an important issue.

Given a batch of packets that have been signed by the sender, BatchVerify outputs True. Given a batch of packets including some unauthentic packets, the probability that BatchVerify outputs true is very low. The computation complexity of BatchVerify is comparable to that of verifying one signature and is increased only gradually when the batch size \( n \) is increased.

2.3 DSA Signature

DSA is another popular digital signature algorithm. Unlike RSA, which is based on the hardness of factoring two large primes, DSA is deemed secure based on the difficulty of solving DLP. A batch DSA signature scheme was proposed in but later was found insecure. Harn improved the security. Unfortunately, Boyd and Pavlovski pointed out in that Harn’s work is still vulnerable to malicious attacks. Here, we propose a batch DSA scheme based on Harn’s work and counteract the attack. The Digital Signature Algorithm (DSA) is specified in this Standard. The specification includes criteria for the generation of domain parameters, \( f \) or the generation of public and private key pairs, and for the generation and verification of digital signatures.

![Digital signature process](image)

**Figure 2.** Digital signature process [5].
3. Enhanced Scheme

In this section, we present 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. In MABS-E, Merkle tree is used to generate marks. An example is illustrated in Figure 5. The sender constructs a binary tree for eight packets. Each leaf
Figure 5. An example of Merkle tree. Each leaf is a hash of one packet. Each internal node is the hash value on both its left and right children [5].

is a hash of one packet. Each internal node is the hash value on the concatenation of its left and right children. For each packet, a mark is constructed as the set of the siblings of the nodes along the path from the packet to the root.

4. Performance Evaluation

In this section, we evaluate MABS performance in terms of resilience to packet loss, efficiency, and DoS resilience. As we discussed before, MABS does not assume any particular underlying signature algorithm.

4.1 Resilience to packet loss

This is also true for all the literature multicast authentication schemes referenced in this paper. Therefore, all the discussions and evaluations of MABS and the literature works are under the assumption that they are using the same underlying signature algorithm. We consider the authentication of digital streams over a lossy network. The overall approach taken is graph-based, as this yields simple methods for controlling overhead, delay, and the ability to authenticate, while serving to unify many previously known hash and MAC-based techniques. The loss pattern of the network is defined probabilistically, allowing both bursty and random packet loss to be modeled. Our authentication schemes are customizable by the sender of the stream; that is, within reasonable constraints on the input parameters, we provide schemes that achieve the desired authentication probability while meeting the input upper bound on the overhead per packet. In addition, we demonstrate that some of the shortcomings of previously known schemes correspond to easily identifiable properties of a graph, and hence, may be more easily avoided by taking a graph-based approach to designing authentication schemes. Multicast stream authentication and signing is an important and challenging problem.
Applications include the continuous authentication of radio and TV Internet broadcasts, and authenticated data distribution by satellite.

The main challenges are fourfold. First, authenticity must be guaranteed even when only the sender of the data is trusted. Second, the scheme needs to scale to potentially millions of receivers. Third, streamed media distribution can have high packet loss. Finally, the system needs to be efficient to support fast packet rates. We use simulations to evaluate the resilience to packet loss. The metric here is the verification rate, i.e., the ratio of the number of authenticated packets to the number of received packets we compare MABS with some well-known loss tolerant schemes EMSS, augmented chain, PiggyBack, tree chain. These schemes are representatives of graph chaining, tree chaining, and erasure coding schemes and are widely used in performance evaluation in the literature. For EMSS we choose the chain configuration, which has the best performance among all the configurations of length. For AugChain, we choose chain configuration. For PiggyBack, we choose two class priorities. For Tree chain, we choose binary tree. For SAIDA, we choose the erasure code 256; 128. For all these schemes, we choose the block size of 256 packets and simulate over 100 blocks. We consider the random loss and the burst loss with a maximum loss length of 10 packets. The verification rates under different loss rates are given in below Figures. We can see that the verification rates of EMSS, augmented chain (AugChain) and PiggyBack are decreased quickly when the loss rate is increased. The reason is that graph chaining results in the correlation among packets and this correlation is vulnerable to packet loss. SAIDA illustrates resilience to packet loss up to a certain threshold, because of the threshold performance of erasure codes. Our MABS and Tree schemes have perfect resilience to packet loss in the sense that all the received packets can be authenticated. This is because all the packets in MABS and Tree schemes are independent from each other.

As we will show later, however, Tree achieves this independency by incurring large overhead and latency at the sender and each receiver and is vulnerable to DoS, while our MABS-B has less overhead and latency and MABS-E is resilient to DoS at the same level of overhead as Tree. One thing needs to be pointed out is that we do not differentiate between MABS-B and MABS-E in above Figures. MABS-B is perfect resilient to packet loss because of its inherent design. While it is not designed for lossy channels, MABS-E can also achieve the perfect resilience to packet loss in lossy channels. In the lossy channel model, where no DoS attack is assumed to present, we can set the threshold \( t \) for MABS-E, and thus each receiver can start batch-verification as long as there is at least one packet received for each set of packets constructed under the same Merkle tree.

4.2 Comparisons over lossy channels

Below Table shows the comparisons between MABS-B and well known loss-tolerant schemes tree chain (Tree), EMSS, PiggyBack, augmented chain (AugChain), and SAIDA. We also include MABS-E and three DoS resilient schemes PRABS, BAS, and LTT in the table just for comparisons even though they are not designed for lossy channels. Previous block-based schemes introduce latency either at the sender or at each receiver or both. The latency is inherent in the block design due to chaining or coding. At the sender side, the correlation among a block of packets has to be established before the sender starts sending the packets. At each receiver, the latency is incurred when the high layer application waits for the buffered packets to be authenticated after the correla-
tion is recovered. This receiver side latency is variable depending on whether the correlation among the underline buffered packets has been recovered or not when the high layer application needs new data and its maximum value is the block size. MABS-B eliminates the correlation among packets. Each packet is independently sent out at the sender.

4.3 Comparisons of signature schemes

We compare the computation overhead of three batch signature schemes in below Table. RSA and BLS require one modular exponentiation at the sender and DSA [38] requires two modular multiplications when \( r \) value is computed offline. Usually one c-bit modular exponentiation is equivalent to 1:5c modular multiplications over the same field. Moreover; a c-bit modular exponentiation in DLP is equivalent to ac 6-bit modular exponentiation in BLS for the same security level. Therefore, we can estimate that the computation overhead of one 1,024-bit RSA signing operation is roughly equivalent to that of 768 DSA signing operations (1,536 modular multiplications) and that of 6 BLS signing operations (each one is corresponding to 255 modular multiplications). According to the report [60] on the computational overhead of signature schemes on PIII 1 GHz CPU, the signing and verification time for 1,024-bit RSA with a 1,007-bit private key are 7.9 ms and 0.4 ms, for 157-bit BLS are 2.75 ms and 81 ms, and for 1,024-bit DSA with a 160-bit private key (without precomputing \( r \) value) are 4.09 ms and 4.87 ms. We can observe that for BLS and DSA the signing is efficient but the verification is expensive, and vice versa for RSA. Therefore, we can save more computation resource at the sender by using our batch BLS and batch DSA than batch RSA. It is also meaningful to use our batch BLS and batch DSA at the receiver to save computation resources.

5. 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] Deering, S. E.: Multicast Routing in Internetworks and Extended LANs. Proc. ACM SIGCOMM Symp. Comm. Architectures and Protocols, 55–64, August (1988).
[2] Ballardie, T. and Crowcroft, J.: Multicast-Specific Security Threats and Counter-Measures. Proc. Second Ann. Network and Distributed System Security Symp. (NDSS 95), 2–16, February (1995).
[3] Judge, P. and Ammar, M.: Security Issues and Solutions in Multicast Content Distribution: A Survey. IEEE Network Magazine, 17(1), 30–36, January/February (2003).
[4] Zhou, Y. and Fang, Y.: BABRA: Batch-Based Broadcast Authentication in Wireless Sensor Networks. Proc. IEEE GLOBECOM, November (2006).
[5] Zhou, Y., Xiaoyan Zhu and Fang, Y.: Multimedia Broadcast Authentication Based on Batch Signature. IEEE Transactions on Mobile Computing, 9(7), 72–77, July (2010).