Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multicast Authentication Using Batch Signature [MABS] in Mobile Ad Hoc Networks

Abirami.N[1]
M.Phil Scholar, VMU, Tamilnadu, India

Sasikala.K[2]
Asst.Prof, VMKVEC, India

Reka.R[3]
Asst.Prof, VMKVEC, India

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. MABS includes two schemes MABS-B & MABS-E. The basic scheme MABS-B eliminates the correlation among packets and thus provides the perfect resilience to packet loss, and 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. Another scheme MABS-E which combines the basic scheme with a packet filtering mechanism to solve the DoS (Denial of Service) impact while preserving the perfect resilience to packet loss. The enhanced scheme MABS-E and MABS-B combines with packet filtering to solve the DoS impact in hostile environments. MABS provides data integrity, origin authentication, and nonrepudiation as previous asymmetric key based protocols.

Keywords— Adhoc Network, Authentication, MABS B & E, DOS, RSA.

I. INTRODUCTION

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. In Symmetric Key Secure data transmission codingschemes (such as the Data Encryption Standard) which use only one digital key in both encoding and decoding a message. In contrast, asymmetric key cryptography schemes (such as the Pretty Good Privacy) use two different digital keys, one for coding and the other for decoding.

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. MABS provides data integrity, origin authentication and nonrepudiation as previous asymmetric key based protocols. Public key is a value provided by some designated authority as an encryptionkey that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures. In Private key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages.

Basically, multicast authentication may provide the following security services:

- Data integrity: Each receiver should be able to assure that received packets have not been modified during transmissions.
- Data origin authentication: Each receiver should be able to assure that each received packet comes from the real sender as it claims.
- Nonrepudiation: 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.

2. LITERATURE REVIEW

Y.Challal, H.Bettahar, and A.Bouabdallah [1] have discussed about the authentication and highlight the issues and challenges related to this security service. Consider a sender that streams data to a set of receivers in a multicast session. We consider a stream as an infinite sequence of packets that are sent successively. Receivers of the multicast session are not trusted. The sender authenticates a multicast message using some authentication procedure that generates the authentication information associated with the message. The message and its authentication information are multicast to receivers. Since most multicast media-streaming applications require real-time transmission, multicast data origin authentication must not induce latencies at the sender before authenticating stream packets, nor at receivers before

verifying the authenticity of received packets. C.K.Wong and S.S.Lam [2] have described about the data confidentiality, authenticity, integrity, and no repudiation are basic concerns of securing data delivery over an insecure network, such as the Internet. Confidentiality means that only authorized receivers will get the data; authenticity, an authorized receiver can verify the identity of the data's source; integrity, an authorized receiver can verify that received data have not been modified; no repudiation, an authorized receiver can prove to a third party the identity of the data's source .

Z.Zhang, Q.Sun, and W.C Wong [3] have proposed a butterfly-graph based stream authentication scheme for lossy networks where the streaming packets could be lost in both random and burst ways. Due to the nice properties of butterfly graph, the proposed scheme is quite robust and efficient. Theoretical analysis and simulation results show that the proposed scheme outperforms existing schemes in terms of overhead and authentication probability while maintaining the same levels of sender / receiver delay and robustness. it is very important to protect the authenticity of the streams in the aspects of integrity and non-repudiation.

3. RSA SIGNATURE

RSA is based on the simple arithmetical fact that it is relatively easy to multiply two large prime numbers but extremely difficult to work backward from the product to find those prime numbers. This technique allows the unique public encryption key (the product of prime numbers) to be disclosed to any one but which can be decoded only with the secretprivate key (the prime numbers). RSA is the standard encryption method for important data, especially data that's transmitted over the Internet.

The RSA signature scheme consists of four phases:

Phase 1:

This is only for how to generate a key before transfer the packets. To it, the sender has to choose any numeric value which should belongs to any group of the public key. So any sender has to collect the key of private from a group of the public key.

Phase 2:

In this phase, we want to provide some signature to every packet before it has to send. To accelerate the authentication of multiple signatures, the batch verification can be used. Given N packets, the sender want to give a private key to verify the batch (Packet) in the receiver side.

Phase 3:

The received batch will be verified here. Before the batch verification, the receiver must ensure all the messages are distinct. To avoid the attacking on the sender's data, this is easy to implement because sequence numbers are widely used in many network protocols and can ensure all the messages are distinct and the data will be verified it has any data loss then it has to go for next step of process.

Phase 4:

In this phase, the receiver would like to check the received data has a perfect authorization or not. If this has the proper authentication, all the batches are removed the signature and merge the data together to view to the receiver.

4. COMPARISON OF MABS-B AND MABS-E

Basic scheme: MABS-B

The basic scheme MABS B targets at the packet loss problem, which is inherent in the internet and wireless networks. It has perfect resilience to packet loss no matter whether it is random loss or burst loss. In some circumstances, however, an attacker can inject forged packets into a batch of packets to disrupt the batch signature verification, leading to Dos. A naive 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 which means more signature verifications at each receiver. In worst case the attacker can inject forged packets at very high frequency and expect that each receiver stops the batch operation and recovers the per packet signature verification which may not be viable at resource constrained receiver devices.

Enhanced scheme: MABS-E

The Enhanced scheme MABS-E, which combines the basic schemeMABS-B and 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 the packet from the real sender never falls into any set of packets from the attacker. Next each receiver only needs to perform Batch verify () 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 doesn't 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.

4.1 Existing System

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.

4.2 PROPOSED SYSTEM

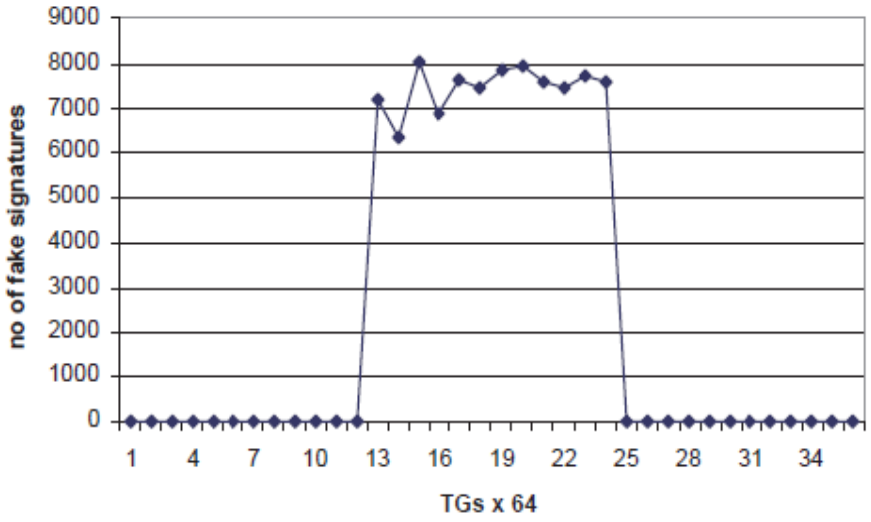
The proposed system overcomes the above mentioned drawbacks. Multicast Authentication based on Batch Signature [MABS] utilizes an efficient asymmetric cryptographic primitive called batch signature which supports the authentication of any number of packets simultaneously with one signature verification, 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.

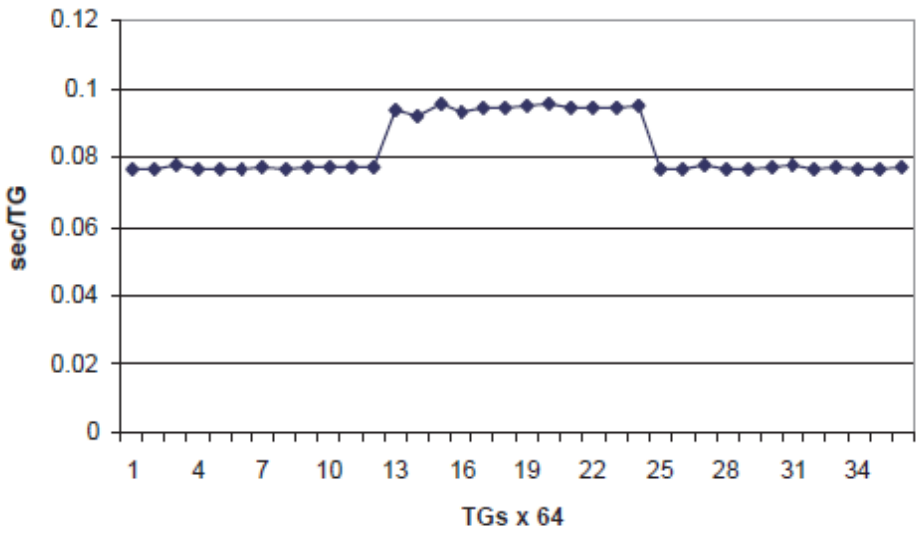
5. EXPERIMENTAL RESULTS

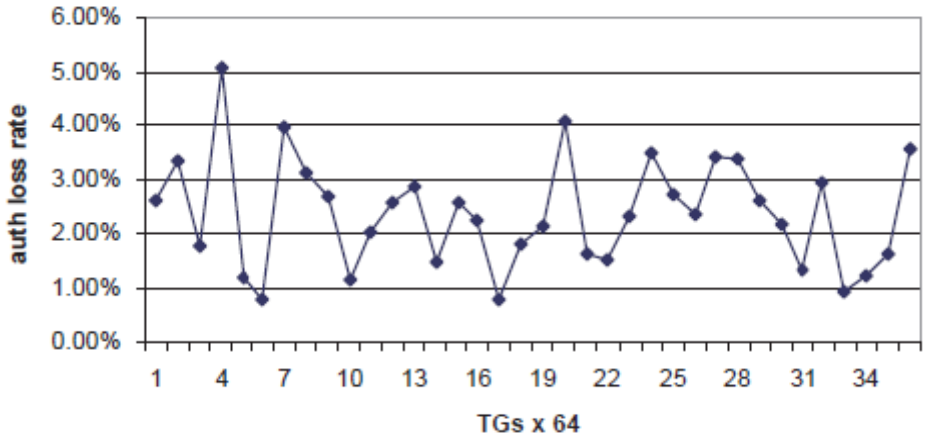
We assume the existence of a DoS attacker with access to the various levels of bandwidth. The interesting independent variables are the following: sender rate and latency; loss rate; average burst length; attacker rate. Our approach fixesa target latency; the protocol is then designed for various bandwidth and reliability characteristics of the channel. The interesting dependent variables are: sender throughput; receiver throughput; bandwidth overhead; authentication loss.

The sender rate is the number of megabits of data packets that can be processed in one second; processing consists of producing the necessary hash, parity, and signature packets for the data packets. The receiver rate is the rate in megabits per second at with which valid data packets can be recovered from a mixture of packets originating from the sender and an attacker. The bandwidth overhead is the percentage of bandwidth devoted to hash, parity, and signature packets. The authentication loss is the percentage of data packets received by the receiver that cannot be verified by the receiver due to the loss or reordering of hash, signature, and parity packets.

The aim is to measure robustness against signature floods even at levels where the adversary could be effective by attacking another limit. For instance, a receiver can perform hashes on about 77,000 packets each second so a factor 10 attack on a 100Mbps link would overwhelm this capacity if it forced the receiver to perform hashes on all of the packets it receives.







6. Conclusion

Multicast authentication batch signature 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. Multicast authentication batch signature provides packet filtering to avoid packet loss, Authenticates any number of packets simultaneously, and Uses signature verification for authentications.

References

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

[2] C.K. Wong and S.S. Lam, "Digital Signatures for Flows andMulticasts," Proc. Sixth Int'l Conf. Network Protocols (ICNP '98),pp. 198-209, Oct. 1998.

[3] 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.

[4] S. Cui, P. Duan, and C.W. Chan, "An Efficient Identity-Based Signature Scheme with Batch Verifications," Proc.First Int'l Conf. Scalable Information Systems, 2006.

[5] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[6] A. Lysyanskaya, R. Tamassia, and N. Triandopoulos, "Multicast Authentication in Fully Adversarial Networks," Proc. IEEE Symp. Security and Privacy (SP '04), May 2004.

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

[8] D. Song, D. Zuckerman, and J.D. Tygar, "Expander Graphs for Digital Stream Authentication and Robust Overlay Networks,"Proc. 2002 IEEE Symp. Security and Privacy (S&P '02), May 2002.

