A DATA PACKET TRANSMISSION AUTHENTICATION USING MULTICAST ROUTING PROTOCOL

S.Navaneethan
Assistant Professor ,Dept of IT/ Sir Issac Newton. College of Engineering & Technology, Nagapattinam

Dr.Kathirvel
Professor, Dept of CSE/ Vivekanandha College of Engineering for Women, Tiruchengode

***Abstract**:* The multicast authentication protocol namely MABS including two schemes MABS-B and MABS-E. The basic scheme (MABS-B) eliminates packet loss and also efficient in terms of latency computation and communication overhead due to effective cryptographic primitive called batch signature which authenticates any number of packets simultaneously. This paper deals with the enhanced scheme (MABS-E) which combines the basic scheme with a packet filtering mechanism to alleviate DOS impact. The file list is displayed in both sender and the receiver but the file content is present in the sender only. The receiver request the file content by sending the file name then the sender verify the request if the receiver is authentic. Then sender splits the file content into packets and signs each packet by generating the key then encrypts the packets and sends to the receiver. The receiver verifies the packets and then decrypts the message using sender's public key. Soundness of the proposal will be tested in prominent Network Simulator.

Key Words: Multicast, MABS-B, MABS-E, DOS

1. INTRODUCTION

Multicast routing protocols are an efficient method to deliver multimedia content from a sender to a group of receivers. Authentication is one of the critical topics in securing multicast [3]. Multicast authentication may provide the following security services include data integrity, data origin authentication, and non repudiation [2].

i. Data integrity

Each receiver should be able to assure that the received packets have not been modified during the transmission.

ii. Data origin authentication

Each receiver should be able to assure that each received packets come from the real sender as it claims.

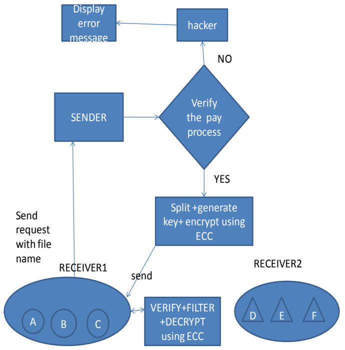
iii. Non repudiation

The sender of the packets should not be able to deny sending the packets to receiver in case there is a dispute between the sender and the receivers. [3]

All the 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. In this paper we propose a novel multicast authentication protocol called MABS [5]. It includes two schemes [5]. The basic scheme 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-B is efficient in terms of less latency, computation, and communication overhead. The enhanced scheme combines MABS-B with packet filtering to alleviate the Dos impact in hostile environments [5].

The rest of the paper is organized as follows: Section 2 provides an architecture diagram and implementation of our models; Simulations and experimental Results are given in section 3. Section 4 we explore related work on different attacks and Section 5 draws up conclusions.

2. ARCHITECTURE DIAGRAM:


Display error message
hacker
NO
SENDER
Verify the pay process
YES
Split +generate key+ encrypt using ECC
Send request with file name
RECEIVER1
send
RECEIVER2
A
B
C
VERIFY+FILTER +DECRYPT using ECC
D
E
F

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 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 [6 - 8].

Authenticating a multicast stream can be achieved by signing and verifying each packet. The per packet signature design has been criticized for its high computation cost. 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. MABS-B uses an efficient cryptographic primitive called batch signature which supports simultaneously verifying the signatures of any number of packets. The merit of batch signature is that the batch size is chosen by each receiver which can optimize its own batch size, so that the batch size will not be unmanageably large.MABS-B [5] uses per packet signature instead of per block signature and thus eliminates the correlation among packets. The internet and wireless channels tend to be lossy due to congestion or channel instability, where packets can be lost [7]. In MABS-B, however, no matter how many packets are lost, the already received packets can still be authenticated by each receiver. This is a significant advantage. Efficiency also achieved because a batch of packets can be authenticated simultaneously through one batch signature verification operation. The packet independency also brings other benefits in terms of smaller latency and communication overhead [8 - 9][1 – 2].

2.2 BATCH BLS SIGNATURE

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

2.2.1 BLS

The BLS signature scheme uses a cryptographic primitive called pairing, which can be defined as a map over two cyclic groups G1 and G2, e :G1->G2. The BLS signature scheme consists of three phases:

1. In the key generation phase, a sender chooses a random integer x∑Zp and computes y=g1^x∑G1.The private key is x and public key is y.

2. Given a message m∑{0,1}* in the signing phase, the sender first computes h= h(m) ∑ G1,where h() is a hash function, then computes ∂=h^x∑G1.The signature of m is ∂.

3. In the verification phase , the receiver first computes h=h(m)∑G1 and then check whether e(h,y)=e(∂,g1).

If the verification succeeds, then the message m is authentic because

e(h,y)=e(h,g1^x)=e(h^x,g1)=e(∂,g1)

One merit of the BLS signature is that it can generate a very short signature. An n-bit BLS can provide a security level equivalent to solving a discrete log problem (DLP) over a finite field of size.

2.2.2 BATCH BLS

Based on BLS, we propose our batch BLS scheme here.

Given n packets{mi, ∂i}, i=1….,n the receiver can verify the batch of BLS signatures by first computing hi=h(m), i=1,…,n and then checking whether e(∏^ni=1hi,y)= e(∏^ni=1∂i,g1). This is because if all the messages are authentic, then

e(∏^ni=1hi,y)=∏^ni=1e(hi,g1^x)

=∏^ni=1e(hi^x,g1)

=e(∏^ni=1∂1,g1)

We prove that our batch BLS is secure to signature forgery as long as BLS is secure to signature forgery.

2.3 REQUIREMENTS TO THE SENDER

In our batch BLS the sender needs to sign each packet. Because a BLS can provide a security level equivalent to conventional RSA and DSA with much shorter signature, the signing operation is more efficient than the RSA signature generation. Moreover BLS can be implemented over elliptic curves. It is used to achieve computation efficiency at the receiver.

2.4 ENHANCED SCHEME

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.

In this section we present an enhanced scheme called MABS-E, which combines the basic scheme MABS-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.

3. PERFORMANCE EVALUATION

We evaluate MABS performance [1 – 2] in terms of resilience to packet loss, efficiency and Dos resilience.

1.Resilience to packet loss

We use simulations to evaluate the resilience to packet loss. The metric here is the verification rate, i.e., the ratio of number of authenticated packets to the number of received packets. MABS-B is perfect resilience 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=1 for MABS-E and thus each receiver can start batch verification as long as there is at least 1 packet received for each set of packets .

2. Efficiency

We consider latency, computation and communication overhead for efficiency evaluation under lossy channels and Dos channels.

3. Dos resilience.

The signing and verification time is less. The signing is efficient. Therefore, we can save more computation resource at the sender.

MABS can achieve more bandwidth efficiency by using BLS. BLS can generate smaller key length.

4. RELATED WORKS

The approaches for detecting packet dropping attacks can be categorized as three classes: multipath forwarding approach, neighbor monitoring approach, and acknowledgment approach. Multipath forwarding [3], [13] is a widely adopted countermeasure to mitigate packet droppers, which is based on delivering redundant packets along multiple paths. Another approach is to exploit the monitoring mechanism. The watchdog method was originally proposed to mitigate routing misbehavior in mobile ad hoc networks [14]. It is then adopted to identify packet droppers in wireless sensor network. When the watchdog mechanism is deployed, each node monitors its neighborhood collect the firsthand information on its neighbor nodes. A variety of reputation systems have been designed by exchanging each node's firsthand observations, which are further used to quantify node's reputation. Based on the monitoring mechanism, the intrusion detection systems are proposed However, the watchdog method requires nodes to buffer the packets and operate in the promiscuous mode, the storage overhead and energy consumption may not be affordable for sensor nodes. In addition, this on the bidirectional communication links; it may not be effective when directional antennas are used. Particularly, this approach cannot be applied when a node does not know the expected output of its next hop since the node has no way to find a match for buffered packets and overheard packets. Note that, this scenario is not rare, for example, the packets may be processed, and then encrypted by the next hop node in many applications that security is required. Since the watchdog is a critical component of reputation systems, the limitations of the watchdog mechanism can also limit the reputation system. Besides, a reputation system itself may become the attacking target. It may either be vulnerable to bad mouthing attack or false praise attack. The third approach to deal with packet dropping attack is the multihop acknowledgment technique [9]. By obtaining responses from intermediate nodes, alarms, and detection of selective forwarding attacks can be conducted. To deal with packet modifiers, most of existing countermeasures are to modified messages within a certain number of hops so that energy will not be wasted to transmit modified messages. The effectiveness to detect malicious packet droppers and modifiers is limited without identifying them and excluding them from the network. Researchers hence have proposed schemes to localize and identify packet droppers, one approach is the acknowledgment-based scheme [10][11] for identifying the problematic communication links. It can deterministically localize links of malicious nodes if every node reports ACK using onion report. However, this incurs large communication and storage overhead for sensor networks. The probabilistic ACK approaches are then proposed in [14] and [15], which seek tradeoffs among detection rate, communication overhead, and storage overhead. However, these approaches assume the packet sources are trustable, which may not be valid in sensor networks. As in sensor networks, base station typically is the only one we can trust. Furthermore, these schemes require setting up pair wise keys among regular sensor nodes so as to verify the authenticity of ACK packets, which may cause considerable overhead for key management in sensor networks [12 -13]. Ye et al. [15] proposed a scheme called PNM for identifying packet modifiers probabilistically. However, the PNM scheme cannot be used together with the false packet filtering schemes .Because the filtering schemes will drop the modified packets which should be used by the PNM scheme as evidences to infer packet modifiers. This degrades the efficiency of deploying the PNM scheme.

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 Dos attack. To overcome these problems, we develop a authentication scheme MABS. We have already discussed that MABS is perfectly resilient to packet loss due to the elimination of the correlation among packets and can effectively deal with Dos attack. We also discuss that the use of batch signature like BLS can achieve the efficiency less than or comparable with the conventional schemes. Further works to test the soundness of our work using network simulator.

REFERENCES

1. Ayyaswamy Kathirvel and Rengaramanujam Srinivasan, “ETUS: Enhanced Triple Umpiring System for Security and Robustness of Wireless Mobile Ad Hoc Networks”, International Journal of Communication Networks and Distributed Systems, Vol. 7, No. 1 / 2, pp. 153 – 187, 2011.
2. Ayyaswamy Kathirvel and Rengaramanujam Srinivasan, “ETUS: An Enhanced Triple Umpiring System for Security and Performance Improvement of Mobile Ad Hoc Networks”, International Journal of Network

Management, Vol. 21, No. 5, pp. 341 – 359, 2011.

3. S.E. Deering, "Multicast Routing in Internetworks and Extended LANs," *Proc. ACM SIGCOMM Symp. Comm. Architectures and Protocols,* pp. 55-64, Aug. 1988.

4. 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.

5. Yun Zhou, Xiaoyan Zhu, Yuguang Fang, "MABS: Multicast Authentication Based on Batch Signature," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 982-993, July 2010.

6. J. Jeong, Y. Park, and Y. Cho, "Efficient DoS Resistant Multicast Authentication Schemes," Proc. Int'l Conf. Computational Science and Its Applications", 2005, pp.353-362.

7. 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.

8. S. Miner and J. Staddon, "Graph-Based Authentication of Digital Streams," *Proc. IEEE Symp. Security and Privacy (SP '01),* pp. 232-246, May 2001.

9. N. Koblitz, "Elliptic Curve Cryptosystems," *Math. Computation,* vol. 48, pp. 203-209, 1987.

10. M. Kefayati, H.R. Rabiee, S.G. Miremadi, and A. Khonsari,"Misbehavior Resilient Multi-Path Data Transmission in Mobile Ad-Hoc Networks", Proceedings of the fourth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '06), 2006.

11. R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Secmr—A Secure Multipath Routing Protocol for Ad Hoc Networks", Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007.

12. B. Xiao, B. Yu, and C. Gao, "Chemas: Identify Suspect Nodes in Selective Forwarding Attacks," Journal Parallel and Distributed Computing, Vol. 67, No. 11, 2007.

13. X. Zhang, A. Jain, and A. Perrig, "Packet-Dropping Adversary Identification for Data Plane Security", Proc. ACM CONEXT Conf. (CoNEXT '08), 2008.

14. S. Marti, T. Giuli, K. Lai, and M. Bakar, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th. ACM Mobile Comp. & Netw. (MobiCom), pp. 255–265

15. F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks", Proc. IEEE INFOCOM, 2004.