IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 8, Issue 5 (Jan. - Feb. 2013), PP 01-03
www.iosrjournals.org

Detecting Intruders and Packet Modifiers in Wireless Sensor Networks

[1]S.Navaneethan, [2]Sudha
[1]*PG Student, Dept of CSE/ PRIST UNIVERSITY, Tiruchirappalli.*
[2]*Assistant Professor, Dept of CSE/ JPRIST UNIVERSITY, Tiruchirappalli.*

***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.*
***Index terms**: MABS-B, MABS-E, DOS*

I. Introduction:

Multicast is 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. Multicast authentication may provide the following security services like

1.Data integrity:

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

2. Data origin authentication:

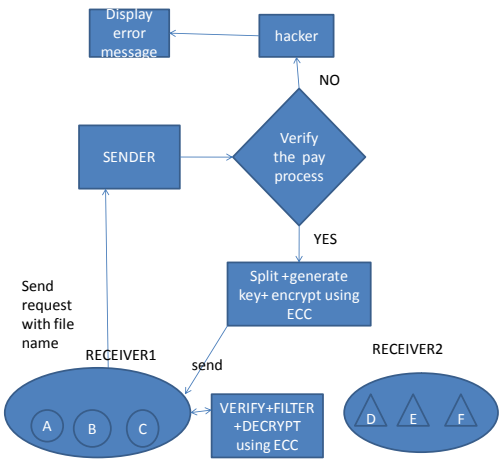
Each receiver should be able to assure that each received packets come from the real sender as it claims.

3. 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.

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. It includes two schemes. 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.

ARCHITECTURE DIAGRAM:



II. 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.

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 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. 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.

Batch Bls Signature:

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

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.

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.

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.

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.

III. Performance Evaluation:

We evaluate MABS performance 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.

Advantages Of Bls:

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.

IV. 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.

References:

[1] S.E.Deering, "Multicast Routing in internetworks and extended LANs".
[2] T.Ballardie and J.Crowcroft," Multicast specific security threads and counter measures".
[3] A.Pannetrat and R.Molva, "Efficient Multicast packet authentication".
[4] J.Jeong, Y.Park, and Y.Cho, "Efficient Dos resistant multicast authentication schemes".
[5] A.Perrig, R.Canetti, D.song, and J.Tygar,"Efficient and secure source authentication for multicast".
[6] V.Miller,"Uses of Elliptic Curves in Cryptography".
[7] N.Koblitz,"Elliptic curve cryptosystems".
[8] S.Cui, p.Duan, and C.W.Chan,"An efficient identity based signature scheme with batch verifications".
[9] R.Gennaro and P.Rohatgi,"How to sign digital streams".
[10] Yun Zhou, Xiaoyan Zhu and yuguang Fang, Fellow, IEEE.