PEER – PEER MESSAGE AUTHENTICATION WITH DIGITAL SIGNATURE IN MOBILE ADHOC NETWORK

MOHD SALMAN (Senior Faculty) Salmank64@gmail.com,
MOHD KHUBEB KHAN Student B.Tech (CTIS) khubeb626@gmail.com,
i-Nurture TMU Moradabad

Abstract-- The Main Objectives of this research are, We are Developing a Digital Signature System in which a sender send a packet with digital sign to multiple users, the receiver verify the signature. 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 non-repudiation 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.

KEYWORDS-- mobile ad hoc networks, wireless networks, transport protocols, performance evaluation, explicit feedback, TCP

INTRODUCTION

Following the widespread use of the Internet, especially the World Wide Web since 1995, MOBILE ADHOC networking has become a buzz word at the beginning of the new millennium. New terms such as MOBILE ADHOC communications, MOBILE ADHOC local area networks (WLANs), MOBILE ADHOC web, MOBILE ADHOC application protocols (WAP), MOBILE ADHOC transactions, MOBILE ADHOC multimedia applications, etc. have emerged and become common vocabulary for computer and information professionals. Among the emerging MOBILE ADHOC technologies, WLANs have gained much popularity in various sectors, including business offices, government buildings, schools, and residential homes. The set of IEEE 802.11 protocols (especially 11a, 11b, and 11g), nicknamed wi-fi, have become the standard protocols for WLANs since late 1990s. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

II RELATED WORK

As we have stated that, 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 coding schemes (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.

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.

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 MOBILE ADHOC 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 MOBILE ADHOC channel can cause packet loss very frequently. The smaller data rate of MOBILE ADHOC 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.

EXISTING 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.

III PROPOSED ALGO

Consider a set of users U with each user u having a signing public key-private key pair (PKu, SKu). To aggregate signatures on a subset of users in U, each user in that subset produces a signature σu on any message Mu. These signatures are aggregated by an aggregating party into a single signature σ, which is the same length as a single signature σu. The aggregating party has access to all the public keys, the messages, and signatures on those message, but it does not have access to any private keys. For the verifier, given a signature σ and the identities of the users who had signatures in the message, the verifier can be convinced that those users signed the message.Since the final aggregate signature is the same as the length of a single signature, we will present an aggregate signature scheme based on BLS signatures [3] described in Section 3.1. It is important to note that this scheme can produce short signatures if specific elliptic curves are used, and a summary of this adaptation on elliptic curves to produce short signatures is also presented above. The aggregation scheme has five algorithms: Key Generation, Signing, Verification, Aggregation, and Aggregate verification. All the parameters are the same as that described in the co-GDH signature scheme above. In fact, the key generation, signing, and verification are exactly the same as the scheme above. We will state them again below for completeness, and then we will provide two additional algorithms that allow us to aggregate signatures and verify these aggregate signatures.

Key Generation

Pick random x R ← Zp, and compute v ← g x 2 . The public key is v ∈ G2. The secret key is x ∈ Zp.

Signing- Given a secret key x and a message M ∈ {0, 1} ∗ , compute h ← (Hash)H(M), where h ∈ G1, and σ ← h x . The signature is σ ∈ G1.

Verification- Given a public key v, a message M, and a signature σ, compute h ← (Hash)H(M) and verify that e(σ, g2) = e(h, v) holds.

Aggregation- For the aggregating subset of users, assign to each user an index i, ranging from 1 to k. Each user ui provides a signature σi ∈ G1 on a message Mi ∈ {0, 1} ∗ of his or her choice. The messages Mi

must all be distinct. Compute σ ← Qk i=1 σi . The aggregate signature is σ.

Aggregate Verification- Given an aggregate signature σ ∈ G1 for an aggregating subset of users, indexed as before, the original messages Mi ∈ {0, 1} ∗ and public keys vi ∈ G2 for all users ui . To verify the aggregate signature σ:

1. Ensure all messages Mi are distinct, and reject otherwise.

2. compute hi ← H(Mi) for 1 ≤ i ≤ k, and accept if e(σ, g2) = Qk i=1 e(hi , vi) holds. Like the co-GDH signature, the bilinear aggregate signature requires only a single element of G1 and has the same length as any individual signature. Therefore, if we use BLS signatures for the individual signatures, we can get a short aggregate signature. Q We will briefly show correctness for the aggregate signature scheme. Given, that σ = i σi = Q i h xi i where hi is the hashed message Mi for user i and the public key for each user i is vi = g xi 2 . Using the bilinear properties, the left-side of the aggregation verification becomes: e(σ, g2) = e(Q i h xi i , g2) = Q i e(hi , g2) xi = Q i e(hi , g xi 2) = Q i e(hi , vi),which is equal to the right hand side. In the next section, we will prove security of this scheme.

IV COMPARISON OF MOBILE ADHOC NETWORK IN RESPECT TO TRANSFER PROTOCOLS AND PERFORMANCE

Type	Coverage	Performance	Standards	Applications
MOBILE ADHOC PAN	Within reach of a person	Moderate	MOBILE ADHOC PAN Within reach of a person Moderate Bluetooth, IEEE 802.15, and IrDa Cable replacement for peripherals	Cable replacement for peripherals
MOBILE ADHOC LAN	Within a building or campus	High	IEEE 802.11, Wi-Fi, and HiperLAN	Mobile extension of wired networks
MOBILE ADHOC MAN	Within a city	High	Proprietary, IEEE 802.16, and WIMAX	Fixed MOBILE ADHOC between homes and businesses and the Internet
MOBILE ADHOC WAN	Worldwide	Low	CDPD and Cellular 2G, 2.5G, and 3G	Mobile access to the Internet from outdoor areas

REFERENCES

[1] Cox, John (2002). "Report forecasts WLAN 'last-mile' boom". Network World Fusion, 08/05/02. http://www.nwfusion.com/news/2002/0805alex.html

[2] IEEE 802.11 (1999). MOBILE ADHOC LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[3] WLAN Association (2002). "MOBILE ADHOC Networking Standards and Organizations", WLANA Resource Center, April 17, 2002. http://www.wlana.org/pdf/wlan_standards_orgs.pdf

[4] KLC Consulting (2003). "Change MAC Addresses on Windows 2000 & XP". http://www.klcconsulting.net/Change_MAC_w2k.htm

[5] Wright, Joshua (2003). "Detecting MOBILE ADHOC LAN MAC Address Spoofing". http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf

[6] Vollbrecht, John, David Rago, and Robert Moskowitz (2001). "MOBILE ADHOC LAN Access Control and Authentication", a white paper from Interlink Networks Resource Library, 2001. http://www.interlinknetworks.com/images/resource/WLAN_Access_Control.pdf

[7] Interlink Networks (2002a). "MOBILE ADHOC LAN Security using Interlink Networks RAD Series AAA Server and Cisco EAP-LEAP", Application Notes at Interlink Networks Resource Library, 2002. http://interlinknetworks.com/images/resource/MOBILE ADHOC_lan_security.pdf.

[8] Walker, Jesse R. (2000). "Unsafe at any key size: an analysis of the WEP encapsulation", 802.11 Security Papers at NetSys.com, Oct 27, 2000. http://www.netsys.com/library/papers/walker-2000-10-27.pdf