International Journal of Computer Science and Informatics

Volume 2 | Issue 3 Article 4

January 2013

Basic Model of Multicast Authentication Based On Batch Signature-MABS

Hilda C.P
CSE Dept, CMRCET, Hyderabad, India ., hildascontact@yahoo.com

Mr. Liaqat Ali khan
Dept.Of IT, MJCET, Hyderabad,India., alykhan113@gmail.com

M.Grace Vennice
CSE Dept, CMRCET, Hyderabad, India ., grace_vennice@yahoo.co.in

Basic Model of Multicast Authentication Based On Batch Signature-MABS

Hilda C.P 1, Mr. Liaqat Ali khan 2, M.Grace Vennice 3, P.V.Shalini 4

2 Dept.Of IT, MJCET, Hyderabad,India.

1,3,4 CSE Dept, CMRCET, Hyderabad, India .

hildascontact@yahoo.com,alykhan113@gmail.com,grace_vennice@yahoo.co.in

Abstract **-** Traditional multicast authentication schemes manage the different involvement of the receivers by letting the sender: Choose the block size, divide a multicast stream into blocks, connect each block with a signature, and spread the effect of the Signature across all the packets in the block. The relationship between packets tends to packet loss which is very common via internet and wireless communication. For which we are going to propose novel multicast authentication protocol called MABS (Multicast Authentication Based on Batch Signature) by including two specified schemes MABS-B and MABS-E. Where MABS-B reduces the packet loss by eliminating the relationship between packets ,and due to its efficient cryptographic primitive called batch signature it provides efficient latency, computation and communication overhead .Where MABS-E improve the Dos impact by combining the basic scheme with a packet filtering mechanism while preserving the perfect resilience to packet loss.

Keyword – *MBAS, Schemes, Digital Signature, Packets, Authentication.*

I. INTRODUCTION

A multicast protocol enables a sender to efficiently disseminate digital media data to many receivers. Due to the time-sensitive requirement of some applications, reliable transmission protocol like TCP (Transmission Control Protocol) is impractical for multicast. Therefore, unreliable transmission protocol such as UDP (User Datagram Protocol) is generally adopted for multicast applications. Multicast protocol is suitable for many applications, e.g. video transmissions, live broadcasts, stock quotes, or news feeds. These applications may have many receivers or distribute time-sensitive data. To ensure secure communications between a sender and its receivers, it is important to implement security measures in a multicast environment.

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

Figure – 1 : Difference between TCP, UDP

An attacker may impersonate a sender to transmit malicious packets to receivers, causing disruptions in the communications. Multicast authentication is used to defend against forged packets injected by the attackers by enabling a receiver to authenticate the packet source and discard malicious packets. There have been many multicast authentication approaches, which can be roughly divided into two categories: symmetric cryptographic primitives and asymmetric cryptographic primitives. Symmetric cryptographic primitives, such as MAC (Message Authentication Code), generally use a symmetric key to authenticate a data source. In MAC, an identical secret key is maintained by the sender and receiver. The sender uses the secret key to generate a MAC for a packet, and the receiver is able to authenticate the packet source by verifying the MAC of the packet with the secret key. Asymmetric cryptographic primitives, such as digital signatures, use an asymmetric key pair to authenticate a data source. In general, an asymmetric key pair consists of two keys; one key is used to generate the signature, while the other key is used to verify the signature. Using digital signatures like RSA, for authentication is popular and believed to be secure; nevertheless, digital signature generation and verification incur significant computation overhead.

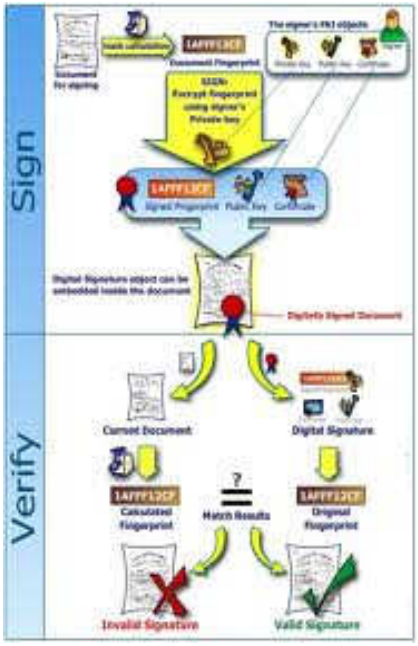

Fig.2 : The Concept of Digital Signature

In order to meet the aforementioned three requirements, we can use asymmetric key techniques. In an ideal case, each packet includes a signature generated with the sender's private key, and each receiver verifies the signature with the sender's public key. As it is well known that existing digital signature algorithms are computationally expensive, the ideal approach raises a serious challenge to receivers' computational capabilities.

II. PREVIOUS WORKS

In this Paper we are going to consider three Conventional Broadcasting authentication protocols:

1. VANET
2. VSN
3. DSRC

Vehicular Ad Hoc Networks (VANETs), inherently provide us a perfect way to collect dynamic traffic information and sense various physical quantities related to traffic distribution with very low cost and high accuracy. Such functionalities simply turn a VANET into a Vehicular Sensor Network (VSN), which is considered essential for achieving automatic and dynamic information collection and fusion in an Intelligent Transportation System (ITS). VSNs have been envisioned to have a great potential to revolutionize human's driving experiences and create a fresh new framework in metropolitan-area traffic flow control, and will undoubtedly take an important part of the future wireless metropolitan-area networks

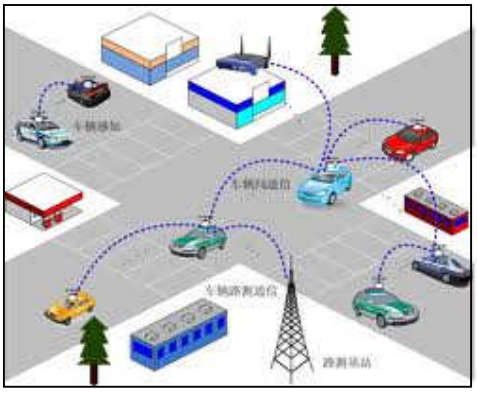

Fig.3: A Simple Functionality representation of VANET

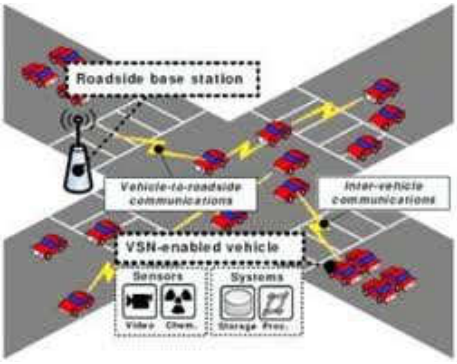

Fig.4: A simple Functionality representation of VSN

According to the Dedicated Short Range Communications (DSRC) protocol, each vehicle in a VANET broadcasts a traffic safety message every 100-300 ms, which keeps the vehicle's driving related information, such as location, speed, turning intention, and driving status (e.g., regular driving, waiting for a traffic light, traffic jam, etc.), to other vehicles. With multi-hop forwarding, the messages will be either terminated by an RSU or dropped when exceeding over their lifetimes.

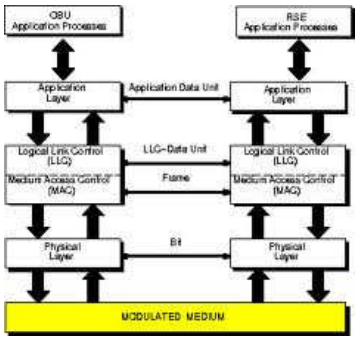

Fig.5: Layered representation of DSRC

When receiving a message, the RSU can either react to it if the sending vehicle of the message is nearby with some requests that can be handled locally (e.g., requesting to turn the traffic light to green in case no any traffic from the other direction of the intersection, and requesting for local map information, etc.), or deliver the information to a traffic control center if the message is considered to contain any possible useful information. The RSU can also monitor and summarize the traffic situation of where it is located and report it to the traffic control center. With all the collected traffic related information, the traffic control center can generate an optimized control and management strategy for traffic light control by analyzing the current traffic load in each intersection. In addition to traffic information collection for traffic flow analysis and control, VSNs can equip current transportation systems with much new value-added functionality, such as serving as a virtual "black box" for each vehicle which keeps the driving record for resolving any possible traffic dispute and reconstructing scene of accidents.

III. DESIGN & IMPLEMENTATION OF SYSTEM

The design process for software system has often two levels. At the first level the focus is on deciding which modules are needed for the system, the specifications of these modules, and how these modules should be interconnected. This is what is called the system design or top-level design.

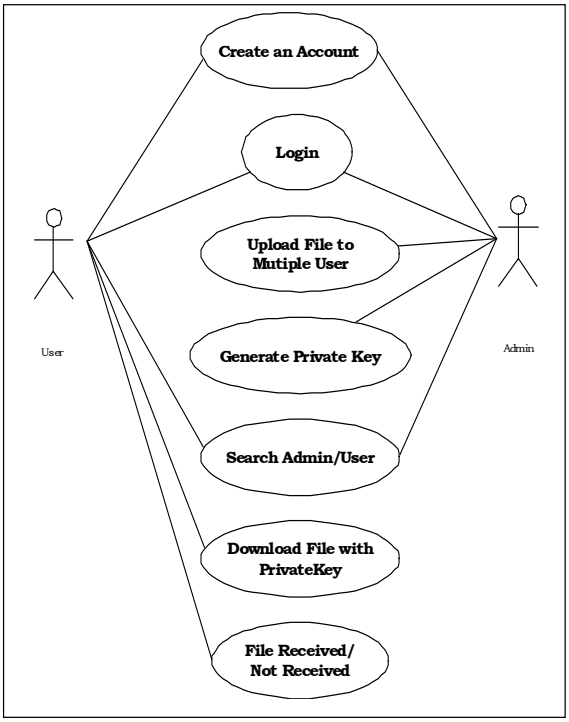

Fig.6: Interoperability Use case Diagram of the system

In the second level, the internal design of the modules, or how the specifications of the module can be satisfied, is decided. This design level often called detailed design or logic design.

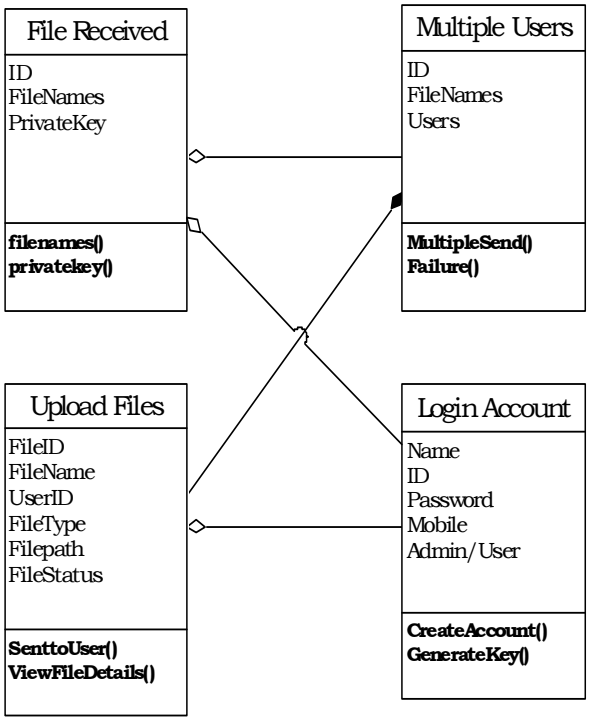

Fig.7: Interoperability Use case Diagram of the system

Our 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. MABS-E is less efficient than MABS-B, it includes the DoS defense, and its overhead is still at the same level as previous schemes.

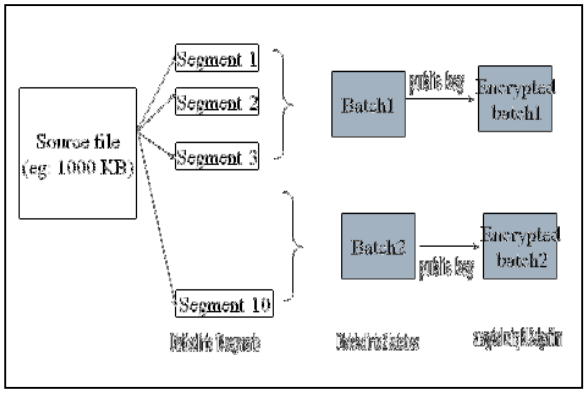

Fig.8: MBAS at Sender Side

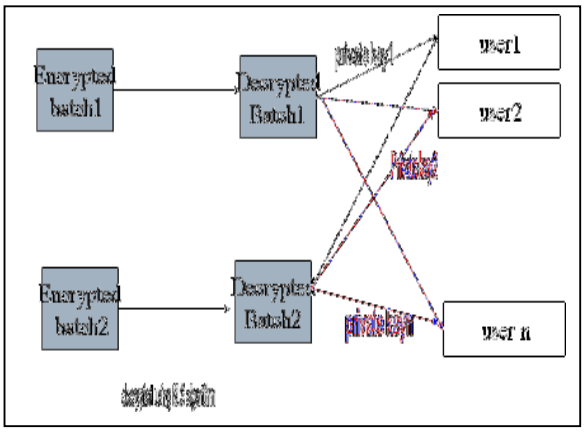

Fig.9: MBAS at Receiver Side

In order to counteract the Boyd-Pavlovski attack, our batch DSA makes an improvement to the Harn DSA algorithm. We replace the hash operation h(m) in the signature generation and verification process with h(r,m). All the other steps are the same as those in Harn's scheme. Though it is simple, our method can significantly increase the security of batch DSA. In the Boyd-Pavlovski attack, the attacker can compute r_i values and because parameters A, C, hi values are known. By introducing r_i into the hash operation, the hash values h_i in are unknown to the attacker. Therefore, the attacker cannot compute r_i values and the forgery attack is defeated. Like the cases in batch RSA and our batch BLS, the attacker may manipulate authentic packets (m_i ,(r_i , s_i) to produce invalid signatures(m_i ,(r_i , s_i), which can still pass the batch verification. The attacker can keep ri unchanged, randomly choose s_i ` i= 1,….., n-1 and solve $s_i$ ` satisfying .

$$\sum_{i=1}^{n} s_i' r_i^{-1} \bmod q = \sum_{i=1}^{n} s_i r_i^{-1} \bmod q.$$

However, this attack does not affect the correctness and authenticity of messages because they have been really signed by the sender. Therefore, the receiver can still accept them because the batch verification succeeds.

IV. RESULTS

The Obtained Results Of The Paper Are As Follows:

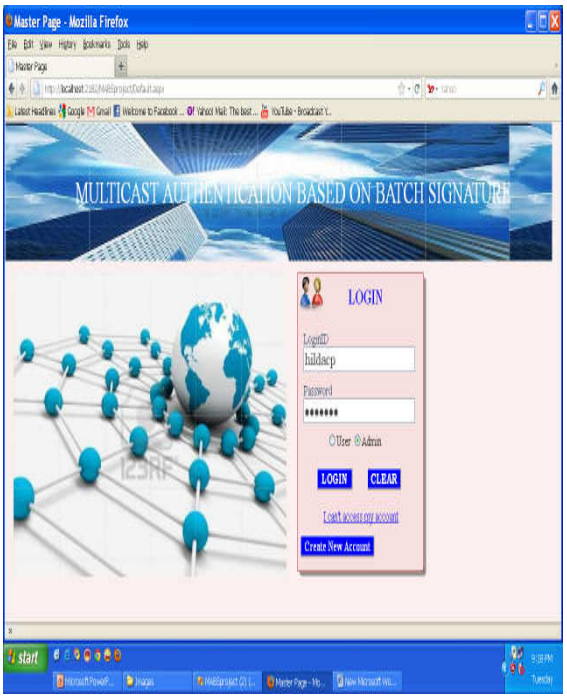

Fig.10: Admin Login Page

Fig.11: After Uploading File Admin Selects Multiple User

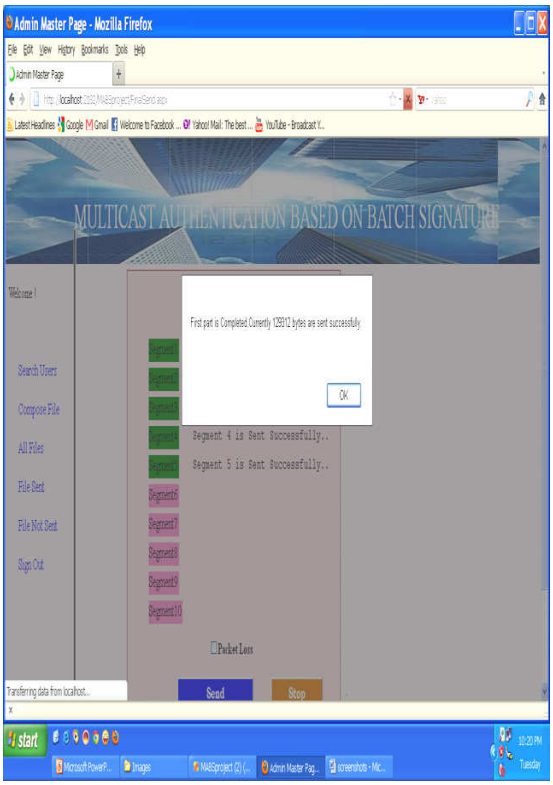

Fig.12: File Sent With Batch Signature

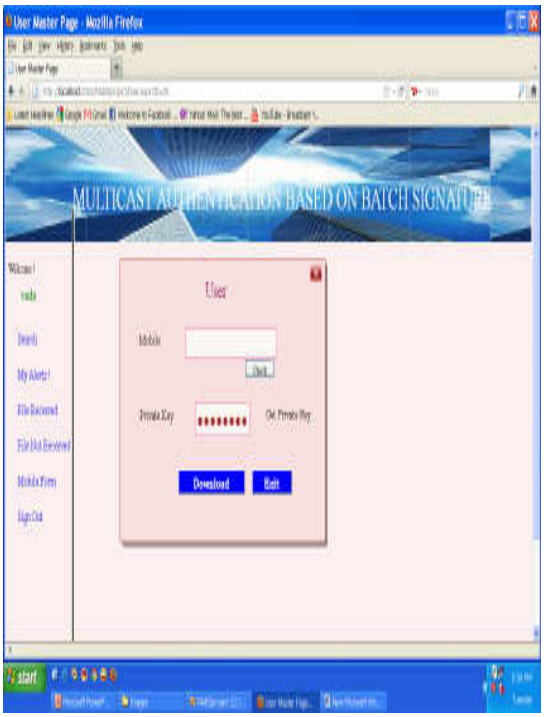

Fig.13: Generating Private Key by giving Security Question Answer

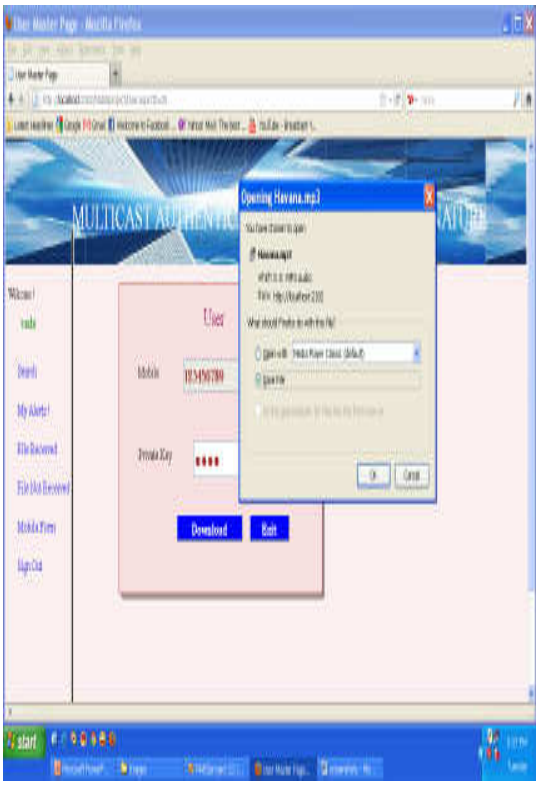

Fig.14: User Providing Private Key to Open File

V. 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. 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.

REFERENCE

[1] C. Boyd and C. Pavlovski, “Attacking and Repairing Batch Verification Schemes,” Proc. Sixth Int’l Conf. Theory and Application of Cryptology and Information Security Advances in Cryptology (ASIANCRYPT ’00), pp. 58-71, Dec. 2000.

[2] Y. Desmedt, Y. Frankel, and M. Yung, “Multi-Receiver/Multi-Sender Network Security:

Efficient Authenticated Multicast/ Feedback," Proc. IEEE INFOCOM, vol. 3, pp. 2045-2054, May 1992.

[3] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast Security: A Taxonomy and Some Efficient Constructions," Proc. IEEE INFOCOM, vol. 2, pp. 708-716, Mar. 1999.

[4] L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, vol. 24, no. 11, pp. 770-772, Nov. 1981.

[5] N.M. Haller, "The S/Key One-Time Password System," Proc.ISOC Symp. Network and Distributed Security, Feb. 1994.

[6] S. Xu and R. Sandhu, "Authenticated Multicast Immune to Denialof Service Attack," Proc. ACM Symp. Applied Computing (SAC '02),2002.

[7] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication," ACM Computing Surveys, vol. 35,no. 3, pp. 309-329, Sept. 2003.

[8] N. Koblitz, "Elliptic Curve Cryptosystems," Math. Computation, vol. 48, pp. 203-209, 1987.

[9] A. Pannetrat and R. Molva, "Authenticating Real Time Packet Streams and Multicasts," Proc. Seventh IEEE Int'l Symp. Computers and Comm. (ISCC '02), pp. 490-495, July 2002.

[10] A. Pannetrat and R. Molva, "Efficient Multicast Packet Authentication," Proc. 10th Ann. Network and Distributed System Security Symp. (NDSS '03), Feb. 2003.

[11] Y. Wu and T. Li, "Video Stream Authentication in Lossy Networks," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '06), vol. 4, pp. 2150-2155, Apr. 2006.

◈◈◈