International Journal of Information Processing, 8(1), 23-29, 2014
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

COMPARISON ANALYSIS IN MULTICAST AUTHENTICATION BASED ON BATCH SIGNATURE (MABS) IN NETWORK SECURITY

Srikanth Bethu[a], K Kanthi Kumar[b], S Soujanya[c], MD Asrar Ahmed[d]

[a]Assistant Professor, Department of Computer Science and Engineering, Holymary Institute of Technology and Science, JNTU Hyderabad - 501 301 India, Contact: srikanthbethu@gmail.com

[b]Associate Professor, Department of Electronics and Communications Engineering, Holymary Institute of Technology and Science, Hyderabad

[c]Assistant Professor, Department of Computer Science and Engineering, Holymary Institute of Technology and Science, JNTU Hyderabad

[d]Department of Computer Science and Engineering, Osmania University, Hyderabad.

Conventional block-based multicast authentication schemes overlook the heterogeneity of receivers by letting the sender choose the block size, divide a multicast stream into blocks, associate each block with a signature and spread the effect of the signature across all the packets in the block through hash graphs or coding algorithms. The correlation among packets makes them vulnerable to packet loss, which is inherent in the Internet and wireless networks. Moreover, the lack of Denial of Service (DoS) resilience renders most of them vulnerable to packet injection in hostile environments. In this paper, we propose a novel multicast authentication protocol, namely MABS, including two schemes. 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. so we discuss their comparisons and performance evaluation of Packet Loss, Comparisons over Lossy Channels, Comparisons of Signature Schemes, computationational overheads *etc.*.

Keywords : Denial of Service (DoS), MABS, MABS-BSignature Schemes.

1. INTRODUCTION

Generally, there are following issues in real world challenging the design. Efficiency: While the sender of multimedia content is usually a powerful server, receivers can have different capabilities and resources. Resilience to packet loss: Packet may be lost during wireless transmission. In the Internet, congestion at routers is a major reason causing packet loss [1].

Resilience to denial of service (DoS) attacks: Forged packets injected into a multicast stream increase the workload of receivers and cause the drop of authentic packets, leading to DoS. A certain level of resilience to DoS attacks should be provided. Recently, batch signature schemes can be used to improve the performance of broadcast authentication [2], [3].

In this paper, we present comprehensive study on this approach and propose a novel multicast authentication protocol called MABS. MABS uses an efficient asymmetric cryptographic primitive called batch signature [3], [4], [5], which supports the authentication of any number of packets simultaneously with one signature verification, to address the efficiency and packet loss problems. MABS provides data integrity, data origin authentication and non-repudiation. In addition, we make the follow-

Schemes	Sender(per packet)	Receiver (per n packets)
Batch RSA	$1\ E$	$1\ E + (2n-2)\ M$
Batch BLS	$1\ E$	$2\ P + (2n-2)\ M$
Batch DSA	$2\ M$	$2\ E + 3n\ M$

Figure 4. Computational Overhead of Different Batch Schemes

Schemes	Latency		Computation Overhead		Communication Overhead
	Sender	Receiver	Sender	Receiver	
Tree [11]	n	1	$1S + (2n-1)H$	$1V + (n\log_2 n + n)H$	$nS + n\log_2 nH$
EMSS [14]	1	n	$1S + nH$	$1V + nH$	$1S + dnH$
PiggyBack [16]	n	1	$1S + nH$	$1V + nH$	$1S + (2n - \sum_{i=1}^{r-1} k_i)H$
AugChain [18]	p	n	$1S + nH$	$1V + nH$	$1S + 2nH$
SAIDA [23]	n	m	$1S + (n+1)H + 2E_{EC}$	$1V + (n+1)H + 2D_{EC}$	$\frac{n}{m}S + \frac{n^2}{m}H$
PRABS [30]	n	m	$1S + 3nH + 2E_{EC}$	$1V + (n\log_2 n + 2n + 1)H + 2D_{EC}$	$\frac{n}{m}S + (\frac{n^2}{m} + n\log_2 n)H$
BAS [31]	1	$2n$	$1S + (n_d + n_h)H + 1E_{EC}$	$1V + (n_d + n_h)H + 1D_{EC}$	$n_sS + (n_d + n_h)H$
LTT [32]	n	m	$1S + nH + 1E_{ECC}$	$1V + nH + 1D_{ECC}$	$\frac{n}{m}S + \frac{n^2}{m}H$
MABS-B	1	1	nS	$1V$	nS
MABS-E	n	1	$nS + (2n-1)H$	$1V + (n\log_2 n + n)H$	$nS + n\log_2 nH$

Figure 5. Comparisons Over Lossy Channels:

hash algorithm MD5 [4] and SHA-1 [5] and the Signature length of three signature algorithms in MABS network generates a 320-bit signature. It is clear that by using BLS or DSA, MABS can achieve more bandwidth efficiency than using RSA and could be even more efficient than conventional schemes using a large number of hashes.

Table 2
Given the Same Security Level as 1,024-bit RSA, BLS Generates a 171- Bit Signature and DSA

Schemes	Length(bits)
→ MD-5	125
→ SHA-1	160
→ RSA	1024
→BLS	171
→DSA	320

3. CONCLUSIONS

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. To overcome these problems, we develop a novel authentication scheme MABS. We have demonstrated that 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.

REFERENCES

1. S E Deering. Multicast Routing in Internetworks and Extended LANs, *in Proceedings of ACM SIGCOMM Symposium on Communication Architectures and Protocols*, pages 55–64, Aug. 1988.
2. T Ballardie and J Crowcroft. Multicast-Specific Security Threats and Counter-

Measures, *in Proceedings of Second Annual Network and Distributed System Security Symposium (NDSS 95)*, pages 2–16, Feb. 1995.
3. P Judge and M Ammar. Security Issues and Solutions in Mulicast Content Distribution: A Survey, *IEEE Network Magazine*, 17(1):30-36, Jan./Feb. 2003.
4. Y Zhou and Y Fang. BABRA: Batch-Based Broadcast Authentication in Wireless Sensor Networks, *in Proceedings of IEEE GLOBECOM,* Nov. 2006.
5. Y Zhou, Xiaoyan Zhu and Y Fang. Multimedia Broadcast Authentication Based on Batch Signature, *IEEE Transactions on Mobile Computing*, 9(7):72–77, July 2010.

Srikanth Bethu is currently the Assistant Professor, Holy Mary Institute of Technology and Science, JNTU Hyderabad, Hyderabad. He obtained his Bachelor of Engineering from JNTU Hyderabad. He received his Masters degree in Computer Science and Engineering from Osmania University, Hyderabad.

K Kanthi Kumar is a Associate Professor, Holy Mary Institute of Technology and Science, JNTU Hyderabad, Hyderabad. He completed BTech from Nagarjuna University, A.P., India, He completed MTech (C and C) from Bharath University, Chennai. Ph.D from JNTUK, Kakinada. He was a Professor since 2010 with the Electronics and Communications Engineering, HITS college, JNTU Hyderabad. During the past 10 years of his service at various institutions he has over 5 research publications in refereed International Journals and Conference Proceedings..

MD Asrar Ahmed is a Software Engineer, Infosys, Hyderabad, since 2011.

S Soujanya is a Assistant Professor, Holy Mary Institute of Technology and Science, JNTU Hyderabad, Hyderabad.