Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Multicast Data Authentication and Detection of Bad Signature

Sneha M. Ramteke* *Assistant Professor,* *Department of Computer Technology, RGCER, Nagpur, India*

Lalasaheb B. Suryawanshi *Department of CSE,* *SGGSIE&T, Nanded, India*

Abstract—Existing digital signature algorithm is computationally expensive the ideal approach of signing and verifying each packet independently raises serious challenge to resource constraint devices. In order to reduce computation overhead we are using batch verifier and these algorithm are resilient to packet loss means if one of packet is lost still it will authenticate batch. In this paper we also identifying bad signature. If batch contain bad signature then the batch is discarded for this we are define divide and conquer verifier. Divide and conquer verifier will divide batch into half instances till bad signature not find.

Keywords —Data authentication, Batch RSA signature, Cryptanalysis, Divide and Conquer verify.

I. Introduction

Multicast is communication between a single sender and multiple receivers on a network. DATA confidentiality, authenticity, integrity, and nonrepudiation are basic concerns of securing data delivery over an insecure network, such as the Internet. Confidentiality means that only authorized receivers will get the data; authenticity, an authorized receiver can verify the identity of the data's source; integrity, an authorized receiver can verify that received data have not been modified; nonrepudiation, an authorized receiver can prove to a third party the identity of the data's source. The authentication of multicast transmissions of data streams over the Internet is a challenging problem. IP multicast is implemented with a best-effort delivery mechanism over the UDP transport protocol, where packet losses are tolerated [1]. Thus, the received stream may differ from the transmitted one. Any authentication scheme for multicast streams should verify as many as possible of the received packets without assuming the availability of the entire original stream. In addition,. it should resist against any types of attacks by an adversary, even when the adversary controls the underlying network. In this paper, our concerns are data authenticity, integrity, and nonrepudiation for delay-sensitive packet flows, particularly Flows to be delivered to large groups of receivers. For an individual message (packet), these concerns can be addressed by one of many available digital signature schemes. However, these schemes are not efficient enoughfor signing/verifying packets individually for delay-sensitive flows, such as packet video [2].

There are following issue to design a multicast authentication protocol:
Efficiency: Efficiency needs to consider for receiver. The server may be powerful but receiver may resource constrained so we have to consider capability of receiver. Second, resilience to packet loss means during wireless transmission packet might be lost. The impact of packet lost on the other packet authenticity is small as possible. In present comprehensive study on this approach and Propose a novel multicast authentication protocol called MABS. The basic scheme (called MABS-B) 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 non-repudiation based on asymmetric key protocols. The existing contributions are: MABS can achieve perfect resilience to packet loss in lossy channels in the sense that no matter how manypackets are lost the already-received packets can still be authenticated by receivers remaining In the second section we are presenting method who will identify bad signature. This method will divide batch into two parts after it will verify two parts if one of the part is unauthentic means that part contain bad signature then algorithm will divide that batch until bad signature not find.

II. Related Work

In this section, we review previous work on block based approach and its limitation. In order to reduce authentication information the SAIDA calculate hash of all packets and calculate signature on concatenated hash and this is the block signature [3][4]. The source applies IDA algorithm to both hashes and signature after that sender attaches piece of signature and hash to all packet in the block. In the receiver side apply IDA algorithm to reconstruct the authentication information and verify packet. This also has drawback it require high Computation overhead due to IDA processing. In the off-line chaining block based scheme the sender embeds in the current block of hash of the following block and so on [5] [6]. Then sender signonly first block, when receiver will get first signed block contains hash ofprevious packet and signature for first packet. Then receiver will start authenticating packet comparing hash of current to previous packet containing hash. If one of the packets is lost then total authentication chain is broken. In the on-line signing scheme if each packet is carrying one time key to sign packet [7][8].in this scheme first for sender will send signed public key for one

time signature scheme. Then it send first block along with one time signature on its hash based on the one time public key sent in previous block .The first block also contain a new one time public key to be used to verify the signature on the second block ,and this structure repeated all block. If one of the packets is lost then total authentication chain is broken. In the Canetti et al. protocol the sender attach each multicast message M, l MACs using l different keys [9]. In the receiver side receiver has to verify message using subset of keys, but receiver must know subset of keys. In the one way chain to generate chain of length k, sender select last element of chain.Then it generate key of chain by applying hash function at last k0 is secret is generated and which are sent securely. Then receiver will check received secret is valid by applying hash function till hash of this secret equal to securely send secret.

In the star chaining the block digest is simply the message digest of the m packet and block signature is block digest signed by digital signature scheme [2]. Each packet is carrying its own authentication information authentication information consist of packet signature, block signature and packet position. When receiver gets the packet it will calculate the hash of that packet and also block digest which compare to received block digest.

III. PROPOSED ALGORITHM

The senders sign each packet with signature and transmit it to multiple receivers. The receiver is resource constrained device means limited memory, computation capacity .Each receiver must assure that packet received from real sender and cannot deny the signing operation by verifying this signature. Each packet is individual authenticated then it will give full accuracy but it gives high computation cost .we also introduced block based scheme .They reduce computation cost but introduces correlation means one of the packet is lost all remaining packet are discarded and also receiver are resource constrained in this approach sender will decide size of packet because of this maybe receiver will be flooded packet and it will discard .In order to avoid this drawback our basic scheme MABS uses batch signature ,which support simultaneously verify many packet. In this receiver will collect n packet $p_i=\{m_i,s_i)$ i=1.....n. Where m_i is data payload, s_i is payload signature. Then receiver will give batch as input to Batch Verify$(p_1,p_2....p_n) \epsilon$\{True, False\}if output is true then receiver knows n packet are authentic if false .Then receiver will understand batch contain bad signature. Then our algorithm will divide batch into two half part then two part are authenticated using Batch Verify method if one of the half batch is not authenticated means it contain bad signaturethen divide batch into two part till bad signature is not authenticated.

1. BATCH RSA SIGNATURE

In order to use RSA, sender choose two large random primes P and Q to get N=PQ ,and calculates two exponent e,d Z_n such that ed=1 mod (N) where (N)=(P-1)(Q-1). The sender publishes (e,N) as the public key and keep d as its private key [10]. A signature of message m can be generated as $\sigma=(h(m))^e$ mod N , where h is hash function. The sender send (m, σ) to receiver to check authenticity of message m by checking σ^e=h(m)mod N.

If there is n packet in batch (m_i,σ_i) ,i=1…n the batch is authenticated using following equation $(\prod_{i=1}^{n} \sigma_i)^e$ mod N=$\prod_{i=1}^{n} h_i$ modN.

If this equation try to fail authenticate batch of packet means attacker succeed to manipulate signature in to packet .The batch has bad signature so we will detect this bad signature using Divide and Conquer algorithm.

2. BATCH DSA SIGNATURE

DSA is a variant integrated Schnorr and ElGamal signature algorithm [11]. Parameters in DSA are defined as follows.

P: a large prime with bit length between 512 to 1024 of the multiple of 64.
q: a large prime divisor of p – 1, and the bit length equal to 160.
g: an element in Z of order q.
x: a secret key belongs to Z
y: a public key $y=g^x$ mod p.
m: a message.

DSA's signing and verifying processes are as Follows.

a. Signing process

Step 1: The signer chooses a random number k belongs to Z.
Step 2: The signer creates signature according to the Following formulas:

$r=(g^k \bmod p) \bmod q$

$s=(k^{-1}(H(m)+xr)) \bmod q$

The signature pair (r, s) of message m will be sent to the verifier

b. Verifying process

To verify the received signature pair (r, s),the verifier compute the following formula

$((g^{sr-1}\ y^{hr-1}) \bmod p) \bmod q=r.$

This is if packet is authentic.

c. Batch DSA

Given n packet $\{m_i,(r_i, s_i)\}$, i=1…n, receiver compute batch signature by computing $h_i=h(m_i)$ and check

$((g^{\sum_{i=1}^{n} s_i r^{-1}}\ y^{\sum_{i=1}^{n} h_i r^{-1}}) \bmod p) \bmod q=\prod_{i=1}^{n} r_I \bmod q$

IV. CRYPTANALYSIS

We provide two methods to forge individual signature and make false batch verification. In the first method, we assume signer Alice sends message to the receiver Bob. Lets$'_i$=h(M$_{(f(i))}$)^d, whereS$'_i$is forged signature ofS$_i$and f(.)is ne to one function, f(i)=j, i=1,2,....t, j=1, 2 ...t.Alice sends the forged pairs (M$_i$, S$'_i$), i=1,2...t ,to Bob . Then Bob will check ($\prod_{i=1}^{t} s'_i$)e=$\prod_{i=1}^{t} h(M_{f(i)})$mod n, Bob isconvinced that message is from Alice.

In the second method, we assume that Alice sends (S'$_1$, M$_1$), (S$'_2$, M$_2$), . . . , (s$'_t$, M$_t$) to Bob and letsS$'_i$ = $a_i \times S_i$, i = 1, 2, . . . , t, where $\prod_{i=1}^{t} a_i = 1$. Since $\prod_{i=1}^{t} s'_i)^e$=($\prod_{i=1}^{t} h(M_i)$mod n) , Bob is convincedthat these messages were signed by Alice.

V. DIVIDE AND CONQUER VERIFY (DCV)

Input to this algorithm is batch with bad signature. This batch consist of (m$_i$, s$_i$) where i=1…..n , m$_i$message, s$_i$signature of m$_i$.

1 If batch consist of n=1 packet then apply the batch verify algorithm if output is true then exit otherwise output bad signature and exit.
2 If batch consist of packet n>1 then apply the batch verify it fails go to the step 3.
3 Divide the batch into two half part till the bad signature not find.

VI. PERFORMANCE EVALUATION

In this section, we evaluate performance in terms of resilient to packet loss, efficiency, authentication latency and DOS resilience.

1. Resilient to packet loss:

The metric here is verification rate means ratio of number of authenticated packets to the number of received packet. The verification rate of EMSS , augmented chain,piggyback are decreased quickly when packet loss id increased. The reason is correlation among the packet. Our MABS and tree chaining are perfect resilient to packet loss because each packet is independent from each other. In tree chaining achieve independency by incurring large overhead and latency at sender and receiver.

2. Efficiency:

We consider authentication latency, computation, and communication overhead for efficiency evaluation. The block based approach requires each receiver to collect an entire block before authenticating every packet in block. These correlations among packet achieve higher computation efficiency, but also longer authentication latency. In the MABS does not have authentication latency, because there isno relationship among packet and receiver can verify batch depend on its buffer size.

3. DOS Resilience:

DoS is method for attacker to consume the resource of receiver. In tree chaining, star chaining, hash chaining in this signatureauthenticated first and then packet are authenticated, attacker can forge signature. The divide and conquer is method to DoS resilience.

VII. EXPERIMENTAL RESULT

In this we calculate performance on number of times batch Verify algorithm called in verify process.If batch signature passes the test, then verifier accept all batch. However if verifier fail to authenticate batch he cannot reject all signature in the batches .The verifier cannot detect the bad signature. The simplest solution checks the all packet one by one.In this if batch has n packet (m$_i$ s$_i$) where i=1….n. in thisit will call n times batch verify algorithm if the batch verify output is true then exit otherwise bad signature packet but it call the batch verify algorithm n times so we have to reduce verification.

In the Matrix method when receiver get batch of packet it will arrange in the matrix form and rows and columns are checked whether bad signature is present or not. In this method minimum batch verify required is (n + n) if matrix is n x n.

If the batch consist of one bad signature, from table 1 show the numbers of times batch verify algorithm called in verify process. In Fig 1, Fig 2 X axis indicates number of message in batch and y axes indicate # of times batch verify algorithm called.

Table 1. DCV and Matrix for one bad signature

Message	DCV	Matrix
16	8	8
64	12	16
100	14	20
400	18	40
900	20	60

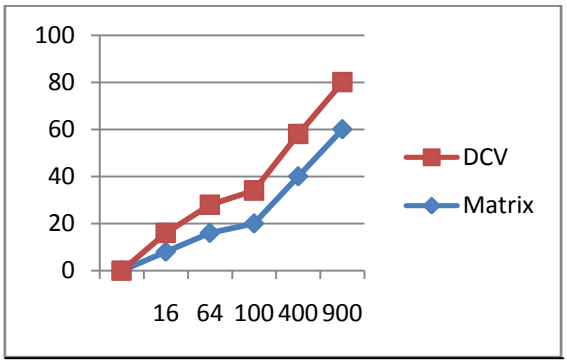

Fig 1. Comparison of Matrix and DCV.

If the batch consists of two bad signature at time number of times Batch verify algorithm called is shown below table. Each batch consist of m message.

Table 2. DCV and Matrix for two bad signature

Message	DCV	Matrix
25	18	14
100	26	24
225	30	34
400	34	44
900	38	64

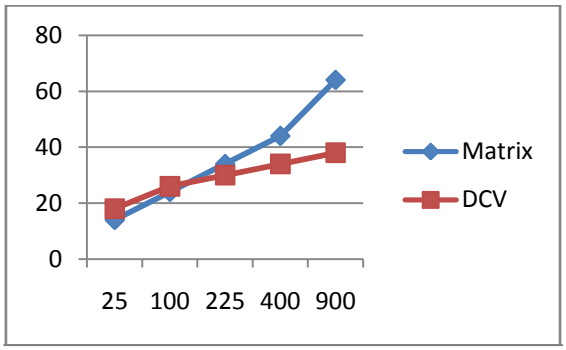

Fig 2.Comparision of Matrix and DCV

The computation time required depend on number times batch verify algorithm called ,in the matrix algorithm batch verify algorithm called more as compare to DCV .

Table 3. Time for Matrix and DCV

Method	Message	Time
Matrix	25	1.092
DCV	25	0.773
Matrix	100	2.283
DCV	100	1.322
Matrix	256	3.535
DCV	256	2.349

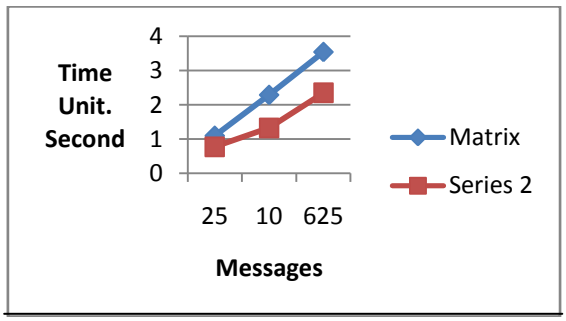

Fig 3. Comparison of Matrix and DCV.

VIII. ANALYSIS OF ILLEGAL SIGNATURE DETECTION

In the Divide and Conquer computation overhead in measured in terms of number of times batch verifier is called. In this we will see two conditions: if only one illegal signature is present and more than two illegal signatures are present.

1. ONE ILLEGAL SIGNATURE

In this case if number of times verifier called is equal to (2logn). Where n is number of packet contain in the batch.

2. MORE THAN TWO ILLEGAL SIGNATURE

In this case if number of times verifier called is equal to 2(blogB-1+2(logn + logb). Where n is number of packet contain in the batch, b number of bad signature contain in the batch.

IX. CONCLUSIONS

While transmitting data in a network, existing system faces some problems like signature verification, congestion, computingblock size, vulnerability to packet loss and lack of resilience to denial of service (DoS) attack. To overcome these problems for this we are using MABS system. MABS will be a perfect solution to packet loss due tothe elimination of the correlation among packets and can effectively deal with DoS attack. If the batch consists of bad signature then the batch verifier will reject this batch for this we also detecting bad signature in the packet using divide and conquer algorithm.

References

[1] Anna Lysyanskaya ,Roberto Tamassia and Nikos Triandopoulos, "Multicast Authentication in Fully Adversarial Network ", IEEE Comm. Magazine, vol. 45, no. 8,pp. 72-77, Aug. 2007.
[2] C. Wong and S. Lam, "Digital Signatures for Flows and Multicasts,"IEEE/ACM Trans. Net., vol. 7, 1999.
[3] J.M. Park, E.K.P. Chong, and H.J. Siegel, "Efficient Multicast Packet Authentication Using Signature Amortization," Proc. IEEE Symp. Security and Privacy (SP '02), pp. 227-240, May 2002.
[4] J. M. Park, E. K. P. Chong, and H. J. Siegel, "Efficient Multicast Stream Authentication Using Erasure Codes," ACM Trans. Info.and Sys. Security,vol. 6, no. 2, May 2003, pp. 258–85.
[5] R. Gennaro and P. Rohatgi, "How to Sign Digital Streams," Information and Computation, vol. 165, no. 1, Feb. 2001, pp. 100–16.
[6] R. Gennaro and P. Rohatgi, "How to Sign Digital Streams," Advances in Cryptology, CRYPTO'97, 1997.
[7] S. Even, O. Goldreich, and S. Micali, "On-line/Off-line Digital Signatures,"Advances in Cryptology – Crypto'89, LNCS vol., no. 435, 1990, pp. 263–75.
[8] S. Even, O. Goldreich, and S. Micali, "On-line/Off-line Digital Signatures," J. Cryptology, vol. 9, no. 1, 1996, pp. 35–67.
[9] R. Canetti et al., "Multicast Security: A Taxonomy and Efficient Constructions," INFOCOM, 1999.
[10] L. Harn,"Batch Verifying Multiple RSA Digital Signatures," IEE Electronic Letters, vol. 34, no. 12, pp. 1219-1220, June 1998.
[11] L. Harn, "DSA-Type Secure Interactive Batch Verification Protocols,"IEE Electronic Letters, vol. 31, no. 4, pp. 257-258, Feb. 1995.
[12] Min-shiang HWANG, Iuon-chung LIN,"Crypanalysis of the Batch verifying Multiple RSA Digital Signarures", INFORMATICA ,2000, Vol. 11 ,no. 1,15-19.

