World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 264-269, 2014
ISSN 1818-4952
© IDOSI Publications, 2014
DOI: 10.5829/idosi.wasj.2014.29.csea.2256

Elliptic Curve Cryptography Using in Multicast Network

V. Khanaa, K.P. Thooyamani and R. Udayakumar

School of Computing Science, Bharath University, Chennai-73, India

Abstract: Multicast is an efficient method to deliver multimedia content from a sender to a group of receivers and is gaining popular applications such as real time stock quotes, interactive games, video conference, live video broadcast, or video on demand. 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. The lack of Denial of Service (DoS) resilience renders most of them vulnerable to packet injection in hostile environment. In this paper, 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 algorithm called batch signature, which supports the authentication of any number of packets simultaneously. The enhanced scheme MABS-E, which combines the basic scheme with a packet filtering mechanism to prevent Dos attack and packet loss and also using elliptic curve cryptography algorithm for improve the performance of MABS (Multicast Authentication Batch Signature).

Key words: MABB-B · DOS · Cryptography · WAP · Multicasting · DLP

INTRODUCTION

The extensive use of mobile communication has created an important demand for value-added services. WAP (wireless application protocol) is a framework for developing application to run over wireless networks. And authentication is one of the critical topics in securing multicast [2-4] in an environment attractive to malicious attacks. There are the following issues in real world challenging the design of Multicast authentication protocol. First, efficiency needs to be considered, especially for receiver the receiver heterogeneity requires that multicast authentication protocol be able to execute on not only the powerful desktop computer but also resource constrained, mobile handset. In particular, latency, computation and communication overhead are major issues to be considered. Second, packet loss is inevitable in the internet, congestion at routes is a major reason causing packet loss.

Efficiency and packet loss resilience can hardly be supported simultaneously by conventional multicast schemes. As well known that existing digital signature algorithm are computationally expensive the ideal approach of signing and verifying each packet independently raises the serious challenge. In order to reduce computation overhead, conventional schemes use efficient algorithm [8, 9] at the expense of increased communication overhead or vulnerability to packet loss [12].

Another problem with scheme in [8-10] is that they are vulnerable to packet injection by malicious attackers. A attacker may compromise a multicast system by intentionally injecting forged packets to consume receiver resource, leading to denial of services (Dos)

In the literature, some scheme [13] attempt to provide the Dos resilience However, they still have the packet loss problem because they are based on the same approach as previous schemes [10, 11].

Corresponding Author: V. Khanaa, School of Computing Science, Bharath University, Chennai-73, India.

Recently, the batch signature schemes can be used to improve the performance of broadcast authentication [5, 6], In this paper, i present comprehensive study on this approach and propose a novel multicast authentication protocol called MABS (in sort for multicast authentication based on batch signature). MABS include two schemes. The basic schemes (called MABS-B) utilize an efficient asymmetric cryptographic called batch signature with support the authentication of any number of packet simultaneously with one signature verification to address the efficiency and packet loss problems in general environment the enhanced scheme (called MABS-E) combines MABS-B with packet filtering to alleviate the Dos impact in hostile environment.

Contribution of the Paper: MABS provides data integrity, origin authentication and non repudiation asymmetric key based protocols. In addition, make the following contribution

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 packet can still be authenticated by receivers.

MABS-B is efficient in terms of less latency, computation and communication overhead. Through MABS-E is less efficient than MABS-B since it include the Dos defense, its overhead is still at the same level as previous schemes.

And I propose new batch signature schemes based on ECC and show the are more efficient than the batch RSA[11] signature schemes.

Existing and Proposed System: Existing system of 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 draw back of the existing system are correlation among packets makes them vulnerable to packet loss, which is inherent in the Internet and wireless networks. and The lack of Denial of Service (DoS) resilience renders most of them vulnerable to packet injection in hostile environments the proposed system is 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. and also present an enhanced scheme MABS-E, which combines the basic scheme with a packet filtering mechanism to alleviate the DoS impact while preserving the perfect resilience to packet loss.the advantages of the proposed system is overcomes the DOS attacks. and handling hackers in the root node & non repudiation process.

Related Work: Scheme in [8, 9] follow the ideal approach of signing and verifying each packet individually, but reduce the computation overhead at the sender by using one-time signature [8] or K time signature.

Three chaining was proposed in [10, 11] by constructing a tree for a block of packet. Each the packet carries the signed root and multiple hashes. When each receiver receive s one packet in the block it used the authentication information in the packet to authenticate it. Each packet is independently verifiable at a cost of per-packet signature verification.

All the schemes [10-12] are indeed computationally efficient since each receiver needs to verify only one signature for block of packets. Another major problem is that most schemes [12, 13] are vulnerable to packet loss even through they are designed to tolerate a certain level of packet loss, if too many packet lost, other packet may not be authenticated. If a block signature is lost, the entire block cannot be authenticated.

Basic Schemes: Target of this paper is to authenticate multicast streams from a sender to multiple receivers. 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 is ales powerful device with resource constraints and may be managed by nontrustworthy person. Each the receiver need to receive that the received packets are really from the sender and the sender cannot deny the signing operation(non repudiation) by verifying the corresponding signature.

In order to fulfill the requirement, the basic scheme MABS-B uses an efficient cryptographic primitive called batch signature [11], which supports simultaneously verifying the signatures of any number of packets. In particular, when a receiver collects, *n* packets:

$p_i = \{m_i, \sigma_i\} \quad i = 1,...,n$

where m_i is the data payload, σ_i is the corresponding signature and n can be any positive integer, it can input them into an algorithm

Batch Verify$(p_1, p_2, ..., p_n) \in \{True, False\}$.

If the output is *True,* the receiver knows the n packets are authentic and otherwise not.

To support authenticity and efficiency, *Batch Verify*() the algorithm should satisfy the following properties:

Given a batch of packets the have been signed by the sender, *Batch Verify*() outputs *True*.

Given a batch of packets including some unauthentic packets, the probability that *Batch Verify* ( ) outputs *True* is very low.

The computation complexity of *Batch Verify* ( ) is comparable to that of verifying one signature and is increased only gradually when the batch size n is increased.

Batch RSA Signature: The sender sends $\{m, \sigma\}$ to a dreceiver that can verify the authenticity of the message m by checking σ^e $h()mod\ N$.

Batch RSA: To accelerate the authentication of multiple signatures, the batch verification of RSA [35], can be used. *M* Given packet $\{m_i, \sigma\}$, $i = 1,...,n$ where m_i is the data payload, σ_i is the corresponding signature and n is any positive integer, the receiver can first calculate $h_i = h(m_i)$ and then perform the following verification:

$$\left(\prod_{i=1}^{n} \sigma_i\right)^e mod\ N = \prod_{i=1}^{n} h_i \ \mathrm{mod\ N.} \qquad (1)$$

The public-key cryptosystem that has been in practical use the longest and is still the most popular system for electronic commerce is RSA. The basic construction is rather simple.

Let the n-bit integer

$$N = pq \qquad (2)$$

be the product of two large primes of roughly the same size. Typically, N has about 1000 bits and p and q each have about 5003 bits. Let e and d be two integers satisfying

ed a 1 (<p(N)), where cp (N)=(p-i)(q-i)-N+1-(p+q) (3)

is the Euler <p function of N, equal to the number of integers 0 < I < N that are relatively prime to N. These integers N,e.d are called, respectively, the RSA modululs, the encryption exponent and the decryption exponent. The first two form the public key and are made publicly known. The integer d, sometimes called the secret exponent, is the private key known only to the person who receives the enciphered message.

Using Euler's theorem from elementary number theory, one can easily show that

Cd = Med = m (Mod N) (4)

Anyone who succeeds in factoring N = pq can immediately break RSA by finding an inverse of e modulo (p-1)(q-1). For many years it was conjectured that conversely, the only way that RSA can be broken (in other words, the only way that the encryption function can be inverted) is to factor N.

ECC Algorithm: The public cryptosystem of ECC is greater flexibility in choosing cryptography system and no known sub exponential time algorithm for ECDLP and small key size(with the same security) and greater speed, less storage.

Let G be an abstract (multiplicative) group (= a set with a multiplication operation) find a computer realization of G such that.

- The operation "exponentiation" a -> b : = a^n can be implemented as a quick, efficient algorithm;
- The inverse operation ("discrete logarithm"), i.e., (DLP) Given a and b ϵ *G*, find n(:=log$_a$(b)") such that

$$b = a^n = \underbrace{a \cdot a \cdots a}_{n\ times},$$

Consider the following elliptic curve $E_{2,1}$ over F_s:

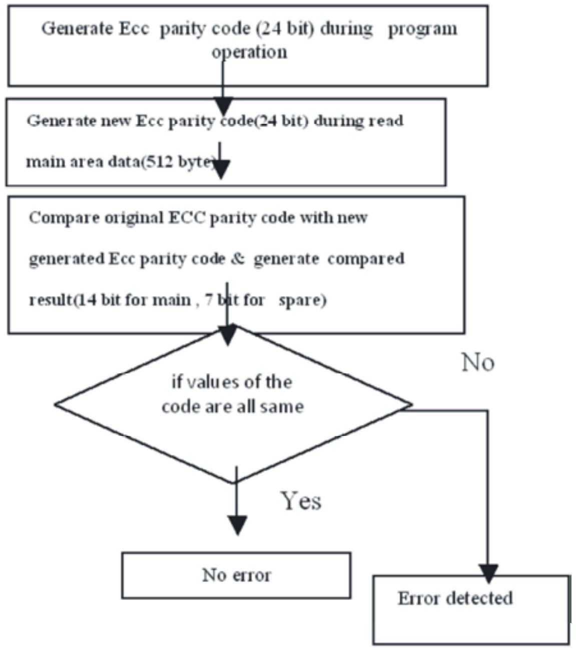
$$E = E_{2,1}: \qquad y^2 = x^3 + 2x + 1$$

Then a quick calculation (exhaustive search) shows that

$E(F_s) =$

$$\{\underbrace{P_\infty}_{P_0}, \underbrace{(0,1)}_{P_1}, \underbrace{(1,3)}_{P_2}, \underbrace{(3,3)}_{P_3}, \underbrace{(3,2)}_{P_4}, \underbrace{(1,2)}_{P_5}, \underbrace{(0,4)}_{P_6}\}$$

Processing Procedure:


Generate Ecc parity code (24 bit) during program operation
Generate new Ecc parity code(24 bit) during read main area data(512 byte)
Compare original ECC parity code with new generated Ecc parity code & generate compared result(14 bit for main , 7 bit for spare)
if values of the code are all same
No
Yes
No error
Error detected

For example, $P_4 = (3,2) \epsilon E(Fs)$ because

$3^3 + 2 \bullet 3 + 1 = 34 = 4 = 2^2$ (mod 5).

The above points P_i have been numbered in such way that

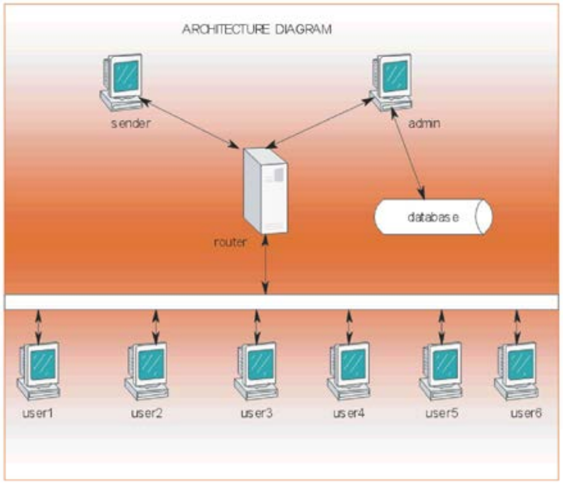
$P_i + P_j = P_{i+j}$ (indices mod 7)

Thus, $\#E(F_s) = 7$, which satisfies the Hasse bound since

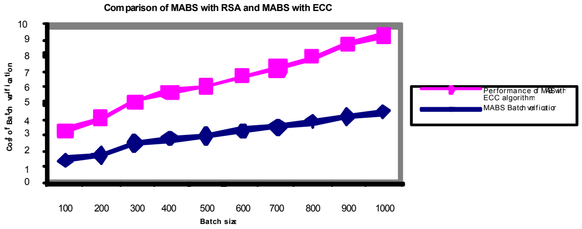
$|(5+1)-7| = 1 \leq 2\sqrt{5} = 4.47.$

Enhanced Scheme: The MABS-B targets at the packet loss problem, which is inherent in the Internet and wireless networks. Some circumstances, the attacker can inject forged packets into a batch of packets to disrupt the batch signature verification. The DoS attack is to divided the batch into multiple smaller batches and perform a batch verification over each smaller batch and this divide-and-conquer approach can be recursively carried out for each smaller batch.

In this section, I present an enhanced scheme called MABS-E, which combines the basic scheme MABS-B and a packet filtering mechanism to tolerate packet injection and also using ECC for improving the performance of the MABS, transferring data from a sender to the receiver the form of the encryption/decryption in secure manner and also implementing and ensure the packet form the real sender never falls in to any set of packet form 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 does not need to divide the set into smaller subsets for further batch verification.



System Architecture:



Admin is a system which having information about all the system connected in the network such as system port no, IP address and status. Every system must communicate with admin or server. Sender is a system which is connected with server and router which having files Files is nothing but text document, or audio file, video etc,. If any client system want to the request to the sender system it send the file to the corresponding system All the files or resources transmitted via the router. Route is a electronic devices that inter connected with the two or more networks and selectively inter change packet of data between them.

Each data packet contain information that a router can use to determine.

If the source and destination on or if the data packet must be transfer from one network to devices.

Client is a system which having port no, IP address which makes a request to any system (any system is server or may be sender system).

Modules Description

Data Integrity: Each receiver should be able to assure that received packets have not been modified during transmissions. This can be done with the help of hashing technique. Here unwanted packets will also be removed

Data Origin Authentication: Each receiver should be able to assure that each received packet comes from the real sender as it claims. This can be achieved through cryptographic technique. Here RSA algorithm is used for data origin authentication.

Non Repudiation: 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. The accessibility is given for those users who paid for it. Once they got access they will receive all the data and even the sender can't forbid.

Handling Hackers: Finding hackers in the root node. and then the sender system intimated to the admin. With the help of the admin hackers system will shutdown.

Performance Evaluation: In this section, performance evaluation of the public-key cryptosystem operation in MABS protocols is given. I considered there factors are examined in the drawback of the existing systems is the correlation among the packets makes them vulnerable to packet loss, which is inherent in the Internet and wireless networks and the lack of Denial of Service (Dos) resilience renders most of them vulnerable to packet injection in hostile environments and I have derived the two factors and also overcomes the DOS attacks, overcoming the hacking & non-repudiation.

The formulations vary depending on the key exchange suit. ECC and RSA key exchange suites. The formulations could not be given in this paper due to space limitations.

Moreover, I have implemented ECC and RSA cryptosystem operations. Table 1 demonstrates approximate comparable key sizes for ECC and RSA cryptosystems. Six different predefined elliptic curves shown in Table 1, as levels 1 and 2. Those curves are recommended MABS Standard. We also included implementations for three additional curves (namely 256P, 283K and 283R in Table 1) which provide much higher security to given an idea about the cost of using more secure curves than those recommended in MABS Standard.

Table 1: Cryptographic Strength of RSA and ECC

Strength Level	ECC	RSA
1	160P, 163K, 163R	1024
2	224P. 233K, 233R	2048
3	256P, 283K, 283R	3072

Finally, I have taken timing of the cryptosystems of Table 1 and used them to sketch the performance of public-key cryptography in MABS.

Analyse the those figures evaluate the effect of cryptosystem choice on the performance of MABS and obtained the following result.

> ECC a best curve option for each security level and MABS protocol. In other words, ECC is better than RSA in MABS. The "R" family of curve (163R, 233R and 283R) performs worse than other curves. Thus, the best curve option is either "P" (160P, 224P, 256P) curves or "K" (163K, 233K, 283K) curves.

The performance of RSA is generally poor. For some cases, it is unacceptably slow (e.g RSA_2048 and RSA_3072, RSA_1024 and 2048.

RSA cryptosystem works well for the client, but bad for the server, then a performance conflict occurs. RSA_1024 and RSA_2048 cause such a conflict for the MABS protocol with server-only authentication.

A similar performance conflict between the client between the client and server is valid for ECC too. For example, the best level 2 curve for client in server-only authentication protocol is 224P, but is 233K for the server. However, the level of conflict in ECC is not so sever since the performances of the conflicting curves are close to each other.

RSA produces more data to be exchanged than ECC. In other words, using RSA requires more transmission time than using ECC. This is another advantage of ECC over RSA. This fact is valid for all security levels and protocols.

Future Enhancement: Blocking the malicious node from the network and it can be recovered with the help of admin.

CONCLUSIONS

In order to reduce the signature verification overheads in the secure multimedia multicasting, block-based authentication schemes and improving the performance of MABS with help of ECC have been proposed 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, I develop a novel authentication scheme MABS I 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. Show that the use of batch signature can achieved the efficiency less than or comparable with the conventional schemes.

REFERENCES

1. Deering, S.E., 1988. Multicast Routing in Internetworks and Extended LANs, Proc. ACM SIGCOMM Symp. Comm. Architectures and Protocols, pp: 55-64.
2. Ballardie, T. and J. Crowcroft, 1995. Multicast-Specific Security Threats and Counter-Measures, Proc. Second Ann. Network and Distributed System Security Symp. (NDSS ’95), pp: 2-16.
3. Judge, P. and M. Ammar, 2003. Security Issues and Solutions in Mulicast Content Distribution: A Survey, IEEE Network Magazine, 17(1) 30-36.
4. Challal, Y., H. Bettahar and A. Bouabdallah, 2004. A Taxonomy of Multicast Data Origin Authentication: Issues and Solutions, IEEE Comm. Surveys & Tutorials, 6(3): 34-57.
5. Zhou, Y. and Y. Fang, 2006. BABRA: Batch-Based Broadcast Authentication in Wireless Sensor Networks, Proc. IEEE GLOBECOM.
6. Zhou, Y. and Y. Fang, XXXX. Multimedia Broadcast Au