MAS: MULTICAST AUTHENTICATION SYSTEM- A COMPARATIVE STUDY

Charles C Sebastian[1], George Mathew Kurian[2], Jazah Javed[3],
Joseph Mathew[4], Asst. Prof. Ansamol Varghese[5]
Dept. of Computer Science and Engineering, Amal Jyothi College of Engineering
Kanjirapally, Kerala, India

Abstract: Wireless Sensor Network (WSN) consists of one or more powerful base stations and hundreds of sensor nodes [1]. Base stations serve as gateways between Internet users and sensor nodes. Due to potential applications in environmental monitoring, target tracking and object detection, WSNs have been drawing great attention in recent years. Security is a very critical problem for WSNs, as they are highly affected by harmful threats. It is always better to authenticate every message being transmitted over the network so as to monitor, identify and prevent possible threats to it. Public Key Cryptography (PKC) is widely used for broadcast and multicast authentication. The intensive use of PKC for multicast authentication, is found to be quite expensive to data constrained sensor nodes. The proposed system is a java application which compares three types of encryption methods namely Hash Message Authentication Code (HMAC), Elliptic Curve Digital Signature Algorithm (ECDSA) using signature amortization and RSA during multicasting of data the results are displayed in the form of a graph. The ECDSA in theory is said to be the most efficient of the three algorithms and this application will prove the same during the multicasting of messages to the sensor nodes from the base station of the WSN.

Index Terms: Multicast authentication, signature amortization, ECDSA, wireless sensor networks, RSA, HMAC, Authentication.

I. INTRODUCTION

A sensor network is a system that consists of thousands of very small stations called sensor nodes [2].The main function of sensor nodes is to monitor, record, and notify a specific condition at various locations to other stations and end users . and this presents a wide range of applications that motivates research in sensor networks. The communication among nodes is done in a wireless fashion, and thus, the name of wireless sensor networks emerged. Several features make wireless sensor networks special compared to other categories of computer networks. The most important feature is the hardware; the sensor nodes have small sizes and have the ability to transfer data at low energy, because we are sending only text. Furthermore, sensor networks are subject to more severe power constraints than POAs, mobile phone, or laptops. The whole network is usually under the administration of one controller, the base station. In a multicast network[3], a single copy of packets is sent by the sender and routed to every receiver within the same multicast group via multicast-enabled routers. Multicast is an efficient and natural way of communicating information for a wide range of applications. Some examples include information broadcasts (e.g., news feeds, weather updates, and stock quotes), multiparty videoconferencing and software updates. For successful implementation of multicasting, many of these applications will require varying degrees of security requirements i.e., confidentiality and authentication. Confidentiality for multicast transmissions can be provided using techniques that utilize symmetric (secret) key cryptography.

Confidentiality would be provided by encrypting the message with the secret key being shared by the sender and the receivers of the multicast group before transmission. The proposed scheme is to enhance ECDSA to implement a secure multicasting scheme in wireless sensor networks that ensures confidentiality, authentication and integrity of messages and reduces the overhead in message transmission significantly. The scheme overcomes the vulnerabilities in symmetric based schemes and reduces the overhead for message authentication significantly. A single signature is used for the authentication of entire multicast messages, which is generated by a variant of elliptic curve cryptography known as Elliptic Curve Digital Signature Algorithm[4].

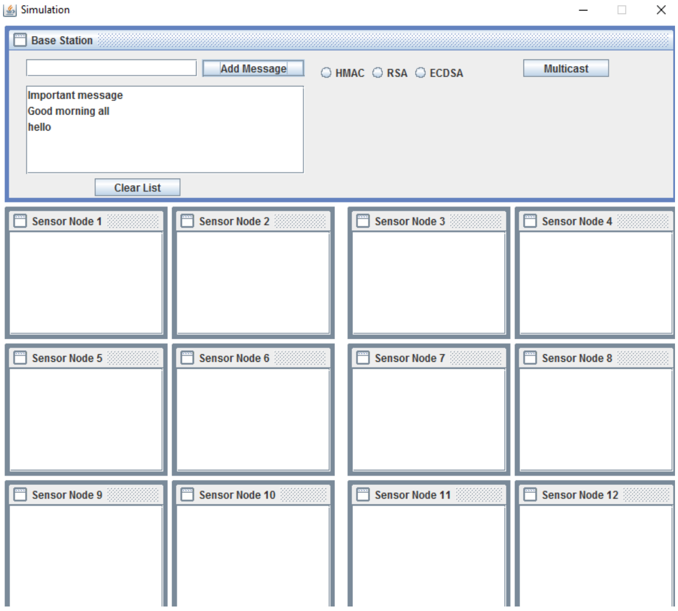
This reduces the overhead of having separate signature for each message significantly. We also compare this newly implemented scheme with the already established schemes like RSA and HMAC. The rest of this paper is organized as follows. The system model is introduced in section II. The proposed PKC based broadcast authentication scheme using signature amortization is presented in section III. The results of the comparisons are presented in section IV. The application of this technique for cloud computing authentication is shown in section V followed by the conclusion in section VI and references in section VII.

II. SYSTEM MODEL

The system designed for comparative purposes is a java application which contains one base station and twelve sensor nodes to form the basic WSN architecture. All three modes of encryption methods are used for the comparison and the results are displayed in the form of a graph.

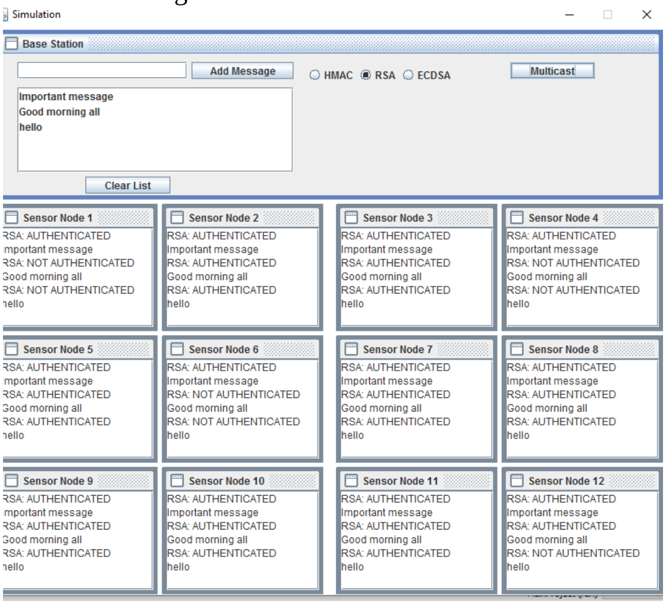
Figure 1: Java application

The users are allowed to perform the comparison in a simulation environment and all the data and time taken for authentication are recorded.



```
Important message
Good morning all
hello
```

Figure 2: Interface for simulation



```
Important message
Good morning all
hello
```

Sensor Node 1

```
RSA: AUTHENTICATED
mportant message
RSA: NOT AUTHENTICATED
Good morning all
RSA: NOT AUTHENTICATED
hello
```

Sensor Node 2

```
RSA: AUTHENTICATED
Important message
RSA: AUTHENTICATED
Good morning all
RSA: AUTHENTICATED
hello
```

Sensor Node 3

```
RSA: AUTHENTICATED
Important message
RSA: AUTHENTICATED
Good morning all
RSA: AUTHENTICATED
hello
```

Sensor Node 4

```
RSA: AUTHENTICATED
Important message
RSA: NOT AUTHENTICATED
Good morning all
RSA: NOT AUTHENTICATED
hello
```

Sensor Node 5

```
RSA: AUTHENTICATED
mportant message
RSA: AUTHENTICATED
Good morning all
RSA: AUTHENTICATED
hello
```

Sensor Node 6

```
RSA: AUTHENTICATED
Important message
RSA: NOT AUTHENTICATED
Good morning all
RSA: NOT AUTHENTICATED
hello
```

Sensor Node 7

```
RSA: AUTHENTICATED
Important message
RSA: AUTHENTICATED
Good morning all
RSA: AUTHENTICATED
hello
```

Sensor Node 8

```
RSA: AUTHENTICATED
Important message
RSA: AUTHENTICATED
Good morning all
RSA: AUTHENTICATED
hello
```

Sensor Node 9

```
RSA: AUTHENTICATED
mportant message
RSA: AUTHENTICATED
Good morning all
RSA: AUTHENTICATED
hello
```

Sensor Node 10

```
RSA: AUTHENTICATED
Important message
RSA: AUTHENTICATED
Good morning all
RSA: AUTHENTICATED
hello
```

Sensor Node 11

```
RSA: AUTHENTICATED
Important message
RSA: AUTHENTICATED
Good morning all
RSA: AUTHENTICATED
hello
```

Sensor Node 12

```
RSA: AUTHENTICATED
Important message
RSA: AUTHENTICATED
Good morning all
RSA: NOT AUTHENTICATED
hello
```

Figure 3:Sample simulation

Once the user completes the simulation, he/she can access the outputs in the form a graph which clearly depicts the findings.

III. SIGNATURE AMORTIZATION

The enhanced scheme using signature amortization for WSNs is proposed to meet
the following properties.

- Low overhead. The computation and communication overhead is to the same degree of the Keyed-Hash Message Authentication Code (HMAC).
- Strong authenticity. Confidence of a receiver in authenticating multicast messages is as strong as each extended block in EB is authenticated by an ECDSA signature.
- Immediate authentication. A receiver can authenticate multicast messages upon receiving them.
- No time synchronization. Time synchronization is not required.
- Resilience to node compromise attacks. It is impossible for an adversary to exploit a compromised receiver to launch a valid multicast authentication.

The enhanced scheme using signature amortization exploits one ECDSA signature to
authenticate all multicast messages. The only one signature is used to authenticate the authenticator in EB0. This authenticator is used to authenticate EB1 that contains b multicast messages in M and one authenticator. The authenticator in EB1, in its turn, is used to authenticate EB2 that contains b multicast messages in M and one authenticator.

The process continues until EBk. As a result, all broadcast messages can be authenticated with only one signature while the overhead of the signature is amortized over them

The signature amortization[5] part is presented by three steps: generating extended blocks step, multicasting extended blocks step and verifying extended blocks step.

1) Generating Extended Blocks Step: The basis to construct extended blocks is provided by following theorem.

Theorem. All multicast messages in M will be authenticated if EB0 is authentic and all ordered pairs <EBi−1,EBi >, 1 ≤ i ≤ k, belong to authenticated relation AR on EB.

Authenticators for extended blocks can be generated by three classes of functions roughly: message encryption, MAC and hash function. Symmetric encryption, MAC and hash
function are efficient to WSNs. Symmetric encryption and MAC require two input parameters: a secret key and a message.

The shared secret key between the sender and receivers is vulnerable to node compromise attacks. Therefore, we adopt a collision resistant hash to produce authenticators for extended
blocks.

The extended blocks are generated as follows.

All n multicast messages in M is partitioned into k blocks B1, . . . , Bk. Every block Bi, 1 ≤ i ≤ k, contains b messages,

denoted by |Bi| = b. These blocks comprise a vector B = [Bi]T
i=1,...,k that is expressed in the matrix form

$$B = \begin{bmatrix} B_1 \\ \vdots \\ B_k \end{bmatrix} = \begin{bmatrix} m_1 & \dots & m_b \\ \vdots & \vdots & \vdots \\ m_{(k-1)b+1}, & \dots & m_{kb} \end{bmatrix}$$

Figure 4: Matrix representation of blocks

The algorithm is as follows:

Algorithm 1 Generation of EB

```
Partition $n$ broadcast messages in $M$ into $k$ blocks $B_1, \dots, B_k$ as shown in equation (1)
Initialize $d_{k+1}$ with a string of random characters
for $i = k; i \geq 1; i = i - 1$ do
    Concatenate messages in $B_i$ to generate $CON(B_i)$ as shown in equation (2)
    Pad $CON(B_i)$ with digest $d_{i+1}$ to generate $PAD(CON(B_i))$ as shown in equation (3)
    Compute digest $d_i$ of $PAD(CON(B_i))$ with a collision resistant hash as shown in equation (4)
    Let $EB_i = [B_i \; d_{i+1}]$
end for
Sign digest $d_1$ with sender $s$'s private key $PR_s$ to generate $EB_0 = d_1 || E(PR_s, d_1)$
Let $EB = [EB_i]^T_{i=0,\dots,k}$
```

Figure 5: Algorithm for extended block

Based on theorem 1 and generating process of EB, authenticating n broadcast messages in M proceeds as follows. The signature in EB0 is used to authenticate d1. d1, in its turn, is used to authenticate EB1 that contains B1 and d2. Then, d2 is used to authenticate EB2 that contains B2 and d3. This process continues until EBk. Eventually, n broadcast messages in M will be authenticated. An example of generating EB for 9 multicast messages, in which every 3 broadcast messages constitute a block is given below

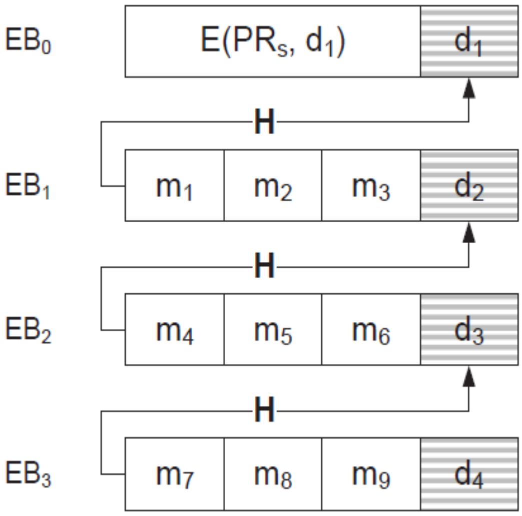


Figure 6: Extended block example

2) Multicasting Extended Blocks Step: In generating extended blocks step, all ordered pairs < *EBi*−1,*EBi* >, 1 ≤ *i* ≤ *k*, belong to *AR* on *EB*. That is *EBi*'s authentication depends on *EBi*−1. Thus, *EBi*−1 should reach receivers before *EBi*. This is fulfilled by the sequential multicast and reliable multicast described as follows.

The sequential broadcast is that extended blocks are multicast according to *AR* on *EB*. Sender *s* broadcasts *EBi*−1 before *EBi*. For simplicity, messages in each extended block are multicast according to their indexes, i.e., sending sequence for *EBi* is *m* (*i*−1)*b*+1,*m*(*i*−1)*b*+2,..,*mib*. Digest *di*+1 in *EBi* could be sent together with a multicast message in *EBi* since the size of a digest is relatively small. On receiving a multicast message *mj* , a receiver in *Rs* checks whether *mj* belongs to current extended block, say, *EBi*, whose digest, *di*, has been received and authenticated with *EBi*−1.

The reliable multicast is performed by acknowledgements and replies. To reduce communication overhead, we let one acknowledgement specify all missing messages of one extended block but the size of an acknowledgement be several bits larger than that to one missing message. The acknowledgement contains two fields. The first field specifies the identity of an extended block. The second field is a bit-vector indicating all missing messages in one extended block. The bit-vector is a mapping to all messages in one extended block. Thus, the size of the bit-vector equals the number of messages in the extended block.

3) Verifying Extended Blocks Step: According to multicasting extended blocks step, *EB*0 reaches receivers in *R* first. *d*1 in *EB*0 is authenticated by the signature, that is, if *D*(*PUs*,*E*(*PRs*, *d*1)) = *d*1, *d*1 is authentic. Extended blocks in *EB*∗ are authenticated in an efficient way, just using a collision resistant hash. Digest *di*, 1 ≤ *i* ≤ *k*, in *EBi*−1 that reaches receivers in *R* in advance is used to authenticate *EBi*, that is, if *H*(*m*(*i*−1)*b*+1
|| . . . ||*mib*||*di*+1) = *di*, *EBi* is authentic.

IV. COMPARISON RESULTS

After the simulation process, it is deduced that the time taken for signing using RSA is the highest among the three. As expected enhanced version of ECDSA had more efficient results proving our assumptions. The results were presented for both signing and verifying a message and two different colors were used to show the difference between these two functionalities. Blue stands for signing ta message for authentication and green is used for representing the verify function for all three techniques under consideration. The comparison results received are as follows

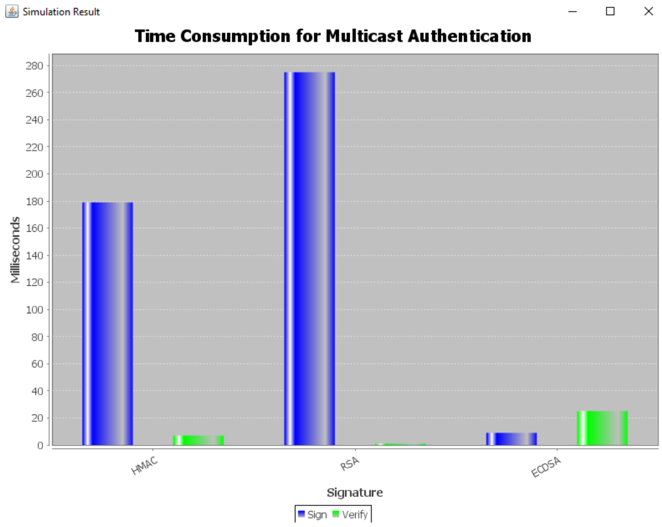


Figure 7: Comparison results

V. ENHANCED ECDSA IN CLOUD COMPUTING

Cloud computing security is the set of control-based technologies and policies designed to comply to the rules and regulations framed by the provider team to support and protect information, data applications and infrastructure associated with cloud computing use. Cloud computing security process should address the issues faced by the cloud users. Cloud Service Provider needs to incorporate the maintenance activity in order to provide the customer's data security, privacy and compliance with necessary regulations [6].

Security Issues in Cloud Storage:

Privacy issue -Cloud service providers request customers to store their account information in the cloud, where cloud service providers have the access to this information.

Multiple copies of user information- When a customer decide to use multiple cloud service, the customer will have to store his/her password in multiple cloud, the more cloud service the customer is subscript to, the more copy of the user's information will be.

Multiple authentication requirements- The multiple copies of account will lead to multiple authentication processes. For every cloud service, the customer needs to exchange his/her authentication information. These redundant actions may lead to an exploit of the authentication mechanism.

In order to address these issues of cloud computing, we propose a new variant ECDSA scheme which utilizes signature amortization that will produces the high level security with the help of parameters.

VI. CONCLUSION

In this paper, we first implemented ECDSA using signature amortization. This scheme employs only one ECDSA signature to authenticate all multicast messages. The overhead of the signature is amortized over all multicast messages. It also does not require time synchronization and achieves immediate authentication. Then we made a comparative study of different authentication techniques like RSA HMAC and ECDSA on a wireless sensor network environment. Comparison results show that the overhead of the new ECDSA scheme is to the same degree of HMAC. The results were in par with our assumptions and proved that this enhanced ECDSA scheme is more efficient than conventional schemes. We also proposed to use this enhanced ECDSA for cloud computing as there are a lot of safety concerns in play.

REFERENCES

[1] I.Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, 2002.

[2] Rachid Ennaji and Mohammed Boulmalf "Routing in wireless sensor networks"Multimedia Computing and Systems, 2009. ICMCS '09. International Conference on : 2009 , 495 - 500

[3] Jung Min Park , Edwin K P Chong and Howard Jay Siegel "Efficient Multicast Packet Authentication using Signature Amortization" Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on : 2002 , 227 – 240

[4] Shwetha Lamba and Monika Sharma "An Efficient Elliptic curve digital signature Algorithm" Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference :2013, 179 – 183

[5] Yongsheng Liu, Jie Li and Mohsen Guizani "PKC based Broadcast authentication using signature amortization for WSNs" IEEE Transactions on Wireless Communications Year: 2012, Volume: 11, Issue: 6 Pages: 2106 - 2115

[6] S Sathish, D Sumathi and P Shivaprakash "Security Services using ECDSA in cloud computing