# Batch Authentication Scheme to Identify the Invalid Signature in Mobile Computing

K.Saradha
Department of Computer Science and Engineering
Dhanalakshmi College of Engineering, Chennai,India
saradha1912@gmail.com

M.Sujithra
Department of Computer Science and Engineering
Dhanalakshmi College of Engineering, Chennai,India
sujithramanohar19@gmail.com

M.Saraswathi
Department of Computer Science and Engineering
Dhanalakshmi College of Engineering, Chennai,India
saras786@gmail.com

***Abstract*—Mobile Computing is an infrastructure wireless net-work that requires the use of an infrastructure device, such as an access point or a base station. It is a communication technology that allows transmission of data via any other wireless enabled device without having to be linked to wired Network. It describes ones ability to use the technology while moving. A Cellular Network is a Communication network where the last link is wireless communication. The network which is distributed over land network areas called cells, each message served by at least one fixed-location transceiver, known as a cell site or base station. A network contains of both normal nodes and some of the attackers. Attackers strategy can be changed at any time from low to high or vice-versa. They corrupt some of the messages (packets) in a transaction. It may be low or high level attack based on the attacker.There are some previous studies which only focuses on Batch identification game model for invalid signatures in Wireless Mobile Networks using digital Signature and In the existing work focus on finding whether the packet is hacked or not. Therefore project deals with Batch Identification Game Model with Complete information (C-BIGM) and Batch Identification Game Model with Incomplete Informa-tion (IBIGM) to defend the normal nodes from the hacker of unacceptable signature. To estimate the efficiency of Batch Identification Game model follows the four aspects:To analysis the time complexity for each Batch Identification algorithm.**

**Keywords—**Mobile Computing; invalid signature; Batch authentication

## I. INTRODUCTION

Using Mobile Computing we help to verifier nodes to verify the Signature in the time efficient and in the light weighted manner of malicious nodes if needed. This project uses Batch Cryptography Technique is a powerful tool to reduce the verification time. Batch Verification and Batch Identification techniques used to detect the attacker in the message transaction path.

The Batch Verification is a technique which only looks after both the messages and signature are considered as a pair which is n(message, signature). Batch verification method which verifies the signature of both the sender and receiver and returns true only if all the n are valid. otherwise, it returns false even there is one invalid signature. As a result, compared with the traditional way, the validity of a batch can be checked more efficiently, and the verifica-tion delay can be remarkably reduced. So we opt for the Batch Identification Technique. The Batch Identification is a Technique which uses divide and conquers method. Which is implemented to gain high performance when the batch verification fails. To find the invalid signature pairs in the packets (messages) we use two techniques. They are CBI and MRI.

- The project hold up the absolute and imperfect information of Batch Identification Game model scenarios at same time.
- The model proposed self adaptive auto match protocol to develop the prediction exactness of node states.
- Simulations to analyze the reason ability of NE, Choose the accuracy of algorithm used.

That project analyzes the performance flow of the three generic Batch Identification algorithms as the defense strate-gies. To reduce the delay and ensure a network of Quality of Service, under the heterogeneous and dynamic attack scenario in Wireless Mobile Networks.

## II. PROPOSED SYSTEM

In our proposed system going to implement the HMAC algorithm for creating a signature for individual signature and RSA algorithm for encrypting and decrypt the orig-inal message from a sender to receiver. We also imple-ment the Batch Cryptography techniques. There will be two directions to apply the batch cryptography concept in Mobile Computing (Wireless Networks): Batch Verification and Batch Identification. It is surrealistic to completely prevent all attackers from generating a false message with invalid signatures. Thus, to a guarantee the performance of

batch verification, We should identify an invalid signature in a batch rapidly. Batch identification is a technique to find the bad signatures within a batch verification fails. Due to the inefficiency of individual identification, divide techniques have been proposed to improve the performance of Batch identification ion. Batch identification consists of two algorithmic programs namely

- Condensed Binary Identification (CBI)
- Multiple Rounds Identification (MRI)

### *A. Condensed Binary Identification(CBI)*

In CBI, Divide the n messages into two group of an equal number of packets. Then, those two groups are verified using Batch Verification individually. If the Batch Verification succeeds, there is no invalid signature in that group. Otherwise, messages in that group will be further divided into two subgroups, and each subgroup is verified individually. The process repeats until all of the messages pass the Batch Verification. CBI improves the efficiency for Batch Verification.

Algorithm 1: Condensed Binary Identification Algorithm

```
1 for true do

2 if n   2d   2 then
3 Verify n messages using it;
4 return;
5 else
6 z = n   d + 1;
7   = b log (z/d) c
8 end
9 Verify the prevenient 2 messages with batch verification;
10 if verification succeeds then
11 n = n   2 ;
12 continue;
13 else

14 identify an invalid signature by basic binary identification after verifying v messages;
15 n = n   1    v;
16 d = d   1;
17 continue;
18 end
19 end
```

Where

- n-> The number of signatures which is needed to be verified in each round.
- d->The upper bound number of invalid signature length nature in a batch.

### *B. Multiple Rounds Identification (MRI)*

In MRI, We identify the invalid signatures in an iterative way which has m (2 m n) rounds. In the first rounds, then pending messages are divided into 1 groups, and each group has 1 messages except the last group. Then,each group is verified respectively. The groups identified with invalid signatures are aggregated as a new pending message batch. In the second round, that new message batch is divided into 2 groups of 2 messages. In general, in round i, 2 < i < m, messages from the contaminated groups of round i-1 are pooled, and arbitrarily divided into i groups of i size except the last group whose size may be smaller than i. A batch verification test is performed on each group. Note that m is set to be 1. Thus every invalid signature ids identified at round m.

Algorithm 2: Multiple Rounds Identification Algorithm

1 Copy n sample messages to test batch;

2 for i m do
3 i = d (n/d)m-i/m e ;

4 i = b n/i c + 1;

5 Divide test batch into i groups of i messages (may be less than i in the last group);
6 for j = 0 to j < i do
7 if Batch verification on group j succeeds then
8 Remove the contents of group j from test batch; 9 end
10 j + +;
11 end
12 i = i + 1;
13 end
14 return test batch;

*C. Encryption and Decryption of Message*

The original message from the sender is encrypted and decrypted using Rivest-Shamir- Adleman algorithm.

1.The text encrypted by following formula: Message M, The sender knows the receiver public key (n,e). So the sender encrypted by the message the using RSA algorithm with receiver public key(n,e)

$C= M^e \bmod n$

2. The text decrypted by following formula : The re-ceiver knows the private key(d,n) and public key (n,e). So the receiver decrypted the message using RSA algorithm with the receiver private key(d,n)

$M=C^d \bmod n$

Algorithm 3: To encrypt and decrypt the message using RSA algorithm

Creating keys

1. Generate (find) two large prime numbers (P and Q)
2. Calculate N = P Q
3. Calculate M = (N) = (P - 1)(Q - 1); ! (Euler totient function)

4. Select any integer E, the rules to select E are:
   a. E is positive integer
   b. 0 < E < M
c. GCD (M, E) = 1 NOTE: It is recommended to use E = 65537 (17bits)
. GCD = Greater Common Divisor
5. Calculate D a use Extended Euclid Theorem (mod inverse) (E * D) = 1 (mod M)

(E * D) mod M = 1 For Encryption:

$C=M^e \bmod N$ For Decryption:
$M=C^d \bmod N$

*D. . Signature Creation*

This project had created a signature for packets using HMAC( Hash - based Message Authentication Code) Algo-rithm. The signature is one important for message transmis-sion. This signature of packets used in Batch Verification. In this method verify the signature of packets of both re-ceiver(sink) and sender. The HMAC algorithm is one of the techniques for creating the signature for message packets. The hash function coupled with a secret key. Reason for using HMAC algorithm follows

- Cryptography hash functions generally execute faster in software than DES which is symmetric block cipher.
- Cryptography hash functions have library code which is widely available.
- There are no export restrictions for cryptography hash functions, whereas symmetric block ciphers, even when used for MACs, are restricted

---

Algorithm 4: To create signature for message packets using HMAC Algorithm

---

1. Attach zeros to the left end of K to create a bbit string K+
2. XOR K+ with ipad to produce the b-bit block Si. 3. Attach M to Si.
4. Apply H to the stream generated in step 3.
5. XOR K+ with opad to produce the b-bit block So
6. Attach the hash result from Step 4 to So.
7. Apply H to the stream generated in Step 6 and output the result. Note: XOR-Bitwiswe exclusive OR

---

## III. Modules Description

A. . *Network formation and source action*

Initially, nodes should be created. Each and every node should maintain two histories. One is for neighbor nodes and another one is for attackers. After Complete Transaction, Attacker history will be updated. Source node will encrypt the entire message using RSA(Rivest Shamir Adelman) al-gorithm and split into packets randomly. Signature is created for each packet. Each packet is appended with source name, packet order.The source will send the particular amount of packets to intermediate nodes based on the number of intermediate nodes. Each packet contains the length of the encrypted message is ten.

*B. Intermediates activity*

Intermediate consists of both normal as well as attackers. If it is the normal node, just it will append its name and forward the packets to the receiver to indicate them as the intermediate node. In the attackers case, if it is the lower attacker, it will corrupt the packets in minimum probability ratio and if it is the high attacker, it will corrupt the packets in the probability ratio and forward to the destination.

*C. Receiver performance based without history of the transaction*

The destination (Sink) will receive the packets and signature will be created for each encrypted packet. After receiving every packet, Batch Verification will be performed for the whole Batch.If Batch verification returns true, then sink will make the decision that Batch is not affected by malicious nodes. So, the sink will decrypt the data and read. If Batch Verification fails, then it will check the history for Attackers. If the history is empty, the sink will choose CBI algorithm in default.

*D. Receiver performance based in mixture of at-tackers history of transaction*

After Batch verification fails, check if attackers strategy is only low in history, then it will choose CBI algorithm or if attackers strategy is only high, then MRI will be selected. If the database consists of both type of attackers, then based on the self-adaptive auto match protocol formula, an algorithm is chosen automatically, After every transaction, receiver updates history for attackers. If attacker attacks continuously three times, then receiver intimate to normal users about the attackers.

*E. Data flow diagram*

The Message transmit from Sender to the Receiver through intermediates. The Sender transmit the message to intermediate nodes with receiver information then the intermediate nodes transmit to the Receiver.

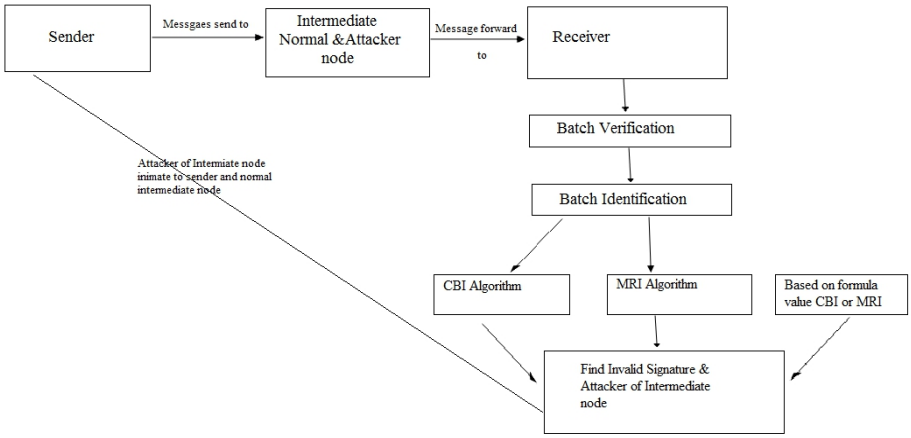


Figure 1. Flow of message transmission

*F. Self-Adaptive Auto Match Protocol*

The self-adaptive auto-match protocol algorithm for which algorithm selected for mixed strategy in attackers history.Self adaptive Auto Match Protocol Algorithm using formula to select the CBI Algorithm or MRI Algorithm. Then produce the futher execution of Batch verification Method in message packets received by the Reciver. This algorithm contain two pharse. These are Initialization pharse and Dicision pharse. The self adaptive auto match protocol mechanism is performed by the follow flowchart.

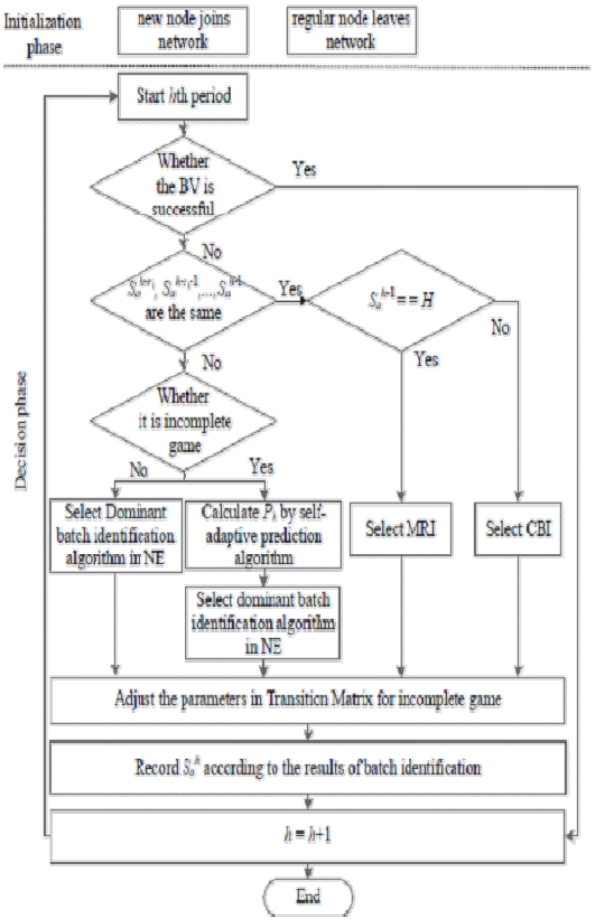


Figure 2. Self Adaptive Auto Match Protocol Process

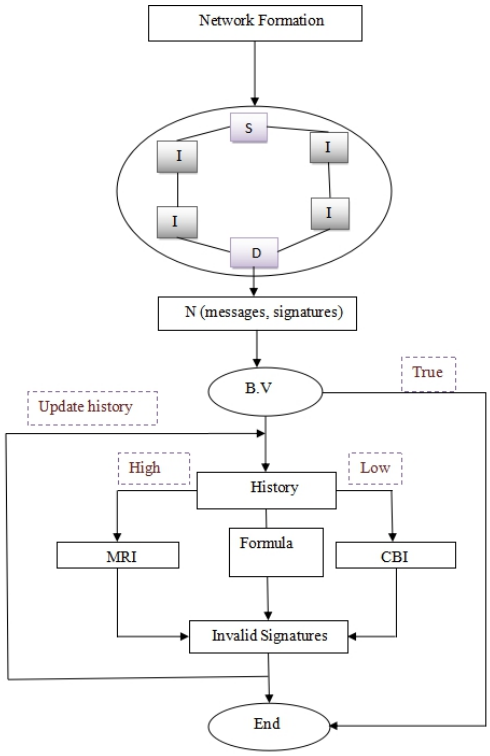


Figure 3. Architecture Diagram

Algorithm 5: Self-adaptive auto match prediction algorithm

```
1 while true do

2 if (Batch verification succeeds) then
3 h = h + 1;
4 continue;
5 else
6 if (Shr1a ,Shr1+1a ,...,Sh1a ) are the same then
7 if (Sh1a == H) then
8 Select MRI algorithm;
9 else
10 Select CBI algorithm;
11 end
12 else
13 if Game with incomplete information then
14 Calculate Ph by self-adaptive prediction algorithm;

15 Select the dominant batch identification algorithm with I-BIGM

16 else
17 Select the dominant batch identification algorithm with C-BIGM;

18 end
19 end
20 end
21 Adjust the parameters in Transition Matrix;
```

22 Record Sha according to the results of batch identification;

23 h = h + 1;
24 if (Process should be ended) then
25 Break;
26 end
27 end

## IV. RESULT

To intimate the secure path for message transaction between Sender and receiver. To improve the time efficiency and Quality of Service in the message transaction in Mobile Computing.

## CONCLUSION

The Batch verification has been performed to identify the presence of false a signature in a Batch and if found, each regular node identified invalid signatures of false mes-sages correctly by choosing appropriate batch Identification algorithm.

## REFERENCES

[1] L. Xiao, Y. Chen, W. S. Lin, and K. J. R. Liu, Indirect Reciprocity Se-curity Game for Large-Scale Wireless Networks, in IEEE Transactions on Information Forensics and Security, 2012.
[2] Y. Liu, D. Bild, R. Dick, Z. Mao, and D. Wallach, The Mason Test: A Defense Against Sybil Attacks in Wireless Networks Without Trusted Authorities, in IEEE Transactions on Mobile Computing, 2015.
[3] B. Alomair and R. Poovendran, Efficient Authentication for Mobile and Pervasive Computing, in IEEE Transactions on Mobile Computing, 2014.
[4] L. Y. Yeh, Y. L. Huang, A. Joseph, S. Shieh, and W. Tsaur, A Batch-Authenticated and Key Agreement Framework for P2PBased Online
[5] A. Fiat, Batch RSA, in Proceedings of CRYPTO, 1989.
[6] Naccache, MRaihi, Vaudenay, and Raphaeli, Can DSA be Improved? Complexity Trade-offs with the Digital Signature Standard, in Pro-ceedings of EUROCRYPT, 1994.
[7] J. Cheon, J. Coron, J. Kim, and M. Lee, Batch Fully Homomorphic Encryption over the Integers, in Proceedings of EUROCRYPT, 2013.
[8] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, An Efficient Signature-Based Scheme for Securing Network Coding Against Pollution At-tacks, in Proceedings of IEEE INFOCOM, 2008.
[9] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. S. Shen, An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Net-works, in Proceedings of IEEE INFOCOM, 2008.
[10] S. Horng, S. Tzeng, Y. Pan, and P. Fan, b-SPECS+: Batch Verifi-cation for Secure Pseudonymous Authentication in VANET, in IEEE Transactions on Information Forensics and Security, 2013.