Cluster Labelling Game Model For Inavlid Signature using Wireless Mobile Networks

[1]Vinoth kumar V
vijayvinoth97@gmail.com
Assistant Professor

[2]Charumadhi J
charumathi.dj@gmail.com

[3]Gomathi R
gomathiravi144@gmail.com

[4]Haripriya k
haripriya6077@gmail.com

[2][3][4]UG students
Department of Computer Science and Engineering
T.J.S. Engineering College

Abstract

Mobile computing is an infrastructure wireless network That requires the use of an infrastructure device such as an access point or a base station. It is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. It describes one's ability to use the technology while moving. A cellular Network or a Wireless Mobile Network is a communication network where the last link is wireless. The network is distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. A network consists of both normal nodes and some of the attackers. Attacker's 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 based on the attacker

Index Terms –

1. Introduction

In past few years Wireless Mobile Networks (WMNs) have been dramatically developed due to the proliferation of inexpensive, widely available wireless mobile devices. People's life has been inseperable from mobile devices which can access the internet at anytime and anywhere. [1]However, due to the openness characteristic of wireless channels, it becomes easier for malicious nodes to interfere the access process by tempering or forgive request messages.

To protect the security of access, one effective manner. The signature verification induces extra delay and computational cost. [2]The way that verifying message signature individually could induce tremendous delay and severely affect the Quality Of Service. The batch cryptographic technique which is used to reduce the verification delay. Batch cryptography was introduced by Fiat in 1990 to RSA –type signature. [3]It focus on two directions to apply the batch cryptography concept in WMNs: *batch verification* and *batch identification*.

Batch verification deals with n (message, signature) pairs as a batch at a time. [4]As a result, compared with the traditional way, the validity of a batch can be checked more efficiently, and the verification delay can be remarkably reduced. [5]Batch verification methods return true if all of the n signatures are valid, and false when there is any invalid one.

[6] *Batch identification* is a technique to find the bad signatures within a batch when the batch verification fails.Due to the inefficiency of individual identification, divide-and-conquer techniques have been proposed to improve the performance of batch identification.[7] Batch identification consists of two algorithms namely Condensed Binary Identification (CBI) and Multiple Rounds Identification (MRI).

2. Preliminaries

2.1 Problem Statement

Generally, signature verification induces extra delay and computational cost. The traditional way that verifying messages signature **individually** could induce tremendous delay.

[8]It will affect severely the Quality of Service (QOS), especially when network traffic is heavy and a large number of signatures need to be verified.

3. Literature Review

[1]With today's technology, many applications rely on the existence of small devices that can exchange information and form communication networks. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. In this work, we

propose two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications [2]security and privacy issues on OSNs are major concerns, we propose a security framework for simultaneously authenticating multiple users to improve the efficiency and security of peer-to-peer (P2P)-based OSNs. In the proposed framework, three batch authentication protocols are proposed, adopting the one-way hash function, ElGamal proxy encryption, and certificates as the underlying cryptosystems. The hash-based authentication protocol requires lower computational cost and is suitable for resource-limited devices.[3] The proxy-based protocol is based on asymmetric encryption and can be used to exchange more information among users. Our system is robust against collusion attacks, and can signicantly reduce the attacking rate for a wide range of attacks.

4. Existing System

In general, secure access is one of the fundamental problems in wireless mobile networks. In the existing system, Digital signature is a widely used technique to protect messages' authenticity and nodes' identities. From the practical perspective, to ensure the quality of services in wireless mobile networks, ideally the process of signature verification should introduce minimum delay. However, most of the existing works focus on designing batch verification algorithms for wireless mobile networks without sufficiently considering the impact of invalid signatures, which can lead to verification failures and performance degradation.

5. Proposed System

Batch cryptography technique is a powerful tool to reduce verification time. There will be two directions to apply the batch cryptography concept in WMNs: Batch verification and Batch identification. It is unrealistic to completely prevent all adversaries (attackers) from generating false messages with invalid signatures. Thus, to guarantee the performance of batch verification, we should identify invalid signatures in a batch rapidly. Batch identification is a technique to find the bad signatures within a batch when the batch verification fails. Due to the inefficiency of individual identification, divide and conquer techniques have been proposed to improve the performance of batch identification. Batch identification consists of two algorithms namely Condensed Binary Identification (CBI) and Multiple Rounds Identification (MRI).

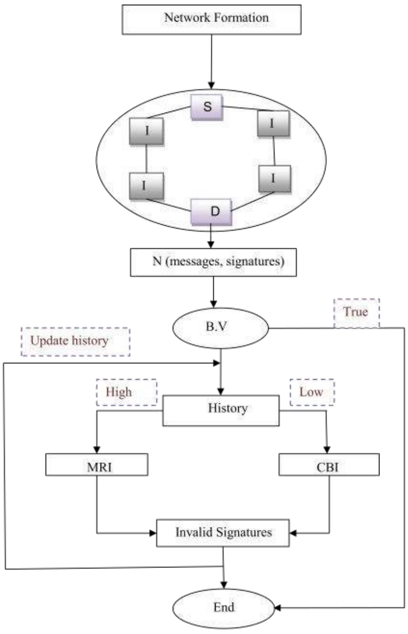

Fig 5: System Architecture

5.1. Batch Verification

Batch verification deals with *n* (message, signature) pairs a batch at a time. Batch verification methods return true if all of the *n* signatures are valid and false when there is any invalid one. As a result, compared with the traditional way, the validity of a batch can be checked more efficiently, and the verification delay can be remarkably reduced.

5.2.Batch Identification

5.2.1.CBI

In Condensed Binary Identification, it first divides the *n* messages into two groups of equal size. 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 sub-group is verified individually. That process repeats until all of the messages pass the batch verification. CBI improves the efficiency for batch verification.

Algorithm 1: Condensed Binary Identification

```
while $true$ do
    if $n \leq 2d - 2$ then
        Verify $n$ messages using II;
        return;
    else
```

```
        $z = n - d + 1$;
        $\theta = \lfloor \log (z/d) \rfloor$;
    end
    Verify the prevenient $2\theta$ messages with batch verification;
    if verification succeeds then
        $n = n - 2\theta$;
        continue;
    else
        identify an invalid signature by basic binary identification after verifying $v$ messages;
        $n = n - 1 - v$;
        $d = d - 1$;
        continue;
    end
end
```

5.2.2.MRI:

In Multiple Rounds Identification (MRI) algorithm, we identify the invalid signatures in an iterative way which has m $(2 \leq m \leq n)$ rounds. In the first round, the n pending messages are divided into $\delta 1$ groups, and each group has $\gamma 1$ 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 $\delta 2$ batch is divided into groups of $\gamma 2$ messages. In general, in round i, 2<i<m , messages from the contaminated groups of round i-1 are pooled, and arbitrarily δi divided into groups of γi size except the last group whose size may be smaller than γi . A batch verification test is performed on each group. Note that is set to be 1. Thus every invalid signature is identified at round m.

Algorithm 2: Multiple Rounds Identification

```
Copy $n$ sample messages to test batch;
while $i \leq m$ do
    $\gamma i = \lceil (n/d)m□im \rceil$;
    $\delta i = \lfloor n/\gamma i \rfloor + 1$;
    Divide test batch into $\delta i$ groups of $\gamma i$ messages (may be less than $\gamma i$ in the last group);
    for $j = 0$ to $j < \delta i$ do
        if Batch verification on group j succeeds then
            Remove the contents of group $j$ from test batch;
        end
        $j++$;
    end
    $i = i + 1$;
end
return test_ batch;
```

5.3: 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 will be updated. Source node will encrypt the entire message and split into packets randomly. Signature is created for each packet. Each packet is appended with source name, packet order. Source will send the particular amount of packets to intermediate nodes based on the number of intermediate nodes.

5.3.1. Intermediates activity

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

.

5.3.2. Receiver performance based on without history of transaction

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 decision that batch is not affected by malicious nodes. So, sink will decrypt the data and read. If batch verification fails, then it will check the history for attackers. If the history is empty, sink will choose CBI algorithm in default.

5.3.3. Receiver performance based on mixture of attacker's history of transaction

After batch verification fails, check if attacker's strategy is only low in history, then it will choose CBI or if attacker's strategy is only high, then MRI will choose. If the database consists of both type of attackers, then based on the self adaptive auto-match protocol formula, algorithm is chosen automatically. After every transaction, receiver updates history for attackers. If attacker attacks continuously 3 times, then receiver intimate to normal users about the attackers.

5.4. BATCH IDENTIFICATION GAME MODEL

We consider the problem between a verifier and its attackers as a dynamic game, where attackers select the attack strategy first, and the verifier picks the batch identification algorithm accordingly. The definition of BIGM is represented by a triple (*PL, S,U*), where *PL* is the player set, *S* denotes the strategy set of players, and *U* stands for the payoff function set. The detailed description is as follows.

5.4.1 Players

The player set is represented by *PL = {PLi}l*
i=1, where *i* is
the index number of a player, and *l* is the total number of players. Obviously, the set *PL* includes two players (*l* = 2).One is the verifier, and the other is the attackers, which arethe verifier's malicious neighbors.

5.4.2 Strategy set

The strategy set of players is *S = {Sa, Sv}*. Different players in the game may have different strategies. For attackers, theadopted strategies fall into two types, high-frequency attack *H* and low-frequency attack *L*, in terms of the total number of invalid signatures. Hence, the strategy set of attackers is denoted as *Sa = {H,L}*. Note that the attack strategy is determined by the sum of invalid signatures of the verifier' smalicious neighbors, while each malicious neighbor can randomly select its false message number. On the other side, the verifier's strategy set is *Sv = {CBI,MRI, II}*, which includes the three batch identification algorithms.

5.4.3 Payoff function

Each regular node acts as a verifier to protect its QoS. Let *Q* denote the communication benefit in an ideal mobile network environment. For the verifier *V* , the payoff function is *uV = bV − cV* , where *bV* is the communication benefit *Q*, and *cV* indicates the total cost of batch verification and batch identification. The cost of batch verification for *n* messages, denoted as *CnB V* , is determined by the batch verification algorithm. The cost of batch identification algorithm is represented by *α*(*j, k*), which is determined by the identification strategy *j ∈ {CBI,MRI, II}*, and the attack
strategy *k ∈ {H,L}*. To simplify notations, we use 1, 2,3
to index the algorithm CBI, MRI, and II. Note that *α*(*j,k*) is determined by the number of required batch verification tests. With the above discussion, the payoff function of the verifier *V* can be defined as *uV = Q − CnBV− α*(*j, k*). Recall that the intention of attackers is to consume the verifier's resources by broadcasting false messages, and eventually to downgrade the QoS of the wireless mobile network. The payoff function of attackers *A* is *uA = bA−cA*, where *bA* is the loss of QoS, which is affected by the verification cost of the verifier. Therefore *bA = CnBV + α*(*j, k*). *cA* indicates the attack cost, which is determined by thenumber of the broadcasted false messages with invalid signatures, denoted by *σ*(*k*) (*k ∈ {H,L}*). Therefore, the payoff function is *uA = CnBV + α*(*j, k*) *− σ*(*k*).

6. Conclusion

Thus, Batch verification has been performed to identify the presence of false signature in a batch and if found, each regular node identified invalid signatures of false messages correctly by choosing appropriate batch identification algorithm.

9. References

[1] L. Xiao, Y. Chen, W. S. Lin, and K. J. R. Liu, "Indirect Reciprocity Security Game for Large-Scale Wireless Networks," in IEEE Transactionson Information Forensics and Security, 2012

[2] B. Alomair and R. Poovendran, "Efficient Authentication for Mobile and Pervasive Computing," in IEEE Transactions on Mobile Computing, 2014

[3] L. Y. Yeh, Y. L. Huang, A. Joseph, S. Shieh, and W. Tsaur, "A Batch-Authenticated and Key Agreement Framework for P2P Based Online Social Networks," in IEEE Transactions on Vehicular Technology, 2012.

[4] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An Efficient Signature- Based Scheme for Securing Network Coding Against Pollution Attacks," in Proceedings of IEEE INFOCOM, 2008

*[5] Z. Lu, W. Wang, and C. Wang, "How can Botnets Cause Storms? Understanding the Evolution and Impact of Mobile Botnets," in
Proceedings of IEEE INFOCOM, 2014*