ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.3

An Efficient Batch Authentication Scheme to Identify Invalid Signatures in Mobile Computing

Mohamed Yusuf Ali D[1], Seshan K[2], Manikandan[3]
Student[1, 2], Assistant Professor[3]
Department of CSE
Dhaanish Ahmed College of Engineering, Chennai, India

Abstract:
Secure access is one of the fundamental problems in mobile computing. Digital signature is a widely used technique to protect messages authenticity and nodes identities. Batch cryptography technique is a powerful tool to reduce verification time Most of the existing system 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. We propose a Batch Identification Game Model (BIGM) in wireless mobile networks, enabling nodes to find invalid signatures with reasonable delay no matter whether the game scenario is complete information or incomplete information.

Keywords: Batch identification, Batch verification, Game theory, Mobile Computing

I.INTRODUCTION

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 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. In the past few years, Wireless Mobile Networks (WMNs) have been dramatically developed due to the proliferation of inexpensive, widely available wireless mobile de-vices [1]. With the increasing number of mobile applications, such as social media networks, GPS, yelp, etc., people's life has been inseparable from mobile devices which can access the Internet at anytime and anywhere. However, due to the openness characteristic of wireless channels, it becomes easier for malicious nodes to interfere the access process by tampering or forging request messages [2]. To protect the security of access, one effective approach is to sign each outgoing message with a digital signature, and let the destination verify each received signature [3]. Generally, sig-nature verification induces extra delay and computational verified [4]. To reduce verification delay and ensure QoS, researchers proposed the batch cryptographic technique which is a promising new direction in computer and communication security. The concept of batch cryptography was introduced 1994 for DSA-type signatures. Currently, researchers 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 [7]. 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. In detail, batch verification methods return true if all of the n signatures are valid, and false when there is any invalid one. In 2008, considering that the verification of massive messages may induce huge time cost in mobile networks, Yu et al. [8] proposed an efficient identity-based batch verification scheme to reduce the delay in network coding. Zhang et al. [9] discussed a batch signature verification scheme for the communications between mobile nodes and the infrastructure to lower the total verification time. Horng et al. [10] presented a group signature and batch verification method for secure pseudonymous authentication in VANET. Unfortunately, even though those schemes could protect the authenticity of messages, their performance can be severely affected if there are invalid signatures existing in the verified batch. Adversaries can negate the advantages of batch verification by polluting signatures within a batch. It is unrealistic to completely prevent all adversaries from generating false messages with invalid signatures. Thus, to guarantee the performance of batch verification, we should identify invalid signatures in a batch rapidly 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 [7]. 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. In detail, batch verification methods return true if all of the n signatures are valid, and false when there is any invalid one. In 2008, considering that the verification of massive messages may induce huge time cost in mobile networks, Yu et al. [8] proposed an efficient identity-based batch verification scheme to reduce the delay in network coding. Zhang et al. [9] discussed a batch signature verification scheme for the communications between mobile nodes and the infrastructure to lower the total verification time. Horng et al. [10] presented a group signature and batch verification method for secure pseudonymous authentication in VANET. Unfortunately, even though those schemes could protect the authenticity of messages, their performance can be severely affected if there are invalid signatures existing in the verified batch. Adversaries can negate the advantages of batch verification by polluting signatures within a batch. It is unrealistic to completely prevent all adversaries from generating false messages with invalid signatures. Thus, to guarantee the performance of batch verification, we should identify invalid signatures in a batch rapidly.

II.RELATED WORK

Indirect Reciprocity Game Modelling for Secure Wireless Networks In this paper, we investigated how mobile botnets evolve via proximity infection and their impacts. 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. By taking advantage of the fact that the message to be authenticated must also be encrypted, we propose provably secure authentication codes that are more efficient than any message authentication code in the literature. The key idea behind the proposed techniques is to utilize the security that the encryption algorithm can provide to design more efficient authentication mechanisms, as opposed to using standalone authentication primitives[21]. We found that the size of a mobile botnet can either increase quadratic ally over time or be exponentially distributed with finite mean. How Can Botnets Cause Storms. "Understanding the Evolution and Impact of Mobile Botnets". In this paper, Simulation results show that our system has much better security performance than the direct reciprocity mechanism, especially in the large- scale wireless network with terminal mobility. Our system can be applied to many wireless networks including cognitive radio networks to improve their security performance. "An Efficient Signature- based Scheme for Securing Network Coding against Pollution Attacks". In this paper, we assume the source is always benign, and only the forwarders can be compromised by adversaries for launching pollution attacks. In future, we will study how to detect and filter forged messages injected by adversaries via the compromised sources. In addition, we will implement CJL's pairing-based signature scheme on sensor nodes and conduct experimental evaluation. 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.

III.PROBLEM FORMULATION

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

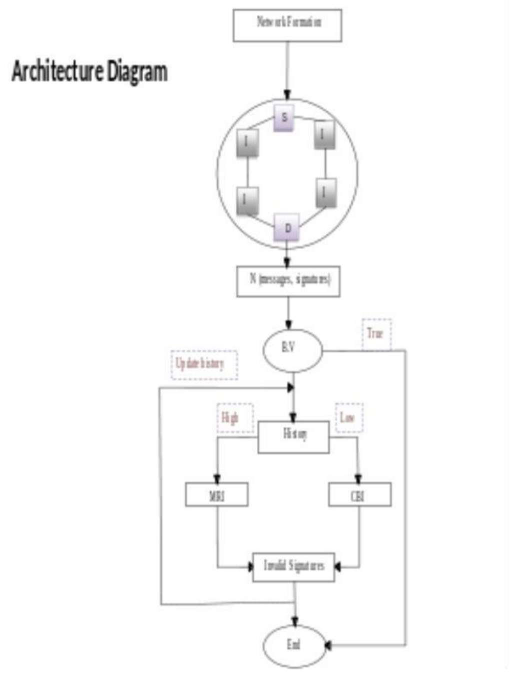
IV.EXISTING SYSTEM

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.

V.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).

VI. ARCHITECTURE



VII. ALGORITHM

Condensed Binary Identification

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.

IMPLEMENTATION

```
while true do
if $n \leq 2d - 2$ then

Verify $n$ messages using II;
return;
$n = \lfloor \log (z/d) \rfloor$;
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
```

Multiple Rounds Identification

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 δ1 groups, and each group has γ1 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 δ2 groups of γ2 messages. In general, in round i, $2 < i < m$, messages from the contaminated groups of round $i - 1$ are pooled, and arbitrarily divided into δi 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 γm is set to be 1. Thus every invalid signature is identified at round m .

IMPLEMENTATION

```
Copy $n$ sample messages to test batch;
while $i \leq m$ do
++ 1;
Divide test ~~b~~atch 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;
```

VIII. CONCLUSION

For selecting suitable batch identification algorithm with high efficiency, we propose a Batch Identification Game Model, named BIGM, which consists of three components. First, we analyze the performance of three generic batch identification algorithms as the defence strategies of our game model, and discuss their advantages under different attack strategies. Then, we give the definition of BIGM, and prove the Nash Equilibriums in the games with complete information and incomplete information. Finally, we design a self-adaptive auto- match protocol to improve the practicability of our game model, considering the transition possibility of attack strategy and nodes' states. From the simulations, we find that our protocol can choose more reasonable batch identification algorithm to reduce delay and ensure network QOS, under the heterogeneous and dynamic attack scenario in WMNs.

IX. REFER ENCES

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

[2]. Y. Liu, D. Bild, R. Dick, Z. Mao, and D. Wal ach, "The Mason Test: A Defense against Sybil Attacks in Wireless Networks without Trusted Authorities," in IEEE Transactions on Mobile Computing, 2015.

[3]. B. A lomair and R. Poovendran, "Efficient Authen ication for Mo-bile 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 P2P- Based Online Social Networks," in IEEE Transactions on Vehicular Technology, 2012.

[5]. A. Fiat, "Batch RSA," in Proceedings of CRYPTO, 1989.
[6]. Naccache, M'Raihi, Vaudenay, and Raphaeli, "Can DSA be Im-proved? Complexity Trade-offs with the Digital Signature Stan-dard," in Proceedings 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 Attacks," 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 Networks," in Proceedings of IEEE INFOCOM, 2008.

[10]. S. Horng, S. Tzeng, Y. Pan, and P. Fan, "b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET," in

[11]. IEEE Transactions on Information Forensics and Security, 2013.

[12]. J. Pastuszak, D. Michalek, J. Pieprzyk, and J. Seberry, “Identifica-tion of Bad Signatures in Batches,” in PKC 2000, LNCS 1751, 2000.

[13]. S. Lee, S. Cho, J. Choi, and Y. Cho, “Efficient Identication of Bad Signatures in RSA-Type Batch Signature,” in IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2006.

[14]. L. Law and B. Matt, “Finding Invalid Signatures in Pairing- based Bathes,” in Cryptography and Coding, 2007.

[15]. M. Stanek, “Attacking LCCC Batch Verification of RSA Signa-tures,” in International Journal of Network Security, 2008.

[16]. B. J. Matt, “Identification of Multiple Invalid Signatures in Pairing-Based Batched Signatures,” in PKC 2009, 2009.

[17]. G. M. Zaverucha and D. R. Stinson, “Group Testing and Batch Verification,” in Proceedings of IEEE ICITS, 2009.

[18]. C. Zhang, P. Ho, and J. Tapolcai, “On Batch Verification with Group Testing for Vehicular Communications,” in Wireless Net-works, 2011.

[19]. C. Lee and Y. Lai, “Toward a Secure Batch Verification with Group Testing for VANET,” in Wireless Networks, 2013.

[20]. J. A. Akinyele, M. Green,S. Hohenberger, and M. W. Pagano, “Machine-Generated Algorithms, Proofsand Software

[21]. Basel Alomair, Member, IEEE, “Efficient Authentication for Mobile and Pervasive Computing”.