iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: II Month of publication: February 2018

DOI: http://doi.org/10.22214/ijraset.2018.2039

Batch Identification based Scheme for Invalid Signatures of game Theory Model in Wireless Mobile Networks

S. Jelin [1], Mr. S. Arun kumar[2],
[1]M.Tech, [2] *Department of computer science SRM university,*

Abstract: In wireless mobile networks the Digital signature has been widely used to ensure the authenticity of messages and identity of nodes. A paramount concern in signature verification is reducing the verification delay to ensure the network QoS. To address this issue, researchers have proposed the batch validation technology. However, most of the existing works focus on designing batch verification algorithms without sufficiently considering the impact of invalid signatures. The performance of batch verification could dramatically drop, if there are verification failures caused by invalid signatures. In this paper, we propose a batch validation for wireless mobile networks, enabling nodes to find invalid signatures with the optimal delay under heterogeneous and dynamic attack scenarios. Specifically, we design an incomplete information of game model of history between a verifier and its attackers, and prove the existence of Nash Equilibrium, toselect the dominant algorithm for identifying invalid signatures. Moreover, we propose an auto-match protocol to optimize the identification algorithm selection, when the attack strategies can be estimated based on history information. Comprehensive simulation results demonstrate that GBIM can identify invalid signatures more efficiently than existing algorithms.

Index Terms: Batch identification, game theory, wireless mobile networks.

I. INTRODUCTION

Wireless Mobile Networks (WMNs) have brought significant convenience by enabling people to use applications on mobile devices (e.g., social media networks and electronic payment) [1]. However, due to their openness, such networks also provide opportunities to malicious nodes, who may threaten the network security by sending tampered or forged messages [2], [3]. To ensure the authenticity of messages and the identity of senders, one approach is to sign each outgoing message with a digital signature, and let the destinations verify the signature of each received message. Generally, signature verification induces extra delay and computational cost. Individual verification, the traditional way, could severely influence the Quality of Service (QoS) and the network availability, especially when there is intensive network traffic with massive signatures to verify, since it would result in unaffordable processing time and delivery delay. To efficiently identify the invalid signatures in bad batches, instead of verifying each signature individually, divide-and-conquer techniques have been proposed [6]. Those method scan dramatically reduce the identification time at different levels. However, there are two limitations in existing works. One is that many methods are designed only for some particular batch types, such as RSA-type batches [7], and pairing-based batches [8]. Though these works are state-of-the-art, it is challenging to apply them with the various batch verification algorithms. The irrr performance may heavily degrade if the ratio of invalid signatures varies when adversaries change attack frequencies and locations. In 2012,Akinyele et al. first proposed an automated tool for selecting the most

II. RELATED WORK

Batch cryptography highlights a novel direction in computer and communication security. The concept of batch cryptography was introduced by Fiat in 1990 for an RSA-type signature [11], and the first efficient batch verifier was proposed by Naccache et al. in 1994 for DSA-type signatures [12].Currently, researchers focus on two directions to apply the batch cryptography concept in WMNs: batch verification and batch identification. A batch verification algorithm is used to determine whether a set of signatures contain invalid ones. In2008, considering that the verification of massive messages may induces huge time cost in mobile networks, Yu et al. proposed an efficient identity-based batch verification scheme to reduce the delay in network coding [13]. Zhang et al [14]discussed a batch signature verification scheme for the communications between vehicles and infrastructure to lower the total verification time. Horng et al. [15] presented a group signature and batch verification method for secure.

The special methods are designed for certain batch signature types such as RSA-type, DSA-type and pairing-type. Lee et al. [7] proposed a method to identify bad signatures in RSA-type batches. Later, Law and Matt [16] presented the quick binary and exponentiation method, to find invalid signatures in the pairing based signature schemes. Stanek [17] showed that method was flawed, and proposed an improved protocol to resist attacks. Matt [8] discussed a solution in pairing-based signature scheme, which can identify nontrivial numbers of invalid signatures in batches. The generic batch identification methods utilize the group testing technique to find invalid signatures with the minimal number of tests, which can be applied with any signature types. Pastuszak et al. designed a divide-and-conquer verifier [6], which split a batch instance into sub ones,and applied the generic test to each sub-batch recursively, until all bad signatures are identified. Zaverucha et al [18]presented and compared some group testing

III. SYSTEM MODEL

A. Network model

We consider that the network has two layers as shown in Figure 1. The bottom layer consists of mobile nodes accessing the network via bluetooth, wifi, GSM, 3G, etc. Each node has its own public/private keys, which are used to sign the outgoing messages and to verify the signatures of the received messages. The top layer is composed of an authority center and base stations. The authority center manages the operations of all legal nodes' keys in network, including generation, distribution, storage, update and destruction. If mobile nodes directly communicate with each other by wifi or bluetooth, they should mutually verify the validity of the other party. Otherwise, base stations forward their messages, and have to verify the validity of requests. Hence, both base stations and mobile nodes can be the targets of attackers. And they should protect their own security, and identify the invalid signatures in the false messages by themselves.

B. Attack model

We assume the network consists of regular nodes (called verifiers), and malicious nodes (called attackers), which are the two players in the game. One verifier may have multiple malicious neighbors round it as attackers. For a verifier, its attackers intend to interpose its batch verification process by broadcasting false messages with invalid signatures, while the verifier needs to identify the invalid signatures quickly to resist that attack. In this paper, the verifier can be a base station ora mobile node. In addition, in our attack model, for a verifier, its attackers have the following preferences.

1) Attackers cannot interfere or control the key pair generation and assignment, since those can be conduct by secure channels or offline methods. They launch attack in the way of broadcasting false messages with invalid signatures, to disturb the batch verification process, and to consume the verifier's resources
2) Attackers may have multiple attack strategies. To maximize the attack effect, attackers can change their attack strategies occasionally. Also, multiple attackers can tack one single verifier simultaneously with different attack strategies.
3) Attackers are divided into different types based on their preferences. For example, some attackers consider the risk of being traced, but others do not have such concerns. Attackers can acquire the public information of the verifier, such as the public key and the cryptographic algorithm.

IV.GENERIC IDENTIFICATION ALGORTHIMS ANDANALYSIS

Generic invalid signature identification algorithms for abad batch usually adopt the group testing technology. In this section, we describe and analyze the idea of three generic algorithms based on the representative group testing technologies, including individual identification, generalized binary splitting(GBS), Li's s-stage [10], [20], to identify d invalid signatures in a batch of n messages.

A. Individual Identification (II)

One simple solution to identify all invalid signatures ina bad batch, is verifying each signature individually. Note
that signatures are not aggregated with others until all invalid signatures have been found. Many batch verification schemes, which mainly focus on the batch verification process, adopt this algorithm. That is, once the batch verification fails, Individual Identification (II) is employed to find all the invalid signatures. Obviously, the time complexity of II is O(n).

B. Condensed Binary Identification (CBI)

Inspired by the basic binary identification algorithm in [9],we present an improved scheme called the Condensed Binary Identification (CBI) algorithm. In the basic binary identification, it first divides the n messages into two groups of the same size. Then, those two groups are verified using batch verification individually. If the batch verification succeeds, it means that there is no invalid signature in that group. Otherwise, messages in that group will be further divided into two sub-groups, and each sub-group is verified individually. That process repeats until all of the messages pass the batch verification. CBI improves the basic binary identification byadjusting the group size for efficiency. Concerning the probability, the ideal situation is that, each sub-group of n/d messages has one invalid signature, where n/d denotes the largest integer not greater than n/d. If we can adjust the sub-group size based on the number of the remaining invalid signatures, it can reduce the reverification times in attacks. CBI is described as Algorithm 1, where z, θ and vare three intermediate variables. The time complexity of CBI is O(d log(n/d)) [21].

C. 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 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.

V. MODULES

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 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.

B. 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.

C. 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.

D. 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.

II. CONCLUSION

In this paper we proposed, 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.

REFERENCES

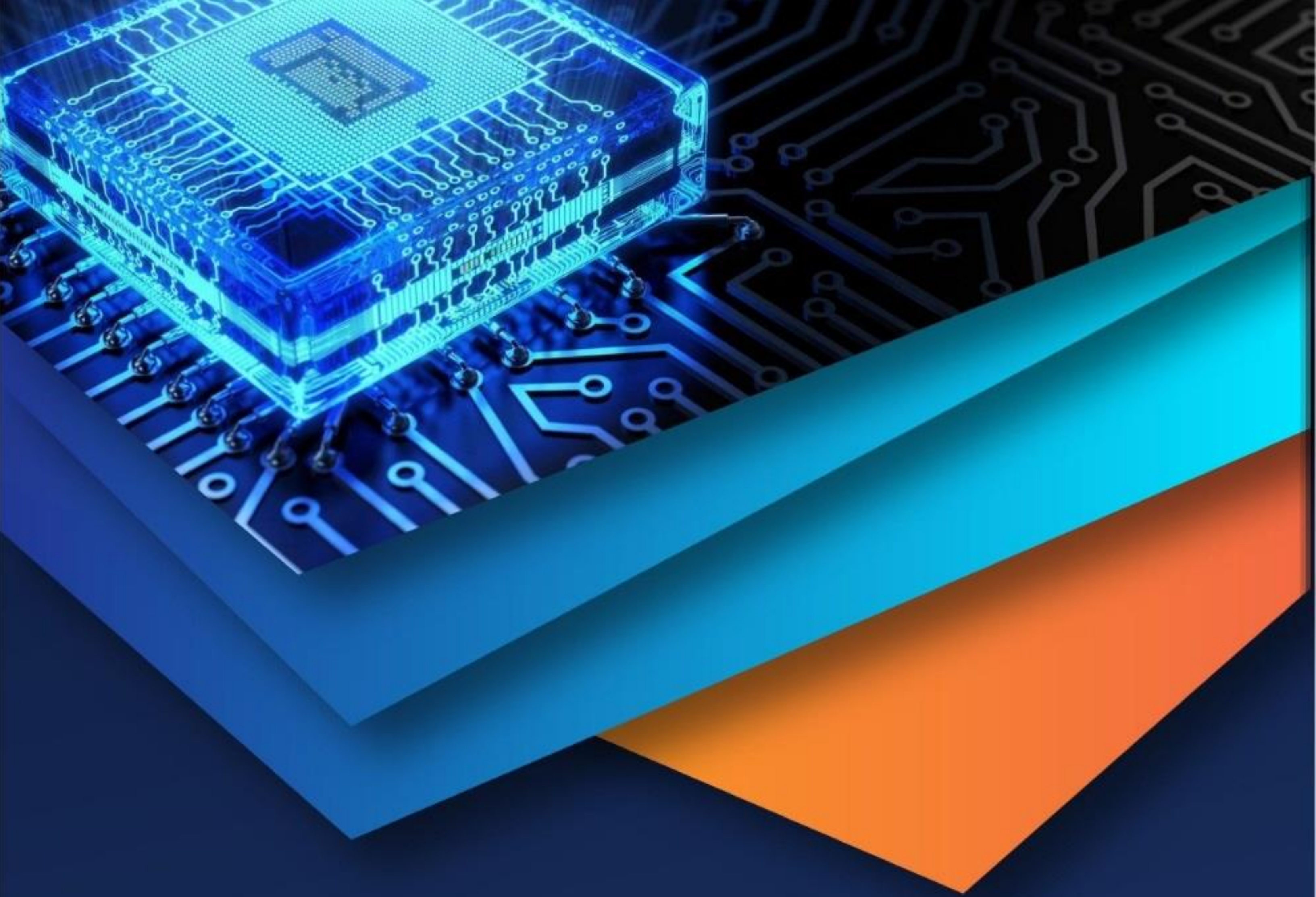
[1] L. Xiao, Y. Chen, W. S. Lin, and K. J. R. Liu, "Indirect Reciprocity Security Game for Large-Scale Wireless Networks," in IEEE Transactionson Information Forensics and Security, 2012.

[2] 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 MobileComputing, 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 Social Networks," in IEEE Transactions on VehicularTechnology, 2012.

[5] A. Fiat, “Batch RSA,” in Proceedings of CRYPTO, 1989.
[6] Naccache, M’Raihi, Vaudenay, and Raphaeli, “Can DSA be Improved? Complexity Trade-offs with the Digital Signature Standard,” 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] Horng, S. Tzeng, Y. Pan, and P. Fan, “b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET,” in IEEE Transactions on Information Forensics and Security, 2013.
[11] J. Pastuszak, D. Michalek, J. Pieprzyk, and J. Seberry, “Identification of Bad Signatures in Batches,” in PKC 2000, LNCS 1751, 2000.
[12] S. Lee, S. Cho, J. Choi, and Y. Cho, “Efficient Identcation of Bad Signatures in RSA-Type Batch Signature,” in IEICE Transactions onFundamentals of Electronics, Communications and Computer Sciences,2006.
[13] L. Law and B. Matt, “Finding Invalid Signatures in Pairing-based Bathes,” in Cryptography and Coding, 2007.
[14] M. Stanek, “Attacking LCCC Batch Verification of RSA Signatures,” in International Journal of Network Security, 2008.
[15] B. J. Matt, “Identification of Multiple Invalid Signatures in Pairing- Based Batched Signatures,” in PKC 2009, 2009.
[16] G. M. Zaverucha and D. R. Stinson, “Group Testing and Batch Verification,” in Proceedings of IEEE ICITS, 2009.
[17] C. Zhang, P. Ho, and J. Tapolcai, “On Batch Verification with Group Testing for Vehicular Communications,” in Wireless Networks, 2011.
[18] C. Lee and Y. Lai, “Toward a Secure Batch Verification with Group Testing for VANET,” in Wireless Networks, 2013.
[19] J. A. Akinyele, M. Green, S. Hohenberger, and M. W. Pagano, “Machine-Generated Algorithms, Proofs and Software for the Batch Verification of Digital Signature Schemes,” in Proceedings ofACM CCS, 2012.
[20] J. Chen, Q. Yuan, G. L. Xue, and R. Y. Du, “Game-Theory-Based Batch Identification of Invalid Signatures in Wireless Mobile Networks,” in Proceedings of IEEE INFOCOM, 2015.



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY