International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Based Scheme of Batch Identification for Invalid Signatures using Game Theory Model in Wireless Mobile Networks

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

Abstract: ***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. 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 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 poor 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. 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, to select 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.***
Keywords: Condensed Binary Identification(CBI), Multiple Rounds Identification(MRI), Attackers, Automatch Protocol, Sink.

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.

II. RELATED WORKS

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 [4], and the first efficient batch verifier was proposed by Naccache et al. in 1994 for DSA-type signatures [5]. 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. In 2008, 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 [6]. Zhang et al [7] discussed a batch signature verification scheme for the communications between vehicles and infrastructure to lower the total verification time. Horng et al. [8] presented a group signature and batch verification method for secure in the system.

On the other hand, batch identification is to find the bad signatures within a batch, when the batch verification fails. Existing batch identification algorithms have been developed into two main branches: special and generic. 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 [6] presented the quick binary and exponentiation method, to find invalid signatures in the pairing based signature schemes. Stanek [7] 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 [8] presented and compared some group testing algorithms for finding invalid signatures. Zhang et al. [10] adopted the group testing technique to find invalid signatures in a batch in mobile networks. Lee et al. [9] proposed a secure batch verification with group testing to improve the real-time performance of mobile networks.

III. SYSTEM MODELS

A. *Network Model*

The base layer comprises of versatile hubs getting to the system by means of GSM, 3G, and so forth. Every hub has its own open/private keys, which are utilized to sign the active messages and to confirm the marks of the got messages. The top layer is made out of a specialist focus what's more, base stations. The expert focus deals with the key operations of every normal hub which can be verified also, approved by disconnected or different strategies, including era, appropriation, stockpiling, redesign, and demolition. In the event that portable hubs specifically speak with each other by Wi-Fi, Bluetooth, and soon. They ought to commonly check the legitimacy of the other party. In the event that base stations forward messages, they have to confirm the legitimacy of solicitations. Subsequently, both base stations what's more, versatile hubs can be assault targets. They ought to ensure their own particular security, and recognize invalid marks in false messages without anyone else's input.

B. *Attack Model*

We expect that the system comprises of customary hubs (called verifiers), and noxious hubs (called assailants), which are the two players in the amusement. For a verifier, its assailants plan to mediate its bunch confirmation handle by broadcasting false messages with invalid marks, while the verifier needs to distinguish the invalid marks rapidly to oppose the assault. Take note of that the verifier is one player and all its malignant neighbors go about as another player. In this paper, the verifier can be a base station or a versatile hub. Initially the network formation is done, once network is formed source node will allow the data to transfer from it through intermediate node and finally reach the destination node. Here batch cryptographic techniques take place. They start with batch verification techniques. If it is true, they directly transfer the messages to receiver else algorithm takes place. In batch identification technique their come CBI and MRI Algorithms and finally identifies the invalid messages. Design Goals and Notations: The fundamental thought of our amusement model is to push consistent hubs to select the reasonable group recognizable proof calculation regardless what the assault methodology. BIGM has solid adaptability to deal with different situations. BIGM is an appropriated conspire which implies that it can function admirably regardless of the possibility that the specialist focus is disconnected. Every consistent hub evaluates current assault technique it confronts and decides the guard methodology concurring to the history data gathered without anyone else. BIGM has the self-advancement capacity to constantly upgrade the determination precision of group recognizable proof calculation from two viewpoints. Generic Batch Identification Algorithms: Nonspecific group distinguishing proof calculations for an awful cluster generally embrace the gathering testing strategy. In this segment, we portray and dissect the possibility of three bland calculations in light of the agent amass testing procedures, including singular distinguishing proof, summed up parallel part.

C. *Condensed Binary Identification*

Propelled by the fundamental parallel distinguishing proof calculation in, we show an enhanced plan called the Condensed Double Identification (CBI) calculation. In the essential paired ID, it first partitions the n messages into two gatherings of equivalent size. At that point, those two gatherings are confirmed utilizing bunch confirmation independently. Something else, messages in that gathering will be further separated into two subgroups, also, every sub-gathering is confirmed independently. CBI enhances the essential parallel distinguishing proof by modifying the gathering size for effectiveness. Concerning the likelihood, the perfect circumstance is that, every sub-gathering of ⌈n/d⌉ messages has one invalid mark, where ⌈n/d⌉ signifies the littlest whole number at the very least n/d. On the off chance that we can modify the sub-gather estimate in view of the quantity of the staying invalid marks, it can lessen the quantity of re verifications in assaults.

D. *Multiple Round Identification*

In Multiple Rounds Identification (MRI) calculation, we distinguish the invalid marks in an iterative way which has m ($2 \leq m \leq n$)

rounds, as depicted in Algorithm 2. In the first round, the n pending messages are partitioned into δ1 bunches; what's more, every gathering has γ1 messages aside from the last gathering. At that point, every gathering is confirmed individually. The gatherings recognized with invalid marks are totaled as another pending message bunch. In the second round, that new message bunch is separated into δ2 gatherings of γ2 messages. A cluster check test is performed on every gathering. In this way every invalid mark is recognized at round m.

E. Implementation Techniques

1) *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.
2) *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.
3) *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.
4) *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

IV. 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. At the fourth time of transaction, source can send packets only by normal node path .For encryption and decryption, RSA algorithm is used.

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 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 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 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] S. 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.