International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 02 | Feb -2017 www.irjet.net p-ISSN: 2395-0072

Self Adaptive Automatch Protocol for Batch Identification Mechanism in Wireless Mobile Network

Ammu.R [1], Harini.M [2], Sumedha.K.R [3] ,Venkata Lakshmi.S[4]

[4]*S.Venkata Lakshmi, Professor, Dept. of Computer Science & Engineering, Panimalar Institute Of Technology, Chennai, Tamilnadu, India*

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. 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.

Keywords: Condensed Binary Identification(CBI), Multiple Rounds Identification(MRI), Attackers, AutomatchProtocol, Sink.

1. 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. 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 cellsite or base station. A network

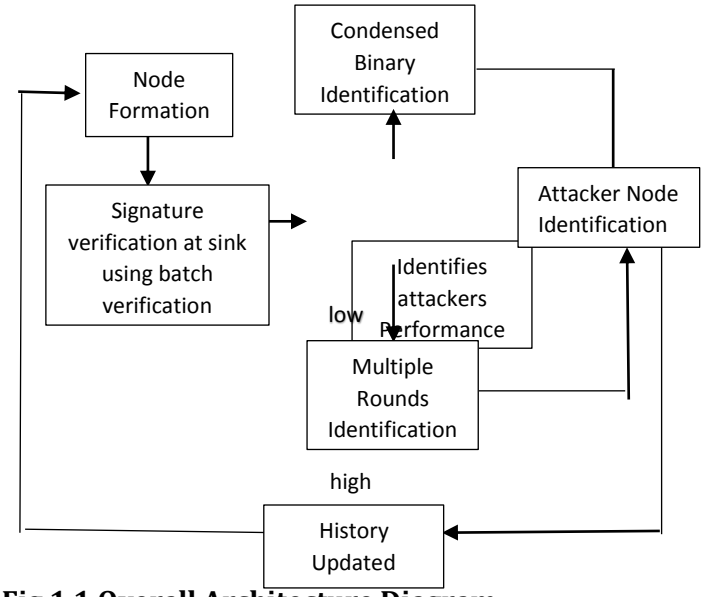

Fig.1.1.Overall Architecture Diagram

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. Digital signature is a widely used technique to protect messages' authenticity and nodes' identities. 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.

2. RELATED WORK

[1]. 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, two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications[3]. In this work ,the cost due to the loss of network services exceeds the illegal security gains of the attack, rational nodes do not have incentive to attack, and hence in the proposed system it reduces the attacking probability in the network. For that a social norm and reputation updating process to build such an indirect reciprocity mechanism the network is developed.[6]. The paper addresses the problem of bad signature identification in batch verification of digital signatures .The verifier, probability distributions for the number of generic tests necessary to identify one, two and three bad signatures, are derived.[2]. Security and privacy issues on OSNs are major concerns hence a security framework for simultaneously authenticating multiple users to improve the efficiency and security of peer-to-peer (P2P)-based OSNs.[5]. A botnet in mobile networks is a collection of compromised nodes due to mobile malware, which are able to perform coordinated attacks. Mobile botnets can propagate at the fastest rate of quadratic growth in size, which is substantially slower than the exponential growth of Internet botnets.[4]. Addressing pollution attacks either require an extra secure channel or incur high computation overhead. In this paper, an efficient signature-based scheme is designed to detect and filter pollution attacks for the applications adopting linear network coding techniques.[7].In this paper , an implementation of the homomorphic evaluation of AES, an amortized cost of about 12 minutes per AES cipher text on a standard desktop computer[10]. New methods in pairing-based signature schemes for identifying the invalid digital signatures in a batch, after batch verification has failed. These methods efficiently identify non-trivial numbers of invalid signatures in batches of (potentially large) numbers of signatures.[9]. As the use of electronic voting systems and e-commerce systems increases, the efficient batch verification of digital signatures becomes more and more important. a new method to identify bad signatures in batches efficiently for the case when the batch contains one bad signature[11]. Finding invalid signatures in batches of signatures that fail batch verification is an instance of the classical group testing problem and hence a new sequential and parallel algorithms is proposed for finding invalid signatures based on group testing algorithms.[8]. Wireless networks are vulnerable to Sybil attacks, in which a malicious node poses as many identities in order to gain disproportionate influence.[12]. In this paper, an efficient identity-based batch signature verification scheme is proposed for vehicular communications. With the proposed scheme, vehicles can verify a batch of signatures once instead of in a one-by-one manner.

3. PROPOSED SYSTEM

Proposed system to improve the performance of batch identification. Batch identification consists of two algorithms namely Condensed Binary Identification (CBI) and Multiple Rounds Identification (MRI).

3.1.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.

3.2. 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.

3.3. Receiver performance based 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.

3.4. Receiver performance based on mixture of attackers 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.

4. EXPERIMENTAL RESULTS

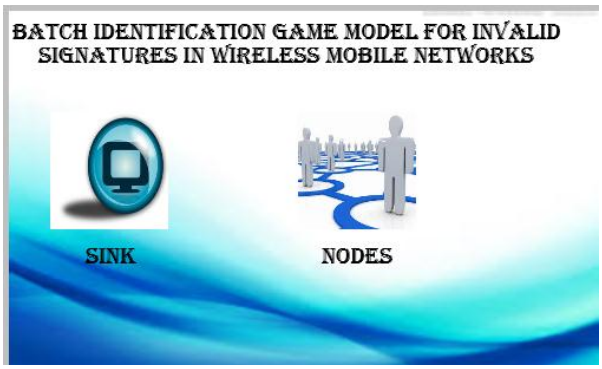

Figure 4.1 –Node formation

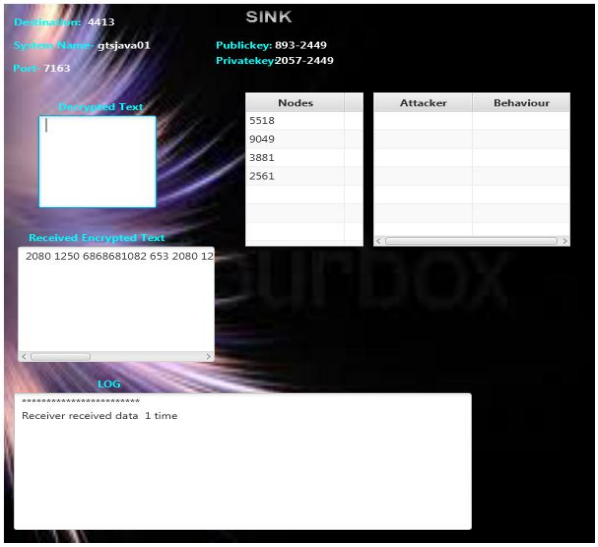

Figure 4.2- Intermediate nodes transfer the messages to the destination

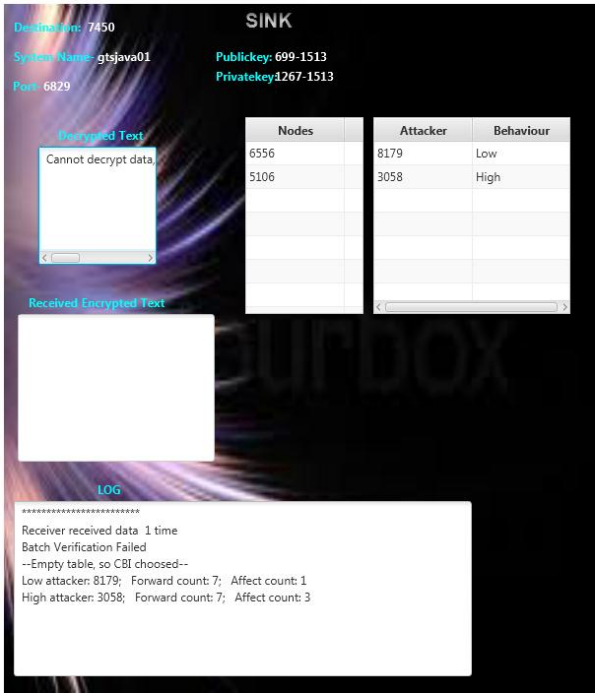

Figure4.3-Finding the corrupted packet

Figure 4.4-Receiver intimate to the normal users about the attackers.

5. CONCLUSION AND ENHANCEMENT

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.

The enhancements as follow: In the fourth time of transaction, source will send the data by using only normal node path & neglect the attacker's path and for encryption and decryption, RSA algorithm is used.

ACKNOWLEDGEMENT

The authors can acknowledge any person/authorities in this section. This is not mandatory.

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 SensorNetworks," 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.
[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 Identification of Bad Signatures in RSA-Type Batch Signature," in IEICE Transactions on Fundamentals 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.