ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A BATCH AUTHENTICATION SCHEMA TO IDENTIFY THE INVALID SIGNATURE IN WIRELESS NETWORK

N.Deepa Assistant Professor*, A.Sakthivel Student, M.Rengesh Student, S.Sai Aravindhan Student
Computer Science, G.K.M College of Engineering and Technology, India

DOI: 10.5281/zenodo.290183

ABSTRACT

Mobile Computing 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. Security is the most important thing in transmission of data. In wireless network the security is less and invalid data can be easily transmit to the receiver by the intermediator(attacker). To improve the security of the data batch cryptography is used. The batch cryptography consist of batch verification and identification. By using these method data protection can be done in the wireless network. To find the intermediator who produce the invalid signature the Nash Equilibrium is used. The nash equilibrium will help in the finding the intermediate node in the dynamically changing network. It will have a history of data transmitted node from the source to the destination.

KEYWORDS: Batch Verification, Nash Equilibriums, Invalid Signature

INTRODUCTION

Now wireless mobile network have been used dramatically by all the mobile, computer, laptop, etc. Since there have been development in mobile application and social network in current scenario the wireless network become domination because it can be used anywhere and anytime. The openness character of the wireless channel will make easier for malicious node to interfere in your data transfer. To protect your message you have to use digital signature in your message to make it more secure. The signature will have more verification delay if the message is large and the quality of service will be affected.

To reduce the verification delay and ensure the quality of service batch cryptographic is used. The batch cryptographic will used two important technique 1.Batch Verification 2.Batch Identification. The Batch verification deals with n message pair as a batch. As compare with the traditional batch verification it will be more efficient. The batch verification will reduce the time delay at the receiver end. The Batch identification will make sure that the whole batch is valid or not. The batch identification will use divide and conquer method in both the sender and receiver end. It will be easy if the message is divided into equal parts. The batch identification will easily identify the invalid signature in the batch which has been created by the intermediate.

Another important technique used is Batch Identification Game Model. The Game Model used to identify the invalid signature in dynamic attack. The game model must have more than two information in order to identify the attack. The game model will use Nash Equilibrium. The nash equilibrium consist of four different player playing card game. The card game could have one looser. The looser will use the winning player strategy to improve his game play. This strategy will improve the performance of batch identification game model. This will help to find out whether the attacker is high attacker or low level attacker. And will have a history of all the data loss or attack which has been done in the transmission and receiving of the message.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Attacker

The attacker or the intermediate are the ones who attack in the transmission and receiving of the message. The attacker are the main cause for the loss of data in the wireless network. The attacker would be present at the node of the wireless network since the message are transmitted through the nodes.There are of two types 1.High-level attacker 2.Low-level attacker. The attacker could have an easy access in the wireless network because of the infrastructure

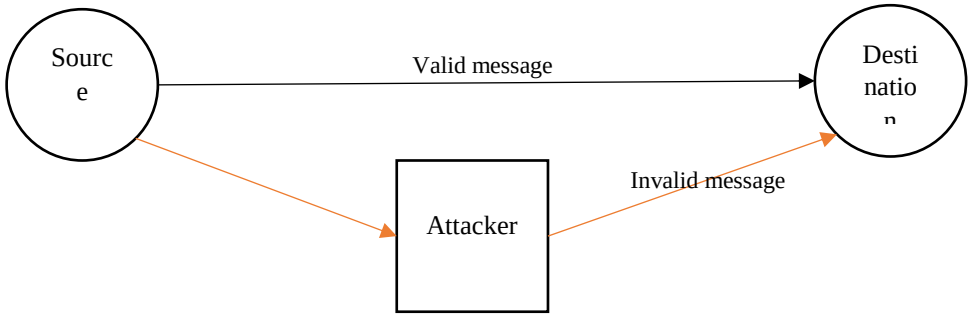

Fig 1

High-level attacker

The high-level attacker are the most dangerous one's in the network. The high-level attacker could have access to 50% of your data.

Low-level attacker

The low-level attacker could have 30% access to your data.

BATCH CRYPTOGRAPHY

The Batch cryptography technique is used for batch verification and batch identification. The batch cryptography is used to improve the quality of the service and to reduce the time delay in the batch identification. The batch cryptography will make sure that only verified user can see the message which has been send through the wireless network. The batch cryptography will use the key exchange so that only the destination(receiver) with that key could open the message to read.

Batch Verification

The Batch verification deals with n(message, signature) pair of batch at the same time. This technique will reduce the time delay in the verification process. This will only return true if all the n-batch has same signature and return false if there is a single invalid signature. As compare with the traditional method of verification this technique will reduce the and improve in the validation of the batch more efficiently.

Batch Identification

The Batch identification will come to process if the batch verification fails. This technique will help to find out the invalid signature or the bad signature in the batch. The batch identification consist of two important technique. This technique is used to find whether the attacker is high level or low level.

1.CBI (Condensed Binary Identification)
2.MRI (Multiple Rounds Identification)

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

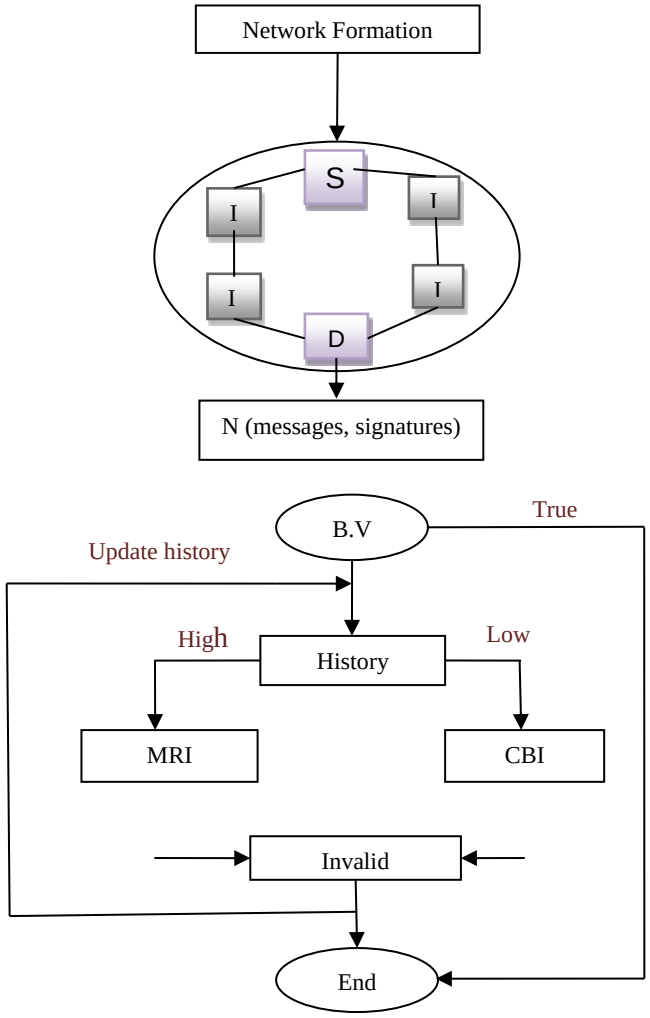

Fig 2

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. The time complexity of CBI is Θ(d log (n/d)).

$$MCBI\ (d, n) = \begin{cases} n\ for\ n \leq 2d - 2 \\ \theta d + k1\ for\ n \geq 2d - 1 \end{cases}$$

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. The time complexity of the MRI is Θ(log(n/d)).

GAME MODEL

The game model consists of two different player playing game. In our model one player will be the attacker and the another player will be receiver. There could be any number of player in the wireless network. The strategy will differ according to the attacker. The attacker will use two type of strategy one will be high level attack and another will be low level attack. The receiver or destination should change dynamically according to the attacker. In the wireless network the chance of finding the strategy is difficult because of the loss of data in the network. The game model will use history of report on the receiver side. This report is used to find out whether the attacker is high level or low level. This report will choose which Batch verification technique should be used.

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).

CONCLUSION

In the above paper we have proposed the crypto graphic technique to find the invalid signature in the wireless network. In the wireless network there could be any number of intermediate in the network. The crypto graphic technique has two algorithm which is used to find the invalid signature and batch verification in the message. Then the game model is used to have a history of the transmission in the table format. The nash equilibrium is used in the game model with the self adaptive and auto match protocol to change continuously to find the node(attacker). These will help in the quality of service and will reduce the time delay in the continuously changing wireless network.

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.
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 Identication 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.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

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 of ACM 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.
21. 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.
22. Y. Ephraim and W. J. J. Roberts, "An EM Algorithm for Markov Modulated Markov Processes," in *IEEE Transactions on Signal Processing*, 2009.
23. "MIRACL Cryptographic Library: Multiprecision Integer and Rational Arithmetic C/C++ Library [Online]," https://www.certivox.com/miracl.
24. "IEEE Trial-use Standard for Wireless Access in Vehicular Environments-security Services for Applications and Management Messages," in *IEEE Standard 1609*, 2006.