Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

BATCH SIGNATURE - ENERGY: MULTIPATH & MULTI PACKET SECURED DATA TRANSMISSION USING ENERGY LEVEL MONITORING

PRAKASH.K.J, N.MAGESHKUMAR

[1]*Final Year IT, Department of IT, Jeppiaar Maamallan Engineering College, Chennai, India*
[2]*Asst.Prof, Department of IT, Jeppiaar Maamallan Engineering College, Chennai, India*

Abstract—*The Data Sender will first split the packets into multiple batches and create Batch signature for every batch and then starts sending the packets to the destination. Secure access is one of the fundamental problems in wireless mobile networks. Digital signature is a widely used technique to protect messages, authenticity and node 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. Batch cryptography technique is a powerful tool to reduce verification time. As it is Wireless network, multiple nodes has to transmit the data in the given network. If any node tries to inject any packet or remove any packet its ID will also be added to the Batch Signature automatically. Verifier first verifies the Signature info before transmitting the packets to the destination. We also implement node energy level estimation in order to verify whether the same node transmits the data or not.*

Keywords *- Data Integrity Security, Deduplication, Cloud storage, Key Distribution*

I. INTRODUCTION

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. In Existing system they use a Batch Identification Game Model (BIGM) in WMNs, enabling nodes to identify invalid signatures with a reasonable delay under heterogeneous and dynamic attacks. To enhance the flexibility of our model, we subdivide BIGM into Batch Identification Game Model with Complete information (C-BIGM) and Batch Identification Game Model with Incomplete information (I-BIGM) to protect regular nodes from the attacks of invalid signatures in different scenarios. In our model, a mobile node may be a regular one or a malicious one, and the game occurs between a regular node and its malicious neighbours. The regular node, as a verifier aims at finding the invalid signatures to eliminate the impact of malicious nodes. The malicious neighbors, as attackers, intend to interpose batch verification process by broadcasting false messages signed by invalid signatures with different frequencies. Our main contributions are summarized as follows:

- To evaluate the effectiveness of batch identification, we recast three generic batch identification algorithms based on the group testing techniques. We analyze and compare the time complexities of these algorithms with experiments. We observe that none of them has universal advantages in all situations. Therefore, we need an auto-match scheme to choose the batch identification algorithm adaptively, when the attack strategy changes.

- We design a game model to find the dominant batch identification algorithm against various attack strategies. We analyze and prove the existence of Nash equilibriums in the complete information scenario and the incomplete information scenario, respectively. Note that the members in strategy set are alternative, as long as these generic batch identification algorithms have their own advantages under different attack strategies. Thus, our gamemodel provides a paradigm to select the dominant one to identify invalid signatures. Furthermore, BIGM is a generic solution, which can be equipped with any batch signature scheme._

- Considering that the dominant strategy may not always be the optimal choice, we propose a selfadaptive auto-match protocol to improve the selection accuracy of the batch identification algorithm based on history information. From the analysis and simulations, we find that it can effectively strengthen the prediction accuracy of nodes, states and the sensitivity of attack perception, and reduce the average identification delay of the whole network.

The modes of data transmission is wired and wireless. Data transmission has a major development and security aspects has many problems. Many security problems are solved using various algorithm. The hackers are more intelligent to break the data transmission. So it become very tough to transmit the data without any interrupt and efficiency of data is also important. Many researchers consider the efficient technology for both wired and wireless network to increase their performance. Attackers can take advantage on security aspects illegally, If they not being caught and punished. Sensitive

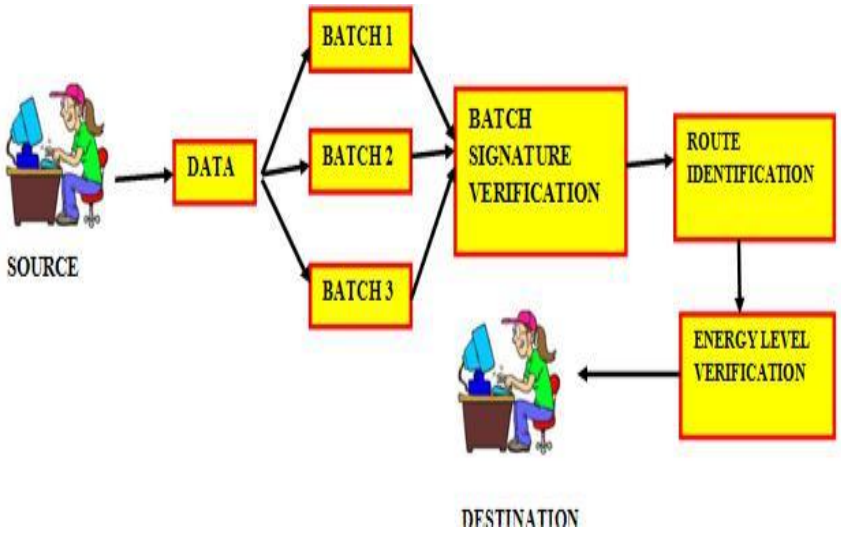
data should be encrypted before sending so that it becomes difficult to retrieve data back to original form. This paper is about secured data transmission by multipath and multi packet using energy level monitoring.

II. RELATED WORK

Due to the openness characteristic in the wireless channel it becomes easy for the hacker node to interfere while transmission takes place. With the increasing number of mobile application, social media and GPS where humans life are inseparable by using these technologies. So it is very important to give a secured way of transmitting data in wireless channels. Because people transmits their personal information through these technologies. So their information must be sent in secured way without any interruption. This can be done by attaching a batch signature for each packet. But the signature verification may cause extra delay. To reduce these things the proposed system was derived.

The Data Sender will first split the packets into multiple batches and create Batch signature for every batch and then starts sending the packets to the destination. As it is Wireless network, multiple nodes has to transmit the data in the given network. If any node tries to inject any packet or remove any packet its ID will also be added to the Batch Signature automatically. Verifier first verifies the Signature info before transmitting the packets to the destination. We also implement node energy level estimation in order to verify whether the same node transmits the data or not. Before transmission of packets the routes and the nodes are identified. Every node's ID and relevant Energy level is noticed by the verified before transmitting the packets. If any variation, then packets are discarded so that malicious packets are not transmitted.

III. SYSTEM ARCHITECTURE



First the data sender will send the dummy packet to the destination to identify the route and nodes present in route. The sender splits the data packet into three sub packet and for each packet unique batch signature id will be added. Each node has to know the before and next nodes id so that data can be transmitted.

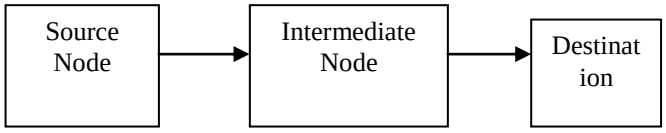
When the hacker node interrupts during data transmission its id will be added to the packet. The packet will be received by next node , while verifying it id will be changed so that node identifies the hacker interrupted and rejects the packet and ask the sender to resend the data. By this way the Batch signature verification and route identification is done.

We also implement Energy level monitoring as energy is very important to transmit the data. For every data transmitted by the node its energy gets reduced. When low energy level node is selected to send a data it may transmit the data slow or data loss may occur. Hence alternate route is selected.
When the energy of node changes more than 5 it identifies the node as malicious node and rejects the packet. By this way energy level verification is done. So through this way we are providing a secured data transmission to the receiver

IV. PROPOSED MODULES

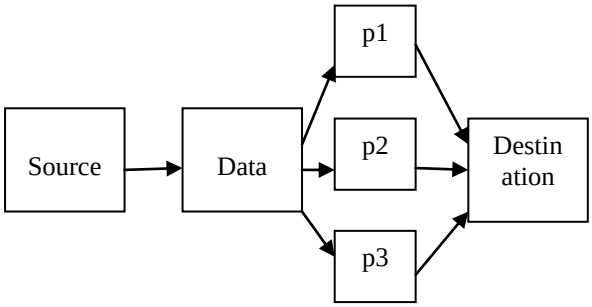
1. SOURCE ROUTING

This module is developed in order to create a network construction. In a network, nodes are interconnected, which monitors all the other nodes. All nodes are sharing their information with each others. Node will be connected with each other to share its own ID to next and previous node.



2. PACKET SPLITTING

In this user data will split into multiple packets with batch signature. Data should be splits and send into destination in secured way. Packet splitting is for security purpose Because if we send data in single packet without any signature there is a chance for loss data or hackers will easily hack the information . So we spilt it and add signature to every packet.

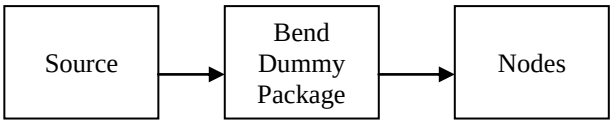


3. BATCH SIGNATURE VERIFICATION

Every node have to know their neighbor's node ID. Before sending the data from source to destination each node will know about the ID of next node. If data is send from one node to another node it will verify its ID with existing ID .If it match with existing signature , data will transfer to next node. If any packets are loss or added to it, that new ID will be added and send to next node so that it will discard that node by verifying its ID.

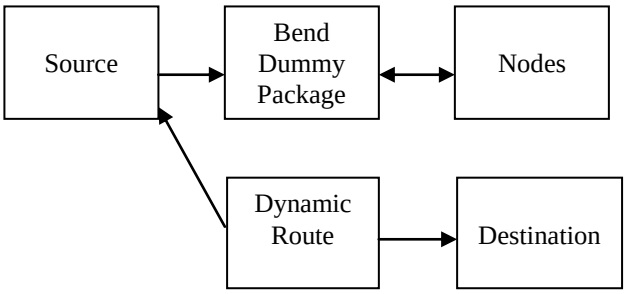
4. ENERGY LEVEL MONITORING

In this module energy level of every node is identified and set route to that path Because the energy level of node is important to transfer data. If low level energy node is selected to send data there is a chance to loss or delay to transfer the data. So we also identify the energy level of every node.



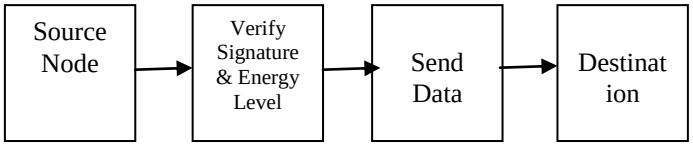
5.DYNAMIC REROUTING

In this module node is constructed to transfer the data from source to destination. Before sending data path is identified to transfer the information. If selected route contain any traffic problem dynamic route is selected and send data through that dynamic route.



6. **Packets delivery**

After verifying node ID and batch signature data will be transferred from source to destination. If any variation, then packets are discarded so that malicious packets are not transmitted.



V.BATCH SIGNATURE ALGORITHM

1. Batch signature

Batch Signature is a important type of authentication in a public key cryptographic system. The batch signature verification may cause extra delay. To improve its performance the digital signature are computed into batch and allocating each batch only once. This increases the performance of transmission but it requires additional information to be carried out to the client.

2. Dynamic Source Routing

The sender of the packet determines the complete sequence of nodes to forward the packet to the destination. It dynamically determines route based on cached information and result of the route discovery.

To send a packet to another host, the sender constructs a source route in the packets header. Each mobile host participating in the ad hoc network maintains a route cache in which it caches source routes. If no route found, the sender may attempt to discover one using the route discovery protocol. Host monitors the correct operation of a route in use, we call route maintenance.

The main advantage of using DSR is to allow multiple routes to any destination and allow each sender to select and control the route. Here no need to keep the routing table inside each node because the entire route is contained in the packet header.

3. RSA Algorithm

Rivest Shamir Adleman algorithm is a public key encryption type algorithm in which one user uses a public key and other user uses a secret key. In this algorithm each station independently and randomly chooses two large primes p and q number and multiplies them to produce n=pq. The size of n is 1024 bits. Pick two large prime number p and q and calculate the n value.

Get Public key as $K_u=\{e,n\}$.

Get Private key as $K_r=\{d,n\}$.

Encryption:

Cipher text $C=P^e \bmod n$

Decryption:

Plain text $P=C^d \bmod n$

The main advantage of RSA as it can be used for both encryption as well as for digital signature. Trapdoor in RSA is in knowing value of n but not knowing the primes that are factors of n.

VI. CONCLUSION

Thus the proposed system provides security to the data. We attach the sender signature with node ID. By this way intermediate node and receiver node can able to know who is the sender. If any interruption while sending or any hacker can try to break the data, receiver can easily identify and block the hacker node. So through this way we are providing a secure data to the receiver.

REFERENCES

[1] J. Chen, K. He, Q. Yuan, G. Xue, R. Du and L. Wang, "Batch Identification Game Model for Invalid Signatures in Wireless Mobile Networks," in *IEEE Transactions on Mobile Computing*, vol. 16, no. 6, pp. 1530-1543, June 1 2017.

[2] A. Abouaomar, A. Filali and A. Kobbane, "Caching, device-to-device and fog computing in 5th cellular networks generation : Survey," *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Rabat, 2017, pp. 1-6

[3] T. Li, H. Zhou, H. Luo, I. You and Q. Xu, "SAT-FLOW: Multi-Strategy Flow Table Management for Software Defined Satellite Networks," in *IEEE Access*, vol. 5, pp. 14952-14965, 2017.

[4] A. T. Siwe and H. Tembine, "Network security as public good: A mean-field-type game theory approach," *2016 13th International Multi-Conference on Systems, Signals & Devices (SSD)*, Leipzig, 2016, pp. 601-606.

[5] P. Pop, M. L. Raagaard, S. S. Craciunas and W. Steiner, "Design optimisation of cyber-physical distributed systems using IEEE time-sensitive networks," in *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 86-94, 12 2016

[6] Y. Liu, D. R. Bild, R. P. Dick, Z. M. Mao and D. S. Wallach, "The Mason Test: A Defense Against Sybil Attacks in Wireless Networks Without Trusted Authorities," in *IEEE Transactions on Mobile Computing*, vol. 14, no. 11, pp. 2376-2391, Nov. 1 2015.

[7] J. Chen, K. He, R. Du, M. Zheng, Y. Xiang and Q. Yuan, "Dominating Set and Network Coding-Based Routing in Wireless Mesh Networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 2, pp. 423-433, Feb. 2015

[8] 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*, vol. 7, no. 4, pp. 1368-1380, Aug. 2012.

[9] L. Xiao, W. S. Lin, Y. Chen and K. J. R. Liu, "Indirect reciprocity game modeling for secure wireless networks," *2012 IEEE International Conference on Communications (ICC)*, Ottawa, ON, 2012, pp. 928-933.

