Securing Data Transmission By Discovering Attacker

Ms. RMeenakshi M.E[1], B Anushiya[2]
[1, 2] Dept of Information Technology
[1, 2] Valliammai Engineering College,Tamil Nadu,India

Abstract- *The Wireless mobile network is the network which consists of mobile nodes used for data connections and data transmission. Nowadays security is the major issue in wireless mobile networks to transmit the data. Data transmission in mobile networks must be efficient. As the technologies increasing, wireless networks becoming more vulnerable. The proposed system uses Batch verification algorithm for secure and efficient transmission. Batch verification deals with n number of nodes simultaneously. The data that is sending through the network splits into batches. Unique signature will be assigned to each and every batches. The signature which is assigned to batches is generated randomly. The signature of batches will be verified before transmitting packets. If any node tries to inject or modify the packets then the signature is added with that particular node. So that no node can modify the packets. Before transmitting the packets energy level of each and every node will be verified. The source node of the network sends a dummy packets to intimate that it is going to transmit data. By sending the dummy packets, it will get the energy level and signature of every node throughout the network. While transmitting packets the sender verifies the signature and the energy level of the node. Finding an energy level of a node is too difficult, because it keeps changing according to the usage of the node. So it is very hard to find energy level for any attacker. During verification of both signature and energy level, if any variation occurs then the packets are discarded. The corresponding path will be discarded then by using dynamic source routing the path will be rerouted. The advantages of this proposed system are the data can be sent efficiently and securely.*

Keywords- Wireless mobile networks, batch verification, Energy level, Dynamic Source Routing(DSR).

I. INTRODUCTION

Wireless mobile networks are literally becoming more vulnerable these days due to dramatic increase in technologies. Security is a problem which plays a vital role in transmitting the data packets. Transmitting data securely is the biggest challenge now a days. The data that is transmitting should have minimum delay. Networks are expecting the data transmission with acceptable data transmission rate. To overcome all these issues the proposed system is implemented. In the proposed system batch verification is an algorithm which has been implemented for secure data transmission. The data will be splitted into batches according to the data file size. Signature will be provided for all nodes. The batch signature is verified and if any variation is identified then the packet will be discarded on that corresponding path alone. Missed data will be resent through next available path which was identified by using Dynamic source routing.

II. LITERATURE SURVEY

Batch verification is the technique which is used in wireless mobile networks for secure transmission. Splitting the data into batches helps to reduce the delay in transmitting. While verifying the attacker can be identified and it will be removed from the network.

RecentlyGuoliangXue, Jing Chen, Kun He, Quan Yuan, Ruiying Du, and Lina Wang in [1] presents that digital signature and the batch cryptography are the commonly used techniques to protect the data transmission. But it fails in producing minimum delay and low verification time. Hence the batch identification game model technique has been introduced. In order to prove the nash equilibrium existence and to secure data it has been identified. This technique helps to identify the invalid signature.

Alomair, B. and Poovendran, presents in [2] the message which is authenticated must be encrypted. It is proposed that three classes of standard authentication codes are used. They are MAC based on block ciphers, cryptographic hash functions and universal hash-function families. It uses the encryption technique in order to produce simplicity and efficiency rather than using long keys. Which in turn reduces the consumption of energy.

Y. Chen, W. S. Lin, and K. J. R. Liu, L. Xiao in [3] presents that some radio nodes performs attacks toidentify illegal gains which produces larger cost. The indirect reciprocity principle is introduced in proposed system in order to combat attacks. It evaluates the stability using the evolutionarily stable strategy concept. It helps in reducing attacker population by satisfying the stability condition. Simulation is performed to identify the security gain.

Chen, K. Du, Y. He, R. Xiang, and Yuan,Ddescribes in [4] that network coding improves performance of the wireless network. The mechanism used in this system are connected dominating set and flow-oriented coding-aware routing. Minimum connected dominating set is constructed by CFCR. It introduces information conformation process which deals with collision problems. It reduces rate of failure. The second contribution is to consider flow coding and CDS at a time.

S. S. M. Chow, M. Du, M. He, R. W. F. Lai, Q. Wang, and Q.Zou presents in [5] the encrypted file is retrieved by using searchable symmetric technique. This technique has been introduced to rely on Boolean expressions for matching of keys. By using fuzzy bloom filters the solutions are built which uses LSH locality sensitive hashing. It increases performances by securing the data and also achieved quality of search.

Anthony D. Joseph, Lo-Yao Yeh, Shiuhpyng Winston Shieh, Woei-JiunnTsaur,Yu-Lun Huang in [6] security and privacy is the major problem in online social networks(OSN) such as facebook. There are three techniques which is been used in this system. They are one way hash function adaptation, El Gamal proxy encryption and cryptosystems certificates.In order to meet the requirements such as flexibility, non-repudiation, authentication this system has been introduced.

III. SYSTEM ARCHITECTURE

The architecture diagram explains the proposed work to be done in this project. It consists of components that can be assembled easily and integrated to obtain the best result.

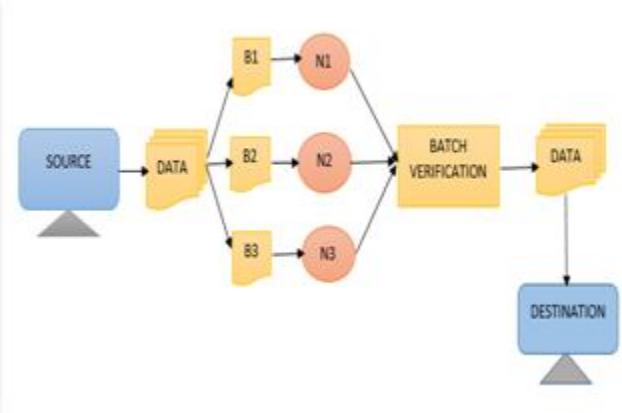

Fig -1: Architecture diagram

IV. IMPLEMENTATION

1.Network creation: The network with n number of mobile nodes is created. Every mobile nodes communicate with each other in that network. Each and every node has their unique ID and neighbour's ID. All nodes will be having the information about every nodes throughout the network. It helps in identifying the paths to transmit the data efficiently.

2. Dividing data packets: In the network, the data will be splitting into batches. A data file splits into batches in order to provide efficiency.While transmitting data from source to destination the data packets is split into multiple batches. Each and every batch has its unique signature which is then verifies to find the invalid signature. Unique ID is generated randomly.

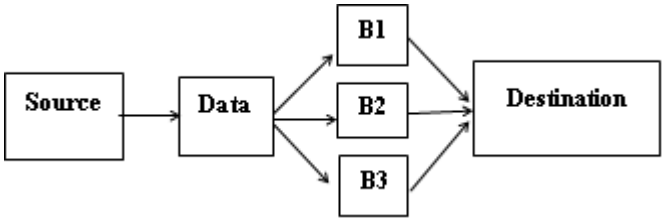

Fig-2 Packet splitting

3. Signature verification: Nodes in the network stores each and every node's ID. The source collects all the signatures of batches and nodes. While transmitting the data it verifies the unique signature with its database. If the ID matches, then the data packets will be transmitted. If it finds any variation in IDs then the transmission will be terminated on that path alone. That data will be rerouted to any other available path in the network which helps in finding the hacker. Because when the hacker tries to modify the data or inject any data, then the corresponding node's ID will be added to existing node. Hence the invalid signature can be identified.

4. Examining Energy level: Energy level of a node is defined as the capability of a node to perform data transmission. Energy level is dynamic that is it keeps on changing according to the usage of a node. Hence it is hard to identify the energy level of a node. It helps to secure the data transmission. The energy level of a node is collected by the source node by transmitting the dummy packets. While transmitting the data packets it verifies the energy level of every node with its available database. If it matches energy level, then the data will be transmitted through that corresponding node. Else it discards the nodes in the network.

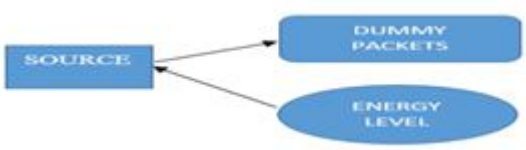

Fig -3: Examining Energy level

5. Secure Transmission: The source node sends the dummy packets throughout the network by intimating that it is going to send the data packet to the destination on this corresponding path. The dummy packets are also send to collect every node's ID and energy level of the node. Then the data is spilt into multiple batches according to the data size. Before transmitting the batches the source node verifies unique ID and Energy level of a node. If the ID and energy level of a node on the path matches the database, then the data packets will be transmitted through that path. If any variation occurs then the packet transmission will be terminated on that path alone rather than terminating the whole transmission. The source discards attacked path and reroute the data packets through any other available path in the network. Thus the data packets are delivered to the destination node securely. It also provides efficient data packets delivery.

Fig-4 Secure transmission

6. Rerouting: Dynamic source routing is an on-demand routing protocol. It is a protocol used to find route in a network. It works under two states. One is route identification and another one is route maintenance. The source node broadcasts requests message throughout the network. Upon receiving the requests message, a destination node reply back to the source node. DSR is used to reroute the data packets in this system. Whenever it finds attacker node in a path, the corresponding path gets discarded and automatically the data packet which is been sent through that path is rerouted to another available path. And that path will be identified using dynamic source routing protocol.

V. BENEFITS

- It reduces additional delay.
- This system also decreases performance degradation.
- It ensures flexibility.

VI. CONCLUSION

With the help of this system, the invalid signature is identified. And it helps in finding the attacker in the network. It leads to secure transmission throughout the network. It also provides minimum delay and improves performance.

REFERENCES

[1] Jing Chen, Kun He, Quan Yuan, GuoliangXue, Fellow, IEEE, Ruiying Du, and Lina Wang [2017], "Batch Identification Game Model for Invalid Signatures in Wireless Mobile Networks", IEEE transactions on mobile computing, volume 16, No.6, June 2017.

[2] B. Alomair and R. Poovendran, "Efficient authentication for mobile and pervasive computing," IEEE Transactions on Mobile Computing, vol. 13, no. 3, pp. 496–481, March 2014.

[3] 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.

[4] Chen, K. Du, Y. He, R. Xiang, and Yuan,D. 'Dominating set and network coding-based routing in wireless mesh networks' ,IEEE Trans. Parallel Distributed System, volume 26, no. 2, pp. 423–433,2015.

[5] S. S. M. Chow, M. Du, M. He, R. W. F. Lai, Q. Wang, and Q.Zou, 'Searchable encryption over feature-rich data', IEEE Trans. Depend. Secure Computer Available: http://doi.org/ 10.1109/TDSC.2016.2593444,2016.

[6] Anthony D. Joseph, Lo-Yao Yeh, Shiuhpyng Winston Shieh, Woei-JiunnTsaur, Yu-Lun Huang, 'A Batch-Authenticated and Key Agreement Framework for P2P-Based Online Social Networks', IEEE Transactions Vehicle Technologies volume 61, no. 4, pp. 1907–1924,2012.