Ensuring Trustworthiness and Security during Data Transmission in Multihop Wireless Networks

[1]S.Nandhini, [2]Mr.S.Franson Varun Richo,
[1]PG Student, [2]Assistant professor,
Francis Xavier Engineering college,
Tirunelveli, TamilNadu, India.

***Abstract* - Ensuring trustworthiness and security in multi hop wireless networks is to improve throughput, efficiency, and packet delivery ratio and it also reduce delay in a secure manner. In this scheme, all the mobile nodes share the master key value with their neighbors and submit trust value information to the accounting center which is based on their energy level, battery power, and how efficiently they relay other node's packet and these values are used to select the path from source to destination. The communication between source and destination is initialized using route-request and route-reply packets through trust based routing protocol. The data packets are sent through only highly trusted nodes. The authentication process is handled by accounting center. The destination prepares symmetric key from its master key and compares it with the symmetric key that was composed from source's master key for authentication purpose. The trusted values will be updated frequently and sent to accounting center through base station for further processing.**

***Index terms* - accounting center, payment reports, trust based routing protocol, trust values.**

I. INTRODUCTION

A multihop wireless network is a communication network in which communication takes place through multiple routes from source to destination and also it takes multiple hops for the data to travel from end to end. Multihop wireless network is used in secure transmission because it can be deployed at low cost and it can be extended to a large extent. Multihop Wireless network is considered as hopeful network as it supports applications such as data sharing, multimedia transmission, and transaction purposes.

In this type of network, some nodes are independent and self-interested called as egotistic nodes which do not relay other's packet because in order to save their own resources. Instead they make use of other altruistic nodes to relay their own packets. Altruistic nodes are those which spend its own resources to relay other's packets. Resources can be bandwidth, energy level, battery power, etc. Egoistic nodes are of two types, one is rational node in which they are brought under the control of malicious node and motivated to misbehave. Second is irrational node in which they misbehave intentionally. This action totally degrades the performance, packet delivery ratio and increases delay in data transmission of multihop wireless networks.

In [1] the reports are sent to the trusted party and evidences are stored in order to resolve the disputes. The classifier in the trusted party classifies them into fair and cheating reports. And evict the cheating nodes by verifying the inconsistencies of the report submission. Hence we develop a scheme to make these selfish nodes to cooperate and information is sent only through highly protected nodes and data is transmitted using trust based routing protocol. The source sends its data packet to its neighbor only when it finds that node to be trusted. The trusted values can be investigated at the accounting center as they are stored in accounting center and communication between accounting center and nodes are done by using base station.

II. RELATED WORKS

The existing payment schemes are tamper-proof-device based and Receipt-based schemes. In tamper-proof device based scheme, tamper proof device is installed in each node to store and manage its credit account. The Self-generated packets forwarded by a node are passed to the TPD to decrease and increase the node's credit account. For receipt-based payment schemes, an offline central unit called

 All Rights Reserved © 2014 IJARCET

accounting center stores and manages node's credit account. Here, proofs of relaying packets are called as receipts which are submitted to the accounting center. The receipts which are submitted to AC are large in size because they carry security proofs to secure the payment which significantly consumes the node's resources and available bandwidth in submitting them.

The existing credit card payment schemes are infeasible for MWNs and it involves complexity in communication and processing overhead. In tamper-proof device based scheme, tamper proof cannot be guaranteed because the nodes are autonomous and the nodes cannot communicate if they do not have sufficient credits during communication system. The Receipt-based scheme imposes more overhead because the receipt size is large and large cryptographic operations are applied on receipts to verify them. It suffers from false accusation and missed detection. It is more vulnerable to collusion attacks. It takes long time to identify the cheaters.

In [1] RACE: In report based payment scheme, the mobile nodes submit light weight payment reports to the accounting center. The accounting center identifies the cheating reports by the inconsistent submission of cheating nodes and requests evidence only when the accounting center needs. By processing the evidences, the accounting center smartly evicts the cheating node from the path and secure data transmission is carried on.

In [2] Stimulating Cooperation in Multi-hop Wireless Networks Using Cheating Detection System, Cheating detection system (CDS) to secure the payment and can identify the cheating nodes effectively under different cheating strategies.It uses statistical methods to identify the cheating nodes that submit incorrect reports.

In [3] FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Multihop Cellular Networks, node cooperation is encouraged to promote fairness. The mechanism applies a fair charging policy by charging the source and destination nodes when both of them benefit from the communication. Large number of public-key-cryptography operations are used.

In [4] ESIP, Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multihop Wireless Networks, a secure cooperation incentive protocol is that which uses the public-key operations only for the first packet in a series and it uses the lightweight hashing operations in the next packets. It has large receipt size.

In [5] An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Dropping Attack in Multihop Wireless Networks, a novel monitoring technique to measure the nodes' frequency of dropping packets based on processing the payment receipts instead of using the medium overhearing technique.

III.SYSTEM MODEL

This scheme has four phases, the initialization phase in where the mobile nodes are created which are suitable for data transmission, and able to move anywhere in the networking environment. They exchange topology discovery packets and master key value with their neighbours and submit trust values to the accounting centre through base station. In route establishment phase, the sender sends the route request to all its neighbours. The route reply packet is sent from receiver to sender through the same path.

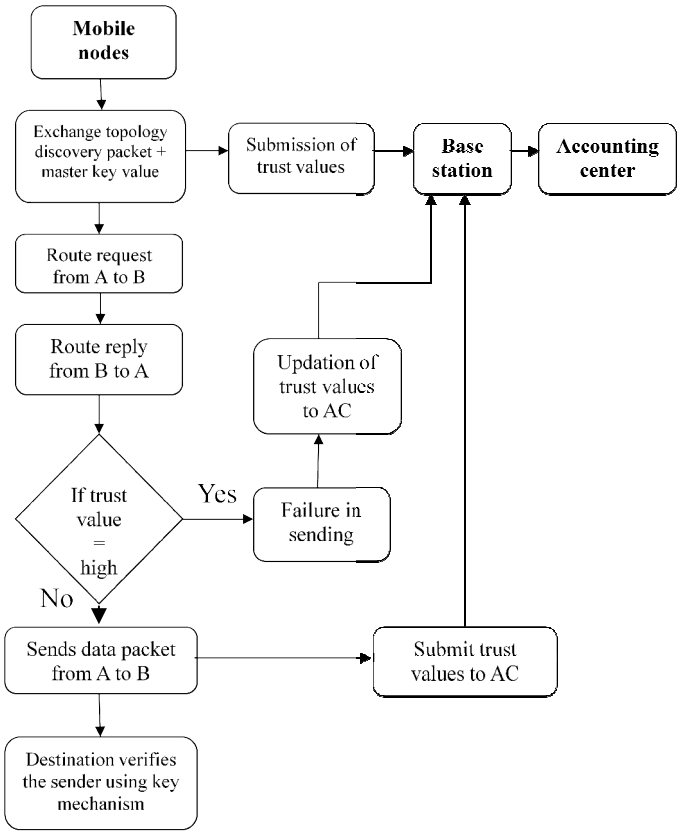

Fig.1. SYSTEM ARCHITECTURE

In data transmission phase, the node transmits data to its neighbour i.e. the node in the established path only when the trust value is high. Otherwise the trust values are reported to base station as low. Then the data transmission is done through the secure trusted path. In updation of trust values phase, the trust values of the node participated in the data transmission are submitted to the accounting centre because their values will be increased or decreased due to their participation in data transmission.

 All Rights Reserved © 2014 IJARCET

IV. PROPOSED SCHEME

A. Initialization phase:

In initialization phase is where the mobile nodes are created which are suitable for data transmission, and able to move anywhere in the networking environment. The base station and accounting centre are assigned. The communication between the mobile nodes and accounting centre is done by using base station. The mobile nodes exchange topology discovery packets in order to discover the topology and master key value with their neighbours for the purpose of authentication. And submit trust values to the accounting centre through base station.

B. Route Establishment phase.

In route establishment phase, the sender sends the route request packet to all its neighbours. The packets are then forwarded to their own neighbours and finally to destination. Then the destination replies with the route reply packet through the same shortest path. The route between source to destination is thus established.

C. Data transmission phase.

In this phase, the sender checks the trust values of its neighbour in the established path. The trust value can be known by contacting accounting centre. When checking the trust value, if it founds to be high, then the sender sends the data to its neighbour. Otherwise, data will be failed to send and trust values will be updated to the accounting centre. Likewise, the neighbour checks the trust value for its neighbour i.e. is the next node in the established path and it forwards the data to it. Then finally the data reaches the destination.

D. Trust Value updation phase.

In updation of trust values phase, the trust values of the node participated in the data transmission are submitted to the accounting centre because their values will be increased or decreased due to their participation in data transmission.

V. RESULTS

The system performance by using this scheme is calculated. The parameters are throughput, delay, and packet delivery ratio. The measure clearly describes that the performance shows better results than the other schemes.

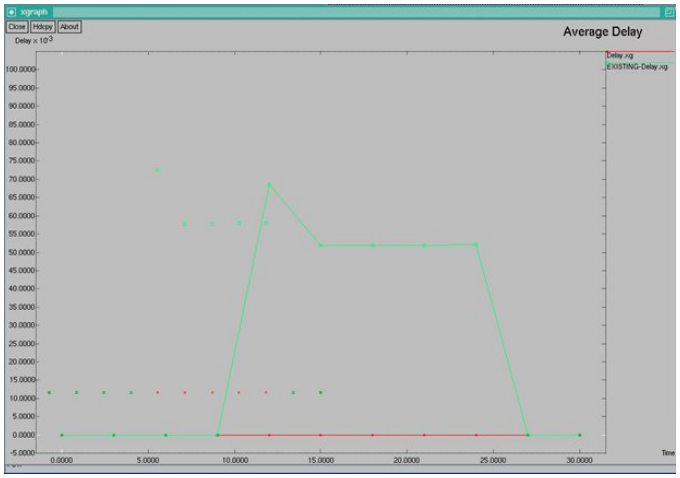

Fig 2. Reduction in Average delay

The average delay time of proposed scheme has been reduced when compared to existing scheme.

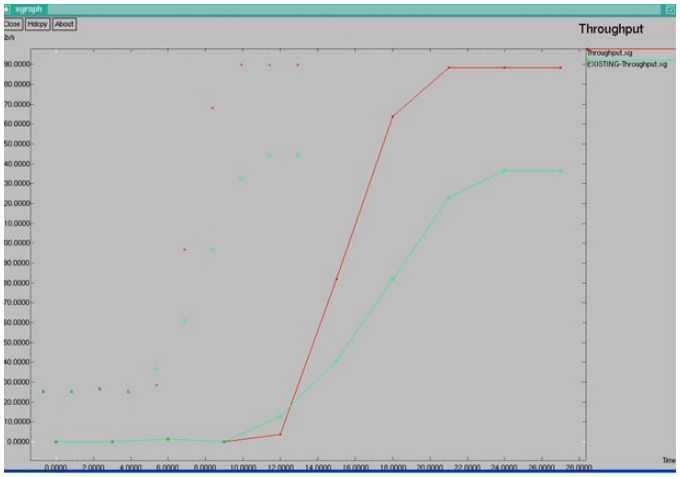

Fig 3. Performance measure.

The performance of the proposed scheme has been highly increased when compared to the existing scheme.

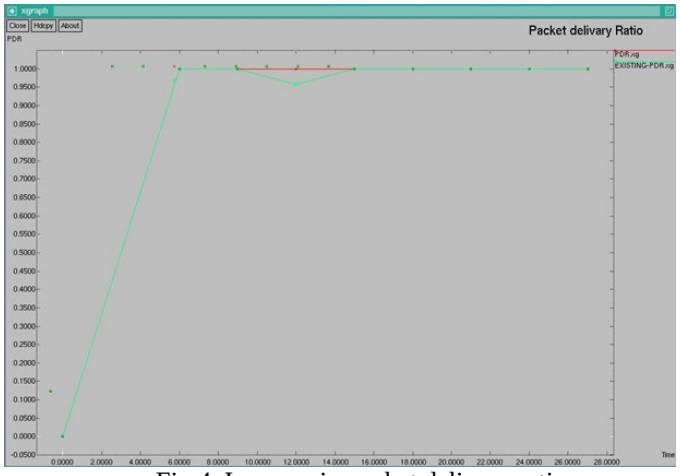

Fig 4. Increase in packet delivery ratio

 All Rights Reserved © 2014 IJARCET

The packet delivery ratio of the proposed scheme has been highly improved when compared to the existing system.

VI.CONCLUSION

Thus, the scheme is used in multihop wireless networks to improve throughput, efficiency, packet delivery ratio and reduce delay in a secure manner. All the mobile nodes share the master key value with their neighbors and submit trust value information to the accounting center which is based on their energy level, battery power, and how efficiently they relay other node's packet and these values are used to select the path from source to destination. Thus, high level of security and trustworthiness is ensured because the nodes transmit data only when the neighbor node founds to be trusted.

ACKNOWLEDGMENT

First of all we thank the almighty for giving us the knowledge and courage to complete the research work successfully. We express our gratitude to all our well wisher who really motivates us in publishing this paper.

REFERENCES

[1] A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks Mohamed M.E.A. Mahmoud and Xuemin (Sherman) Shen, Fellow, IEEE , vol. 24 No. 2, February 2013.

[2] M. Mahmoud and X. Shen, "Stimulating Cooperation in Multihop Wireless Networks Using Cheating Detection System," Proc. IEEE INFOCOM '10, Mar. 2010.

[3] M. Mahmoud and X. Shen"FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 11, no. 5, pp. 753-766, May 2012

[4] M. Mahmoud and X. Shen, "ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-Hop Wireless Networks," IEEE Trans. Mobile Computing, vol. 10, no. 7, pp. 997-1010, July 2011.

[5] M. Mahmoud and X. Shen"FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 11, no. 5, pp. 753-766, May 2012

[6] S.Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, vol. 3, pp. 1987-1997, Mar./Apr. 2003.

[7] M. Mahmoud and X. Shen, "PIS: A Practical Incentive System for Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010

[8] M. Mahmoud and X. Shen"FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 11, no. 5, pp. 753-766, May 2012

[9] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit Based Incentive Scheme for Delay-Tolerant Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 4628-4639, Oct. 2009.

[10] N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "Node Cooperation in Hybrid Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 4, pp. 365-376, Apr. 2006.

AUTHOR(S) PROFILE

Ms. S. Nandhini is presently studying M.E. Second year Network Engineering in Francis Xavier Engineering College, Tirunelveli. She has completed her B.Tech Information technology from J.J College of Engineering and Technology, Trichy. She is an member of Computer Society of India. Her field of Interests are Networking, Mobile computing.

Mr. S. Franson Varun Richo is presently working as an Assistant Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E. Computer science and engineering from Karunya University, Coimbatore and his M.E Computer science and engineering from satyabama university, Chennai. His area of interests are Networking and Mobile computing.

 All Rights Reserved © 2014 IJARCET

 All Rights Reserved © 2014 IJARCET