Secure and Reliable Routing Protocols for Heterogeneous Trust Management Multihop Wireless Networks

Miss Komatwar Tejashwi Deepak[#1], Prof V.R Chirchi[*2]
[#]*PG Student, PG Department of MBES College of engg Ambajogai, BAMU University*
[#]*Assistant Professor, PG Department of MBES College of engg.Ambajogai*

ABSTRACT-*The aim of this paper provides E-STAR used for establishing stable and reliable routes in heterogeneous multihop wireless networks. The payment system in E-STAR used to reward the nodes which relay others' packets and charges those that send packets from source to destination.The trust values depends on nodes' public-key certificates and then develop two routing protocols to direct communicate between them and then highly-trusted nodes having sufficient energy to reduce the probability of breaking the route. E-STAR can stimulate the nodes not only to relay packets, but also to maintain route stability. Experimental results show that E-STAR can secure the payment and trust calculation without error. Simulation results show that routing protocols can improve the packet delivery ratio and route stability.*

Keywords- securingheterogeneous multihop wireless networks, packet dropping and selfishness attacks, trust systems, and secure routing protocols

I. Introduction-

The multihop wireless networks contains mobile nodes which needs the communication between source and destination, it depends on the other nodes to relay the packets [1]. The multihop packet transmission can spread the network coverage area using limited power and best spectral area efficiency. The network can be useful for data sharing and multimedia data transmission [2]. But malfunctioned nodes frequently drop packets and break the routes due to faulty malicious nodes. The routes' stability is based on nodes'behavior; randomly selecting the intermediate nodes will degrade the nodes' communication.In HMWNs, breaking the routes increases the packet delivery latency and may cause network partitioning and the multi-hop communication to fail.

In this paper, E-STAR is used to secure protocol for Establishing STAble and reliable Routes in HMWNs. The nodes requires the proofs of relaying packets that's called receipts and then submit them to TP. SRR(shortest reliable route) and BAR(best available route) are used to calculate trust values and energy. A node's trust values are attached to its public-key certificate to be used in making routing decisions. The simulation results demonstrate that our routing protocols can improve the packet delivery ratio due to establishing stable routes.In section 2, reviews the related works. In section 3 includes algorithms, in section 4, flow chart of E-STAR framework. In section 5, includes hardware and software specification and section 6, includes the advantages. In section 7 includes experimental results and section 8, includes conclusion.

II. Literature Review-

S. Marti, T. Giuli, K. Lai, and M. Baker [3] hasreviewed overall concept on the reputation-based schemes which reduce packets loss in the data transmission. When a node N_A sends a packet to the node N_B then N_C is relay node between them. Reputation-based schemes suffer from false accusations where some honest nodes are falsely identified as malicious. Thesenodes that drop packets temporarily, may be falsely identified as malicious by its neighbors. In order to reduce the false accusations, the schemes should use tolerant thresholds to guarantee that a node's packet dropping rate can only reach the threshold if the node is malicious. In this schemes, it is difficult to optimize the threshold between honest and malicious node in HMWNs. Therefore, which can -not guarantee route stability or reliability in HMWNs.

Sprite [4], PIS [5], and ESIP [6]have discovered the payment schemes that use credits to encourage the nodes to relay others' packets. In Sprite [8], the message sends source node to destination node that established the route. Each intermediate node verifies the signature and submits a signed receipt to TP to claim the payment. In PIS [9], that reducesthe receipts' number and generates a fixed size receiptper route of number of messages. In ESIP [10], the payment scheme uses a communication protocol that can transfer messages from the source node to the destination with limited use of the public key cryptography operations.Public key cryptography is used for only one packet and the efficient hashing operations are used in next packets.

Theodorakopoulos and Baras [7] analyze the issue of evaluating the trust level as a generalization of the shortest-path problem in an oriented graph, where the edges correspond to the opinion that a node has about other node.

Velloso et al. [8] have proposed a human-based model which builds a trust relationship between nodes in ad hoc network.

Lindsay et al. [9] have developed information the framework to quantitatively measure trust and model trust propagation in ad hoc networks.

M. Yu and K. Leung [10], secure routing protocols with quality of service support have been proposed.

III. ALGORITHMS-SHA-1Algorithm Framework

- Step 1: Append Padding Bits…. Message is padded with 1's and 0's
- Step 2: Append Length....64 bits are appended to the end of the padded message
- Step 3: Prepare Processing Functions….
- Step 4: Prepare Processing Constants....
- Step 6: Processing Message in 512-bit blocks (L blocks in total message)…. This is the main task of SHA1 algorithm which loops through the padded and appended message in 512-bit blocks

RSA Algorithm Framework

This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on a public and private key system.

The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key; this makes the RSA algorithm a very popular choice in data encryption.

IV. ARCHITECTURE OF E-STAR –

E-STAR isasecureprotocolforEstablishingSTAbleandreliableRoutesinheterogeneous multihopwirelessnetworksasshowninFig.1.Inwirelessnetworkinformationtransmissionfromsourcetodestinationandeachandeverynode willhaveadistinctiveidentificationandreporttothe relied on source and destination.The trusted partieswilloverviewtrustvaluesforeachandeverynode withtheirnodesearlierbehavior.Afterupdatingthetrustvaluestheroutingestablishmentproceduarecarriedoutviabywayof SRRandBAR.WhereasSRRwilldiscoverashortestandreliablepathanditavoidsthelowdependedonnodes .BARwilltofindessentiallythemostsecureone.

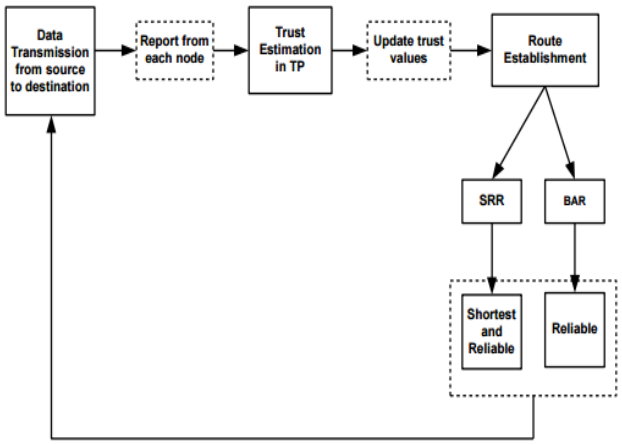

Fig.1.SystemArchitecture

A . DataTransmission:

The messages are sent from source node to the destination node through a route with the intermediate nodes. The route is situated by using the routing protocols. There as on of the source nodes signature is to ensure the authenticity and integrity of the message. Additionally, secure the fee through enabling TP to ensure that the source has sent messages. Every node in the route composes are ceipt and submits it when the node has a connection to the depended on get together to say the fee andupdateitstrustvalues.Everyintermediatenodeverifiesthesourcenodesignatureandstoresthosesignatureswith hashmessageforcomposingtherecord. Are port is the primary proof for taking part in a route and sending, forwarding and receiving quantity of messages.

B. Trust Values:

Once TP receives a receipt, it first checks whether the receipt has been processed before making use of its specified identifier. Then, it verifies the credibility of the receipt by means of computing the node's signatures and hashing them. If the report is legitimate, the trust get together verifies the destination node's hash message. The relay node depends on the intermediate node. The relay node displays the trust values and reward value in secure manner. The quality of sent messages is signed by means of the source node and the number of delivered messages has been computed from the number of hashing operations. Trust values are calculated from intermediate node's behavior for predicting the unlikely future behaviors. The trust method decreases the trust values of the two nodes in broken link. The

nodes that break routes which are in increasing order then trust level degrades trust values.

V. HARDWARE AND SOFTWARE SPECIFICATION -

Hardware Configuration

- **Processor** **-Pentium** –IV
  - ❖ Speed - 1.1Ghz
  - ❖ RAM - 256MB(min)
  - ❖ Hard Disk - 20GB
  - ❖ Key Board - StandardWindows Keyboard
  - ❖ Mouse - Two or Three Button Mouse
  - ❖ Monitor - SVGA

Software Configuration

- Operating System : Windows XP
- Programming Language : JAVA
- Front end : Swings & AWT

VI. Advantages:

1. Reduce the probability of breaking the routes.
2. E-STAR integration can deliver messages through reliable routes and allow the source nodes to prescribe their required level of trust.
3. Decrease the energy efficient routing protocols of minimal-hop metric.
4. The information packet header in DSR depends on all of intermediate node deals with source and destination in reduce of throughput.
5. Optimized Link State Routing(OLRS) is based on neighbor selection protocol, in that each node only manages a subset of network topology data.

VII.EXPERIMENTAL RESULTS –

In this experimental, we select the source and destination and then send the request to send and receive the packets as shown in fig.2. During data transmission these selected nodes are used to generate the relay nodes and then we view the result of them. We can view the result of energy levels which depends on intermediate nodes as well as other nodes. And also view the result of reward values of relay node as well as amount of nodes in network.

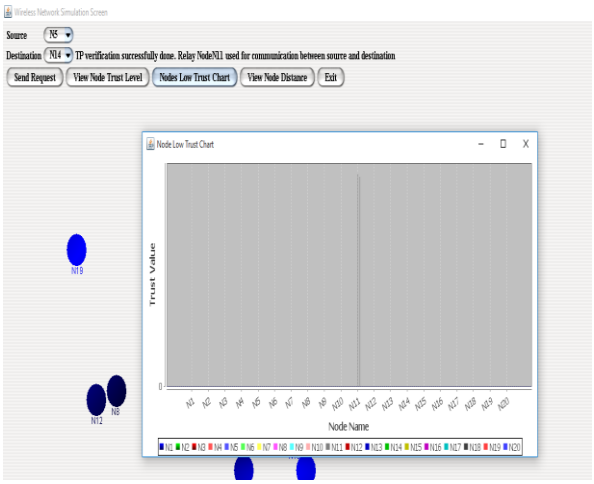

Fig.2. Graph of relay node

In fig.2, relay node gain the reward values, because which is based on communication between source and destination. The source nodes will loss the amount because it is sending file to the destination. In above graph, the relay node loss the energy and it has low trust values during data transmission among the source and destination. The packet delivery ratio shows in below fig.3.

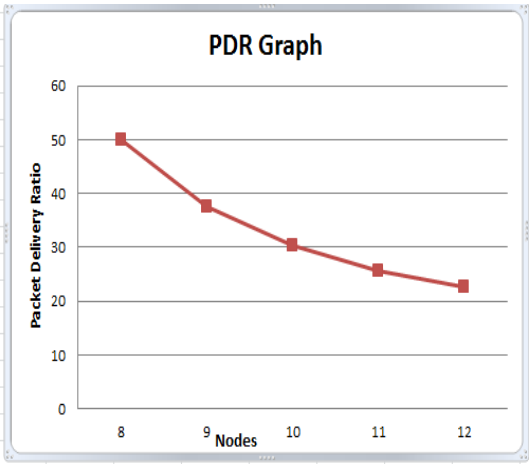

Fig.3. Graph of Packet Delivery Ratio.

As shown in above fig.3 the packet delivery ratio significantly degrades as the number of low –trusted nodes increases due to the nodes who involving in routes more frequently. Packet loss as shown in below fig.

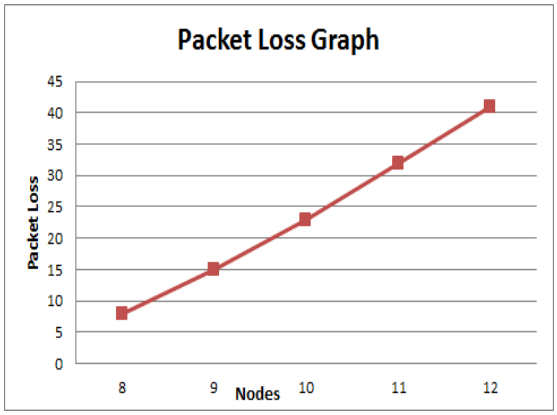

Fig.4. Graph of Packet loss.

As shown in above fig. packet loss increases in order of increasing order of number of nodes. Low-trusted nodes based on packet loss.

CONCLUSION-

In this paper, we proposed an E-STAR protocol. E-STAR stands for Establishing STAble and reliable Routes in the Heterogeneous Multihop Wireless Networks. The main goal this project is to reduce the probability of route breaking stable along with reliable routes in the wireless networks. In this project, Best Available Route(BAR) protocol means direct communication between source and destination send data with shortest path as well as reliable path. And Shortest Reliable Route (SRR) means relay node between source and destination. Finally it proved that this protocol achieved high packet delivery in HMWNs.

REFERENCES –

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

[2] C. Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, Jan. 2007.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Mis-behavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom'00, 255-265, Aug. 2000.

[4] 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.

[5] M. Mahmoud and X. Shen, "PIS: A Practical Incentive System For mobile ad hoc network, sensor network, and delay-tolerant network. Multi-Hop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, Oct. 2010.

[6] 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.

[7] G. Theodorakopoulos and J.S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 318-328, Feb. 2006.

[8] P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model," IEEE Trans. Network and Service Management, vol. 7, no. 3, pp. 172-185, Sept. 2010.

[9] S. Lindsay, Y. Wei, H. Zhu, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006.

[10] M. Yu and K. Leung, "A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 8, no. 4, pp. 1888-1898, Apr. 2009.