Establishing Stable and Reliable Routes for Heterogeneous Multihop Wireless Networks

Pavithra . N[#1], Nija Shining Gold. T.L[*2]

[1]PG Scholar, Ponjesly College of Engineering, Nagercoil, India

[2] Assistant Professor, Ponjesly College of Engineering, Nagercoil, India

***Abstract*-We propose E-STAR for establishing stable and reliable routes in heterogeneous multihop wireless networks. E-STAR combines payment and trust systems with a trust-based and energy-aware routing protocol. The payment system rewards the nodes that relay other's packets and charges those that send packets. The trust system evaluates the node's competence and reliability in relaying packets in terms of multi-dimensional trust values. The trust values are attached to the node's public-key certificates to be used in making routing decisions. We develop two routing protocols to direct traffic through those highly-trusted nodes having sufficient energy to minimize the probability of breaking the route. By this way, E-STAR can stimulate the nodes not only to relay packets, but also to maintain route stability and report correct battery energy capability. This is because any loss of trust will result in loss of future earnings. Moreover, an efficient anonymous communication protocol, called MANET Anonymous Peer-to-peer Communication Protocol (MAPCP), for P2P applications over MANET was proposed. MAPCP also maintains high packet delivery fraction even under selective attacks. The efficient implementation of the trust system, the trust values are computed by processing the payment receipts.**

Keywords-Securing heterogeneous multihop wireless networks, packet dropping and selfishness attacks, trust systems,payment system and secure routing protocols.

I.INTRODUCTION

In multihop wireless networks, when a mobile node needs to communicate with a remote destination, it relies on the other nodes to relay the packets [1]. This multihop packet transmission can extend the network coverage area using limited power and improve area spectral efficiency.The multihop wireless network implemented in many useful applications such as data sharing and multimedia data transmission. It can establish a network to communicate, distribute files, and share information. However, the assumption that the nodes are willing to spend their limited resources, such as battery energy and available network bandwidth.

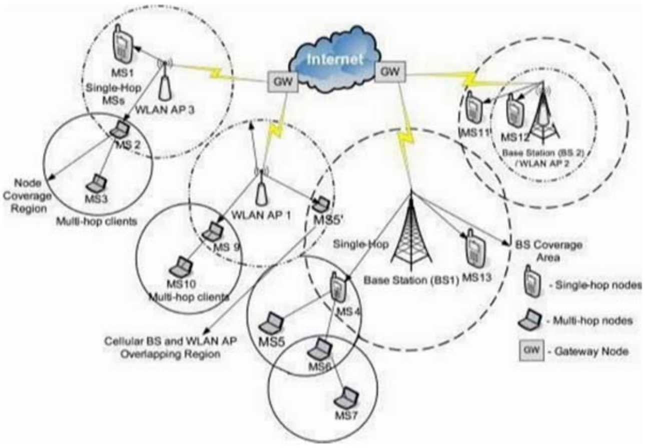

Figure 1: A logical Multihop wireless network architecture

A set of wireless communication nodes performing self-configuration in a dynamic mode for formation of network excluding fixed infrastructure or centralized supervision is termed as mobile ad hoc network (MANET). Often, there may be random changes in the network topology as nodes are mobile. In addition to the role of router, the nodes also play the role of end host. The routing protocol in such a network is an authority to determine the routes and offering communication among end points via intermediate nodes. The MANET is well-liked and attractive since they offer good communication in the changing infrastructure for the applications such as rescue operations, tactical operations, environmental monitoring, conferences[2] .The primary goal of routing protocols in ad-hoc network[11] is to create a path (minimum hops) between source and destination with minimum overhead and minimum bandwidth use so that packets are transmitted in a timely and orderly manner. A MANET protocol should function effectively over a large range of networking context from small ad-hoc group to larger mobile multi-hop networks.

II. RELATED WORKS

Reputation-based schemes[3] suffer from false accusations where some honest nodes are falsely identified as malicious.This is because the nodes that drop packets temporarily, e.g., due to congestion, may be falsely identified as maliciousby 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. However, this increasesthe missed detections where some malicious nodes are not identified. Moreover, tolerant threshold enables the nodes with high packet dropping rate to participate in routes, and enables the malicious nodes to circumvent the scheme by dropping packets at a rate lower than the scheme's threshold. When a node's reputation value is above the threshold,it does not have incentive to relay packets because it does not bring more utility. The system proposed the concept that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem to categorizing the nodes based upon their dynamically measured behavior. So in this section the two extensions are introduced to the Dynamic Source Routing algorithm [4] to mitigate the effects of routing misbehavior, such as watchdog and path rater. The watchdog identifies misbehaving nodes, while the path rater avoids routing packets through these nodes.

In ESIP [5], 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. Unlike ESIP that aims to transfer messages efficiently, E-STAR aims to establish stable and reliable routes.In [6], payment is used to thwart the rational packet-dropping attacks, where the attackers drop packets because they do not benefit from relaying packets. A reputation system is also used to identify the irrational packet-dropping attackers once their packet-dropping rates exceed a threshold.

Theodorakopoulos and Baras [7] analyze the issue of evaluating the trust level as a generalization of the shortestpath problem in an oriented graph, where the edges correspond to the opinion that a node has about other node. The main goal is to enable the nodes to indirectly build trust relationships using exclusively monitored information. In [8], Velloso et al. have proposed a human-based model which builds a trust relationship between nodes in ad hoc network. Without the need for global trust knowledge, they have presented a protocol that scales efficiently for large networks. In [9], a secure routing protocol with quality of service support has been proposed. The routing metrics are obtained by combing the requirements on the trustworthiness of the nodes and the quality of service of the links along a route.

III.PROPOSED SYSTEM

The heterogeneous Multihop Wireless Networks has mobile nodes and offline Trusted Party (TP) whose public key is known to all the nodes. The mobile nodes have different hardware and energy capabilities.. Each node has a unique identity and public/private key pair with a limited-time certificate issued by TP. Without a valid certificate, the node cannot communicate nor act as an intermediate node. TP maintains the node’s credit accounts and trust values. Each node contacts TP to submit the payment reports and TP updates the involved node’s payment accounts and trust values.

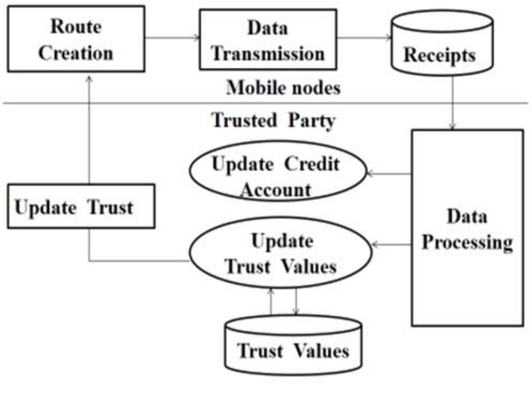

Figure 2 : E-STAR in Multihop Wireless Network

The Fig. 2 presents the Architecture for E-STAR in multihop wireless network. In wireless network data transmission from source to destination and each node will have a unique identity and report to the trusted party. The trusted party will evaluate a trust value for each node with their node’s past behaviour. After updating the trust values the routing establishment process are done through by SRR and BAR. Whereas SRR will find a shortest and reliable path and it avoids the low trusted nodes. BAR will find the most reliable one.

A. DATA TRANSMISSION PHASE

The source node sends messages to the destination node through a route with the intermediate nodes. For transferred data packets source node computes the signature with hash message and sends the packet to the first node in the route. TP ensures that source node has sent messages. Each intermediate node verifies source node signature and stores signatures with hash message for composing the report. The destination node generates a hash messages to acknowledge the received message and the destination node sends ACK packet to each intermediate node. Each intermediate node verifies the hash messages for composing the report. Each node in the route composes a report and submits it when it has a connection to TP to claim the payment and update its trust values.

B. TRUST ESTIMATION PHASE

Trust Party receives a report, it first checks if the report has been processed before using its unique identifier. Then, it verifies the authority of the report by computing the node signatures with hash message. If the report is valid, trust party verifies the destination node’s hash message. TP clears the report by rewarding the intermediate nodes and debiting the source and destination nodes. The number of sent message is signed by the source node and the number of delivered messages can be computed from the number of hashing operations done. The trust values are calculated from each node based on node’s trustworthiness and reliability in relaying packets. The proposed system relies on the multidimensional trust values instead of single trust value to precisely predict the node’s future behavior. Trust values are used to decide which nodes to select or avoid in routing. The trust values are calculated from the following formula:

T (1) = (No of packets that are forwarded in last t sessions) / (Total no of incoming packets in last t sessions) //depicts the probability that node will relay a packet successfully

T (2) =1-((No of sessions broken by node in the last t sessions)/t)) // depicts the probability that node will not break a route

T (3) = No of session that node at least f packets/t //depicts the node’s ability to keep a route connected for a minimum number of packets

T (4) = No of session node participated in the period t/m //total number of sessions node participated in the last period

T xyz (i) = Tx (i) x Ty (i) x Tz (i) //the probability that a packet will reach the destination node through the intermediate nodes

Txyz (i) = Trust value denotes the Route reliability
x, y, z=Intermediate node
i = 1,2,3,4(dimensions)

TABLE I. Numerical Examples for Route Reliability

Case	$\tau^{(i)}_{w}$	$\tau^{(i)}_{x}$	$\tau^{(i)}_{y}$	$\tau^{(i)}_{z}$	$\tau^{(i)}_{wxyz}$
1	**0.7**	**0.7**	**0.7**	**0.7**	**0.2401**
2	**0.7**	**0.3**	**0.7**	**0.7**	**0.1029**
3	**0.7**	**0.7**	**0.7**	**-----**	**0.343**
4	**0.3**	**0.3**	**0.3**	**0.3**	**0.0081**
5	**0.7**	**0.3**	**0.7**	**-----**	**0.147**
6	**0.7**	**0.7**	**0.7**	**-----**	**0.343**

C. ROUTE ESTABLISHMENT PHASE

1) SRR Protocol

SRR protocol establishes the shortest route that can satisfies the source nodes requirements is trusted enough to act as a relay. This protocol avoids the low-trusted nodes. In this protocol the source node embeds its requirements in the RREQ packet, and the nodes that can satisfy these requirements broadcast the RREQ packet, the source node broadcasts RREQ packet .The RREQ packet contains the identities of the source and destination nodes, the maximum number of intermediate nodes, trust and energy requirements and the source node's signature and certificate then the source node is trust requirements are verified at each intermediate node can have low trust values, then verified at each subsequent intermediate nodes till it reaches at the highly trusted nodes. Each intermediate node ensures that it can satisfy the source node's trust/energy requirements. It also verifies the packet's signature using the public keys extracted from the node's certificates. These verifications are necessary to ensure that the packet is sent and relayed by genuine nodes and the nodes can satisfy the trust requirements because their trust values are signed by TP.

The intermediate node signs the packet's signature forming a chain of signatures of the nodes that broadcast the packet. This signature authenticates the intermediate node and proves that the node is the certificate holder and thus the attached trust values belong to the node. The signature also enables the trust system to make sure that the intermediate nodes have indeed participated in the route to hold them responsible for breaking the route. Finally, the intermediate node broadcasts the packet after adding the signature chain and its identity and certificate. If a node receives the same request packet from different nodes, it processes only the first packet and discards the subsequent packets. The destination node composes the RREP packet for the route traversed by the first received RREQ packet, and sends it to the source node. This route is the shortest one that can satisfy the source node's requirements. The source node's requirements cannot be achieved if it does not receive the RREP packet within a time period. It can initiate a second RREQ packet but with more flexible requirements. The source node verifies the hash message and the node's certificates to make sure that the nodes satisfy its trust requirements and the future destination node was reached, then it starts data transmission.

2) BAR Routing Protocol

The BAR routing protocol enables, the destination node to select the best reliable route in the network. The source node sends RREQ packet to the intermediate nodes, an intermediate node broadcasts the RREQ packet after attaching its identity and certificate, the number of messages it commits to relay. The intermediate nodes are motivated to report correct energy commitments to avoid breaking the route and thus degrading their trust values. The RREQ packet flooding generates few routes, because each node broadcasts the packet once, it cannot find the better routes. So the BAR protocol allows each node to broadcast the RREQ more than once if the route reliability or lifetime of the recently received packet is greater than the last broadcasted packet.
Destination selects the route with high reliability that is calculated by the formula given below. So it considered the route path with high reliability for broadcasting the packet. The route reliability calculated for the first trust value is simplicity, but the other trust values can also be considered using weighting factors. The source node can attach the weighting vector (w1, w2, w3, w4) to the RREQ packet. The Destination node calculates the total route reliability as follows:

Total route reliability = [((w1 x T (1)) + (w2 x T (2)) + (w3 x T (3)) + (w4 x T (4))]
Where w1+ w2+ w3+ w4 = 1

The destination node receives the first RREQ packet and waits for a while to receive more RREQ packets if there are. Then, it selects the best available route if a set of feasible routes are found. If there are multiple routes with lifetimes, atleast to send messages, the destination node selects the most reliable route, otherwise, it establishes multiple routes to send messages such a way that reduces the routes and maximizes the reliability. Then the destination node composes the RREP packet sends that packets to the route.

```
//Establish stable route based on trust value
 Initialize N number of nodes in the network i=1,….N
 S broadcast RREQ packet to all the nodes
 TP compute the trust value of each node in the network
 If (nodes that relay messages more successfully)
 Highest trust value
 Else
 Lowest trust value
 End if
 Select the highest trust nodes
 Based on the highest trust value select the route and update the trust values
 S select the stable route
 D composes RREP packet for the first received RREQ packet and reply to S
```

IV. CONCLUSION AND FUTURE WORK

The proposed E-STAR uses payment and trust systems with trust-based and energy-aware routing protocol to establish stable and reliable routes in wireless networks. E-STAR stimulates the nodes not only to relay others' packets but also to maintain the route stability. It also punishes the nodes that report incorrect energy capability by decreasing their chance to be selected by the routing protocol. The proposed SRR and BAR routing protocols is evaluated them in terms of overhead and route stability. These protocols can make informed routing decisions by considering multiple factors, including the route length, the route reliability based on the node's past behavior, and the route lifetime based on the node's energy capability. Performance evaluation is done based on the results of the simulation done using ns2. From the results it is proved that the route reliability and packet delivery ratio has been improved using this protocol. The security of packet is decreased with untrusted nodes. In future work provide security for each packet, so that the intruders can't able to get or damage the packets.

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] Sevil Sen, and John A. Clark, "A grammatical evolution approach to intrusion detection on mobile ad hoc networks", Proceedings of the second ACM conference on Wireless network security (WiSec '09).

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

[4] Johnson, D. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks", In C. Perkins, editor, Ad Hoc Networking, chapter 5, pp. 139-172. Addison-Wesley, 2001.

[5] 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.

[6] M. Mahmoud and X. Shen, "An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in Multihop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 60, no. 8, pp. 3947-3962, Oct. 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] 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.

[10] Kartik Kumar Srivastava et al ,"Secure Data Transmission in MANET Routing Protocol",Int.J.Computer Technology & Applications,Vol 3 (6), 1915-1921

[11] Mohamed M.E.A. Mahmoud, Xiaodong Lin, Senior Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE "Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks", IEEE transactions on parallel and distributed systems", vol. 26, no. 4, april 2015.