ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 9, March 2016

Stable and Reliable Energy Aware and Trust Based Secure Routing Protocol for Heterogeneous Multihop Wireless Networks

Veerangan.V[1]
PG Scholar
Dept. Of CSE
Veltech University
nrajkumar@veltechuniv.edu.in[1]

SaranRaj.S[2]
Assistant Professor
Dept. Of CSE
Veltech University
saranraj@veltechuniv.edu.in[2]

Rajkumar.N[3]
Assistant Professor
Dept. Of CSE
Veltech University
nrajkumar@veltechuniv.edu.in[3]

***Abstract*— In multihop wireless networks, when a mobile node wants to communicate with a destination, it relies on the other nodes to forward the packets. This multihop packet transmission can extend the network coverage area using limited power and improve area distance efficiency. In the proposed multihop wireless network E-STAR integrates the payment and trust systems with the routing protocol with the goal of enhancing route reliability and stability. The payment system describes to charge the nodes that send packets and reward those forwarding packets. The trust system is important to evaluate the nodes' trustworthiness and reliability in forwarding packets in terms of multi-dimensional trust values and the trust values are calculated for each node and developed two routing protocol is used to send the packets through highly trusted nodes having sufficient energy to minimize the possibility of breaking the route. To strengthen the trust evaluation, recommendation from each node is included in trust calculation by TP (Trusted Party). This protocol is implemented over the MANET network and simulated using Java. Performance evaluated from the parameters such as packet delivery ratio, call acceptance ratio and route lifetime.**

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

I. INTRODUCTION

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. Drawbacks in the existing routing protocols such as DSR [6] assume that the network nodes are willing to relay other nodes' packets. This assumption is reasonable in disaster recovery because the nodes pursue a common goal and belong to one authority, but it may not hold for civilian applications where the nodes aim to maximize their benefits, since their cooperation consumes their valuable resources such as bandwidth, energy, and computing power without any benefits. In civilian applications, selfish nodes will not be voluntarily interested in cooperation without sufficient incentive, and make use of the cooperative nodes to relay their packets, which has negative effect on the network fairness and performance. Fairness issue arises when a selfish node takes advantage from the cooperative nodes without contributing to them, and the cooperative nodes are unfairly overloaded. The selfish behavior degrades the network performance significantly resulting in failure of the multi-hop communication. In addition, some nodes may break routes because they do not have sufficient energy to relay the source nodes' packets and keep the routes connected. Because of this uncertainty in the nodes' behavior, randomly selecting the intermediate nodes will degrade the routes' stability.

This proposed system overcomes these drawbacks by the following techniques, trust and payment system [3]. The payment system uses credits to charge the nodes that send packets and reward those relaying packets [7]. The trust system is essential to assess the nodes' trustworthiness and reliability in relaying packets. A node's trust value is defined

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 9, March 2016

as the degree of belief about the node's behavior. The trust values are calculated from the nodes' past behaviors and used to predict their future behavior.

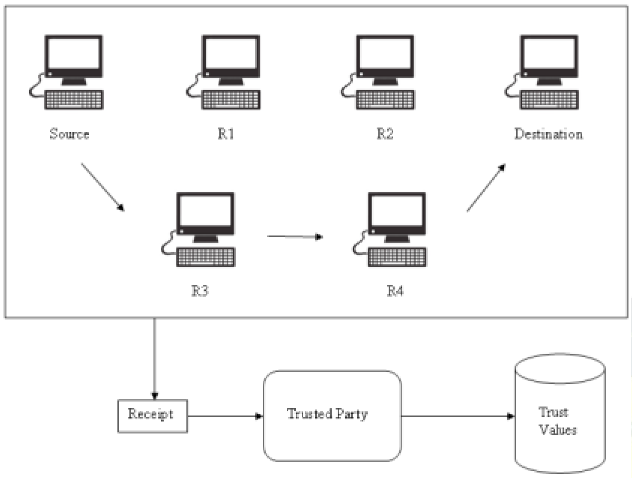

Fig: 1: Data is transferred Via Highly Trusted Nodes (R1, R2 – Low Trusted Nodes), (R3, R4 - Highly Trusted Nodes)

The Fig.1 shows the Data is transferred Via Highly Trusted Nodes. In network architecture from source to destination the data is transferred through the intermediate nodes (i.e) routes. The route R1, R2 are the low trusted nodes and R3, R4 are the highly trusted nodes. For each node it maintains a receipt and it submit to the trusted party. The trusted party will calculate the trust values. After calculating the trust value it will produce a payment receipt for highly trusted nodes.

II. LITERATURE REVIEW

ESIP For Multihop Wireless Networks

In multi-hop wireless networks [5], selfish nodes do not relay other nodes' packets and make use of the cooperative nodes to relay their packets, which has negative impact on the network fairness and performance. Incentive protocols use credits to stimulate the selfish nodes' cooperation, but the existing protocols usually rely on the heavy-weight public-key operations to secure the payment [4]. The proposed technique involved in the secure cooperation incentive protocol that uses the publickey operations only for the first packet in a series and uses the light-weight hashing operations in the next packets, so that the overhead of the packet series converges to that of the hashing operations. Hash chains and keyed hash values are used to achieve payment non repudiation and prevent free riding attacks.

Reliable Routing Against Selective Packet Drop Attack in DSR Based Manet

A mobile ad hoc network (MANET) is a self organizing and self-configuring wireless system [9]. Mobile nodes communicate using wireless interfaces without a fixed network infrastructure. In these environments each node may act as source or as a router. Nodes that cannot communicate directly depend on their neighbors in order to forward their messages to the appropriate destination. The dynamic topologies, mobile communications structure, decentralized control, and secrecy creates many challenges to the security of systems and network infrastructure in a MANET environment. Consequently, this extreme form of dynamic and distributed model requires a revaluation of conventional approaches to security enforcements. This system proposes a new routing mechanism to conflict the common selective packet dropping. A selective packet drop is a kind of denial of service where a malicious node attracts packets and drops them selectively without forwarding them to the destination.

Trust Model For Secure And QoS Routing In MANET

MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration and limited battery-based energy of mobile nodes. Most ad hoc network routing protocols [8] becomes inefficient and shows dropped performance while dealing with large number of misbehaving nodes. Such misbehaving nodes [1] support the flow of route discovery traffic but interrupt the data flow, causing the routing protocol to restart the route-discovery process or to select an alternative route if one is available. The newly selected routes may still include some of misbehaving nodes, and hence the new route will also fail. This process will continue until the source concludes that data cannot be further transferred. The routing control messages are secured by using both public and shared keys [2], which can be generated on-demand and maintained dynamically.

Trust Management in Mobile Ad Hoc Networks Maturity - Based Mode

In mobile ad hoc network trust management based on the concept of human trust and applies this model to ad hoc networks [10]. This model builds for a trust relationship to all neighbors for each node. The trust is based on previous

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 9, March 2016

individual experiences of the node and on the recommendations of its neighbors. The recommendations improve the trust evaluation process for nodes that do not succeed in observing their neighbors due to resource constraints or link breakage. The Recommendation Exchange Protocol (REP) which allows nodes to exchange recommendations about their neighbors. The proposal does not require disseminate the trust information over the entire network. Instead, nodes only need to keep and exchange trust information about nodes within the radio range without the need for a global trust knowledge.

Routing Misbehavior in Mobile Ad Hoc Networks

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 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.

III. PROPOSED WORK

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 limitedtime 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.

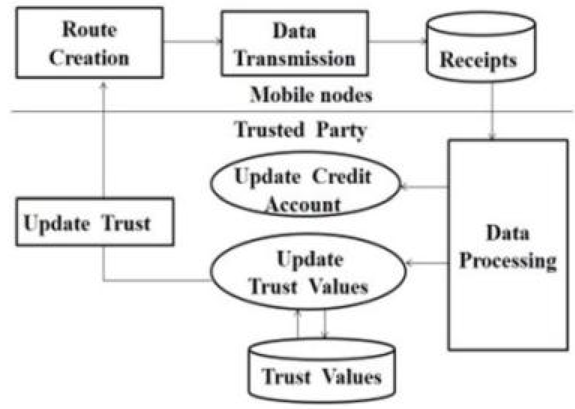

Figure 2: E-STAR in Multihop Wireless Network

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.

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.

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

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 9, March 2016

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)

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

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 9, March 2016

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.

IV. Result

We implement a heterogeneous multihop wireless network by randomly deploying m nodes in an area. n is the number of nodes having low and medium trust values. The number of nodes having high trust values is m - n and their trust values are uniformly distributed in [0.8, 1). A node with a trust value of 0.6 breaks routes with the probability of 1 - 0.6 = 0.4. By this way, the trust values can be used to simulate the variety in the nodes' lack of resources and malicious actions. Performance is analyzed using the following metrics.

Performance Metrics

A. Packet Delivery Ratio (PDR)

The Packet Delivery Ratio (PDR) is the total number of packets received by the destination nodes to the total number of packets sent by the source nodes.

B. Call Acceptance Ratio

The call acceptance ratio is the ratio of times a route is established after sending a RREQ packet.

C. Route Lifetime

The route lifetime is the number of packets sent in one route before it is broken.

Performance of the proposed protocol establishes more stable routes by selecting reliable intermediate nodes and therefore it delivers packets more successfully compared with DSR in terms of total number of packets generated, received, forwarded and packet delivery ratio, call acceptance ratio, route lifetime.

The Route Lifetime of SRR is same as the Route Lifetime of BAR. Both of the Route Lifetime is increased with increases in time. The hop length of BAR protocol is higher than that of SRR protocol. Because BAR protocol only considers the highly trusted nodes where as the SRR protocol gives important to both of the highly trusted nodes and minimum hop distance.

V. Conclusion

The proposed protocol uses payment and trust systems with trust-based and energy-aware routing protocol to establish stable and reliable routes in wireless networks. Our proposed work 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 nodes' past behavior, and the route lifetime based on the nodes' energy capability. Performance evaluation is done based on the results of the simulation done. From the results it is proved that the route reliability and packet delivery ratio has been improved using this protocol.

References

[1] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in Proc. IEEE/AC, pp. 255–265, August 6-11, 2000.

[2] M. Mahmoud and X. Shen, "ESIP: Secure incentive protocol with limited use Of public-key cryptography for multi-hop wireless networks", IEEE Transactions On Mobile Computing, vol. 10, no. 7, pp. 997-1010, July 2011.

[3] 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 Transactions on Network and Service Management, vol. 7, no. 3, pp.172–185, September 2010.

[4] Shilpa S G , Mrs. N.R. Sunitha, B.B. Amberker, "A Trust Model for Secure and QoS Routing in MANET", International Journal of Innovative Technology & Creative Engineering (ISSN: 2045- 8711), vol.1no.5 may 2011.

[5] M. Mahmoud and X. Shen, "PIS: A practical incentive system for multi-hop wireless networks", IEEE Transactions on Vehicular Technology, vol. 59, no.8, pp. 4012-4025, 2010.

[6] N. Bhalaji and A. Shanmugam, "Reliable routing against selective packet drop attack in DSR based MANET", Journal of Software, vol. 4, no. 6, pp. 536-543, August 2009.

[7] J.Gunasekaran, M.Ezhilvendan, P.Vijayanand, S.Rajasekaran, S.Murugesan "Report Based Payment Scheme for Multihop Wireless Networks". ISSN: 2319 - 1163 vol. 2, Issue. 4, pp. 459 – 464, APR 2013.

[8] 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 Journal on Selected Areas in Communications, vol. 25, no. 1, January 2007.

[9] K. Liu, J. Deng, and K. Balakrishnan "An acknowledgement-based approach for the detection of routing misbehavior in MANETs", IEEE Transaction on Mobile Computing, vol. 6, no. 5, pp 536–550, May 2007.

[10] S. Lindsay, Y. Wei, H. Zhu and K. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 305–317, 2006.