Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 5, May -2016

A TRUST SYSTEM FOR ESTABLISHING STABLE AND RELIABLE ROUTES IN HETEROGENEOUS MULTIHOP WIRELESS NETWORKS

SECURE INTER HOP VERIFICATION WITH ONION PROTOCOL FOR RELIABLE ROUTING IN WIRELESS SENSOR NETWORKS

P.JAYASHRI[1], D.DURAI KUMAR[2]

[1,2] *M.Tech-INFORMATION TECHNOLOGY, GANADIPATHI TULSI'S JAIN ENGINEERING COLLEGE*

Abstract — *Stable and reliable route establishment in heterogeneous multihop wireless networks is a challenging task. Nodes are typically autonomous, self interested and may belong to different authorities. Malfunctioned nodes frequently drop packets and break routes due to faulty hardware or software and malicious nodes actually break routes to disrupt data transmission. Because of this uncertainty in the nodes behavior, randomly selecting the intermediate nodes will degrade the routes stability and also endanger the reliability of data transfer. This project presents the trust management scheme that uses two kinds of trust called E-Star and predictability trust. For the secure transmission I used onion protocol. The trust system evaluates the nodes competence and reliability in relaying packets in terms of multi dimensional trust values using payment system rewards. The trust values are attached to nodes public key certificate to make routing decisions. Trust system aims to improve the collaboration between the nodes in wireless networks by predicting the future behavior based on the previous behavior. The trust system typically does this by observing and storing the neighbor's behavior. Based on the trust values each node with which to collaborate and can improve the packet delivery ratio and stability. TA implementation is also achieved for successful validation of concatenated keys there by reward is provided to the intermediate hops.*

Keywords *- Trust Management Scheme, E-STAR, Predictability Trust, Onion Protocol, Payment System, Packet Delivery Ratio.*

I. INTRODUCTION

In multi hop wireless networks, when a source node wants to communicate with a destination node, it has to take help from the intermediary nodes to transfer the packet from source to destination. This multi hop packet transmission takes network coverage and it will improve the performance and efficiency. Now a day at low cost network can be deployed. We consider the civilian applications of multi hop wireless Networks, where the nodes have long relation with the network. We also consider heterogeneous multi hop wireless networks (HMWNs), where the nodes' mobility level and hardware/energy resources may vary greatly. HMWNs can implement many useful applications such as data sharing and multimedia data transmission. In military and disaster-recovery applications, the nodes' behavior is highly predictable because the network is closed and the nodes are controlled by one authority. However, the nodes' behavior is unpredictable in civilian applications for different reasons. The nodes are typically autonomous and self-interested and may belong to different authorities. The nodes also have different hardware and energy capabilities and may pursue different goals. In addition, malfunctioned nodes frequently drop packets and break routes due to faulty hardware or software, and malicious nodes actively break routes to disrupt data transmission. Since the mobile nodes are battery driven and one of the major sources of energy consumption is radio transmission, selfish nodes are unwilling to lose their battery energy in relaying other users' packets.

Only one intermediate node can break a route, and a small number of incompetent or malicious nodes can repeatedly break routes. When a route is broken, the nodes have to rely on cycles of time-out and route discoveries to re-establish the route. These route discoveries may incur network-wide flooding of routing requests that consume a substantial amount of the network's resources. Breaking the routes increases the packet delivery latency and may cause network partitioning and the multi-hop communication to fail. Hence, in order to establish stable routes and maintain continuous traffic flow, it is essential to assess the nodes' competence and reliability in relaying packets to make informed routing decisions. In this paper, I used E-STAR; a secure protocol for Establishing Stable and Reliable routes in HMWNs.

II. RELATED WORKS

2.1 Trust System

E-STAR integrates trust and payment systems with a trust-based and energy-aware routing protocol. The payment system uses credits (or micropayment) to charge the nodes that send packets and reward those relaying packets. Since a Trusted Authority (TA) may not be involved in the communication sessions, an offline trusted party is required to

manage the nodes' credit accounts. The nodes compose proofs of relaying packets, called receipts, and submit them to TA. The payment system can stimulate the selfish nodes to relay others' packets to earn credits. It can also enforce fairness by rewarding the nodes that relay more packets such as those at the network center. However, the payment system is not sufficient to ensure route stability.

2.2 Energy-aware routing

The trust-based and energy-aware routing protocols, called the shortest reliable route (SRR) and the best available route (BAR). My goal is to establish stable routes to reduce the probability of breaking them due to the following reasons,

- Lack of energy: an intermediate node may not have sufficient energy to relay the source node's packets and keep the route connected; and

- Node behavior: the nodes may break routes due to malicious action, malfunction, low hardware resources, etc.

SRR protocol establishes the shortest route that can satisfy the source node's requirements including energy, trust, and route length. For BAR protocol, the destination node may learn multiple routes and establishes the most reliable one.

2.3 E-STAR

Result demonstrates that E-STAR can secure the payment and trust calculation without false accusations. The used routing protocols can improve the packet delivery ratio due to establishing stable routes.

The main benefits of integrating the payment and trust systems with the routing protocol can be summarized as follows. First, it fosters trust among the nodes by making knowledge about the nodes' past behavior available. Relaying packets by unknown nodes entails a certain element of risk, so a source node needs to trust the nodes that relay its packets. Second, this integration can deliver messages through reliable routes and allow the source nodes to prescribe their required level of trust. Third, it can punish the nodes that break routes by giving more preference to the highly-trusted nodes in route selection, and thus in earning credits. Fourth, the integration of the payment and trust systems with the routing protocol can punish the nodes that report incorrect energy capability. This is because the routes will be broken at these nodes and their trust values will degrade.

Finally, a node may use a greedy strategy: never earn too much unneeded credits and stop relaying others' packets after earning sufficient credits. The integration of the payment and trust systems not only stimulates the nodes to cooperate in relaying packets to earn credits, but also stimulates the wealthy nodes to cooperate to maintain good trust values. This is because the nodes lose trust over time if they do not cooperate. By this way, in addition to payment, trust is another incentive for cooperation.

E-STAR aims to establish stable and reliable routes. 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.

2.4 Dynamic Source Routing (DSR)-Based Routing.

Dynamic source routing (DSR)-based routing [DSR] involves two main processes: route discovery and route maintenance. To execute the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the network. If an intermediate node has routing information to the destination in its route cache, it will reply with a RREP to the source node. When the RREQ is forwarded to anode, the node adds its address information into the route record in the RREQ packet. When destination receives the RREQ, it can know each intermediary node's address among the route. The destination node relies on the collected routing information among the packets in order to send a reply RREP message to the source node along with the whole routing information of the established route.

DSR does not have any detection mechanism, but the source node can get all route information concerning the nodes on the route. In our approach, we make use of this feature. In this paper, a mechanism [so-called cooperative bait detection scheme (CBDS)] is presented that effectively detects the malicious nodes that attempt to launch gray hole/ collaborative black hole attacks. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a black hole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defense architectures to achieve the aforementioned goal.

III. SYSTEM MODEL

Source will find out the optimum path and it will collect primary key of all intermediate node. Data first encrypted using AES algorithm and then with corresponding primary key of all the hops.

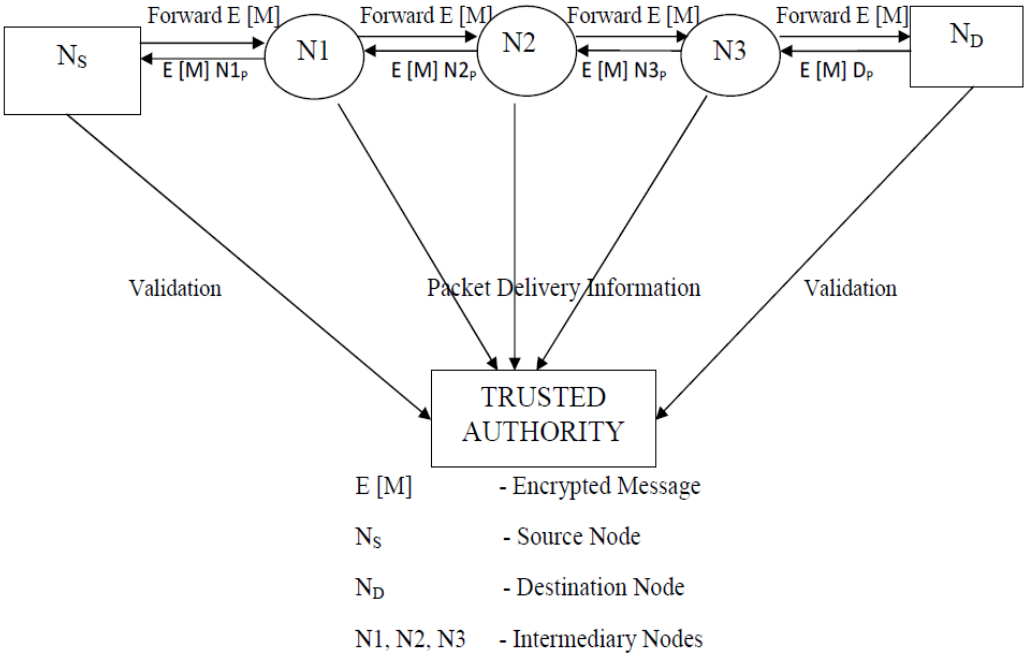

Figure 1. Overall Diagram

This wholesome is transmitted to first hop, where initial decryption is achieved using decryption key of that node. Its id and secondary key are collected which is transmitted to both source and destination node. Same way all the ID's and secondary key are collected and concatenated, so as to verify both source and destination. TA implementation is also achieved for successful validation of concatenated keys their by reward is provided to the intermediate hops.

IV. THE PROPOSED SYSTEM

In this proposed system the source node selects the routing path based on request response. Then it transmits the data to destination. In the modification process I used onion protocol. Every node while registering, server will provided with Id, primary key, secondary key and decryption key. Source will find out the optimum path based on previous history verification and it will collect primary key of all intermediate node.

Data first encrypted using AES algorithm and then with corresponding primary key of all the hops. This wholesome is transmitted to first hop, where initial decryption is achieved using decryption key of that node. Its id and secondary key are collected which is transmitted to both source and destination node. Same way all the ids' and secondary key are collected and concatenated, so as to verify both source and destination. TA implementation is also achieved for successful validation of concatenated keys their by reward is provided to the intermediate hops. The advantage over this proposed system considers both misbehavior detection and incentives namely payment scheme.

V. IMPLEMENTATION

5.1 NODE CONSTRUCTION PHASE

The heterogeneous multihop wireless networks consist of Trusted Authority (TA) and n-number of nodes; they are represented in the form of table. Each node before entering the network must register itself to the Trusted Authority. The Trusted Authority (TA) [3] maintains reputation score for all the nodes in the network. The probability of reputation can be varied based on the score. The node with low reputation (1) is checked with higher probability and the node with high reputation (0) is checked with low probability.

Each node has unique ID, primary key, secondary key, decryption key which are randomly generated, the coverage area of each node is considered as finite. Hence before the node creation each and every node is assigned with a coverage area by giving the starting and ending range.

Each node maintains forward history and contact history [3]. Since the node is mobile each node has dynamically changing memory, battery and mobility. When a node comes within the transmission range of other node then they both come into contact and the evidence of contact is registered in the contact history using E-STAR.

5.2 ROUTE REQUEST AND SELECTION PHASE

The trust-based and energy-aware routing protocols are Shortest Reliable Route (SRR) and the Best Available Route (BAR). 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[1][2].SRR protocol establishes the shortest route that can satisfy the source node's requirements including energy, trust, and route length. It is useful in establishing routes that avoid the low-trust nodes, e.g., malicious nodes, with low overhead.

The rationale of the SRR protocol is that the node that satisfies the source node's requirements is trusted enough to act as a relay. For BAR protocol, the destination node may learn multiple routes and establishes the most reliable one. It is not dependent on the available battery energy of nodes, but also on other factors such as the cooperation strategy (or the node's willingness for relaying packets) and the link quality and stability.

5.2.1 E-STAR protocol

E-STAR has three main phases.

- Data Transmission phase
- Update Credit-Account and Trust Values phase
- Route Establishment phase

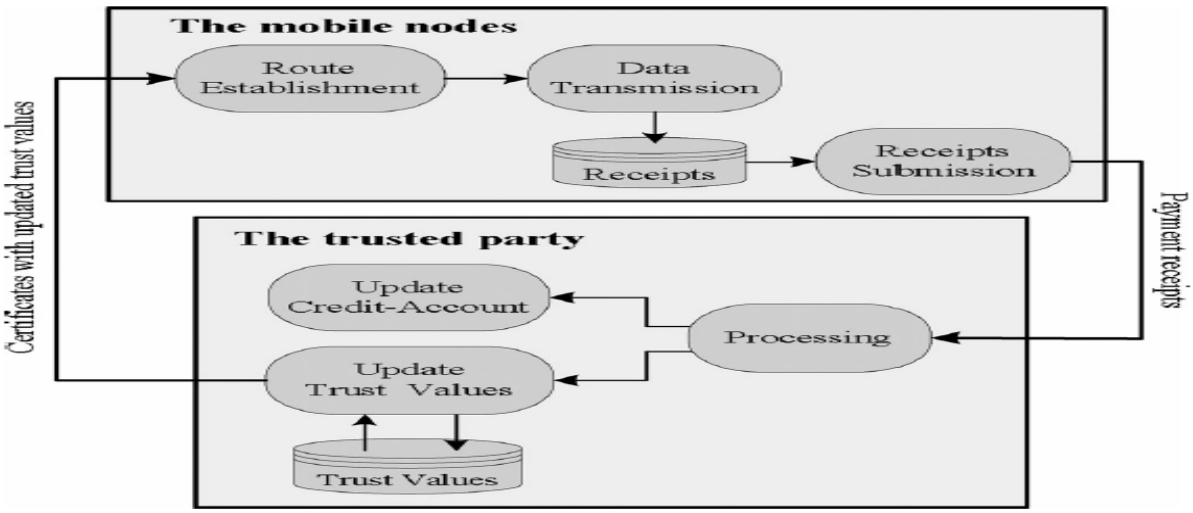

Figure 2. E-STAR Architechture

In Data Transmission phase, the source node sends messages to the destination node. In Update Credit-Account and Trust Values phases, TP determines the charges and rewards of the nodes and updates the nodes' trust values. Finally, in Route Establishment phase, trust-based and energy-aware routing protocol establishes stable communication routes.

5.3 PACKET FORWARDING

Here the packet is forwarded using onion protocol [5]. Every node while registering, server will provided with Id, primary key, secondary key and decryption key. Source will find out the optimum path and it will collect primary key of all intermediate node. Data's first encrypted using AES algorithm [6] and then with corresponding primary key of all the hops. This wholesome is transmitted to first hop, where initial decryption is achieved using decryption key of that node. Its id and secondary key are collected and then transmitted to both source and destination node. Same way all the ids and secondary key are collected and concatenated, so as to verify both source and destination.

5.4 INTEGRITY CHECK

The Trusted Authority (TA) may not be involved in the communication sessions; an offline trusted party is required to manage the nodes' credit accounts. Each node has a unique identity (ID), primary key, secondary key, decryption key with a limited-time certificate issued by TA. Without a valid certificate, the node cannot communicate nor act as an intermediate node. TA maintains the nodes' credit accounts and trust values. Each node contacts TA to submit the payment receipts and TA updates the involved nodes' payment accounts and trust values.

VI. SECURITY ANALYSES

Every node while registering, server will provided with Id, primary key, secondary key and decryption key. Source will find out the optimum path based on previous history verification and it will collect primary key of all intermediate node.

Data first encrypted using AES algorithm and then with corresponding primary key of all the hops. This wholesome is transmitted to first hop, where initial decryption is achieved using decryption key of that node. Its id and secondary key are collected which is transmitted to both source and destination node. Same way all the ids' and secondary key are collected and concatenated, so as to verify both source and destination. TA implementation is also achieved for successful validation of concatenated keys their by reward is provided to the intermediate hops. The advantage over this proposed system considers both misbehavior detection and incentives namely payment scheme.

VII. CONCLUSION

Finally using E-STAR, trust-based and energy-aware routing protocol to establish stable/reliable routes in HMWNs. 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. 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. It is useful in establishing routes that avoid the low-trust nodes, e.g., malicious nodes, with low overhead. The analytical results have demonstrated that E-STAR can secure the payment and trust calculation without false accusations. Moreover, the results have demonstrated that E-STAR can improve the packet delivery ratio due to establishing stable routes.

REFERENCES

[1] A. Boukerche, "Performance evaluation of on-demand routing Protocols," ACM/Kluwer Mobile Networks and Applications, 2004.
[2] J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with untraceable routes for mobile ad-hoc networks," InACM MOBIHOC'03, 2003.
[3] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, April 2012
[4] R. Lu, X. Lin, H. Zhu and X. Shen, "Pi: A practical incentive protocol for delay tolerant networks," in IEEE Transactions on Wireless Communications, vol.9, no.4, pp.1483-1493, 2010.
[5] S.Arun Karthick and K.Sudhakar, "Secure neighbor discovery system for ad-hoc through aasr protocol," IRACST -International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 4, No.6, and December 2014
[6] Y. Zhang, W. Liu, W.Lou, and Y. G. Fang, "MASK: Anonymous On "Demand Routing in Mobile Ad hoc Networks," IEEE Trans. on Wireless Comms., vol. 5, no. 9, pp. 2376–2386,Sept.2006

