IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Secure, Reliable and Load Balanced Routing Protocols for Multihop Wireless Networks

Mitali V. Patil[1], Prof. Vaishali Jadhav[2]

Student, Computer Engineering, SCOE, Navi Mumbai, India[1]

Prof. IT Department, SCOE, Navi Mumbai, India[2]

Abstract: In multihop wireless networks, route stability is very challenging task and major research problem. The routes in this network are frequently breaks presence of malicious nodes, faulty nodes, or due to lack of energy of intermediate nodes. Hence there should be the hybrid approach in which route stability should be achieved by considering all the causes of frequent routes failure. In this paper, the novel secure and load balanced E-STAR (LBE-STAR) for HMWNs. LBE-STAR E-STAR trust method and payment systems with a trust-based and energy-aware routing protocol along with load balancing algorithm. LBE-STAR is based on existing E-STAR routing protocol with contribution of efficient load balancing functionality. The payment system based on rewards and changes in which nodes that relay others' packets are rewarded and charge those that send packets. The trust system evaluates the nodes' reliability and competence in relaying packets in terms of multi-dimensional trust values. The load balancing is achieved by using disjoint path communication approach. In this paper, two variants of LBE-STAR algorithm proposed such as LB-SRR (shortest reliable route) and LB-BAR (Best Available Route). Overall objective of designing the LBE-STAR routing protocol is to achieve the security, reliability and load balancing in multihop wireless networks.

Keywords: Securing heterogeneous multihop wireless networks, packet dropping and selfishness attacks, trust systems, load balanced 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. 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.

In this paper, we are considering heterogeneous multihop 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. The applications like military and disaster-recovery, 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.

Multihop wireless network are frequently used in many real life applications. The communication in such networks is based on routing protocols in which the communication between two remote nodes is done by other intermediate nodes. Therefore this creates the chances security threats during the packet transmission from one node to another. All nodes in network are battery constraint hence the routes may break if the battery of any node expires. Similarly the malicious node also frequently breaks the current routes. Due to the uncertainty of nodes behaviour, random selection of intermediate nodes will resulted into routes stability degradation. It will also endanger the reliability of data transmission and degrade the network performance in terms of packet delivery ratio (PDR). 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. To solve the problem of stable route establishment in multihop wireless networks, recently E-STAR (Establishing STAble and

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

reliable Routes) routing protocol is proposed for HMWNs (Heterogeneous Multihop Wireless Networks). The simulation performance of this protocol shows the efficiency in terms of reliability, security and stable routes. The problem associated with E-STAR is that it did not address the load balancing scenarios. This is motivation for this research work. The following sections of the paper are organized as follows: Section II will describe related works in the field of Multihop wireless networks. Section III and IV will outline the approach taken by the proposed system. The framework will be evaluated in Section V. Finally, Section VI will describe concluding thoughts and ideas for future work in this area.

II. LITERATURE SURVEY

The task of email spam filtering is nothing but automatically removing unwanted, harmful, or offensive email messages before they are delivered to a user — is an important, large scale application area for machine-learning methods. In this chapter investigates several categories of the recent related methods on spam filtering.
This study is used to show how the different spam filtering techniques are used to combat spam. We studied these ten papers which have used different techniques for spam filtering, which are described as follows:
In[1] author proposes ESTAR with alert-anonymous location based efficient routing protocol in which protocols can make informed routing decisions by considering multiple factors, including the route length, reliability based on the nodes' past behavior, and its lifetime based on the nodes' energy capability.
In[2] author presented ESTAR with MAPCP-MANET Anonymous Peer-to-peer Communication Protocol in whichP2P applications over MANET was proposed. MAPCP also maintains high packet delivery fraction even under selective attacks. But Security is not provided for each packet, as the intruders can able to get or damage the packets. In[3], author proposes ESTAR with fuzzy rule based engine. In this method, If new nodes are inserted or deleted in network then this network does not disturbed.

In [4], author presented another reputation based method in order to eliminate using the channel overhearing technique based on two-hop ACK technique. NA accuses its neighbor NB of dropping a packet, if NA does not receive an ACK packet from the two hop-away nodes NC. Reputation-based schemes 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 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. However, this increases the 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.
In [5], author proposed the payment based security system for wireless networks. In this paper, author introduced Sprite, a simple, cheat-proof, credit- based system for stimulating cooperation among selfish nodes in mobile ad hoc networks. This approach provides incentive for mobile nodes to cooperate and report actions honestly. Compared with previous approaches, this system does not require any tamper- proof hardware at any node. Furthermore, author proposed a formal model of our system and proves its properties.
In [6], another payment based system proposed by author for multihop wireless networks. In this paper, first, previous methods differences are investigated, and a payment model is developed for the efficient implementation of micropayment in MWNs. Second, based on the developed payment model, an incentive system is proposed to stimulate the nodes' cooperation in MWNs. Third, a reactive receipt submission mechanism is proposed to reduce the number of submitted receipts and protect against collusion attacks. Extensive analysis and simulations demonstrate that proposed incentive system can secure the payment and reduce the overhead of storing, submitting, and processing payment receipts significantly, which can improve the system's practicality due to the high frequency of low-value payment transactions.
In ESIP [7], 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.

In [8], 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.
In [10], 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 [12], 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. There are many other methods [13]-[18] proposed for security.

III. PROPOSED SYSTEM

As shown in figure 1, the proposed routing scheme for heterogeneous multihop wireless networks.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

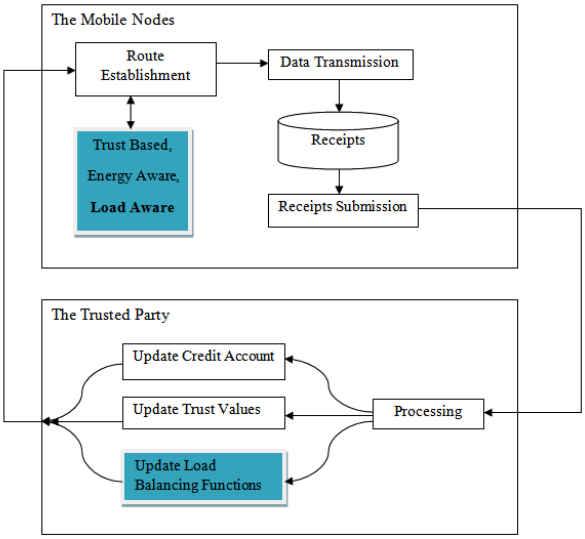

Fig 1: PROPOSED SYSTEM OF LBE-STAR

The main contributions of this paper are: 1) LBE-STAR integrates payment and trust systems with the routing protocol with the goal of enhancing route reliability and stability; 2) we propose a multi-dimensional trust system based on processing the payment receipts; 3) LBE-STAR stimulates the nodes not only to relay others' packets even if they have many credits, but also to stabilize the routes and report their energy capability truthfully to increase their chance to participate in future routes; 4) we propose trust-based and energy-aware routing protocols to establish stable routes; and 5) we proposed the load balancing algorithm to deliver the QoS (Quality of Service) performance guaranteed. Below sections are discussing the key terminologies of proposed routing methods.

3.1 Data Transmission Phase

The destination node generates a one-way hash chain by iteratively hashing a random value hSS times to obtain the hash chain {hS, hS-1,…,h1, h0}, where hi-1= H (hi) for 1 ≤ i ≤ S and h0 is called the root of the hash chain. The node signs h0 and R to authenticate the hash chain and link it to the route, and sends the signature to the source node in route establishment phase. In order to acknowledge receiving the message mi, the destination node sends ACK packet containing the preimage of the last released hash chain element or hi. Each intermediate node verifies the hash chain element by making sure that hi-1 is obtained from hashing hi, and saves hi for composing the receipt and removes hi-1. The underlying idea is that $\varepsilon_s(i)$ and hi are undeniable proofs for sending and receiving i messages, respectively. Each node in the route composes a receipt and submits it when it has a connection to TP to claim the payment and update its trust values. A receipt is a proof for participating in a route and sending, relaying, or receiving a number of messages. A receipt contains R, ts, i, (mi), h0, hi, Cm, and an undeniable cryptographic token for preventing payment manipulation. Cm is data that depends on the used routing protocol, such as the number of messages the intermediate nodes commit to relay. The cryptographic token contains the hash value of the last source node's signature and Auth_Code. Auth_Code is the authentication code that authenticates the hash chain and the intermediate nodes to hold them accountable for breaking the route. If I messages are delivered, the format of the receipt is <R, ts, i, (mi), h0, hi, Cm, H ($\varepsilon_s(i)$, Auth_Code)>, $\varepsilon_s(i)$ and Auth_Code are hashed to reduce the receipt's size.

3.2 Update Credit Account and Trust Values

Once TP receives a receipt, it first checks if the receipt has been processed before using its unique identifier (R, ts). Then, it verifies the credibility of the receipt by computing the nodes' signatures (j(i) and Auth_Code) and hashing them. The receipt is valid if the resultant hashes value is identical to the receipt's cryptographic token. Below equations are used for trust values during the routing phase. The destination node generates a one-way hash chain by iteratively hashing a random value hSS times to obtain the hash chain {hS, hS-1,…,h1, h0}, where hi-1= H (hi) for 1 ≤ i ≤ S and h0 is called the root of the hash chain. The node signs h0 and R to authenticate the hash chain and link it to the route, and sends the signature to the source node in route establishment phase. In order to acknowledge receiving the message mi, the destination node sends ACK packet containing the preimage of the last released hash chain element or hi. Each intermediate node verifies the hash chain element by making sure that hi-1 is obtained from hashing hi, and saves hi for composing the receipt and removes hi-1. The underlying idea is that $\varepsilon_s(i)$ and hi are undeniable proofs for sending and receiving i messages, respectively.

Each node in the route composes a receipt and submits it when it has a connection to TP to claim the payment and update its trust values. A receipt is a proof for participating in a route and sending, relaying, or receiving a number of messages. A receipt contains R, ts, i, (mi), h0, hi, Cm, and an undeniable cryptographic token for preventing payment manipulation. Cm is data that depends on the used routing protocol, such as the number of messages the intermediate nodes commit to relay. The cryptographic token contains the hash value of the last source node's signature and Auth_Code. Auth_Code is the authentication code that authenticates the hash chain and the intermediate nodes to hold them accountable for breaking the route. If I messages are delivered, the format of the receipt is <R, ts, i, (mi), h0, hi, Cm, H ($\varepsilon_s(i)$, Auth_Code)>, $\varepsilon_s(i)$ and Auth_Code are hashed to reduce the receipt's size.

$$TP \rightarrow N_K: Cert_K = ID_K, t_e, t_j, K_K-, \tau_K, \{H(ID_K t_e, t_j, t_i, K_K-, \tau_K)\}K_{TP+}, \quad (3.1)$$

$$\tau_K^{(2)} = 1 - \frac{\text{NO.of sessions broker in the last } \omega \text{ sessions}}{\omega} \quad (3.2)$$

$$\tau_K^{(1)} = \frac{\text{NO.of packets that are relayed in the last } \omega \text{ sessions}}{\text{Total No.of incomin packets the last } \omega \text{ sessions}} \quad (3.3)$$

$$\tau_K^{(3)} = \frac{\text{NO.of sessions that } N_K \text{ relayed at least } \delta \text{ packets}}{\omega} \quad (3.4)$$

$$\tau_K^{(4)} = \frac{\text{NO.of swssions } N_K \text{ participated in the period t}}{M} \quad (3.5)$$

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

3.3 Route Establishment Phase

In this phase we present two routing protocols called the Load balanced shortest reliable route (LB-SRR) and the load balanced best available route (LB-BAR). LB-SRR establishes the shortest route that can satisfy the source node's trust, energy, and route-length requirements, but the destination node selects the best route in the LB-BAR protocol. The routing protocols have three processes: 1) route request packet (RREQ) delivery; 2) Route selection; and 3) route reply packet (RREP) delivery.

LB-SRR: To establish a route to the destination node ND, the source node NS broadcasts RREQ packet and waits for RREP packet. The source node embeds its requirements in the RREQ packet, and the nodes that can satisfy these requirements broadcast the packet. The destination node establishes the shortest route that can satisfy the source node's requirements. The rationale of the LB-SRR protocol is that the node that satisfies the source node's requirements is trusted enough to act as a relay. The protocol is useful to establish a route that avoids the low-trusted nodes as well as achieve the load balancing.

3.4 Load Balancing

Load balancing is a computer networking system for the dividing workloads into the multiple computing resources, such as computers, a computer cluster, network links, central processing units or the disk drives. Load balancing aims to optimize resource use, maximize throughput, minimize response time, & ignore the overload of some one of the resources. Using multiple components with load balancing instead of a one component might be enhance the reliability from the redundancy Load balancing is usually provided by dedicated software or the hardware, like as the multilayer switch or the Domain name system server process. Load balancing is a core networking solution liable for the dividing incoming traffic among servers hosting the same application content. By balancing application requests across multiple servers, a load balancing prevents any application server from becoming a single point of the failure, this are enhancing overall application existence & responsiveness. For example, when one application server becomes unavailable, the load balancing simply direct all new application requests to other available server in the pool. Load balancing also improves server utilization and maximize availability. Load balancing most straightforward methodology of the scaling out into the application server infrastructure. As application demand increase, new servers can be easily added to the resource pool, and the load balancing will immediately begin sending traffic to the new server.

IV. CONCLUSION

The work presented in this paper proposes efficient, secure and reliable routing protocol for heterogeneous multihop wireless networks with goal of improving the security against different types of vulnerabilities, energy efficiency, load balancing etc. The proposed routing protocol is based on existing E-STAR protocol. The algorithm is designed by considering the load balancing and satisfying the requirements like more trust values, more remaining energy, minimum route length and minimum load on mobile nodes. Overall objective of proposed LBE-STAR routing protocol is to establish reliable and stable routes. Proposed LBE-STAR stimulates the nodes not only to relay others' packets but also to maintain the route stability.

REFERENCES

[1] Mohamed M.E.A. Mahmoud, Xiaodong Lin, "Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 26, NO. 4, APRIL 2015.

[2] X. Li, Z. Li, M. Stojmenovic, V. Narasimhan, and A. Nayak, "Autoregressive Trust Management in Wireless Ad Hoc Networks," Ad Hoc & Sensor Wireless Networks, vol. 16, no. 1-3, pp. 229-242, 2012.

[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] K. Liu, J. Deng, and K. Balakrishnan, "An Acknowledgement-Based Approach for the Detection of Routing Misbehavior in MANETs," IEEE Trans. Mobile Computing, vol. 6, no. 5, pp. 536-550, May 2007.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] A. Jøsang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.

[14] A. Withby, A. Jøsang, and J. Indulska, "Filtering Out Unfair Ratings in Bayesian Reputation Systems," The Icfain J. Management Research, vol. 4, no. 2, pp. 48-64, 2005.

[15] P. Resnick and R. Zeckhauser, "Trust among Strangers in Internet Transactions: Empirical Analysis of Ebay's Reputation System," Proc. NBER Workshop Empirical Studies of Electronic Commerce, 2000.

[16] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," Proc. Third Int'l Symp. Information Processing Sensor Networks (IPSN), 2004.

[17] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation Systems," Comm. ACM, vol. 43, no. 12, pp. 45-48, 2000.

[18] N. Bhalaji and A. Shanmugam, "Reliable Routing against Selective Packet Drop Attack in DSR Based MANET," J. Software, vol. 4, no. 6, pp. 536-543, Aug. 2009.