Indian Journal of Emerging Electronics in Computer Communications,
Volume.3, Issue.1, 2016, Page.532-537
www.scientistlink.com/ijeecc

Hop Verification Using Neighbor Broadcasting for Inter and Intra Reliability Link Routing in Wireless Sensor Networks

Varsha Paul[1], Rekha P[2]
[1]PG Scholar, [2]Assistant Professor
[1,2]Electronics and Communication Engineering,
Saveetha Engineering College, India
[1]varshapaul20@gmail.com,[2]rekhap@saveetha.ac.in

Abstract : *In wireless sensor networks, malicious nodes can repeatedly break routes. Breaking the routes will increase the packet delivery latency. Hence we propose a protocol known as E-STAR for establishing stable and reliable routes in heterogeneous multihop wireless sensor networks. The payment and trust systems are combined in E-STAR with a trust based and energy aware routing protocol. The nodes that relay other packets are rewarded by the payment system. The nodes competence and its reliability in relaying packets are evaluated by the trust system. The trust values which are needed to make routing decisions are attached to the nodes public key certificates. SRR and BAR are two routing protocols which are developed to direct traffic to those highly trusted nodes having sufficient energy to minimize the probability of breaking the route. The nodes are stimulated by E-STAR to not only relay the packets but also to maintain route stability and maintain correct battery energy capability. Through analytical results it is proved that E-STAR can secure payment and trust calculation without false accusations. The packet delivery ratio and route stability is improved by using E-STAR protocol.*

Keywords - *AES – Advanced Encryption Standard; BAR – Best Available Route; E-STAR – Establishing Stable And Reliable Routes; HMWNs – Heterogeneous Multihop Wireless Networks; SRR – Shortest Reliable Route.*

I. Introduction:

When a mobile node in a multihop wireless network needs to communicate with a remote destination, it has to rely on other nodes to relay the packets. The network can be deployed readily and at a low cost in developing and rural areas. The energy resources and node's mobility level may vary greatly. Many useful applications such as multimedia data transmission and data sharing are implemented in HMWNs. The behavior of the nodes is highly predictable in military and disaster-recovery applications. This is because it is a closed network and the nodes are controlled by one authority. The nodes pursue different goals and have different hardware and energy capabilities. Malfunctioned nodes break routes due to faulty hardware or software and frequently drop packets. The malicious nodes disrupt data transmission by actively breaking the routes.

Mobile nodes are battery driven. The selfish nodes present in the network will not be willing to lose their battery energy to relay other packets. The network connectivity is more when more nodes are cooperative in relaying the packets. The nodes having large hardware resources perform packet relay more successfully than other nodes. A route is broken in HMWNs when an intermediate node moves out of the radio range of its neighbors in the route. Hence randomly selecting the intermediate nodes will degrade the stability of the route. The reliability of data transmission is also endangered. The nodes have to rely on cycles of time-out and route discoveries to re-establish a new route when a route is broken. The breaking of routes leads to increase in packet delivery latency and failure in multi-hop communication.

E-STAR is a secure protocol for establishing stable and reliable routes in HMWNs. Payment system and trust are integrated with a trust based and energy-aware routing protocol. Credits are used by the payment systems to charge the nodes that send the packets and reward those relaying packets. The selfish nodes are stimulated by the payment system to relay other packets, to earn credits. The payment system may not be sufficient to ensure the stability of the route.

Two trust-based and energy and energy-aware routing protocols called Best Available Route (BAR) and the Shortest Reliable Route (SRR) are developed. The SRR protocol establishes the shortest route that satisfies the source node's requirements which includes trust, energy and route length. The BAR protocol is used for establishing the best available route. E-STAR, without false accusations can secure the payment and trust calculation. Through simulation results, it is demonstrated that the routing protocols can improve the packet delivery ratio due to establishing stable routes.

II. RELATED WORK:

The malicious nodes that drop packets are identified by the reputation-based schemes to avoid them in routing with a rate more than a predefined threshold. False accusations are possible in reputation-based schemes. Some honest nodes may be identified as malicious. This occurs due to congestion as the nodes that drop packets temporarily may be falsely identified as malicious by its neighbors. Fault accusations can be reduced by using tolerant thresholds. This helps to guarantee that a node's packet dropping rate can only reach the threshold if the node is malicious. The process may not be applicable as it increases missed detections and some malicious nodes are not identified. The black-hole attackers that drop all the packets they are supposed to relay are identified by reputation-based schemes. The detection of gray-hole attackers is very low. Determining the trustworthiness of a node in heterogeneous multihop wireless network is not effective by using threshold as the nodes packet dropping rates vary greatly. The route stability or reliability cannot be guaranteed by using these schemes. The micropayment is used by payment schemes to encourage the nodes to relay other packets. There is consumption of energy and other resources due to relaying the packets. Hence packet relaying can be charged. The micropayment can be used by the nodes to get their packets delivered. The source node signs the identities of the nodes in the route and the message for each message as in Sprite [1]. The signature is verified by each intermediate node and submits a signed receipt to TP to claim the payment. As one receipt is composed for each message, the receipts overwhelm the network. A fixed size receipt per route can be generated to reduce the number of receipts. In ESIP [2], a communication protocol is used by payment scheme to transfer the messages from source node to destination with limited use of public key cryptography. The E-STAR aims to establish stable and reliable routes than ESIP that aims to transfer messages efficiently [7].

The issue of evaluating the trust level was analyzed by Theodorakopoulos and Baras [3]. The edges correspond to the opinion that a node has about another in an oriented graph. The objective is to enable the nodes to indirectly build trust relationships by using exclusively monitored information. A human- based model which builds a trust relationship between nodes in ad hoc network was proposed by Velloso et al. [4]. An information theoretic framework to quantitatively measure trust and model trust propagation in ad hoc networks was developed by Lindsay [5]. A secure routing protocol has been proposed with quality of service support in [6].

III. PROPOSED SYSTEM:

The goal is to establish stable and reliable routes in heterogeneous multihop wireless sensor networks. The nodes are assigned with node Id, public key and primary key. The source node sends a route request to the destination. Based on the route response, the source node selects the routing path. The source node encrypts the packets using AES (Advanced Encryption Standard) encryption and sends it to the neighbor node. By using E-STAR protocol the misbehavior node if any is detected. The misbehavior node is kept in sleep mode and the packets are sent to the neighboring node to transmit it to the destination. The payment is done to each node as per the energy consumed to transmit the packet.

NODE CONSTRUCTION:

The network is constructed with N number of nodes. This is done so that the nodes can request data from other nodes in the network. Since the nodes are mobile we can assume that the nodes move across the network. The network is used to store all the nodes information like node Id and other information related to the node. Each node will have a public key and a private key. The network will also monitor all the nodes communication for security purpose.

ROUTE REQUEST BASED ON ROUTING TABLE SELECTION:

In this, the source node sends hello interval request to all intermediate nodes for identifying minimum hop count and the capacity of the intermediate nodes based on node connectivity. The routing table in the RREQ (Route REQuest) packet can be used to estimate how many neighbors have not been covered by the RREQ packet from previous intermediate node. The RREQ packet is validated by each intermediate node and it updates its routing tables. Finally the RREQ reaches the destination node.

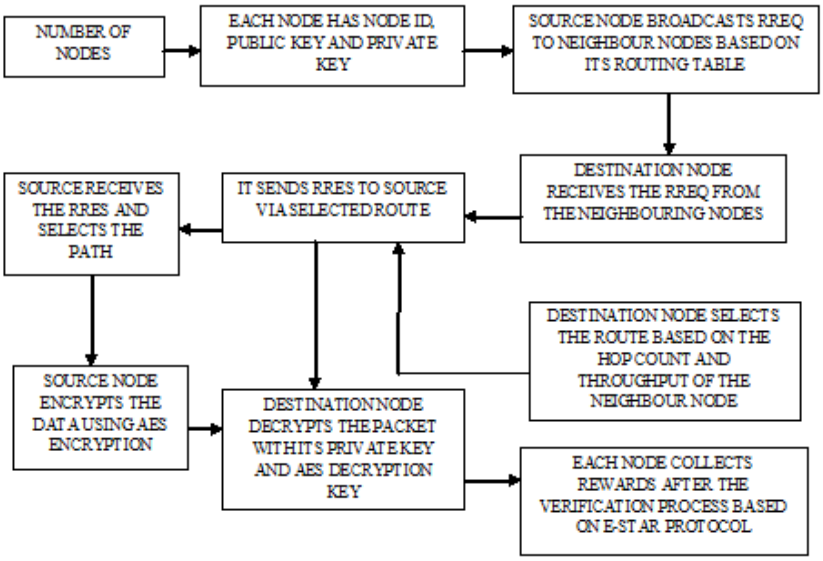

FIGURE 1: ARCHITECTURE DIAGRAM

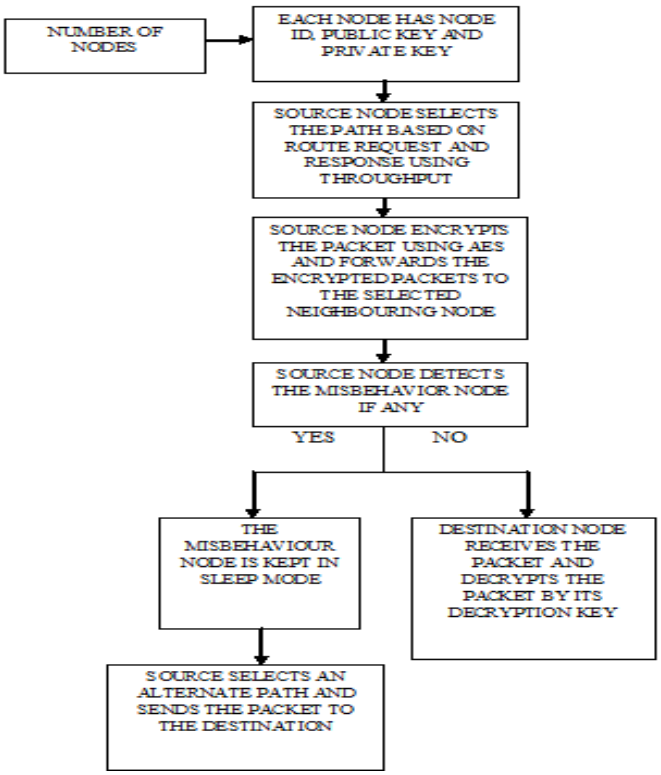

FIGURE 2: DATA FLOW DIAGRAM

ROUTE SELECTION FROM SOURCE SIDE PROCESS:

After the RREQ reaches the destination node it is verified by the destination node. The route is selected by the destination node based on hop count and throughput. The packet is assembled by the destination node and broadcasts it back to the source node. Each intermediate node validates the RRES (Route RESponse) packet and updates its routing tables. After the route selection, source encrypts the data based on AES encryption and it collects the selected neighbor nodes public key from the routing table.

PACKET FORWARDING USING TTL WITH ENERGY:

In this process the source node forwards the encrypted packet to neighbor node based on the selected route. The neighbor node gives its own private key for one part of decryption process. It is then sent to the next neighbor node. Similarly each neighbor node gives its own private key for one part of decryption process. If a misbehavior node receives the packet, the TTL (Time To Leave) gives its decryption key but the packet is not decrypted. This improves the nodes security.

DETECTION OF MISBEHAVIOR NODE:

The neighbor node decrypts the packet and finally sends it to the destination node. If any unknown node enters the network inside, it is kept in sleep mode. The destination node decrypts the packet with its private key. The original data is finally viewed by the destination node. Since the paths capacity will vary, the paths will be changed dynamically as per data transfer along the network. This increases the packet delivery ratio and decreases the average end-to-end delay.

PAYMENT CALCULATION USING ENERGY:

The energy consumed by each node for packet transmission will be calculated. The payment is done to each node as per the energy consumed.

IV. SIMULATION RESULTS:

The performance is evaluated by simulating a wireless sensor network with a 1700x900 meter field in which 26 nodes are placed in the network. The sensors adopt IEEE 802.11 Mac protocol width of 50 meter. This is done in order to transmit the data from the source to destination. The packet delivery and throughput is improved. The misbehavior node is detected and kept in sleep mode condition. Further an alternate path is detected for the energy consumed and introduced for the node reliable path built to secure transmission for encrypted packets in the network at x and y coordinates (1700,900) in order to emulate.

NUMBER OF NODES	26
PACKET SIZE	1000
TRAFFIC TYPE	CBR
PACKET DROP NODE	1
MISBEHAVIOR NODE	1
TTL EXPIRED NODE	1
OUT OF COVERAGE NODE ENTERED	1
INITIAL ENERGY	100J
RESIDUAL ENERGY	50J
PAYMENT COST	LOW COST
NODE SECURITY	ENCRYPTION USING AES
TRANSMISSION RANGE	800
PROTOCOL	AODV
GRID AREA	(1700,900)
PARAMETERS	THROUGHPUT(MBPS), PACKET DELIVERY RATIO, ENERGY CONSUMPTION (J)
SIMULATION TIME	55min

TABLE 1: Simulation Table

NETWORK vs. PROBABILITY:

X-axis is the Transmission Density of the nodes and Y-axis is the packet delivery ratio for analyzing the parameters such as key verification, node life time, secure data transmission and neighbor node selection. The performance of these parameters is high.

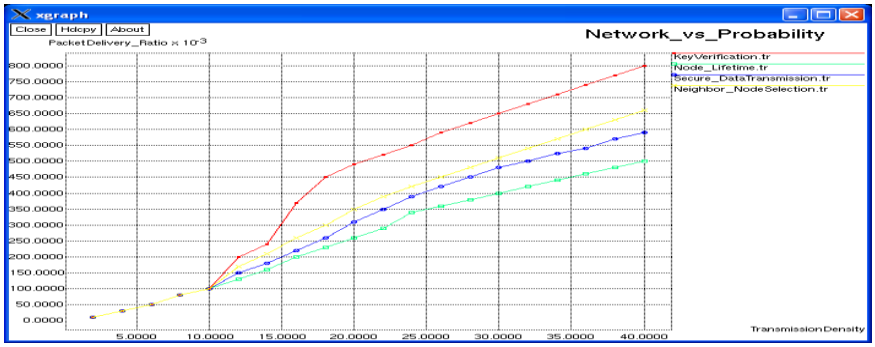

FIGURE 3: NETWORK vs. PROBABILITY

THROUGHPUT vs. MAX QUEUE LENGTH:

X-axis is the number of nodes and Y-axis is the Throughput (mbps) for analyzing the parameters such as Secure key performance, Data transmission, Key verification, Packet transfer and throughput. The throughput of each curve is highly increased with maximum queue length of this interference.

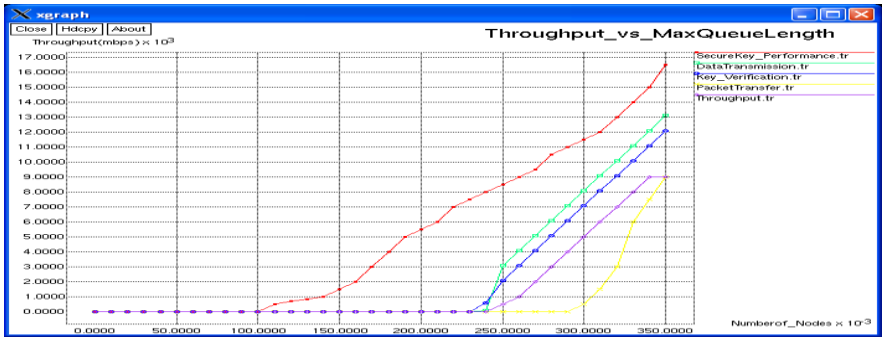

FIGURE4: THROUGHPUT vs. MAX QUEUE LENGTH

ENERGY CONSUMPTION vs. SIMULATION TIME:

X-axis is the simulation time and Y-axis is the energy consumption for analyzing the parameters such as initial energy and residual energy from the assigned 100J energy in the network. The payment is done as per the energy consumed.

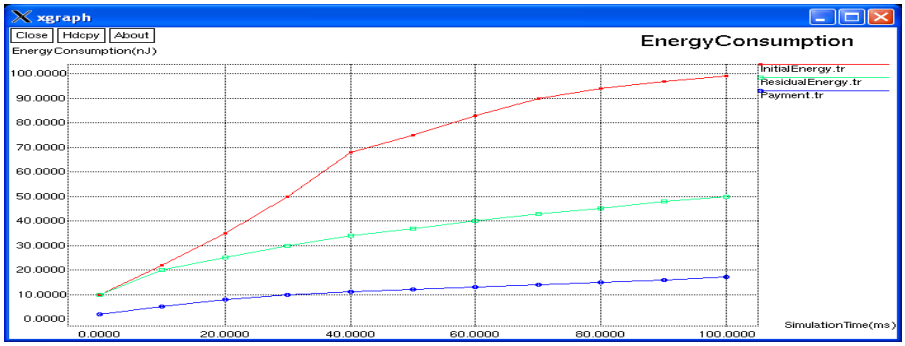

FIGURE 5: ENERGY CONSUMPTION vs. SIMULATION TIME

V. CONCLUSION AND FUTURE WORK:

E-STAR uses payment and trust systems with trust-based and energy aware routing protocol to establish stable and reliable routes in heterogeneous multihop wireless networks. It maintains route stability and stimulates the nodes to relay packets. The nodes that report incorrect energy capability are punished by decreasing their chance to be selected by the routing protocol. SRR and BAR routing protocols are proposed and evaluated in terms of overhead and route stability. The routes established by SRR meets the source nodes trust and energy requirements. Low trust nodes such as malicious nodes with low overhead can be avoided by the establishment of these routes. When compared to SRR, the destination nodes establish the most reliable routes with more overhead in BAR. It is proved through analytical results that E-STAR can secure the payment and trust calculation without false accusations. E-STAR can improve the packet delivery ratio due to establishing stable routes. In future, E-STAR will improve to reduce the packet delay. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks.

REFERENCES

[1] S. Zhong, J. Chen, and R. Yang et al (2003), "Sprite: A Simple, Cheat-Proof, Credit Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, vol. 3, pp. 1987-1997.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.