ARTICLE

SECURED OPTIMAL ROUTING BASED ON TRUST AND ENERGY MODEL IN WIRELESS SENSOR NETWORKS

A Senthil Kumar[1], E Logashanmugam[2]

** [1]Research Scholar, Dept. of Electronics and Communication Engineering, St. Peter's University, Chennai, Tamil Nadu, INDIA*

[2]Professor and Head, Dept. of Electronics and Communication Engineering, Sathyabama University, Chennai, Tamil Nadu, INDIA

ISSN 0976-3104

ABSTRACT

Objective: *In Wireless sensor networks, nodes have deployed to monitor and collect the physical or environmental condition and cooperatively pass the data to the main control node through the network. The data forwarded to the main control node should be efficient and trustable one.* ***Method:*** *In this method a Scalable Energy based Trust model for Security nodes and Data Encryption (SETS-DE) with the private key is proposed. The nodes have very limited capability so profound computations for security mechanisms are not suitable hence; the trust values of nodes are computed for security purpose by using its energy consumption value. The data collected from the sensor node is passed through the trusted nodes. Even though the trusted node might become malicious but the encrypted data cannot be hacked or modified by the corresponding node.* ***Improvement:*** *This proposed method improves the performance measures for packet delivery, throughput and efficiently reduces the energy consumption.*

KEY WORDS
Wireless sensor networks, Nodal energy, Trust based security, Single Message encryption,

INTRODUCTION

A Wireless Sensor Network (WSN) is a group of nodes structured into a cooperative network. Each node consists of processing capability, memory, a RF transceiver, a power source such as battery; solar cells etc., and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-manage after been deployed in an ad hoc manner. Sensor nodes popularly used for monitoring several applications such as environment for battlefield surveillance, military, wild animals. These sensor nodes have severely restricted to resources such as energy, memory and computational power.

In a typical WSN application, the sensor nodes spread in a region from where they collect data to achieve certain goals. Data collection may be a continuous, periodic, or event-based process. The WSN must be very stable in some of its applications such as security monitoring and motion tracking. Systems of 1000s or even 10,000 nodes were anticipated to process an application. Security and privacy are critical services needed for these systems. Security is a broadly used term encircling the characteristics of authentication, integrity, privacy, non-repudiation, and anti-playback. When the dependency on the information provided by the networks has been increases, then the risk of secure transmission of information over the networks has also increased.

To protect WSNs against malicious and selfish behavior, various methods of secured routing protocols had developed which mainly rely on cryptographic basics and authentication mechanisms. Nodes in the network may be compromised due to lack of energy and performs malicious attacks such as packet droppings and packet modifications to disrupt the normal operations of sensor networks.

Received: 16 Nov 2016
Accepted: 12 Feb 2017
Published: 5 April 2017

RELATED WORK

Multi-hop relay had proposed to enhance the coverage area and to forward traffic effectively between the (Base Station) BS and the (Mobile Station) MS consists of several intermediate mobile nodes in between. The novel technical solutions and algorithms for multi-hop relay is analyzed, including the separation of control and data, effective signal-to-interference-plus-noise ratio (SINR)-based routing algorithms, and cooperative relay schemes. Several techniques were proposed but energy consumption is higher for processing the data during transmission. Dynamic Source routing protocol had proposed in multi-hop wireless ad hoc networks, which is composed of the two mechanisms such as Route Discovery and Route Maintenance. This two mechanisms work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. Generally, routing mechanisms are selfish in nature, which leads inappropriate behavior in the network and leads to performance degradation in the entire network [1].

Optimal Forwarder based on Energy and Trust for Routing (OFETR) protocol had proposed to select and prioritize nodes forwarder list based on energy and trust value to improve the network lifetime. This protocol consists of Energy Watcher, Trust Manager and Optimal Forwarder to record the energy values, track the trust values and to address the problem of forward list [4]. Trust-based secure routing model had proposed in which micro Timed, Efficient, Streaming, Loss tolerant Authentication (micro TESLA) algorithm

***Corresponding Author**
Email:
senthilkumarstpeters@gmail.com

is used to ensure that the data should not be tampered by malicious nodes i.e. to authenticate the data packets between source and destination nodes [5].

A robust Trust-Aware Routing Framework for dynamic WSNs had proposed to provide protection against the identity deception through replaying routing information. TARF secures the multi-hop routing in WSNs against intruders misdirecting the multi-hop routing by evaluating the trustworthiness of neighboring nodes. It identifies such intruders by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput [6].

A scalable cluster-based hierarchical trust management protocol for wireless sensor networks had implemented to effectively deal with selfish or malicious nodes. A trust management protocol is applied in which a SN may adjust its behavior dynamically according to its own operational state and environmental conditions. A SN is more likely to become selfish when it has low energy or it has many unselfish neighbor nodes around [7].

A highly scalable hierarchical trust management protocol for clustered WSN had proposed. Here each node subjectively evaluates other peers periodically. Peer to peer trust evaluations are reported from sensor nodes, a cluster head obtain trust report of all sensor nodes present in its cluster and this cluster head performs a statistical analysis to identify and exclude malicious node from the network. This trust-based IDS scheme considers the effect of both social trust and QoS trust on trustworthiness or maliciousness [8]. Scalable Trust Based Secure (STBS) [9-10] wireless sensor networks had proposed new components for trust management systems even there is a change in the network. When the new nodes deployed in the existing network, the trust relationship should be maintained between the newly deployed nodes and the existing nodes. However, maintaining scalable energy based trust relationship between the nodes in the network is difficult in this existing method.

Scalable energy based trust model for security nodes and data encryption

A novel and scalable energy based trust model for node security method with the encryption of data is proposed. Data Encryption Standard (DES) is applied to assure message passing security in this proposed method. Generally, nodes have limited capability and consume high energy for security purposes; hence instead of implementing heavy security mechanisms, a node based trust factor, which includes both energy consumption and selfishness factor, is designed. The nodes may break routes due to malicious action, malfunction, low hardware resources; and having low processing energy is all characterized as node behavior. The objective of this proposed model in WSN is to identify the trusted nodes and to pass the encrypted messages to the trusted nodes. By improving security and reducing energy consumption level improves the novelty of the proposed SETS-DE mechanism. Here, three-tier system such as Mobile Sink (MS), Access Point (AP) and Motes (M) are proposed in order to derive optimal routing, maximize the network lifetime and secure transmission of data.

Phase 1: Tier 1 to Tier 2

In this phase, RREQ is broadcasted from the source node present in the mobile sink to the intermediate node relies in AP. The threshold value ranges from 0.7 and 1.0 for AP and Motes. If the trustworthiness of the mobile node matches with the threshold value, then the AP transmits the request to the second phase.

Phase 2: Tier 2 to Tier 3

RREQ is passed from the intermediate node to the destination node present in the Mote. The mote has predefined threshold value. If the intermediate node's trust value matches with the predefined threshold value of the destination the RREP is sent via the same path.

Selfishness Factor

In this mobile sink phase, the source node sends the Route Request (RREQ) to the AP through the intermediate nodes. The trust model is proposed to calculate the trustworthiness of the each node present in the network and the trustworthiness factor for each node is evaluated by their residual energy. The node may change to malicious node due to lack of their residual energy. The malicious node in the network is identified by the selfishness factor. The selfishness factor can be derived by the ratio of RREQ to the number of Route Reply (RREP).

$$Selfishness\ Factor\ = {}^{No\ of\ RREQ}\!\big/\!_{No\ of\ RREP}$$

Energy calculation

It is necessary to calculate the energy level in each node in order to identify the average energy consumed by the nodes for the data transmission. This includes energy spent for sending, receiving and processing the data from mobile sink to destination via AP. The residual energy level in the node can be evaluated by using the below equation.

$$Energy\ consumption = Initial\ energy - Current\ energy$$

Nodal trust value

The trustworthiness of the nodes or nodal trust can be calculated by using two factors such as selfishness of the node and the available energy level of the node after processing the requests. It can effectively guide the data route in choosing nodes with high trust to avoid black holes.

$$Trust\ value = \sum_{i=0}^{n} (S_{reply_{(i)}} + Potential\ energy\ of\ the\ node_{\ (i)})$$

$$S_{reply} \succ Successful\ Reply$$

Algorithm for SETS-DE

```
Step 1: Broadcasts RREQ from SN to AP
Step 2: Identifying Trust value of each node
        (a)   Calculate Selfishness factor

        (b)   Calculate energy component

Step 3: Checks for the threshold value of AP
Step 4: If trust value matches with the threshold value, then the RREQ passes to the second phase.
Step 5: Again step 2 process continues
Step 6: If threshold value of intermediate nodes matches with the threshold value of Motes, then RREP is passed to the source.
Step 7: The trusted route had discovered, and data is sent via in this route from the source to the sink.
Step 8: The data is encrypted with private key, even the trusted nodes become malicious it cannot access the data.
```

Reliable data transmission

Once the reliable and trusted route is discovered, the data passed from the source node to destination node present between the tier 1 and tier 3. The data is encrypted with the symmetric key even the intermediate node become malicious, it cannot modify the information contained with it. To ensure the secured and reliable data transmission, the threshold values are fixed and verified for the intermediate nodes by the AP and the motes. The goal is to maximize the ratio of successful packets reaching the sink and to reduce the energy consumption. The data encryption Standard (DES) can be implemented by using the security key management technique.

SIMULATION RESULTS AND ANALYSIS

In order to analyze the performances of the proposed method SETS-DE, the packet delivery rate, packet loss rate, delay rate and throughput are compared through simulations with the existing method.

Packet delivery rate

The Packet delivery rate is the ratio of the total packets delivered by the sender node to the corresponding receiver node in the network. The equation for PDR is shown below, where n represent the number of nodes in the network.

$$PDR = \frac{\sum_0^n Pkts\ Received}{time} \qquad (1)$$

Packet loss rate

Packet Loss Rate (PLR) is the ratio of the packets lost during packets transmission sent by the sender to their corresponding receivers. The fig 2 shows the packet loss rate for the proposed SETS_DE and the existing STBS. The packet lost rate is lower for the proposed SETS_DE mechanism. The equation for PLR is given below,

$$PLR = \frac{\sum_0^n PktsLost}{time} \qquad (2)$$

Delay

Delay refers to the latency time between sent packets and the received packets. The delay is calculated by using the equation shown below,

$$Delay = \frac{\sum_0^n (PktRecvTime - PktSentTime)}{n} \quad (3)$$

Where 'n' represent the number of nodes.

The average delay is plotted and it is shown clearly that the delay value is low for the proposed model SETS-DE than the existing STBS method)

Throughput

Throughput is defined as the total number of successfully received packets. The average throughput is calculated by using the equation shown below.

$$Throughput = \frac{\sum_0^n Pkts\ Received\ (n) * Pkt\ Size}{1000} \quad (4)$$

The SETS-DE method has achieved greater average throughput when compared to the STBS mechanism. The security measures had improved the network performance greatly.

Residual energy

The amount of energy remaining in a node at the current instance of time is said to be as residual energy. A measure of the residual energy gives the rate at which energy is consumed by the network operations. Fig 5 shows the proposed scheme has higher residual energy compared to the existing method STBS

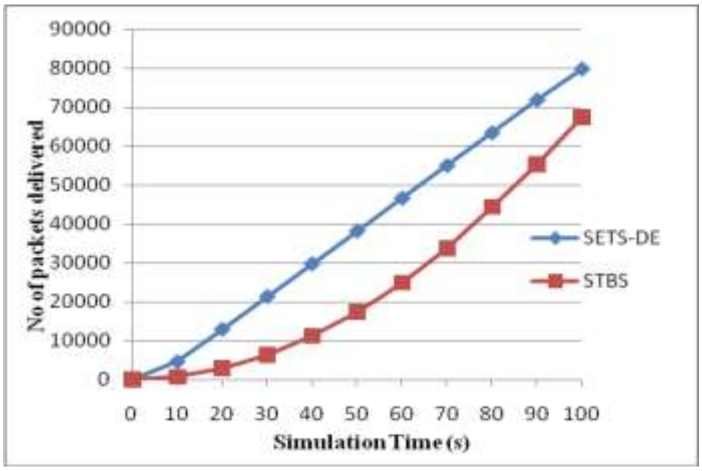

Fig: 1. Packet delivery rate.

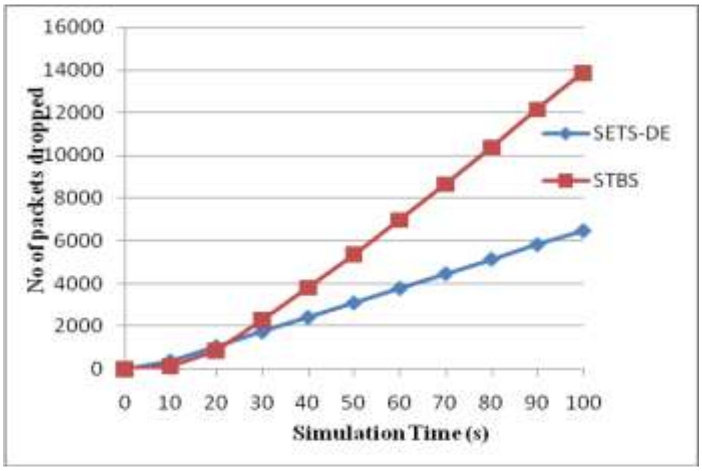

Fig. 2: Packet loss rate.

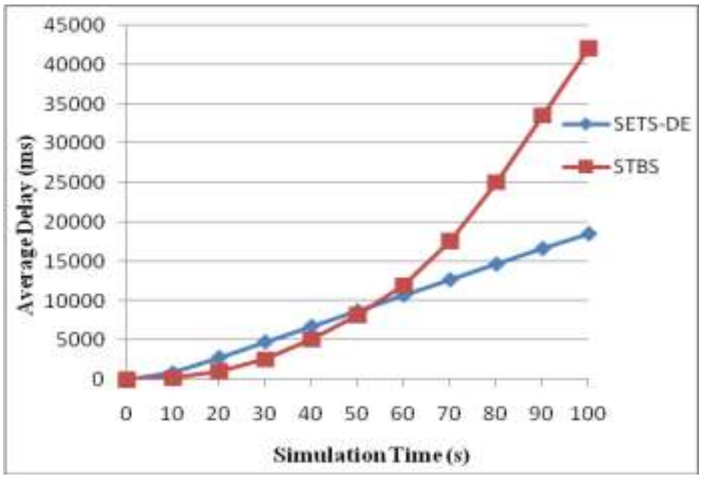

Fig. 3: Delay.

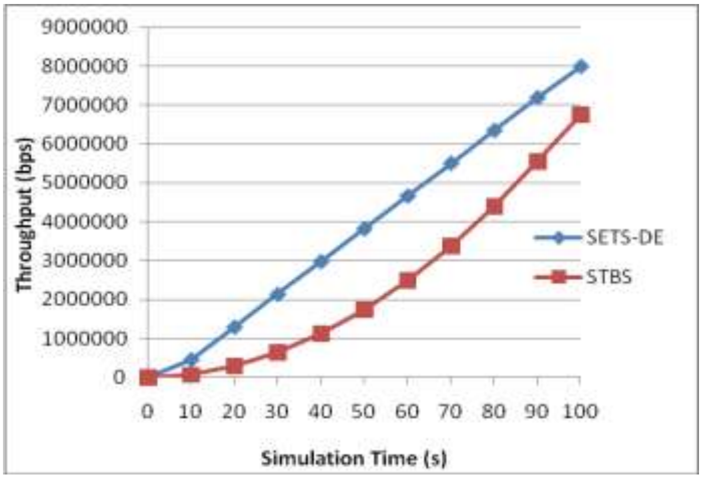

Fig. 4: Throughput.

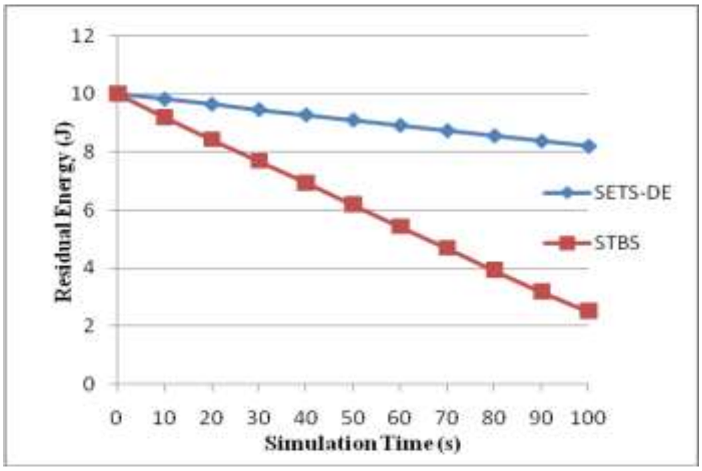

Fig. 5: Residual energy.

CONCLUSION

The Scalable Energy based Trust model for Security nodes, Data Encryption (SETS-DE) model is proposed for improving the scalability and reliability of wireless sensor networks in three tier based system. This proposed algorithm gives an efficient output in terms of energy consumption and trust based security nodes. This proposed scheme can be applied in high security requirement environmental scenarios. Simulation analysis shows better performance for packet delivery, throughput and average delay for the proposed scheme is comparatively low. This improves the security in significant to the energy consumption of nodes. In future, the overall end-to-end delay can be further reduced by using secured energy based algorithms.

CONFLICT OF INTEREST

There is no conflict of interest.

ACKNOWLEDGEMENTS

None

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Johnson D, Maltz A, Broch J. [2001] DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks, Ad hoc networking, 5: 139-172.

[2] Chughtai O, Badruddin N, Awang A Rehan M. [2013] A cooperative selection reactive routing protocol for wireless sensor networks, Research and Development (SCOReD), IEEE Student Conference, pp. 495-499.

[3] Yuxin L, Dong M, Ota K, Liu A. [2013] Active Trust: Secure and Trustable Routing in Wireless Sensor Networks, IEEE Transactions on Information Forensics.

[4] Maqbool S, Nidhi C, Shivraj D. [2013] Selecting Optimal Forwarder Based on Energy and Trust for Routing in WSN, In Computational Intelligence and Communication Networks (CICN), 5th International Conference, pp. 368-373.

[5] Wei, Liu Y, Qing, Nan Y. [2015] A trust-based secure routing algorithm for wireless sensor networks, In Control Conference (CC), 34th Chinese, pp. 7726-7729.

[6] Guoxing Z, Shi W, Deng J. [2012] Design and implementation of TARF: a trust-aware routing framework for WSNs, IEEE Transactions on dependable and secure computing, 9(2): 184-197.

[7] Fenye B, Chen R, Moon C, Jin-Hee C [2012] Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection, IEEE transactions on network and service management, 9(2): 169-183.

[8] Bao, Fenye, Ray Chen, Moon Jeong Chang, and Jin-Hee Cho. [2011] Trust-based intrusion detection in wireless sensor networks. In IEEE International Conference on Communications (ICC), pp. 1-6.

[9] Agrawal A, Wei R. [2014] Scalable Trust-Based Secure WSNs," Journal of Computer and Communications, 2(7):17.

[10] Pathan K, Al-Sakib and Hong C S. [2007] A secure energy-efficient routing protocol for WSN, In International symposium on parallel and distributed processing and applications, Springer Berlin Heidelberg, pp. 407-418.