Energy Efficient Protocol In Wireless Sensor Network For Secured Data Transfer

Nami Susan Kurian, Assistant Professor,
Dept of Electronics and Communication Engineering,
Rajalakshmi Institute of Technology,
Chennai, Tamil Nadu
Email: namisusan7@gmail.com

Hemamalini K,
Dept of Electronics and Communication Engineering,
Rajalakshmi Institute of Technology,
Chennai, Tamil Nadu
Email: hemamalinik.2016.ece@ritchennai.edu.in ,

Arthi S
Dept of Electronics and Communication Engineering,
Rajalakshmi Institute of Technology,
Chenni, Tamil Nadu
Email: arthis.2016.ece@ritchennai.edu.in

Deepadharshini B
Dept of Electronics and Communication Engineering,
Rajalakshmi Institute of Technology,
Chenni, Tamil Nadu
Email: deepadharshinib.2016.ece@ritchennai.edu.in

***Abstract*—In the existing wireless sensor networks, security is a very important constrain. Malicious nodes can repeatedly break routes. Breaking the routes increases the packet delivery latency. In this paper, we propose a protocol in which routing path is selected based on request response by source. Transmission of data to destination is done using E-STAR protocol. We also deploy onion protocol in which every node while registering, server will provide an Id, primary key, secondary key and decryption key. Source will findout the optimum path and it will collect primary key of all intermediate node. Data is first encrypted using AES algorithm and then with related primary key of all the hops. This wholesome is transmitted to first hop, where initial decryption is achieved using decryption key of that node. ID and secondary key are collected and it is then transmitted to both source and destination node. In this way, all the id's and secondary key are collected and concatenated to verify both source and destination. Trusted third party implementation is also achieved for successful verification of concatenated keys thereby reward is provided to the intermediate hops.**

Keyword—Localization, Data Aggregation, Residual Energy, Relay nodes, Collabrator.

I. INTRODUCTION

The four basic components of a sensor node are: a sensing unit, a processing unit, a transceiver unit and a power unit. The additional components such as a location finding system, a power generator and a mobilizer can be incorporated based on the application needs.The WSN is built of "nodes", where each node is connected to one (or sometimes several) sensors. In a wirelesss network, there can be 'n' no of nodes deployed to perform some specific applications. Currently, data is obtained from multiple number of sensors and is aggregated at an aggregator node. The aggregator node [1] then forwards only the aggregate values to the base station. The most important limitations of sensor node is its computing power and energy resource, the data aggregation is done by simple algorithms. e.g. averaging.

The cryptographic methods cannot be used beacuse the compromised nodes helps attackers in hacking the information. Because if this reason, trustworthness of data from individual sensor nodes is important Hence, more sophasticated algorithms are needed for daa aggregation in the furture WSN. In the presence of stochastic errors such algorithmshould produce estimates which are close to theoptimal ones in information theoretic sense. Thus,for example, if the noise present in each sensor is aGaussian independently distributed noise with zeromean, then the estimate produced by such an algorithm should have a variance close to the CramerRao lower bound (CRLB) [2], i.e, it should be close tothe variance of the Maximum Likelihood Estimator (MLE). However, such estimation should be achieved without supplying to the algorithm the variances of the sensors, unavailable in practice. 2. The algorithm should also be robust in the presence of non-stochastic errors, such as faults and malicious attacks, and, besides aggregating data, such algorithm should also provide an assessment of the reliability and trustworthiness of the data received from each sensor node. Trust and reputation systems have a significant role in supporting operation of a wide range of distributed systems, from wireless sensor networks and e-commerce infrastructure to social networks, by providing an assessment of trustworthiness of participants in such distributed systems. A trustworthiness assessment at any given moment represents an aggregate of the behaviour of the participants up to that moment and has to be robust in the presence of various types of faults and malicious behaviour. There are a number of incentives for attackers to manipulate the trust and reputation scores of participants in a distributed system, and such manipulation can severely impair the performance of such a system [3]. The main target of malicious attackers are aggregation algorithms of trust and reputation systems [4].

II. RELATED WORK

This paper ***"Secure and Reliable Routing Protocols for Heterogeneous Multihop Wireless Networks"*** propose a protocol named E-STAR for establishing steady and trusty routes in heterogeneous multihop wireless networks. E-STAR protocol incorporates the payment and trust systems with a trust-based and energy-aware routing protocol. Payment system(trusted third party) rewards the nodes that relay others packets and charges those that send packets. The trust system (TTP) evaluates the nodes ability and reliability in relaying

packets in terms of multi-dimensional trust values. Two routing protocols is developed to direct traffic through those highly – trusted nodes. These

trusted nodes have sufficient energy to minify the probability of breaking the route. E-STAR [5] can maintain route stability and battery energy capacity in this way. Loss of trust will result in loss of earnings.

This paper *"**Energy-Efficient Routing Protocols in Wireless Sensor Networks: Survey" highlights o**n* the energy efficient routing protocols that are formulated for Wireless Sensor Networks with better statement of the issues and operations in each protocol. They are divided into four main schemes- (a) Network Structure (b) Communication Model (c) Topology Based and (d) Reliable Routing. Network Structure routing protocols cut down the traffic overhead. whereas Topology based routing protocols drop-off the energy consumption. Communication Model based routing protocols assurance the successful delivery of data and hence the throughput can be increased with this protocol. In reliable Routing Protocols, performance is based on environmental conditions. But, lifetime of the node is a challenging factor.

This paper *"**Performance Evaluation of on Demand Routing Protocols AODV and Modified AODV (R-AODV) in Manets"***, explains about mobile ad hoc networks. In case of MANRTS, there is no centralized infrastructure to proctor or assign the resources used by MN. Routing is complex when the central coordinator is absent unlike in cellular networks. The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for MANETS in which routes are exstablised based on the demand. Route request is send through difeerent paths and reaches the destination. Only a single route reply is expected through the best path. As the topology is changing faster,the route reply may not arrive to the source node and this results in sending several route request messages and degrading the performance of the routing protocol.

This paper *"**Anonymous Secure Communication in Wireless Mobile Ad-Hoc Networks" higlights the security aspects related to adhoc networks. As Ad-hoc network is a dynamic, infrastructureless network, m***alicious intermediate nodes in wireless mobile ad- hoc networks are a danger questioning the security as well as anonymity of exchanged information. To protect anonymity and achieve security of nodes in mobile ad- hoc networks, an anonymous on-demand routing protocol - RIOMO is proposed. Pairing-based Cryptography is used for developing ID's of the nodes[6].

LEACH: low energy adaptive clustering hierarchy is a routing algorithm in which nodes are static, homogenous with same initial energy. Cluster [7] assigns TDMA schedule for their members. Data is transmitted from source node to cluster head (CH) to base station (Single direct transmission). After certain period, CHs are again detected through setup phase. After the selection of CH is done, advertisement packet is send. Each node, except CHs, listens to the advertisement and joins the closest CH. Once the CH knows the members, schedules are created for them for data transmission.

III. PROPOSED SYSTEM:

Every node while registering, server will provide Id, primary key, secondary key and decryption key. Sources will find out the optimum path by considering hop count and capacity and it will collect the primary keys of all intermediate nodes. Data is first encrypted using AES algorithm [8] 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 particular node. Then its id and secondary key is transmitted to both source and destination node. Same way all the id's and secondary keys are collected and concatenated, so as to verify both source and destination. Reward is provided based on successful validation of keys based on TPA implementation.

A. ARCHITECTURE DIAGRAM

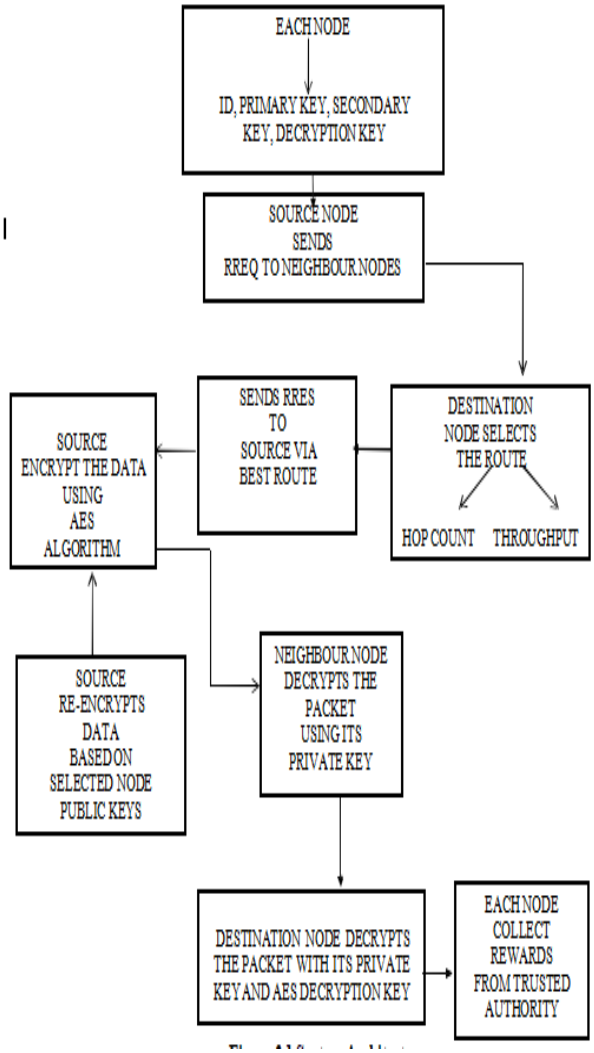


Figure 1: Architecture Diagram

B. SYSTEM ARCHITECTURE

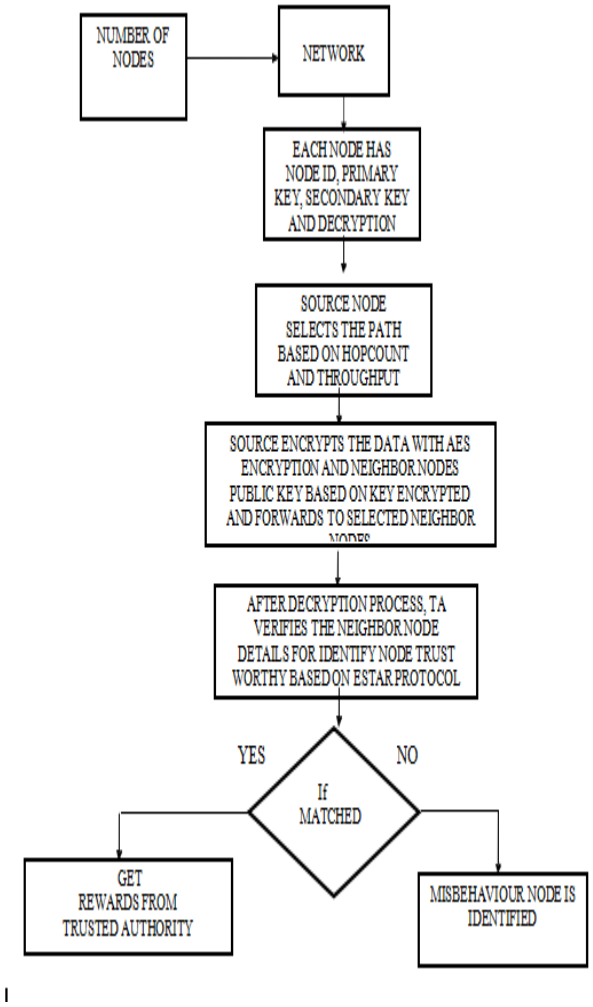


Figure2 :System Architecture

In the proposed protocol, each node have an ID, Primary key, Secondary key and Decryption key. Sourse node sends RREQ to all neighbours. The destination node sends RRES base don the hop count(via best route). The source encrypts data using AES algorithm and re-encrypt data based on th public key. The neighbouring node on receiving the data decrypts the data using its private key but it cannot see the data inside. The destination node decrypt data using its private key and AES decryption key. After the transmission, the trusted nodes will get rewards.

Security is the most important aspect in wireless networks. By using the AES algorithm and re-encryption methods, security is assured and data can reach the intended receiver without being attacked by the intruders.

IV. METHODOLOGY

A. Node Construction

Consider a network with 'n' number of nodes. We assume that the nodes are mobilein nature. Each node is having public and private key. This information is monitored by the network for security purpose. The proposed protocol works as follows.

B. Route Request Based On Routing Table Checking

Source sends hello packet to all the intermediate nodes to identify the destination having minimum hop count [9]. Routing table in RREQ packet can be used to find how many of its neighbours have not been covered. Each intermediate nodes update its rotuing packet after validating the RREQ packet. RREQ finds the destination at the end.

C. Route Selection And Source Side Encryption Process

Route request is initiated by the source node and it is then send to all other nodes by the process of flooding and is then verified by the destinaion node. The destination node selects route based on hop count and the throughput. The destination node initiates a Route reply packet and broadcast to the source node. The intermediate nodes verify the Route repl packet and broadcast it to the source updating its routing table. After route establishment, source send encrypted data based on AES encryption.

D. Packet Forwarding

Source node forwards the encrypted packet based on the selected route. Neighbor node gives its own private key for one part of decryption process. After that it will send to next neighbor node.

E. Decryption Process

In this step, neighbor node decrypts the packet and finally sends to destination node. Then the destination node decrypts the packet with its private

key and AES decryption key. Finally destination node views the original data.

F. Trusted Authority

Trusted authority identifies the trustworthiness of the nodes and provides rewarsd to intermediate nodes. After successful data transmission, each neighbor node in selected path sends its id and secondary keys to trusted authority [10] for collected rewards. Then trusted authority checks both details are match or not. If match means, it gives rewards to the nodes.

V. RESULTS

A. Throughput

The average rate or usual amount of messages that are delivered successfully across a communication channel is called throughput. Throughput can also be defined as the number of packets that successfully reaches the destination. The proposed protocol provides high throughput compared to existing protocols as there is no chance of packet loss since we provide high security.

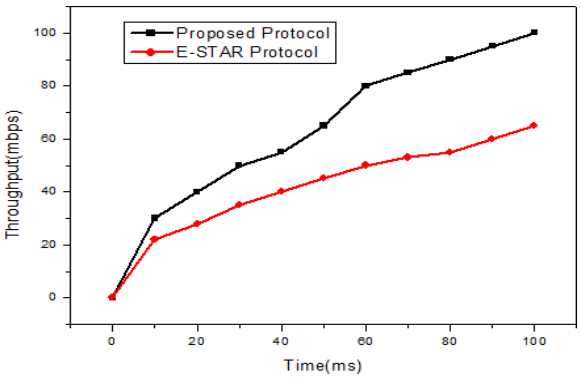
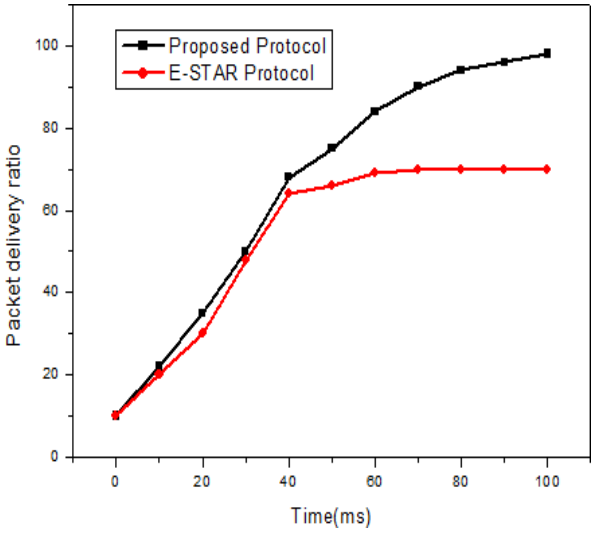


Figure 3: Time vs Throughput

B. Packet Delivery Ratio:

The number of packets delivered for a particular period of time is defined as the packet delivery ratio. Figure 4 shows the comparision of packet delivery ratio of proposed protocol to the existing one.propsed protocol provides high packet delivery ratio as the number of packets delivered within a time is more.

Figure 4: Time vs Packet Delivery



C. Energy

Energy efficiency is most important in WSN as the working of a sensor node is based on on-board batteies. Energy efficiency of sensor nodes in proposed and existing protocol are shown in Fig 4.4.Energy efficiency is the more for proposed protocol as there is no chance for retransmission.

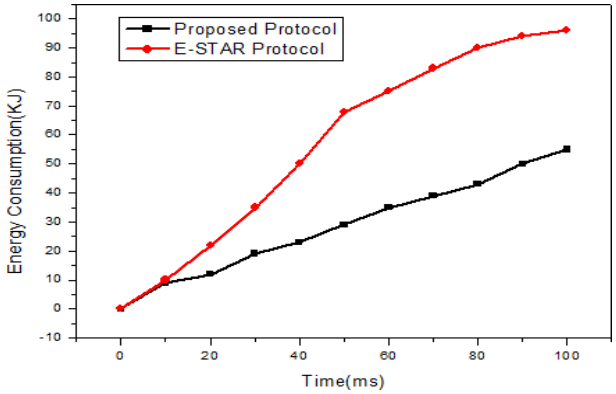


Figure 5: Time vs Energy consumption

VI. CONCLUSION

In this paper, every node while registering, server will provide an Id, primary key, secondary key and decryption key. Sources will find out the optimum path and it will collect primary key of all intermediate node. Data is first encrypted using AES algorithm and then with corresponding primary key of all the hops. Then the wholesome is transmitted to first hop, where initial decryption is achieved using decryption key of that node. Then, id and secondary key are collected and 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. TPA implementation is also achieved for successful validation of concatenated keys there by reward is provided to the intermediate hops. There is high security maintained, and the energy of sensor nodes are conserved effectively. The proposed protocol shows less delay and high throughput than other protocols. Hence, the proposed protocol can perform well with low delay and high energy efficiency in many sensor network applications.

REFERNECES

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J., vol. 13, no. 4, pp. 175-193, 2009.

[2] 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 J. Selected Areas in Comm., vol. 25, no. 1, Jan. 2007.

[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] 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.

[5] G. Indirania and K. Selvakumara, "A Swarm-Based Efficient Distributed Intrusion Detection System for Mobile Ad Hoc Networks (MANET)," Int'l J. Parallel, Emergent and Distributed Systems, vol. 29, pp. 90-103, 2014.

[6] H. Li and M. Singhal, "Trust Management in Distributed Systems," Computer, vol. 40, no. 2, pp. 45-53, Feb. 2007.

[7] 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.

[8] 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.

[9] Nami Susan Kurian ; B. Priya, "EHMBA: An energy efficient hybrid MAC multihop broadcast protocol for asynchronous duty-cycled wireless sensor networks", International Conference on Information Communication and Embedded Systems (ICICES2014).

[10] Nami Susan Kurian ; B. Priya, "EMBHMAC: An efficient multihop broadcast based hybrid MAC protocol for wireless sensor networks", Proceedings of IEEE International Conference on Computer Communication and Systems ICCCS14.