A Secure and Efficient Lifetime Routing Optimization for End-to-End Communication in WSN

MD Raziya¹, Dr G Satyanarayana², Dr. C P V N MohanRao³
¹,²,³ Computer Science Engineering Department,
¹,²,³ Avanthi Institute of Engg & Technology, Narsipatnam, Visakhapatnam (Dt), A.P., India

Abstract: Lifetime optimization and security are two conflicting design issues for multi-hop wireless sensor networks (WSNs) with non-replenishable energy resources. In this paper, we first propose a novel secure and efficient end-to-end routing protocol to address these two conflicting issues through two adjustable parameters: energy balance control (EBC) and probabilistic based random walking. We then discover that the energy consumption is severely disproportional to the uniform energy deployment for the given network topology, which greatly reduces the lifetime of the sensor networks. To solve this problem, we propose an efficient non-uniform energy deployment strategy to optimize the lifetime and message delivery ratio under the same energy resource and security requirement. We also provide a quantitative security analysis on the proposed routing protocol. Our theoretical analysis demonstrate that the proposed end to end routing protocol can provide an excellent tradeoff between routing efficiency and energy balance, and can significantly extend the lifetime of the sensor networks in all scenarios. For the non-uniform energy deployment, we also demonstrate that the proposed end-to-end routing protocol can achieve a high message delivery ratio while preventing routing attacks. We adopt a novel approach of group key communication scheme in our design, such that there is a unique group key, called as path key, to protect data transmitted in the entire routing path. Rather than using multiple shared keys to repeat to perform encryption and decryption over every link, we implement end-to-end path keys to reduce the overheads of key generation. Therefore, we can see that by implementing these concepts we can improve efficiency of network and provide more security of transferred message.

Index Terms— Security, Wireless Sensor Networks, Frequency hopping, Dijkstra’s Algorithm, Encryption and Decryption

1. INTRODUCTION

The outstanding progress in natural philosophy, technology sealed the trail for the expansion of micro-electronics, thus facilitating the manufacture of tiny chips and small devices. The communication technology is undergoing transformation because of the planning and improvement of small devices and thus expedited the planning and advancement of WSN with low price and low energy consumption.

WSN has many applications in military, health and in different industrial sectors. Due to the characteristics of WSN, sensor nodes are typically attributed with restricted power, low information measure, low memory size and restricted energy. Due to the measurability and energy effectiveness options, investigators prompt many routing protocols for cluster-based WSN. Routing could be a method of determinative a path between supply and destination upon request of information transmission. In WSN, the network layer is employed to implement the routing of the incoming information. It is illustrous that in multi-hop networks the sensing node cannot reach the sink directly. So, intermediate detector nodes have to be compelled to relay their packets. The implementation of routing tables offers the answer. These contain the lists of node possibility for any given packet’s destination.

Numerous improved hierarchal routing protocols were suggested in many research papers. But, some requirements for the routing protocols are conflicting.
Always selecting the shortest route towards the base station causes the intermediate nodes to deplete faster, which result in a decreased network lifetime. At the same time, always choosing the shortest path might result in lower energy consumption and lower network delay. Since the routing objectives are tailored by the application, different routing mechanisms have been proposed for different applications. These routing mechanisms primarily differ in terms of routing objectives and routing techniques.

The majority routing protocols are vulnerable to uncounted security risks. Attacks comprising Cluster Head (CH) are in the main harmful. Because of resource restrictions, the general public key based algorithms like Rivest Shamir Adelman (RSA) and Diffie-Hellman are terribly complicated and energy-consuming for WSN. In several cases, multiple sensing element nodes are needed to beat environmental obstacles like obstructions and line of sight constraints. Also, the setting to be monitored doesn't have an associate degree of existing infrastructure for energy economical communication. Therefore, it becomes imperative for sensing element nodes to survive on tiny, finite sources of energy and communicate through a wireless communication. Security could be a crucial issue because of inherent limitations in WSN.

II. LITERATUR SURVEY

A few protocols explored in literatures (He et al. 2003, Chipara et al 2006, Parvaneh Rezayat et al. 2010) deliver the messages in the network based on their deadline. Though these protocols reduced the communications delay involved in message transfer by dynamically varying the transmission power, the power utility in the network can still be reduced. Sridevi and Rumeniya [3] presented a review on the existing routing protocols for WSN by considering energy efficiency and QoS. It was focused on the main motivation behind the development of each protocol and explain the function of various protocols in detail. The protocols were compared based on energy efficiency and QoS metrics. Kirida Ezhillarasi and M. Jenolin Rex [4] derived the optimal communication range and communication mode to maximize the Network Lifetime. The intra-cluster scheduling and inter-cluster multi-hop routing schemes were used to maximize the network lifetime. It was considered a hierarchal network with Cluster Head nodes having larger energy and processing capabilities than normal SNs. The solution is formulated as an optimization problem to balance energy consumption across all nodes with their roles. A two tier network with the objective of maximizing network lifetime is presented while fulfilling power management and coverage objectives.

Sung Keun Lee et al. [5] proposed a routing protocol that can provide QoS that appropriately reflects changes in network status regarding reliability and delay, even in circumstances with a deficiency in sensor node resources. This algorithm has the advantage of minimizing the routing control messages and therefore can safely operate from an energy-efficient perspective, as the algorithm utilizes broadcast messages regularly transmitted by the sink node. It was observed that the sensor node establishes a routing table based on the shortest route towards a sink, the energy efficiency of the foothold, and the least amount of congestion.

Udit Sajjanhar and Pabitra Mitra [6] developed the Distributive Energy Efficient Adaptive Clustering (DEEAC) protocol. This protocol is adaptive in terms of data reporting rates and residual energy of each node within the network. It is a modification of the LEACH's stochastic cluster-head selection algorithm by considering two additional parameters, the residual energy of a node relative to the residual energy of the network and the spatiotemporal variations in the data reporting rates of a node relative to the network. Since this protocol evenly distributes energy-usage among the nodes in the network by efficiently adapting to the variations in the network, our optimal cluster-head selection saves a large amount of communication energy of sensor nodes.

Wendi Rabiner Heinzelman et al. [7] described a clustering-based routing protocol that minimizes global energy usage by distributing the load to all the nodes at different points in time. It outperforms static clustering algorithms by requiring nodes to volunteer to be high-energy cluster-heads and adapting the corresponding clusters based on the nodes that choose to be cluster-heads at a given time. At different times, each node has the burden of acquiring data from the nodes in the cluster, fusing the data to obtain an aggregate signal, and transmitting this aggregate signal to the base station.

Zahra Rezaei and Shima Mobinineja [8] conducted extensive research to address these limitations by developing schemes that can improve resource efficiency. It was also summarized some research results which have been presented in the literature on energy saving methods in sensor networks. Although many of these energy saving
V. Vinoba and A. Indhumathi [9] proposed a novel energy efficient routing protocol by using quadratic assignment technique. This protocol achieves energy efficiency by finding an optimal path to transfer the data from source to destination. In this work the proposed routing protocol, is to process the multiple route in finding the shortest path. It is also proposed that the Temporally Ordered Routing Algorithm which uses the Destination sequenced distance vector and find out the multiple route for neighbor node list table.

M.G.Annapoorani and M.S.Kokila [10] analyzed the fundamental characteristics and energy limitations of the WSN. To solve the energy limitation of WSN this system uses an efficient strategy to forward data toward the sink was developed. It enabled the nodes to choose multiple next hops. With this system, the remaining energy of the nodes will be increased and the life time of the whole network will be increased, too. The Tree approach designs the path for data routing that maximizes the data gained from the sensors under multiple possible neighbors as next hop. This solution is reduces the energy consumed for each node, and consequently increases the network lifetime.


Shaojie Wen et al. [12] presented an energy-efficiency opportunistic multicast routing protocol (EOMRP) for themulticast energy consumption minimization problem. In mobile wireless sensor networks. The protocol divides the network into grids, so each node determines their own coordinates according to the grid. The nodes only need to know the topology of their own grid, instead of the topology of the entire network. In order to better represent the impact of the movement on transmission, the nodes in the same grid determine the priority in light of the transmission delay factor and expected transmission cost.

Loh and Yi Pan [13] proposed an energy-aware routing protocol, Energy Clustering Protocol (ECP) that routes essages via cluster heads. Unlike other clustered configurations, it exploits nodes at the boundaries of the cluster (border nodes) to assist in the forwarding of packets as well as to reduce dependency on and energy expenditure of cluster heads. It was also demonstrated that a hierarchical routing protocol design that can conserve significant energy in its setup phase as well as during its steady state data dissemination phase.

Xufei Mao et al. [14] studied that how to select and prioritize the forwarding list to minimize the total energy cost of forwarding data to the sink node in a wireless sensor network (WSN). It was observed that previous protocols, i.e., ExOR and MORE, did not explore the benefit of selecting the appropriate forwarding list to minimize the energy cost. The transmission power of each node was fixed and each node can adjust its transmission power for each transmission. Optimum algorithm was used to select and prioritize forwarder list.

Yeong Hong Wang et al. [15] introduced the Hierarchy-Based Multipath Routing Protocol (HMRP). It has many paths to disseminate data packets to the sink. The data aggregation mechanism involves in every nodes apart from the leaf nodes reducing the energy consumption in the networks. Based on the layered network, sensor nodes have multipath routes to the sink node through candidate parent nodes. Jiann-Liang Chenet al. [16] introduced an adaptive method based on redundancy node and dual routing protocol for WSN. Redundancy node can divide the wireless sensor network into operating and sleeping modes. Dual routing protocol individually designs two kinds of different routing protocols in the sensor node, using the merits of these two different kinds of routing protocols to accomplish the mission of sending the data. The scenario set up is when the wireless sensor network has been used for a long time; the power kept in these sensor nodes is different. It is possible that some sensor nodes contain lower power because the heavy load of work, and some with more power because of less work load.

Mohammad Shaheer Zaman and G Rama Murthy [17] proposed a new routing scheme which exploits the redundancy and geometrical properties of the wireless network. This approach was taken to combine the ideas of directional flooding, leveling, clustering and disjoint multipath routing to achieve an optimal routing scheme in terms of average energy consumed and total number of transmitted packets. Processing and structuring of the network before the implementation of the directional flooding algorithm improves the performance considerably when compared to the implementation of directional flooding algorithm without any pre-processing.

Saeed Rasoili et al. [18] proposed a new multi path routing algorithm for real time applications in wireless sensor network connectivity, backbone nodes work with duty-cycling and non-backbone nodes turn off radios to save energy.

Techniques look promising, there are still many challenges that need to be solved in the sensor networks.

www.ijeecm.org
networks namely QoS and Energy Aware Multi-Path Routing Algorithm (QEMPAR) which is QoS aware and can increase the network lifetime. Simulation results show that the proposed algorithm is more efficient than previous algorithms in providing quality of service requirements of real-time applications. It performed paths discovery using multiple criteria such as energy remaining, probability of packet sending, average probability of packet receiving and interference.

K. Vanaja and R. Umarani [19] deals with the fault management to resolve the mobility induced link break. The proposed protocol is the adaptive fault tolerant multipath routing (AFTMR) protocol which reduces the packet loss due to mobility induced link break. In this fault tolerant protocol, battery power and residual energy are taken into account to determine multiple disjoint routes to every active destination. When there is link break in the existing path, AFTMR initiates Local Route Recovery Process. vitality utilization.

III. PROBLEM STATEMENT/SPECIFICATION

Security issues in ad-hoc networks are similar to those in sensor networks and have been well enumerated. Energy efficiency is one of important key factor in designing a wireless sensor network system. Large energy consumption will affect the lifetime of the sensor networks. A WSN consists of a large number of small and cheap sensor nodes that have limited energy, processing power and memory storage capacity. Node’s role and functions relative to network communication or the network topology cause some nodes to die quicker than the others do. The main problem is that energy consumption is concentrated which have to transmit over long distance.

Most of the security mechanisms require the use of some kind of cryptographic keys that need to be shared between the communicating parties. The purpose of key management is to

- Initialize system users within a domain.
- Generate, distribute and install keying material.
- Control the use of keying material.
- Update, revoke and destroy keying material.
- Store, backup/recover and archive keying material.

However, key management is an unsolved problem in WSN. Traditional Internet style key management protocols based on infrastructures using trusted third parties are impractical for large scale WSNs because of the unknown network topology prior to deployment and serious node constraints such as limited power and limited transmission range.

IV. PROPOSED SYSTEM

We propose a novel design end-to-end routing protocol for finding shortest path and provide authentication of communication entities in the network. A secure and efficient end-to-end Secure Routing protocol. That can address energy balance and routing security concurrently in WSNs. Each sensor node needs to maintain the energy levels of its immediate adjacent neighboring grids in addition to their relative locations. Using this information, each sensor node can create varying filters based on the expected design tradeoff between security and efficiency we can protect the source location information from the adversaries. In this project, we will focus on two routing strategies for message forwarding: shortest path message forwarding, and secure message forwarding. After completion of authentication process, the group key manager will generate polynomial equation and generate six points. The group key manager will send any three points to individual user and using those points each user will generate secret key. Using this secret session key each user will perform the encryption and decryption of transferred message. Before performing encryption and decryption process, we can find shortest route by using end-to-end routing protocol. After that, the sender will encrypt message and convert into cipher format. The completion of encryption process the sender will send that cipher format data to destination node through the path. The destination node will retrieve that data and perform the decryption process. By performing decryption process, the destination node will get original message.

A. Advantages of Proposed System:
- Reduce the energy consumption
- Provide the more secure for packet and also routing
- Increase the message delivery ratio
- Reduce the time delay
- Reduce the overheads of encryption and decryption process
- Generating polynomial equation and generate six points.

B. Implementing Steps

1) Group Key Generation Process

The group key manager will generate group key for all users and use that key for encryption of broadcasting message. The implementation process of group key generation is as follows.

The group key manager will choose two random numbers and generate one secret key.
After generating those values the group key manager will generate polynomial equation as follows
\[ F(x) = \text{secret key} + a_0x + a_1x^2 \]
Here \( a_0, a_1 \) and secret key are generated randomly.

After completion of polynomial equation we can divide secret key into six parts. Where any three subsets will again reconstruct secret key. After dividing six parts the server will send any three subsets \((x_0, y_0), (x_1, y_1)\) and \((x_2, y_2)\) to individual user.

2) Generation of Secret Key by Users
Each user will retrieve the subset points and get the same secret key for all users. The generation of secret key can be done by using three subset points and again reconstruct the polynomial equation. The reconstruction of polynomial equation is as follows.

\[
\begin{align*}
L_0 &= (x - x_0)(x - x_1)(x - x_2) \\
L_1 &= (x - x_0)(x - x_1)(x - x_2) \\
L_2 &= (x - x_0)(x - x_1)(x - x_2)
\end{align*}
\]

By using those values, we can reconstruct polynomial equation by using following equation.
\[ F(x) = \sum_{j=0}^{2} y_j L_j(x) \]

After using that equation, we can get original polynomial equation and get the secret key. After that, the sender will choose the destination node id and send that id to group key manager. By using, those ids of sender and receiver the group key manager will find out shortest route by calculating shortest distance between nodes or users or group members.

3) Generation of distance matrix and finding Shortest Routing:
Module the group key manager will generate distance matrix and finding shortest route. The implementation process of distance matrix is as follows.
The group key manager will get all nodes of distance points and using those points, we can generate distance matrix. Take the each node distance points and calculate difference between each node put into matrix format. This process will repeat until completion of all nodes distance. The distance of each node to other node is as follow.
\[ d_{i} = (x_1 - x_2) + (y_1 - y_2) \]
Finding distance source node to other nodes by Using following formula
\[
\begin{align*}
\text{int max}=0; \quad \text{int min}=d_i;
\end{align*}
\]
After finding distance of each node, we can arrange the path from source node to destination node.
So that the data send through path and reached destination node.
After finding the path source node will transfer the data through path to destination node. Before sending data to destination node, the source node will encrypt the data and transfer to destination node.
The implementation procedure encryption and decryption is as follows.

4) Encryption Process:
The sender node will enter transferred message and convert that message to unknown format. By converting plain format, data into unknown format is known as encryption process. The implementation procedure of encryption process is as follows.
The sender node will take message and key as input of encryption process.
The sender node gets single character from message and converts into decimal value. Take the decimal value and key perform the xor operation until message length is completed.
After completion of xor operation take the each decimal value and convert into eight-bit binary format.
Take the each eight-bit binary data and partition into equal parts.
Take those equal parts and reverse those binary partitions. Performing this reverse process until the message binary bits of data is completed.
Take those binary reverse bits and generate 32 * 32-matrix format.
Take that matrix and perform circular rotation from outer circle to inner circle.
After completion of circular rotation read each eight-bit binary format and convert into decimal value. This process continues until all matrix data is completed.
Take those decimal values as cipher format data and send to destination node through the path. The destination node will retrieve cipher format data and convert into plain format data by performing decryption process.
The implementation process of decryption is as follows.
5) Decryption Process:
the destination node will perform decryption process for converting cipher format data into plain format.
The destination node will take cipher format data and key as input to decryption process.
The destination node takes each decimal value from cipher data and converts into eight-bit binary format data.
Take those binary format data and generate 32 * 32-matrix format.
Take those matrix format data and perform reverse circular rotation from outer circle to inner circle.
After completion of circle rotation process, take each eight-bit binary format data and performing equal sub partition.
Take those partitions binary data and perform the reverse process of both sub parts.
After completion of reverse process take each eight-bit binary format data and convert into decimal format until completion of cipher binary format data.
Take decimal value and key perform the xor operation between them until completion of all decimal values.
Take the xor data and convert into character format it will get plain format message.

By implementing those concepts we can improve the network efficiency and also provide more security of transferring message.

V. DIJKSTRA’S ALGORITHM-SHORTEST PATH

Working steps
First we'll describe Dijsksta's algorithm in a few steps, and then expound on them further:

STEP 0.
Temporarily assign C(A) = 0 and C(x) = infinity for all other x.
C(A) means the Cost of A
C(x) means the current cost of getting to node x
Step 1.
Find the node x with the smallest temporary value of c(x).
If there are no temporary nodes or if c(x) = infinity, then stop.
Node x is now labeled as permanent. Node x is now labeled as the current node. C(x) and parent of x will not change again.

STEP 2.
For each temporary node labeled vertex y adjacent to x, make the following comparison:
if c(x) + Wxy < c(y), then c(y) is changed to c(x) + Wxy
assign y to have parent x

STEP 3.
Return to step 1.
Before diving into a little more tricky graph, we'll stick with the original graph introduced above. Let's get started.
i. Step 0.
Temporarily assign $C(A) = 0$ and $C(x) = \infty$ for all other $x$. $C(A)$ means the Cost of $A$ $C(x)$ means the current cost of getting to node $x$.

The following graph has changed a little from the one shown above. The nodes no longer have labels, apart from our starting point NodeA and our goal NodeB.

VI. EXPERIMENTAL/SETUP AND RESULTS

![Fig. 3 System Architecture for Secret Sharing](image)

![Fig. 4 Route Prediction](image)

![Fig. 5 Security maintaining](image)
VII. CONCLUSION AND FUTURE SCOPE

This model captures evolving heterogeneous networks where intelligence is introduced at a fraction of nodes. Finally, proposed dynamic routing policies to be implemented in a network overlay. The threshold based policy that is optimal for overlays with non-overlapping tunnels, and provides alternate policy for general networks that demonstrates superior performance in terms of both throughput and delay. uniquely localize failures

REFERENCES


Author’s Profile:

MD RAIIYA completed B.Tech IT (Information technology) from Vignan Institute of Engineering for Womens Research Centre under the jntuk. M.Tech Dept. of Computer Science and Engineering from Avanthi Institute of Engineering and Technology narsipatnam, Andhra Pradesh. Under jntuk.

Dr. G SATYANARAYANA is Professor and head of the Department of Computer Science and Engineering, Avanthi Institute of Engineering & Technology - Narsipatnam. He did his PhD from GITAM University and his research interests in networks,information security , data warehousing and mining. he had published more than 10 national and international papers

Dr. C P V N MohanRao is Professor in the Department of Computer Science and Engineering, Avanthi Institute of Engineering & Technology - Narsipatnam. He did his PhD from Andhra University and his research interests include Image Processing, Networks, Information security, Data Mining and Software Engineering. He has guided more than 50 M.Tech Projects