© 2018 IJSRSET | Volume 4 | Issue 9 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Energy Efficient and Secure Routing Scheme in Wireless Sensor Network

Vidyadhar Mohite, Prof. Aparna A. Junnarkar
Department of Computer Engineering, Modern College of Engineering Savitribai Phule, Pune University Pune, Maharashtra, India

ABSTRACT

Nodes in many wireless sensor networks (WSNs) are powered by batteries with limited energy. Enhancing network lifetime and saving energy are two basic issues for WSNs. Some energy-saving routing algorithms can reduce total energy consumption of a WSN, however, they place too heavy burden of forwarding data packets on several key nodes so that these nodes quickly drain out available battery energy, making network lifetime shortened. These papers propose technique known as Secure Energy Efficient Routing Protocol for WSNs. Here in proposed system user first generate the network and form the clusters. After that cluster head and DCH is selected in each cluster. The work of DCH is the send location to the base station. The cluster members encrypt the data using encryption algorithm and send to the CH with hash of encrypt data. CH verifies data of each member. If any CH is faulty or not able to forward all members data then BS allocate the DCH as a CH and then CM send data to that CH and this CH forward the data to BS. The proposed protocol route the data securely by consuming less energy and enhance the network lifetime.

Keywords: Wireless sensor networks, reliability, routing protocol, energy efficiency.

I. INTRODUCTION

A wireless sensor network (WSN) is a shared sensing technology that can be used to observed physical phenomenon and can be easily deployed and therefore it is useful for various applications. A sensor network is made up of many distributed sensor nodes which requires an ad-hoc routing paradigm. Sensor networks application ranges from essential social problems such as environmental and habitat monitoring, traffic control, emergency scenarios, and health care, to economical issues such as production control and structure monitoring. In remote locations, many sensor network applications require thousands of sensor nodes which will be deployed this makes battery replacement impractical. Further, energy conservation plays a vital role for sensor networks. But the major issue of decreasing sensor node's energy consumption has not been resolved perfectly. If all sensor nodes transfer packets directly to the base station, the furthest nodes from the base station will die early.

To decrease useful energy consumption number of protocols have been developed. These protocols can be divided into three classes. In the first class protocol control the transmission power level at each node by increasing network capacity while keeping the network connected. Protocols in the second class make routing decisions depend on power optimization goals. Protocols in the third class control the network topology by finding which nodes should participate in the network operation (be awake) and which should not (remain asleep).

Hierarchical (clustering) method can aid in reducing useful energy consumption. Clustering is especially useful for applications that require scalability to hundreds or thousands of nodes. Scalability in this context intend the need for load balancing, efficient resource utilization, and data aggregation. Routing protocols can also employ clustering.

Existing routing protocols do not consider mobility in sensor nodes and in the BS, and these are not directly applicable to mobile WSN. In mobile WSN communication links may come up and fail very dynamically. The routing protocol has to take care of the connectivity problem also in such a WSN setup. There will be significant loss of data packets because of the failed links apart from all other reasons such as frequent death of sensor nodes or noise of the wireless links.

In this paper, a novel routing protocol, which is known as Energy-Efficient and Reliable Routing protocol for mobile wireless sensor network (E2R2), is implemented. The proposed protocol is a hierarchical one. The primary goal of this is to achieve energy efficiency and to provide connectivity to the nodes. The mobility of the nodes is considered while routing decisions are made. The objective behind such routing is that the data packets need to move through suitable routes in spite of node mobility and in presence of subsequent link failures.

In this paper we study about the related work done, in section II, the proposed approach modules description, mathematical modeling, algorithm and experimental setup in section III and at final we provide a conclusion in section IV.

II. LITERATURE REVIEW

In this paper [1], authors proposed Energy-Efficient and Reliable Routing Protocol for mobile Wireless Sensor Network (WSNs). The routing algorithm aims are to saves the energy in WSN and clustering algorithm are using for to improve the energy efficient performance in WSN. The clustering techniques are identifies the shortest path in WSN and it used for to select the cluster head. Optimized Ratio Energy Algorithm (OREA) are used for dissipate energy efficiently. To increase the lifetime of WSN Power-Aware Distance Source Routing (PADSR) clustering algorithm are used and it improve performance of the system.

In this paper [2], authors proposed system to identify problem in multi hop wireless networks for medical applications. Energy consumption has become a major problem of sustainable development of communication networks particularly in medical applications. In this they used a control and sleeping mechanism for obtaining routing strategy within maximum network energy efficient.

In this paper [3], authors present a new technique known as mobile wireless sensor networks (MWSNs). Previously methods in WSNs like data collection, network reliability, routing protocols, reliable data transmission and network topologies are not applied in MWSNs. They introduce a new features stability, security, and reliability in this. Reliability is important factors in MWSNs. Reliability are data transmission determines the practical value of MWSNs. For the comparisons they used a time, energy efficiency, delay, network size, reliability and scalability are used.

In this paper [4] authors proposed ICMDS (Inter-Cluster Multiple Key Distribution techniques for WSNs this scheme secure the entire networks. ICMDS techniques works in two phases for implementing a sensor nodes while communicating with the CH. A recovery phenomena is also stated at the time when a CH ceases to function due to its high energy consumption

In paper [5], authors present techniques known as energy efficient Adaptive Slice based Secure Data Aggregation (ASSDA) these scheme promote network performance under the limitation of node resource. Secure Data aggregation (SDA) it prevent network from being compromised and it is improve the lifetime of WSNs. These techniques improve the efficiency of data slicing, reduce energy consumption, prolong the network life time.

This paper [6] author proposed On-Demand Data-Driven energy familiar with routing protocol. Therefore, it can be better applied in sensor networks. Analyze result shows that the energy aware routing algorithm and it requires less energy than the traditional algorithms for most realistic cases.

In [7] Wireless Sensor Networks (WSNs), how to advance network Quality of Service (QoS) is a challenging problem. The important factors of QoS is Energy efficiency, network communication traffic and failure tolerance, which are closely related with the applied performance of WSNs. Quality of service routing protocol called as Directed Alternative Spanning Tree (DAST) is proposed to balance the above three factors of QoS directed tree-based model is used for data transmission more motivated and efficient. It is based on Markov, a communication state predicted mechanism is proposed to choose reasonable parent, and packet transmission to double-parent is submitted with alternative algorithm.

In this paper [8], author use technique such as Energy-efficient Routing Algorithm to Prolong Lifetime (ERAPL) and it is able to dramatically prolong network lifetime while efficiently expends energy. To find the optimal solution of the proposed programming problem Genetic algorithms are used. In sensor network data dissemination schemes are required for periodic low-rate flooding of data by allowing recovery from failure.

In paper [9] proposed multipath scheme and its results in several partially disjoint multipath schemes. It used for find that braided multipath is a viable alternative for energy-efficient recovery from isolated and patterned failures.

III. PROPOSED APPROACH

Problem Statement

Design an energy efficient, reliable routing and secure protocol in a wireless sensor network to protect the data loss and enhanced the network lifetime

Proposed System Overview

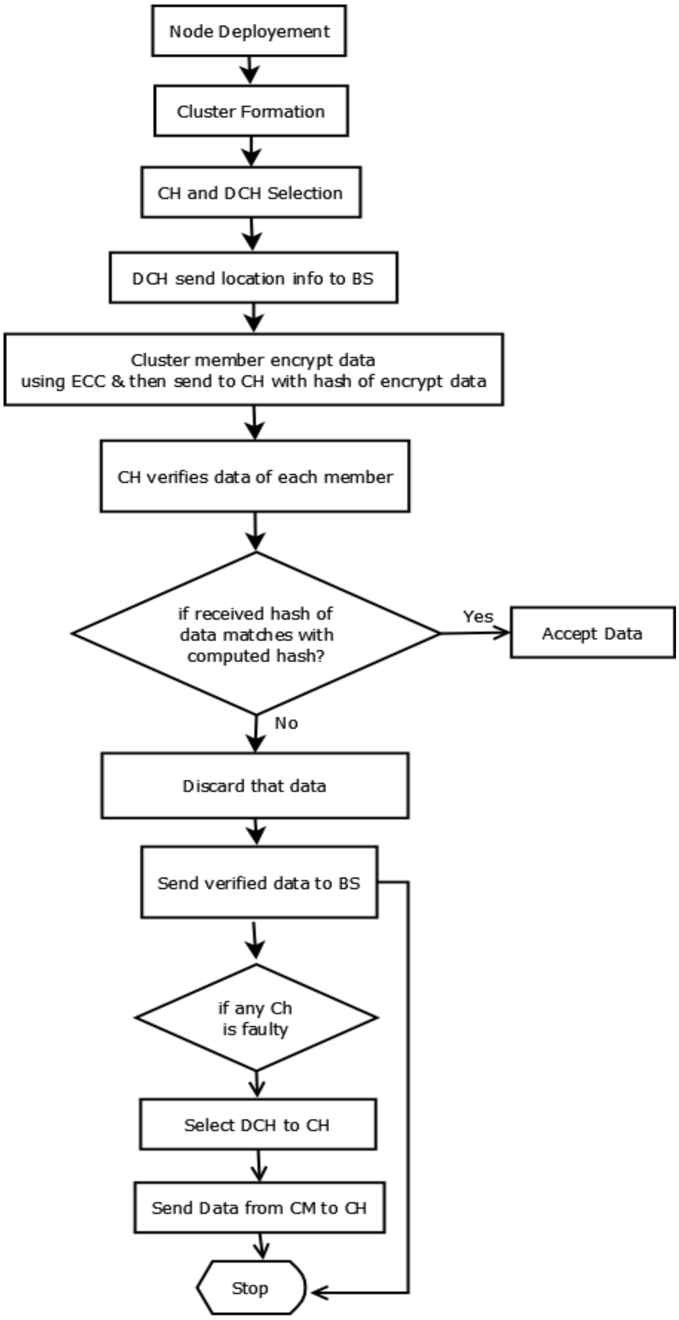

Figure 1. Proposed System Architecture

The proposed protocol is a hierarchical one. Contribution system secure the data using ECC encryption algorithm and also generate the hash of encrypted data. Here in proposed system user first generate the network and form the clusters. After that cluster head (CH) and DCH is selected in each cluster. The work of DCH is the send location to the base station (BS). The cluster members encrypt the data using ECC encryption algorithm and send to the CH with hash of encrypt data. CH verifies data of each member, if received hash of data matches with computed hash then accept the data, otherwise discard it and send verify data to the BS. If any CH is faulty or not able to forward all members data then BS allocate the DCH as a CH and then CM send data to that CH and this CH forward the data to BS.

1. Generation of Network: It generate network of sensor nodes. Those nodes are connected through the edges.
2. Formation of Cluster: The clustering process is performed in network system; the sensor nodes are divided into group of clusters. Numbers of clusters are generated in the sensor network.
3. Selection of Cluster Head: Cluster head is selected from clusters. Aggregator selections are done use of highest remaining energy of nodes.
4. Selection of DCH: DCH is selected from clusters. In this system two DCH are selected. DCH nodes are called as cluster management nodes. DCH responsibility of collecting current location information from the cluster members and communicating with BS.
5. Encryption and Hash Generation: Cluster member encrypt the data using ECC encryption algorithm. It is lightweight method and provides the security to the data. Also CM generates the hash of encrypted data. CM sends this encrypted data along with hash of data to the CH.
6. Data Verification: CH verifies data of each member. If received hash of data matches with computed hash then accepts the data otherwise discard the data.

IV. ALGORITHM

Input: Sensed Data
Output: Energy efficient secure data routing at Sink Node
Process:

1. Create a network graph as Graph g(v) where; V is vertices/nodes.
2. Do the clustering on the numerous nodes and divide the nodes into numerous of clusters.
3. Compute The No Of Nodes, Energy, Speed, And Coverage Radius In Each Cluster.
4. Flag F=0 should be Zero and F=1 for Previous Round of Cluster Head.
5. On The basis of all parameters Calculate Threshold and set the Cluster Head.
6. Calculate percentile score of degree and energy of node and on the basis of it select two DCH.
7. Compute the hash of data
8. Collect the data from Each Node, encrypt it using ECC and send to cluster head along with hash of encrypted data.
9. Checks the data at cluster Head, if received hash of data matches with computed match then accept the data, otherwise discard the data.
10. Send verified data to the BS.
11. If any CH is faulty then select DCH as a CH and send data from CM to that CH and then this CH forward the data to BS.
12.

V. MATHEMATICAL MODEL

Let T be a system such that,
T= {Input, Process, Output}
Input:
Sensing Information
I= {I1, I2, ..., In}
I is a set of input represents sensing information needs to be sending to base station.
Process
1. Set of sensor nodes.
   N= {N1, N2, ..., Nm}
   S is a set of sensor nodes in a network.

Set up phase

2. Cluster Formation

C = {C1, C2, ..., Cn}

F is set of clusters created in set up phase.

Each cluster contains number of sensor nodes.

3. Cluster Head Selection

Selection of Cluster head

CH= {CH1, CH2, ..., CHn }

CH is set of cluster heads, which are use full for communication among clusters.

5. DCH Selection

In this network two DCH are selected in each cluster.

DCH= {DCH11 DCH12, DCH21 DCH22, ..., DCHn1 DCHn2}

To select CH and DCH following process used.

- Percentile Score (P_d) of a sensor node for degree:

Pd = {(number of candidate nodes who have lower degree (d) than the degree of the candidate node concerned, inside the cluster) /N} × 100

- Percentile Score (Pe) of a sensor node for energy level:

Pe = {(number of candidate nodes who have less energy level (e) than the energy level of the candidate node concerned, inside the cluster)/N} × 100

- Percentile Score (Pm) of a sensor node for mobility:

P_m = {(number of candidate nodes who have less mobility level than the mobility level (m) of the candidate node concerned, inside the cluster)/N} × 100

- Cumulative Credit Point (CCP) for each node inside a cluster :

$CCP = (w_1)P_d + (w_2)P_e + (w_3)P_m$

where w_1, w_2, and w_3 are weight factors are given to different parameters for Degree, Residual Energy, and Mobility

$$w_1 + w_2 + w_3 = 1$$

6. Location Information sending

L = {L1, L2, …., Ln}

L represents the set of location information's.

7. Data Sending

D = {E, H}

Where, D represent the data send by CM to CH in which contain,

E = Encrypted data

H = Hash of encrypted data.

8. Verified Data

V = Represent the verified data from CH. If received hash of data is matched with computed hash then accept it, otherwise discard the data.

Output:

The secured routed data at base station.

VI. RESULTS AND DISCUSSION

A. Experimental Setup

The system is built using Java framework on Windows platform. The Net beans IDE are used as a development tool. For network generation Jung tool is used. The system doesn't require any specific hardware to run; any standard machine is capable of running the application.

B. Experimental Result

Table 2 describes the energy required in Joules after attack energy and before attack energy in existing system.

Table 2. Energy Consumption Comparison in Existing System in before and after attack

	After Attack Energy	Before attack Energy
Energy in J	800	1000

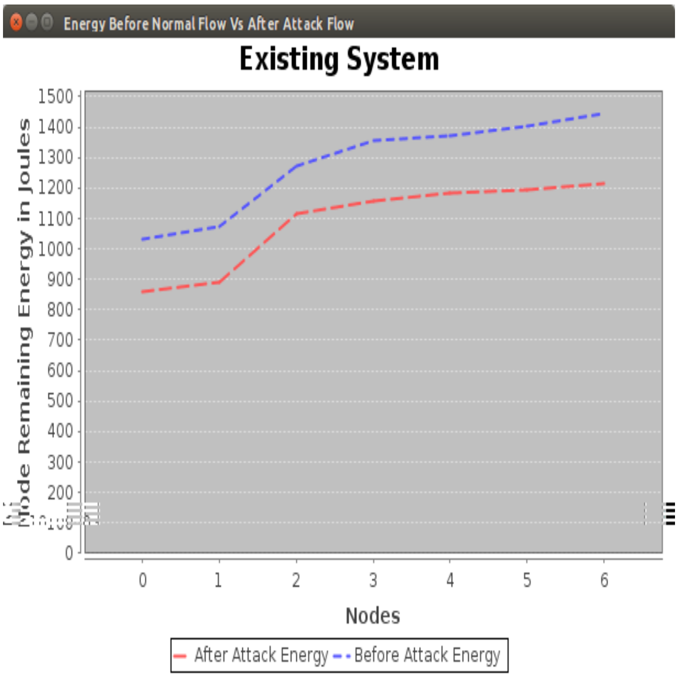

Figure 2. Existing System Energy Flow Graph

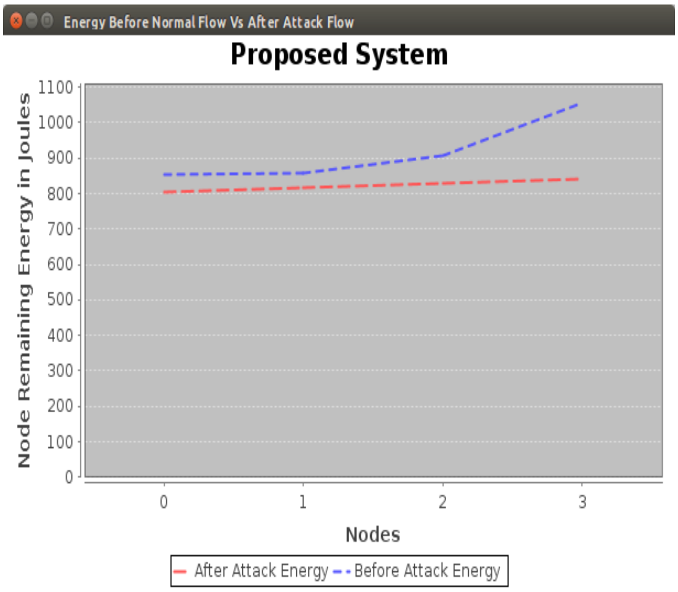

Figure 3. Proposed System Energy Flow Graph

Figure 2 represent the graphical comparison of energy consumption in after attack energy and before attack energy in existing system. X axis represent the systems and y axis represent the energy consumed in Joules. After attack energy requires 800 J energy and before attack energy requires 10000Joules of energy for data routing from cluster member to base station through cluster heads and DCH.

Table 3 describes the energy required in Joules after attack energy and before attack energy in proposed system.

Table 3. Energy Consumption Comparison in Proposed system in before and after attack

	After Attack Energy	Before attack Energy
Energy in J	800	1000

Figure 3 represent the graphical comparison of energy consumption in after attack energy and before attack energy in proposed system. X axis represent the systems and y axis represent the energy consumed in Joules. After attack energy requires 800 J energy and before attack energy requires 10000 Joules of energy for data routing from cluster member to base station through cluster heads and DCH.

VII. CONCLUSION AND FUTURE SCOPE

This paper proposed an energy efficient and secure routing protocol to enhance the network lifetime in wireless sensor network. Each cluster contains one CH node and the CH node is assisted by two DCH nodes, which are also called cluster management nodes. If any CH is faulty or not able to forward all members data then BS allocate the DCH as a CH and then CM send data to that CH and this CH forward the data to BS. Also the cluster members encrypt the data using ECC encryption algorithm and send to the CH with hash of encrypt data. CH verifies data of each member, if received hash of data matches with computed hash then accept the data, otherwise discard it. This system provides energy efficient and secure routing protocol and enhance network lifetime.

VIII. REFERENCES

[1]. Hiren Kumar and Deva Sarma, "E2R2: energy-efficient and reliable routing for mobile wireless sensor networks", 1932-8184 IEEE 2015].

[2]. A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," 2000].

[3]. A. Manjeshwar and D. P. Agarwal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," in Proc. 15th IPDPS Workshops, 2000, pp. 2009–2015.

[4]. A. Manjeshwar and D. P. Agarwal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," in Proc. IPDPS, 2002.

[5]. O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks," IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366–379, Oct.–Dec. 2004.

[6]. M. Ye, C. Li, F. Chen, and G. J.Wu, "EECS: An Energy Efficient Clustering Scheme in Wireless Sensor Networks," Int. J. Ad Hoc Sens. Netw., vol. 3, no. 2/3, pp. 99–119, 2007.

[7]. M. Liu, J. Cao, G. Chen, and X. Wang, "An Energy-Aware Routing in Wireless Sensor Networks," Sensors, vol. 9, pp. 445–462, 2009.

[8]. P. Ji, C. Wu, Y. Zhang, and Z. Jia, "DAST: A QoS Aware Routing Protocol for Wireless Sensor Networks," in Proc. ICESS, 2008, pp. 259–264.

[9]. Y.-H. Zhu, W.-D. Wu, J. Pan, and Y.-P. Tang, "An Energy-Efficient Data Gathering Algorithm to Prolong Lifetime of Wireless Sensor Networks," Comput. Commun., vol. 33, no. 5, pp. 639–647, Mar. 2010.

[10]. D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks," ACM SIGMOBILE Rev., vol. 5, no. 4, pp. 10–24, Oct. 2001.