Malicious Node Identification In Energy Efficient Trust Node Based Routing Protocol (M-Eetrp) For Lifetime Improvement In Wsn

Nandoori Srikanth, Muktyala Siva Ganga Prasad

Abstract: ***Uneven Deployment of sensor nodes, Irregular terrains, energy limitations, malicious attacks, and interfered wireless links, are the key parameters which degrades the performance of WSN. To improve lifetime of the network sensor nodes are driven into sleep states, once they complete their sensing task. Irregular Terrains like military areas, plateaus suffers with uneven deployment of sensor nodes, and malicious attacks. Mobile node based data gathering is the efficient technique for lifetime maximization in WSN fixed up in irregular terrains like plateaus and also to avoid security based issues. The mobile node based data gathering techniques also suffer from energy limitations of mobile nodes. This paper explores an effective method of utilizing energy resources of mobile nodes without any malicious attacks by proposing "Malicious node identification in energy efficient trust node based routing protocol". Malicious node identification is the key parameter in WSN to make the network more energy efficient. This Protocol gives better results compared with existing algorithms with the Improvement of Network lifetime by 67% and energy consumption as 30%.***

Index Terms: ***WSN, Data aggregation, Trust Node, malicious node, Built in Self-Test.***

I. INTRODUCTION

The WSN has opened an attracting possibility of transforming gross mechanical actions into subtle sensory responses [1]. WSN is an arrangement of group of sensor nodes to sense the physical environment and communicate through wireless links. These sensor nodes has less maintenance, and their energy resources follows scavenging principle. The performance parameters of WSN depend on terrain structure, quality of wireless links, energy resources, uneven deployment etc. [2]. Irregular terrain structure is also one of the key parameter which degrades the performance of WSN. To overcome this problem, mobile nodes are introduced among clusters for data collection, due to mobile based data gathering high end data isolation can be provided to sensor nodes. The data gathered from various sensor nodes are aggregated and send to the base station and these smart sensors nodes works on command controlled strategies that have one or more memory unit, sensors, processor, and an actuator and power supply [3]. Energy efficiency is the key research area in WSN which leads to improve network lifetime, link quality, and throughput. In this paper efficient utilization of energy resources is greatly enhanced by improving cluster based routings; these cluster based routings can be improved by introducing mobile data collectors in sub clusters for data collection. These mobile nodes (Mobile Data Collectors - MDC) collect data individually from each node and forward to cluster head after data aggregation [4]. Along with MDCs some high energized nodes (Trusted nodes) are deployed in sub clusters for data transmission to MDCs in even number of rounds. These sensor nodes can maintain in sleep state up to a long time, until the mobile node gives wake up notification.

Motivation of the Paper:

Even mobile node based data aggregation gives better results in irregular terrains [5], it suffers from energy limitations. The mobile node (MDC) has to move around the sub cluster, and collect data from each sensor node , and forward to cluster head [6]. The selection of mobile node is based on its threshold level, if mobile node energy is less than threshold level, then the mobile node is not used for data collection [9]. To overcome this problem, and also to improve energy efficiency, A Malicious Node Identification in energy efficient trust node based routing protocol (M-EETRP) is proposed, in which cluster is divided into sub clusters and each sub cluster is assigned with at least one mobile node.

Contributions of the Paper:

In this research, all nodes are organized into clusters, again each cluster is divided into sub clusters, and each sub cluster is assigned with a mobile node for data collection. In each sub cluster some high energy nodes are assigned as trusted nodes. These trusted nodes are used to minimize the energy consumption of mobile nodes during data aggregation.

- Malicious node identification in energy efficient trust node based routing protocol (M-EETRP) is proposed, which aims to minimize energy consumption for data gathering and transmission in WSN.
- M-EETRP protocol is utilized to optimize the sub clustering algorithm rules to upsurge the network lifetime, based on the applications like plateaus and military areas.

Revised Manuscript Received on May 10 ,2019

Nandoori Srikanth, Department of ECE, Koneru Lakshmiah Educational Foundation, Green Fields, Vaddeswaram,,India.

Muktyala Siva Ganga Prasad, Department of ECE, Koneru Lakshmiah Educational Foundation, Green Fields, Vaddeswaram,,India.

- This protocol differs from the traditional clustering approaches due to uneven deployment and placement of sensor nodes in plateaus.
- M-EETRP utility system to concurrently ponder two elements: trustworthiness of nodes and energy efficiency.

II. Methodology

In wireless sensor networks, to improve lifetime, energy efficiency, several protocols are proposed based on trust values of nodes. In existing works, mobile nodes (MDCs) are introduced for data aggregation in fixed wireless sensor networks and forward that sensed data to cluster head. This kind of proposals [7] [8] gives good results in military applications, plateaus, hill and valley places, etc. In this research, malicious node identification in energy efficient trust node based routing protocol is proposed. Fig. 1 shows the scenario of trust node based routing protocol in WSN. In this work, cluster is divided into sub clusters and some high energized nodes in each sub cluster are assigned as trusted nodes. In sub cluster the mobile nodes are moving around the sub cluster to gather the data in odd number of rounds like 1, 3, 5 etc. In even rounds 2, 4, 6 etc. data collection is done by trusted nodes and forward to MDC. In even rounds of data collection, the MDCs are in static condition, they get the data from trusted nodes. This alternative round of data collection gives better results and increase the lifetime of the network in up to a great extent. When Mobile Node (MN) comes near to the sensor node (SN), then Sensor node gets off from sleep mode and sends data to MN. If the mobile node is stationary, the trust node will send the data to MN.

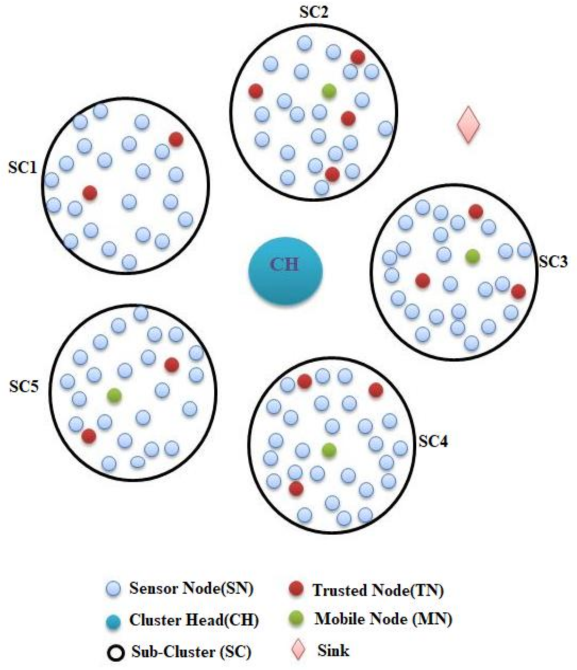

Figure 1. Scenario of trusted node in WSN

A. Energy Consumption model for proposed algorithm

The Energy consumed by mobile data collector [9] to collect data from each sensor node with a message bit length 'k' is given as

$$E_{(MDC)} = k \times E_{(elec)} + k \times E_{(s)} \times r_h^2 \quad (1)$$

Where E $_{(MDC)}$ is the Energy consumed by Mobile data collector node, and r_h is the average distance between mobile data collector and cluster head.

$$r_h^2 = \frac{L^2}{2\pi K} \quad (2)$$

RE is the residual energy consumed by the cluster head for R bits of data transmission in particular round, and it is expressed as

$$E = \left(\frac{T}{f} - 1\right) \times k \times E_{(elec)} + \frac{T}{f} \times k \times E_{(d)} + k \times E_{(elec)} + \propto (fs) \times r_d \quad (3)$$

Where,

T is the number of nodes equally dispersed over the square area L × L.

$E_{(d)}$ is the energy consumed per bit report to the base station, and r_d is the distance between cluster head to the base station.

B. Malicious node identification

Malicious node identification is one of the complex challenges in WSN. In these types of applications, if MDC is malicious, then the entire data sensed by the sub cluster is corrupted at the receiver end. So identification of malicious node is very important for cluster head. In present research, BIST (Built in self-test) based malicious node identification is proposed to identify malicious nodes in an effective way and reducing the energy consumption of nodes. The entire sub cluster data depends on mobile node of particular sub cluster. Hence data accuracy as well as data transmission within time slot is also important. Before every odd round of data collection, the BIST is performed by CH and trusted nodes. There are two cases to check or to identify whether the mobile node is a malicious or not.

Case-I: if the mobile node able to send the data, but it is a fault data. (Fault)

Case-II: if the mobile node able to send the correct data, but it is received as a fault data due to link failure. (Link fail)

In Case – I, if mobile node transmits in-correct pre-defined data sequence to cluster head, then CH instruct trusted nodes to check the MDC by receiving predefined data sequence from MDC to trusted nodes. If trusted nodes receive data in-correctly, then the CH will decide that MDC is a fault node, and removed from the network.

In Case – II, , if mobile node transmits in-correct pre-defined data sequence to cluster head, then CH instruct trusted nodes to check the MDC by receiving predefined data sequence from MDC to trusted nodes. If trusted nodes receive data correctly, then the CH will decide that an error is occurred due to link failure but not due to mobile node. Then the link connected between MDC and CH is discarded and replaced with another.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Algorithm of Malicious Node Identification

```
R = no. of rounds
Sequence formation ←R
No. of bits in sequence= [0, 1]
X falls in the condition
 if
MN → $\sum_{n=1}^{N}$ seq[1]
    And
MN → $\sum_{n=1}^{N}$ seq[0]
Denote
X = no malicious node is detected
Else
Y= malicious node is detected
End if
```

III. PERFORMANCE ANLYSIS

. In previous works, authors proposed cluster based routings by introducing a mobile data collector among clusters, and further it can be improved by assigning mobile nodes to sub clusters for data collection. In this research, the energy consumption is greatly reduced at node level. Election of MDC is based on its threshold level, and its previous malicious behavior. This M-EETRP algorithm is compared with NBBTE (Node Behavioral Strategies Banding Trust Evaluation Algorithm), and SNIDP (Suspicious node information dissemination protocol), GLBD, MLPA techniques [10]. The M-EETRP performance is evaluated under the following metrics: (i) Energy efficiency (ii) Energy Consumption (iii) Throughput, (iv) Lifetime of the network

A. Results and Discussions

The outcomes of conventional algorithms SNDP, MLPA, NBBTE, and GLBD are compared with proposed algorithm M-EETRP. The network simulator-2 is used for implementation and compares the outcomes of proposed system with existed protocols.. The M-EETRP protocol is implemented with number of nodes 50, with uneven deployment in the area of 1320*1032 m with in the field of coverage as shown in Table 1. The base station is located inside the sensing field i.e. at center of sensing area.

Table-1 Simulation parameters

Parameters	Values
Simulation Period	100ms
Coverage Area	1320*1032
No of Nodes	51
No of sink node	1
No of mobile node	5
No of Sub cluster	5
No of Cluster Head	1
Traffic Type	CBR
Agent Type	UDP
Routing protocol	AODV
Initial power	100 J
Transmission Power	1 J
Receiving Power	1 J
Queue Type	Drop-Tail

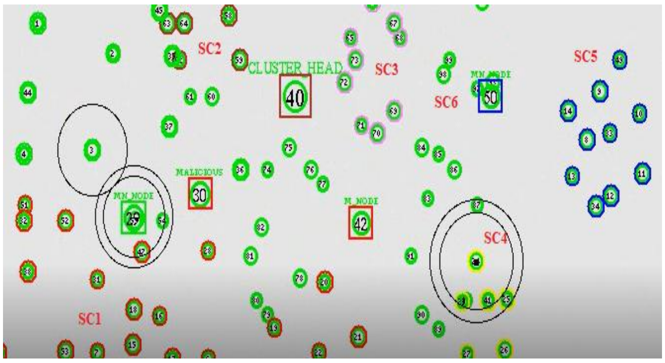

Figure 2. Malicious node identification in EETRP

After few rounds of data collection, MDC nodes are forwarding data to the BS through CH. From proposed M-EETRP protocol network can check mobile data collectors' malicious behavior. From figure 2 MDC 30 is identified as malicious node during simulation.

Energy Consumption

The Energy consumption of the network includes energy consumed by the sensor nodes, transceiver, processor, and memory unit. The energy consumption and lifetime improvement have linear in relationship. The figure 3 shows energy consumption comparison graphs of various protocols. The energy consumption of M-EETRP protocol is 30% and other EETRP is 32%, NBBTE algorithm is 65%, SNDP is 80%.

Network Lifetime

The network lifetime is depends on number of data gathering rounds that those sensor nodes can withstand with minimum residual energy. Lifetime is the key parameter which decides throughput and robustness of the network. The lifetime of the node depends on energy consumption of sensor node, and remaining residual energy of the node. The figure 4 shows lifetime comparison graphs of various protocols. The lifetime of M-EETRP protocol is 67.89% and other NBBTE algorithm is 35%, SNDP is 20%, EETRP is 66%,.

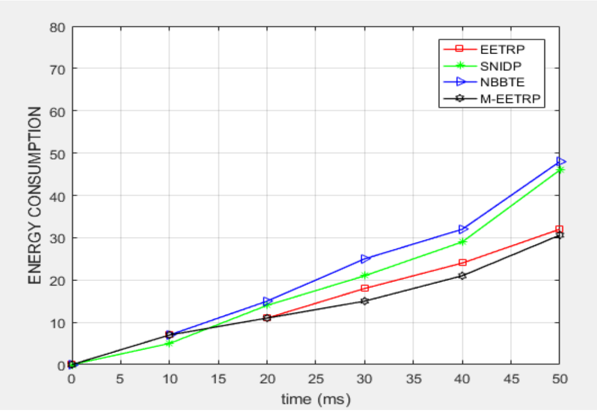

Figure 3. Energy consumption comparison graph with existing system

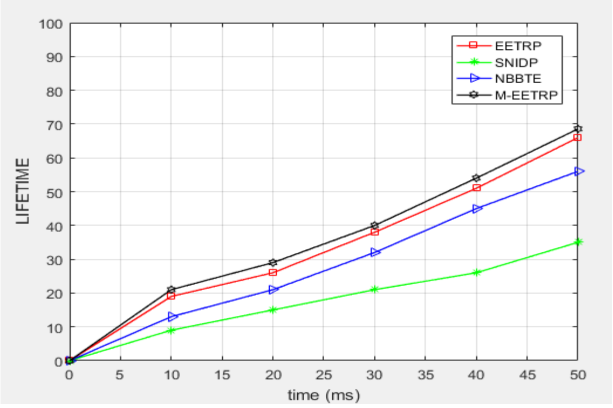

Figure 4. Network lifetime comparison with existing systems

Table-2 Comparison between existing and proposed protocols

PARAMETER	NBBTE	SNIDP	EETRP	M-EETRP (proposed)
Packet delivery rate	77%	72%	97.77%	97.82%
Control overhead	1265 packets	1564 packets	2373 packets	1948 packets
Energy Consumption	65%	80%	32%	30.68%
Energy efficiency	35%	20%	68%	68.57%
Throughput	542 Kbps	244 Kbps	1153 Kbps	1246 Kbps
Loss	432 packets	564 packets	154 packets	150 packets
Lifetime	35%	20%	66%	67.89% (1400 Rounds)

IV. CONCLUSION

Cluster based routings are introduced to give efficient results in irregular terrain structures. Mobile data collector based routing is an efficient routing technique compared to traditional approaches. Due to this M-EETRP protocol, data isolation is highly provided and malicious behavior of nodes can be easily identified. The Mobile data collector collects data from sensor nodes in first round of data collection, and in next round MDC can collect data from trusted nodes. This simultaneous trust based routing gives a good increment in lifetime of network. In this research again lifetime is increased by introducing malicious behavior identification techniques. The performance of this M-EETRP routing protocol is assessed and compared based on energy consumption, throughput, lifetime, PDR, energy efficiency as shown in Table 2.. Most of the energy is saved due to introducing of mobile nodes for data collection. Apart from this we are reducing the load for mobile data collector also. In general, the mobile data collectors have high energy resources. But it is not possible in all terrains. This M-EETRP gives better results in military and plateaus, and irregular terrains where multi-hop communication is complex. This work is further enhanced by Trust node based routing to improve lifetime of the network.

REFERENCES

1. L F. Akyildiz, T. Melodia, and K. R. Chowdhury,: 'A survey on wireless multimedia sensor networks', *Computer Netw. (ElseVier)*, Mar. 2007, 51, (4), pp. 921-960.
2. Mhatre and C. Rosenberg, 'Design guidelines for wireless sensor networks communication: clustering and aggregation', *Elsevier Ad Hoc Networks*, Jan. 2004, 2, (1), pp. 45-63.
3. Awwad, Samer A. B. and Ng, Chee Kyun and Noordin, Nor Kamariah and A. Rasid, Mohd Fadlee (2011) *'Cluster based routing protocol for mobile nodes in wireless sensor network'. Wireless Personal Communications*, 61 (2), pp. 251-281.
4. Po-Han Huang, Shi-Sheng Sun, and Wanjiun Liao, 'GreenCoMP: Energy-Aware Cooperation for Green Cellular Networks', *IEEE Transactions on mobile computing*, 2017, 16, (1), pp. 143-157.
5. Syed Muhammad Sajjad, Safdar Hussain Bouk, and Muhammad Yousaf, 'Neighbor Node Trust Based Intrusion Detection System for WSN'. *Procedia Computer Science*, 2015, 63, pp. 183-188.
6. Poornima, A.S. & Amberker, B.B.. (2011). Secure data collection using mobile data collector in clustered wireless sensor networks. *Wireless Sensor Systems, IET*. 1: 85 – 95
7. B. A Mohan, H. Saroja Devi, 'A hybrid approach for data collection using multiple mobile nodes in WSN (HADMMN)'. *In. Proc. IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2016, 5, pp. 736-739.
8. Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku, and Zhou Su, "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation". *Proceedings of the Symposium on Simulation of Systems Security (SSSS'08)*, Ottawa, Canada, 2008, April 14 – 17, pp. 836-843.
9. Sayyed, Ali & Buss Becker, Leandro. (2015). Optimizing speed of mobile data collector in Wireless Sensor Network. 1-6. *International Conference on Emerging Technologies (ICET)*
10. Nandoori Srikanth, Muktyala Sivaganga Prasad, "Energy Efficient Trust Node Based Routing Protocol (EETRP) to Maximize the Lifetime of Wireless Sensor Networks in Plateaus " *Internationl journal of Online and Biomedical Engineering*, 2019, 15, (6), pp. 113-130.
11. Srikanth, N. & GangaPrasad, M.S. (2019). Green comp based energy efficient data aggregation algorithm with malicious node identification (geed-m) for lifetime improvement in wsn. 8(4), COMPUSOFT, An International Journal of Advanced Computer Technology. PP-3117-3125.
12. Nandoori Srikanth and Muktyala Siva Ganga Prasad, "Energy Efficient Clustering Protocol using Genetic Algorithm", Journal of Engineering Science and Technology Review 11 (6) (2018) 85 - 93

AUTHORS PROFILE

1. **Nandoori Srikanth** is one of the part time Ph.D. scholars in Koneru Lakshmiah Educational Foundation, from the department of Electronics & Communication Engineering. He published many research papers in various reputed journals and he is working as an Assistant professor in NRI Institute of Technology. His Research area is Wireless Sensor Networks. His research interests are wireless ommunications,

2. **Muktyala Sivaganga Prasad** is one of the Professors in Koneru Lakshmiah Educational Foundation, from the department of Electronics & Communication Engineering. He published many research papers in various reputed International journals and he guided many more researchers in the fields of wireless communication, Antennas and wireless sensor networks. His research interests are wireless communications, Antennas and signal processing.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication