ENERGY AWARE FACTOR BASED LOCATION SECURITY GREEDY ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORK

Parthasaradhi Mayasala

Research Scholar, Department of CSE, SVCE-Tirupati, JNTUA-Anantapur,
Ananthapuramu, AndraPradesh 515002, India
urssaradhi@gmail.com

Dr. S Murali Krishna

Professor, Department of CSE, SV College of Engineering, Karakambadi Road
Tirupati, AndraPradesh 517507, India
muralikrishna.s@svcolleges.edu.in

Abstract

In wireless sensor networks, all the sensors are deployed at untrustworthy environments and base station is far away from the sensors. To increase the lifetime of the sensor network entire region is divided into clusters. The sensors in the cluster have been communicated thorough the cluster heads. All the sensor in the network are busy in sensing, transmission of the messages, due to this any sensor will gone into dead state which causes delay in data transmission. This affects the traffic overload in other paths. To overcome this problem we are proposing an energy aware factor based location security algorithm which transmits the messages in a route which is selected based on reliability and energy levels of the different routes. The proposed methodology also includes homorphic energy-based encryption encrypts the data related to the sensor node with less computational complexity. Heuristic conditions are used for optimizing the sampling rate and battery level for tackling the battery capacity constraints of the wireless sensor nodes.

***Keywords*: Wireless Sensor Network, Location Privacy Preserving, Energy Based Homomorphism Encryption**

1. Introduction

Wireless Sensor networks cope with the hard trouble like node replication, node failure, packet losing and change with the aid of an adversary to disrupt conversation. Many schemes have been proposed to mitigate these issues but only some can efficaciously and correctly perceive the severity of the network [1]. In addition Wireless Sensor networks are prone to attacks on data classifications. Widespread adoption of WSNs, particularity for mission-vital tasks, hinges at the improvement of sturdy safety mechanisms in opposition to such attack [2]. The symmetric-key based schemes calls for complex key management, lacks of scalability, and isn't always resilient to massive numbers of node compromise attacks for the reason that message sender and the receiver should percent a secret key [3].

In this paper, data gathering can be performed simultaneously with Greedy Protocol. Once a node depletes its energy, its sensing quality and overall network connectivity degrade. Energy based homomorphism encryption undergoes the key generation, encryption and decryption process on the basis of the energy level. Once the data received to the sensor and it finds the best paths to transmits the data using Energy Aware Factor based Location Security.

The remainder of this paper is organized as follows: In Section 2, the literature review on mobile sink scheduling framework towards energy harvesting and throughput maximization is provided. Details of assumed models to the work are given in Section 3. The proposed work is given in Section 4. The results are compared with existing techniques are provide in Section 5. The paper is concluded in Section 6 with conclusion and future research directions.

2. Related Works

There exist many approaches to the problem of mobile sink routing in WSNs towards achieving throughput maximization and energy conservation through data encryption technique. The several methods have been proposed to increases the location of the source in wireless sensor networks from baseline routings to context-aware location privacy (CALP) [4]. J Lopez at all were proposed a mechanism to evolve the privacy to the IOT [5]. H Wang at all and Jing Yang Koh at all were developed probabilistic based scheme to increase the Source Location Privacy [6-7]. Q Zhou at all proposed DLSA (Dark-Light Stripe Alternation) against the Global Attacker Hiding in FOG [8]. All these methods are considering the basic encryption and decryption schemes to prevent the node compromising attacks which makes huge computations and require huge resource consumption. All these techniques are using Forward Aware Factor based algorithms for path selection.

3. Assumed Models For Work

3.1. *Network model -wireless sensor network*

The wireless sensor network has a group of sensors with unique address. This entire network is divided into regions with regional heads. Each region is again divided into clusters based on fastest message delivery ratio. Each cluster is identified using unique address. Every cluster has a special node known as cluster head [9]. Cluster head has the special features for long life existence and it has the capabilities of communicating with all the sensors and with base station either single of multi hop channel. All the sensor nodes with in a cluster are directly or indirectly communicated with cluster head and vice versa. The cluster heads which are nearer to the base station are directly communicated with it and the cluster heads which are far to the base station are communicated through the regional heads. Routing of the data towards base station can be employed using graph model which helps to create routing table with dynamic updates easily. The below two diagrams are depicting the communication of the sensors with the base station.

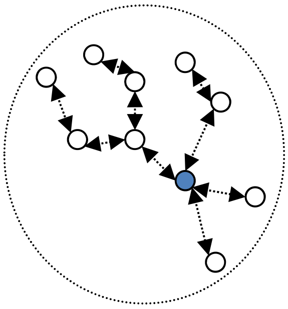

Fig. 1. Individual sensor communicating with cluster heads

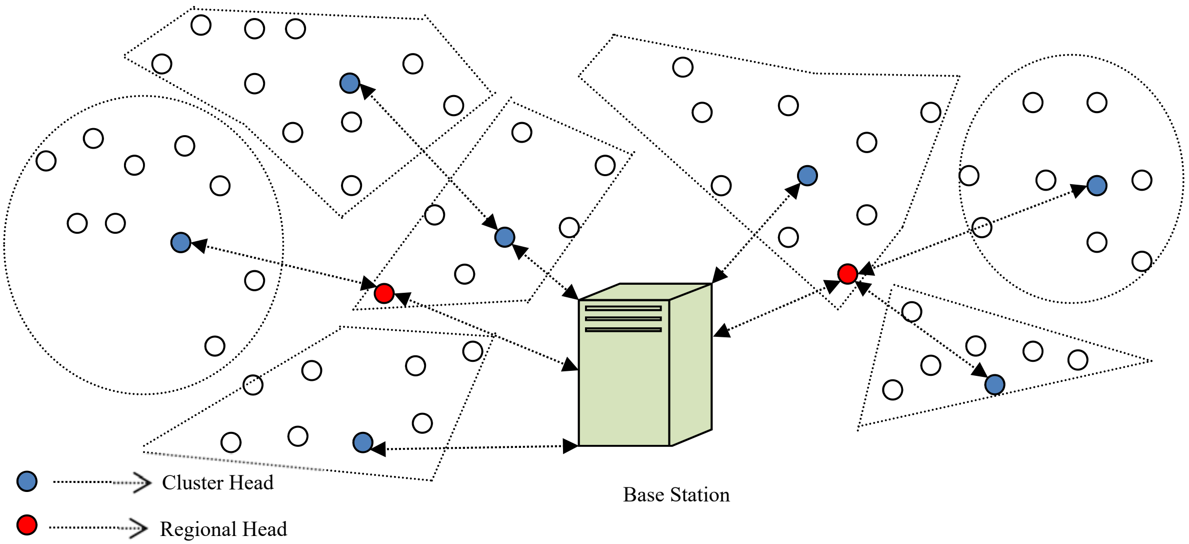

Figure 2: cluster heads communicating with base station

The regional nodes are selected by the base station and cluster heads are selected by the regional heads based on the characteristics of the nodes towards increasing the life time of the network.

3.2. *Data classification attack model*

The data classification attack is launched by unauthorized to obtain the information of the sensor information maliciously. The malicious nodes establish the attack on multiple gateways through the several intermediate nodes in order to gather the information. In addition it blocks the energy charging of the mobile sink. The Node characteristics are taken as features and it is extracted using Kalman Filter and Linear Regression mechanisms [10-11].

3.3. *Forward Aware Factor Constraints*

In this Module, we establish a model based on the forwarding node details about energy and node utilization of data or load. The descriptions and definitions are as follows.

- All sensor nodes are isomorphic, and that they have restricted abilities to store, compute, and communicate data. The power of sensor nodes is restricted and Nodes die after laborious power entirely. Locations of Nodes and Sink do now no longer extrade after being fixed and a node can't reap absolutely the function depend upon its very own vicinity device [12].
- Nodes can range transmission electricity consistent with the distance to its receiver. The cluster head can broadcast message to all sensor nodes with inside the cluster. The distance among the sender and receiver may be computed primarily based totally at the obtained signal strength. Regional heads nodes aren't decided on the beginning; at the contrary, they spring up in the course of the topology evolution. Importance nodes have extra connections, whose degree and density are substantially better than neighbour nodes. As time is going on, the quantity of statistics turns into large with the boom of nodes [13].

4. Proposed Model

In this section, System infrastructure and framework is discussed as it is composed of cluster heads and some fixed sensor nodes to establish a greedy routing for energy aware factor towards data forwarding. Cluster head is employed to collect the sensing data with inclusion of spatial and temporal information of the nodes. The sensor node shares the details of it using energy based homomorphism encryption. When sensor detects an event then the message route will be selected based on reliable transmission and energy level of all the sensors in the path towards cluster head.

4.1. *Energy based homomorphism encryption*

In this section, energy based homomorphism encryption model is determined based on energy computation of the node through cipher text generation cycle. It generates the cipher text based on the energy constraints of the nodes. Process of the homomorphism encryption includes following process:

Step-1: Key generation at Sender
- Key is considered is odd number $K \xi [1,P]$

Step-2: Encryption
- Encrypt (P, M)
- $C = K + M \bmod P$

Step-3: Decryption
- Decrypt (P, C)
- $M = C + P - K$

Where, C is a Cipher Text, K is a Key, M is a Message and P is a Energy Level of receiver

4.2. *Energy aware factor based location security*

The Energy Aware Factor based Location Security algorithm provides all the reliable links to transmit the data and prevents the unauthorized node accessing. The algorithm includes the following process:

Algorithm: Energy Aware Factor based Location Security
Input: Sensed Energy Data from self & neighbour nodes
Output: Reliable Energy efficient Route selections
Variables:
PRDT-Predicted Reliability Difference Threshold
EDT-Energy Difference Threshold

R_a-Best Reliable Transmission Route
R_b-Best Reliable Energy Route
Reliable Difference (RD)= R_b.Reliable - R_a.Reliable
Energy Difference (ED) = R_b.Energy - R_a.Energy

Procedure:

```
    Step-1:Start
    Step-2: if $R_a$== $R_b$  then,
    Step- 3: Selected Route is $R_a$
    Step- 4: else if RD>PRDT then,
    Step-5: Selected Route is $R_b$
    Step-6: else if ED < EDT then,
    Step-7: Set $R_b$ is invalid path and delete from list
    Step-8: else
    Step-9: Repeat Step-2 to Step 9 for next reliable route
    Step-10: End if
    Step-11: Stop
```

Calculation of PRDT-Predicted Reliability Difference Threshold

$$PRDT = RouteScore(T_i) + \left(n * \frac{RouteScoure(T_i) - RouteScore(T_1)}{T_i - 1} \right) \qquad \text{Eq. (1)}$$

Route Score (T_i) is predicted reliability score at time T_i
Route Score (T_1) is initial reliability score at time T_1
n is number of hopes to cluster head in the respective path
Route Score T_i is calculated as:

$$T_i = RT * RSSI \qquad \text{Eq. (2)}$$

RT is Reliable Transmission rate of the respective node, it is calculated as:

$$RT = \frac{1}{FPDR * RPDR} \qquad \text{Eq. (3)}$$

Where, FPDR is Forward Packet Delivery Ratio
RPDR is Reverse Packet Delivery Ratio

5. Results

In this Section, we simulate our proposed Energy Aware Factor for Greedy Routing Protocol with inside the wireless Sensor Network the use of NS2 Simulator. Through experiment, we demonstrate the performance of network in throughput, network overhead, packet delivery ratio, and packet loss. In the Simulation, the set up of the network is described in the following Table 1:

Simulation Parameter	Value
Simulator	NS2
Topology Size	1000m *1000m
Number of Nodes	200
Bandwidth of the Network	2Mbps
Traffic type	CBR
Pause Time	10s,20s
Data Packet size	512 bytes
Buffer size	30 packets
Simulation Time	30 minutes

Table 1. Simulation parameters used to build a protocol

The following subsections shows the comparison of proposed energy aware factor based location security with existing method forward aware factor based route selection and followed with table of comparison with above specified aspects of wireless sensor network.

5.1. *Throughput:*

The throughput of proposed system and existing system is shown in Fig.3.

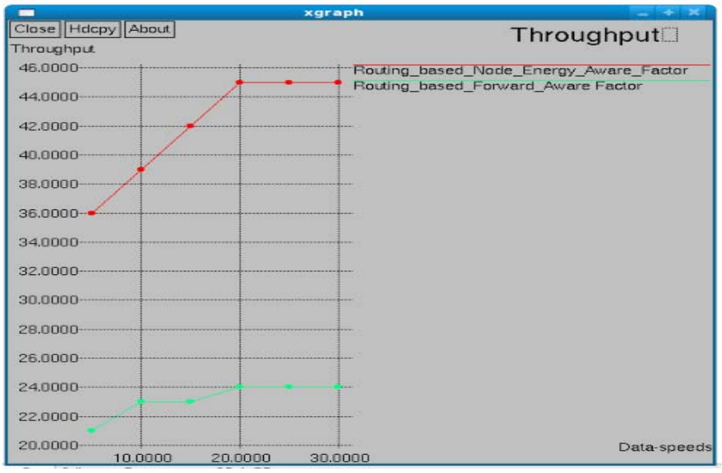

Fig. 3. Performance analysis of throughput on proposed methodology

5.2. *Performance* analysis of traffic

The traffic overhead of proposed system and existing system is shown in Fig.4.

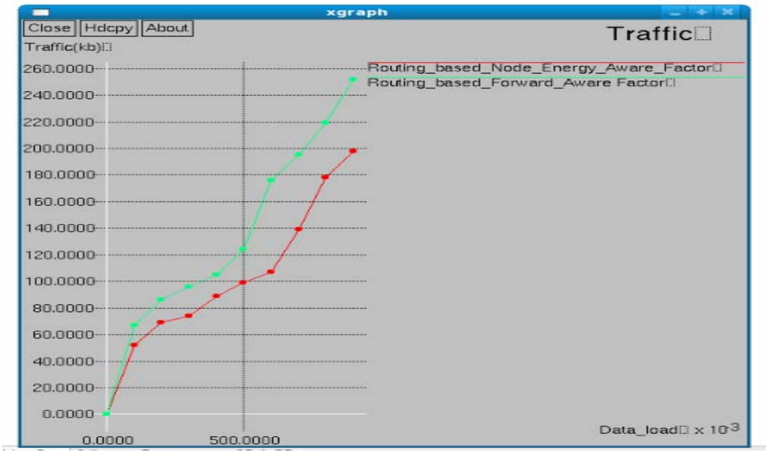

Fig. 4. Performance analysis of traffic towards proposed methodology

5.3. *Packet delivery ratio*

The packet delivery ratio of proposed system and existing system is shown in Fig.5.

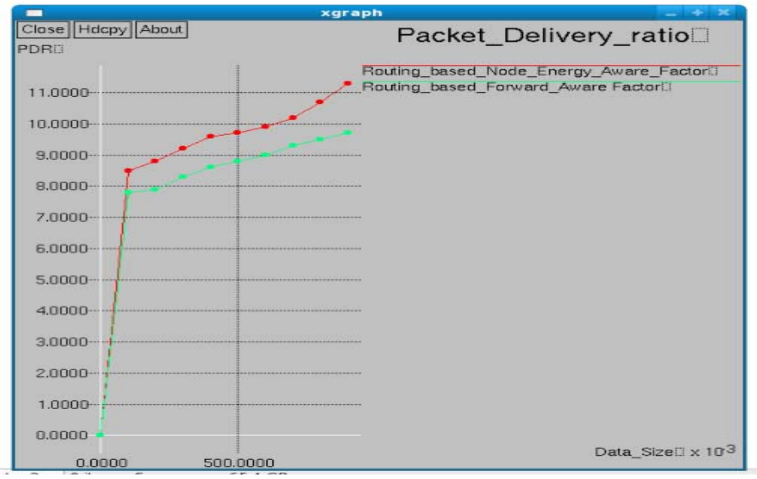

Fig. 5. Performance analysis of packet delivery ratio of the proposed methodology

5.4. *Packet loss computation*

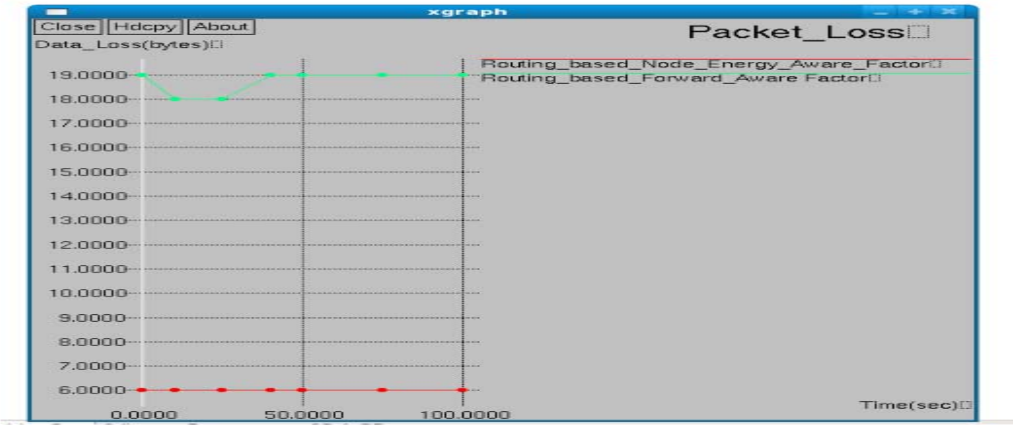

Fig. 6. Performance analysis of packet loss computation on proposed methodology

A detailed description of exting system vs proposed system is given in below Table 2, followed by diagramatic represntation in Fig. 7.

Technique	Forward Aware Factor – Existing	Energy Aware Factor Based Location Security – Proposed
Throughput in mbps	66.42	69.26
Overhead in mbps	14.56	12.59
Packet Delivery Ratio	98.28	99.85
Packet loss in Percentage of data lost	0.29	0.26

Table 2. Performance evaluation of the proposed methodology

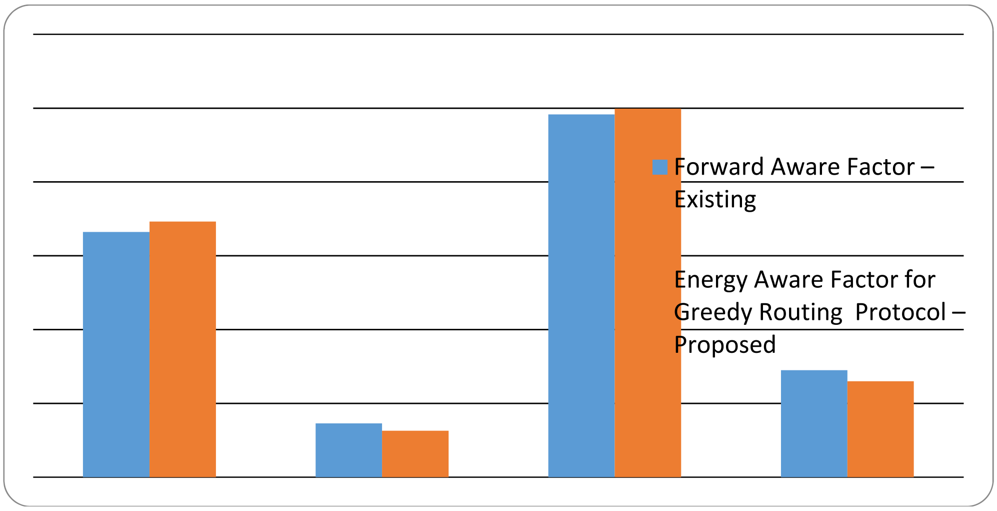

Fig. 7. Performance evaluation of the proposed methodology

6. Conclusion

We designed greedy routing protocol in the Wireless Sensor Networks with homomorphism encryption with Energy Aware Factor based Location Security algorithm. This protocol avoids the node compromising attacks from attackers and also takes less energy resources due to fewer computations for encryption and decryption by share the data to the neighbours. Data securing mechanism can further increase the packet delivery ratio and throughput of the network on greedy routing strategies.

References

[1] C. Ma, J. He, H. H. Chen, and Z. Tang, “Coverage overlapping problems in applications of IEEE 802.15.4 wireless sensor networks,” in Proc. IEEE Wireless Commun. Netw. Conf., pp. 4364–4369, 2013.

[2] S. Sharma, A. Yadav, M. Panchal and P. D. Vyavahare, "Classification of Security Attacks in WSNs and Possible Countermeasures: A Survey," 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1-6, 2019.

[3] [3] G. Han, X. Yang, L. Liu and W. Zhang, "A Joint Energy Replenishment and Data Collection Algorithm in Wireless Rechargeable Sensor Networks," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2596-2604, Aug. 2018.

[4] [4] Mauro Conti, Jeroen Willemsen, and Bruno Crispo, “Providing Source Location Privacy in Wireless Sensor Networks: A Survey”, IEEE Communications Surveys & Tutorials, Vol. 15, No. 3, pp. 1238-1280, Third Quarter 2013.

[5] Javier Lopez, Ruben Rios, Feng Bao, Guilin Wang, “Evolving privacy: From sensors to the Internet of Things”, in Elsevier J. FGCS, Vol. 75, p.46 - 57, March-2017.

[6] Hao Wang, Guangjie Han, Wenbo Zhang, Mohsen Guizani, Sammy Chan, “A Probabilistic Source Location Privacy Protection Scheme in Wireless Sensor Networks”, IEEE Transactions on Vehicular Technology, Volume: 68, Issue: 6, pp. 5917-5927, June 2019.

[7] Jing Yang Koh, Derek Leong, Gareth W.Peters, IdoNevat, Wai-Choong Wong , “Optimal Privacy-Preserving Probabilistic Routing for Wireless Networks”, IEEE Transactions on Information Forensics and Security, Vol. 12, No. 9, p.2105-2114, Sep-2017.

[8] Qian Zhou , Xiaolin Qin, “Preserving Source Location Privacy against the Global Attacker Hiding in FOG”, IEEE-ICNSC, p.1-6, March-2018.

[9] Islam M. Tanash, FedaaYaseen,M F. Al-Mistarihi, Basheer Al-Duwairi, MShurman, “Source Location Privacy in a Cluster-Based Wireless Sensor Networks against Local Adversary”, IEEE-ICICS, p.348-351, April-2017.

[10] C. N. Burger, T. L. Grobler and W. Kleynhans, "Discrete Kalman Filter and Linear Regression Comparison for Vessel Coordinate Prediction," 2020 21st IEEE International Conference on Mobile Data Management (MDM), pp. 269-274, 2020.

[11] A. Ribeiro, I. D. Schizas, S. I. Roumeliotis and G. Giannakis, "Kalman Filtering in Wireless Sensor Networks," in IEEE Control Systems Magazine, vol. 30, no. 2, pp. 66-86, April 2010.

[12] Ali Nassiri, M. A. Razzaque, Abdul Hanan Abdullah, “Isolated Adversary Zone for Source Location Privacy in Wireless Sensor Networks”, IEEE-IWCMC, p.108-113, Sep-2016.

[13] Guangjie Han, Xu Miao, Hao Wang, Mohsen Guizani, Wenbo Zhang, CPSLP: A Cloud-Based Scheme for Protecting Source Location Privacy in Wireless Sensor Networks Using Multi-Sinks, IEEE Transactions on Vehicular Technology, Volume: 68, Issue: 3, pp. 2739-2750. March 2019.

Authors Profile

Parthasaradhi Maysala, received the B.Tech and M.Tech degrees in Computer Science and Engineering from JNTUA Anantapur, Andhra Pradesh, India, in 2011, 2014 respectively. At present he is a full-time research scholar in SV College of Engineering, Tirupati, affiliated to JNTUA Anantapur.

Dr. S. Murali Krishna, received the B.Tech degree in Computer Science and Engineering from SV University, Tirupati, Andhra Pradesh, India, in 2002, the M.Tech degree in Computer Science and Engineering from JNTUH University, Andhra Pradesh, India, in 2005, Hyderabad, and the Ph.D. degree in Computer Science and Engineering from JNTUA University, Ananthapur, Andhra Pradesh, India, in 2011. He is currently working as a Professor and Head with Department of Information Technology, SV College of Engineering (Autonomous), Tirupati, Andhra Pradesh, India. He authored/co-authored research articles in conferences, book chapters and journals. His current research interests include Text Mining, Pattern Recognition, Wireless Sensor Networks, Data analytics, and Machine Learning.