www.s2is.org
International Journal on Smart Sensing and Intelligent Systems
ISSN 1178-5608

SELADG: SECURE ENERGY EFFICIENT LOCATION AWARE DATA GATHERING APPROACH FOR WIRELESS SENSOR NETWORKS

M. Roseline Juliana [1], S.Srinivasan[2]

[1]Associate professor, Department of ECE,
St. Michael College of Engineering & Technology,
Kalaiyar kovil, Tamilnadu, India

[2] Professor & head, Department of CSE,
Anna University Regional office,
Madurai, Tamilnadu, India

E mails: roselinejulianaphd2014@hotmail.com[1], srinivasandr2007@hotmail.com[2]

Submitted: Apr. 12, 2015 Accepted: Aug. 10, 2015 Published:Sep. 1, 2015

Abstract-Recent trends in wireless sensor networks leads to the development of new protocols for data gathering. In this paper, a secure energy efficient location aware data gathering approach is introduced to secure data gathering. An Elliptic Curve Diffie Hellman Key Exchange (ECDHKE) algorithm is utilized for key generation and key exchange between the sensor nodes to maintain security and prevent the data from malicious nodes. The performance of the proposed scheme is validated in terms of packet drop, throughput, energy consumption, residual energy and network lifetime. The proposed scheme achieves better performance than the existing EEHA and SMART schemes.

Index Terms— Data gathering, Key exchange, Key generation, Malicious nodes, Network lifetime, Residual energy, Sensor nodes, and Wireless Sensor Networks (WSNs)

I. INTRODUCTION

Wireless Sensors are habitually power-driven by batteries and the nodes have limited computing capability and memory resources. Due to the limitations of battery life, the nodes are built with power consumption in mind and usually take a large amount of time in a little power sleep mode. Wireless Sensor Networks (WSNs) are emerging applications of pervasive computing, which consist of low power, small and intelligent nodes and one or more base stations. The base station acts as a gateway between sensor nodes and the end user. Potential applications for such large-scale wireless sensor networks exist in a variety of fields, including environmental monitoring, medical monitoring, home security, surveillance, military operations, and industrial machine monitoring.

Sensor network applications can be classified based on its operational archetype: data gathering and event driven. The data gathering application needs sensor nodes to intermittently update their data to the base station. In event driven application, the sensor nodes send data only, during an interest of event occurs. Though, planning security protocols is a challenging task for a WSN. Also, energy efficiency is a significant concern in WSNs. Moreover, wireless transmission is a vital source of power consumption. Hence a significant part of communication in WSNs is due to data gathering. Data gathering plays a vital role in WSN since the aggregation methodology reduces the amount of power consumed for data transmission between the sensor nodes. There are many gathering techniques used in WSN:

- Tree based aggregation
- In network aggregation

Usually, WSN composed of sink node sometimes termed as a Base Station and many small sensor nodes. The nodes monitor a location area and aggregated the information. Sensor details are communicated to the base station with the help of wireless hop by hop transmissions. To preserve the energy this geographical information can be aggregated at intermediate sensor nodes based on some aggregation function. Aggregation policy reduces the amount of traffic, it helps to minimize the energy consumption. Two main encounters in the secure data gathering are confidentiality and integrity of data. While existing encryption is used to result end to end confidentiality in WSN. The aggregator node needs to decrypt the encrypted data to complete aggregation. It reveals the plain text at the aggregator nodes, which makes the data susceptible to attacks. Likewise, an aggregator node can include the false data during the data gathering process and make the base station or destination node to accept the corrupted false data.

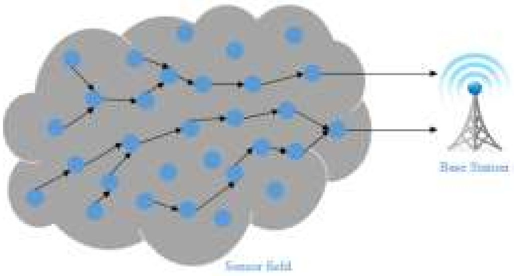

Figure.1.Data gathering in sensor network

In this paper, a novel secure energy efficient location based data gathering approach is proposed for WSNs. One important factor is to reduce the energy consumption of the sensors in order to increase the lifetime of the network. The security mechanisms are incorporated to provide high level secure data gathering. The node location information is periodically updated to find out the nearest neighbor node for data forwarding. The node distance is estimated based on the Euclidean distance to determine the neighbor node for data packet forwarding. The data gathering approach scheme utilizes only lesser energy for data transmission. Hence it improves the network lifetime. Extensive simulations are conducted to compare the proposed method with the existing methods.

The advantages of the proposed method:

- Efficiency: Data gathering is an important energy efficient approach to reduce the power and resource usage based on in-network processing to reduce the number of messages transmitted.
- Accuracy: The proposed method provides higher accuracy ratio based on selecting the energy efficient factors. Hence, the unwanted packet loss are reduced.
- Security: Even though the wireless links are vulnerable to eavesdropping, a good secure data gathering approach should be robust to such attack. The proposed method uses the Elliptic Curve Diffie Hellman Key Exchange (ECDHKE) to provide secure data gathering in WSN.

The remainder of this paper is organized as follows. Section 2 summarizes the related works in secure energy based data gathering schemes. Section 3 describes about the proposed Secure Energy Efficient Location Aware Data Gathering Approach. Section 4 describes the performance analysis. And finally, the paper is ended with the conclusion and future work at section 5.

II. RELATED WORK

This section deals with the works related to the recent secure energy aware data gathering and routing schemes. *Yoo et al* [1] designed a secure energy and reliability aware data gathering protocol. It provides energy efficient reliable data transfer. This protocol provides protection against the network layer attacks spoofed, altered or replayed routing information, Sybil attacks, sinkhole attacks, selective forwarding, HELLO flood attacks, acknowledgement spoofing attacks and wormhole attacks. *Zhou et al* [2] proposed a trust aware and location based secure routing protocol to protect the WSN against routing attacks. This protocol was extended from GPRS protocol incorporates the security mechanism. *Ahvar et al* [3] investigated the fuzzy based energy aware routing protocol for WSN. FEAR protocol considers the energy balancing and energy saving. A fair trade off was calculated between energy balancing and energy saving based on the fuzzy set concept. *Bahi et al* [4] suggested a secure data aggregation technique in WSN. This scheme was based on elliptic curve cryptography, which exploits a smaller size keys. Moreover, the use of higher number of operations on cypher-texts were allowed. It prevents the difference between two identical texts from their cryptosystems. Watermarking based authentication method was used to provide secure aggregation.

Boloorchi [5] introduced a semi centralized approach. It was based on traditional clustering, symmetric and asymmetric key management and threshold secret sharing. The threshold secret sharing approach was explored to estimate the proper parameters. Confidentiality of data, integrity and dependability of the sensed information was enhanced in a circulated manner. *Jin et al* [6] designed a hop based energy aware routing algorithm for WSN. The hop based algorithm can enhance the energy among multi hop routing in sensor networks. Because, it can estimate the optimal hop number and the respective intermediate nodes. Hop based Energy Aware Routing (HEAR) algorithm was used, that was completely localized and distributed. *Hara et al* [7] proposed a secure data aggregation strategy. Hence, a lightweight verification algorithm was utilized to determine the aggregated data includes any false impact. *Kumari et al* [8] studied four multi path randomized routing approach. The random propagation shares were distributed based on one hop neighborhood information. For each share, the sink TTL initial value enhances the efficiency of shares depends on two hop neighborhood details.

Li et al [9] introduced the secure and energy efficient data aggregation methodology to detect the attacker nodes. Here, all the aggregated results were signed with the private keys.

Moreover, pairwise shared key was used on each link for secure data transmission. Each node retrieves the aggregated output from its parent node and authenticates the aggregated output of the parent node. *Lu et al* [10] formulated a distributed secure data collection approach through chaotic compressed sensing. The chaotic compressed sensing was applied to the compressed-encrypted data. An active node matrix algorithm sensing matrix generation algorithm was discovered to improve the data transmission. To evaluate the efficiency of the system, the secret key crack, hijack jamming, forgery and reply attacks were evaluated. *Samundiswary et al* [11] suggested a trust based energy aware greedy perimeter stateless routing protocol (TEGPSR). This protocol incorporates the trust based mechanisms in EGPSR protocol. *Zahariadis et al* [12] proposed a trust aware geographical routing approach for WSN. This approach depends on both the direct and indirect observations to formulate the trustiness for each neighboring node to defend against the routing attacks.

Leligou et al [13] proposed a routing protocol with trust and location information in WSN. This protocol was utilized for balancing trust and location information. Also, different ways to incorporate the trust in location aware routing were investigated. *Zhan et* [14] *al* suggested a trust aware routing model. It provides trusted and energy efficient route. It opposes the harmful attacks established out of identity trick. *Crosby et al* [15] designed a location based trusted detection of compromised nodes in WSN. Hence, the compromised nodes were detected and provide respective actions. A verification algorithm was used for the verification of the location information of the sensor nodes. *Feng et al* [16] formulated a node behavioral strategies banding belief theory of the trust evaluation algorithm. The node behavior strategies and modified evidence theory were incorporated in this model. Moreover, a trust factor and the coefficients were established to attain the direct and indirect trust values by estimating the weighted average of trust factors. The fuzzy set method was applied to form the vector evidence. The evidence difference was determined between the indirect and direct trust values that combines the revised D-S evidence combination rule.

Zhao et al [17] formulated a secure geographical routing protocol. This protocol utilizes the location pairwise keys for secure routing of packets. *Duan et al* [18] designed a Trust aware Secure Routing Framework (TSRF). Primarily, the features of common attacks were analyzed on trust routing approaches. Then, the trust derivation scheme and specific trust calculations were formulated based on the analysis. *Mao and Yuxin* [19] introduced a hybrid algorithm which combines a key based secure routing algorithm and counter based intrusion detection algorithm. This combined algorithm can able to protect the data gathering in WSN. *Huang et al* [20] proposed a secure encrypted data aggregation scheme to remove the redundant sensor readings without the encryption policy. Security and privacy aggregation were provided and the duplicate instances was composed as a single packet.

Villas et al proposed a novel spatial correlation aware algorithm to tackle the routing and load balancing issues in the WSN. The aggregration quality of the routing tree constructed by the proposed algorithm was higher than the existing algorithms [21]. *Xiao et al* presented a centralized algorithm to find the near-optimal energy allocation strategy for improving the precision of the gathered data received by the sink. A localized alterative algorithm that is scalable and adaptable to the large-scale distributed WSN was developed. The data aggregation precision and convergence of the proposed algorithm were improved [22]. *Yi et al* proposed a novel partial matrix completion algorithm to enable efficient data collection in WSN. With the comprehensive usage of the band-limited feature of the sensory data, the recovery accuracy was improved irrespective of the low sampling ratio [23]. *Naznin and Chowdhury* presented an energy efficient data gathering method to maximize the network lifetime and throughput rate. A load balanced data collection scheme was designed by dividing the network into the clusters and routes that provide ultimately higher packet delivery ratio [24]. *Wu et al* proposed a novel posterior belief clustering algorithm to optimize the tradeoff between target tracking performance and energy consumption rate of the sensor in WSN. The target tracking under dynamic environment was modeled by using partially observable Markov decision processes [25].

III. SECURE ENERGY EFFICIENT LOCATION AWARE DATE GATHERING APPROACH

Due to the nature of hostile environmental condition and exclusive properties of wireless sensor networks, it is a crucial task to protect the complex information. Moreover, wireless sensor networks affect with the security issues that the traditional networks do not face. Hence, security is a major problem for wireless sensor networks and it is necessary to investigate the security deliberations. The proposed system uses the Elliptic Curve Diffie Hellman Key Exchange (ECDHKE) Algorithm. Figure.2. describes the flow of the proposed method. The following sections describe the interaction between the energy consideration and data gathering process.

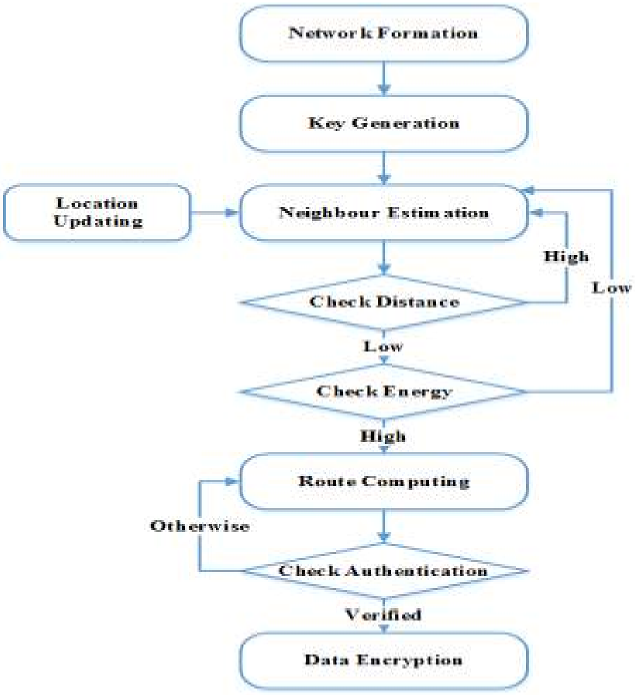

Figure 2. Flow of the proposed Secure Energy Efficient Location Aware Data Gathering Approach

a. Security Requirements

The security requirements for wireless sensor networks are data confidentiality, data integrity source authentication and availability.

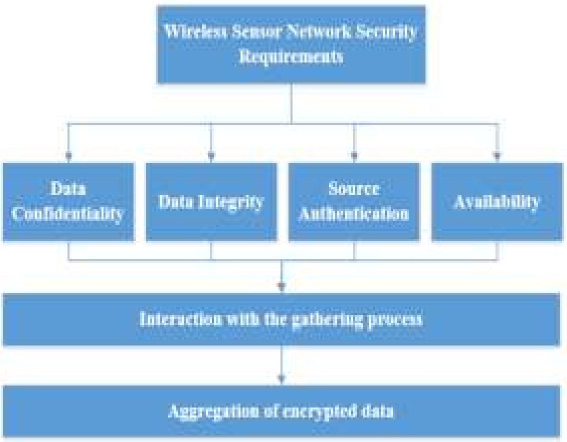
Wireless Sensor Network Security Requirements
Data Confidentiality
Data Integrity
Source Authentication
Availability
Interaction with the gathering process
Aggregation of encrypted data

Figure.3. Interaction between wireless sensor network security and data gathering process

a.i Data Confidentiality

Data confidentiality improves the secrecy of sensed data and the sensitive data is never revealed to the unauthenticated nodes/parties. Also, in many of the applications the sensor node transfers sensitive information like secret keys. Hence, it is essential to build the secure communication channels between sensor nodes. The data like sensor ids and public keys must be encrypted to protect against the security attacks. In some cases, the routing information also need to maintain confidential as unauthorized nodes can use the information to deduce the sensor network performance. The typical method to keep the sensitive data is to encrypt the information with a help of a secret key that only intended by the authenticated receivers. The proposed scheme uses the ECDHKE algorithm to exchange the keys between the nodes. This results lesser delay and energy consumption and also provides the end-to-end confidentiality.

a.ii Data Integrity

Data confidentiality does not prevent data from being changed. Data integrity guarantees that a data being transferred are never corrupted. Data may be altered due to the unreliable communication channels. If the gathered data is compromised, then it might be corrupted data during the data gathering process.

a.iii Source Authentication

The sensor networks uses a shared wireless medium and the sensor nodes need the authentication mechanisms to identify the unauthenticated packets. Without the source authentication policy, an adversary node can attack the network and access the sensitive information. If two nodes are interacting, authentication can be maintained by establishing the symmetric key cryptography. The multiple sender and the receiver can share a secret key to determine the MAC for all forwarded data.

a.iv Availability

Availability guarantees the survivability of network performance against Denial of Service attacks (DOS). DOS attack can be launched at any layer and might disable the target node permanently.

b. Route Formation

The sensor nodes broadcast the HELLO packet throughout the network to discover the node location and the energy of the particular node. There are two major criteria used for route selection.

1. Distance among the nodes.
2. Energy computation

b.i Neighbor node selection

The neighbor nodes are estimated based on the Euclidean distance. The packets are forwarded to the shortest distance nodes. Consider the two points x = (x_1, x_2,…,x_n) and y= (y_1, y_2,…,y_n). The distance from x to y or from y to x is given by:

$$\mathrm{d}\ \mathrm{x},\mathrm{y} \ = \mathrm{d}\ \mathrm{y},\mathrm{x}\ = \overline{\ y_1 - x_1{}^{2} + \ y_2 - x_2{}^{2} + \cdots + \ y_n - x_n{}^{2}}$$

$$= \overline{{}_{i=1}^{n}\ y_i - x_i{}^{2}} \qquad (1)$$

Eqn (1) is used to compute the distance between the sensor nodes. The shortest distanced neighbor nodes are selected to forward the data.

Neighbor Discovery Algorithm

```
func Neighbor discovery
    Broadcast the RTR packet with source information
end func
```

Receiver side RTR packet algorithm

```
Receive RTR ()
Retrieve the sender location from RTR packet
Retrieve the receiver location
Calculate the distance between Source to Destination (d(S, D) and Receiver to Destination (d (R, D)
if (d (S, D) < d (R, D))
        if (packet type! = broadcast)
        add the entry to neighbor table with flag 1
        else
        add the entry to neighbor table with flag 0
Send RTR reply packet to sender with receiver information
end if
end
```

At the receiver side, the RTR packet algorithm is established. The sender location is retrieved from the RTR packet. Also, the receiver location is also notes. Then, the distance from source to destination and receiver to destination is estimated. If the distance from (S, D) is lesser than (R,D) then the checks the packet type. Then, the entry 1 will be appended to the neighbor table else it will be 0. At last, the RTR reply packet will be forwarded to the sender with the receiver information.

b.ii Energy Analysis of proposed routing protocol

There a several routing protocols are proposed for wireless networks which can be observed in the background of wireless sensor networks. In the proposed protocol, nodes route the data packets destined eventually for the base station through the intermediate nodes. The intermediate nodes are selected such that the transmit amplifier energy is minimized. Hence node 1 transmit to node 3 through node 2 if and only if:

$$E_T \ k, d = \ d_{12} \ + E_T \ k, d = \ d_{23} \ < E_T \ k, d = \ d_{13}$$

(2)

Or

$$d_{12}^2 + \ d_{23}^2 < \ d_{13}^2 \qquad (3)$$

Consider the distance between the sensor nodes is *l*. if the energy transmitted a single *k* bit data from a node places a distance *nl* from the base station by direct communication method.

$$E_{dir} = \ E_T \ k, d = n * l \ = E_{elec} * k + \ \varepsilon_{amp} * k * \ nl \ ^2$$

$$= k \ (E_{elec} + \varepsilon_{amp} n^2 l^2) \qquad (4)$$

Each node forwards the packet to the nearest node to the base station. Accordingly, node placed a distance *nl* from the base station may require *n* spreads a distance from *l* and *n-1* receives.

$$E_{MTE} = n * \ E_T \ k, d = l \ + \ n - 1 \ * E_R \ k$$

$$= n \ E_{elec} * k + \varepsilon_{amp} * k * l^2 \ + \ n - 1 \ * \ E_{elec} * k)$$

$$= k \ (\ 2n - 1 \ E_{elec} + \varepsilon_{amp} \, nl^2 \qquad (5)$$

Hence, the direct communication needs less energy than the MTE routing if:

$$E_{dir} < E_{MTE} \qquad (6)$$

MTE denotes the minimum transmission energy.

The messages are encrypted based on the key generation algorithm and the resulted encrypted data are combined at the base station shown in Figure.4.

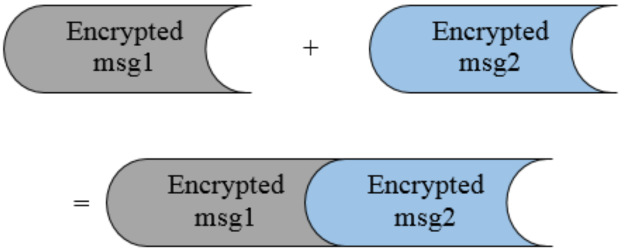

Figure.4. Final encrypted data

IV. PERFORMANCE ANALYSIS

In this section, the Secure Energy Efficient Location Aware Data Gathering Approach is presented, where a source location estimate is obtained through the periodic HELLO packets. The simulation was performed in NS2 and the total number of nodes is 500 nodes in the area of 1000m x 1000m. Table 1 shows the simulation parameters.

Table 1 Simulation Parameters

Parameters	**Values**
Total number of sensor nodes	500
Simulation area	1000 X 1000m
Node distribution	Random
Simulation Time	50ms
Initial Energy	15J

a. Comparison of With and Without Secure Data Gathering Approach

The performance of the proposed data gathering scheme is validated and compared with the existing data gathering scheme without security measures. The performance is evaluated based on the following constraints: packet drop, energy consumption, network lifetime, throughput and residual energy.

a.i Packet drop

Packet drop is the amount of packets failed during the data transmission. Figure.5. depicts the comparison between the proposed scheme and the existing data gathering model. The result shows that the proposed scheme can result lesser packet drop than the existing approach during data transmission.

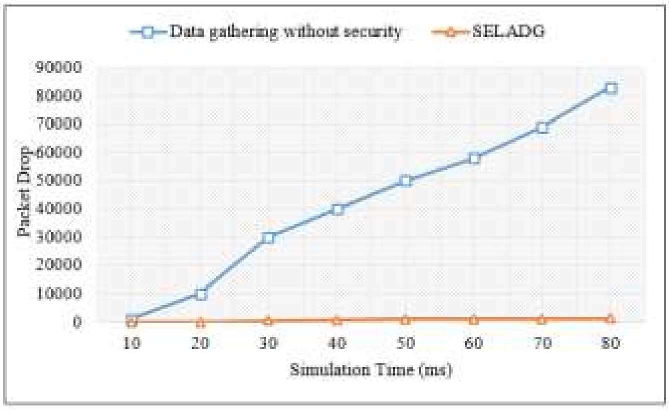

Figure.5. Packet drop between SELADG (proposed) and existing data gathering approach without security mechanism

a.ii Energy Consumption Analysis

Based on the throughput measure the energy consumption is evaluated between the proposed SELADG and the existing approach. The proposed method utilizes lesser energy than the existing approach.

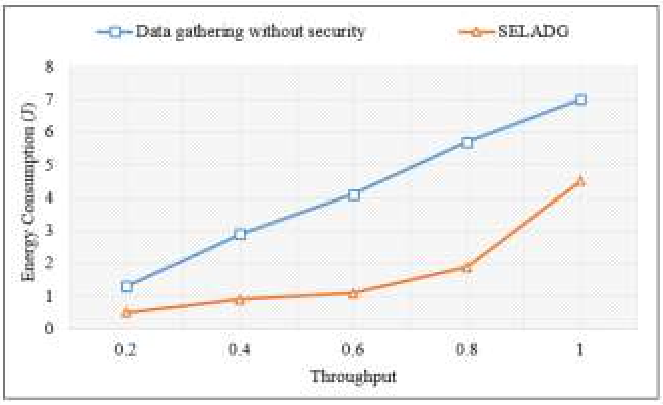

Figure.6. Energy consumption vs throughput

The remaining energy is captured after the data transmission. The proposed system has higher residual energy than the existing approach which is shown in Figure.7.

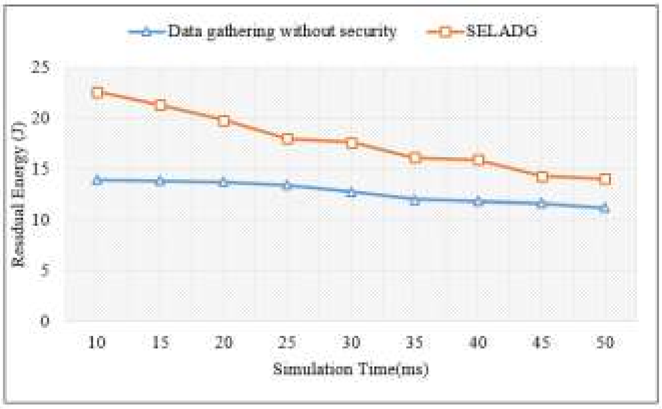

Figure.7. Residual energy between SELADG and the existing data gathering approach without security

a.iii Network Lifetime

The proposed system has better residual energy due to the proposed energy criteria which is shown in Figure.6 and Figure.7. Hence the lifetime is improved for the proposed methodology. The comparison graph is shown in Figure.8. It shows the proposed method can result better network lifetime than the existing approach.

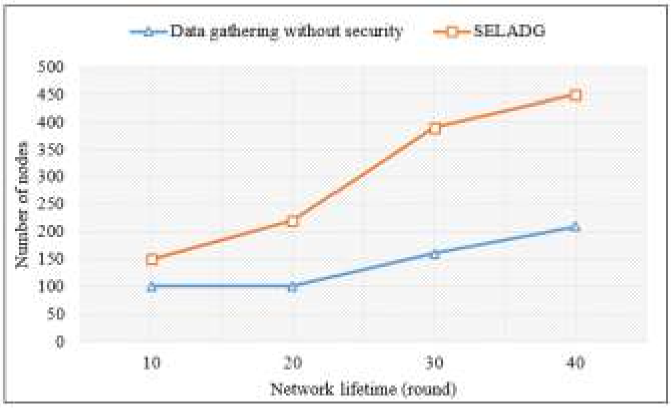

Figure.8. Network lifetime vs number of nodes

a.iv Throughput Analysis

Throughput is the total number of data packets that have been received at time *t* by a destination. Figure.9.shows that the proposed scheme can result better throughput than the existing approach.

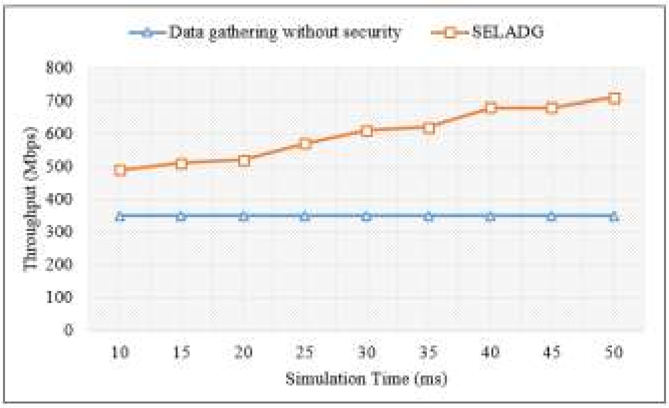

Figure.9. Throughput vs simulation time

b. Comparison of Secure Data Gathering Approaches

In order to show the efficiency of the proposed method, the results are compared with the existing two approaches Energy Efficient and High Accuracy (EEHA) [26] and Slice-Mix-AggRegaTe (SMART) [27-28].

b.i Data Gathering Accuracy

The accuracy is defined as the ratio among the selected summation by the data gathering method used and the real summation of all the individual sensor nodes. The data gathering results can be used to make critical decisions. Figure.10 shows the comparative accuracy analysis for the proposed SELADG with the existing EEHA and SMART approaches. The proposed method results higher accuracy than the existing methods.

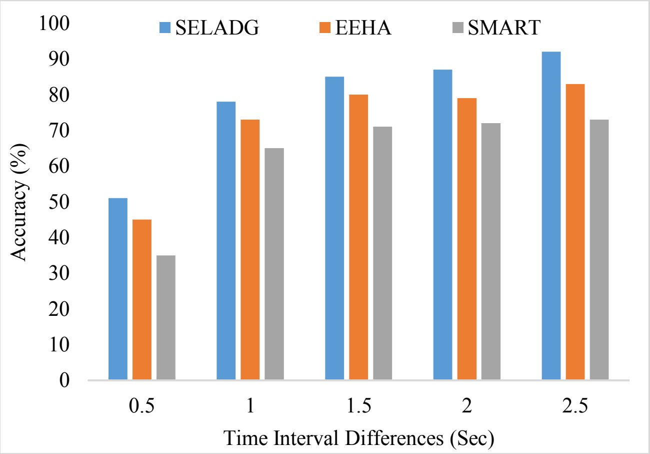

Figure.10 Comparison for Data Gathering Accuracy between SELADG, EEHA and SMART

b.ii Remaining Energy

After the data gathering process gets completed, we noted the remaining energy level for the proposed method and the existing methods EEHA and SMART. It is shown in Figure.11 and it proves that the proposed method preserves more energy than the existing methods.

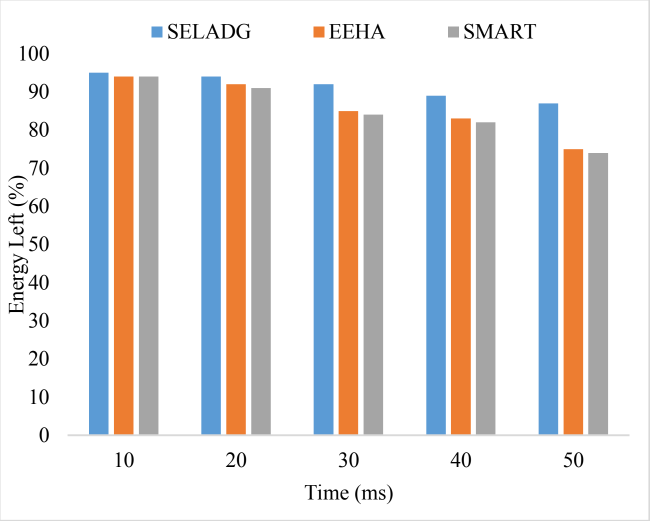

Figure.11 Comparison for Remaining Energy between SELADG, EEHA and SMART

Detection of the selfish node is the significant concern in the WSN. The detection rate of the selfish behavior of the nodes is observed by using the proposed SELADG method. Figure.12 shows the graph illustrating the comparison of the detection ratio of the existing EEHA and the proposed SELADG method. From the graph, it is clearly understood that the proposed SELADG method achieves improved detection ratio, when compared to the EEHA method.

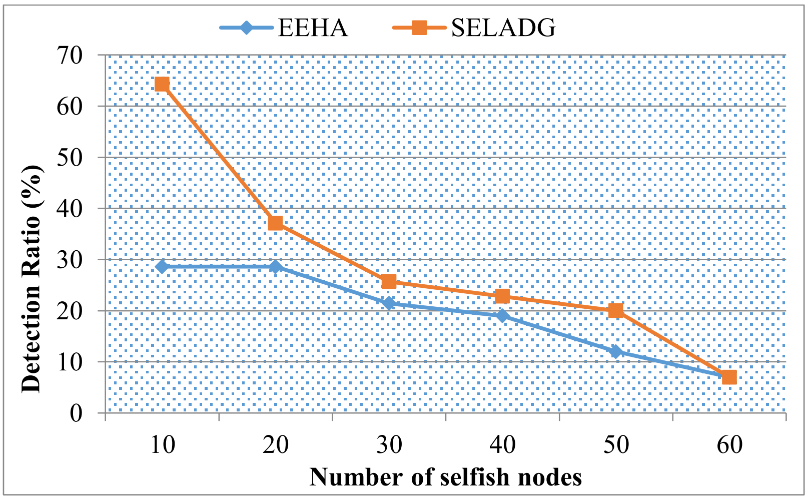

Figure.12 Comparative analysis of the detection rate of the existing EEHA and proposed SELADG approaches

The false positive rate is calculated as the percentage of normal variations detected as anomalies. The detection of the false alarm leads to the improved performance of the whole network. The comparative analysis of the false positive rate of the existing EEHA and proposed SELADG techniques is depicted in the Fugure.13. The proposed SELADG method yields better result than the existing EEHA techniques.

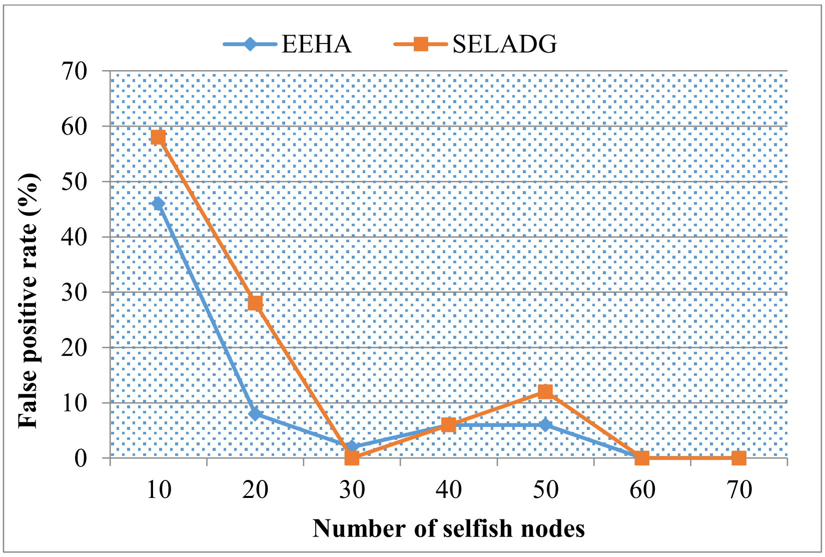

Figure.13 Comparison of the false positive rate of the existing EEHA and proposed SELADG approaches

Figure.14 shows the comparison of the routing overhead of the existing EEHA and proposed SELADG method with respect to the number of selfish nodes. Moreover, increase in the load results in more dropping of packet in WSN. In this analysis, the proposed SELADG technique incurs less overhead than the existing EEHA method.

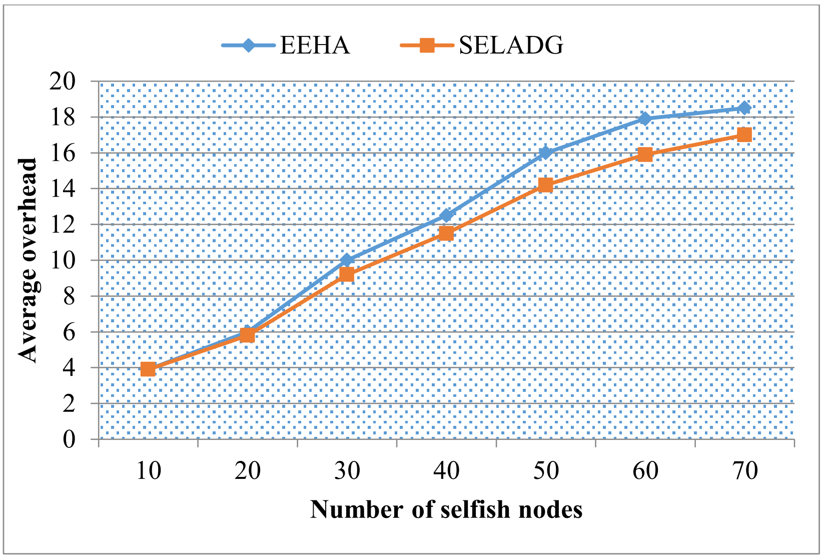

Figure 14. Comparative analysis of the average overhead of the existing EEHA and proposed SELADG approaches

V. CONCLUSION AND FUTURE WORK

In this paper, a secure energy efficient location aware data gathering approach is proposed. This scheme utilizes the properties of node location and energy to improve the lifetime of node and network. Also the security mechanism termed Elliptic Curve Diffie Hellman Key Exchange is incorporated for secure data gathering between source and receiver. The routing is performed based on the neighbor node and highest energy node selection. The proposed scheme is compared with the existing data gathering scheme without the security measure. The experimental result shows that the proposed method can perform better in terms of packet drop, throughput, energy consumption, residual energy and network lifetime. In future work, the proposed structure is incorporated with a super node and clustering concepts to provide better and secure data gathering.

REFERENCES

[1] S. Yoo, S.-h. Kang, and J. Kim, "SERA: a secure energy reliability aware data gathering for sensor networks," *Multimedia Tools and Applications,* pp. 1-30, 2011/01/29 2011.

[2] Y. M. Zhou and L. Y. Li, "A Trust-Aware and Location-Based Secure Routing Protocol for WSN," *Applied Mechanics and Materials,* vol. 373, pp. 1931-1934, 2013.

[3] E. Ahvar, A. Pourmoslemi, and M. J. Piran, "Fear: A Fuzzy-based Energy-aware Routing Protocol for Wireless Sensor Networks," *arXiv preprint arXiv:1108.2777,* 2011.

[4] J. Bahi, C. Guyeux, and A. Makhoul, "Secure Data Aggregation in Wireless Sensor Networks: Homomorphism versus Watermarking Approach," in *Ad Hoc Networks*. vol. 49, J. Zheng, D. Simplot-Ryl, and V. M. Leung, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 344-358.

[5] A. T. Boloorchi and M. H. Samadzadeh, "Energy-efficient and secure in-network storage and retrieval for WSNs: an adaptive approach," *The Journal of Supercomputing,* vol. 65, pp. 961-977, 2013/08/01 2013.

[6] W. Jin, C. Jinsung, L. Sungyoung, C. Kwang-Cheng, and L. Young-Koo, "Hop-based energy aware routing algorithm for wireless sensor networks," *IEICE transactions on communications,* vol. 93, pp. 305-316, 2010.

[7] V. Kumar and S. Madria, "Secure Data Aggregation in Wireless Sensor Networks," in *Wireless Sensor Network Technologies for the Information Explosion Era*. vol. 278, T. Hara, V. Zadorozhny, and E. Buchmann, Eds., ed: Springer Berlin Heidelberg, 2010, pp. 77-107.

[8] C. Ranhotigamage and S. C. Mukhopadhyay, “Field Trials and Performance Monitoring of Distributed Solar Panels Using a Low Cost Wireless Sensors Network for Domestic Applications”, IEEE Sensors Journal, Vol. 11, No. 10, October 2011, pp. 2583-2590.

[9] B. Kumari, N. Vikram, and M. M. Reddy, "Secure Data Collection in Wireless Sensor Networks Using Random Routing Algorithms," *International Journal of Computer Science and Telecommunications,* vol. 2, pp. 50-55, 2011.

[10] H. Li, K. Li, W. Qu, and I. Stojmenovic, "Secure and Energy-Efficient Data Aggregation with Malicious Aggregator Identification in Wireless Sensor Networks," in *Algorithms and Architectures for Parallel Processing*. vol. 7016, Y. Xiang, A. Cuzzocrea, M. Hobbs, and W. Zhou, Eds., ed: Springer Berlin Heidelberg, 2011, pp. 2-13.

[11] W. Lu, Y. Liu, and D. Wang, "A Distributed Secure Data Collection Scheme via Chaotic Compressed Sensing in Wireless Sensor Networks," *Circuits, Systems, and Signal Processing,* vol. 32, pp. 1363-1387, 2013/06/01 2013.

[12] P. Samundiswary, M. P. Kumar, and P. Dananjayan, "Trust Based Energy Aware Greedy Perimeter Stateless Routing for Wireless Sensor Networks," *Journal of Communication and Computer,* vol. 8, pp. 848-854, 2011.

[13] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis, and P. Karkazis, "A novel trust-aware geographical routing scheme for wireless sensor networks," *Wireless personal communications,* vol. 69, pp. 805-826, 2013.

[14] H.-C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis, and T. Zahariadis, "Combining trust with location information for routing in wireless sensor networks," *Wireless Communications and Mobile Computing,* vol. 12, pp. 1091-1103, 2012.

[15] G. Zhan, W. Shi, and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," *Dependable and Secure Computing, IEEE Transactions on,* vol. 9, pp. 184-197, 2012.

[16] G. V. Crosby, L. Hester, and N. Pissinou, "Location-aware, Trust-based Detection and Isolation of Compromised Nodes in Wireless Sensor Networks," *IJ Network Security,* vol. 12, pp. 107-117, 2011.

[17] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory," *Sensors,* vol. 11, pp. 1345-1360, 2011.

[18] H. Zhao, Y. Li, M. Zhang, R. Zheng, and Q. Wu, "A New Secure Geographical Routing Protocol Based on Location Pairwise Keys in Wireless Sensor Networks," *International Journal of Computer Science Issues (IJCSI),* vol. 10, 2013.

[19] J. Duan, D. Yang, H. Zhu, S. Zhang, and J. Zhao, "TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks," *International Journal of Distributed Sensor Networks,* vol. 2014, 2014.

[20] Y. Mao, "A secure mechanism for data collection in wireless sensor networks," *Applied Mathematics & Information Sciences,* vol. 5, pp. 97-103, 2011.

[21] S.-I. Huang, S. Shieh, and J. Tygar, "Secure encrypted-data aggregation for wireless sensor networks," *Wireless Networks,* vol. 16, pp. 915-927, 2010.

[22] L. A. Villas, A. Boukerche, H. A. De Oliveira, R. B. De Araujo, and A. A. Loureiro, "A spatial correlation aware algorithm to perform efficient data collection in wireless sensor networks," *Ad Hoc Networks,* vol. 12, pp. 69-85, 2014.

[23] S. Xiao, B. Li, and X. Yuan, "Maximizing precision for energy-efficient data aggregation in wireless sensor networks with lossy links," *Ad Hoc Networks,* vol. 26, pp. 103-113, 2015.

[24] K. Yi, J. Wan, L. Yao, and T. Bao, "Partial Matrix Completion Algorithm for Efficient Data Gathering in Wireless Sensor Networks," *IEEE Communications Letters,,* vol. 19, pp. 54-57, 2015.

[25] M. Naznin and A. S. Chowdhury, "ZDG: Energy efficient zone based data gathering in a wireless sensor network," in *International Conference on Networking Systems and Security (NSysS)*, 2015, pp. 1-7.

[26] B. Wu, Y. Feng, and H. Zheng, "POSTERIOR BELIEF CLUSTERING ALGORITHM FOR ENERGY-EFFICIENT TRACKING IN WIRELESS SENSOR NETWORKS," *International Journal on Smart Sensing and Intelligent Systems,* vol. 7, pp. 925-941, 2014.

[27] X. Zhao, J. Minz, and S. K. Lim, "Low-power and reliable clock network design for through-silicon via (TSV) based 3D ICs," *IEEE Transactions on Components, Packaging and Manufacturing Technology,* vol. 1, pp. 247-259, 2011.

[28] H. Wenbo, L. Xue, N. Hoang, K. Nahrstedt, and T. Abdelzaher, "PDA: Privacy-Preserving Data Aggregation in Wireless Sensor Networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, 2007, pp. 2045-2053.