Energy Aware Hierarchal Data Aggregation and Trust Based Data Integrity Verification for WSN

Masthan Ali A.H[1], Ali Ahammed G.F[2], Reshman Banu[3]

[1]Research Scholar, VTU, Belagavi

[2]VTU, Center for Post-Graduation studies, Mysore

[3]Dept. of ISE, GSSSIETW, Mysore

Email:[1]masthan_ali_8@yahoo.com, [2]aliahammed78@gmail.com, [3]reshma127banu@gmail.com

ABSTRACT

Currently the demand of wireless sensor networks has gained huge attraction due to its wide range of applications. Generally, these nodes are equipped with limited power resource and deployed in harsh environment where replacing these resources is a tedious task. Due to these issues, minimizing the energy consumption is a prime task to prolong the network lifetime. To overcome the challenging issue of data aggregation we introduced a novel combined mechanism which performs clustering and trust computing process to improve the data aggregation. According to this scheme, we arrange the nodes as normal node, advanced node and super nodes based on their residual energy parameters. The proposed model uses hierarchal scheme where we present a new mechanism for optimal number of cluster formation and cluster head selection. After selecting the cluster head, we apply trust computation scheme which provides sensing trust, link trust and node trust. The node trust is computed as direct and indirect trust. This trust mechanism is used as hop-by-hop manner to maintain he data integrity. The experimental study shows that proposed approach achieves better performance and maintains the security aspects of WSN.

Keywords

WSN lifetime, data aggregation, trust management, clustering, security

Article Received: 10 August 2020, Revised: 25 October 2020, Accepted: 18 November 2020

Introduction

Nowadays, the demand of wireless sensor network has increased due to their advances in communication and significant use in widespread applications in real-world applications such as medical application [1], smart home [2], military application [3], environmental monitoring [4], traffic administration [5] and many more [6]. The sensor network is composed of large number of tiny sensor nodes. According to the application, these sensor nodes sense and collect the data such as temperature, pressure, humidity, light, voltage, etc... Generally, the collected data is stored as multidimensional data. Moreover, these sensor nodes are resource-constrained which are generally deployed in an unattended even hostile area where replacing the power and other resources is not possible. Due to these issue, these networks are not considered as a feasible solution in critical application scenario where high quality of service and long network lifetime is desired. Hence, maintaining the traffic and reduced computation overhead is the primary task to prolong the network lifetime. However, to deal with this issue of network lifetime, energy aware routing schemes are widely adopted in various real-time systems. These routing protocols are categorized as route processing, network structure, network operation and communicator initiator based protocols. Below given figure 1 shows the classification and sub-classification of these routing protocols.

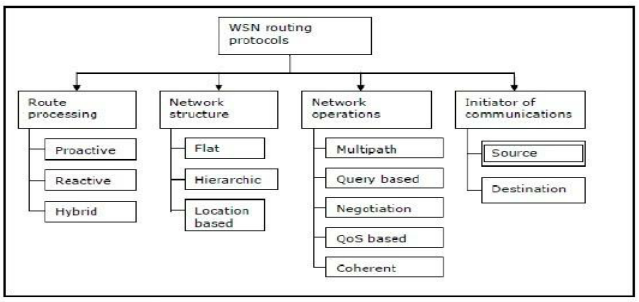

Fig.1. Classification of WSN routing protocols.

The main aim of routing scheme to carry the data to the destination node. Hierarchal routing have gained significant attention to improve the network lifetime. However, these techniques do not consider the quality of data collected by sensor node. Sensor nodes collect data and transmit to the next hop. During this collection process, the redundant data causes additional energy consumption which can lead towards the degraded network lifetime. To overcome this issue, data aggregation scheme is widely adopted which helps to minimize the outliers in the data minimized the retransmission frequency.

Data aggregation is technique which combines the data coming from child nodes in an energy efficient manner. This process is called as data aggregation which uses aggregation functions such as SUM, AVG, MIN, MAX, COUNT, etc. These functions minimizes the data redundancy resulting in increasing the network lifetime while ensuring the better quality of data collection. Several techniques have been reported for data aggregation such as compressive sensing data aggregation [7], heuristic approach [8], and entropy based data aggregation [9]. Similarly, optimization based schemes are also adopted to improve the aggregation

performance such as particle swarm optimization (PSO) [10], genetic algorithm (GA) [11], and firefly optimization [12]. Generally, the data aggregation techniques can be classified as structure based [15, 16] and structure-free data aggregation approach [17, 18]. In structure based approaches, several structures are formed using sensor nodes to collect the data, aggregate and transmit to the base station. These structures are follow the chain-based, tree-based, cluster based, and hierarchal cluster based models. The superior node is assigned as leader node in chain based structure, root node in tree based structure and cluster head in cluster based mechanisms. These nodes are responsible for data collection and aggregation. However, these techniques fail to obtain the desired performance in terms of accuracy, fault-tolerance, security and latency [13]. Security and energy consumption are the two major challenging issue while maintaining the quality of data aggregation. Currently secure data aggregation has become the prime concern for research community to improve the overall communication performance. The main security requirements are integrity, confidentiality, authentication and freshness.

We propose a novel combined scheme which performs both clustering and trust computing operations to enhance the data aggregation process. As per the proposed method, we arrange the nodes as normal node, advanced node and super nodes based on their residual energy parameters. Subsequent to cluster head selection, we perform trust computation mechanism which provides sensing trust, link trust and node trust. The node trust is further computed as direct and indirect trust. This trust mechanism is used as hop-by-hop manner to maintain he data integrity.

Rest of the article is organized in following sections: section II presents a brief literature review about existing techniques of data aggregation, section III presents the proposed energy efficient and secure data aggregation, section IV describes the experimental analysis and section V presents the concluding remarks about this scheme.

Literature Survey

This section presents the brief literature review about existing techniques of secure and energy efficient data aggregation in wireless sensor network.

Kang et al. [14] focused on achieving the tradeoff in terms of network delay and energy cost for data aggregation tasks. Currently, duty cycled WSN are adopted where communication and sensing capabilities are periodically switched ON and OFF to minimize the energy consumption when node is in ideal mode. This periodic switching process causes complexity in data aggregation. To deal with data aggregation issue, authors introduced distributed delay efficient data aggregation scheduling (DEDAS-D) approach for duty cycled WSN.

Haseeb et al. [15] used structure based data aggregation mechanism and incorporated security aspects in Internet of Things (IoT) with WSN. The first phase of this approach performs node clustering based on varying communication radius. This helps to mitigate the energy hole around the base station. In next phase, A-star heuristic algorithm is applied to obtain the routing paths. Later, a security scheme is applied to protect the communication link. This security model uses unbreakable one time pad (OTP) encryption for data security.

Fang et al. [18] developed a combined scheme which focuses on both energy-efficient and secure data aggregation called as cluster-based private data aggregation (CSDA). This approach is the modified version of CPDA (Cluster-based Private Data Aggregation) and SMART. These two schemes suffer from the computational complexity issue and loss of data. To overcome this issue, authors incorporated intrusion detection scheme to secure the network from sinkhole and selective forwarding attacks. Moreover, this scheme uses data slicing scheme to minimize the energy consumption. Similar to this data slicing process, Hua et al. [19] developed energy efficient secure data aggregation approach to prevent the node compromisation in the network. This article presented Adaptive Slice-based Secure Data Aggregation (ASSDA) which considers limitation of node resources.

Merad Boudia et al. [20] discussed about the importance of WSN in IoT technology and elaborated the advantages of data aggregation to maintain the energy consumption and security of the network. In these networks, false data ejection and impersonation attacks are the challenging issues which affect the network performance. Generally, the data can be verified by using either end-to-end approach or hop-by-hop approach. The end-to-end approach can be performed after receiving the data at the end. This leads to loss of legitimate data. On the contrary, the hop-by-hop approach verifies data at each hop which significantly improves the aggregation process. Hence, authors presented hop-by-hop verification scheme. This scheme utilizes Elliptic Curve El Gamal (ECEG) protocol and message authentication code (MAC) modules to incorporate the security aspects. Later, a distributed computing scheme is applied for concealed data aggregation.

Shobana et al. [21] proposed cluster-based systematic data aggregation model (CSDAM) for WSN. During the first phase, the sensor network is created and clusters are formed which include active and sleep node. Further, the cluster head is selected based on existing energy level and geographic location to the base station. This cluster head acts as the aggregator node. Further, a three stage data aggregation scheme is presented which uses threshold to select the aggregation.

Hu et al. [22] presented chain based privacy-preserving data aggregation scheme. In this approach, the nodes are arranged as a tree topology. The leaf nodes establish the connection with other nodes to form the chain topology. To ensure the security, the tail node divides the data into J fragments. The tail node keeps one fragment and distributes $(J-1)$ fragments to the neighboring nodes. These nodes inject some fake fragments to divert the adversaries.

Roslin et al. [23] studied that during the data fragmentation phase, the adversaries or attackers can inject forged fragments which can degrade the quality of aggregation. Hence, these fragments must be verified to observe the correctness of data. To deal with these issues, authors presented trust based approach for data aggregation to verify the integrity of data fragments. This approach constructs a tree based on the trust values and encrypted data with the shared symmetric key. Further, this encrypted data is divided into fragments and a homomorphic MAC tag is

incorporated. After receiving the signed blocks, the aggregator nodes perform the SUM aggregation to aggregate the data.

Boubiche et al. [24] reported that most of the existing secure data aggregation techniques use encryption based modeling to protect the data but the key generation and distribution consumes addition energy. To overcome this issue, authors presented a new approach of secure data aggregation which is called as SDAW (secure data aggregation watermarking-based scheme in homogeneous WSNs). For security, a lightweight fragile watermarking scheme is developed which is used to authenticate the data for aggregation. Similarly, the links between sensor node and aggregation node, links between aggregator and base station are also secured by using watermarking technique.

Qi et al. [25] developed an asymmetric key encryption scheme based on elliptic curve cryptography scheme for WSNs. First of all, a key generation scheme is applied to generate the cryptography keys periodically. Later, a homomorphic scheme is applied to achieve the encrypted data. Finally, a hop-by-hop verification is performed using rotation MAC generation algorithm.

Proposed Model

This section presents the proposed solution for energy aware and secure data aggregation to improve the energy efficiency and reliability of communication. We assume that the network has only one sink node and location of other sensor nodes can be obtained by using our previous mechanism []. We model a sensor network in the form of edge-weighted graph denoted as $G = (V, E)$ where V denotes the vertex set. Each vertex in vertex set represent a senor node including sink node which is denoted as $V = v_1, v_2, \dots, v_n$. These sensor nodes consume a specific power level. This set is denoted as P which contains k power levels. For each sensor node$v \in V$ the consumed power level is represented as $p(v) \subseteq P$. Here, E denotes an edge if u and v have connectivity as $(u, v) \in E$. This denotes the bidirectional communication link between nodes. Here, the data collection request is denoted as (s, R) where s represent the source node and $R \subset V$ is the data source node. As discussed before, hierarchal network communication is widely adopted where cluster head performs data processing, aggregation and transmission tasks. Hence, optimal cluster formation and cluster head selection are the important phases to improve the network performance. We assume that n number of sensor nodes is deployed uniformly in the 2D square geographical region. All of these sensor nodes and base station become stationary after deployment and cluster head (CH) performs the data aggregation. We use a radio model to compute the energy required to transmit L bit data packet over distance d. This can be expressed as:

$$E_{Tx}(L, d) = \begin{pmatrix} L \times E_{elec} + L \times \epsilon_{fs} \times d^2 & if\ d \le d_0 \\ L \times E_{elec} + L \times \epsilon_{mp} \times d^4 & if\ d \ge d_0 \end{pmatrix} \quad (1$$

Where E_{elec} denotes the energy dissipation to operate the transmitter or receiver circuitry, ϵ_{fs} is the energy dissipation per bit in free-space model and ϵ_{mp} is the energy dissipation of multipath model for d_0 distance which is given as:

$$d_0 = \sqrt{\frac{\epsilon_{fs}}{\epsilon_{mp}}} \quad (2)$$

Similarly, the amount of energy required to receive the packet is given as:

$$E_{Rx}(L) = L \times E_{elec} \quad (3)$$

Optimal number of clusters

Selection of optimal number of clusters plays important role to improve the communication performance and minimizes the energy consumption. Let us consider a network area $A = M \times M$ square meters where n number of sensor nodes are deployed uniformly. The distance of node to base station or node to its corresponding cluster head is d_0. Thus, the energy dissipation by CH in a round can be given as:

$$E_{CH} = \left(\frac{n}{k}\right) \times L \times (E_{elec} + E_{DA}) + L \times \epsilon_{fs} \times d_{BS}^2 \quad (4)$$

Where k is the number of clusters is, E_{DA} is the energy consumption in data aggregation, d_{BS} is the distance between base station and CH, which is computed as:

$$d_{BS}^2 = \int \sqrt{(x^2 + y^2)} \times \frac{1}{A} \quad (5)$$

Similarly, the energy dissipated by cluster member node is given as:

$$E_{CM} = L \times \left(E_{elec} + \epsilon_{fs} \times d_{CH}^2\right) \quad (6)$$

Where d_{CH} denotes the average distance between CH and cluster member node which is given as:

$$d_{CH}^2 = \int\int (x^2 + y^2) \times \rho(x, y) dx dy = \frac{M^2}{2\pi k} \quad (7)$$

Where $\rho(x, y)$ denotes the node distribution and M is the network area. Thus, the total energy consumed in each round in each cluster can be given as:

$$E_T = E_{CH} + E_{CM} \quad (8)$$

With the help of Eq. (4) and Eq. (6), the total energy consumption can be expressed as:

$$E_T = L \times \left(2 \times n \times E_{elec} + n \times E_{DA} + \epsilon_{fs} \times (k \times d_{BS}^2 + n \times \frac{M^2}{2\pi k}\right)$$

With the help of this, we can obtain the optimal number of clusters as:

$$k_{opt} = \sqrt{\frac{n}{2\pi}} \times \sqrt{\frac{\epsilon_{fs}}{\epsilon_{mp}}} \times \frac{M}{d_{Bs}^2} \quad (10)$$

Based on the distance and optimal number of clusters, using Eq. (5) and (10), we compute the probability of node to become a cluster head. This can be given as:

$$p_{opt} = \sqrt{\frac{2}{n\pi}} \times \sqrt{\frac{\epsilon_{fs}}{\epsilon_{mp}}} \times \frac{1}{0.765} \quad (11)$$

CH selection

This scheme categorizes sensor nodes into three categories as normal node, advanced node and super node. Here, the node which are having higher residual energy level are known as advanced node and super node whereas remaining nodes are treated as normal node. Let us consider that m nodes are the advanced nodes and m_0 are the super nodes among these advanced nodes. The initial energy of normal node, advanced node and super node is denoted as E_0,

$E_0 \times (1+\alpha)$ and $E_0 \times (1+\beta)$,respectively. Based on residual energy level, it is obvious that advanced and super nodes have the higher probability to become the cluster head. At this stage, we present assign an optimal weight to the previous probability p_{opt}. Let us denote the weighted election probabilities as p_n , p_a and p_s for normal, advanced and super nodes. These probabilities can be computed as:

$$p_n = \frac{p_{opt}}{(1+m\times(\alpha-m_0\times(\alpha-\beta)}$$
$$p_a = \frac{p_{opt}}{(1+m\times(\alpha-m_0\times(\alpha-\beta)}\times(1+\alpha) \quad (12)$$
$$p_s = \frac{p_{opt}}{(1+m\times(\alpha-m_0\times(\alpha-\beta)}\times(1+\beta)$$

With the help of these probabilities, we derive a new threshold function to select node as CH for each type of node i.e. normal, advanced and super node. The threshold function for normal node is given as:

$$T(s_n) = \begin{pmatrix} \frac{p_n}{1-p_n\times\left(r \bmod \frac{1}{p_n}\right)} & if\ s_n \in G' \\ 0 & otherwise \end{pmatrix} \quad (13)$$

Where r denotes the current round, G' is the set of normal nodes, $\frac{1}{p_n}$ round of each epoch. Similarly, we compute the threshold for advanced and super nodes as:

$$T(s_a) = \begin{pmatrix} \frac{p_a}{1-p_a\times\left(r \bmod \frac{1}{p_a}\right)} & if\ s_a \in G'' \\ 0 & otherwise \end{pmatrix}$$
$$T(s_s) = \begin{pmatrix} \frac{p_s}{1-p_s\times\left(r \bmod \frac{1}{p_s}\right)} & if\ s_s \in G''' \\ 0 & otherwise \end{pmatrix} \quad (14)$$

Incorporating security for secure data aggregation

The previous section describes the complete process of data aggregation where we perform optimal number of cluster selection and cluster head selection to maximize the network lifetime. Here, maintaining the security during aggregation is a challenging task. In order to maintain the integrity, we present a trust computation strategy where we present data sensing trust, link trust and node trust.

Computing the sensing trust

The sensing trust helps to maintain the consistency and fault tolerance in the network. Generally, the data sensed by sensor nodes is spatio-temporal correlation which denotes the similarity between collected data in the current cluster. The probability density function can be described as:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad (15)$$

μ denotes the mean value, and σ denotes the variance. The closer value of μ represents the higher trust. Let for node i, the trust value can be computed as:

$$T_{data}(i) = 2\left(0.5 - \int_{\mu}^{v} f(x)dx\right) = 2\int_{v}^{-\infty} dx \quad (16)$$

where v denotes the value of sensed data by node i. Further, to resist the data modification attackers we use mean absolute deviation.

Computing the link trust

The trust value of communication link is evaluated based on the packet error rate and packet loss rate. The probability of bit error rate is obtained as:

$$P_{ber} = \frac{1}{2} erfc\left(\sqrt{SNR}\right)$$
$$= \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N_0}}\right) \quad (17)$$

Based on this, the packet error rate can be computed as $P_{per} = 1-(1-P_{ber})^{\eta}$ where η is the number of payload in a packet. Similarly, the packet loss rate can be computed as:

$$P_{plr} = \frac{n_{rec}}{n_{sens}} \quad (18)$$

Where n_{rec} denotes the number of packets received successfully, and n_{sent} denotes the sum of sent packets. Based on these values of packet error rate and packet loss rate, the link quality can be computed as follows:

$$L_q = (1-P_{per}).P_{plr} \quad (19)$$

Computing the node trust

In order to compute the node trust, we require two parameters which are known as direct trust and indirect trust. The direct trust is obtained by the observation of any node and indirect trust is recommended by a third party node. The direct and indirect trust values are computed as:

$$T_{direct} = \left(\frac{s+(P_{plr}+P_{per}).(s+f)}{s+f}\right).R_{el} \quad (20)$$

Where s denotes the number of successful communication, R_{el} denotes the residual energy levels, and f is unsuccessful transmission. Similarly, the indirect trust can be computed as:

$$T_{indirect} = \frac{\sum_{j=1}^{n} T_{j,i}}{n} \quad (21)$$

n denotes the number of nodes as trust recommender and $T_{j,i}$ is the recommender trust value of node i recommended by node j. Finally, the node trust value can be computed as :

$$T_{node} = w_{direct}.T_{direct} + (1-w_{direct}).T_{rec} \quad (22)$$

Where $0 < w_{direct} \leq 1$ is the weight value of trust

Results and discussion

This section presents the experimental analysis of proposed energy aware secure data aggregation in WSN. This approach is simulated using MATLAB simulation tool running on windows platform. The windows operating system machine is equipped with 16GB RAM, 8 GB NVIDIA graphic card, 1TB storage space and Intel i5 processing unit. The outcome of proposed model is compared with existing techniques such as Trust Assisted Global and Greedy Congestion-aware Data Aggregation for (TAG–GCDA) [26], hamming residue method (HRM) [27] and belief-based trust evaluation mechanism (BTEM) [28] in terms of communication overhead, energy consumption, packet delivery ratio and packet loss rate. Below given table shows the complete set of simulation parameters used in this work.

Table.1. Simulation parameters used in this experiment

Parameters	Values
Network Area	2000 mx2000m
Number of Nodes	500
Transmission range	250 m
Packet Size	1000 bits
Initial Energy	100J
Node deployment	Uniform Random

The communication overhead is the measurement of total number of packets transmitted from source to destination node in direct or hop-by-hop manner. This overhead includes data collection, security considerations and data aggregation. Below given figure 1 shows the comparative analysis of communication overhead for varied node scenario where we have considered 50 -500 number of nodes.

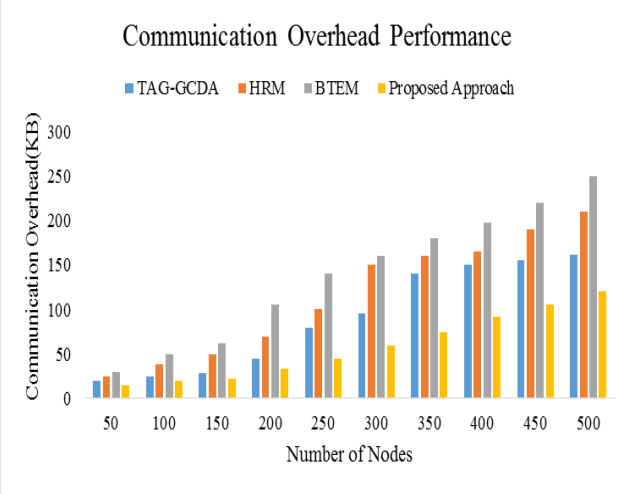

Fig.1. Comparative analysis of communication overhead

The performance quality of these schemes is arranged as BTEM, HRM, TAG-GCDA and Proposed Approach in the increasing order. The average performance of these schemes is obtained as 139.5, 115.8, 90 and 58.7 KB. In existing techniques, as the number of nodes is increasing, the overhead also increases. The graph analysis shows that the performance of proposed approach for 500 nodes is better when compared with existing techniques for 200 nodes. Initially, for 50 nodes, the performance of proposed approach is increased by 50%, 66%, and 33% by using BTEM, HRM and TAG-GCDA, respectively. Similarly for 500 nodes, the performance of proposed approach improved by 52%, 42.85%, and 25.46% by using aforementioned techniques.

In next phase, we measure the performance in terms of total energy consumed by network during the entire simulation period. This energy consumption includes energy consumed by several processes such as data sensing, collection, processing and aggregation at the cluster head. We use the same similar experimental setup as depicted in figure 1. The energy consumption performance for this scenario is depicted in figure 2.

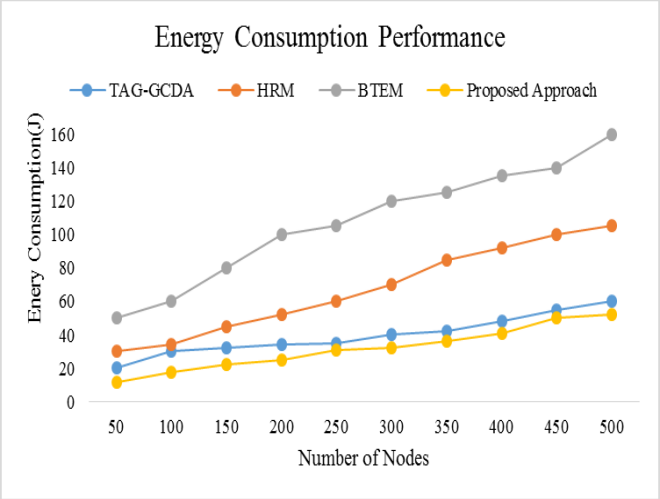

Fig.2. Energy consumption performance

The average energy consumption is obtained as 107.5 J, 67.3J, 39.6J and 31.9 using BTEM, HRM, TAG-GCDA and proposed approach. Proposed approach achieves superior performance as energy consumption performance is improved by 70.32%, 52.60%, and 19.44% when compared with aforementioned techniques. For 50 node scenario, the proposed approach consumes energy as 52J, BTEM consumes 50 J, HRM consumes 30J and TAG-GCDA consumes 20J. Similarly, for 500 node scenario, we obtained that the proposed approach consumes maximum energy as 52 J, BTEM consumes 160J, HRM consumes 105J, and TAG-GCDA consumes 60J. This shows that proposed approach outperforms in low density and high density network scenarios.

In next phase, we focus on the packet delivery performance analysis for varied number of data packets. Here, we measure the efficiency of network to deliver the specific data packets in the given time interval. For this experiment, we have considered 15 data packets for 50 sensor node, 30 data packets for 100 node, 45 data packets for 150 nodes, 60 data packets for 200 nodes, 75 data packets for 250 and so on. Finally, 150 data packets for 500 nodes.

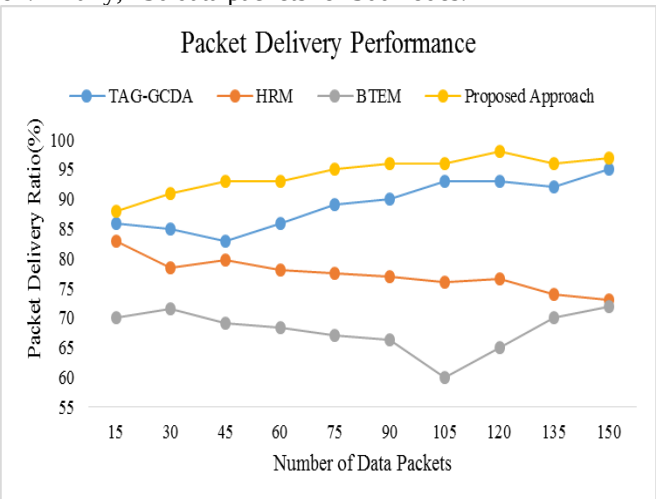

Fig. 3. Packet delivery performance for varied data packets

The average packet delivery performance is obtained as 67.94%, 77.335%, 89.2%, and 94.3 using BTEM, HRM, TAG-GCDA and proposed approach respectively. Based on

this average performance analysis, we obtain that the performance of proposed model is improved by 38.79%, 21.94%, and 5.71% when compared with BTEM, HRM, and TAG-GCDA techniques.

Similarly, we measure the packet drop rate performance for varied number of data packets. We considered the same experimental scenario as used in packet delivery performance measurement.

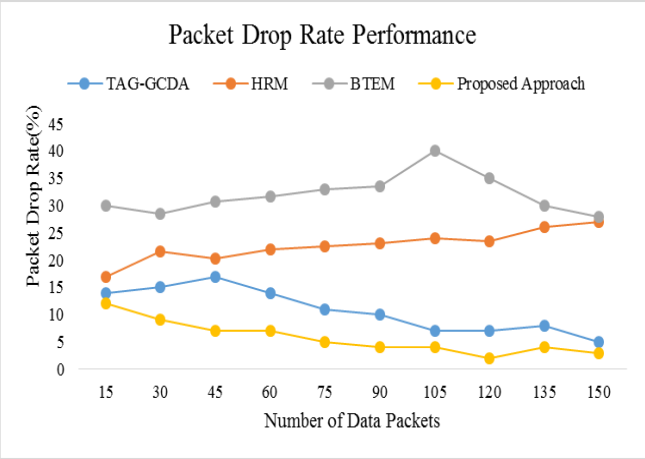

Fig. 4. Packet drop rate performance of data packets

From this experiment, we obtain the average packet drop rate as 32.06, 22.665, 10.8 and 5.7 using BTEM, HRM, TAG-GCDA and proposed approach. This comparative analysis shows that performance of proposed model is improved by 82.22%, 74.85%, and 47.22% when compared with BTEM, HRM, and TAG-GCDA schemes, respectively.

Conclusion

In this work, we have presented a novel data aggregation scheme to improve the network lifetime. The conventional data aggregation schemes suffer from the high energy consumption and fails in maintaining the security during data aggregation process. Hence, we present a combined approach to accomplish these objectives. First of all, we present an energy aware cluster formation and cluster head selection. In this approach, the nodes are divided as normal node, advanced and super node based on their energy levels. We proposed a model to compute the optimal number of cluster formation and CH selection. The CH node is responsible for aggregation. Further, we present trust computation based mechanism to incorporate the security aspects. The experimental study shows improved performance of the system in terms of communication overhead, energy consumption, packet delivery, and packet drop rates.

References

[1] Gao, L., Zhang, G., Yu, B., Qiao, Z., & Wang, J. (2020). Wearable human motion posture capture and medical health monitoring based on wireless sensor networks. Measurement, 166, 108252.

[2] Khan, M., Silva, B. N., & Han, K. (2016). Internet of things based energy aware smart home control system. Ieee Access, 4, 7556-7566.

[3] Ali, A., Ming, Y., Chakraborty, S., & Iram, S. (2017). A comprehensive survey on real-time applications of WSN. Future internet, 9(4), 77.

[4] Botero-Valencia, J., Castano-Londono, L., Marquez-Viloria, D., & Rico-Garcia, M. (2018). Data reduction in a low-cost environmental monitoring system based on LoRa for WSN. IEEE Internet of Things Journal, 6(2), 3024-3030.

[5] Lah, A. A. A., Latiff, L. A., Dziyauddin, R. A., Kaidi, H. M., & Ahmad, N. (2017, December). Smart traffic monitoring and control architecture and design. In 2017 IEEE 15th Student Conference on Research and Development (SCOReD) (pp. 72-76). IEEE.

[6] Ali, A., Ming, Y., Chakraborty, S., & Iram, S. (2017). A comprehensive survey on real-time applications of WSN. Future internet, 9(4), 77.

[7] Wang, X., Zhou, Q., Gu, Y., & Tong, J. (2019). Compressive sensing-based data aggregation approaches for dynamic WSNs. IEEE Communications Letters, 23(6), 1073-1076.

[8] Liu, B. H., Pham, V. T., Nguyen, T. N., & Luo, Y. S. (2019). A heuristic for maximizing the lifetime of data aggregation in wireless sensor networks. arXiv preprint arXiv:1910.05310.

[9] Zhang, J., Lin, Z., Tsai, P. W., & Xu, L. (2020). Entropy-driven data aggregation method for energy-efficient wireless sensor networks. Information Fusion, 56, 103-113.

[10] Yin, X., Li, S., & Lin, Y. (2019). A Novel Hierarchical Data Aggregation with Particle Swarm Optimization for Internet of Things. Mobile Networks and Applications, 24(6), 1994-2001.

[11] Kim, T. H., & Madhavi, S. (2020). Quantum Data Aggregation Using Secret

Sharing and Genetic Algorithm. IEEE Access, 8, 175765-175775.

[12] Mosavvar, I., & Ghaffari, A. (2019). Data aggregation in wireless sensor networks using firefly algorithm. Wireless Personal Communications, 104(1), 307-324.

[13] Li, X., Liu, W., Xie, M., Liu, A., Zhao, M., Xiong, N. N., ... & Dai, W. (2018). Differentiated data aggregation routing scheme for energy conserving and delay sensitive wireless sensor networks. Sensors, 18(7), 2349.

[14] Kang, B., Nguyen, P. K. H., Zalyubovskiy, V., & Choo, H. (2017). A distributed delay-efficient data aggregation scheduling for duty-cycled WSNs. IEEE Sensors Journal, 17(11), 3422-3437.

[15] Haseeb, K., Islam, N., Saba, T., Rehman, A., & Mehmood, Z. (2020). LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. Sustainable Cities and Society, 54, 101995.

[16] Yousefi, H., Yeganeh, M. H., Alinaghipour, N., & Movaghar, A. (2012). Structure-free real-time data aggregation in wireless sensor networks. Computer Communications, 35(9), 1132-1140.

[17] Koupaee, M., Kangavari, M. R., & Amiri, M. J. (2017). Scalable structure-free data fusion on wireless sensor networks. The Journal of Supercomputing, 73(12), 5105-5124.

[18] Fang, W., Wen, X., Xu, J., & Zhu, J. (2019). CSDA: a novel cluster-based secure data aggregation scheme for WSNs. Cluster Computing, 22(3), 5233-5244.

[19] Hua, P., Liu, X., Yu, J., Dang, N., & Zhang, X. (2018). Energy-efficient adaptive slice-based secure data aggregation scheme in WSN. Procedia Computer Science, 129, 188-193.

[20] Merad Boudia, O. R., Senouci, S. M., & Feham, M. (2018). Secure and efficient verification for data aggregation in wireless sensor networks. International Journal of Network Management, 28(1), e2000.

[21] Shobana, M., Sabitha, R., & Karthik, S. (2020). Cluster-based systematic data aggregation model (CSDAM) for real-time data processing in large-scale WSN. Wireless Personal Communications, 1-19.

[22] Hu, S., Liu, L., Fang, L., Zhou, F., & Ye, R. (2019). A Novel Energy-Efficient and Privacy-Preserving Data Aggregation for WSNs. IEEE Access, 8, 802-813.

[23] Roslin, S. E. (2020). Data validation and integrity verification for trust based data aggregation protocol in WSN. Microprocessors and Microsystems, 103354.

[24] Boubiche, D. E., Boubiche, S., Toral-Cruz, H., Pathan, A. S. K., Bilami, A., & Athmani, S. (2016). SDAW: secure data aggregation watermarking-based scheme in homogeneous WSNs. Telecommunication Systems, 62(2), 277-288.

[25] Qi, X., Liu, X., Yu, J., & Zhang, Q. (2020). A privacy data aggregation scheme for wireless sensor networks. Procedia Computer Science, 174, 578-583.

[26] Uvarajan, K. P., & Gowri Shankar, C. (2020). An Integrated Trust Assisted Energy Efficient Greedy Data Aggregation for Wireless Sensor Networks. Wireless Personal Communications, 1-21.

[27] Alotaibi, M. (2019). Security to wireless sensor networks against malicious attacks using Hamming residue method. EURASIP Journal on Wireless Communications and Networking, 2019(1), 8.

[28] Anwar, R. W., Zainal, A., Outay, F., Yasar, A., & Iqbal, S. (2019). BTEM: Belief based trust evaluation mechanism for Wireless Sensor Networks. Future Generation Computer Systems, 96, 605-616.