

Trust Oriented Efficient Data Aggregation and Malevolent Node Detection in the Internet of Things Sensor Network

¹Swathi S and ²Yogish H. K

¹Research Scholar, Department of Computer Science and Engineering, M. S. Ramaiah Institute of Technology, Bengaluru, India

Email: s.swathieswar@gmail.com

²Professor & Head, Department of Information Science and Engineering, M. S. Ramaiah Institute of Technology, Bengaluru, India

Email: yogishhk@gmail.com

Abstract—Sensor technologies that enable monitoring and sensing of various environmental events in the Internet of Things are driven by limited energy resources and computing constraints. To improve energy efficiency, the sensor node is required to perform data aggregation process to eliminate redundancy in the information obtained from adjacent nodes before transmitting to the local access point. However, the sensor nodes are vulnerable to many security threats, the information gathered can be falsified by malevolent nodes. Many solutions for reliable information aggregation and malevolent node detection have been introduced in the existing literature. However, all these solutions have certain limitations that do not meet the requirements of maintaining higher energy efficiency, maximum security, and low computational overhead. To this end, this paper proposes a quantitative trust model for evaluating the reliability factors of each communicating node. The model computes trust values based on the behavioral analysis of each node, and the optimal nodes with higher trust values are selected for the clustering and data aggregation process. Malevolent nodes are identified by a trusted entity located in the base station that uses statistical analysis for the received sensor node information. The proposed model is implemented on a numerical computing tool. The effectiveness and scope of the proposed system are assessed regarding packet delivery ratio, network overload, and energy utilization. The outcome shows that proposed model achieved 16% improvement in the packet delivery ratio, 16.6% improvement in reduction of network overhead, and 27.73% improvement regarding energy efficiency compared to existing method.

Index Terms— Data Aggregation, Internet of Things, Malevolent Node Detection, Sensor Network, Security, Trust Evaluation.

I. INTRODUCTION

With the advent of the Internet of Things (IoT), there has been a tremendous increase in connected devices for various applications. The IoT ecosystem consists of devices or nodes that function on sensing to capture the events observed in the surrounding environment [1]. These sensor nodes are characterized by their small size,

wireless connectivity, limited energy resources, constraint computing, processing, and storage capacity [2]. The sensory information collected by sensor nodes is mainly associated with the redundancy factor, which creates a burden on sensor nodes while processing these data [3]. In order to increase the service durability of sensor nodes, the critical process is to eliminate redundancy in the information received from neighboring nodes before it is transmitted to the base station (BS). Data aggregation is one of the effective mechanisms to exclude redundant information, which, after aggregating, provides fused information to the BS, enhancing the energy efficiency of the sensor nodes [4]. The process of data aggregation in the IoT sensor network scenario is depicted in Figure 1.

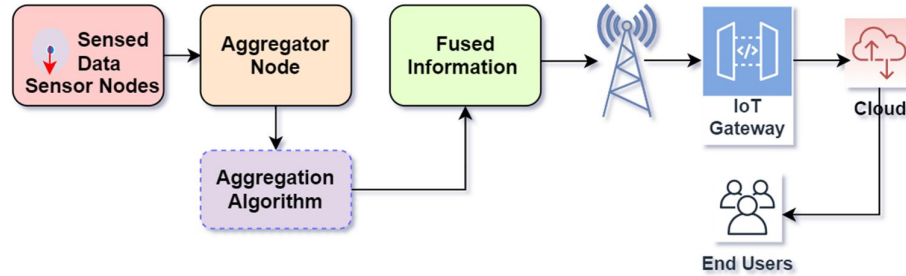


Figure 1. Data aggregation process in IoT Sensor network

The aggregator node receives the sensory information from the sensor nodes and aggregates using various algorithms like centralized, tiny aggregation, etc., which provides the fused data to the BS. The information is further shared with the end-user through IoT gateways and cloud systems. However, potential vulnerabilities associated with sensor nodes in the IoT ecosystem raise significant concern about the confidentiality and integrity of the collected data. Malevolent nodes in the network can falsify the aggregated information [5]. The prime reason behind this is that the sensor nodes are vulnerable to various security threats and attacks due to their design constraint, network heterogeneity, and lack of standard protocols. In the IoT ecosystem, the connection between sensor nodes is carried out without considering the sensor networks' responsible factors and design principles [6]. Since IoT is heterogeneous, and it is subject to the involvement of varied nature of application which makes IoT different from the sensor network. Therefore, the routing protocols in both network follows different methodology [7]. Most of the existing solutions are based on encryption techniques that are highly recursive in their operation and significantly impact the resource utilized by the constraint sensor nodes [8]. Currently, there are different types of attacks being investigated in sensor networks. However, the fact is that the existing solutions mostly depend on the adoption of cryptographic operations, the most suitable option for providing security against these attacks [9-10]. These solutions require a large range of memory and very repetitive operations that leads to faster energy consumption. Apart from encryption, researchers have also focused on introducing secure routing techniques against security threats and attacks. However, it has been observed that the existing routing approach is effective in resisting specific attacks and cannot identify the spiteful behavior of the nodes [11]. In this context, it has been found that trust-based solutions provide a slightly better security feature for carrying out information gathering and detection of attacks in the network [12]. In a trust-based approach, a reliability factor of nodes is computed based on the analysis of node behavior with the other nodes in the network. In the existing literature, the solution based on trust factors evaluation is also associated with some limitations and issues such as non-consideration of delay, link quality, reselection of aggregators, and balanced factor between energy efficiency and communication performance. To maintain the integrity of data and a maximum layer of protection to the network, it is vital to evaluate the reliability factor associated with each communicating node considering the network's responsible factors. This paper presents a quantitative trust model to address security issues associated with data aggregation and communication processes in the IoT sensor network. The significant contribution of the proposed system is highlighted as follows:

- An efficient and trust evaluation model is designed to evaluate the reliability of nodes for carrying out data aggregation tasks.
- The trust value is computed based on the behaviour of sensor nodes, including
- The BS carries out detection of malevolent nodes based on the report that contains information about the trusted nodes and untrusted nodes.
- Benchmarking is done to validate the effectiveness and performance of the proposed model.

The remaining section of this paper is organized as follows: Section II discusses the existing works in the context of reliable data aggregation and spiteful node processes in the network. Section III highlights the problem description. Section IV presents the system design and methodology adopted for the proposed quantitative trust model. Section V discusses the outcome and performance analysis of the proposed model. Finally, the entire contribution of this paper is concluded in Section VI.

II. RELATED WORK

Extensive research efforts have been made to address security issues in sensor networks. This section mainly focuses on the review of literature based on trust and attack detection mechanisms, which offers significant decision-making in the process of ensuring reliable communication operations in WSNs. The authors' work in the study of [13] focused on addressing security issues associated with IPv6-oriented sensor networks. A distributed system is designed that uses the probability estimation technique to identify malevolent nodes in the network. A cooperative decision-making process is carried out to analyse the malevolent behaviour of sensor nodes. An intrusion detection system (IDS) introduced by [14] for WSNs is developed based on the trust score computed for the communicating nodes in the network. The authors used this IDS to isolate attacks based on the network traffic and node behaviour. The study showed detection of jamming, flooding, and selective forwarding attacks. The work done in [15] designed a security algorithm based on the cryptography concept to enable robust authentication against Sybil attacks. The model validation is carried out considering different performance metrics such as time taken for key sizes, energy utilization, data delivery rate, and throughput. The study of [16] developed a trust monitoring system for secure data aggregation in a sensor network. In this method, every node computes the trust value of their adjacent nodes and afterward executes CH selection, data aggregation, and data reporting to the centralized centre. A recent work of [17] has suggested a trust model designed based on the approach of game theory to provide a better layer of protection to the network against denial-of-service (DoS) attacks in a sensor network. Similarly, in [18] transformation approach is considered against DoS in the Zigbee-sensor network. An effective information aggregation technique using the trust level and reputation method is given by [19] to ensure the reliability of aggregated information. The study adopted fuzzy logic and reputation method for node trust evaluation and secure path selection, respectively. The study outcome shows that this approach is energy-efficient and robust against attacks in the network. A Self-attestation scheme was adopted in the study of [20] to evaluate the trust level of the nodes in the sensor network for ensuring the integrity of data provided by the sensor nodes. Also, the use of blockchain technology for trust modelling is used in the work of [21] to detect security threats. In [22], trust computation is done using a clustering-based mechanism, where the node's constraint was considered a prime factor in the routing operation. In [23], fair trust-based malevolent node detection and isolation are suggested based on the neighbour-weight trust computation mechanism. This mechanism considered trust update factors-based reputation, which overlooks significant issues associated with network security, mean behaviour of nodes, and trust recovery issues [23]. Few research works have been found towards the adoption of soft computing approaches. The authors in [24] used the least squared technique for trust calculation. In [25], cross-layer combined with fuzzy logic is used for trust evaluation. In [26], secured routing approaches are mentioned to compute node trust levels for efficient data transmission. The analytical model developed in [27][28][29] improves energy efficiency and trust computation for alleviating malevolent nodes in the network.

III. PROBLEM DESCRIPTION

This section highlights significant problems identified for the above discussed existing literature.

- While designing a security model for efficient data aggregation, the existing schemes have less focus on energy-constraint factor of the nodes. Also, lack of focus on data correlation despite trust computation being done from multiple perspectives.
- The security solution for the data aggregation model is also not considered a latency factor, which is important for some applications in the IoT context.
- Most of the existing methods suffer in detecting multiple attacks.
- The current solution does not consider a recovery mechanism for nodes that are identified as compromised nodes.
- Systematic evaluation of direct and indirect trust values is necessary to increase the life of the network.
- Most existing trust-based solutions involve recursive operations and are subject to computational complexity.

IV. SYSTEM MODELLING

This section presents the design and methodology adopted for building an efficient model for enabling a secure data aggregation process and detection of malevolent nodes in the IoT sensor network. Before discussing the core operations of the proposed model, this section presents the motivation behind the proposed work in the next subsection.

A. Motivation

The sensor network is considered a pillar of the IoT ecosystem that plays a significant role in the process of event monitoring, tracking, and data sense. But owing to the constraint nature of sensor nodes, heterogeneity of the IoT ecosystem, a significant concern arises regarding the security of data sensed by constraint sensor nodes. Thus, a crucial requirement is to protect the network against dynamic security threats. At the same time, integrity and confidentiality must be maintained even if there is a presence of malevolent nodes in the network. To date, there are many solutions proposed by the researchers. However, such existing solutions are not much suitable for the IoT context due to their complexity and design to the specific attacks. Hence, the context of IoT demands exploratory analysis of the possible vulnerabilities, attacks, security design challenges, and potential solutions from the perspective of maximum-security requirements for both data and IoT devices.

B. System Design

The proposed system aims to design and develop a quantitative trust model (QTM) for ensuring the confidentiality and integrity of the aggregated data in the IoT sensor network. The proposed model uses an analytical methodology to construct an efficient collaborative trust modeling at the sensing layer and detection of malevolent nodes at the centralized local data access point (BS). The entire operation of the proposed QTM is carried out in two phases. The schematic architecture of the proposed system QTM is mentioned in figure 2. In the first phase of implementation reliability factor associated with each node is computed. The SN monitors the behavior of their adjacent SN and communication activities such as data forwarding, remaining energy, preserving data integrity, and many more. The proposed QTM computes linear trust factor (i.e., direct trust) and non-linear trust value (indirect trust) of nodes. Based on the computation of nodes' linear and non-linear reliability factors, QTM computes the final reliability factor as consolidated trust score (CTS). The obtained CTS is then used to execute significant operations in the network, such as clustering, aggregation, and conveying aggregated information to the BS.

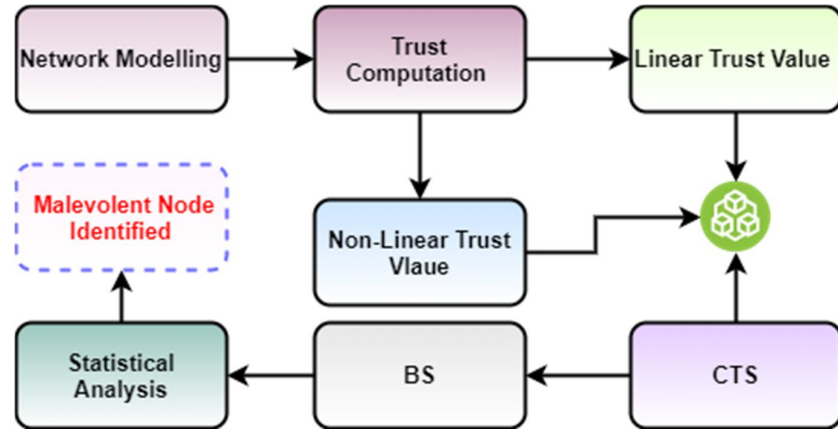


Figure 2. Schematic architecture of the proposed system QTM

In the second phase of implementation, the trusted and secure component located at BS carries out the process of malevolent nodes detection based on the statistical analysis. The information related to detection operation is reported back to the network via BS, which consists of a query that alerts valid SN to not select the malevolent node as data aggregator node in the clustering process. Moreover, the BS maintains a list of all identified malevolent nodes and discards their participation in data aggregation. The core objective of the proposed QTM is to provide an effective decision-making process towards secure data aggregation, detection, and isolation of the malevolent nodes.

C. Network Modelling

The proposed study considers a homogenous sensor network in the IoT ecosystem, where SNs are static and deployed randomly in the deployment area of $M \times N$. The study also considers that the network is not being compromised during the initial phase of network modelling and SN deployment. The sensor network (N) can be numerically represented as follows:

$$N \ni \{SN_1, SN_2, SN_3, \dots, SN_N, BS\} \quad (1)$$

Each SN has a fixed communication range (CR), and it can use the direct or multi-hop path to communicate with BS. The study also assumes that BS is secure and can be compromised due to enough resources and robust security features. A trusted component located at BS that can perform statistical analysis to carry out an operation of malevolent node detection. BS broadcasts a query message (msg) to SN to execute the DA process, and upon receiving the msg, SN initiates the setup phase for clustering. The study adopts the concept of LEACH protocol in the CH selection process. The following energy model expression can give the energy consumed by SN to forward kbit data to distance “d”:

$$E_{Tx}(k, d) = \begin{cases} k \times E_r + k \times E_u \times d^2, & \text{if } d_c > d \\ k \times E_r + k \times E_a \times d^4, & \text{if } d_c \leq d \end{cases} \quad (2)$$

Where, E_r refers to the energy needed for functioning transmitter and receiver E_u and E_a refers to unit energy required to function amplifier circuit, d_c denotes crossover distance computed as follows:

$$d_c = \sqrt{\frac{E_u}{E_a}} \quad (3)$$

Moreover, the energy consumed while receiving packets E_{Rx} can be given as follows;

$$E_{Rx} = k \times E_r \quad (4)$$

D. Trust Computation

The proposed system QTM computes the linear trust (α) value and non-linear trust (β) value associated with SN to compute the final CTS. The computation of α is carried out based on the behaviour metrics (Bm) of the SN, which contains a metric such that: $Bm \ni \{B1, B2, B3 \dots Bn\}$. Table I present details of these metrics as follows:

TABLE I. DESCRIPTION OF BEHAVIOR METRICS FOR TRUST COMPUTATION

Sl.NO	Metrics	Description
1	B1	A pattern of sensory data reporting
2	B2	A pattern of data forwarding
3	B3	A pattern of maintaining data integrity
4	B4	A pattern of reporting the data timely
5	B5	A pattern of reporting about remaining energy
7	B6	A pattern of trust recommendation <i>tR</i>

The aggregator node (AN) and regular node (SN) both collaboratively participate in the process of α computation. The AN is accountable for observing $Bm_i \ni \{F1, F4\}$ and SN is accountable for observing $Bm_j \ni \{F2, F3, F5, F6\}$. The interaction between two communicating SN-1 and SN-2 will be considered successful when both have identical behaviour patterns, and else the interaction will be considered a condition of failover. In these cases, the proposed QTM initializes two control variables $f_s()$ and $f_f()$ for $\forall Bm$. The control variable f_s increments corresponding Bm by count 1 for every successful interaction of communicating SNs. In case of failover, the control variable f_f will increment corresponding Bm by count 1. The computation of α is considered as multi-criteria decision analysis, numerically given as follows:

$$\alpha(SN_i) = \sum_{i=1}^4 W_i(Bm_i) \times P(Bm_i) \quad (5)$$

Where W_i denoted the weighting factor, and P denotes expected values of Bm in the range [0,1]. The computation of P is numerically expressed in equation 8.

$$W(Bm_i) = \frac{f_s(Bm_i)}{f_{stot}(SN_i)} \quad (6)$$

Where, f_{stot} is the control variable that indicates the total count for overall successful interaction for SN_i numerically given as follows:

$$f_{\text{stot}}(SN_i) = \sum_{i=1}^4 f_S(Bm_i) \quad (7)$$

$$P(Bm_i) = \frac{f_S(Bm_i)+1}{f_S(Bm_i)+f_S(Bm_i)+2} \quad (8)$$

Since W and $P \in Bm_i$ ranges between $[0, 1]$, the value of α also ranges between $[0, 1]$. Further, the model QTM computes reliability factor (rF) as follows:

$$rF(SN_i) = \begin{cases} \frac{1}{f_{\text{stot}}(SN_i)}, & \text{if } f_{\text{stot}}(SN_i) > 2 \\ 0.8, & \text{Otherwise} \end{cases} \quad (9)$$

From equation 9, it can be analyzed that rF of SN_i highly depends on the increasing number of successful SN interactions. The computation of β is carried out based on the trust recommendations (tR) acquired from the adjacent SNs. In this process, the proposed QTM system filters out the misleading recommendations to assist computation of precise value of β numerically given as follows in equation 10:

$$\beta(SN_k) = \sum_{k=3}^{Bn-1} W_j(SN_k) \times \left(\frac{\alpha_{SN_j}^r}{r_{\text{max}}} \right) \quad (10)$$

Where, SN_k refers to the k adjacent nodes of SN_j which is the adjacent node of SN_i . Therefore, the SN_i and SN_j are the communication nodes and SN_k is adjacent nodes of the two communication nodes. Figure 3 represents this scenario in a more descriptive form. The symbol W_j refers to the weighting factor for SN_k for computing β , the coefficient r denotes recommended trust value and r_{max} is the maximum value of r equal to a hundred. The computation of the weighting factor W_j can be numerically expressed as follows in equation 11:

$$W_j(SN_k) = \frac{f_{\text{stot}}(SN_j)}{\sum_{k=3}^{Bn-1} f_{\text{stot}}(SN_j)} \quad (11)$$

Further, based on the obtained value of α and β , CTS will be computed using a reliability factor (rF) that indicated a degree of behaviour reliability among the communicating SN. The computed value of CTS lies in the range $[0,1]$. The CTS value greater than 0.8 will be considered true SN; else, it is a malevolent SN. The computation of CTS value is expressed in the numerical equation 12 as follows:

$$CTS = rF(SN_j) \times \alpha(SN_j) + (1 - rF(SN_j)) \times \beta(SN_j) \quad (12)$$

Where $CTS \leftarrow$ ranges $[0,1]$

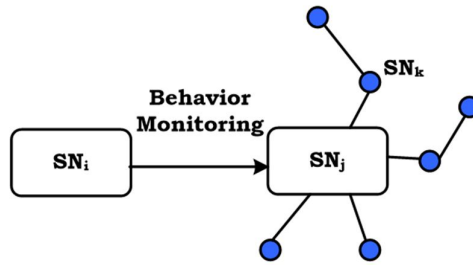


Figure. 3. A generic representation of communication adjacent sensor node behavior observation

D. Malevolent Node Identification

Both AN and BS are responsible for carrying out the identification of the malevolent nodes. Initially, the AN computes CTS of their corresponding regular SNs. Then, it detects and flags the SN having CST score less than the mean of CTS of adjacent SNs and conveys this information along with the aggregated data to the BS. However, if the acknowledged CTSs of SN_i via BS is less compared to the CTSs measured by SN_k in the network. Then it indicates that conveyed CTS followed Gaussian distribution, and the variance of Malevolent

SN is not known. The trusted component located at BS then considers this problem as a statistical estimation problem where the objective is to identify a malevolent node. Therefore a statistical analysis is carried out using equation 13 as follows:

$$Htest = \frac{\mu - \overline{CTS(SN_i)}}{e} \quad (13)$$

Where $Htest$ hypothetical test, μ indicates hypothetical mean and $\overline{CTS(SN_i)}$ from equation 13 and e refers to sample error given in equation 14 and 15 as follows:

$$\overline{CTS(SN_i)} = \sum \frac{CTS(SN_i)}{SN_N} \quad (14)$$

$$e = \sqrt{\frac{\sum_{j=1}^{SN_N} CTS(SN_j) - \overline{CTS(SN_i)}}{SN_N}} \quad (15)$$

The study compares the outcome of the $Htest$ with the value obtained from the cumulative distribution function to check the difference of sample mean from the hypothetical mean of the user-based significance level. The BS maintains two hypothetical values null and critical. Suppose the statistical analysis shows that there is no much difference between the sample and the hypothetical average. In that case, the analysis admits a null hypothesis, or else it accepts a critical hypothesis, which indicates the node is malevolent. The BS makes a list for the nodes with critical hypothesis values and further conveys it to the network with a query message. The true nodes will alert the AG and not communicate with the compromised nodes to carry out any network-related task.

V. RESULT ANALYSIS

This section presents the outcomes and performance analysis of the proposed system QTM. The development of the proposed QTM is performed in a numerical computing environment. The effectiveness of the proposed system is assessed based on the comparative analysis considering energy utilization, network overhead, and data delivery rate as significant performance metrics. The outcome of the proposed scheme is compared with the existing approaches, namely, SecLeach [31], CBTRP [32]. The simulation parameters for experimental purposes are described in table II.

TABLE II SIMULATION PARAMETERS

SI. NO	PARAMETERS	VALUES
1	Simulation area	100 x 100 m ²
2	Packet length	512 bytes
3	Number of SN	500
4	Number of malevolent nodes	5 (%)
5	Simulation time	2000
6	Initial energy	5mj

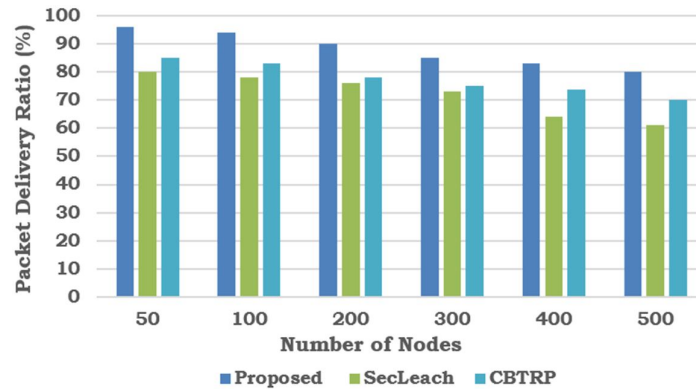


Figure 4. Packet delivery ratio

In figure 4, analysis is carried for accessing the performance of packet delivery ratio by the proposed system compared with existing methods. The graphical observation illustrates that the proposed QTM outperforms other

methods, improving 16% and 11.6% over SecLeach and CBTRP, respectively. The existing method, CBTRP, showed a gain of 4.93% of improvement over SecLeach.

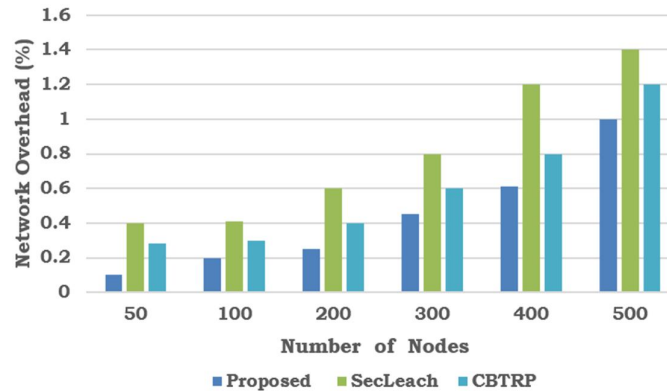


Figure 5. Network Overhead

In figure 5, analysis is carried for accessing performance regarding network overhead. The outcome of the proposed system QTM compared with existing methods SecLeach and CBTRP. The graphical observation illustrates that the proposed QTM outperforms SecLeach and CBTRP methods, improving 36.6% and 16.1%, respectively. The existing method, CBTRP, showed a gain of 20.5% of improvement over SecLeach.

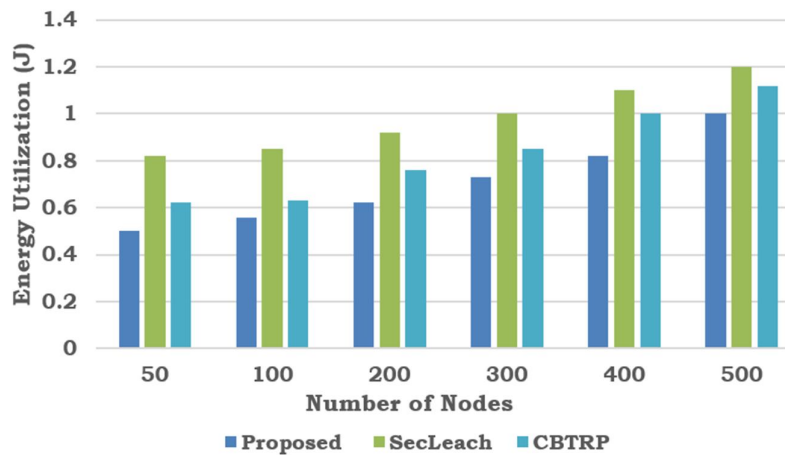


Figure6. EnergyUtilization

In figure 6, analysis is carried for accessing performance regarding energy utilized by the sensor nodes during network activities. The graphical observation proves that the proposed QTM outperforms existing methods SecLeach and CBTRP, improving 27.73% and 12.51% over SecLeach and CBTRP, respectively. The existing method, CBTRP, showed a gain of 15 % of improvement over SecLeach. The reason behind the better performance achieved by the proposed system is that the simple and non-recursive implementation approach for trust computation and data aggregation. The proposed system provides a secure mechanism for data aggregation by allowing only trusted nodes and discarding the participation of malicious sensor nodes. The proposed model enables a secure routing operation by selecting only trusted nodes in the data forwarding operation. The uniqueness of the proposed system is that it maintains maximum security in the network, such as confidentiality, integrity, and privacy of the data from the process of aggregation to the base station transmission.

VI. CONCLUSION

This paper has introduced an efficient security mechanism for secure data aggregation and malicious sensor node detection in the network. An approach of quantitative trust modelling is carried out to the reliability factors of the sensor nodes based on their behavioural metrics and observation, and further, two trust factors are fused to

compute the final trust score for each participating node in the network. Before any data networking activities, the aggregator node forwards the list of trust scores with the unique identity of nodes for which the trust score is being computed. The trusted component located at the base station uses statistical analysis to detect the presence of malicious nodes. The simulation outcome exhibited the effectiveness of the proposed QTM in terms of network performance metrics and energy efficiency. The proposed system has achieved a 16% improvement in the packet delivery ratio, 16.6% improvement in reduction of network overhead, and 27.73% improvement regarding energy efficiency. In the future work, the proposed study will be extended towards incorporating recovery mechanism for the compromised node identified in the network enhancement using machine learning technique.

REFERENCES

- [1] Vidhyotma, Singh J. (2019) IoT: Architecture, Technology, Applications, and Quality of Services. In: Hu YC., Tiwari S., Mishra K., Trivedi M. (eds) Ambient Communications and Computer Systems. Advances in Intelligent Systems and Computing, vol 904. Springer, Singapore
- [2] Li, S., Xu, L.D. & Zhao, S. The internet of things: a survey. *Inf Syst Front* 17, 243–259 (2015).
- [3] Geetika Dhand, S.S. Tyagi, Data Aggregation Techniques in WSN: Survey, *Procedia Computer Science*, Volume 92, 2016, Pages 378–384, ISSN 1877-0509
- [4] Ozdemir, Suat, and Yang Xiao. "Secure data aggregation in wireless sensor networks: A comprehensive overview." *Computer Networks* 53, no. 12 (2009): 2022–2037.
- [5] Sathya, Duraisamy. "Secured data aggregation in wireless sensor networks." *Sensor Review* (2018).
- [6] Nguyen TD, Khan JY, Ngo DT (2017) An effective energy-harvesting-aware routing algorithm for WSN-based IoT applications. In: IEEE international conference on communications (ICC), pp 1–6
- [7] Agnihotri, Shailja, and K. R. Ramkumar. "A survey and comparative analysis of the various routing protocols of Internet of Things." *International Journal of Pervasive Computing and Communications* (2017).
- [8] Rehman SU, Khan IU, Moiz M, Hasan S (2016) Security and privacy issues in IoT. *Int J Commun Netw Inf Secur* 8(3):1–147
- [9] Burhanuddin MA, Mohammed AAJ, Ismail R, Hameed ME, Kareem AN, Basiron H (2018) A review on security challenges and features in wireless sensor networks: IoT perspective. *J Telecommun Electron Comput Eng* 10(1–7):17–21
- [10] Tellez M, El-Tawab S, Heydari MH (2016) IoT security attacks using reverse engineering methods on WSN applications. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 182–187
- [11] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." *IEEE Communications Surveys & Tutorials* 17, no. 3 (2015): 1294–1312.
- [12] Fang, Weidong, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni, and Yinxuan Yang. "Trust-based attack and defense in wireless sensor networks: a survey." *Wireless Communications and Mobile Computing* 2020 (2020).
- [13] Grgic, K., Zagar, D., & Cik, V. K. (2016). System for Malevolent node detection in IPv6-based wireless sensor networks. *Journal of Sensors*.
- [14] Sajjad SM, Bouk SH, Yousaf M. Neighbor node trust based intrusion detection system for WSN. *Procedia Comput Sci*. 2015;63:183–188.
- [15] Beno, M. (2017). Secure data aggregation in wireless sensor Network Fujisaki Okamoto (FO) authentication scheme against Sybil attack. *Journal of Medwell Systems*. <https://doi.org/10.1007/s10916-017-0743-2>.
- [16] Potukuchi RV, Kant K. Secure data aggregation and intrusion detection in wireless sensor networks. *Proceedings of International Conference on Signal Processing and Communication (ICSC)*; 2015
- [17] Abdalzaher MS, Samy L, Muta O (2019) Non-zero-sum game-based trust model to enhance wireless sensor networks security for IoT applications. *IET Wirel Sensor Syst* 9(4):218–226
- [18] Chen H, Meng C, Shan Z, Fu Z, Bhargava BK (2019) A novel Low-rate Denial of Service attack detection approach in ZigBee wireless sensor network by combining Hilbert-Huang Transformation and Trust Evaluation. *IEEE Access* 7:32853–32866
- [19] Kumar M, Dutta K. LDAT: LFTM based data aggregation and transmission protocol for wireless sensor networks. *J Trust Manag*. 2016;3(1):2.
- [20] Desai SS, Nene MJ (2019) Node-level trust evaluation in wireless sensor networks. *IEEE Trans Inf Forensics Secur* 14(8):2139
- [21] She W, Liu Q, Tian Z, Chen JS, Wang B, Liu W (2019) Blockchain trust model for Malevolent node detection in wireless sensor networks. *IEEE Access* 7:38947–38956
- [22] Khan T, Singh K, Abdel-Basset M, Long HV, Singh SP, Manjul M (2019) A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. *IEEE Access* 7:58221–58240
- [23] Zawaideh F, Salamah M, Al-Bahadili H. A fair trust-based Malevolent node detection and isolation scheme for WSNs. *Processes & Systems (IT-DREPS)*. 2nd international conference on the applications of information Technology in Developing Renewable Energy; 2017.

- [24] Liu Y, Li C (2018) Secure distributed estimation over wireless sensor networks under attacks. *IEEE Trans Aerosp Electron Syst* 54(4):1815–1831
- [25] Umar IA, Hanapi ZM, Sali A, Zulkarnain ZA (2017) TruFiX: a configurable trust-based cross-layer protocol for wireless sensor networks. *IEEE Access* 5:2550–2
- [26] Qin D, Yang S, Jia S, Zhang Y, Ma J, Ding Q (2017) Research on trust sensing based secure routing mechanism for wireless sensor network. *IEEE Access* 5:9599–9609
- [27] Ahmed A, Bakar KA, Channa MI, Haseeb K, Khan AW (2015) TERP: A trust and energy aware routing protocol for wireless sensor network. *IEEE Sens J* 15(12):6962–6972
- [28] Yogeesh, A.C., Patil, S.B., Patil, P., Roopashree, H.R. (2019) Integrated framework for secure and energy efficient communication system in heterogeneous sensory application, *International Journal of Electrical and Computer Engineering*, 2019, 9(4), pp. 2695–2702.
- [29] Roopashree, H.R., Kanavalli, A., (2016) Joint algorithm for energy-conservation and secure key generation in wireless sensor network, *International Journal of Applied Engineering Research*, 2016, 11(4), pp. 2250–2257.
- [30] Roopashree, H.R., Kanavalli, A., (2016) SARDS: Secured anonymous routing with digital signature in wireless sensor network, *Indian Journal of Science and Technology*, 2016, 9(7).
- [31] Oliveira, Leonardo B., Hao Chi Wong, Marshall Bern, Ricardo Dahab, and Antonio Alfredo Ferreira Loureiro. "SecLEACH-A random key distribution solution for securing clustered sensor networks." In *Fifth IEEE International Symposium on Network Computing and Applications (NCA'06)*, pp. 145-154. IEEE, 2006.
- [32] Safa, Haidar, Hassan Artail, and Diana Tabet. "A cluster-based trust-aware routing protocol for mobile ad hoc networks." *Wireless Networks* 16, no. 4 (2010): 969-984.