Trust aware angle based secure routing approach for wireless sensor network

Hemavati Patil[1], **Vishwanath Tegampure**[2]
[1]Department of ISE, Guru Nanak Dev Engineering College, Karnataka, India
[2]Department of ECE, Bheemanna Khandre Institute of Technology, Karnataka, India

Article Info

Article history:

Received Jan 18, 2023
Revised Jul 14, 2023
Accepted Aug 30, 2023

Keywords:

Angle
Decryption
Encryption
Mobile agent
Routing
Security
Wireless sensor network

ABSTRACT

Security in wireless sensor network (WSN) is an important approach in the present context as data breaching is becoming more. The data to be routed from source to destination needs more security as WSN has no specific security approach by default. This paper proposes trust based security in WSN using approach. The secure line is drawn from head node to its cluster end point called as angle to provide the security to the nodes which are transferring the data to the head node. Secure line becomes the trust worth line where mobile agent migrates to all the corresponding nodes which are along or near to the secure lines, collects the data and encrypt them. Finally, the data is sent to sink node from head node using a secure path. The agent paradigm is responsible for creating the angle from head node to cluster boundary. Multiple angles can be created if numbers of nodes are more and deployed at different locations. The result shows that the security provided is much better to combat the intruder involvement to breach data along with better network lifetime and minimum delay than compare to conventional techniques.

Corresponding Author:

Hemavati Patil
Department of ISE, Guru Nanak Dev Engineering College
Bidar, Karnataka, 585403, India
E-mail: hbpatilbidar@gmail.com

1. INTRODUCTION

Wireless sensor network (WSN) are inexpensive, low-power (battery-operated), versatile, compact, and can connect over short distances. Depending on user needs, WSN nodes can be manually or arbitrarily distributed. WSNs have provided new perspectives for applications including monitoring, tracking, and surveillance. WSNs have garnered a lot of attention recently as a result of substantial developments in wireless and mobile communication technology as well as the wide development of possible applications [1], [2]. WSNs are nonetheless dynamically created from a number of power-constrained sensor nodes and a management node with long-lasting power. WSNs are self-organized, autonomous systems made up of back-end data centres, management nodes, and common sensors. First, the management nodes, which are intermediary collecting nodes, receive real-time sensor data from a specified pervasive environment from the common sensors [3]. The sensor information from the administrator nodes will then be sent to the back-end data-centre for additional processing and analysis. Certainly, wireless transmission mechanisms are used for all node-to-node interactions. Node deployment, energy usage while sacrificing accuracy, information report, node/link heterogeneity, fault tolerance, security, scalable, associated devices, connections, availability, aggregation of data, quality of service (QoS), and dynamic changes are among the significant design concerns in WSN [4]. When designing the WSN systems, the three main constraints taken into account are power usage, bandwidth, and storage capacity [5]. The sensors are typically installed in unsupervised locations where it is hard to replenish or change the battery [6]. The transmission expense is highest in WSN [7] when compared to the procedures for sensing and computing. In general, privacy protection and node authentication are indeed the two main security concerns that sensor nodes would be most concerned about [8]. By achieving data confidentiality through security measures, privacy enables secure network connections among sensor nodes and the management station. Additionally, a well-designed authentication method can guarantee that no authorised node may engage unlawfully and obtain sensitive data from WSNs. As a consequence, various different strategies to protect communications in WSNs have been put forth.

WSN routing is difficult due to the decreased bandwidth and battery-powered operation of the nodes. Ad hoc network routing techniques turned proven to be ineffective for sensor networks [9]. This is a result of the many ways that ad hoc and sensor networks have varied routing needs. In contrast to ad-hoc networks, communications in sensor networks, for example, is from several sources to a single sink. For WSN, several authors have developed routing algorithms, although they are only effective for specific scenarios. The node's data might be sent by a single path or several pathways [6]–[10]. When compared to single path routing, multipath routing uses less energy. In general the angle in degrees can be calculated using the formula:

$$cosA = (b * b + s * s - a * a) / 2bs$$

Where b is len(AS), a is len(S-BS), S is len(A-BS) and A is $\cos^{-1}(S)$ measured in degrees. Node, intermediate node and base station will form a triangle at the node A. Multi-hop routing raises a number of security and privacy challenges. Some of these problems, including as spying, sinkholes, Sybil manipulation, clones, wormholes, and spoofing, undermine the availability and reliability of the system [11].

Many security mechanisms have been put out for WSNs; nevertheless, due to sensor resource limitations, a few of these security mechanisms are not suitable for WSNs. As a result, such acceptance in WSNs is unfeasible. This is due to the design among most WSNs being unstable. Certain WSNs, in contrast to other networks, have mobile nodes which sometimes alter the topology of the network systems. As a result, such mobile networks cannot employ the current protocol created for static nodes. Additionally, the WSNs transport a lot of data, which raises the load just on WSN's wireless communications network [12], [13]. The majority of WSN routing protocols and security options are not appropriate for WSNs. This is because WSNs' resource limitations are to blame. The kind of security measures that may be used for WSNs are greatly influenced by these limitations [14], [15].

Agents are intelligent programmers located inside an environment that detect the surroundings and react on it to accomplish the objectives [10], [16]. They are a type of computer program that can complete a specified task in an independent manner. The agents carry out the following tasks: i) removing redundant information among nearby sensors by data fusion at the operational level; ii) removing redundant information between many sensors by application context-aware processing data at the node; and iii) lowering communication cost by convolving information at the cumulative task level. The components of mobile agent platforms include agents, an agent server, an interpretation, and transport protocols. Acquiring mobile agents and transmitting them for action by a local interpreter is the responsibility of an agent server. Agents can indeed be programmed in the languages Java, Tcl, Perl, and XML. Using an agent interpreter relies on the kind of agent language/script being utilised. The essential services are provided by an agent platform: generation of mobile and static agents, transit for mobile agents, security, communication messages, and persistence. Aglets, Grasshopper, Concordia, Voyager, and Odyssey are a few of the agent systems that use Java. Stationary and mobile agents are the two categories into which agents fall. Mobile agents are employed to collect information from various nodes and aggregate it, whereas static agents are employed to determine the path here between nodes.

The proposed work uses secure line to accept the updated data from the sensor nodes and the secure line is generated in the form of angle created from the head node (HN). The angle is created which covers most of the nodes in its line and more than one angle can be created in the given cluster. The cluster with HN is created and angle is drawn from the HN. The data generated from the nodes are sent to HN using secure line. On the secure line a mobile agent has been injected from the HN which passes through the secure line and gets the updated data from the nodes which are near to the secure line. Finally, the agent will submit all the received data to HN and later HN will send the data to sink node (SN). The proposed work improves the residual energy, provides security, reduces the overall delay and importantly improves the network lifetime of the sensor network. The rest of the paper has been organized as follow; section 2 depicts the literature review, section 3 provides the details of the proposed work along with its working and algorithms, section 4 describes the results of the proposed work and finally section 5 gives the conclusion of the paper.

2. LITERATURE REVIEW

Maheswari and Karthika [17] mentioned that, due to use of WSN in several sectors; it has become a popular study topic. Security, network longevity, and energy dissipation minimization are thought of as the three main QoS considerations in the design of WSN. Although clustering is a widely used energy-efficient strategy, it produces a hot spot problem. In order to meet QoS requirements like energy, longevity, and security, this study presents a unique safe unequal clustering method with intrusion detection approach. The provisional cluster heads are first chosen by the proposed method utilizing three input factors, including residual energy, distance to base station (BS), and distance to neighbours, using an adaptive neural fuzzy based clustering approach. The deer hunting optimization (DHO) method is used to pick the best CHs after the TCHs contend for the concluding CHs. The DHO based clustering algorithm uses remaining energy, distances to BS, node degree, node centralization, and connection quality to construct a fitness value. The cluster maintenance phase is used for load balancing to increase the effectiveness of the recommended method. Lastly, a powerful intrusion detection system employing a deep belief network is implemented on the CHs to recognize the existence of offenders in the network in order to accomplish security in cluster based WSN. To guarantee the suggested method's exceptional effectiveness in terms of energy conservation, network longevity, PDR, average latency, and intrusion detection rates, a comprehensive set of experiments was carried out.

Wang *et al.* [18] pointed out that intruders might employ the technique of hop-by-hop retracing in contexts where sensor networks are utilized to track hazardous objects or priceless resources to identify the secured objects. The phantom routing with locational angle (PRLA) is a novel source-protected technique in WSN that is proposed in this work. In PRLA, inclination angles are added and utilised to guide paths, preventing the selection of pathways that are damaging to the originating location's privacy. According to simulation findings, PRLA extends the protection duration by approximately to 50% with only slightly increasing energy overhead when contrasted to the phantom single-path routing protocol suggested in the research. The inclination angle can be calculated using the formula, $\alpha_i = \arccos\frac{H^2+h_i^2-h_s^2}{2*H*h_i}$ where α_i is the inclination angle.

R. *et al.* [19] suggested that the type of route that is built is crucial to the routing path. The effectiveness of transmission of data would be extremely high if the pathway between the sensor node and BS can be built in a straight line or very nearly in a straight line. By measuring the angle among the present node, the likely next node, and the BS using the cosine of that angle, the nodes that appear to be in a straight line may be located. The largest cosine angle will create a route that is almost straight whether this angle is the greatest amongst possibilities for the likely next node. Depending on this angle measuring method, which is created statically over a specific time period, the latest work creates the forwarding table. These RT elements will be used to statically create the route. The information would eventually use this route to transport the information towards BS. In the simulation, two alternative RT search criteria are contrasted. Insertion in the RT is employed in the first strategy. In contrast, the second technique determines the greatest angular entrance and uses it as the subsequent forwarding node. In the route creation process, which is static when looking at the work that is now being done? The simulation result is contrasted with the usual next node selection, which chooses the first entry in the forwarding table when building a route.

Mohapatra *et al.* [20] described that regardless of the fact that localization methods for wireless sensor networks have been researched for many years, there is still disagreement on the possibility of WSN positioning techniques which are straightforward, accurate, decentralised, and energy-efficient. Localization is not a major issue for static WSNs since once node placements are established, they are not expected to change. Mobile sensors, on the other hand, frequently need to estimate their position, which requires time, energy, and other resources that the sensing application needs.

Gupta *et al.* [21] mentioned that geographical routings are becoming more and more popular due to their scalability and capacity for local decision-making. Most frequently, greedy approaches are used in geographical routing protocols, which have the void node problem (VNP). An energy-efficient angular three-dimensional routing protocol (EA3DR) for wireless sensor networks is presented in this study. By taking into account leftover energy, the following hop is chosen from a certain conical angle (3D angle) towards the destination node. The choice of conical angle is influenced by network density. The conical angle can be adjusted in EA3DR in order to recover from VNP. If the packet becomes caught in the concave vacuum, it recovers by going back and chooses a different, more acceptable path. The suggested technique ensured packet receipt while using up a lot of leftover energy and cutting down on traffic congestion.

Zhang *et al.* [22] proposed robust based ant colony optimization for data transmission in WSN. The construction of energy-efficient route architecture for WSNs depends heavily on secure data transfer. Much emphasis has been made to the data transmission path's security. While ignoring the effects of malicious nodes, the majority of researchers simply pay attention to the security between data and route. In this study, before building the data transmission line, we first use the Bayesian voting method to identify the faulty nodes and delete them from the network. In order to extend the lifespan of the network, the authors suggest a new robust optimization based on ant colony optimization (ROACO) based robust optimization for choosing the path for transmitting data, in which the likelihood formula for choosing the node path takes into account a wide range of factors, including connection security, inconsistent data, node paths, and the remaining energy of the nodes. The suggested approach increases the percentage of the network's effective paths, decreases node load, and extends the lifespan of the network. Many researchers have worked on routing in WSN or optimization in WSN but very little work has been carried out on link security in WSN especially on secure clustering approach.

3. PROPOSED WORK

This section describes the system environment, working principle of the proposed work. The sensor network consists of sensor nodes, HN and sink nodes. The sensor network is divided into number of clusters and cluster consists of HN and remaining nodes are acting as common node. Based on the density of the nodes, the cluster formation is carried out i.e., cluster is created in such a manner where maximum nodes are being covered. The HN selection is done based on the criteria of maximum node coverage, sufficient residual energy and near to SN. In the conventional cluster based information gathering techniques gets data from the nodes either in time driven or event driven manner and each should has to use its residual energy to send the sensed data to HN or SN using direct path or multipath technique. In general, the cluster head (CH) selection is done based on the equation proposed for low energy adaptive clustering hierarchy (LEACH) type of networks which is as shown below. T(n) is the threshold value, P is the desired percentage of CH’s, r is the current round and G is the nodes which are not acted as CH’s. Our propose work is more advanced than the existing (1) for the selection of CH.

$$T(n) = \begin{cases} \frac{P}{1-P(rmod\frac{1}{P})} & if\ n \in G \\ 0 & otherwise \end{cases} \tag{1}$$

There are possibilities that the data breach may occur when the data is transmitted from sensor node to HN/SN. The data security is a major concern as the data may be confidential for particular application and needs security. The proposed work uses trust aware secure angle based data security. The system environment is as shown in Figure 1. Considering the maximum coverage of nodes in the cluster and secure angle has been drawn from the HN. The angle starts from the HN and ends at the cluster boundary end. Once the angle has been created, the mobile agent (MA) will be passed through the secured line to collect the data from the nodes which are near to the secure line (20 mts range). Agent collects the data encrypt it and migrate to next node and does the same. Finally, the data will be decrypted at the HN and decrypted data is sent to SN.

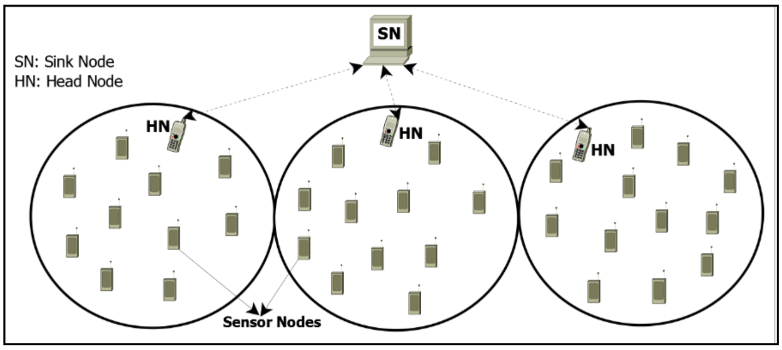

Figure 1. System environment

Multiple angles are created to cover all the nodes in the cluster network. In the HN database the angle information is stored and informed among all the nodes in the cluster. The data gathering process is carried out in time division multiple access (TDMA) manner or event driven manner. In TDMA based approach, once the time stamp expires, the HN injects the MA which travels in on the secure line and collects the data from the nodes which are near to the secure line and encrypts the received data using the Advanced encryption standard (AES) security approach. The MA works autonomously, acts upon the environment; goal oriented and completes the assigned task within the stipulated time with better security than the conventional approaches. The working scenario of the proposed work is as shown in the Figure 2.

WSN has gotten faster because to the increasing demand for actual facts. To get around their limitations, WSNs frequently use a multi-hop transmission scheme. Attacks on the source information and nodes' ids while hopping are the main issue with multi-hop transmissions. When a source node transmits information to a destination via numerous intermediary nodes in a resource-constrained WSN, there exists a risk of intrusion, identification tracking by an adversary, information extracting, and information tampering by the intermediary nodes. In (2) shows the secure line creation in the form of angle using tangent equation [23]. Start and end positions are required to draw the secure line from one point to another. The majority of the time, WSNs operates in hostile settings and is vulnerable to side channel assaults like differential calculation. The attacker in such attacks keeps an eye on the system, performs the same action again, and carefully checks the amount of power used on a cycle-by-cycle manner.

$$\emptyset = tan - 1((y2 - y1)/(x2 - x1)) \tag{2}$$

Where (x1, y1) is secure line’s initial position and (x2, y2) is secure line’s final position.

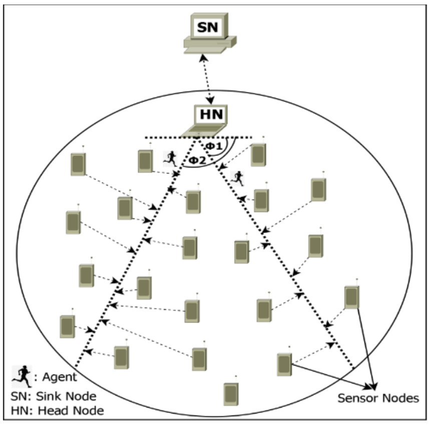

Figure 2. Working scenario

Consider about a packet as being ‘n’ bits long. The total energy used to transfer data between a transmitter and receiver is ‘n’ bits over a given distance, which is given in (3) as:

$$E_{Tot} = n * E_{radio} + n * E_{sensing} + n * E_{others} \tag{3}$$

Angle constructor agent (ACA):

The head manager agent (HMA) created the mobile agent known as ACA. The angle is mostly constructed via ACA based on node density. When using a time-driven HN, draw the prefixed angle (selection of angle is done based on the number of nodes coverage). HMA creates the angle in the desired direction whenever HN gets the interest or when the time stamp expires. Once the angle has been built, HMA informs HBB with angle information. Once the angle is built, ACA's efforts are done, and it will perish. The construction of the angle ensures that the initial node discovers its subsequent node, which is situated at or near the specified angle. Same process continues with the next nodes until the boundary of cluster reaches. In (2) has been used for the creation of angle geographically updated on to the SN database.

Algorithm

Abbreviations: TDMA: Time Division Multiple Access, HN: Head Node, ACA: Angle Constructor Agent, MA: Mobile Agent, AES: Advanced Encryption System, SN: Sink Node.

a) Angle based secure data transmission

```
(1). START
(2). TDMA Expired?
        If yes, all nodes should sense the environment and go next
           Else
        Wait until it expires. Repeat 2.
```

```
(3). The HN Creates secure line called as angle from HN to sensing boundary. The ACA Helps in creating angle.
(4) If angle is created then
        HN calls MA for data collection securely using AES.
    Else
        HN Waits until angle is created using ACA.
(5) MA submits the secured data to HN and dies.
(6) If HN received all the data from multiple MA's then
        Consolidated secured data sent to SN with link security.
    Else
        HN has to wait until all data to be received.
(7) All the secured data decrypted at the SN.
(8) END
```

4. RESULTS AND DISCUSSION

The outcomes of the proposed trust-aware angle-based secure routing strategy in WSN is shown in this section. We used the agent paradigm on the sensor network to create secure lines using angles. The difficulty of gathering and safeguarding the data transmission from the sensor node to the HN and from the HN to the SN determines whether the suggested technique will be successful. How does the sensor network technique compare to conventional secure-leach (sleach) and LEACH is the fundamental query. This can be because security measures in WSN are rather ineffective and require more attention to provide effective secure WSN for all applications. The efficiency of the suggested work in comparison to other traditional approaches is depicted in the following graphs.

Three parameters which include average energy usage, packet delivery ratio, and computation analysis have been used to illustrate the performance of the proposed work. Among the implications made for this study are the following:

- Since the entire sensor nodes are fixed, there doesn't appear to be any movement in the networks.
- There would be power loss in the network since the power would be low in the sensor network.
- Each node has the same computing power.
- Strong nodes would help the handshaking mechanism.
- If the node is breached in some way, the hacker must have access to the data on the node.

Average energy is the whole amount of energy used for transmission, receptions, sensing, aggregation, encryption, decryption, and angle generation is referred to as energy consumption. To deliver the detected data to HN and HN to SN, the suggested makes use of the multipath routing approach. When there is a transmission between a node and an HN, less energy is also needed for angle generation, agent movement, and encryption. In general, the suggested method uses less energy than the other two typical techniques, LEACH [24] and SLEACH [25]. Because data transmission needs more energy and there isn't a sufficient secure routing management mechanism, there is higher energy consumption. The curve of energy usage is depicted in Figure 3. Average energy calculation presents in (4):

$$\mathrm{E_{Avg}} = \mathrm{E_{sensing}} + \mathrm{E_{trasreception}} + \mathrm{E_{angle\ creation}} + \mathrm{E_{crptography}} \tag{4}$$

PDR is the packet delivery ratio, expressed as a percentage of the total number of packets sent, is the ratio between the total number of packets sent and the total quantity of packets delivered. The calculation formula for calculating it is given in (5):

$$\mathrm{PDR} = (\mathrm{No.ofpacketsreceived} \,/\, \mathrm{No.ofpacketssent}) * 100 \tag{5}$$

As contrasted to the SLEACH and LEACH protocols, the PDR of the suggested work is superior. As the number of nodes rises, the PDR ratio climbs as well. The PDR is superior for the suggested task and performs worse by the traditional SPIN procedure with the inclusion of the two key generation proposal. Figure 4 provides a description of the PDR.

Computation analysis is the total time needed for the sender to sense the data, send the sensed data to HN, then transfer the data from HN to SN through encrypted connections while taking key generation, encryption, and decryption into consideration is used to compute computation analysis. The time overall consumption in the suggested work is extremely less than comparison to both the traditional protocols, according to the computation analysis, which is computed based on the timing factor in milliseconds. This is owing to the two-tier proposal. SLEACH and the suggested work need much less computing time than the LEACH technique. The calculation time fluctuates as the number of nodes changes; however, the suggested approach has a much bigger difference when compared to both protocols. Analyses of computations have been presented in Figure 5.

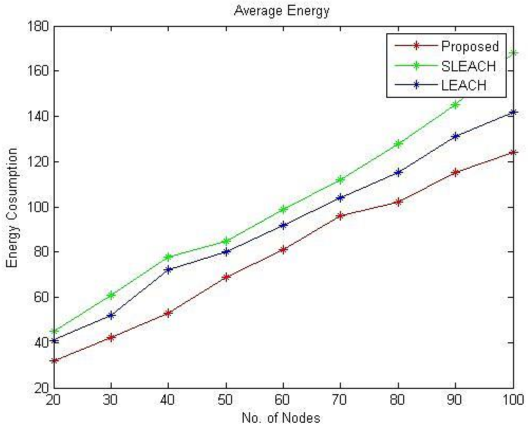

Figure 3. Average energy

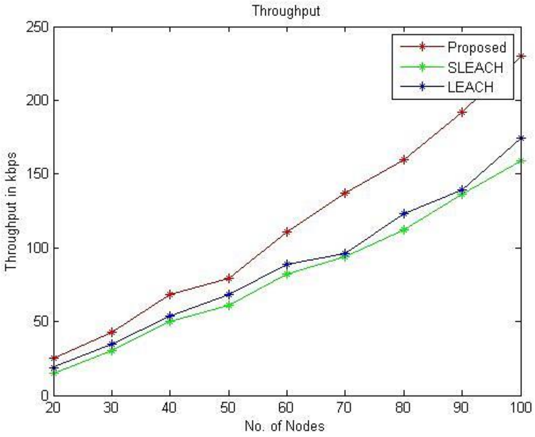

Figure 4. Packet delivery ratio

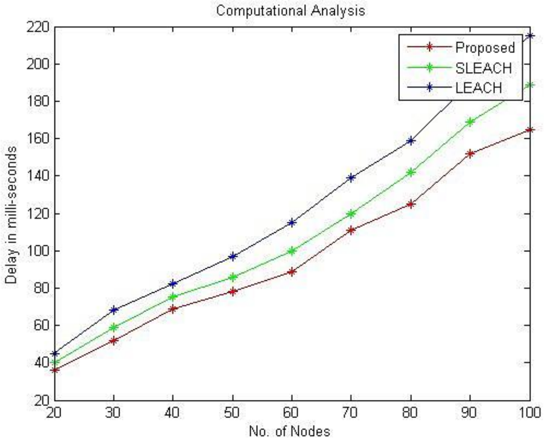

Figure 5. Computation analysis

5. CONCLUSION

Multiple researches has been carried-out to provide the end to end link security to the data being transferred from source node to head node and head node to sink node. The complexity was high and approaches were not effective. The proposed work i.e., trust aware angle based secure routing approach for WSN uses secure angle to bring the data from source node to head node using mobile agent paradigm. The proposed approach provides link security, decreases node energy usage, minimizes the overall delay and also provides very good throughput than compare to conventional methods like LEACH and SLEACH. Results shows that proposed work holds good in all applications whether it may be in static application or multimedia application. In our case we have done simulation considering static application.

ACKNOWLEDGEMENT

We thank VTU Belagavi for giving us an opportunity to conduct the research. Also, we hereby declare that, we haven’t received any research grants or contract from any of the organizations.

REFERENCES

[1] Z. Huanan, X. Suping, and W. Jiannan, “Security and application of wireless sensor network,” *Procedia Computer Science*, vol. 183, pp. 486–492, 2021, doi: 10.1016/j.procs.2021.02.088.

[2] M. Majid *et al.*, “Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review,” *Sensors*, vol. 22, no. 6, pp. 1–36, Mar. 2022, doi: 10.3390/s22062087.

[3] A. J. Williams, M. F. Torquato, I. M. Cameron, A. A. Fahmy, and J. Sienz, “Survey of Energy Harvesting Technologies for Wireless Sensor Networks,” *IEEE Access*, vol. 9, pp. 77493–77510, 2021, doi: 10.1109/ACCESS.2021.3083697.

[4] M. Kaur and A. Munjal, “Data aggregation algorithms for wireless sensor network: A review,” *Ad Hoc Networks*, vol. 100, no. 3, pp. 1–20, Apr. 2020, doi: 10.1016/j.adhoc.2020.102083.

[5] P. Sangulagi, S. Patne, and A. V. Sutagundar, “A New Approach for Energy Efficient Routing and Aggregation in Wireless Sensor Network,” *International Journal on Emerging Technologies*, vol. 6, no. 2, pp. 320–326, 2015.

[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” *Computer Networks*, vol. 38, no. 4, pp. 393–422, Mar. 2002, doi: 10.1016/S1389-1286(01)00302-4.

[7] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, *Wireless sensor networks*. USA: Springer, 2006.

[8] N. Sharma, I. Kaushik, V. K. Agarwal, B. Bhushan, and A. Khamparia, “Attacks and Security Measures in Wireless Sensor Network,” in *Intelligent Data Analytics for Terror Threat Prediction*, Wiley, 2021, pp. 237–268, doi: 10.1002/9781119711629.ch12.

[9] R. K. Yadav and R. P. Mahapatra, “Energy aware optimized clustering for hierarchical routing in wireless sensor network,” *Computer Science Review*, vol. 41, Aug. 2021, doi: 10.1016/j.cosrev.2021.100417.

[10] P. Sangulagi, A. V. Sutagundar, and S. S. Manvi, “Agent based information aggregation and routing in WSN,” *Communications in Computer and Information Science*, vol. 142, pp. 449–451, 2011, doi: 10.1007/978-3-642-19542-6_85.

[11] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, “QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks,” *Wireless Personal Communications*, vol. 110, no. 4, pp. 1637–1658, Feb. 2020, doi: 10.1007/s11277-019-06788-y.

[12] O. Oladayo and A. Ashraf, “A Secure and Energy-Aware Routing Protocol for Optimal Routing in Mobile Wireless Sensor Networks (MWSNs),” *International Journal of Sensors, Wireless Communications and Control*, vol. 9, no. 4, pp. 507–520, Sep. 2019, doi: 10.2174/2210327909666181217105028.

[13] O. O. Olufemi and A. Pamela, “An Efficient Multipath Routing Protocol for Decentralized Wireless Sensor Networks for Mission and Safety-Critical Systems,” *International Journal of Sensors, Wireless Communications and Control*, vol. 10, no. 3, pp. 368–381, Nov. 2020, doi: 10.2174/2210327909666190531113558.

[14] O. O. Olakanmi and A. Dada, "Wireless Sensor Networks (WSNs): Security and Privacy Issues and Solutions," *Wireless Mesh Networks - Security, Architectures and Protocols*. IntechOpen, May 13, 2020. doi: 10.5772/intechopen.84989.

[15] S. A. Jilani, C. Koner, and S. Nandi, “Security in Wireless Sensor Networks: Attacks and Evasion,” *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTEA 2020*, pp. 1–5, 2020, doi: 10.1109/NCETSTEA48365.2020.9119947.

[16] A. M. Bongale, C. R. Nirmala, and A. M. Bongale, “Energy efficient intra-cluster data aggregation technique for wireless sensor network,” *International Journal of Information Technology*, vol. 14, no. 2, pp. 827–835, Mar. 2022, doi: 10.1007/s41870-020-00419-7.

[17] M. Maheswari and R. A. Karthika, “A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks,” *Wireless Personal Communications*, vol. 118, no. 2, pp. 1535–1557, May 2021, doi: 10.1007/s11277-021-08101-2.

[18] W. P. Wang, L. Chen, and J. X. Wang, “A source-location privacy protocol in WSN based on locational angle,” *IEEE International Conference on Communications*, pp. 1630–1634, 2008, doi: 10.1109/ICC.2008.315.

[19] R. M, N. TK, and N. B. R, “Angle Based Static Routing in WSN using Triangular method,” *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 5, no. 8, pp. 1340–1348, 2018.

[20] S. Mohapatra, S. Kar, and S. Behera, “Different Approaches of Angle of Arrival Techniques In Wireless Sensor Networks,” vol. 2, no. 4, pp. 388–397, 2013.

[21] N. K. Gupta, R. S. Yadav, and R. K. Nagaria, “Energy Efficient Angle based Route Selection in 3D Wireless Sensor Networks,” *2019 58th Annual Conference of the Society of Instrument and Control Engineers of Japan, SICE 2019*, pp. 388–393, 2019, doi: 10.23919/SICE.2019.8859871.

[22] Z. Zhang, J. Li, and N. Xu, “Robust optimization based on ant colony optimization in the data transmission path selection of WSNs,” *Neural Computing and Applications*, vol. 33, no. 24, pp. 17119–17130, Dec. 2021, doi: 10.1007/s00521-021-06303-0.

[23] P. Kułakowski, J. Vales-Alonso, E. Egea-López, W. Ludwin, and J. García-Haro, "Angle-of-arrival localization based on antenna

arrays for wireless sensor networks," *Computers & Electrical Engineering*, vol. 36, no. 6, pp. 1181-1186, 2010, doi: 10.1016/j.compeleceng.2010.03.007.

[24] P. Sivakumar and M. Radhika, "Performance Analysis of LEACH-GA over LEACH and LEACH-C in WSN," *Procedia Computer Science*, vol. 125, pp. 248–256, 2018, doi: 10.1016/j.procs.2017.12.034.

[25] I. Ouafaa, E. Mustapha, K. Salah-Ddine, and E. H. Said, "Performance analysis of SLEACH, LEACH and DSDV protocols for wireless sensor networks (WSN)," *Journal of Theoretical and Applied Information Technology*, vol. 94, no. 2, pp. 304–311, 2016.

BIOGRAPHIES OF AUTHORS

Hemavathi Patil completed her M.Tech in the stream of CSE (Fuzzy Logic Sets). In the year 2005 she has completed her B.E from GUG Gulbarga, Karnataka, India. Currently, Pursuing Ph.D. from Visvesvaraya Technological University, Belagavi, Karnataka. She is a Life member of IETE and ISTE. Her area of interest is computer network (wireless sensor network). She can be contacted at email: hbpatilbidar@gmail.com.

Vishwanath Tegampure completed Ph.D. in the stream Control System in the year of 2014. He is working as Professor in EC Dept. Bheemanna Khandre Institute of Technology, Bhalki Karnataka, India. He has more than 30 years teaching & 12 years research experience. He is published several papers in national and international reputed journal. His area of interests is wireless sensor network, control system, communication. He is a lifetime member of ISTE, IETE. He can be contacted at email: tsvrec1@rediffmail.com.