ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)

https://doi.org/10.17559/TV-20230617000742
Original scientific paper

Enhanced Secured and Real-Time Data Transmissions in Wireless Sensor Networks using SFRT Routing Protocol

R. JAYAMALA*, A. SHERYL OLIVER, J. JAYANTHI, Nithya. N.

Abstract: Wireless Sensor Networks (WSN) track and record environmental changes using sensor nodes. When designing sensors, consider antenna type, components, memory, lifespan, security, computing power, communication protocol, energy consumption, etc. Wireless sensor networks (WSN) are ad hoc. This network links tiny sensor nodes that share few resources (both severely constrained at the node level). This paper proposed a Secure and Fast Real-Time (SFRT) Routing Protocol, which is used to secure real-time data transmissions in WSN. The proposed method not only increases the reliability of WSN but also offers a more robust solution in case a sensor node link fails. Discarding packets, launching a denial-of-service attack, using black holes, launching a selective forwarding attack, and flooding the network with hello packets are some proposed security measures. It maintains high packet throughput in the presence of malicious nodes while using little energy. Simulations have helped examine recommended safety measures. The unique approach outperformed state-of-the-art methods in the NS2 simulation in all relevant metrics, including network longevity, packet delivery rate, energy efficiency, network throughput, and end-to-end delivery latency. Most current methods necessitate multiple retransmissions before success is declared, increasing data transmission costs by 5% compared to the best approach. The proposed method is highlighted for its ability to increase network lifetime by 20% and reduce the total delay by 30%.

Keywords: end-to-end delay; packet delivery; secure and fast real-time routing protocol; security; throughput; wireless sensor networks

1 INTRODUCTION

A Wireless Sensor Network (WSN) is a distributed, self-organizing system composed of numerous small sensors capable of exchanging data wirelessly. Sentinel nodes can exchange data more quickly in close radio proximity. This would enhance their capacity for perceiving, observing, and identifying the numerous tangible components of their immediate surroundings. As more people become aware of how wireless sensor networks can be advantageous in various fields, their adoption rate steadily increases [1]. One of the biggest problems with the wireless sensor node is that it needs power to function. Since WSNs are frequently employed in crucial uses, protecting them has become necessary. One of the biggest obstacles that must be overcome before progress can be made is ensuring the security of wireless sensor networks (WSNs). Selective forwarding, wormhole assaults, sinkhole assaults, and wormhole flooding are just a few examples of attacks that can be launched at the network layer [2]. An adversary can easily take advantage of these routing protocols on a particular WSN because security is not a top priority in most real-time communication and coordination routing protocols. Routing systems used in WSNs must incorporate real-time safety measures that are not overly complicated but are still very effective. To get around obstacles, such as the fact that most data is only relevant for a brief period, real-time routing security must use the characteristics already present in the sensor network [3]. Many uses for WSNs depend critically on being able to exchange data in real-time. To give one specific example, if a fire has to be extinguished, the proper action must be taken in the affected zone as soon as possible lest further serious harm occurs. When decisions are made using the data gathered and provided by the sensors, the data must remain accurate so that the firefighters' safety is not compromised [4]. One way to accomplish this is by checking that the information is correct. When attempting to develop multi-hop routing in WSN, researchers face several obstacles due mainly to the large number of concurrent constraints that must be satisfied. For the study to be fruitful, these limitations must be met. One of the most important things to remember when designing sensor nodes is how little energy they will consume. Most sensor nodes rely on nonrenewable, finite energy sources for operation. In addition to not requiring wired power supplies, applications that use WSNs need to run for several months or even years without recharging or replacing batteries. In addition to the absence of this prerequisite, this capacity must be present. The deployment of WSNs necessitates this feature. To ensure the WSN lasts as long as possible, the power consumption must be considered during the design of the multi-hop routing. To achieve this, multi-hop routing should account for energy usage [5, 6].

2 RELATED WORKS

The network's lifetime was extended by reducing the strain on the nodes closest to the base station, as was done with the uneven clustering implemented in [7]. A hidden area far from the base station, called the far zone, is likewise avoided by incoherent clustering concepts. To adapt to the peculiarities of this form of the sensor network, it is required to build an efficient protocol for energy utilization. Cluster-based sensor networks are viable due to the unequal energy consumption of sensor networks, which allows them to efficiently utilize the limited energy resources of the distributed sensor nodes. The fact that sensors in cluster-based networks are organized into groups enables this. Heterogeneous sensor networks can be used because of the asymmetry in clustering. The most significant possibility for considerably prolonging the networks' lifetime lies with this approach. An organization that considers energy efficiency, as suggested in [8], can boost a network's effectiveness over its lifetime. Nodes in a wireless sensor network often have partial amounts of energy. The deployment is a one-and-done deal, making it hard to restock the energy reserves. As the sensor nodes are responsible for a wide variety of tasks and pieces of equipment, their individual energy needs will vary. This means the sensor network can draw power from many sources. Even in low-power sensor networks, so-called "hotspots" can emerge periodically and frequently in practical settings. Find the most efficient path for data to travel across the web. They focused on covering as many nodes as possible when implementing maximal lifetime scheduling. Routing protocols will create and maintain reliable, high-throughput communication routes that minimize energy consumption. Because of the increased energy consumption caused by "hotspots," some nodes in the network will fail prematurely and shorten the network's lifespan. To fulfil the needs of such a sensor network, a protocol that uses less power is essential. Using the energy-efficient scheduling strategy described in [9] improves the efficiency of directional sensor networks. Data collection, storage, processing, transmission, and application are intertwined into every stage of the production of social goods and daily life due to the expansion of human detection zones. When unequal clustering is used with a tweaked sleep scheduling algorithm, as described in, a network's lifespan can be significantly extended by avoiding the Far-zone. Simply developing the time that individual nodes in the network remain operational would achieve this goal. The proposed solution adjusts the clustering tactic to keep the network online longer and improves the sleeping schedule. The sensor nodes in a wireless sensor network are low-cost and compact, and the routing protocols govern the methods of information exchange between them. It is easy to see how the wireless sensor network could be helpful in a wide range of situations. Its scientific significance is high, and it has many practical applications in areas like environmental monitoring, efforts to rescue and aid people in need, remote control in potentially dangerous situations, and many others. It will be put to use in many arenas and lauded by many. This year, [10], we finished developing the Trust-Based Secure and Energy-Efficient Routing Framework for WSNS. In addition to unearthing fraudulent activities, this study proved that data exchanged between sensors in a wireless network is safe. The WSN's connection to the central hub must always be secure. Any network attacker found to have used fraudulent means to gain access will be dealt with severely. The sensor verifies the correct trust value before sending data to the base station. In that case, the data will be rejected. In addition to improving throughput, it protects networks from many deception assaults. In [11], IM-LEACH was used to boost the efficiency of wireless sensor networks. This research uses clustering approaches to show that energy consumption can be decreased while WSN scalability increases. The IM-LEACH clustering method was used to cut back on power consumption during the study's course. The cluster setup procedure comes first, followed by the scheduling of the cluster manager. Each node in the LEACH network picks an arbitrary integer and checks it against the limit. Without regard to its energy level, every network node takes on the role of a cluster leader [12]. This is true regardless of the node's energy state. The low-energy cluster head will die before all its data is sent to the base station. To find a solution, each node will report its current energy level to the node responsible for finding a solution.

The cluster's initiator node must choose which nodes can serve as the cluster's leader. If multiple candidates exist for the cluster's leader, the initiator will select the one with the most available energy and eliminate the other. Information will be sent to the central hub in a way that does not slow things down too much. Results from a study on how to make wireless sensor networks more energy efficient were published in [13]. If we complete this task, the WSN network's functionality will be enhanced, and its long-term existence will be ensured. The base station sets the threshold for energy efficiency, and that is how it knows which channel to use. This aids in reducing the amount of energy consumed. If the energy stored in a node exceeds the threshold, that node will be chosen as the cluster's leader [14]. The cluster head selection procedure disregards values below a specified threshold to maximize the node's lifetime. A significant amount of data transfer capacity is sacrificed because the Energy Level Value must be calculated at the base station before being sent to the cluster head. As a result, fewer data packets will be filled, and less bandwidth will be used. In this, we read about creating an efficient energy-saving routing algorithm for WSNs that considers the need for sleep. As part of this research project, an algorithm was developed to determine when sensors should sleep to reduce their power consumption and extend the network's operational lifetime. Cluster-based routing is an effective method for decreasing a network's power consumption. As soon as a cluster of nodes is formed, a single leader is selected at random from among the members of the cluster. Each network node has an equal probability of being awake or asleep, with probabilities p and $1-p$, respectively [15, 16]. The node should be permitted to participate in network activity once it is awakened from its current sleep state. Nodes that have been asleep for a while will come to life after a certain amount of time has passed. This method determines which node should be placed in the sensor node's sleep mode to conserve the required energy. Both a tree structure and a set of nodes that are either active or inactive can be compiled from a breadth-first search (BFS). The project cannot be finished in a short amount of time. Each node that takes too long to respond or fails before the timeout elapses affects the entire routing structure and uses more power than usual [17]. This paper introduces the Secure and Fast Real-Time (SFRT) Routing Protocol. By considering the network quality, the delay time for a packet, and the remaining power in the sensor nodes located on the next hop, this protocol distributes work following an optimal forwarding decision. Additionally, it suggests bolstering network safety by incorporating packet header authentication, transport encryption, and destination decryption.

3 PROPOSED SECURE AND FAST REAL-TIME ROUTING PROTOCOL

Location Management, Routing Management, Power Management, Neighborhood Management, and Security Management are the five core functional components of the SFRTRouting Protocol. Using their distance from three randomly selected neighbours, the location management system determines the precise location of each sensor node. The power supply controls the on/off state of the transceiver and the transmission power of the sensor node. The task of the neighbourhood manager is to identify a set of potential forwarding nodes. Moreover, it keeps track of the nodes' connections with their neighbours. If there are any issues with forwarding, the route management will evaluate the situation and decide on the best course of action. The security management system encrypts and decrypts data in particular packet header fields and performs authentication procedures.

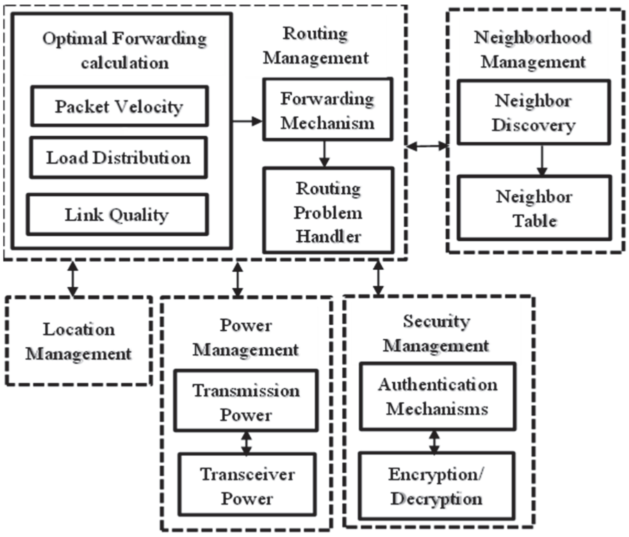

Figure 1 Architecture of of SFRT routing protocol

When forwarding data, routing management must calculate three factors to ensure accuracy. Packet rate, battery life, and connectivity are three factors to consider. Predictions of sensor communication are made after researching the quality of the wireless link at the physical layer. Additionally, the remaining power is expected to distribute the traffic pressure equitably across the entire forwarding process. A router's administration will ultimately forward data to its best one-hop neighbour in the network. To find out which of the 66 paths provided the most favourable route, we ran an NS-2 simulation with four different grid network topologies (low density, high density with multiple traffic sources, medium density, and high density with one traffic source).

Algorithm: Proposed SFRT Routing Protocol.

For Fast Realtime Routing Protocol.

Sept 1: Need to calculate Optimal Forwarding (*OF*); *OF* includes three Parameters: Packet Velocity (*PV*), Remaining Power (*RP*) and Link Quality (*LQ*).

Sept 2: To Calculate *PV*, product of exhaustive search (μ) and Packet Ratio (*PR*).

Sept 3: To Calculate *RP*, product of μ and Maximum Voltage (*Vo*).

Sept 4: To Calculate *LQ*, product of μ and Maximum Velocity (*Ve*). $OF = \mu \times PR + \mu \times Vo + \mu \times Ve$.

For Secure Realtime Routing Protocol.

Sept 1: Assign each node is static and Store of its location.

Sept 2: Calculate Sink node.

Sept 3: Pseudo random function for master key and packet ID to uploadin to sensor nodes.

Sept 4: Hard mathematical function with its reverse calculation is stored in each sensor node.

Step 5: Two master keys ($k1$, $k2$) are stored during program uploading into sensor nodes.

Where $k1$ is used as a masterkey in all nodes for encryption and decryption purpose and $k2$ is used as a master key for a new node.

Security Enhancement in SFRT Routing Protocol.

The study's results with One-time Pad have enhanced the safety afforded by SFRTRP. The issue with creating random numbers and the data quality are two of the many addressed by the patch. One of the most critical factors to consider while designing a secure SFRTRP routing protocol is the strict deadline that real-time routing protocols must meet. Each packet transported through a wireless sensor network (WSN) should undergo encryption, decryption, and authentication at each hop in the network. Given that sensor nodes double as routers, this is essential. Therefore, the SFRTRP security upgrade must keep real-time routing between the source and the destination. Furthermore, SFRTRP uses a random generating function encrypted using mathematics to address the issue of obtaining random values. Specific packet header fields are encrypted using the result of the random process. The packet's identifier and its source and destination addresses are stored here. The authentication procedure that follows decryption in SFRTRP fixes the problem of shaky data. These are the main dissimilarities between the SFRTRP securities. The security system's generation of a secure packet could have a mistake in its header information. If an unauthorized node listens in on a particular packet, it will not be able to figure out where it came from or where it is going. Since the secure packet is only suitable for a limited time, the following chapter presents a dynamic mathematical method for decryption that was devised to foil any attempts by an opponent to decipher the packet. The suggested security system is based on the following presumptions:

a. When a piece of software is loaded into a sensor node, the node will store a pseudo-random function. This function will be a function of the master key and the packet ID.
b. Each sensor node is permanently installed and fully self-aware. To sum it all up, Sink is a solid platform for your computer.
c. Information is saved whenever a Programme is sent to a sensor node.
d. Each node in the sensor network stores a complex mathematical function and the inverse computation before the deployment of the network.
e. Whenever new software is installed in sensor nodes, two master keys are generated and stored. When a new node is added to a running WSN, it will use $k2$ for encryption and decryption, while $k1$ will be used as a master key for all nodes.

The results of the decryption procedure are verified for accuracy during authentication. Decryption methods are successful if they yield a value between 0 and R, indicating that the object is genuine. If that is the case, the item's supposed legitimacy is questioned. It is worth noting that the mathematical function used for encryption in this proposal was selected based on a far more challenging mathematical process for decryption. This is important to remember going ahead. One thing to remember is that adding a new sensor device to a WSN can be accomplished by reusing an existing control packet. The new value R is encrypted in this control packet with the same algorithm and $k1$ as the original master key.

4 SIMULATION RESULTS AND DISCUSSION

Network Simulator 2 (NS2) simulates the routing protocol since it is user-friendly and readily available. The acronym NS designates a discrete event simulator made for network research. Tab. 1 provides the metrics that will be used to assess the subsequent simulation parameters.

Table 1 Simulation parameters

Network Area	500 m × 500 m
Number of nodes	100 to 900 in increment of 100
Number of rounds	1500
Node density	0.0052 nodes/m^2
Initial energy	0.2 J
Base station location	(50, 50), (105, 105), (220, 220)
Transmitter/receiver energy	50 nJ/bit
Power transmission	1 mW

Network Lifetime Enhancement of SFRTRP: The simulation results are compared to the proposed model, the Ant colony optimization (ACO) algorithm, the Particle swarm optimization (PSO) algorithm, the Energy efficient target-oriented scheduling (EETS) protocol, and the cluster-based LEACH protocol. For this simulation, a single node covers an area of 500 square meters, so there will be 100 nodes. Other possible values for these aspects include starting nodal Energy of 1 joule, a packet size of 500 bytes, and a channel bandwidth of 1 Mbps. The three measurements utilized for performing a performance analysis are:

- The lifetime.
- The packet delivery ratio.
- The residual Energy.
- The average end-to-end delay.
- The throughput.
- The path establishment time

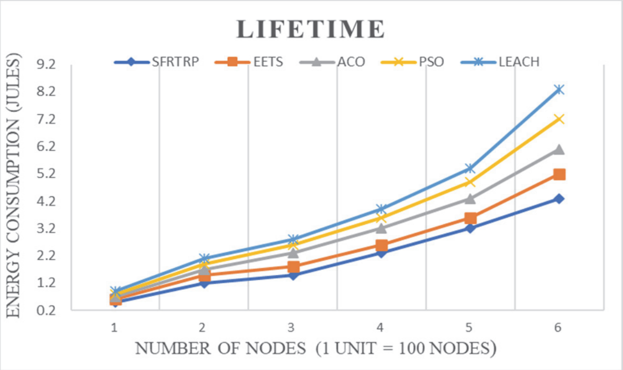

Figure 2 Life time comparison

Lifetime: When a node in a network experiences failure for the first time, its "lifetime" begins. Put another way, a round is a time that elapses between two consecutive cluster heads. As more and more simulation nodes are added to the network, its lifespan grows steadily. If there are many nodes, the network will last longer. The sensors' remaining power determines which nodes are operational. The given SFRT Routing Protocol has a lifespan of 483 nodes, while the other approaches in use today have a lifespan of only 100 nodes. You can see from Fig. 2 that the proposed SFRT Routing Protocol outperforms LEACH, the Particle Swarm Optimization Algorithm, and the Ant Colony Optimization Method.

Control overhead: A packet's "control message cost" is the sum of the times it must undergo transmissions of control messages (CTS, ACK, and RTS). The "control message cost" includes the price of these communications. Control overhead is the sum of all transactions involving control messages in a given period. Reduced latency and fewer collisions are achieved using control messages to limit the available bandwidth and the number of letters.

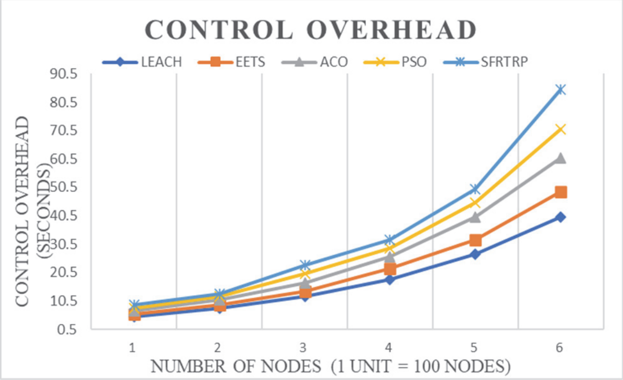

Figure 3 Control overhead comparison

The number of rounds and the overall time required are significantly reduced using the proposed protocol. The proposed method is superior to the other two ways, as seen in Fig. 3. As a result of the improved clustering strategy, the control overhead value dropped dramatically in subsequent rounds. This was because of an adjustment made to how clusters were generated. The last round's 20% cut shows improvement over prior reductions of 10% and 5%.

Path Establishment Time: The path setup time, measured in milliseconds, is how long it takes to establish a connection between a source node and an end node. Using both a primary and a secondary path establishment, the proposed architecture for the SFRT Routing Protocol ensures precise routing.

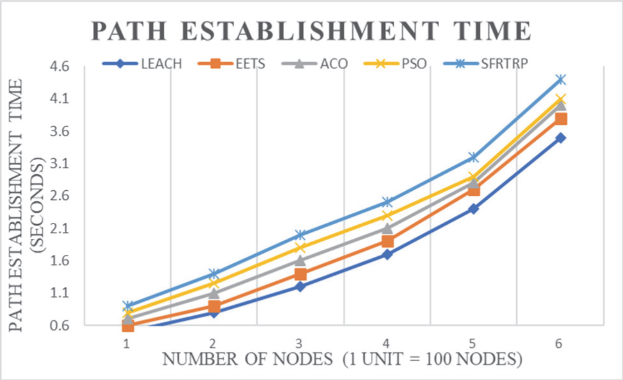

Figure 4 Path Establishment time comparison

Fig. 4 shows that at node 100, the shortest possible path establishment time using the provided SFRTRP is 0.38 seconds. This exemplifies how the time needed to build a path is reduced by 46% compared to when employing the LEACH method.

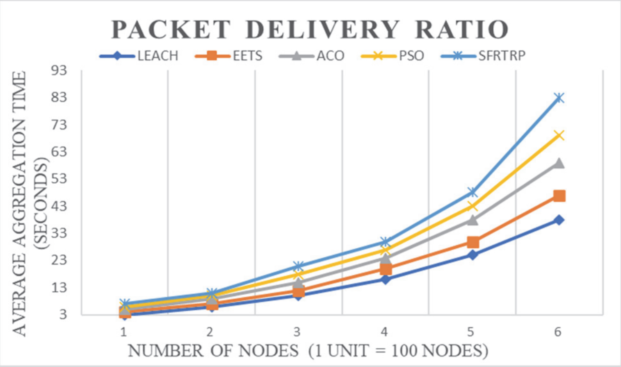

Figure 5 Packet delivery ratio comparison

Packet delivery ratio: The ratio of the number of packets received by the receiver to the total number of packets sent by the sender is known as the "packet delivery ratio." The packet delivery ratio and packet loss ratio are two related measurements. The term "packet loss" refers to the difference between the total number of packets sent and the total number of packets received over a predetermined period. As shown by the comparison graph in Fig. 5, when compared to other methods, the suggested method results in a significantly lower packet loss. The graph displays the reduced packet loss rate; hence this must be the case. The simulation is run to get the values for the three methods. The most recent round's results show improvement over earlier ones, with a 20% drop.

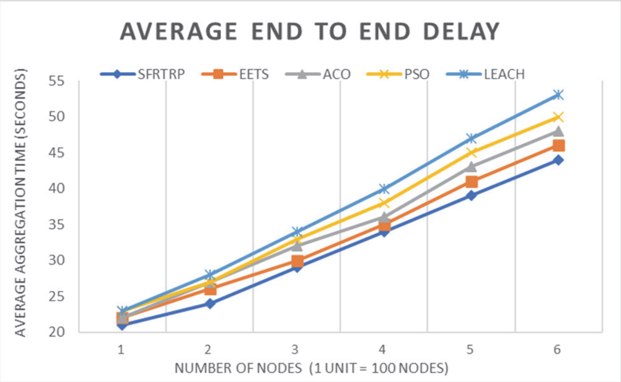

Figure 6 Average end to end delay comparison

Average End to End Delay: End-to-end latency is the total time a packet travels from its source node to its destination node. Time spent at each hop along the path is factored into this metric. The average end-to-end latency is calculated by counting the number of packets that reach their destination successfully despite a delay at an intermediate node in the network. One of the benefits of the proposed SFRT Routing Protocol system is a decrease in end-to-end delay. The main reason is that a primary routing path can be established faster. Furthermore, an alternate path can be established in less time if a network link breaks. When used during the relay phase, the proposed routing protocol reduces latency compared to previous methods. This is thus because it is used while "relaying." Fig. 6 compares the typical latency in the proposed technique to the earlier phase, showing a 30% increase in efficiency.

Throughput: The total number of data transfers required for each packet's end-to-end delivery is considered when calculating the transmission cost. The term "throughput" refers to the number of successfully delivered data packets within a given period. You can get high throughput values compared to competing protocols using the right algorithmic schedule adjustment with minimal packet loss. Fig. 7 is a comparison graph showing how much better the proposed model is than the baseline model.The throughput of the proposed work is enhanced when compared with the existing methodologies by 29%

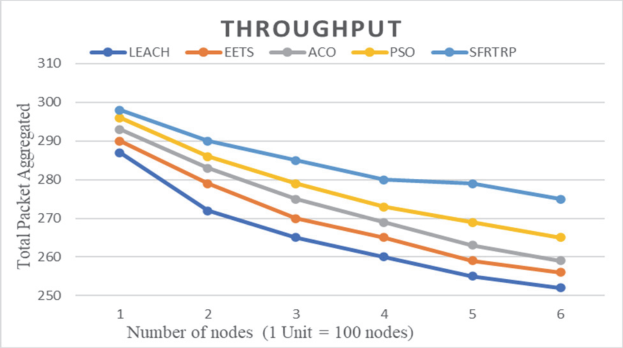

Figure 7 Throughput comparison

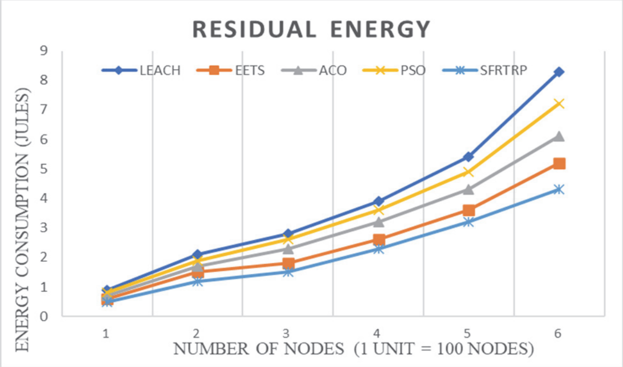

Figure 8 Residual energy comparison

Residual Energy: The wireless sensor network must account for energy consumptio. The more time is spent in the simulation, the less residual energy there is in the network. If a vital link along the route is broken, the SFRT Routing Protocol will attempt to find an alternative way. As can be seen in Fig. 8, the proposed design generates significantly more surplus energy than competing approaches. There is never a drop in efficiency while using the SFRT Routing Protocol. The energy consumption of the proposed work is reduced and is of 36% of energy saved when compared with the existing methodologies. Since malicious nodes discard every incoming packet without exception, the malicious node's trustworthiness will inevitably drop below the trust threshold.

Table 2 Comparison of SFRT algorithm and existing algorithm

Algorithms	LEACH	EETS	ACO	PSO	SFRT
Control overhead	0.8%	3.1%	1.3%	2.6%	3.7%
Path Establishment Time	20%	17.5%	14.3%	12.8%	11.76%
Packet delivery ratio	81.61%	84.68%	88.5%	95.4%	98.4%
Average End to End Delay	6.3%	2.9%	4.1%	5.4%	1.7%
Throughput	86.66%	88.78%	91.6%	97.6%	99.3%
Residual Energy	36%	26%	29%	31%	24%

The time required to identify malicious nodes is reduced and dropped packets occur less frequently overall. A hostile node commits a "hello flood attack" when it broadcasts a sufficient number of hello packets to convince more distant nodes that it is their immediate neighbour. As a result, the malicious node will discard many data packets. A selective forwarding attack occurs when a malicious node selectively forwards or discards packets that are essential to the network's operation, whereas a black hole attack occurs when packets are destroyed.

5 CONCLUSIONS

The proposed SFRT Routing Protocol is an efficient data aggregation algorithm that discovers minimal-effort solutions to the many challenges arising during data-gathering and organization processes. The research led to the developing a technique for constructing aggregation trees that avoids this type of collision. The algorithm follows a binary search tree protocol. To reduce environmental impact, the least resource-intensive strategy for building the tree was calculated. Data aggregation with minimal delays has been demonstrated, and an aggregation tree has been constructed to put this theory into practice. Conversation confidentiality was ensured by employing asymmetric key cryptography. Security measures that are too stringent make it difficult for WSN to use its resources and energy, which leads to a rapid drain of power. Excluding malicious nodes from a network has improved service quality for all users (QoS). This tactic helps protect networks from malicious nodes that act in their self-interest and lead to packet loss, DoS attacks, or black holes.

6 REFERENCES

[1] Huangshui, H., Youjia, H., Meiqin, Y., & Xue, S. (2021). Trust based secure and energy efficient routing protocol for wireless sensor networks. *IEEE Access*, *10*, 10585-10596. https://doi.org/10.1109/ACCESS.2021.30759

[2] Praveena, N G. & Prabha, H. (2014). An efficient multi-level clustering approach for a heterogeneous wireless sensor network using link correlation. *J Wireless Com Network*, *168*(2014). https://doi.org/10.1186/1687-1499-2014-168

[3] Samuda, P., Praveena, N G., Nithiya, C., Komathi, B. J., Pavithra, J., & Kiruthika, V. (2022). Arduino based Customized Smart Glasses for the Blind People. *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 1136-1141. https://doi.org/10.1109/ICAIS53314.2022.9742799

[4] Eswaramoorthy, V., Vinoth Kumar, K., & Gopinath, S. (2021). Fuzzy logic based DSR trust estimation routing protocol for MANET using evolutionary algorithms. *Technical Gazette*, *28*(6), 2006-2014. https://doi.org/10.17559/TV-20200612102818

[5] Shankar, V. & Biradar, R. V. (2017). Energy utilization and security enhancement using particle swam optimization (PSO). *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering*, 389-391. https://doi.org/10.1109/ICPCSI.2017.8392323

[6] Vinoth Kumar, K., Jayasankar, T., Eswaramoorthy, V., & Nivedhitha, V. (2020). SDARP: Security based Data Aware Routing Protocol for Ad hoc Sensor Networks. *International Journal of Intelligent Networks (Elsevier-KeAi)*, *1*, 36-42. https://doi.org/10.1016/j.ijin.2020.05.005

[7] Youjia, H., Huangshui, H., & Yuxin, G. (2022). Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm. *IEEE Access*, *10*, 11538-11550. https://doi.org/10.1109/ACCESS.2022.3144015

[8] Honguntikar, V. & Biradar, G. S. (2017). Frog-Based Routing Algorithm to Enhance the Network Lifetime of Wireless Sensor Networks. *International Journal of Computer Network & Information Security*, *9*(8), 9-15. https://doi.org/10.5815/ijcnis.2017.08.02

[9] Ramesh, K. & Somasundaram, K. (2016). Wireless sensor network lifetime enhancement using modified clustering and scheduling algorithm. *Circuits and Systems*, *7*(8), 1787-1793. https://doi.org/10.4236/cs.2016.78154

[10] Ramachandran, S. & Shanmugam, V. (2012). Performance Comparison of Routing Attacks in Manet and WSN. *International Journal of Ad hoc, Sensor & Ubiquitous Computing*, *3*. https://doi.org /10.5121/ijasuc.2012.3405

[11] Vinoth Kumar, K., Jayasankar, T., Prabhakaran M., & Srinivasan, V. (2017). Fuzzy Logic based Efficient Multipath Routing for Mobile Adhoc Networks. *Applied Mathematics & Information Sciences*, *11*(2), 449-455. https://doi.org/10.18576/amis/110213

[12] Prabakaran, D. & Sheela, K. (2021). A Strong Authentication For Fortifying Wireless Healthcare Sensor Network Using Elliptical Curve Cryptography. *2021 IEEE Mysore Sub Section International Conference (MysuruCon), Hassan, India*, 249-254.

[13] Naga Ravikiran, D. & Dethe, C. G. (2018). Improvements in Routing Algorithms to Enhance Lifetime of Wireless Sensor Networks. *International Journal of Computer Networks & Communications (IJCNC)*, *10*(2), 23-32. https://doi.org/10.5121/ijcnc.2018.10203

[14] Gopikrishnan, S. & Priakanth, P. (2018). Lifetime enhancement in wireless sensor networks using binary search tree based data aggregation. *Journal of applied research and technology*, *16*(6), 524-543. https://doi.org/10.22201/icat.16656423.2018.16.6.749

[15] Gopinath, S., Vinoth Kumar, K., Elayaraja, P., Parameswari, A., Balakrishnan, S., & Thiruppathi, M. (2021). SCEER: Secure cluster based efficient energy routing scheme for wireless sensor networks. *Materials Today: Proceedings (Elsevier)*, *45*(2), 3579-3584. https://doi.org/10.1016/j.matpr.2020.12.1096

[16] Mukesh, M., Gupta, G. S., & Gui, X. (2021). Network Lifetime Improvement through Energy-Efficient Hybrid Routing Protocol for IoT Applications. *Sensors*, *21*(22), 7439. https://doi.org/10.3390/s21227439

[17] Youjia, H., Huangshui, H., & Yuxin, G. (2022). Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm. *IEEE Access*, *10*, 11538-11550. https://doi.org/10.1109/ACCESS.2022.3144015

Contact information:

R. JAYAMALA, Assistant Professor
(Corresponding Author)
Department of Computer Science and Engineering,
University College of Engineering (BIT Campus), Anna University Trichirappalli
E-mail: jayamala_r@outlook.com

A. SHERYL OLIVER, Assistant Professor
Department of Computational Intelligence,
SRM Institute of Science and Technology, Chennai
E-mail: sherylviniba@gmail.com

J. JAYANTHI, Professor
Department of Computer Science and Engineering,
Sona College of Technology, Salem
E-mail: jayanthij@sonatech.ac.in

Nithya. N., Assistant Professor
Department of CSE, K. Ramakrishnan College of Engineering
E-mail: nithyasrichithra@gmail.com