ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2023.0429

IMPROVING THE SECURITY BASED ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

S.Vijayarangam[1], Kavita V Wagh[2], Vishal Gangadhar Puranik[3] and S. Selvakanmani[4]

[1]*Department of Computer Science Engineering, Sri Indu College of Engineering and Technology, India*

[2]*Department of Electronics and Telecommunication Engineering, Vasantdada Patil Pratishthan's College of Engineering and Visual Arts, India*

[3]*Department of Electronics and Telecommunication Engineering, JSPM's Bhivarabai Sawant Institute of Technology and Research, India*

[4]*Department of Information Technology, RMK Engineering College, India*

Abstract

Wireless sensor networks (WSNs) have become one of the most popular wireless communication systems in the world. Various attacks have been launched against the WSN individual nodes over the past few years, and the overall security of the network has gradually deteriorated. In this research, we propose a secure uneven clustering method for WSN. The proposed method is based on a trust score evaluation model with the objective of identifying malevolent users in WSNs. The trust score is used to determine whether or not a node is malicious. The results show that the proposed Trust Algorithm outperforms the currently used LEACH algorithm, the TASRP algorithm and the FLSO algorithm in terms of the percentage of packets that are successfully delivered across all use cases and density of nodes.

Keywords:

Security, Routing Protocol, Wireless Sensor Network

1. INTRODUCTION

Wireless sensor networks (WSN), make it possible to deliver wireless services by detecting the environment around them. The wasteful use of energy is one of the most prominent problems of WSN, which also happens to be one of its advantages. A considerable amount of effort is being put into the creation of innovative routing protocols that have the potential to dramatically cut the amount of energy that is being utilized. There are two basic types of wireless sensor networks, namely organized and unstructured ones [1].

Various attacks that have been launched against the WSN individual nodes over the past few years, the network overall security has gradually deteriorated. At the routing level, it is possible to carry out attacks such as black hole attacks, Sybil attacks, spoofing attacks, and denial of service (DoS) attacks [2]. These are only some of the types of attacks that can be carried out. Attacks that in some way interfere with service present the greatest challenge to the network ability to maintain its integrity.

A number of researchers are spending a significant amount of effort into developing an enhanced and more secure routing system for the WSN. This algorithm was developed by us and is presented here as part of this article. Malicious nodes in a WSN contribute to the issue of excessive energy consumption by the network as a whole. We arrived at the realization that conserving energy on sensor nodes requires not engaging in activities that are destructive to the environment [3].

It is necessary to provide a secured path in such a way that the path can be determined through the calculation of trust, which then determines the validity of the participating nodes. This must be done in such a manner that it is possible for the suggested path to be decided. This needs to be done in such a way that the trust computation may be used to figure out the advised course forward. When it comes to routing, trust is determined by how confident a node is in the capacities of its surrounding nodes to transmit and receive packets safely. This confidence is measured by how many packets a node is certain its neighbors can send and receive safely. The number of a node neighbors is one of the factors that is used to determine its level of confidence. This research proposes the use of a brand-new trust-based safe routing protocol called Energy Aware Trust Based Safe Routing Algorithm (EATSRA) [4].

Trust metrics are being utilized by EATSRA in order to answer concerns regarding the safety of our protocol. These metrics keep track of things like the activity of individual nodes, the rate at which packets are transmitted, the quality of the signal that is received, and the amount of energy that is not being utilized. This system identifies and thwarts attacks launched by malicious nodes, which results in a rise in operational efficacy and a drop in energy usage [5]. It is possible to conduct an analysis of the dependability of nodes that are located in close proximity to the network in order to identify whether or not they provide a risk to the safety of the wireless sensor network. When conducting a trust assessment, it is necessary to take into consideration both direct and indirect trust, which are frequently referred to as suggested trust values [6].

Regardless of whether or whether the interaction between the surrounding nodes was successful, it is referred to as direct trust, which describes the interaction between the nodes. The term recommendation trust refers to an indirect form of trust that can be developed when one node refers another node to another. This type of trust can be established when one node refers another node to another [7]. The successful and efficient communication between nodes, as well as decisions regarding which path to take to arrive at the destination, is values of trust. However, throughout the course of time, trust in certain nodes might fluctuate, and along with that shift, the value that is placed on the reliability of that node can also shift [8]. Only those nodes that have a high trust score are utilized for the communications, as this is the criterion that is employed to determine which nodes are utilized. When coupled, direct and indirect trust enable the overall trust of the nodes to be utilized as a targeting mechanism for specific attacks on the network. This enables a higher degree of precision [9].

When transmitting data from one node to another, numerous alternative routing strategies are used, in order to cut down on the amount of energy that is wasted in the process [10]. The only two forms of routing that should be available from efficient

communication protocols are low-energy routing and routing based on mutual confidence [11]-[15]. The authors of this paper provide an trust score evaluation model with the objective of identifying malevolent users in WSN. This model utilizes spatio-temporal constraints in conjunction with a technique known as a decision tree in order to identify the route that will result in the greatest amount of success.

The proposed routing protocol provides a more beneficial choice for the purpose of facilitating effective communication since it makes use of a trust-based routing approach that is both energy-efficient and dependable. This makes the recommended routing protocol the superior option. One of the many benefits of this work is that it enables safe routing, which is made feasible by a technique that takes use of trust in determining whether or not nodes are malicious.

The authors develop a new trust-based security system that makes use of decision trees and assigns trust ratings to individuals in order to locate potential invaders. The performance of the network will be improved in terms of throughput, the percentage of packets delivered, and reduced delay. The key advantage of the trust-based security paradigm that is being offered here is the ease with which rogue nodes may be recognized and removed, and this advantage is essential to the paradigm.

2. PROBLEM DEFINITION

The authors of this work recommend employing a hybrid metaheuristic optimization technique as a means of overcoming these challenges that are associated with MANETs. Imagine a massively addressable network of nodes with a size of L ($L \geq 2r_n$) with a sensor node S dispersed at random throughout the network, and clusters $n \in N$ built by assigning each node to one of $C_1, C_2, \ldots, C_n$, with radii $r_1, r_2, \ldots, r_n$. This particular network would consist of L2RN nodes in their entirety. After this process, clusters are created from the nodes that are grouped together $r_1 \leq r_2 \ldots . r_n$ in the same location.

The sensor node *S* is located in the geometric center of the 2D MANET network, and that this location was achieved without sacrificing any feature of the network generality in the process. It has been shown that the locations of the sensor nodes arrange themselves in the shape of a straight line that runs in a direction that is perpendicular to the axis of coordinates, and the point that constitutes the line center (x_i, y_i) is located at $C_i (i \in [1,n])$.

This research is to find ways to cut down on the neighborhood distance *L* to the greatest degree possible so that MANET clusters can keep their squared cross-sectional areas different from one another while being contained inside those areas. The purpose of this research is to find ways to cut down on the neighborhood distance L to the greatest extent possible. In order for MANETs to achieve their goal, they will seek to maintain the integrity of their cross-sectional regions and guarantee that their clusters are contained inside those areas. The (*L, X*), where *X* stands for the collection of coordinates for the sensor nodes (x_1, $y_{1\ldots.}$, x_i, y_i,$\ldots\ldots\ldots$,x_n, y_n):

According to the findings of the study, the objective may be described as follows:

Minimize *L,s.t*

$$|x_i| + r_i \leq \frac{L}{2}, \forall 1 \leq i \leq n \tag{1}$$

$$|y_i| + r_i \leq \frac{L}{2}, \forall 1 \leq i \leq n \tag{2}$$

$$\sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2} \geq r_i + r_j, \forall 1 \leq i < j \leq n \tag{3}$$

If each of these three factors is satisfied, then the comprehensive plan that was established to address the problem that has been recognized can be put into action to find a solution to the issue. The purpose of this study is to focus in on the exact spots where there is inconsistency in the distance between the circles and find a solution to the problem.

The $E(X)$ serves as a symbol for the energy function that is the topic of discussion. The table that follows explains how this function approximatively determines whether or not a solution is feasible while avoiding overlaps in its application.

$$E(X) = \sum_{k=1}^{n} \frac{1}{2}\left(O_{vk}^2 + O_{hk}^2\right) + \sum_{i=1}^{n-l} \sum_{j=i+1}^{n} \frac{1}{2} O_{ij}^2 \tag{4}$$

where,

O - overlapping between clusters.

O_{vk} - overlap between *k*:

$$O_{vk} = Max\left\{|x_k| + r_k - \frac{L}{2}, 0\right\} \tag{5}$$

where,

O_{hk} - overlap between *k* and sphere

$$O_{hk} = Max\left\{|y_k| + r_k - \frac{L}{2}, 0\right\} \tag{6}$$

where,

O_{ij} - overlap between clusters

$$O_{ij} = Max\left\{r_i + r_j - \sqrt{\left(x_i - x_j\right)^2 + \left(y_i - y_j\right)^2}, 0\right\} \tag{7}$$

Due to the restrictions that $L \geq 2r_n$ placed on the study, it will be challenging to achieve overlap between contemporaneous clusters in actual practice. The core focus of the inquiry, which we will refer to as $<L_{CLB}, E(X)>$, is demonstrated by the following function, which can be found up above. Given that the goal is to find a solution that is practical while simultaneously reducing the length of the neighborhood to its shortest feasible value, utilizing *L* as the evaluation function appears to be the most prudent course of action given that the purpose is to find the shortest possible value for the length of the neighborhood.

If an algorithm finds a lot of possibilities that are exactly the same size, it can be difficult to tell which optimal solution is the best. The development of shorter-length L_C, it is now possible to find a solution to this problem.

2.1 SYSTEM MODEL

In the event that there are nodes in between, we will not consider the distance traveled between the sink and the source to be zero $d>0$. This is because the distance between the sink and the source may be broken up into multiple segments. Instead, we are going to behave as though d is greater than zero. The hypothesis

underlying this study is that nodes that are spatially close to one another but can be distinguished from one another using a $d>0$ are all situated at the same overall distance from the root.

In order to determine the total number of hops, research will need to use the $h = D/d$, which may be located below. We have access to the aforementioned items in order to facilitate an easier completion of this process. The following equation can be used to generate a close approximation of the throughput of the multi-hop link in this scenario:(8) where

$$T = \frac{\log(1+\beta)}{h}(P_{suc})^h \tag{8}$$

where

P_{suc} - message probability at sink

$\beta>0$ - minimum SIR.

The network will be wasting more power than is strictly necessary if the node desire for more spectrum leads in a deterioration in the total spectral performance of the hops. It is possible to send a single packet in the time that has been allotted for that slot because it has been predetermined how the time would be used during the transmission. This allows for more efficient use of the time.

During transmission, both the location of a packet and the channel gain are held steady at the values they had prior to the transmission. This takes place when the packet is sent in fragments as opposed to being sent fully at once. To determine the signal-to-interference ratio, also known as the SIR, just divide the total quantity of the signal that was intended by the total amount of the interference. This particular symbol denotes the aforementioned proportional value.

$$SIR = \frac{g_0 d^{-\alpha}}{\sum_{i\in\Phi_{\text{int}}} g_i r_i^{-\alpha}} \tag{9}$$

where

r_i - distance between node i to Rxreceiver, and

α - path-loss exponent.

g_i - channel gain and

P_{suc} is computed using channel gains g_i and defined:

$$P_{suc} = e^{-\lambda_{\text{int}} k \prod d^2 \beta^2/\alpha} \tag{10}$$

where $k = \Gamma(1+2/\alpha)\Gamma(1-2/\alpha)$

2.2 CLUSTER HEAD FORMATION

It is helpful to use a level-based clustering strategy in order to determine the threshold that plays a role in the process of building the clusters. This is because using this method will generate more trustworthy results than using any other clustering method. In order for a node to take part in the competition for CH, it is necessary for that node to produce a random number. If the test threshold $T(i)$ is lower than the evaluated threshold, the random integer is transformed into a CH by applying the following formula:

$$T(i) = \frac{P_{opt}}{1 - p_{opt}\left(r.\text{mod}\left(\frac{1}{P_{opt}}\right)\right)} * \frac{E_i(r)}{E_{avg}(r)} \tag{11}$$

For each nodes $E_i(r) > 0$, r - iteration,

$E_i(r)$ - node energy.

E_{avg} - residual energy

$$E_{avg} = \frac{\sum E_i(r)}{N} \text{ and}$$

N - nodes.

The energy consumption is defined as:

$$E_n T_{rx}(L,D) = \begin{cases} LE_{n(elec)} + L\varepsilon_{fres} D^2, D < D_0 \\ E_{n(elec)} + L\varepsilon_{m_{pat}} D^4, D \geq D_0 \end{cases} \tag{12}$$

where,

D_0 - threshold distance.

L - data packet size.

$\varepsilon_{m_{pat}}$ - energy loss in multipath.

ε_{fres} - energy loss in free space.

$$D_0 = \sqrt{\frac{\varepsilon_{fres}}{\varepsilon_{m_{pat}}}} \tag{13}$$

2.3 PROPOSED TRUST BASED ROUTING

In the course of this investigation, we make use of the OR process after determining, with the help of the tolerance constant, whether or not nodes are safe. A model of the tolerance constant is utilized so that secure nodes that provide adequate protection for the WSN can be selected. A tolerance constant is established for each node by taking into consideration trust, connectivity, energy rate, and quality of service as inputs. We normalize all of the numbers by dividing them by the greatest feasible value in order to accommodate for the different ranges of values for the parameters. According to the equation, the tolerance constant for the j^{th} node is denoted by the TC_j.

$$TC_j = 0.25[T_j + C_j + E_j + QoS_j] \tag{14}$$

Only M trusted nodes are selected from the network total of N nodes, where $M \leq N$ is the total number of nodes. Safe nodes are those that meet or surpass established standards for dependability, availability, efficiency, and quality of service. Safe nodes can also be defined as nodes that fulfill or exceed all of these criteria simultaneously. Information does not pass via the intermediate nodes. In this scenario, the nodes that meet a given standard of security are selected. Therefore, if TC_j is higher than the threshold, node j^{th} is considered a secure node, which is also sometimes referred to as a malicious node.

2.3.1 Trust:

The trust score of a node represents the degree to which it is able to rely on its neighbors to supply it with various services. The reliability of the j^{th} node is determined by multiplying the direct and indirect trustworthiness of that node by the weights associated

with each of those categories. It is determined, whether or not the j^{th} node may be trusted.

$$T_j = \alpha.DT_j+(1-\alpha).IT_j \quad (15)$$

where

DT_j - direct trust score,

IT_j - indirect trust score

α - weight coefficient.

The trust score of a node is calculated by taking into account both its behavior and its residual energy. mainly due to the fact that the attacking node would often brag to its neighbors through the Hello packet about how many resources it has accessible to it. Taking energy into account can be a useful tool for assisting in the detection of these kinds of attacks. The calculation will tell research how much direct trust research should have in the j_{th} node.

$$DT_j = \beta.e_j + (1-\beta).nc_jnt_j \quad (16)$$

where

e_j - residual energy.

nc_j - total packets sent and

nt_j - total packets sent via j.

β - weight coefficient.

The data in the neighbor table, we can apply the following equation in order to derive the j^{th} node level of indirect trust:

$$IT_j = \sum_{k\in nnj} T_{jk}+T_k|nn_j| \quad (4)$$

Indirect trust is determined by taking the mean of the trust scores of the nodes that have j as a neighbor recommendation.

3. PERFORMANCE ANALYSIS

We tested the proposed strategy by simulating it with the NS2 simulator. The sensor nodes have been dispersed throughout a square grid of 200 × 200 m^2. The 20–100 sensor nodes that have been placed each have an initial energy of 0.5 J. The efficiency of the proposed algorithm is evaluated in comparison to that of other algorithms that are very similar to it.

3.1 SIMULATION PARAMETERS

Experiments conducted with WSNs investigate five distinct network topologies, each with a different number of nodes (20, 40, 60, 80, and 100 respectively) and random beginning positions. In each scenario, 5% of the nodes in the network are malicious, and these nodes are selected at random. While distributed denial-of-service attacks are in place, a round of routing in WSN is analogous to a study of the network topology.

Table.1. Simulation Parameters

Parameter	Value
Area (m^2)	200 m × 200 m
Energy of nodes	2 J
No. of sensor nodes	50–300
Packet size	1024 bits
Initial energy	0.5 J
Mobility model	Random way mobility
E_{elec}	50 nJ/bit
Mobility speed	10 m/s to 50 m/s

In this instance, the level of trust between the nodes is immediately enabled after being set to 0.5. The simulation lasts for a total of 3600 seconds, during which time each node transmits data once every ten seconds. The transmission of simulated traffic with a constant bit rate (CBR), consisting of 1500 bytes for each Data packet and 25 bytes for each Hello packet, is performed.

All of the tests were carried out on the basis of the premise that the starting energy of the nodes was 5 J and that the initial energy of the sink was 100 J. Every node has a transmission range of 15 meters and shares the same sense radius and radio propagation radius with the other nodes. In this investigation, we focus on both stationary and roaming nodes, with the exception of the central sink node, which is treated as a fixed point.

In the case of the mobile example, the velocity of the nodes often range anywhere from 0 to 30 meters per second. We apply the same WSN configuration to both of the different sized scenarios so that we can highlight how similar the two scenarios are to one another.

A comparison of the proposed CH is shown in Table.2, together with the results of the comparison of the packet delivery ratio. The proposed Trust Algorithm outperforms the LEACH Algorithm, the TASRP Algorithm, and the FLSO Algorithm in terms of the percentage of packets that are successfully delivered across all use cases and density of nodes.

Table.2. Packet Delivery Ratio

Number of Nodes	LEACH	TASRP	FLSO	Proposed Algorithm
50	89.08	95.16	95.16	100.22
100	91.11	94.14	95.16	99.21
150	95.16	96.17	97.18	100.22
200	89.08	97.18	99.21	100.22
250	87.06	94.14	95.16	97.18

The outcomes of the throughput tests conducted on the proposed CH in comparison to the currently implemented LEACH, TASRP Algorithm, and FLSO are presented in Table.3, respectively. According to these data, the Trust Algorithm that was proposed offers superior performance across the board for the various node densities that were evaluated.

Table.3. Throughput

Number of Nodes	LEACH	TASRP	FLSO	Proposed Algorithm
50	61530	134510	152474	159243
100	70836	144402	162974	185288
150	113018	154642	163076	213154
200	116609	158725	173338	215226
250	156011	223175	245229	314360

Table.4 Delay

Number of Nodes	LEACH	TASRP	FLSO	Proposed Algorithm

50	0.0810	0.0607	0.0506	0.0405
100	0.0607	0.0506	0.0202	0.0202
150	0.0911	0.0810	0.0202	0.0202
200	0.1316	0.1215	0.0810	0.0709
250	0.1721	0.1417	0.0911	0.0911

The effects of the interval of time between the recommended CH are represented in Table.4. According to the findings, the proposed Trust Algorithm has a lower overall delay for all of the different node densities when compared to the currently used LEACH algorithm, the TASRP Algorithm, and the FLSO.

The results of the calculation used to determine the average amount of energy consumed by the desired CH are presented in Table.4. When compared to the currently used LEACH algorithm, the TASRP Algorithm, and the FLSO, the proposed Trust Algorithm is able to produce a lower average energy usage across the board for all of the node densities.

Table.5. Average energy consumption

Number of Nodes	LEACH	TASRP	FLSO	Proposed Algorithm
50	10.8822	10.2242	10.2040	9.4346
100	13.0485	12.4817	11.9553	10.8215
150	14.7897	13.8685	13.2206	12.3298
200	16.6220	15.2959	14.4050	13.8483
250	22.4123	21.2279	20.4890	19.8107

In Table.5, an analysis of the proposed control overhead for CH is shown. According to the findings, the Trust Algorithm delivers lower overhead control for all of the node density when compared to the currently used LEACH, the TASRP Algorithm, and the FLSO. This is the case regardless of which algorithm is being used.

4. CONCLUSION

In this research, we provide a secured uneven clustering method for WSN. The objective of this method is to ensure that the data transmission process is both dependable and effective while consuming the least amount of energy possible. The proposed solution improves network dependability, as well as energy efficiency and longevity. This is accomplished by reducing the number of hot spots by unequal clustering. The cluster stage contributes significantly to the prolonged network lifetime in addition to playing a crucial role. Extensive simulation proved that the proposed model, despite the presence of attackers, prolonged the sensor node mortality and increased throughput.

REFERENCES

[1] S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks", *Proceedings of International Conference on Communication, Computing and Security*, pp. 146-151, 2011.

[2] P. Vivekanandan and A. Sunitha Nadhini, "A Survey on Efficient Routing Protocol using Mobile Networks", International *Journal of Advances in Engineering and Technology*, Vol. 6, No. 1, pp. 370-382, 2013.

[3] V. Balasubramanian and A. Karmouch, "Managing the Mobile Ad-Hoc Cloud Ecosystem using software Defined Networking Principles", *Proceedings of International Symposium on Networks, Computers and Communications*, pp. 1-6, 2017.

[4] M. Maalej, S. Cherif and H. Besbes, "QoS and Energy Aware Cooperative Routing Protocol for Wildfire Monitoring Wireless Sensor Networks", *The Scientific World Journal*, Vol. 2013, pp. 1-11, 2013.

[5] M. Chen, T. Kwon, S. Mao, Y. Yuan and V.C. Leung, "Reliable and Energy-Efficient Routing Protocol in Dense Wireless Sensor Networks", *International Journal of Sensor Networks*, Vol. 4, No. 1-2, pp. 104-112, 2008.

[6] S. Murthy and G. Varaprasad, "Digital Signature-based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", *IEEE Sensors Journal*, Vol. 12, No. 10, pp. 2941-2949, 2012.

[7] A. Ahmed and A.W. Khan, "TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network", *IEEE Sensors Journal*, Vol .15, No. 12, pp. 6962-6972, 2015.

[8] T. Khan and K. Singh, "TASRP: A Trust Aware Secure Routing Protocol for Wireless Sensor Networks", *International Journal of Innovative Computing and Applications*, Vol. 12, No. 2-3, pp. 108-122, 2021.

[9] L. Gong and Z. Zhao, "Fine-Grained Trust-Based Routing Algorithm for Wireless Sensor Networks", *Mobile Networks and Applications*, Vol. 2021, pp. 1-10, 2021.

[10] W. Lou, "An Efficient N-to-1 Multipath Routing Protocol in Wireless Sensor Networks", *Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems*, pp. 1-8, 2005.

[11] K. Zhang and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks using Group Key Management", *Proceedings of IEEE International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-5, 2008.

[12] R. Sumathi and M.G. Srinivas, "A Survey of QoS Based Routing Protocols for Wireless Sensor Networks", *Journal of Information Processing Systems*, Vol. 8, No. 4, pp. 589-602, 2012.

[13] L. Daanoune and A. Ballouk, "A Comprehensive Survey on LEACH-based Clustering Routing Protocols in Wireless Sensor Networks", *Ad Hoc Networks*, Vol. 114, pp. 102409-102415, 2021.

[14] S. Kaur and R. Mahajan, "Hybrid Meta-Heuristic Optimization based Energy Efficient Protocol for Wireless Sensor Networks", *Egyptian Informatics Journal*, Vol. 19, No. 3, pp. 145-150, 2018.

[15] U. Meena and A. Sharma, "Secure Key Agreement with Rekeying using FLSO Routing Protocol in Wireless Sensor Network", *Wireless Personal Communications*, Vol. 101, pp. 1177-1199, 2018.