International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

Chief Editor
Dr. J.B. Helonde

Executive Editor
Mr. Somil Mayur Shah

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURITY BASED ENERGY EFFICIENT ROUTING PROTOCOL FOR WSN WITH HYBRID OPTIMIZATION TECHNIQUES

Deepika Yajamanam, Prof. V. Raghunatha Reddy
Department of Computer Science & Technology Sri Krishnadevaraya University, Anantapur, India
Department of Computer Science & Technology Sri Krishnadevaraya University, Anantapur, India

DOI: 10.5281/zenodo.8310994

ABSTRACT

The use of wireless sensor networks (WSNs) for data collection and transmission through wireless networks has grown significantly. Security is a key design consideration for WSNs since open wireless transmission media are vulnerable to attacks. The security offered by current methods is insufficient because they treat data encryption and routing as two separate problems. So, a novel method called TFEESRP (Trust and Fitness-based Energy Efficient Secured Routing Protocol) is proposed in this paper with the integration of a data encryption phase and a data path selection phase. In the data path selection phase trust and fitness-based optimization techniques like Ant Colony Optimization and Particle Swam optimization (PSO) techniques are used and in the data encryption phase Rivest Shamir Adleman (RSA) security algorithm is used for secured packet transfer through the optimal selected path. The performance of the proposed technique is evaluated in terms of Energy Consumption, End-to-End delay, Packet Delivery Ratio, and Throughput of routing protocol.

Keywords: Ant Colony Optimization Algorithm (ACO), Particle Swarm Optimization Algorithm (PSO), Rivest Shamir Andleman (RSA) , Wireless Sensor Networks (WSN).

1. INTRODUCTION

Wireless Sensor Networks (WSNs) play a key role in several applications, including agriculture, healthcare, military operations, and target-tracking methods [1], [2]. WSNs comprises one or more sink node, the low-cost and small size of sensor nodes. Sensor nodes in a WSN are frequently randomly placed in areas that are often beyond human reach which are known as sensor fields or fields of observation. For instance, the sensor nodes in the battery system have insufficient energy sources. It is difficult to manually recharge the energy source of the sensor node due to the unsupervised and complex deployments of sensor nodes [3, 4]. Three different types of actions are carried out by wireless sensors: event processing, interacting with nearby nodes, and event sensing. Among these, energy use must be an important resource for communication. It's important to keep in mind that routing protocols must be energy-efficient to prolong the lifespan of sensor nodes and the sensor network. Therefore, the two main issues in the WSN that need to be addressed are energy efficiency and network longevity.

Until now, energy-effective routing has been a significant hurdle to overcome. To choose a path for data transfer in the network, a WSN's nodes (routers) must adhere to a protocol for data communication. Many energy-efficient data communication protocols are set up to distribute the energy burden over all nodes, reducing a WSN's power consumption.

Similarly, a crucial difficulty is the security of the data transmitted across the sensor network. Maintaining security and confidentiality is difficult because of the unconstrained wireless networking feature of WSN and the limited capabilities of nodes [5]. There are no security measures in place, which means that sending data outside of the network or storing it within the system could result in the loss of data.

The two most often used authentication methods in wireless networks are encryption and cryptographic keys. Although encryption guarantees privacy, honesty, and authenticity, it has a hefty cost in terms of processing and

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

energy. It is easier to identify misbehaving nodes using trust-based protocols. Compared to conventional defense methods, the trust management paradigm is more adaptable, scalable, and reliable. Sharing and security services can be made available by developing trust relationships between sensor nodes. In an open network setting, the trust model improves protection based on the computation of a node's confidence values. As a result, techniques that are based on trust and reputation offer simple answers to the problem of security in WSNs.

The main objective of this work is to provide secure data transmission from the sensor node to the Base Station through an optimal path along with the effective utilization of energy. The remainder of this paper is organized in the following way. Section 2 presents the review of the literature and the proposed methodology is presented in section 3. The results and experimental analysis are carried out in section 4 and finally, the concluding remarks are presented.

2. REVIEW OF LITERATURE

Generally, most of the routing protocols' primary focus is to attain power conservation in WSNs [6]–[9]. With regards, some of them focused on the energy-efficient routing protocol [10]–[12], energy-efficient cluster-based routing protocol [13]–[16], trust with key management-based routing system for achieving high security [17], [18], and optimization-based routing technique with security [19]–[22]. Similarly, research by Sharma et al. [23] evolved a clustering routing protocol for WSNs. Furthermore, they have combined different sensor nodes, and then the resulting clusters are translated into hierarchical management systems that have various cluster heads and base stations. The simulated results show that they attained better results in terms of end-to-end delay and energy consumption. At the end of the research, they recommended that will enhance the performance by adopting network security and privacy concerns with varying environmental conditions.

A work by Mehta and Saxena [24] presented a Multi-Objective Based Clustering, and Sailfish Optimizer (SFO) guided routing approach toward sustaining energy efficiency in WSNs. Based on the evaluation of fitness function, they have selected the cluster head. With regard, they have minimized the number of dead sensor nodes and minimized the energy consumption of the routing protocol. For the transmission of data, the suggested model selected an optimal path after the selection of the cluster head. The suggested model performance was compared with four traditional methods namely, genetic algorithm, grey wolf optimization, particle swarm optimization method, and ant lion technique with specific to packet delivery ratio, energy consumption, network lifetime, and network throughput ratio. The demonstrated results show that the suggested model gives better performance while the average measure of the number of alive sensor nodes (24.4%) and energy consumption (21.9%).

A work by Sun et al. [25] presented a secure routing protocol based on Multi-objective Ant-colony optimization for WSN. By adopting the trust value of route path and residual energy, the ant colony optimization method has been enhanced. The performance of the suggested model tested using network simulator version 2 that the resulting outcome attained better performances in terms of average energy consumption, routing load, and data packet loss ratio. But the limitation of this study as only considered the four constraints and two objective functions. So, further needs to enhance the system performance by assuming more constraints and objective functions which should minimize the network failure probability, maximize the network reliability, and maximize the network lifetime Rao et al. [26] presented a cluster-head selection protocol based on the PSO method. However, the simulated results have shown that the distance between the sink and a selected channel does not cover the uniformity of the entire region, which causes unstable energy intake in the network layer.

Similarly, a study by Adnan et al. [27] presented a cuckoo search clustering method, where they incorporated two sensor nodes of different sorts. The simulated result shows that the suggested protocol consumes more energy for 20% of nodes than the left behind 80% of nodes. However, it suffers from unbalanced energy consumption due to non-uniform Channel distribution problems in the network. A study by Elhabyan and Yagoub [28] presented a two-tier PSO-based routing and clustering protocol. However, these approaches also suffered from unbalanced energy consumption issues and have not considered balanced energy consumption.

In some cases, most of the researchers have assumed both routing and clustering protocols in the isolated entity module. Subsequently, in very few cases, the network channels are directly communicated with a sink node. Hence, they have integrated the optimization issues with routing and clustering protocol via an efficient meta-

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

heuristic approach. A study by Sugandh and Panday [29] has extended the lifetime of the network path and nodes via an energy-efficient LEACH protocol. Moreover, it has a low packet loss rate and high energy efficiency through the selection of cluster heads. The drawback of the suggested method has more communication overhead. From the above review, it has been observed that most of the routing protocols have failed to categorize the various factors like QoS aware, cluster-based routing protocol, postured-based routing protocols, and thermal-aware, security-aware, and cross-layered routing protocols. So, the study needs to focus on solving the various routing problems by considering appropriate factors like path loss, energy efficiency, latency, and network node stability ratio [30].

In addition, to address the issues of energy consumption, a few of the researchers suggested PSO [31], and [32] techniques. However, these algorithms face the issues of unbalanced and balanced energy consumption problems. The study of the RSA algorithm used with MAODV with PSO has yielded good results[33].

Also, none of them has focused all these routing protocols on a single network. So, the present study planned to propose an efficient routing protocol which is a combination of trust and fitness-based optimization methods along with security towards solving the various routing issues by considering the related factors namely path loss, energy efficiency, latency, and network stability.

3. PROPOSED TFEESRP APPROACH

This paper presents an improved model of TFEESRP, where we consider both the security and efficiency of the system by proposing a routing protocol that integrates key management, trust, and fitness-based optimization approaches. Initially, the sensor nodes are deployed, and the trust level of the sensor node is calculated by considering the packet delivery rate and end energy of the sensor node. By calculating the trust level, the malicious nodes are weeded out from the system and every sensor node can identify the best neighbors for sending packets to a specific destination. Furthermore, fuzzy rules are created, and the cluster head is formed based on the selected cluster in the network node that has a higher trust score. To select the best path among available paths the PSO algorithm is applied and it also helps to find the best fitness value for the transmission process. After finding the optimal path by using the two optimization techniques now the data can be transmitted from the source node to the base station by using the security algorithm RSA. The flowchart of the TFEESRP method is represented in Fig. 1.

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

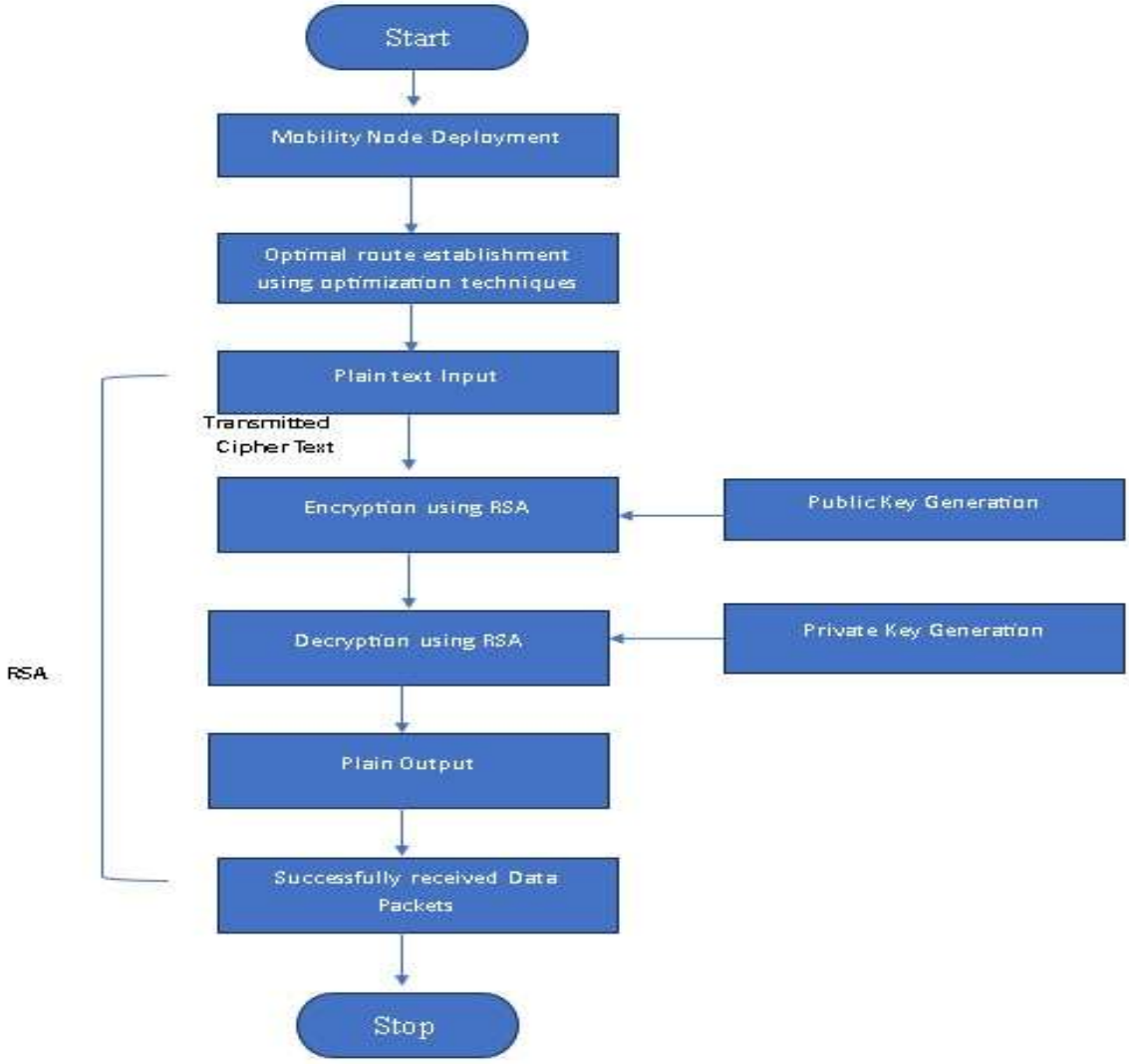

Fig 1. Flowchart of the TFEESRP method

Initially, the sensor nodes are randomly organized in the region of the network for gathering information from neighbor nodes. Reliable ACO and PSO optimization with the AODV routing protocol technique is used for best route selection. Finally, the RSA is used to protect the transmitted data. The process is repeated until all the data packets are received by the destination nodes.

System Architecture

In a wireless sensor network, the suitable route has been predicted based on the selection of neighbor nodes responsible for data transfer between the source and the endpoint. Furthermore, the neighbor node is selected based on attained trust and fitness value.

Trust and Fitness based Computation

For computing the trust level of a SN packet delivery rate and energy of the SN is considered. The packet delivery rate is considered because certain nodes may behave selfishly. In such conditions, the sensor nodes will not show interest to forward packets, in order to preserve their energy. Thus, it checks the packet delivery rate of SNs along the communication path. For calculating the fitness of SN residual energy and energy consumption of every node is considered. The residual energy is considered because, if the selected node has more residual

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

energy it leads to prolonging network lifetime. In the case of energy consumption, if nodes consume more energy, they will dry very soon which leads to reducing network lifetime.

If the packet input equals the packet output, then the sensor nodes behave normally. A trust threshold is set and the sensor nodes can participate in routing, only when its energy is greater than or equal to the threshold. The sensor node cannot participate in routing if its trust level is less than the threshold. In this way, malicious nodes are weeded out from the communication path.

As all the SNs along the communication path are trustworthy, the packets are forwarded in full swing. So, lesser energy consumption is observed. The energy consumption of sensors is inversely proportional to the lifetime of the network.

To extend the lifetime of a WSN, TFEESRP is used by incorporating trust and fitness level computation. TFEESRP employs ants to come up with a short, energy-efficient, and trustworthy route. It is quite successful because of the computation of short routes with trustworthy nodes. A node is claimed as trustworthy by two deciding parameters and they are packet delivery rate and its energy level. The packet delivery rate is calculated by the total number of packets being sent by the node to the total number of acknowledgments being received by that node.

If the number of packets sent and the same number of acknowledgments are received then the node is pretty trustworthy. The energy threshold is calculated and the number of nodes that are above the energy threshold along the path is calculated. This yields effective routing and thus the lifetime is improved.

The trust level of every node is calculated by the one-hop neighbor in order to determine its trust and the trust level is updated in the trust table maintained by every SN. The trust level is calculated for every period of time and is overwritten in the trust table, so as to save memory. The node energy is calculated by the below assumption.

1. If the node is fully energized, then the energy value is 1.
2. If the energy of a node is > 0 then the energy value is energy/100.
3. A completely energy-drained node's energy value is 0.

The energy value (EN) between every two nodes is computed and the value obtained is the energy threshold. The packet delivery rate is computed by the one-hop neighbor and the values are normalized between [0, 1].

The packet delivery rate is calculated by using the following assumptions

1. If $sent_{pk} = T_{ack}$, then
   the packet delivery rate is fixed at 1.
2. If $T_{ack} > 0$, then
   the packet delivery rate is $T_{ack}/100$.
3. If $T_{ack} = 0$,then
   the packet delivery rate is 0.

Both these values are integrated and the trust level is computed by the below given formula.

$$TL_{xy} = (PDR + EN)/2 \qquad 1$$

Where PDR and EN are the packet delivery rate and the energy of two nodes and the value of TLxy lies in between 0 and 1.

Optimization Technique

Particle Swarm is a nature-inspired optimization technique. Every particle has its fitness value associated with it to evaluate the quality of the solution. Using PSO, clustering and routing problems are addressed, and fitness value is to find the best path from the CH to the Base station [34]. The working principle of PSO is provided below.

$$Vi\ (t+1) = \omega Vi\ (t) + c1r1\ (pbest\ (i,t) - Pi\ (t)) + c2r2\ (gbest\ (t) - Pi\ (t))$$
$$Pi\ (t+1) = Pi\ (t) + Vi\ (t+1) \qquad 2$$

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

where V denotes the velocity, ω is the inertia weight used to balance the global exploration and local exploitation, $r1$ and $r2$ are uniformly distributed random variables within the range [0, 1], and $c1$ and $c2$ are positive constant parameters called "acceleration coefficients."

In this approach, the lifetime of a network is extended by considering the trust and fitness level of nodes. The trust level of nodes is computed by considering energy and packet delivery rate as well as fitness level is computed by using residual energy and energy consumption. The trust and fitness levels are computed by using equations 1 and 2.

This is passed into the ACO as input. By calculating the trust level, the malicious nodes are weeded out from the system. The nodes with a trust value greater than or equal to the threshold can only participate in routing.

The probability of data packet transmission from the source to the destination node through the best route is given by

$$p(s,d) = \begin{cases} \frac{[TL[(s,d)]^{\alpha}[\frac{1}{d_{sd}}]^{\beta}(p_{f_{sd}})^{\gamma}}{\sum_{\forall v\_n}[TL(s,v_n)]^{\alpha}[\frac{1}{d_{s,v_n}}]^{\beta}(p_{f_{s,v_n}})^{\gamma}} \end{cases} \quad 3$$

Where $TL(s,d)$ is the trust level of nodes between s and d
d_{sd} is the distance between the source and the destination node
$p_{f_{sd}}$ is the amount of pheromone between s and d
v_n are the valid nodes
α, β and γ are constants that belong to [0,1]

When the backward ant is back to the source node s to d, then the routing table is updated by the following

$$p_f(u) = (1-\rho)p_f(u-1) + \frac{N_{sd}}{d_{sd}} \quad 4$$

ρ is the evaporation constant that belongs to [0,1].

With the above approaches, the optimal route path is identified. Now the data packets are get encrypted and decrypted with the use of the RSA algorithm.

Rivest Shamir Adleman (RSA) security algorithm

In this research, the RSA algorithm is used for securing sensitive data and secure data transmission, because RSA provides more reliable encryption than other encryption standards. The RSA consists of four steps such as the generation of the key, distribution of the key, data encryption, and data decryption. The public key will be known to all, but the private key generated during the data encryption will be sent to the receiver node and a reasonable amount of time will be allotted to decrypt the data.

Input: Generate or choose large random prime numbers.
Output: Public Key (n, e) and private key (d).
1. Two different prime numbers such as p and q are generated.
2. Compute the modulus $n = p \times q$.
3. Compute the $\varphi(n) = (p-1) \times (q-1)$.
4. Choose for public exponent an integer e such that $1 < e < \varphi(n)$ and $gcd(\varphi(n), e) = 1$.
5. Compute the private exponent $d = e - 1 mod \varphi(n)$ (employing the extended Euclidean algorithm).
6. Public key=(e, n).
7. Private key(d).

Eq. (5) is written as Eq. (6) by interchanging d and e values.

$$(m^e)^d \equiv m(mod\ n) \quad (5)$$
$$(m^d)^e \equiv m(mod\ n) \quad (6)$$

The sender A can send an encryption message to the B without requiring a prior exchange of secret keys. The data A transmits through a public key (n, e) to B on a route, which is reliable. For encryption, it considers an integer m that lies between (0, n) such that gcd of $\{m, n\}$ must be equal to one. From m and n the cipher text c

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

calculated, which shows in Eq. (7). The data is successfully transferred using the RSA encryption algorithm. During B sends the data to A in the decryption process the s, m is recovered from C employing the private key exponential d by Eq. (8).

$$c = m^e \ (mod\ n) \quad (7)$$

$$c \equiv (m^e)^d \equiv m(mod\ n) \quad (8)$$

The RSA algorithm is a common public key cryptography for data encryption and decryption process. The powerful encryption and optimized key management scheme always help to achieve authentication and integrity of data and mitigate the overheads of a network system. In this algorithm, the key length is directly proportional to the security and inversely proportional to network performance. Hence, hacking time is reduced, which represents that the time available for hackers has been reduced. In this way, the data packets are securely sent from source to destination with optimistic energy. The simulation results of the TFEESRP method are described in the following section.

Experimental Analysis

This section briefly explained the experimental result of the TFEESRP method evaluated with the NS2 software tool. In this paper, 500 nodes are distributed randomly in 500 x 500 m. The time taken for each simulation is 300 seconds. The experimental result of the proposed work is compared with the existing protocols such as FF (Flooded Forward ant routing) as proposed in [35], Ad hoc On-Demand Distance Vector routing (AODV) [36], TLACO [37], and TFLACO [38].

The performance metrics employed in this work are packet delivery ratio, end-to-end delay, energy consumption, and packet loss. These performance parameters are taken by varying the number of nodes (static/fixed nodes) and by a varying number of rates. The process repeats until entire data packets are received to the destination nodes.

Energy Consumption:

The value of the energy consumption is considered as joules. The energy consumed on sleep, idle, transmission and receive with respect to the total energy consumed, which is expressed in Eq. (9).

$$\text{Energy consumption} = \text{Current value} - \text{Initial energy value} \quad (9)$$

The energy consumption of the proposed method is studied by varying the number of nodes from 10 to 100 in Table 1 and it can be observed that the proposed method conserves energy efficiently with the help of optimization techniques when compared to FF and TLACO. This is represented in Fig 2 by taking Energy consumption values along the y-axis.

Table 1
Analysis of Energy Consumption

Number of Nodes	**Energy Consumption**				
	FF	**AODV**	**TLACO**	**TFLACO**	**TFEESRP**
10	2	2	3	2	2.5
20	3	3	5	2.5	3.4
30	4.8	4.2	6.9	3.1	4.15
40	6	5	8	4	5.1
50	8.3	6	10.4	5.5	6.55
60	10	7	13	6.5	8.4

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

70	12	8.5	16	7.5	9.5
80	13	10	17	8	9.7
90	15.5	11	20.5	10	10.5
100	17	13	24	11	12.5

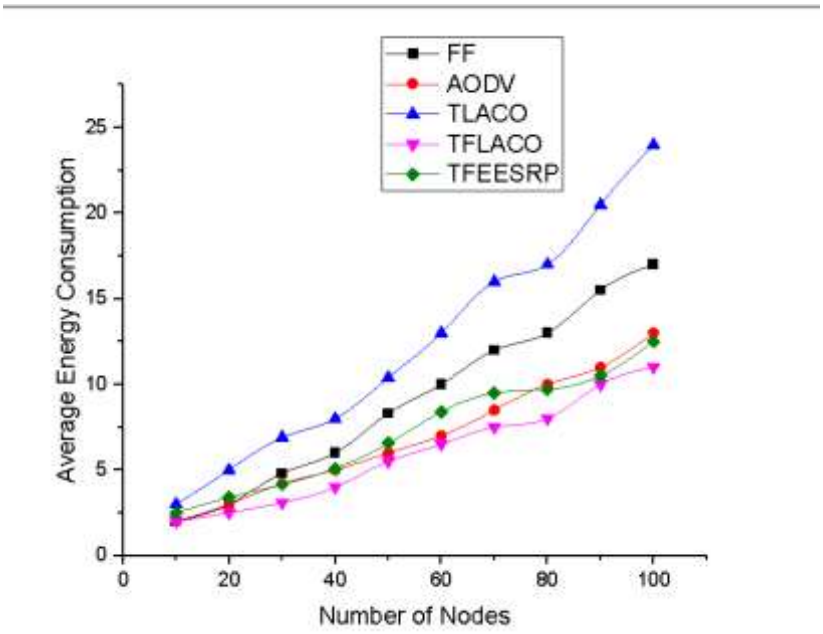

Fig 2 Analysis of Energy Consumption with Respect to Time

End-to-end delay

The end-to-end delay defines the time a packet takes to be transmitted across a network from the transmitter to the receiver. The performance of delay is measured in Sec. The end-to-end delay is expressed in Eq. (10).

$$\text{End to End Delay} = \text{Packet Recived Time} - \text{Packet Transmited Time} \quad (10)$$

From Table 2, it can be observed that the number of nodes is varied from 50 to 500. The end-to-end delay is measured in seconds and is taken as the y-axis. From Figure 3, it is proved that the proposed method takes less amount of time to deliver the packets when compared to the other systems.

Table 2
Analysis of End-to-End Delay

Number of Nodes	**End-to-End Delay**				
	FF	**AODV**	**TLACO**	**TFLACO**	**TFEESRP**
50	7.5	7	5	3.75	3.46
100	9	7.75	6	4.25	4.15
200	10.25	8.5	6.75	4.5	4.35

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

300	11.25	8.75	7.25	5	4.75
400	12	9.25	7.5	5.25	5.05
500	12.75	9.75	8	5.75	5.35

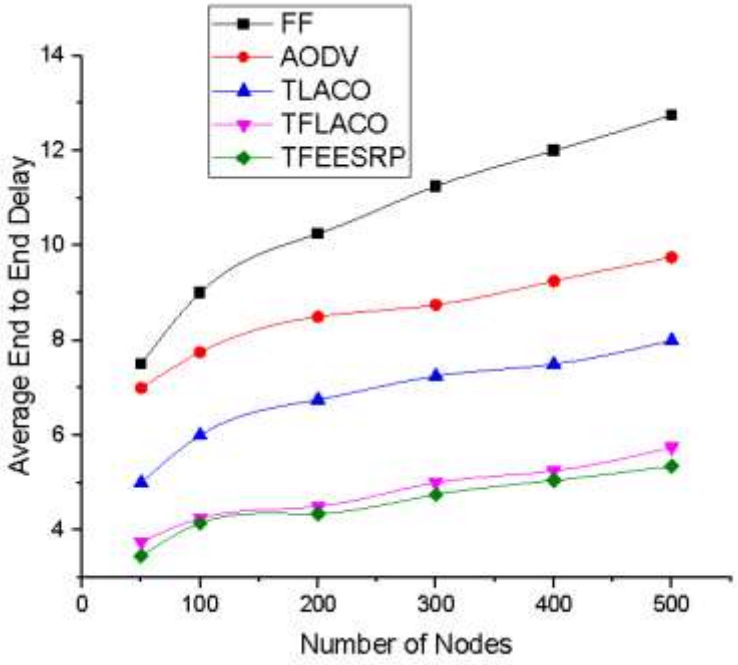

Fig. 3 Analysis of End-to-End Delay

Packet Delivery Ratio

The PDR is the total percentage of the packets successfully received at the destination. The formula of PDR is expressed in Eq. (11).

$$PDR = \frac{\text{Total number of packets received}}{\text{Total number of packets sent}} \quad (11)$$

In Table 3, it can be observed that the number of nodes is varied from 50 to 500. In Figure 4, the average packet delivery ratio (in percentage) is considered at the y-axis to the number of nodes at the x-axis. From Table 3, it is evident that the TFEESRP provides a greater packet delivery ratio than the other existing systems.

Table 3
Analysis of Packet Delivery Ratio

Number of Nodes	**Packet Delivery Ratio**				
	FF	**AODV**	**TLACO**	**TFLACO**	**TFEESRP**
50	70	75	80	85	87
100	65	75	75	85	86
200	55	75	70	80	81
300	50	60	65	75	77
400	50	55	65	70	72

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

500	45	50	55	65	66

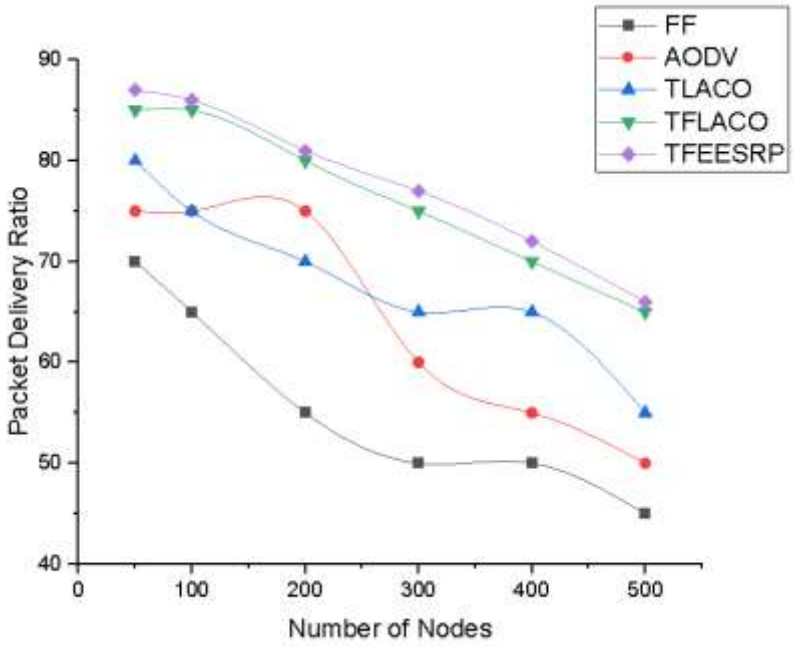

Fig 4 Analysis of Packet Delivery Ratio

Throughput

Throughput is the amount of data transferred per unit of time.

$$\text{Throughput} = \frac{\text{Number of transferred bits}}{\text{Time taken (secs)}} \quad (12)$$

In Table 4, it can be observed that the time is varied between 10 and 100 seconds. The average throughput in kbits/second is considered as the y-axis. From Figure 5, it is evident that the TFEESRP shows the highest throughput compared with the existing approaches.

Table 4
Analysis of Throughput

Number of Nodes	**Throughput**				
	FF	**AODV**	**TLACO**	**TFLACO**	**TFEESRP**
10	2.4	4	8	8.5	8.7
20	3.1	4.5	8.8	9.1	9.34
30	3.7	5	9.3	9.5	9.62
40	4.1	5.3	9.6	9.7	9.74
50	4.2	5.5	9.7	10	10.25

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

60	4.4	5.7	9.8	10.5	10.64
70	4.5	5.9	10	11	11.34
80	4.7	6.1	11	12	12.33
90	5	6.4	11.4	12.8	12.93
100	5.2	6.4	11.7	13	13.24

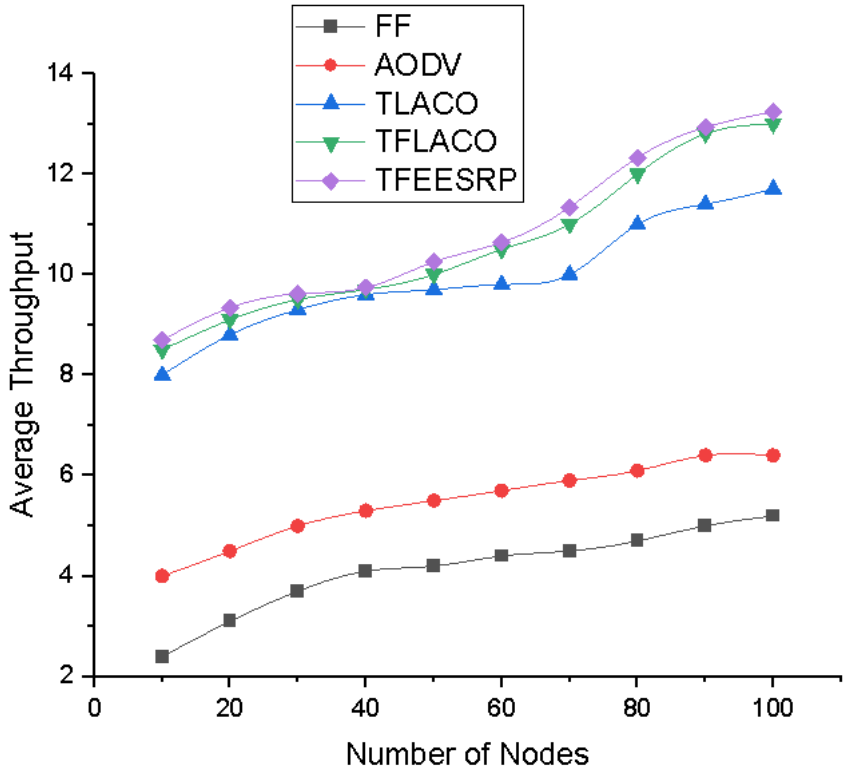

Fig 5 Analysis of Throughput

4. CONCLUSION AND FUTURE SCOPE

Maintaining the security of the data packets with less energy consumption is a major challenging task in Wireless Sensor Networks. As the energy consumption is condensed, the lifetime of the sensor network is improved. In addition to this providing security to the data transmission also conserves the energy by reducing the need for retransmission due to attacks. The proposed routing protocol selects the optimal routes in multiple routes for transferring the required data to the destination. The proposed protocol checks the quality of the routes before sending data, because sending through low-quality routes may cause retransmission, congestion, and waste of energy. The proposed work used ACO and PSO-based optimization techniques to select the optimal route with reduced energy consumption. Finally, the transmitted data packets are secured by using RSA, because RSA provides more reliable encryption than other encryption standards. The simulation results show the performance of the proposed technique against the existing protocols with benchmark performance metrics such as packet delivery ratio, end-to-end delay, throughput, and energy consumption.

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

REFERENCES

1. M. Hawa, K. A. Darabkh, R. Al-Zubi, and G. Al-Sukkar, "A Self-Learning MAC Protocol for Energy Harvesting and Spectrum Access in Cognitive Radio Sensor Networks," J. Sensors, vol. 2016, pp. 1–18, 2016.
2. [2] K. A. Darabkh, W. Y. Albtoush, and I. F. Jafar, "Improved clustering algorithms for target tracking in wireless sensor networks," J. Supercomput., vol. 73, no. 5, pp. 1952–1977, May 2017.
3. [3] G. P. Gupta, M. Misra, and K. Garg, "Energy and trust aware mobile agent migration protocol for data aggregation in wireless sensor networks," J. Netw. Comput. Appl., vol. 41, pp. 300– 311, May 2014.
4. [4] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proc. of the 33rd Annual Hawaii International Conference on System Sciences, vol. vol.1, p. 10, 2000.
5. [5] Z. Al Aghbari, A. M. Khedr, W. Osamy, I. Arif, and D. P. Agrawal, "Routing in wireless sensor networks using optimization techniques: a survey," Wireless Personal Communications, vol. 111, no. 4, pp. 2407–2434, 2020.
6. [6] Z. Jin, Y. Jian-Ping, Z. Si-Wang, L. Ya-Ping, and L. Guang, "A Survey on Position-Based Routing Algorithms in Wireless Sensor Networks," Algorithms, vol. 2, no. 1, pp. 158–182, Feb. 2009.
7. [7] S. Nikoletseas and P. Spirakis, "Probabilistic Distributed Algorithms for Energy Efficient Routing and Tracking in Wireless Sensor Networks," Algorithms, vol. 2, no. 1, pp. 121–157, Feb. 2009.
8. [8] A. Alemdar and M. Ibnkahla, "Wireless sensor networks: Applications and challenges," in Proc. of 2007 9th International Symposium on Signal Processing and Its Applications, pp. 1–6, Feb. 2007.
9. [9] T. Amgoth and P. K. Jana, "Energy-aware routing algorithm for wireless sensor networks," Comput. Electr. Eng., vol. 41, pp. 357–367, Jan. 2015.
10. [10] W. Zhang, G. Han, Y. Feng, and J. Lloret, "IRPL: An energy-efficient routing protocol for wireless sensor networks," J. Syst. Archit., vol. 75, pp. 35–49, Apr. 2017.
11. [11] S. B. Lande and S. Z. Kawale, "Energy Efficient Routing Protocol for Wireless Sensor Networks," in Proc. of 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), pp. 77–81, Dec. 2016.
12. [12] H.-H. Liu, J.-J. Su, and C.-F. Chou, "On Energy-Efficient Straight-Line Routing Protocol for Wireless Sensor Networks," IEEE Syst. J., vol. 11, no. 4, pp. 2374–2382, Dec. 2017.
13. [13] K. Muthukumaran, K. Chitra, and C.Selvakumar, "An energy-efficient clustering scheme using multilevel routing for wireless sensor network," Comput. Electr. Eng., vol. 69, pp. 642-652, Jul. 2018.
14. [14] K. A. Darabkh, N. J. Al-Maaitah, I. F. Jafar, and A. F. Khalifeh, "EA-CRP: A Novel Energy-aware Clustering and Routing Protocol in Wireless Sensor Networks," Comput. Electr. Eng., vol. 72, pp. 702-718, Nov. 2018.
15. [15] S. Nikolidakis, D. Kandris, D. Vergados, and C. Douligeris, "Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering," Algorithms, vol. 6, no. 1, pp. 29–42, Jan. 2013.
16. [16] R. Sujee and K. E. Kannammal, "Energy efficient adaptive clustering protocol based on genetic algorithm and genetic algorithm inter cluster communication for wireless sensor networks," in Proc. of 2017 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–6, Jan. 2017.
17. [17] P. Khatri, "Using identity and trust with key management for achieving security in Ad hoc Networks," in Proc. of 2014 IEEE International Advance Computing Conference (IACC), pp. 271–275, Feb. 2014.
18. [18] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," IEEE Trans. Netw. Serv. Manag., vol. 9, no. 2, pp. 169–183, Jun. 2012.
19. [19] S. Dhanalakshmi and M. Sathiya, "An Improved Ant Based Routing Technique in WSN with High Security," no. September, pp. 1771–1778, 2015.
20. [20] D. Srinath, V. Subedha, and S. Venkatraman, "ACO based mobile agent for secured key management in manet," ARPN J. Eng. Appl. Sci., vol. 10, no. 11, pp. 4877–4881, 2015.
21. [21] S. Ganesh, "Efficient and Secure Routing Protocol for WSN-A Thesis," 2017.
22. [22] T. Rahayu, S.-G. Lee, and H.-J. Lee, "A Secure Routing Protocol for Wireless Sensor Networks Considering Secure Data Aggregation," Sensors, vol. 15, no. 7, pp. 15127–15158, Jun. 2015.

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

23. [23] N. Sharma, B. M. Singh, and K. Singh, "QoS-based energy-efficient protocols for wireless sensor network," Sustain. Comput. Informatics Syst., vol. 30, p. 100425, Jun. 2021.
24. [24] D. Mehta and S. Saxena, "MCH-EOR: Multi-objective Cluster Head Based Energy-aware Optimized Routing algorithm in Wireless Sensor Networks," Sustain. Comput. Informatics Syst., vol. 28, p. 100406, Dec. 2020.
25. [25] Z. Sun, M. Wei, Z. Zhang, and G. Qu, "Secure Routing Protocol based on Multi-objective Ant colony-optimization for wireless sensor networks," Appl. Soft Comput., vol. 77, pp. 366–375, Apr. 2019.
26. [26] P. C. S. Rao, P. K. Jana, and H. Banka, "A particle swarm optimization- based energy efficient cluster head selection algorithm for wireless sensor networks," Wirel. Networks, vol. 23, no. 7, pp. 2005–2020, Oct. 2017.
27. [27] M. A. Adnan, M. A. Razzaque, M. A. Abedin, S. M. Salim Reza, and M. R. Hussein, "A Novel Cuckoo Search Based Clustering Algorithm for Wireless Sensor Networks," pp. 621–634, 2016. 3856 Mercy et al.: An Energy- Efficient Optimal multi-dimensional location, Key and Trust Management Based Secure Routing Protocol for Wireless Sensor Network
28. [28] R. S. Y. Elhabyan and M. C. E. Yagoub, "Two-tier particle swarm optimization protocol for clustering and routing in wireless sensor network," J. Netw. Comput. Appl., vol. 52, pp. 116– 128, Jun. 2015.
29. [29] Sugandh and R. Panday, "Energy Efficient-Long Life LEACH Variant Protocol for MANET Environment," Int. J. Comput. Sci. Inf. Technol., vol. 7, no. 5, pp. 2320–2325, 2016.
30. [30] F. T. Zuhra, K. A. Bakar, A. Ahmed, and M. A. Tunio, "Routing protocols in wireless body sensor networks: A comprehensive survey," J. Netw. Comput. Appl., vol. 99, pp. 73–97, Dec. 2017.
31. [31] P. C. S. Rao, P. K. Jana, and H. Banka, "A particle swarm optimization-based energy efficient cluster head selection algorithm for wireless sensor networks," Wirel. Networks, vol. 23, no. 7, pp. 2005–2020, Oct. 2017.
32. [32] R. S. Y. Elhabyan and M. C. E. Yagoub, "Two-tier particle swarm optimization protocol for clustering and routing in wireless sensor network," J. Netw. Comput. Appl., vol. 52, pp. 116– 128, Jun. 2015.
33. [33]V.L. Vinya and G. Venkateswara Rao, "An Energy Efficient Multicast Route Establishment using AODV with PSO Algorithm and RSA for Secured Transmission" Journal of Intelligent Engineering & Systems., vol.12, pp. 257– 266, April 2019.
34. [34] Elhabyan, R. S., & Yagoub, M. C. (2015). Two-tier particle swarm optimization protocol for clus- tering and routing in wireless sensor network. Journal of Network and Computer Applications, 52, 116–128.
35. [35] Y. Zhang, L.D. Kuhn, M.P.J. Fromherz, "Improvements on Ant Routing for Sensor Networks", M. Dorigo et al.(Eds.), ANTS 2004, LNCS 3172, pp. 289-313, 2004.
36. [36] C. Perkins, and E. Royer, "Ad-hoc on-demand distance vector routing", 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999. Proceedings, pp 90-100 , 25-26 Feb 1999.
37. [37] Dr.V.Raghunatha Reddy , A.Rajasekhar Reddy, "Lifetime Improvement of WSN by Trust Level based Ant Colony Optimization", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6497-6501.
38. [38] Y. Deepika, Dr V. Raghunatha Reddy, "Trust and Fitness based Lifetime Enhancement of Wireless Sensor Networks", *Journal of Xidian University*, Vol 15, Issue 10, 2021 pp. 451-460

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.