Energy Efficient Location-Based Trust, and Key Management for Sensor Networks based on Advanced Hybrid Multi-Level Clustering Ant Colony Optimisation Algorithm

S. Sudha Mercy[1], J.M. Mathana[2], J.S. Leena Jasmine[3]

[1]Jeppiaar Institute of Technology, Tamilnadu, India
(e-mail:sudhamercy.phd@gmail.com)
[2]St Peter's Institute of Higher Education and Research, Tamilnadu, India
(e-mail:jm.mathana@gmail.com)
[3]Velammal Engineering College, Tamilnadu, India
(e-mail:leenavictorece@gmail.com)

Abstract: Wireless Sensor Networks (WSN) has been extensively used due to its numerous uses such as object detection, biomedical health surveillance, natural disaster relief, environmental surveillance, and video surveillance. However, the vulnerability to protection contributes to increased electricity use and higher transmission costs. On the other hand, energy efficiency is a vital consideration because of the energy resource limitation of storages in sensor nodes. This research therefore introduces the Enhanced Energy-Efficient Location-based Key Management Optimisation (EEELKO) Protocol. The research's involvement consists of three main stages. The first is to establish an effective grouping protocol with high confidence values for the chosen nodes, using fuzzy based trust management. A secure data validation based on confidence and distance-specific management is then applied to the Elliptical Curve Logic Discrete Secure Algorithm (ECLDSA). Safe routing together with increased energy performance is facilitated with key and trust management, energy and position parameters implemented in the optimisation algorithm. The quality parameters such as packet distribution ratio, energy efficiency, and performance and end-to-end delays are used for validation of the data. The proposed approach was implemented in MATLAB software. The obtained solution achieves a greater throughput and delivery ratio with lower energy consumption. It also increases the reliability and the performance when compared to conventional methods.

Keywords: Wireless Sensor Network, optimisation technique, Energy efficiency, Key Management, Data protection, Network lifetime

1. INTRODUCTION

At the present scenario, WSNs have been applied for different applications such as natural disaster relief, environment monitoring, biomedical health monitoring, Border target tracing and investigation, real-time monitoring, seismic sensing, and investigation of the hazardous environment (Ahlawat and Dave, 2018; Arora et al., 2016; Chien-Chung Shen et al., 2001; Liao et al., 2011). By the way of growing acclamation of WSNs and varied application, most of the researchers have suggested effective approaches for increasing the network lifetime and attaining optimal results. In addition, due to limitations of the storage capacity in batteries, in WSN, the energy effectiveness will be a crucial factor (Ramluckun and Bassoo, 2018). Subsequently, the WSNs consist of different sensor nodes that are linked together as well as to a base station (BS). It also consists processing of data, sensing of data via sensor nodes and transmitted to the BS. In the hazardous environment, the reinstallation and charging of sensor nodes are difficult and, in a few cases, not possible. Due to this, energy conservation is a challenging issue (Kaur and Mahajan, 2018; Yanlong Li et al., 2013).

From the review of the literature, it is found that the key management technique can be an effective solution to build the security of WSNs (Al Ameen et al., 2012; Attoungble and Okada, 2011). However, the resources in WSNs are very less (For instance, small storage space, less node computing power and weaker interaction capability). In addition, the node deployment is not an easy task for the different environment, which includes varied network configuration, ease of control and huge network scale. But conventional key management approaches cannot be directly applied in WSNs. So, it is necessary to focus on efficient key management approach for attaining low energy consumption, highly secure and reliable communication (Brar et al., 2016; Gao et al., 2018; Martins and Guyennet, 2011; Prasad et al., 2011; Qiu et al., 2016). Hence, a novel approach that is based on Enhanced Energy Efficient Location-based Key Management Optimisation (EEELKO) protocol is proposed in the paper. This section has given a brief introduction to wireless sensor networks and security issues in the network. The next section reviews the existing literature on the optimisation approaches, and key management in WSN, and identifies a research gap. The third section has framed a detailed methodology to implement the proposed idea. The system model description and the performance metrics are also discussed in the same section. The section following that discusses the implemented results and compares its performance metrics with the existing studies. The final section examines the results and gives a conclusion for the manuscript.

2. LITERATURE REVIEW

There are plenty of research conducted for enhancing the energy effectiveness of the WSN along with the lifetime of the network using various approaches involving trust and key management, and clustering.

A study by Xu (Xu, 2006) and Weck (Jourdan and de Weck, 2005) discussed the node implementation approach with the help of a genetic set of rules in an obstacle intrusion background. But the suggested approach does not consider the location of the sink node in the network. Similarly, Aziz et al. (Aziz et al., 2010)has proposed particle swarm optimisation technique on the basis of node deployment strategy by considering mobile nodes towards attaining optimal results of coverage and energy consumption. However, it has limited node movements by node energy. Few of the researchers have recommended that Ant Colony Optimisation (ACO) approach solves WSN problems like cross-layer (Gajjar et al., 2016), mobile sink path selection (Kumar et al., 2018; Zhong and Zhang, 2012), routing (Gajjar et al., 2016; X. Liu, 2017), , mobile sink path selection (Kumar et al., 2018; Zhong and Zhang, 2012) and coverage (Lin et al., 2012).

Research by Liu and Cui (W. Liu and Cui, 2009) suggested a grid network-based nodes deployment approach using ACO, that can be utilized for the normal target positioning, and whereas parameters impact its execution, yet the arrangement got by running calculation isn't really ideal. A study by Liu (X. Liu, 2012) suggested a grid nodes deployment approach via improved ACO approach; however, it has poor stability (Sun et al., 2015). For this purpose, Chang and Shen (Chang and Shen, 2016) applied tree construction based energy-efficient scheme for reducing the data transmission distance. In our study, we have collected the information via the root node by visiting the mobile sink. In this approach, sensor hubs close to the root has been expired because of the hotspot issue. Also, it suffers a higher deferral of mobile sink since it doesn't think about the space while gathering the information. Similarly, research by Miao et al. (Miao et al., 2018) reduced the latency of data gathering through a mobile sink in multi-hop communication. They considered only on sensor along with a similar data rate since not considered the non-uniform data rate (Kumar et al., 2018). Optimizing the energy that is wasted during transmission will boost the lifetime of the system with every single layer. The process is then simplified to separate the layers and boost the lifetime of the network (Ye and Mohamadian, 2014). CHS is selected without any added WCN using a hierarchy that consumes less power and has adaptive clustering. It also supports the multiple level clustering that is adaptive for WSNs that may be aware of its location or not (Yi et al., 2007). These WSNs have higher latency and scalability, which makes it compatible only for smaller networks. Another type of clustering known as EEMC (Energy Efficient Multilevel Clustering) also consumes less energy and has less latency for the WSN and forms multiple level clustering with reduced over-heading (Jin et al., 2008). However, the problem of channel overlapping has not been considered in the paper which regularly takes place in WSN. In this paper, CHs are chosen on the basis of the communication between every sensor and its neighbouring sensors. This communication takes place through three different ways and contains lots of remaining energy. Multiple level clustering is not supported in this algorithm, and only smaller distance has been considered for the transmission (Mann and Singh, 2017).

A novel clustering technique using fuzzy-logic system has been suggested in Hai et al. (Hai et al., 2017) to identify the optimum grouping structure of 3D-WSN on the basis of the life of the network and consumption of energy. The volume of clustering hierarchies connected to non-clustering ones and the number of rounds that have been clustered again have less energy efficiency when compared with other protocols. A novel routing protocol based on clustering through energy efficient secure routing has been created by Kumar et al. (Muthurajkumar et al., 2017). This technique has been used to solve the performance problem using security techniques and also for giving a routing path that is efficient to those who are using it. Hence, this algorithm is more suited for collecting data, routing and sensing to improve the ability of the network (Logambigai et al., 2018). Even though a lot of these algorithms have been proposed recently, there are still problems with the energy, especially with the way the clusters are selected. In order to solve these problems in selecting the cluster head and routing technique, a novel algorithm will be proposed in this paper that will be more energy efficient as compared to existing techniques.

3. METHODOLOGY

In this study, EEELKO protocol is proposed for enhancing the performance of energy efficiency. The contribution of the research is three-fold.

Initially, an effective grouping protocol is created with high confidence values for the chosen nodes, using fuzzy based trust management. A secure data validation based on confidence and distance-specific management is then applied to the ECLDSA. Safe routing together with increased energy performance is facilitated with key and trust management, energy and position parameters implemented in the optimisation algorithm.

3.1 System framework

Figure 1 displays the EEELKO protocol device design for the sensor networks, and the related flowchart as seen in Figure 2.

The proposed system combines the trust attribute, key management and the optimised route using ACO. The trust value was modified here on the basis of the optimisation approach. In addition, the Figure defines key generation, route estimation and packet drop.

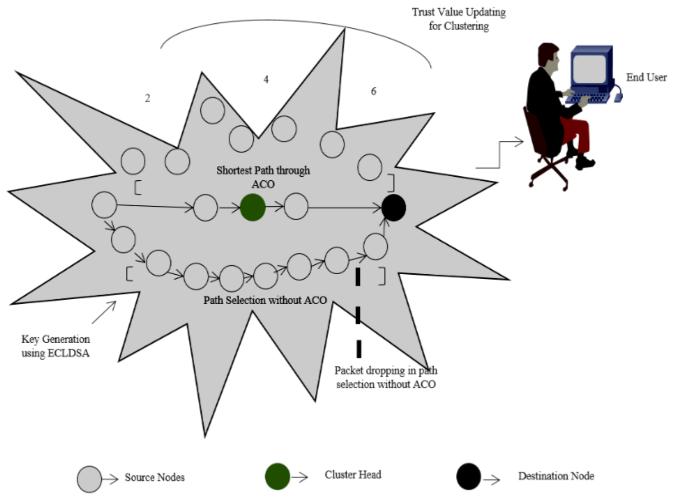

Fig. 1. The Architecture of Proposed Method.

The trust model helps to achieve an important, trustworthy path, leading to the right service node. It forms a clustering protocol on the basis of measured values, which decreases the node energy depletion. The encryption key for a given packet is often presented utilising the ECLDSA algorithm to safely transfer the packet. Finally, an optimisation method is used to send these packets to their target location in the shortest route in a safe manner.

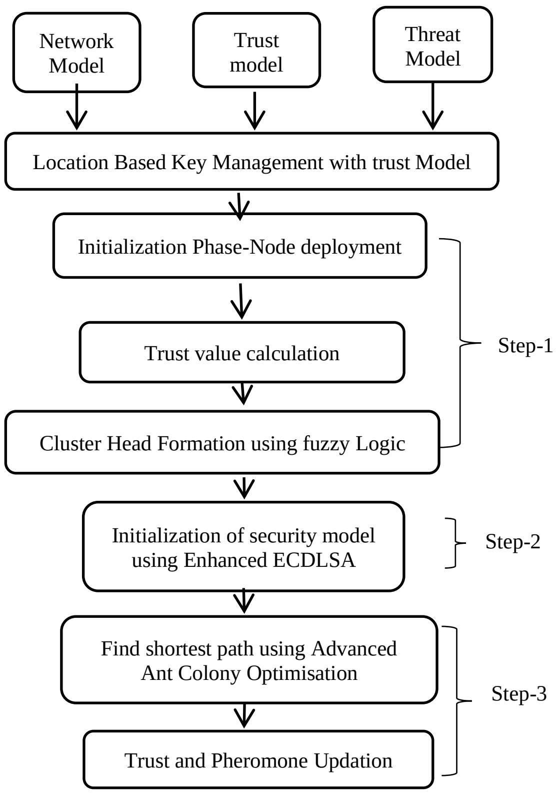

Fig. 2. Flowchart of EEELKO Protocol.

The proposed approach is classified into three segments. The first is to initialise the input parameters such as direction, threshold and trust value. Then each node's position and trust value is determined. The obtained values are integrated into the fuzzy logic system in order to generate dynamic rules for the creation of the clusters and selected cluster heads. Secure packet transmission is then allowed and the ECDSA framework offers protection against connection loss. Trust and key value are combined to ensure protected movement of data from source to destination using a hybrid optimisation technology. Trust, main, and pheromone value are revised at a regular interval to achieve three-tier protection.

There are various circumstances where the live span of WSNs need to be increased, particularly in larger applications and long term applications. This can be achieved by EEELKO protocol.

3.2 Trust Based CH selection using the Fuzzy Logic system

The sensor node position, the route parameters and threshold value of the whole node, energy and network power were considered in the initialization of the sensor node. The configuration of the cluster node path is performed to swap the node data and the linkages between the nodes are established. Moreover, the trust value was created on the basis of a parameters like node energy, threshold or initial trust, trust position and frequency of the most frequently visited packages in a given sensor node. It is necessary to identify the transmission route from the origin to the destination with the minimum possible distance. This route transfer must consider both time and energy. The parameter specifications are chosen based on the distance between the nodes of the network. Also, an iterative optimisation approach for multiple variables and sensor location is calculated from the expression

$$S = [s_{ij}]n \times 2 \tag{1}$$

It represents the actual position (S) of the data between the two sensors represented by i and j.

$$d_{ij}(x) = \left(\sum_{(m=1)}^{n} (s_{ia} - s_{ja})^2 \right)^{\frac{1}{2}} \tag{2}$$

The direct trust in-between these nodes may be calculated using the probability equation as shown in the equation,

$$Q_{i,j}(t) = \frac{|p_{i,j}(t) - \Delta p(t)|}{p_{i,j}(t)} \tag{3}$$

$$Q_{i,j}(t) = \frac{|p_{i,j}(t) - \Delta p(t)|}{p_{i,j}(t)} \tag{4}$$

$$R_{i,j}(t) = \exp[-b\,[n_i(t) - n_j(t)]^2] \tag{5}$$

$p_{i,j}(t)$–Volume of output data with respect to time

$P_{p_{i,j}}(t)$–Volume of data repetitiveness

$\Delta p(t)$- Volume of dynamic reference value

$R_{i,j}(t)$- Data similarity (correlation),

$n_i(t)$and $n_j(t)$ - output monitoring value,

a and b - comparison coefficient.

The representation of weights are given below:

$$W = \{w_P, w_Q, w_R\}^T \tag{6}$$

Hence, the direct trust of the sensor nodes after trade-off is

$$D' = DW$$

The algorithm for EEELKO protocol is given as supplementary document.

Initially, there is no communication of data between the nodes. Hence the initial value is $D' = \{0, 0, 1\}$ and the nodes would perform the update of D' in accordance with WSNs update cycle Δt. It is then assumed that the finally obtained trust value is final and largest value. Also, the value with higher time interval has lesser effect on the current value. The time weakening function is represented by,

$$x(k) = \begin{cases} x(k-1) - \frac{1}{n}, & 1 \leq k < n \\ 1, & k = n \end{cases} \tag{7}$$

The design equations of the connected nodes can be grouped to identify the trust value as shown in equation 8.

$$D'_{i,j}(t_{n+1}) = \frac{D'_{i,j}(t_{n+1}) + x(n)D'_{i,j}(t_n)}{2} \tag{8}$$

The time diminishing function x(k) makes sure that the estimation trust value is continued. Additionally, the previous cycle's trust value is modified appropriately, which also maintains the time efficiency of the trust value to a certain extent. This trust value can be estimated using the expression in equation 9.

$$I_{i,j}(t) = \frac{\sum D''_{i,k}(t) D''_{k,j}(t)}{\sum D''_{i,k}(t)} \tag{9}$$

Here, I denote the indirect trust value between the two adjacent nodes. Also, j and k are continuous nodes. Hence, using equation 8, the indirect trust value with respect to time can be computed. Finally, the combined trust value is computed. It is assumed that one entity has the ability to calculate the trust of the other entities. The comprehensive trust value for an entity E can be represented by

$$\phi_{i,j}(t) = \sigma D''_{i,j} + \frac{1}{n} \sum I_{i,j} \tag{10}$$

Here, σ represents the weighted value of the amount of direct trust. From this, the weighted values of the other trust are1-σ. Hence, the combined trust degrees Ω can be represented by $\sigma D + (1-\sigma) I$. Also, n is the volume of the entity nodes and ϕ is group of continuous nodes. Hence, the highest energy and trust level is selected as the cluster head.

3.3 Secure shortest path calculation using ECLDSA and Advanced ACO

An Elliptical Curve Cryptography (ECC) method has been used to render a stable routing from origin to destination. Using the above steps, the trust values were created and the Q' value was selected, that lies between the WSNs because it depends on trust. kP is computed, which provides two points in space and is depicted in graphical coordinates as two points, which are the base points xR and yR co-ordinates. The public key 'k' is produced and validated, and its value is wholly reliant on the trust value produced at the initial step. This k is assured of publicly validated by the certification body and that it is created from the trustworthy framework. The primary requirement is that its value would be placed in the elliptical curve. If the values do not appear on the curve, then the node is skipped and searched again. Also, m is the binary field extension, and xor operation is carried out between the bit's m and k using a 160-Bit hash function Secure Hash Algorithm - 1 (SHA-1). The convolution operation is carried out to produce a private key. If the key is not matched, authentication is prevented or limited to delete unauthorised entry, for access to the particular node.

$$e = sha - 1(m \oplus k), \tag{11}$$

$$s = d(k_R - e) * modQ \tag{12}$$

When the trust value approaches the original threshold value, the zones are chosen for the shortest path to be determined by initialising the parameters of ACO. The nodes are released sufficiently from the entire sensor nodes; the node then adjusts its value to all the other nodes in a manner that adjusts the value to all the other nodes. This pheromone importance is dependent on protection permit criteria, routing parameters such as the direction of the cluster head and the trust value. Once the shortest path is identified, other pathways can search for identification of the shortest path along with this trust value and the authority selected. The permission for any node relies on the created trust value. At first a security algorithm is used to produce a key and if this key agreement suits a trust attribute, a further double check is carried out for security, such as the inspection of the table and source as well as the destination node. When this is completed, the location of the nodes or the verifying technique will be validated and correspondence will be rendered if any of the above conditions are fulfilled, and the pheromone is continuously tested to ensure effective energy delivery and security for three stages. For the ant colony optimisation, the route with the least distance is obtained using equations 15 and 16. Here, P and T represents the node's pheromone and trust value, while d_i is the distance between the nodes. Based on the obtained pheromone value, the selected node is sent to the CH, which allots the trust value to the selected node.

$$P = TrustManagement + KeyManagement \tag{13}$$

$$TrustValueT = 1 - \left(\frac{d_i}{\sum d_i}\right) \times 100 \tag{14}$$

$$\begin{aligned} KeyManagement = e = sha - 1\left(m \bigoplus k\right), s \\ = d(k_R - e) * modQ \end{aligned} \tag{15}$$

P = T + e

3.4 Performance evaluation metric

In this research, the effectiveness of the proposed approach is measured based on different parameters like the delay, throughput and the delivery ratio.

3.4.1 Average end-to-end delay

This value is calculated from the origin to the end node through all the nodes in between, hence known as end to end delay. It combines different delays together to form the total delay. These different delays include transmission delay, time for route identification, and queuing in the network (Sharma and Patheja, 2002).

3.4.2 Average Throughput

The throughout is the volume of data received at the destination within a specific span of time. When calculated for all the data, the mean of the throughput is known as average throughput. It is defined as the overall packets within the period of transmission. As shown in equation 16 (Behera and Panigrahi, 2015).

$$T = \frac{\text{Totalnumberofreceivingpacketsfromnode}}{\text{Datatransmissionperiod}} * 8 \qquad (16)$$

3.4.3 Packet Delivery Ratio (PDR)

The ratio between the total packets send and received is known as packet delivery ratio. It is required to compute the stability of the route. When the number of packets transferred is high, it is necessary to ensure that the PDR is high to avoid more packet losses. Hence, a higher PDR represents better network (Baisakh, 2013).

$$TPDR = \frac{\sum \text{number of packets sent received}}{\sum \text{ number of packets send}} \qquad (17)$$

3.4.4 Average Energy Consumption

The average amount of energy used by individual nodes during the transfer from the origin to the end node is known as Average Energy Consumption. It unit is Joule.

$$AEC = \frac{\text{Total energy consumed}}{\text{Total no.of available nodes}} \qquad (18)$$

4. RESULTS AND DISCUSSION

The proposed EEELKO approach is implemented through Network Simulator -2 simulation software. It is a well-known simulator that can be utilised for a variety of protocols for multiple layers. Figure 3 depicts the proposed simulation model with a virtual area of 10,000 m2. This is performed using Ad-hoc based routing protocol and considering the performance parameters like the PDR, AEC, overheads, throughputs, delays, and network lifetime. These parameters used for designing the nodes are shown in Table 1.

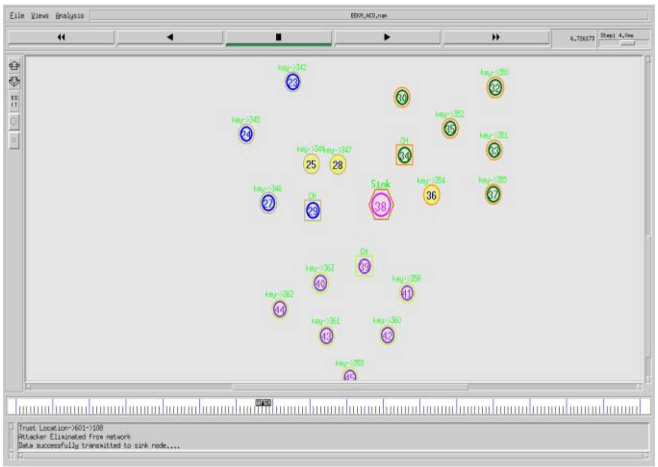

Fig. 3. Simulation model of EEELKO.

Table 1. Simulation Parameters.

Parameters	**Values**
Number of nodes	23
Network size	100 × 100 m2
Node placement	Random
Node mobility	Mobility
MAC layer protocol	IEEE 802.11
Routing protocol	DSDV
Dimension of Topography(x,y)	959,1040
Queue Type	Drop tail
Bandwidth	12MB
Initial Energy	20.0
Time simulation	17s
Antenna	Antenna/Omni Antenna

More packets can be expected to be received at the end station by providing security through the ECLDSA algorithm. Due to this security procedure, there would not be any unauthorised nodes and attacks between the links. Therefore, more packets have been received in this algorithm to achieve the higher throughput. It therefore has the highest PDR as shown in Figure 4.

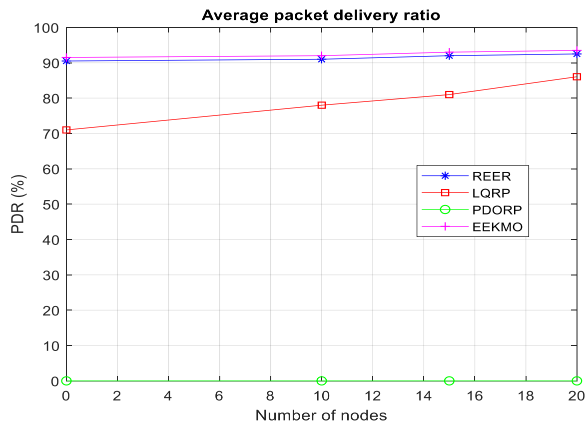

Fig. 4. Packet Delivery Ratio.

The end to end delay differs depending on how a network device is applied and operated. ACO has been integrated, and is used to optimise the packet transport to reach the end node as fast as possible. Any node has easily forwarded packets to the base station. The proposed approach has greatly reduced the delay. Figure 5 indicates that in comparison to existing strategies, the planned approach has lesser delays.

The energy efficiency of the network must be measured such that less energy is needed to transfer the packets from the origin to the end node. The collection and optimisation algorithm for shortest distance energy is exploited efficiently from the fuzzy-based cluster scenario that saves the energy across all nodes. From Figure 6, it can be seen that in comparison to other existing techniques, the proposed approach has used fewer resources.

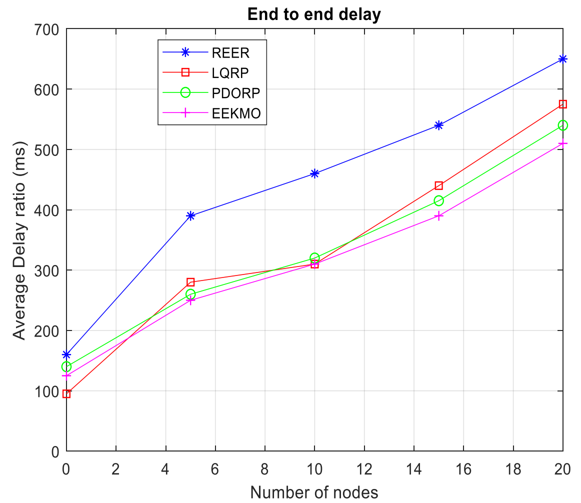

Fig. 5. End-to-End Delay of Data Packets.

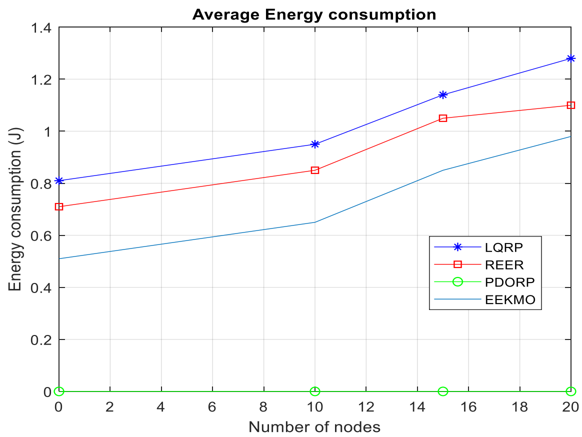

Fig. 6. Energy efficiency.

Due to the ECLDSA algorithm, most of the packets successfully reach the end node. Figure 7 shows the proposed approach is able to achieve a high throughput of 659 kbps.

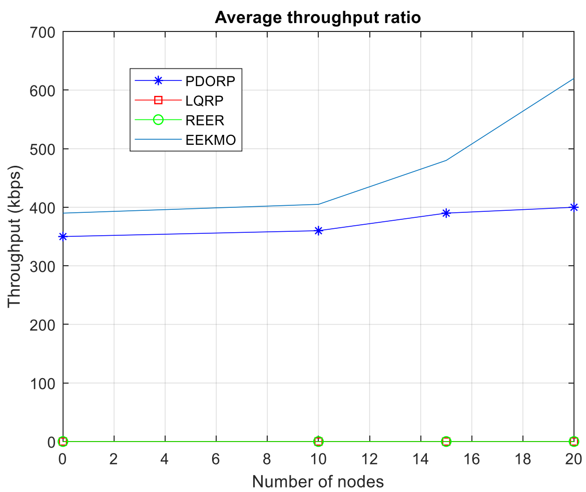

Fig. 7. Throughput.

The performance of the proposed EEELKO approach is compared with existing approaches in terms of delay, PDR, throughout, and energy consumption in table 2.

Table 2. State of Art Performance Comparison.

S. No	Parameters	PDORP(Brar et al., 2016)	LQRP(Priya et al., 2017)	REER (Yahya & Ben-Othman, 2009)	EEELKO (Proposed)
1	Energy consumption (J)	-	1.1	1.31	0.95
2	End-to-end delay (ms)	590	650	700	565
3	Packet Delivery Ratio (%)	-	78	93	99
4	Throughput (kbps)	410	-	-	688

The approach is compared with Robust and energy-efficient multipath routing protocol (REER) (Yahya and Ben-Othman, 2009), Prevailing-Directional Transmission-based energy-aware Routing Protocol (PDORP) (Brar et al., 2016), and Link Stability Based Routing Protocol (LQRP) (Priya et al., 2017), methods. The proposed EEELKO protocol has consumed lesser energy of 0.95J. Similarly, a higher PDR and throughput of 99% and 588kbps has been achieved which is higher than the other three compared algorithms. The end to end delay is 565 ms, which is lesser than the existing techniques. Hence, the overall results show the proposed EEELKO approach has a superior performance.

5. CONCLUSION

In this research, the proposed EEELKO protocol is implemented for improving the network security and energy efficiency of the system. The approach has been implemented in three stages. Initially, a fuzzy based rule with trust management is offered to identify the most efficient clustering protocol. After this, ECLDSA approach is applied to improve the security and authenticate it better. Finally, the ant colony optimisation approach is implemented for transmitting the packets through the shortest available path. While, this depends on the location based ACO. The value of the pheromone is computed through the node location. Hence, a high PDR can be achieved rapidly, which also decreases the delay and increases the energy efficiency.

Using a cluster system, an effective routing through cluster head nodes can be accomplished in WSN for increased energy efficiency. In addition, fuzzy rules have been implemented with respect to energy analysis, node deployment, cluster formation and cluster head selection. High energy conservation and the durability of the network are the key relevance of the proposed process. The simulation results indicate that the current solution, focused on network durability and energy consumption, is more effective than previous work. It has also lowered the delay and reduced electricity consumption.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

CONFLICT OF INTEREST

No potential competing interest was reported by the authors.

REFERENCES

Ahlawat, P., & Dave, M. (2018). An attack model based highly secure key management scheme for wireless sensor networks. *Procedia Computer Science*, *125*, 201–207. https://doi.org/10.1016/j.procs.2017.12.028

Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, *36*(1), 93–101. https://link.springer.com/article/10.1007%252Fs10916-010-9449-4

Arora, K. V., Vishal, S., & Monika, S. (2016). A survey on LEACH and other's routing protocols in wireless sensor network. *Optik-Int J Light Electron*, *127*(16), 6590–600. http://sci-hub.tw/10.1016/j.eij.2018.01.002

Attoungble, K. J. M., & Okada, K. (2011). Localization with ratio-distance (LRD) for distributed and accurate localization in wireless sensor networks. *IEICE Transactions on Communications*, *E94-B*(7), 1944–1951. https://doi.org/10.1587/transcom.E94.B.1944

Aziz, N. A. A., Mohemmed, A. W., & Zhang, M. (2010). Particle swarm optimization for coverage maximization and energy conservation in wireless Sensor Networks. In *Applications of Evolutionary Computation Lecture Notes in Computer Science* (pp. 51–60). Springer. https://doi.org/10.1007/978-3-642-12242-2_6

Baisakh, B. (2013). A review of energy efficient dynamic source routing protocol for mobile ad hoc networks. *International Journal of Computer Applications*, *68*(20), 6–15. https://doi.org/10.5120/11693-3603

Behera, A., & Panigrahi, A. (2015). Determining the network throughput and flow rate using GSR and AAL2R. *International Journal of UbiComp*, *6*(3), 09–18. https://doi.org/10.5121/iju.2015.6302

Brar, G. S., Rani, S., Chopra, V., Malhotra, R., Song, H., & Ahmed, S. H. (2016). Energy efficient direction-based PDORP routing protocol for WSN. *IEEE Access*, *4*, 3182–3194. https://doi.org/10.1109/ACCESS.2016.2576475

Chang, J.-Y., & Shen, T.-H. (2016). An efficient tree-based power saving scheme for wireless sensor networks with mobile sink. *IEEE Sensors Journal*, *16*(20), 7545–7557. https://doi.org/10.1109/JSEN.2016.2601327

Chien-Chung Shen, Srisathapornphat, C., & Jaikaeo, C. (2001). Sensor information networking architecture and applications. *IEEE Personal Communications*, *8*(4), 52–59. https://doi.org/10.1109/98.944004

Gajjar, S., Sarkar, M., & Dasgupta, K. (2016). FAMACROW: Fuzzy and ant colony optimization based combined mac, routing, and unequal clustering cross-layer protocol for wireless sensor networks. *Applied Soft Computing*, *43*, 235–247. https://doi.org/10.1016/j.asoc.2016.02.019

Gao, Y., Ao, H., Feng, Z., Zhou, W., Hu, S., & Tang, W. (2018). Mobile Network Security and Privacy in WSN. *Procedia Computer Science*, *129*, 324–330. https://doi.org/10.1016/j.procs.2018.03.083

Hai, D. T., Son, L. H., & Vinh, T. Le. (2017). Novel fuzzy clustering scheme for 3D wireless sensor networks. *Applied Soft Computing*, *54*, 141–149. https://doi.org/10.1016/j.asoc.2017.01.021

Jin, Y., Wang, L., Kim, Y., & Yang, X. (2008). EEMC: An energy-efficient multi-level clustering algorithm for large-scale wireless sensor networks. *Computer Networks*, *52*(3), 542–562. https://doi.org/10.1016/j.comnet.2007.10.005

Jourdan, D. B., & de Weck, O. L. (2005). Layout optimization for a wireless sensor network using a multi-objective genetic algorithm. *2004 IEEE 59th Vehicular Technology Conference. VTC 2004-Spring (IEEE Cat. No.04CH37514)*, *5*, 2466–2470. https://doi.org/10.1109/VETECS.2004.1391366

Kaur, S., & Mahajan, R. (2018). Hybrid meta-heuristic optimization based energy efficient protocol for wireless sensor networks. *Egyptian Informatics Journal*. https://doi.org/10.1016/j.eij.2018.01.002

Kumar, D. P., Amgoth, T., & Annavarapu, C. S. R. (2018). ACO-based mobile sink path determination for wireless sensor networks under non-uniform data constraints. *Applied Soft Computing*, *69*, 528–540. https://doi.org/10.1016/j.asoc.2018.05.008

Liao, W.-H., Kao, Y., & Wu, R.-T. (2011). Ant colony optimization based sensor deployment protocol for wireless sensor networks. *Expert Systems with Applications*, *38*(6), 6599–6605. https://doi.org/10.1016/j.eswa.2010.11.079

Lin, Y., Zhang, J., Chung, H. S.-H., Ip, W. H., Li, Y., & Shi, Y.-H. (2012). An ant colony optimization approach for maximizing the lifetime of heterogeneous wireless sensor networks. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *42*(3), 408–420. https://doi.org/10.1109/TSMCC.2011.2129570

Liu, W., & Cui, L. (2009). Ant based approach to the optimal deployment in wireless sensor networks. *Journal of Communication*, *30*(10). http://sci-hub.tw/10.1016/j.amc.2014.10.091

Liu, X. (2012). Sensor deployment of wireless sensor networks based on ant colony optimization with three classes of ant transitions. *IEEE Communications Letters*, *16*(10), 1604–1607. https://doi.org/10.1109/LCOMM.2012.090312.120977

Liu, X. (2017). Routing protocols based on ant colony optimization in wireless sensor networks: a survey. *IEEE Access*, *5*, 26303–26317. https://doi.org/10.1109/ACCESS.2017.2769663

Logambigai, R., Ganapathy, S., & Kannan, A. (2018). Energy–efficient grid–based routing algorithm using intelligent fuzzy rules for wireless sensor networks. *Computers & Electrical Engineering*, *68*, 62–75.

https://doi.org/10.1016/j.compeleceng.2018.03.036

Mann, P. S., & Singh, S. (2017). Energy efficient clustering protocol based on improved metaheuristic in wireless sensor networks. *Journal of Network and Computer Applications*, *83*, 40–52. https://doi.org/10.1016/j.jnca.2017.01.031

Martins, D., & Guyennet, H. (2011). Security in wireless sensor networks: a survey of attacks and countermeasures. *International Journal of Space-Based and Situated Computing*, *1*(3), 151–62. http://sci-hub.tw/10.1016/j.chaos.2016.02.025

Miao, Y., Sun, Z., Wang, N., Cao, Y., & Cruickshank, H. (2018). Time Efficient Data Collection With Mobile Sink And vMIMO technique in wireless sensor networks. *IEEE Systems Journal*, *12*(1), 639–647. https://doi.org/10.1109/JSYST.2016.2597166

Muthurajkumar, S., Ganapathy, S., Vijayalakshmi, M., & Kannan, A. (2017). An intelligent secured and energy-efficient routing algorithm for MANETs. *Wireless Personal Communications*, *96*(2), 1753–69. http://sci-hub.tw/10.1016/j.compeleceng.2018.03.036

Prasad, X., Gupta, M., & Patel, R. (2011). A reliable security model irrespective of energy constraintsin wireless sensor networks. *International Journal of Advanced Computer Science and Applications*, *2*(4), 20–9. http://sci-hub.tw/10.1016/j.chaos.2016.02.025

Priya, D., Haripriya, & Kulothungan. (2017). An energy efficient link stability based routing scheme for wireless sensor networks. *2017 International Conference on Communication and Signal Processing (ICCSP)*, 1828–1832. https://doi.org/10.1109/ICCSP.2017.8286711

Qiu, B., Chen, X., & Wu, Q. (2016). A key design to prolong lifetime of wireless sensor network. *Chaos, Solitons & Fractals*, *89*, 491–496. https://doi.org/10.1016/j.chaos.2016.02.025

Ramluckun, N., & Bassoo, V. (2018). Energy-efficient chain-cluster based intelligent routing technique for Wireless Sensor Networks. *Applied Computing and Informatics*. https://doi.org/10.1016/j.aci.2018.02.004

Sharma, S., & Patheja, P. S. (2002). Improving AODV routing protocol with priority and power efficiency in mobile Ad hoc WiMAX network. *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, *2*(1), 87–93.

Sun, X., Zhang, Y., Ren, X., & Chen, K. (2015). Optimization deployment of wireless sensor networks based on culture–ant colony algorithm. *Applied Mathematics and Computation*, *250*, 58–70. https://doi.org/10.1016/j.amc.2014.10.091

Xu, Y. X. (2006). AGA approach to the optimal placement of sensors in wireless sensor networks with obstacles and preferences. *IEEE Conference on Consumer Communications and Networking*, 127–131. http://sci-hub.tw/10.1016/j.amc.2014.10.091

Yahya, B., & Ben-Othman, J. (2009). REER: robust and energy efficient multipath routing protocol for wireless sensor networks. *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, 1–7. https://doi.org/10.1109/GLOCOM.2009.5425587

Yanlong Li, Junyi Wang, Yuqing Qu, Mei Wang, & Hongbing Qiu. (2013). A new energy-efficient transmission scheme based ant colony algorithm for wireless sensor networks. *2013 8th International Conference on Communications and Networking in China (CHINACOM)*, 473–478. https://doi.org/10.1109/ChinaCom.2013.6694642

Ye, Z., & Mohamadian, H. (2014). Adaptive clustering based dynamic routing of wireless sensor networks via generalized ant colony optimization. *IERI Procedia*, *10*, 2–10. https://doi.org/10.1016/j.ieri.2014.09.063

Yi, S., Heo, J., Cho, Y., & Hong, J. (2007). PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks. *Computer Communications*, *30*(14–15), 2842–2852. https://doi.org/10.1016/j.comcom.2007.05.034

Zhong, J., & Zhang, J. (2012). Ant colony optimization algorithm for lifetime maximization in wireless sensor network with mobile sink. *Proceedings of the Fourteenth International Conference on Genetic and Evolutionary Computation Conference - GECCO ’12*, 1199. https://doi.org/10.1145/2330163.2330328