ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20240823001937
Original scientific paper

Improving IoT Network Longevity with Attack Repellent Energy (SARE) Algorithm for Energy-Efficient and Secure Routing

INDRA PANDIAN*, SHANTHI THIRUGNASAMBANTHAM, KARTHIKEYAN BALASUBRAMANIAM, KIRUBABURI RAVICHANDRAN

Abstract: The current IoT architecture necessitates energy-efficient and secure routing algorithms, particularly in wireless infrastructures where the risk of security issues is elevated. One of the significant challenges is the lack of precise knowledge about the residual energy of nodes, which leads to complications in the Cluster Head (CH) selection process. This research addresses the problem by proposing an attack-repellent algorithm that identifies potential CHs with accurate knowledge of residual energy, while minimizing computational overhead for security purposes. The proposed Secure Attack Repellent Energy (SARE) algorithm selects CHs based on the K-Nearest Neighbor (KNN) algorithm, which evaluates residual energy by considering the battery voltage attached to each node. This algorithm also incorporates key renewal and a secure key exchange mechanism to enhance security, with frequent link key exchanges bolstering the network's robustness against attacks. SARE algorithm introduces a novel method for CH selection that reduces the likelihood of incorrect selections due to imprecise energy information, thereby extending the network's operational lifespan. In addition to energy efficiency, the algorithm emphasizes security by frequently updating encryption keys to guard against potential breaches, ensuring that even if a key is compromised, the damage is limited to a short timeframe. To demonstrate its effectiveness, the SARE algorithm is compared with the Low Energy Adaptive Clustering Hierarchical routing (LEACH) and TSRF algorithms. Results show that the SARE algorithm significantly outperforms these existing protocols. The SARE algorithm extends the network's lifetime by 1.15 times longer than the classical LEACH protocol and improves network throughput by 1.42 times compared to the LEACH routing protocol. Additionally, the SARE algorithm effectively mitigates HOTSPOT and Energy Hole issues, which are common problems in wireless sensor networks.

Keywords: cluster head selection; energy-efficient routing; IoT architecture; secure routing algorithms; wireless sensor networks

1 INTRODUCTION

New Wireless protocols have resulted in increased IoT architecture and more advanced growth in the area of manufacturing, Industries, power sector, Health industries and geriatric care. The Wireless hybrid network serves to be the important protocol to sophisticate one's lifestyle inside the smart home environment. The recent smart city projects across the globe have brought new situations and challenges to the researchers in providing potential solution to energy and security issues in the architecture [1-4]. The Energy based attacks and loss of network connectivity due to compromised security aspects create major chaos in the smart environments. These networks are battery powered and with minimal attack mitigation options; these network objects are exposed to third parties for data sharing and resource sharing in some occasions. Wireless sensor node consists of battery (i.e) power unit, process unit, sensor unit and power generation unit. The sensor unit senses the data and preprocess as per the network requirement. The data is turned to packet and transmitted to sink through routing protocols. The routing protocols mainly influence the network lifetime.

The network lifetime is mainly determined by the CH selection. The node in hybrid network has reduced memory, power and transmission capability (i.e.) resource starving in nature. Providing better security and giving a light weight security algorithm to sensor nodes are still challenging issues to the hybrid wireless IoT environment. Node heterogeneity in the network can have variation in the energy level, Transmission capacity, microprocessor, computational capability etc.. The WSN has a numerous tiny embedded processing machines which share data and work towards single objective. The necessary security has to be given properly without sacrificing the energy to the major extent in the network. Wireless Sensor Networks (WSN) have potential applications like live monitoring of battle field events, avalanche breakdown events in ice mounts, agricultural monitoring in many occasions. The sensor units connected with the sensor nodes may vary in smart environment [5-8]. Some of the nodes will be connected with low power sensor devices; however the high power sensor nodes may be equipped with sensors like camera, vibrators in some cases actuators as well. Fig. 1 illustrates the typical Wireless Hybrid architecture with key exchange mechanism.

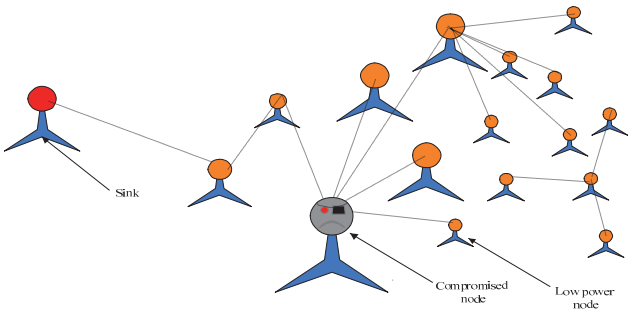

Figure 1 Hybrid wireless architecture for IoT environment

The key sharing methodology should be unique and robust so that the compromised node should not provide gap to attack the network [9-11]. The key sharing methodology proposed in this work is novel and changes based on time, which makes the network more robust and hack proof in nature. In response to the escalating challenges faced by resource-constrained IoT devices, the proposed Secure Attack-Proof Routing Algorithm (SARE) emerges as a promising solution, aiming to simultaneously address the pressing issues of energy efficiency and security within the dynamic and diverse IoT landscape. The existing protocols, including TSRF and LEACH, have demonstrated limitations in offering a comprehensive remedy to the energy scarcity and security vulnerabilities that characterize IoT networks. The objective of this research is to develop a new energy-efficient and secure routing algorithm for heterogeneous IoT environments. The research aims to achieve this by:

Improving CH selection: By using the KNN algorithm and considering battery voltage, the research aims to identify CHs with more accurate residual energy information.

Enhancing security: The proposed SARE algorithm incorporates key renewal and secure key exchange mechanisms to improve the network's resistance against attacks.

Extending network lifetime: By selecting energy-efficient CHs and implementing security measures, the research aims to prolong the overall lifespan of the IoT network.

2 RELATED WORKS

Many researchers have evolved in the recent years after the era of Industry 4.0 on wireless routing protocols. Single path routing algorithms mainly concentrate on energy, link stability and delay [12]. The link quality is measured using the receiver signal strength indicator metrics and energy is mainly indicated with the battery level voltages and expenditure formulae. The link scheduling is also the main concern in providing quality of service in the network lifetime enhancement. The Heterogeneous-Energy and Traffic-Aware Sleep-Awake Cluster-Based protocol provided a solution with column generation method to joint routing and scheduling problem [13]. Clustering is an efficient solution for large level sensor networks. LEACH routing algorithm is a widely used basic clustering approach for wireless hybrid routing algorithm [14]. The Cluster Head (CH) selection process is periodically revised on probability approach to select CH for corresponding clusters. The random number generator is primarily used to make probability based decision making. The TSRF routing protocol provides solution to the clustering problem with residual energy in the battery and frequent key revision improves the network security aspects and energy efficiency. The algorithm Traffic and Energy Aware routing protocol in [15] works on random energy heterogeneous traffic environment. The TEAR does not select low energy and high traffic nodes as CH role. TEAR has the capability to reduce the drop packets and provide better routing path. However the redundant packet transmissions are not concentrated, which is also a primary concern in improving the network lifetime. The Sleep-awake energy efficient distribution (SEED) algorithm utilizes duty cycling mechanism to avoid redundant data communication [16]. It has the disadvantages of idle listening, since its radio is in sleep state for maximum duration. More concentration on increasing the network lifetime could result in reduced throughput to the network. The algorithm SEED utilizes time division multiplexing mode scheduling on cluster members leading more idle hearing problem in the network. The present routing protocols compute the path cost using link costs; this lossless mechanism misuses the spatial spectrum reusability in wireless media. FSFT [17] algorithm provides improved sensor network lifetime on considering network residual battery and voltage level. The voltage value can be used as a better indicator for judging the present left over energy level of the node. The voltage level (V) in the node decreases exponentially and is drastically reduced after a threshold value. The battery recovery based lifetime enhancement (BRLE) [18] approach utilizes the node idle time to use as battery recovery time. The discontinuous discharge of the battery can be able to improve the network lifetime and to aid the battery health condition to the suitable extent. The CH selection is based on the residual energy, battery recovery rate and Markov approach. The Markov model is a memory less module capable to give better selection based on the present state of the battery level [19-23].

The above algorithm provides better decision making on improving the network lifetime and provides better solution as well. However the algorithm key rotation scheme was not specific and not an auspicious solution to existing security problems in the heterogeneous environment. The proposed work provides a better solution by selecting CH based on the remaining residual energy through Voltage indication and frequently changing the network key with EX-OR methodology. The operation is more efficient in that it reduces the frequent key sharing and also provides keen security to the network. Hybrid encryption is a new concept that can be utilized in the Internet of Things. This method of encryption provides high security while requiring less processing power. In order to mitigate security risks while increasing encryption speed and reducing computational complexity, Hybrid security algorithms are used. Information integrity, confidentiality, and non-repudiation in data sharing for IoT are the goals of this hybrid method [24-27].

3 PROPOSED WORK

The nodes in present IoT environment are resource starving and heterogeneous in nature. The traditional key sharing and security algorithm depletes its energy soon and makes the network more prone to security attacks. The present IoT nodes and network do not support traditional high density algorithm and require new light weight key sharing and CH selection algorithm to repel security attacks and prolong the network lifetime. The LEACH and TSRF algorithm lacks in security aspects and repeated CH election process, which in-turn depletes the energy. The proposed algorithm is designed to have more knowledge on resources available to tackle energy related attacks in the network. Information exchange with single key makes the network prone to attackers and deciphering of key is quite easy. Different key exchange strategy consumes additional energy consumption sacrificing energy and increases the computational load to the network. The incorporation of key renewal and secure key exchange mechanisms in the SARE algorithm does provide a strong layer of security to Wireless Sensor Networks (WSNs). These mechanisms, through the exchange of link keys, make the network very secure in case of an attack because even if the key is compromised, the network is protected. This dynamic approach reduces the vulnerability window so that the nodes can communicate securely while at the same time conserving energy. Consequently, SARE provides an efficient solution to security and lifetime issues in resource-scarce IoT applications.

SARE Algorithm.

Input: Voltage (V), Residual energy status (E_r), Distance to sink (dist).

Output: CH selection (P_{CH})

Begin process:

Initial Cluster formation with election protocol,

for (E_r>threshold)

admit participants for election;

Cluster formation through *K* nearest neighbor approach for distance d_0;

Compute the internal distance and energy cost with radio model using voltage equation and security data key exchange protocol

While (E_r > threshold)

Opt the CH for cluster i and declare to all participants:

Approach XOR operation for key exchange and compute data load to the CH

Form layer and cluster with sink

start communication

End process

K nearest Neighbor algorithm

Data set to be loaded

Initialize K to the neighbor

Calc the distance between reference and current value

Sum the distance

Sort the array with smallest to largest with respect to distance

Pick the first K entries

Secure key exchange protocol

Fig. 2 illustrates the key sharing and key rotation procedure followed in the proposed work. The CH rotation is done after t seconds.

Generate n random secret key

Share the key with the present CHs, the CHs encrypts the data using ex-or operation

En = Sn Ex − OR Dn

the data is forwarded towards sink in multihop fashion, again encrypting with corresponding cluster key.

The base station decrypts with the corresponding key with n jump keys:

*Di = S*1 *Ex − OR S*2 *Ex − OR S*3 *Ex-OR - - - - En*

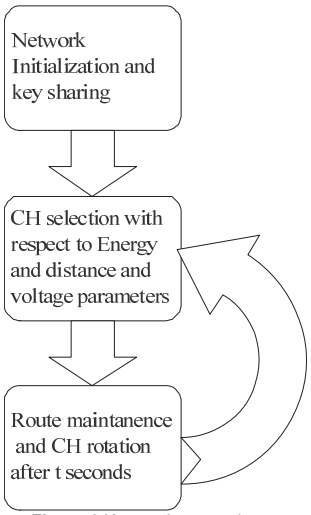

Figure 2 Key exchange scheme

Math Model:

Eq. (1) illustrates the cumulative distance between the CH candidates with respect to its clusters. The node having minimum distance d becomes the potential CH election candidate. The distance calculation is computed with the Eq. (1).

$$d = \sqrt{\left[\sum_{x=i+1}^{cs}\left(x_i - x_{i+1}\right)^2 + \sum_{y=y+1}^{cs}\left(y_i - y_{i+1}\right)^2\right]} \tag{1}$$

where *d* cumulative distance of nodes with Clusters, *x* position of *i*th node inside the Region of Interest, *y* position of *i*th node inside the Region of Interest.

The distance threshold for cluster ring size selection is calculated with the following Eq. (2). The antenna parameters mainly influence the threshold distance.

$$d_0 = \frac{\varepsilon_0}{\varepsilon_1} \tag{2}$$

The energy dissipated from the battery is calculated with Eq. (3), where *E* is the energy, *V* indicates the Voltage (V) of the node, *I* is current drawn from the Battery and *t* is the radio operation duration (i.e) data bit rate.

$$E = V \cdot I \cdot t \tag{3}$$

The Eq. (4) and Eq. (5) elucidate the amount of energy consumed by the node with time constant.

$$E = v_b\left[1 - e^{-\pi}/RC\right] \cdot I \cdot t \tag{4}$$

$$\Delta E = v_b\left[1 - e^{-\pi}/RC\right] \cdot I \cdot \Delta t \tag{5}$$

Energy dissipated by the node for transmitting and receiving a bit of data is given by the following Eq. (6), Eq. (7) and Eq. (8).

$$E_{tx}\left(k, d\right) = E_{elec}k + E_{fs}kd^2;\ d < d_0 \tag{6}$$

$$E_{tx}\left(k, d\right) = E_{elec}k + E_{mp}kd^2;\ d > d_0 \tag{7}$$

$$E_{rx}\left(k\right) = E_{elec}k \tag{8}$$

K - No. of bits, *D* - Distance, E_{elec} - Energy dissipated per bit to run the transmitter or the receiver circuit, E_{rx} - Energy dissipated during receiving data, E_{fs} (pJ/(bit−m^{-2})), E_{mp}(pJ/(bit−m^{-2})) - Energy dissipated per bit to run the transmit amplifier based on the distance between the transmitter and receiver.

Data load computation.

Probability of choosing *x* state to y state for *n* steps is given by Eq. (9).

$$P_{xy} = P_r \cdot \left(P_n = y \middle| P_0 = x\right) \tag{9}$$

The probability of single-step transition from *x* to *k* is given by Eq. (10).

$$P_{xk} = P_r \cdot \left(P_1 = q \middle| P_0 = x\right) \tag{10}$$

For a time-homogeneous Markov chain in Eq. (11).

$$P_r\left(P_n = y\right) = \sum_{r \in s} P_{ry} P_r \cdot \left(P_{n-1} = r\right) \tag{11}$$

Generalized probability of choosing r steps is explained in Eq. (12).

$$P_r\left(P_n = y\right) = \sum_{r \in s} P_{ry} P_r \cdot \left(P_0 = r\right) \tag{12}$$

$$P = \begin{matrix} S_1 \to S_2 \to S_3 \\ S_1 \to P_{r11} \to P_{r12} \to P_{r13} \\ S_2 \to P_{r21} \to P_{r22} \to P_{r23} \\ S_3 \to P_{r31} \to P_{r32} \to P_{r33} \end{matrix} \tag{13}$$

4 RESULTS AND DISCUSSION

The proposed algorithm is simulated in Matlab based environment with 200 nodes and 500 × 500 m environment. The nodes are distributed in random fashion and have equal Initial Energy. Tab. 1 illustrates the simulation prelims considered in the proposed work. The node energy considered is different and the key exchange happens when the voltage of the current CH reduces to a threshold level. The algorithm is compared with the bench mark protocol LEACH and TSRF security based algorithm for heterogeneous environment to prove its novel working. Fig. 3 illustrates the node deployment inside the region of Interest in simulation environment

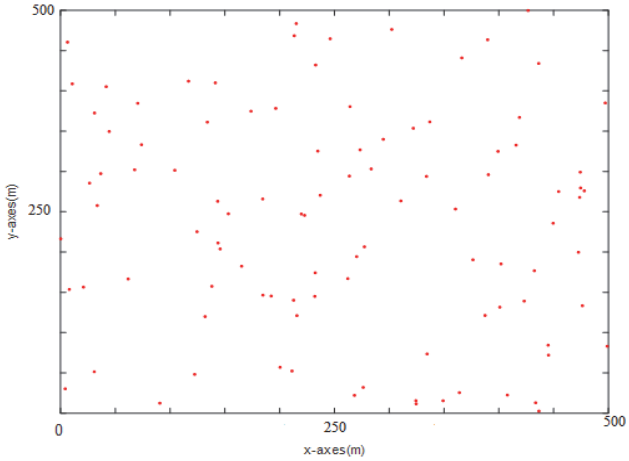

Figure 3 Region of interest of the proposed work

Table 1 Network prelims considered in simulating the proposed work

Parameters	Value
Number of nodes used in simulation	200
Eelec	50 nJ/bit
Efs	10 pJ /bit-m^2
IntialEnergy(E)	2 Joule, 3 Joule and 5 Joule
Probability (P) to be a CH in corresponding Cluster	0.1
Data message size	2000 bytes
Header data bytes	50 bytes

MATLAB simulations used 200 nodes in a 500 × 500 m area. The network employed different initial energy levels, and important exchanges occurred when the Cluster Head (CH) voltage dropped below a threshold. The method was tested against LEACH and TSRF in various settings. SARE beat LEACH in simulations, boosting network longevity by 1.15 times and throughput by 1.42 times. The SARE algorithm reduced HOTSPOT and Energy Hole, proving network stability. Despite hostile nodes, the method outlasted previous protocols 1.36 times. SARE's CH selection and key rotation improved network stability and energy savings. The simulation is done with 1 - 5 malicious nodes randomly deployed across the region of Interest. The malicious node does not relay data and mainly creates acknowledgement imitating successful delivery. The sender believes in successful delivery and loses its energy by sending repeated data to malicious nodes. Fig. 4 illustrates the lifetime comparison of the proposed work with LEACH and TSRF algorithms. The proposed work outperforms the existing LEACH protocol by 1.36 times for 5 malicious nodes. The battery voltage based CH selection and key rotation aspects have improved the network lifetime and enhanced energy saving in the network.

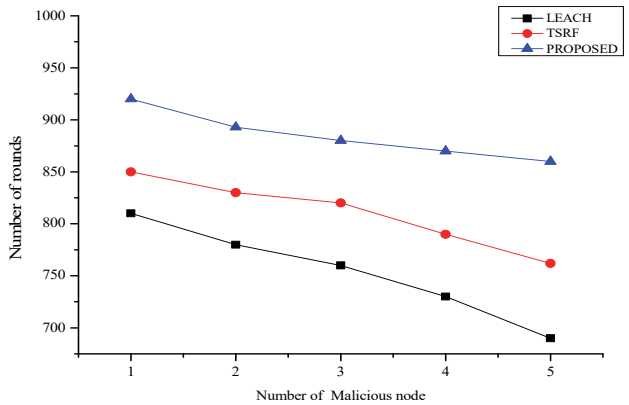

Figure 4 Network lifetime comparison with TSRF and LEACH routing protocols

Fig. 5 illustrates the data speed rate of the proposed algorithm; the proposed algorithm outperforms the LEACH and TSRF protocol with 1.25 times increased network speed due to high link stability and better CH selection.

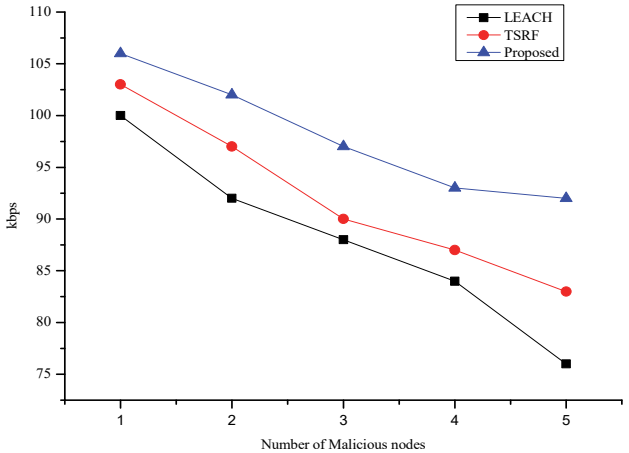

Figure 5 Network speed comparison with LEACH and TSRF routing protocols

Fig. 6 elucidates the drop packet in case of all the three algorithms. The proposed algorithm provides reduced drop packets.

Fig. 7 elucidates the return packets rate, the proposed algorithm provides low return packets, thereby reducing

the energy consumption through return packets inside the network.

Fig. 8 elucidates the energy map of the proposed algorithm; the proposed algorithm avoids energy-hole issue and HOTSPOT problem inside the network. The sensor nodes very near the sink are loaded equally with nodes far away from the sink. The algorithm provides unequal clustering and equal load is given to all the nodes inside the network. The sink is located in 250, 750 to understand unequal clustering in better means (RoI). The node having more energy is loaded most in the network.

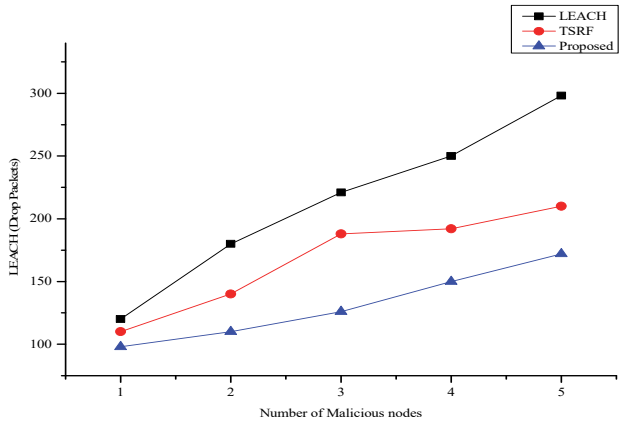

Figure 6 Drop packets comparison of LEACH, TSRF and proposed algorithm

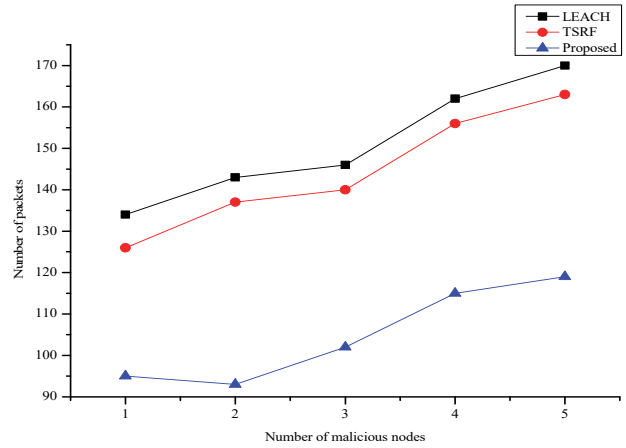

Figure 7 Return packet rate of LEACH, TSRF and Proposed

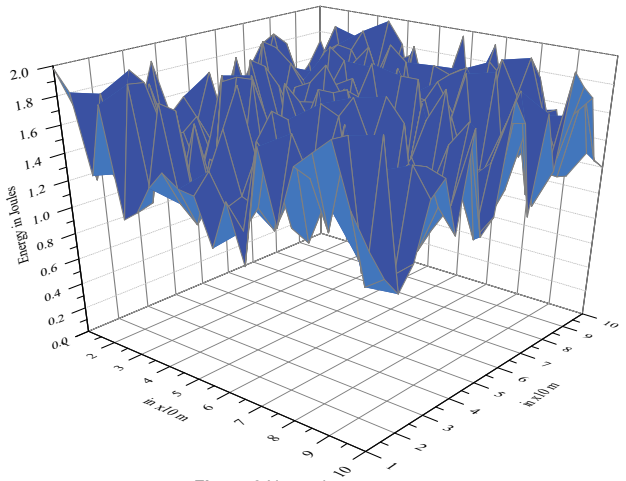

Figure 8 Network energy map

Fig. 9 illustrates the throughput map of the network with respect to region of interest (RoI). The nodes having more energy are loaded most in the network.

Tab. 2 discusses the evaluation of the proposed research with modern routing algorithm and larger networks. SARE achieves a longer network lifetime across all sizes, surpassing both traditional (LEACH, TSRF) and modern algorithms (TEAR, SEED) by up to 15% in larger networks. SARE's throughput remains consistently higher, particularly in medium and large networks, due to optimized CH selection and low retransmission rates. SARE demonstrates superior energy efficiency, consuming around 10 - 20% less initial energy than other algorithms by focusing on residual energy and efficient routing. SARE maintains the lowest packet drop rate across all network sizes, which underscores its reliability and robust security features.

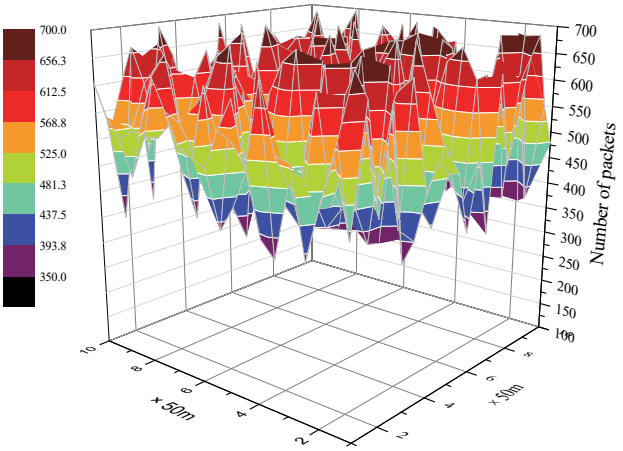

Figure 9 Throughput map of the network

Table 2 Evaluation of the proposed research with modern routing algorithm and larger networks

Network Size	Algorithm	Network Lifetime / hours	Throughput / Packets/sec	Energy Efficiency (% of Initial Energy Used)	Packet Drop Rate / %
Small (50 Nodes)	SARE	120	15	30%	2%
	LEACH	90	10	45%	5%
	TSRF	100	12	40%	4%
	TEAR	110	13	35%	3%
	SEED	105	11	38%	4%
Medium (200 Nodes)	SARE	115	20	35%	3%
	LEACH	80	14	50%	6%
	TSRF	90	17	43%	5%
	TEAR	105	19	37%	4%
	SEED	95	16	42%	5%
Large (500 Nodes)	SARE	110	25	38%	4%
	LEACH	70	16	55%	7%
	TSRF	85	19	48%	6%
	TEAR	95	21	40%	5%
	SEED	90	18	45%	6%

Table 3 Computational complexity analysis of proposed algorithms

Algorithm	CH Selection Complexity	Encryption Complexity	Key Renewal Complexity	Overall Computational Complexity
SARE	O(kn)	O(n)	O(1)	O(kn+n)
LEACH	O(n)	O(1)	No key renewal	O(n)
TSRF	O(nlogn)	$O(n^2)$	O(1)	$O(n^2 logn)$
TEAR	O(kn)	$O(n^2)$	O(1)	$O(kn+n^2)$
SEED	$O(n^2)$	$O(n^2)$	No key renewal	$O(n^2)$

The table compares five algorithms in terms of computational complexity SARE, LEACH, TSRF, TEAR, and SEED based on their computational complexities in CH selection, encryption, key renewal, and overall processing. SARE and TEAR both exhibit O(kn) complexity in CH selection, while LEACH and TSRF show more efficient O(n) and O(nlogn) complexities, respectively. Encryption complexity varies significantly, with simpler algorithms like SARE and LEACH achieving O(n) or O(1), whereas TSRF and SEED have higher $O(n^2)$ encryption demands. Key renewal is minimal or absent in most, except SARE and TEAR, which efficiently handle it with O(1) complexity. In terms of overall computational complexity, LEACH is the most efficient O(n), while SEED and TSRF are more computationally intensive ($O(n^2)$ and $O(n^2 \log n)$, respectively), making LEACH suitable for low-resource environments and SEED better for security-critical tasks despite higher resource demands.

5 CONCLUSION

The SARE method is recommended for effectively addressing the energy and security challenges faced by resource-starved IoT devices. The network is significantly safeguarded against assaults due to the utilization of the routing protocol key exchange. Both the TSRF and LEACH protocols exhibit a lifetime that is 1.36 times shorter than the suggested strategy. The technique offers advantages such as high throughput, reduced data loss, and a decreased frequency of return packets. Additionally, the suggested technique achieves load balancing by evenly distributing the workload across all nodes in the network. This effectively resolves the issues of HOTSPOT and energy holes in wireless hybrid sensor networks. The proposed SARE algorithm aims to enhance resilience against environmental attacks.

6 REFERENCES

[1] Balakrishnan, S. & Vinoth Kumar, K. (2023). Hybrid Sine-Cosine Black Widow Spider Optimization based Route Selection Protocol for Multihop Communication in IoT Assisted WSN. *Technical Gazette, 30*(4), 1159-1165. https://doi.org/10.17559/TV-20230201000306

[2] Zahedi, A., Arghavani, M., Parandin, F., & Arghavani, A. (2018). Energy Efficient Reservation-Based Cluster Head Selection in WSNs. *Wireless Personal Communications, 100*(3), 667-679. https://doi.org/10.1007/s11277-017-5189-9

[3] Ponni, R., Jayasankar. T., & Vinothkumar, K. (2023). Investigations on Underwater Acoustic Sensor Networks Framework for RLS Enabled LoRa Networks in Disaster Management Applications. *Journal of Information Science and Engineering, 39*(2), 389-406

[4] Sharma, D., Ojha, A., & Bhondekar, A. P. (2019). Heterogeneity Consideration in Wireless Sensor Networks Routing Algorithms: A Review. *Journal of Supercomputing, 75*(5), 2341-2394. https://doi.org/10.1007/s11227-018-2635-8

[5] Kumar, K. V. & Balakrishnan, S. (2023). Multi-objective Sand Piper Optimization Based Clustering with Multihop Routing Technique for IoT Assisted WSN. *Brazilian Archives of Biology and Technology, 66*, e23220866. https://doi.org/10.1590/1678-4324-2023220866

[6] Han, D., Li, S., Peng, Y., & Chen, Z. (2020). Energy Sharing-Based Energy and User Joint Allocation Method in Heterogeneous Network. *IEEE Access, 8*, 37077-37086. https://doi.org/10.1109/ACCESS.2020.2975293

[7] Lee, S. H., Kim, M., Shin, H., & Lee, I. (2021). Belief Propagation for Energy Efficiency Maximization in Wireless Heterogeneous Networks. *IEEE Transactions on Wireless Communications, 20*(1), 56-68. https://doi.org/10.1109/TWC.2020.3023079.

[8] Shagari, N. M., Idris, M. Y. I., Salleh, R. B., Ahmed, I., Murtaza, G., & Shehadeh, H. A. (2020). Heterogeneous Energy and Traffic Aware Sleep-Awake Cluster-Based Routing Protocol for Wireless Sensor Network. *IEEE Access, 8*, 12232-12252. https://doi.org/10.1109/ACCESS.2020.2965206

[9] Thiruppathi, M. & Vinoth Kumar, K. (2023). Seagull Optimization-Based Feature Selection with Optimal Extreme Learning Machine for Intrusion Detection in Fog Assisted WSN. *Technical Gazette, 30*(5), 1547-1553. https://doi.org/10.17559/TV-20230130000295

[10] Genta, A., Lobiyal, D., & Abawajy, J. H. (2019). Energy Efficient Multipath Routing Algorithm for Wireless Multimedia Sensor Network. *Sensors, 19*(17), 3642. https://doi.org/10.3390/s19173642

[11] Haseeb, K., Abbas, N., Saleem, M. Q., Sheta, O. E., Awan, K., Islam, N., Ur Rehman, W., & Salam, T., (2019). RCER: Reliable Cluster-Based Energy-Aware Routing Protocol for Heterogeneous Wireless Sensor Networks. *PLoS One, 14*(9), e0222009. https://doi.org/10.1371/journal.pone.0222009

[12] Jameasha, S., Gowtham, M. S., Gopinath, S., & Kumar, K. V. (2022). Investigation on Thermal Energy Aware Routing in Integrated Network for Efficient Energy Storage. *Materials Today Proceedings, 66*(3). https://doi.org/10.1016/j.matpr.2022.04.980

[13] Ramesh, S., Rajalakshmi, R., Dwivedi, J. N., Selvakanmani, S., Pant, B., Bharath Kumar, N., & Fissiha Demssie, Z. (2022). Optimization of LEACH Protocol in Wireless Sensor Network Using Machine Learning. *Computational Intelligence and Neuroscience, 2022*, 5393251. https://doi.org/10.1155/2022/5393251

[14] Adday, G. H., Subramaniam, S. K., Zukarnain, Z. A., & Samian, N. (2022). Fault Tolerance Structures in Wireless Sensor Networks (WSNs): Survey, Classification, and Future Directions. *Sensors, 22*(16), 6041. https://doi.org/10.3390/s22166041

[15] Kumar, K. V., Jayasankar, T., Eswaramoorthy, V., & Nivedhitha, V. (2021). SDARP: Security Based Data Aware Routing Protocol for Ad hoc Sensor Networks. *International Journal of Intelligent Networks, 1*, 36-42. https://doi.org/10.1016/j.ijin.2020.05.005

[16] Sun, H., Song, Q., & Xu, Z. (2023). A Method for Using the Residual Energy in Waste Li-Ion Batteries by Regulating Potential with the Aid of Overvoltage Response. *Proceedings of the National Academy of Sciences, 120*(14), e2213130120. https://doi.org/10.1073/pnas.2213130120

[17] Hosseinzadeh, M., Ahmed, O. H., Lansky, J., Mildeova, S., Yousefpoor, M. S., Yousefpoor, E., Yoo, J., Tightiz, L., & Rahmani, A. M. (2023). A Cluster-Tree-Based Trusted Routing Algorithm Using Grasshopper Optimization Algorithm (GOA) in Wireless Sensor Networks (WSNs). *PLoS One, 18*(9), e0289173. https://doi.org/10.1371/journal.pone.0289173

[18] Eswaramoorthy, V., Kumar, K. V., & Gopinath, S. (2021). Fuzzy Logic Based DSR Trust Estimation Routing Protocol for MANET Using Evolutionary Algorithms. *Tehnički vjesnik/Technical Gazette, 28*(6). https://doi.org/10.17559/TV-20200612102818

[19] Li, J., Tu, T., Li, Y., Qin, S., Shi, Y., & Wen, Q. (2022). DoSGuard: Mitigating Denial-of-Service Attacks in Software-Defined Networks. *Sensors, 22*(3), 1061. https://doi.org/10.3390/s22031061

[20] Fathy, C. & Ali, H. M. (2023). A Secure IoT-Based Irrigation System for Precision Agriculture Using the Expeditious Cipher. *Sensors, 23*(4), 2091.

https://doi.org/10.3390/s23042091
[21] Feng, Q., Chu, S. C., Pan, J. S., Wu, J., & Pan, T. S. (2022). Energy-Efficient Clustering Mechanism of Routing Protocol for Heterogeneous Wireless Sensor Network Based on Bamboo Forest Growth Optimizer. *Entropy, 24*(7), 980. https://doi.org/10.3390/e24070980
[22] Xu, Y., Jiao, W., & Tian, M. (2020). Energy-Efficient Connected-Coverage Scheme in Wireless Sensor Networks. *Sensors, 20*(21), 6127. https://doi.org/10.3390/s20216127
[23] Keum, D. & Ko, Y. B. (2022). Trust-Based Intelligent Routing Protocol with Q-Learning for Mission-Critical Wireless Sensor Networks. *Sensors, 22*(11), 3975. https://doi.org/10.3390/s22113975
[24] Allimuthu, U. & Mahalakshmi, K. (2022). Efficient Mobile Ad Hoc Route Maintenance Against Social Distances Using Attacker Detection Automation. *Mobile Networks and Applications*, 1-32. https://doi.org/10.1007/s11036-022-02040-3
[25] Jayasankar, T., Kiruba Buri, R., & Maheswaravenkatesh, P. (2024). Intrusion Detection System Using Metaheuristic Fireworks Optimization Based Feature Selection With Deep Learning on Internet of Things Environment. *Journal of Forcasting, 43*(2), 415-428. https://doi.org/10.1002/for.3037
[26] Xia, Z., Wei, Z., & Zhang, H. (2022). Review on Security Issues and Applications of Trust Mechanism in Wireless Sensor Networks. *Computational Intelligence and Neuroscience, 2022*, 3449428. https://doi.org/10.1155/2022/3449428
[27] Kumar, K. V. & Thiruppathi, M. (2023). Oppositional Coyote Optimization based Feature Selection with Deep Learning Model for Intrusion Detection in Fog Assisted Wireless Sensor Network. *Acta Montanistica Slovaca, 28*(2). https://doi.org/10.46544/AMS.v28i2.18

Contact information:

INDRA PANDIAN
(Corresponding Author)
Department of ECE,
Government College of Engineering,
Salem, India
E-mail: dr.indra_pandian@rediffmail.com

SHANTHI THIRUGNASAMBANTHAM
Department of ECE,
Kings College of Engineering,
Thanjavur, India

KARTHIKEYAN BALASUBRAMANIAM
Department of IT,
Panimalar Engineering College,
Chennai, India

KIRUBABURI RAVICHANDRAN
Department of CSE,
University College of Engineering,
Pattukottai, India