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

https://doi.org/10.17559/TV-20210729085331
Preliminary communication

OELB - IH Algorithm for Secure Data Routing to Improve the Network Location Advisory Privacy Performance in WSN

A. ARIVARASI*, P. RAMESH

Abstract: Wireless network performance greatly depends on the number of factors such as output, delay packet delivery rate, packet drop rate, and many others. Each quality of service parameter greatly depends on other parameters also. However, the only obstacle which stops the performance achievement is security issues. In most cases, the adversary involves learning the network data to identify the routing strategy, data transmission strategy, and so on. When the adversary is capable of identifying the traffic and routing strategy, the adversary can perform different network. To improve the network performance and safeguard the network transmission using an Iterative heuristic algorithm, an efficient neighbor discovery-based security enhancement algorithm with Optimized Elastic Load Balancing (OELB) protocol is applied. In this Optimized Elastic Load Balancing Routing with Iterative Heuristic (OELB-IH) algorithm to provide secure communication in the sensor network. In this work, the Receiving Signal Strength Indication (RSSI) value to estimate the transmission support and transmitting signal range estimate to identify the nearest coverage nodes. The iterative heuristic algorithm performs tracking and seeking to achieve the node location and transmission error. In this OELB protocol, to identify the lower transmission path with lower energy consumption, it helps to multipath communication over the network. In this proposed has produced efficient results on security performance and throughput performance compared to other existing methods (SPAC, CPSLP, RRA).

Keywords: receiving signal strength; routing strategy; seeking; tracking; transmission error

1 INTRODUCTION

It is very difficult from such other wireless networks on the intrinsic properties of these networks, such as mobile or cellular networks to route the wireless sensor network. A continuous stream of messages indicating the presence of the event being monitored, and on the contrary, the discrete messages reveal the absence of that event. For example, in military application monitoring a specific area, a continuous stream of messages indicate the existence of enemy soldiers and the quantity of them passing by that sensor. Due to the relatively large number of sensor nodes, it is impossible to establish a global solution, and the maintenance cost of the ID for deploying a large number of sensor nodes is high. As a result, traditional IP-based protocols are not used in wireless sensor networks. In wireless sensor networks, the data obtained is sometimes more important than knowing the identity of the data sent by the node. Unlike typical communication networks, almost all sensor network applications require a stream of data perceived from multiple sources at a particular base station. However, this does not impede other forms of data flow (e.g., multicast or point-to-point).

Deployment of wireless sensor networks can be based on their network structure and application type, as it requires consideration of both design and communication challenges for effective communication. In addition, its network challenges have a major impact on the design of the routing protocol and thus reduce its performance. The data generated by the WSN sensor node is overkill. Accordingly, the data set is used to couple the energy efficiency of the same data packet from the optimized data transmission performance of different nodes and routing protocol. Due to power constraints, computing power, and storage resources, this has been found to be a challenge in identifying the appropriate cryptosystem for wireless sensor networks. Data confidentiality is usually important in many wireless sensor networks, as the information sent by the sensor nodes can include personal information, such as remote medical monitoring of patients. Sensor nodes are easy to use in difficult areas. The sensors monitoring the surrounding environment help. When the sensor reports a monitored object such as the appearance of a rare animal, it sends a series of messages to the sink through multi-hop wireless communications.

The transmission rate at which the messages arrive reveals the quantity and nature of the event being triggered. Communication pattern helps the adversary to learn the network topology, which in turn assists him in determining the location of some important nodes such as the source node location or the sink node location. The shared wireless medium can know the source hop back hop in order to find out the origin of its radio broadcast and thereby lead to multiple hop communication. To propose a technique for preserving the Source routing Privacy that relies on randomizing the message delivery path using multipath routing and deviate the adversary away from the source node location using tunnels with faked messages.

2 RELATED WORK

This chapter discusses the existing solution for secure data transmission and routing methods. Both are used in EnhAnced Protocol for Source location (EAPS) [1], to adjust the radius of contamination during angle-based and efficient routing. DynaPro [2], as a middleware for application for differential privacy, uses a Hierarchical Random Graph (HRG). Instead, because to add a noise directly to the network of data and topology, DynaPro of noise, add the HRG. In [3], the distribution of the generation and detection path fully utilizes the energy of the non-hot as necessary to achieve the safety and energy efficiency required to create any number of detection paths. A private key is a location-aware end-to-end security framework in [4] that combines multiple keys into geographic locations based on their location and stores each node. This location awareness performance effectively limits exposed nodes in the vicinity without affecting the ultimate impact on device data security, for example, by using public-key cryptography (PKC) [5], such as typical one-time cost, which is often used for WSN security, once in the network life of a wireless sensor network. The impact of energy costs is being considered.

The route optimization algorithm [6] adjusts the transmission line by protecting weak nodes (nodes with low transmission capacity) in order to increase the life cycle of the network. In recent years, more effective methods have been proposed to solve the problem of maximizing the life of wireless sensor networks. [7] proposed a cooperative communication method to improve spatial diversity and maximize the lifetime for data aggregation. It adopted the data compression method based on compressive sensing theory to prolong the lifetime of WSN [8].

Author protocol [9] has been proposed by the showy mutual authentication, key exchange, including the perfect forward secrecy and privacy measures to support safe route optimization (RO) and handover management. In [10] proposed the hot spot method is to minimize the energy consumption, to create a redundant path without a hot spot with a wealth of energy. Limited energy and data transmission in wireless sensor network (WSN) deployment environments are Trusted Sensing-Based Secure Routing Mechanism (TSSRM) [11] with sense, reliability, and lightweight capabilities and the ability to withstand many common attacks. Traditional wireless sensor networks data privacy protection is primarily based on encryption technology. For example, end-to-end data collection and privacy protection [12] use homomorphic encryption technology. In [13], to propose a data aggregation privacy protection method CDA. Homomorphic encryption is used to collect encrypted data through a sink node. A hierarchical random map is used to represent the model network map [14]. Instead of adding noise directly to the nodes rather than noise is added with the probabilities of connection between the nodes in the graph.A Compressive Sensing based Clustering Joint Annular Routing Data Gathering (CS-CARDG) [15] was proposed to improve network life. Key Techniques used in CS CARDG Project: The central idea is to retrieve a finite-dimensional signal from the linear measurement panel if the signal base or dictionary [16] is rare. In [17], a new bandwidth-efficient Co-Authentication (BECAN) method was proposed to filter infused erroneous data. Random graph characteristics are based on the development of sensor nodes and cooperative bit compression authentication technology. Such an environment and habitat monitoring, and military surveillance and tracking, some of the new applications [18], has been recognized as a ubiquitous and universal method for. The authors of [19], secure routing protocol named trust, have developed a trust that is not protocol. Node trust (or distrust) is graded according to the conformance value obtained by protocol testing and calculation. By taking the "peer" attribute in consideration of effective routing schemes, the trust-based scheme proposes to be forced to cooperate with wireless mobile networks [20]. CPSLP [21] author proposes a scheme that in each transmission the packet destinations changes randomly. In addition, multiple sinks are adopted to create many routing paths. In [22] designs a message sharing scheme and maps the original message to a set of messages shares with short length and with minimum energy. RRA [23] Routing is done through agent node which confuses the parasitic nodes and helps in source location privacy of the networks.

3 IMPLEMENTATIONOF THE PROPOSED WORK

This work proposes a technique to protect the privacy of the original location and prevent enemies from tracing the location of the source of the information flow hop by jumping. The proposed received signal strength indicator (RSSI) values to estimate the node receiving strength to identify the distance. It monitors the location of the source of protection during the delivery of data packets in two.

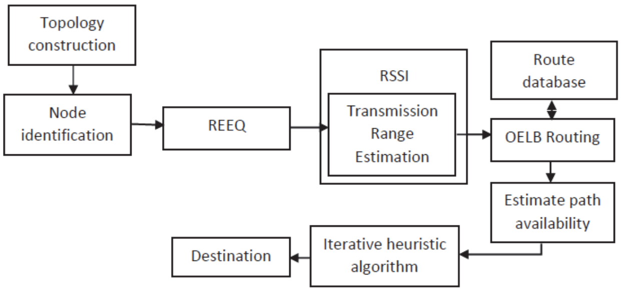

Figure 1 Implementation of the proposed method

Stages. In the first stage, multipath routing and the second is to use the tunnel with RREQ Replica messages. Each time the source discovers a sink node, it sends a watch Replica packet. When using fixed multipath with surveillance data packets, enemies who could easily track the packets sent a hop back to their original location.

The sensor network uses the Optimized Elastic Load Balancing (OELB) protocol, which is designed based on a multi-route strategy as every transmitted packet takes the dynamic route (default route), and the block diagram is shown in Fig. 1. The single-path routing strategy doesn't protect the source location privacy. To explore patterns for OELB traffic and can easily find hop by hop considering the location of the source terminal in a short period of time. In this work, OELB relies on two levels to protect the original location. The first step is to use a multi-way routing approach where each packet is approximated in a different direction. Routing Protocol for OELB based protocol uses multipath routing to achieve source location privacy.

3.1 Transmission Range Estimation

The sensor node locations are determined by RSSI value, and then the SNs transfer the information with their adjacent nodes to interchange the radio signal strength of them. In this work, to anew heuristic algorithm is proposed to minimize the localization error. The formulated method utilizes both the deployment information and adjacent nodes distance approximation by RSSI to build the probability function unknown nodes to the correct position. In the ranging phase, the calculation of distances of unknown Sensor Nodes (SNs) and beacon nodes to improve the location accuracy.

$$N_r = N_t \left(\frac{\vartheta_0}{4\pi d} \right) \tag{1}$$

Where N_r denotes signal power of transmitter; d represents the distance of the transmitter & receiver (in meters); n is path loss constant. In practical conditions, due to the presence of a number of paths, noise, etc., the received power has a difference in calculations with the free space propagation model. The different studies have revealed the common logarithm of the distance path model used in Eq. (2).

$$NL\left(d\right) = NL_0 + n\log_{10}\frac{d}{d_0} + S \tag{2}$$

Where the d_0 is reference distance, path loss at the reference distance as NL_0 and Gaussian random variable S.

$$RSSI = N_r - NL\left(D\right) \tag{3}$$

The $RSSI$ of the receiver node is given Eq. (3) to calculate the distance and receiving strength.

3.2 Optimized Elastic Load Balancing (OELB) Protocol

OELB considers only neighbors with a lower hop count and doesn't consider neighbors with equal hop count in the sensor list. Consider adding sink nodes to the routing table of each node in a sink list. After the initialization and Transmission Range Estimation, every node has two lists of sensor list (Si) and sink list (Ai). For, i.e., node i, if the sender's hop count is equal to the node I's hop count, then the node is saved to the sink list, and if the sender's hop count is lower than the node I's hop count, it's saved to sensor list. The sensor list contains only neighbor with a lower hop count, which can be further divided into two lists, the neighbor with a lower hop count but having the same hop count, denoted as equal list Xi and neighbor with different lower hop count denoted as a further list, Yi. Accordingly, when the messages transmitted from the source to the sink nodes, select the next-hop from its sensor node list; therefore, delivery paths will change on every transmitted message randomly.

```
Input: Trace of Network NeT, Details of Node locationLoc
(Si), Sink Node (Ai)
Output: Location identification
Startup
        Incoming packets are received as P.
        Extract source address Saddr
                Saddr = P.S_ADDR
        Extract Location information
        N-Loc = NeT(Ni(Loc)).
 Location details are verified using the ELB algorithm.
        If correct then
        Identify the node located before that.
                L = Ls(Ni)@Tα-1
 Estimate the rate of the packet received.
Tpr = ∑packets (Ni) €Nt(current Time Location
To calculate the weighted average of security.
Estimate belief value for the sink (Ai) node
Tn(si) = Time packet rate (Si) × Ai location.
If Tn(si)<T as then //T is the value of the threshold
 The packet has been forward.
                End
        Else
Packet Drop and search for another sink node.
Yi ← Si*Ai // to identity the nearest node.
        End.
Stop.
```

To protect the location of the source node, it has to make it difficult to find the location of the return port by randomizing the host supply route. Each message takes a different path and, consequently, making the difficulty to the adversary to trace the message back to the source location

3.3 Iterative Heuristic Algorithm

This algorithm is developed through the behavior of the sink node and reduces a signal error. This method performed a two-mode there are seeking and Tracking, respectively.

Seeking Network:

In this mode network, data packets are stores the present position of the sensor data. Calculate the fitness value for all the coordinate points by Eq. (4). Select the coordinate points and replace them with the best data transmission points. The current fitness define a set of node weights (W) where the node index set $i = 1, 2, 3, \ldots, n - 1$.

$$C_f\left(i\right) = \sum\nolimits_{i=0}^{n} O_i\left(s\right) W_n\left(i\right) \tag{4}$$

Where s - Sink node and best fitness function to be calculate as B_f follow equation.

$$B_f\left(i\right) = W_{n,\left[\frac{i}{I}\right]} + \frac{i \text{ model}}{I}\left(W_{b,\left[\frac{i}{I}\right]+1} - W_{b,\left[\frac{i}{I}\right]}\right) \tag{5}$$

I - Number of iteration

$$R_i = \frac{\left(\left|C_f - \right|B_f\right)}{\left(B_{min} - B_{max}\right)} \tag{6}$$

C_f - Current Fitness
B_f - Best Fitness

If the objective is to minimize the solution, then $B_f = B_{min}$ otherwise $B_f = B_{max}$.

Tracking network:

In this sub, the model depicts the tacking of node behavior and update the velocities for each sink direction. Check the velocity for in range, and if not, it has to be set equal to the maximum limit.

```
Objective function f(x); where x = (x1, x2,..., xn)
Input parameters for algorithms
Create population (initial) of 'n' IoT sensor and node
location point, xi; where i =1, 2...n
While (I<$i_{max}$ )
        For each sensor, calculate the fitness value and
assign them
        Update best fitness valuepbest=xbest
        Keep present value as new-xbest
        End for
        Select the sensor with the best-fitness value($B_f$)
        For i=1: n

                If $B_f$= 1, Start seeking network
                Else: Start tracing network
        End for

End while

Process the end results
```

The above algorithm performs a tracking node location and data transmission to minimize the localization error on the network.

4 RESULT AND DISCUSSION

In this simulation, the NS2 simulation tool is is used to implement our proposed work and measure its performance.The implementation was carried out through NS-2 and Tool Command Language (TCL) language. This configuration completes the test of the RAM's 4 GB Intel i5 processor. This method has evaluated the performance of the proposed technique in designing routing security in WSN. The Tool Command Language (TCL) script is used to code the network environment.

Tab. 1 shows the values for the various parameters considered during the simulation. A sensor network with 70 nodes is randomly deployed, while dynamic nodes move around the WSN with mobility at a speed of 0.5m/s. throughout the simulation. Tab. 1 shows the simulation parameters of the proposed method. In the proposed method using network simulator (NS2) for node and data

transferring improving the performance, node quantity is 500 and the simulation time completed in 30 sec each node transfer using the types of CBR traffic, Then the node speed 20 m/s and the each packets sixe is 512 kb, In the total number of packets of 484 is sends the queuing length for 50 and the processing data size is 242 mb.

In this proposed method, Optimized Elastic Load Balancing Routing with Iterative Heuristic (OELB-IH) and Adaptive Trust Sector-Based Authenticated System (ATSAS) [24] results are compared to existing method Cloud-based protecting Source-Location Privacy (CPSLP) [23], Random Routing Algorithm(RRA) [22], and Protection scheme based on Anonymity Cloud (SPAC) [21]

Security analysis: Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity availability and Identify potential weaknesses and threats.

PDR: number of packets delivered in total to the total number of packets sent from source node to destination node in the network.

End-to-end analysis: End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination

Throughput Analysis: In data transmission, network throughput is the amount of data moved successfully from one place to another in a given time period

These parameters can improve the network performance based on the number of packets send and receive in secure routing.

Table 1 Simulation parameters of the proposed method

Parameter	Value
Simulator	NS2
Node quantity	500
Simulation Time	30 sec
Type Traffic	CBR
Node Speed	20 m/s
Packet Size	512 MB
Queue length	50
Process data size	242 mb
Total packet	484

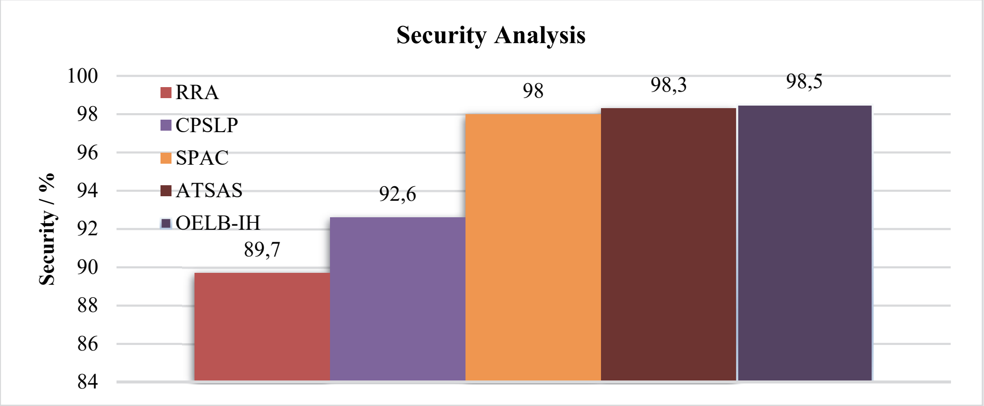

Figure 2 Comparison of security analysis

The proposed methods have produced different results on various parameters of network security. At the conclusion of this study, the proposed method OELB-IH offers 98.5% protection compared to existing approaches to ATSAS, SPAC has 98% security on the wireless sensor network. Fig. 2 shows the security analysis of the existing methods RRA, CPSLP, SPAC, ATSAS, and the proposed method OELB-IH.

Fig. 3 represents how the packet delivery rate of those initially proposed work. The proposed method operates based on the OELB protocol and RSSI value to achieve greater packet distribution over a sensor network. In this proposed method, OELB-IH provides a 0.97% delivery ratio; similarly, the existing method ATSAS provides a 0.95% delivery ratio. This suggests that the proposed OELB-IH is more efficient in data delivery compare to other all RRA, CPSLP, APAC, and ATSAS.It provides a comparison of two obtained by the conventional method and the method proposed in the final end to end delay. At this end to end delay performance of the proposed method OELB-IH, less time delay compared to other existing methods ATSAS, RRA, CPSLP, and SPAC. In this result, the proposed method OELB-IH provides a 0.28 × 10^2 ms provide, and ATSAS is 0.31 × 10^2 ms average time delay performance; similarly, the existing methods CPSLP and SPAC provide a 0.43 × 10^2 ms and 0.38 × 10^2 ms average time delay, and its comparison is shown in Fig. 4.The throughput performance produced by OELB-IH, ATSAS, RRA, CPSLP, and SPAC protocols has been presented in Fig. 5, where they have produced higher throughput with the normalized value of 1940 kbps.

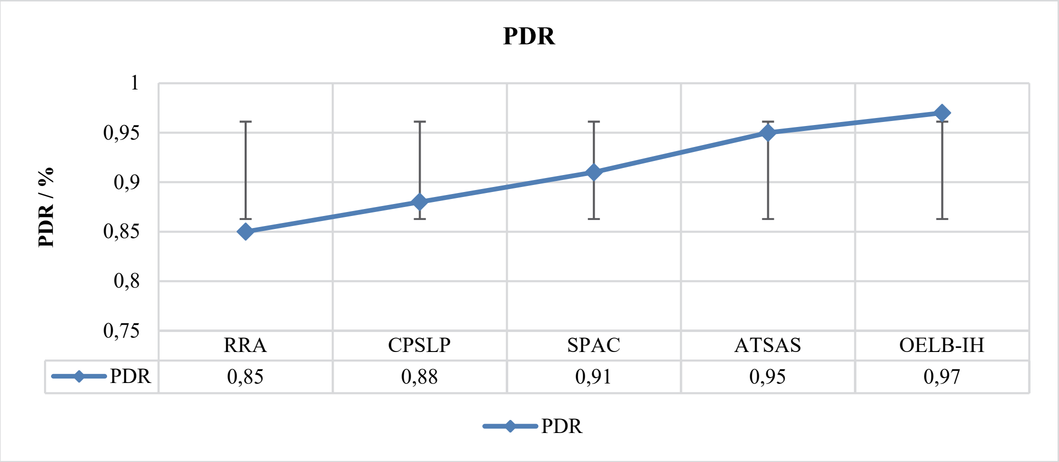

Figure 3 Analysis of packet delivery ratio

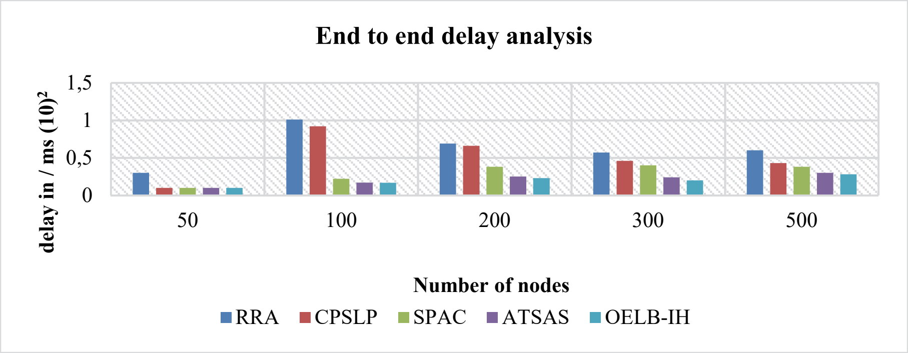

Figure 4 Comparison of End to End analysis

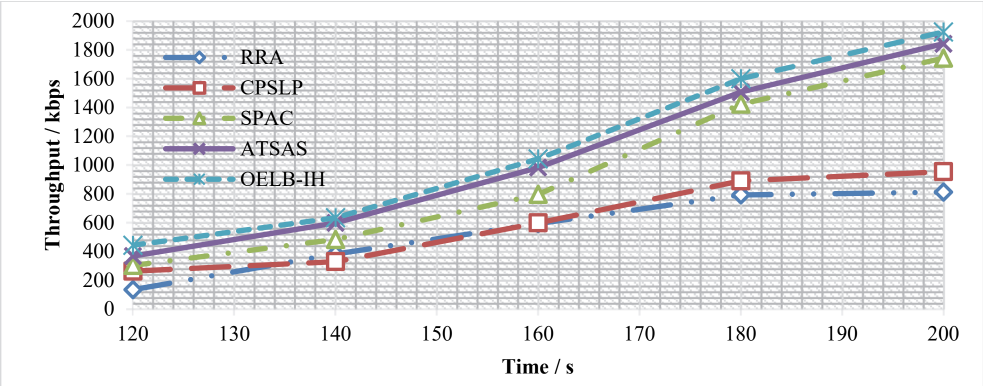

Figure 5 Analysis of throughput

5 CONCLUSION

This work presents a shared solution for designing wireless networks to solve secure communication with location privacy and improve the quality of transmission in the network. Multipath communication for estimate relation of low power and distance using the optimal protocol.The iterative heuristic algorithm provides a location privacy and transmission localization error on the network.In this proposed method Optimized Elastic Load Balancing Routing with Iterative Heuristic (OELB-IH) algorithm provides efficient multipath communication to achieve the network performance. Finally, simulation has been performed with varying conditions. The method has produced higher packet delivery performance up to 0.97% with the 0.28 × 10^2 ms end to end delay.

6 REFERENCES

[1] Jia, Z., Wei, X., Guo, H., Peng, W., & Song, C. (2017). A Privacy Protection Strategy for Source Location in WSN Based on Angle and Dynamical Adjustment of Node Emission Radius. *Chinese Journal of Electronics*, *26*(5), 1064-1072. https://doi.org/10.1049/cje.2016.08.022

[2] Li, S., Liu, Z., Huang, Z., Lyu, H., Li, Z., & Liu, W. (2019). DynaPro: Dynamic Wireless Sensor Network Data Protection Algorithm in IoT via Differential Privacy. *IEEE Access*, *1-1*. https://doi.org/10.1109/ACCESS.2019.2953470

[3] Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks. *IEEE Transactions on Information Forensics and Security*, *11*(9), 2013-2027. https://doi.org/10.1109/TIFS.2016.2570740

[4] Kui, R., Wenjing, L., & Yanchao, Z. (2008). LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks. *IEEE Transactions on Mobile Computing*, *7*(5), 585-598. https://doi.org/10.1109/TMC.2007.70753

[5] Bicakci, K., Gultekin, H., & Tavli, B. (2009). The impact of one-time energy costs on network lifetime in wireless sensor networks. *IEEE Communications Letters*, *13*(12), 905-907. https://doi.org/10.1109/LCOMM.2009.12.091331

[6] Mao, Y., Zhao, H., & Yan, D. (2018), Weak node protection to maximize the lifetime of wireless sensor networks, *Journal of Systems Engineering and Electronics*, *29*(4), 693-706. https://doi.org/10.21629/JSEE.2018.04.04

[7] Xu, H. L., Huang, L., & Sun, H. (2016) Maximum lifetime data aggregation for wireless sensor networks with cooperative communication. *International Journal of Sensor Networks*, *20*(3), 187-198. https://doi.org/10.1504/IJSNET.2016.075369

[8] Frezzetti, A. & Manfredi, S.(2016) A two-layer controller scheme for efficient signal reconstruction and lifetime elongation in wireless sensor networks. *IEEE Sensors Journal*, *16*(7), 2172-2179. https://doi.org/10.1109/JSEN.2015.2507865

[9] Shin, D., Sharma, V., Kim, J., Kwon, S., & You, I. (2017). Secure and Efficient Protocol for Route Optimization in PMIPv6-Based Smart Home IoT Networks. *IEEE Access*, *5*, 11100-11117. https://doi.org/10.1109/ACCESS.2017.2710379

[10] Jun, L., Mianxiong, D., Ota, K., &Anfeng, L. (2014). Achieving Source Location Privacy and Network Lifetime Maximization Through Tree-Based Diversionary Routing in Wireless Sensor Networks. *IEEE Access*, *2*, 633-651. https://doi.org/10.1109/ACCESS.2014.2332817

[11] Qin, D., Yang, S., Jia, S., Zhang, Y., Ma, J., & Ding, Q. (2017). Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network. *IEEE Access*, *5*, 9599-9609. https://doi.org/10.1109/ACCESS.2014.2332817

[12] Castelluccia, C., Chan, A. C. F., & Mykletun, E. (2009), Efficient and provably secure aggregation of encrypted data in wireless sensor networks, *ACM Trans on Sensor Networks*, *5*(3), 1-36. https://doi.org/10.1145/1525856.1525858

[13] Li, S. Y., Liu, Z. B., & Dong, K. (2019) Dynamic network data protection algorithm using differential privacy in the Internet of Things. *IEEE Smart IoT*, 1-8. https://doi.org/10.1109/SmartIoT.2019.00053

[14] Yuan, Y., Liu, W., Wang, T., Deng, Q., Liu, A., & Song, H. (2019). Compressive Sensing based Clustering Joint Annular Routing Data Gathering Scheme for Wireless Sensor Networks. *IEEE Access*, 1-1. https://doi.org/10.1109/ACCESS.2019.2935462

[15] Yin, Y., Chen, L., Xu, Y., & Wan, J. (2018) Location-Aware Service Recommendation With Enhanced Probabilistic Matrix Factorization, *IEEE Access*, *6*, 62815-62825. https://doi.org/10.1109/ACCESS.2018.2877137

[16] Lv, C., Wang, Q., Yan, W., & Li, J. (2018) A sparsity feedback-based data gathering algorithm for Wireless Sensor Networks. *Computer Networks*, *141*, 145-156. https://doi.org/10.1016/j.comnet.2018.05.022

[17] Rongxing, L., Xiaodong, L., Haojin, Z., Xiaohui, L., & Xuemin, S. (2012). BECAN: A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*, *23*(1), 32-43. https://doi.org/10.1109/TPDS.2011.95

[18] Chen, J., Yu, Q., Zhang, Y., Chen, H.-H., & Sun, Y. (2010) Feedback Based Clock Synchronization in Wireless Sensor Networks: A Control Theoretic Approach, *IEEE Trans. Vehicular Technology*, *59*(6), 2963-2973. https://doi.org/10.1109/TVT.2010.2049869

[19] Shi, Q., Qin, L., Ding, Y., Xie, B., Zheng, J., & Song, L. (2019). Information-Aware Secure Routing in Wireless Sensor Networks. *Sensors*, *20*(1), 165. https://doi.org/10.3390/s20010165

[20] Usman, A. B. & Gutierrez, J. (2019) DATM: A dynamic attribute trust model for efficient collaborative routing. *Ann. Oper. Res.*, *277*, 293-310. https://doi.org/10.1007/s10479-018-2864-5

[21] Han, G., Miao, X., Wang, H., Guizani, M., & Zhang, W. (2019). CPSLP: A Cloud-Based Scheme for Protecting Source-Location Privacy in Wireless Sensor Networks Using Multi-Sinks. *IEEE Transactions on Vehicular Technology*, 1-1. https://doi.org/10.1109/TVT.2019.2891127

[22] Wang, N., Fu, J., Li, J., & Bhargava, B. K. (2019). Source Location Privacy Protection based on Anonymity Cloud in Wireless Sensor Networks. *IEEE Transact ions on Information Forensics and Security*, 1-1. https://doi.org/10.1109/tifs.2019.2919388.

[23] Wang, N. & Zeng. J. (2017) All-Direction Random Routing for Source-Location Privacy Protecting against Parasitic Sensor Networks. *Sensors*, *17*(3), 614. https://doi.org/10.3390/s17030614

[24] Arivarasi, A. & Ramesh, P. (2021). An improved source location privacy protection using adaptive trust sector-based authentication with honey encryption algorithm in WSN. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-021-03021-2

Contact information

A. ARIVARASI, M.E., Research scholar
(Corresponding author)
Department of EEE,
University College of engineering, Anna University,
Ramanathapuram, Tamilnadu, India
E-mail: arivarasi.ece@gmail.com

P. RAMESH, M.E., Phd, Assistant professor
Department of EEE, University College of Engineering, Anna University,
Ramanathapuram, Tamilnadu, India
E-mail: ramesh2905@gmail.com