SN Computer Science (2023) 4:219
https://doi.org/10.1007/s42979-022-01647-3

ORIGINAL RESEARCH

A Survey Paper: An Energy and Secure Aware Routing Protocol for Wireless Sensor Network

M Asharani[1] · H R Roopashree[1]

Received: 3 November 2022 / Accepted: 17 December 2022 / Published online: 17 February 2023

Abstract
Wireless Sensor Network (WSN) is an emerging technology which can contain large number of sensor nodes used to collect process and transmit the psychical or environmental information in various type of applications like medical, military, etc. The data security in the wireless network is most important factor which must be considered when designing the routing protocol for data transmission. Some of the conventional routing protocols presented the secure data transmission which failed to consider the energy consumption. One of the most difficult tasks when building a routing model for a wireless sensor network is energy efficiency (WSN). Different energy-efficient routing strategies are created to move data packets across cluster heads (CH) in a safe way; however, in a WSN context, extending network life and maintaining high scalability pose a challenging task.

Keywords Energy efficiency · Routing protocol · Security · Wireless sensor network

Introduction

Wireless Sensor Network (WSN) is a self-controlled wireless communication system which has more number of sensor nodes with low-priced and more capabilities of data collection, processing, and transmission speed [1–3]. Used sensor nodes to gather the data and which is transmitted to the base station for the data processing through the WSN path [4, 5]. Every individual sensor node has four important blocks which are a sensor block, a transceiver block, a processor block, and a battery unit [6]. Finding a reliable path for data transmission in a network is a technique called routing. That means, the routing protocols give set of rules to the way of communication between two nodes which is most important aspect in the WSN. In recent years, the routing protocols are designed based on the low-energy consumption [7, 8]. The scalability and energy efficiency are key aspect for the design of WSN: the clustering-based routing protocol presents low power consumption and scalability to the network [9]. Security is one of the significant requirement of the WSN application which must be consisted when designing of the routing protocol, but the routing protocol designing is mainly focused on the performance not for security [10, 11]. The attacker can attack the WSN system to perform the malicious activity. Some of main attack are Worm hole Attack, Black hole Attack, Denial of Service Attack, Distributed denials of service attack, and byzantine Attack. The attack in the WSN is classified into two types such as active attack and passive attack. An attacker attacks the particular network and tries to make change in data are denoted as active attack. An attacker attacks a network and tries to learn about data and makes use of data is denoted as passive attack. A block hole attack and wormhole attack are the some type of active attacks [12–14]. The secure routing protocol and the cryptography algorithm are used to prevent the WSN system from the attacker [15] (Fig. 1).

In both commercial and military applications, wireless sensor networks (WSNs), a new subset of wireless networks, are quickly gaining recognition. To monitor changes in the environment or the state of physical objects, a wireless sensor network (WSN) is a wireless network made up of

This article is part of the topical collection “Advances in Computational Approaches for Image Processing, Wireless Networks, Cloud Applications and Network Security” guest edited by P. Raviraj, Maode Ma and Roopashree H R.

✉ M Asharani
asharanim@gsss.edu.in

H R Roopashree
roopashreehr@gsss.edu.in

[1] Department of CSE, GSSSIETW, Mysuru, Karnataka 570016, India

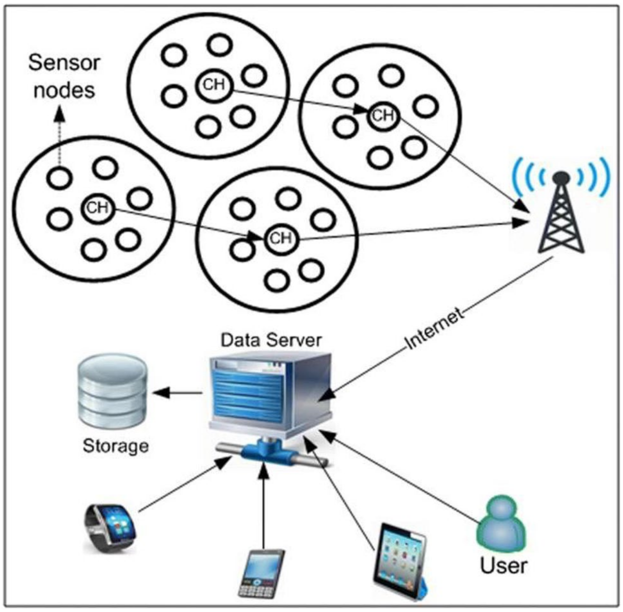

Fig. 1 WSN architecture

scattered independent sensor devices. A WSN is made up of an interconnected system of tiny sensor nodes that can interact and share data. These nodes gather environmental information like pressure, humidity, temperature, or pollution levels and transmit it to a base station. The latter sends the information to a wired network, sets off an alarm, or initiates an action depending on the type and volume of data being observed. Typical applications include monitoring weather and forests, battle surveillance, physical environmental conditions, tracking animal and human movement in woods and along borders, and pollution detection. Wireless local area networks and they both employ the same transmission medium, which is air (WLANs). The key distinction is that sensors, unlike devices connected to local area networks, have a relatively limited energy source, typically a battery, which depletes quickly. Therefore, it becomes necessary to create new MAC protocols that are energy conscious. Since a WSN has fewer resources than a typical WLAN, there is little doubt that the two are different. Common uses include weather and forest monitoring, battlefield.

Literature Survey

Tamilarasi and Santhi [16] presented wormhole attack detection with secure path detection using Particle Swarm Optimization algorithm (PSO) in the wireless sensor network. The author presented the path detection in tree step of process: in the first step, the author calculated the 'K' paths from source to using the ad hoc on demand multi-path distance vector protocol to reach the destination. In second step, wormhole path was determined by changing the feedback data and detection data from the end station node which is identified by the source node. Finally, the PSO algorithm is used to detect the optimal path to the secure data transmission. However, the routes generated by the PSO were considered only the energy; it failed to consider the distance.

Ahutu and El-Ocla [17] developed the MAC Centralized Routing Protocol (MCRP) to reduce the energy consumption of the nodes. The routing path identification and observation over the network topology were achieved using the high-energy BS in MCRP. The wormhole attacks were effectively detected by implementing the centralized network intelligence in the MCRP. However, the nodes in the network were consumed more energy during the initialization phase.

Aliady et al. [18] Ad-hoc On-Demand distance Vector (AODV) protocol proposed energy-saving solution to identify wormhole attack in WSN. The author described a two-step, energy-efficient solution for detecting wormhole attacks that are based on a connection between two nodes or nearby pieces of information. The sensor nodes are attached to the data transmission line that has been chosen in the first stage. The protocol is relieved from testing a later stage in the second step when a stage is passed. The proposed AODV successfully detected wormholes with 100% accuracy. However, the AODV's performance was examined in a static setting.

Mythili et al. [19] proposed Spatial and Energy Aware Trusted Dynamic Distance Source Routing (SEAT-DSR) protocol to increase the life time of the network, throughput, packet delivery radio and focus on the reduction of end-to-end delay while data transmission in WSN. Moreover, the standard clustering algorithm and the new hierarchical trust mechanism are used in this work. This work improved the packet transfer rate of the data transmission in WSN using the SEAT-DSR algorithm. The communication range of the proposed method is 50 m which is one of the advantage of the system. However, the average packet transmission rate of the SEAT-DSR was less, because the malicious nodes exist in the network.

A secure cluster-based routing protocol (SCBRP) was developed which presented the secure energy-efficient transmission in the Wireless Sensor Networks [20]. The SCBRP technique uses the firefly algorithm-based adaptive particle swarm optimisation in the wireless communication between source and the destination. To address energy-efficient-based clustering, safe routing, and security verification, the author divided this proposed work into three categories. In the first step, the multi-objective-based PSO algorithm used to cluster the sensor node. In the second step, the data encryption, shortest path identification, and data integrity are the processes used to achieve the secure routing. The fuzzy logic approach is verified the security level. This proposed method reduced the encryption time and decryption time. However, the SCBRP technique does not analyse under large-scale environment.

One of the most challenging issues when developing a routing model for a wireless sensor network is energy efficiency (WSN) [21]. Although a range of energy-efficient routing algorithms are meant to be used to carry data packets across cluster heads (CH), maintaining high scalability and extending network life in a wireless sensor network (WSN) environment are difficult undertakings. Data packets are distributed to the destination using the suggested Exponentially Ant Lion Whale Optimization (E-ALWO) technique, resulting in an energy-efficient and trust-based routing architecture. The E-ALWO approach, on the other hand, was developed by fusing the idea of an exponentially weighted moving average (EWMA) with the algorithms for ant lion optimization (ALO) and whale optimization (WOA). On the other hand, a routing path finding algorithm was necessary.

The most important considerations for the effective design of protocols to provide multi-hop safe routing in Wireless Sensor Networks are lifetime optimization based on minimal energy usage and security (WSN) [22]. In this study, we put forth the Secured Quality of Service (QoS) aware Energy Efficient Routing Protocol, a brand-new routing protocol. This protocol is designed to increase WSN security while also utilising the most energy possible. It is based on trust and energy modelling. In the proposed work, a key-based security mechanism and an authentication technique are used to establish trust ratings. To increase communication security, three separate trust scores—direct, indirect, and overall—are computed. This paper also proposes a cluster-based secure routing method where the cluster head is selected for cluster-based safe routing based on QoS measurements and trust scores. The secure routing method has been successfully finished by choosing the final path based on path-trust, energy, and hop count. In spite of this, disregard the secure routing protocol.

Tiny sensor nodes make comprise a wireless sensor network (WSN) [23]. The use of WSN in various fields has greatly increased during the past few years. The restricted processing capabilities of the sensor nodes and the security concerns of data transmission in the WSN limit the scope of WSN applications. Numerous algorithms using nature-inspired optimization have been developed to address the issues of energy efficiency and security in WSN (NIO). In the proposed work, two NIO algorithms designed to achieve energy efficiency and security in WSN are tested against two opportunistic routing algorithms, namely the Intelligent Opportunistic Routing Protocol (IOP) and Trust-based Secure Intelligent Opportunistic Routing Protocol (TBSIOP). Nevertheless, ignoring the identification of safe routing protocol and node attack.

Effective connectivity with the data collecting centre and dependable data exchange between numerous sensors are the main problems with WSN [24]. Clustering is the most effective tactic for increasing WSN performance metrics. An efficient WSN solution is required to get around the clustering algorithms' drawbacks, such as lower cluster head (CH) lifetime. For this, an effective CH selection method, an optimised routing protocol, and trust management are necessary. It is recommended that a fuzzy type-2 logic-based clustering algorithm and the Cuckoo search optimization approach be used together to maximise the level of trust and, consequently, the network lifetime. A multi-hop routing approach and an intra-cluster communication method based on thresholds are also utilised to lessen the amount of energy lost from CHs that are far from the base station. Have to put your attention on locating secure routing protocols and attack-free routes.

For these uses, numerous algorithms and methods have been developed, but trust-based algorithms surpass traditional methods [25]. Data integrity, authenticity, and availability are all provided by a trust technique, which offers the highest level of security. Data overhead is a problem that arises when using the trust-based approach and causes other problems like congestion in the system. Additionally, it directly impacts the data aggregation process. As a result of these combined effects, the network's overall lifetime is significantly decreased. To resolve the issue, this paper suggests using the RSAR protocol, short for realisable secure aware routing. The calculation of each sensor node's trust factor initiates the RSAR. Then, using the conditional tug of war optimisation technique, the values are estimated using the best trust inference model.

Rapid advancements in inter-node communication techniques have been made possible by wireless sensor networks [26]. They are made out of sensor nodes that can sense, communicate, and compute. Routing algorithms will take measures to route the data from a node if it is unable to send data to the base station from a particular node in a WSN. To manage data routing in a clustered WSN, the suggested work deals with a routing algorithm based on trust awareness and compression sensing data. Compressed sensing is typically used for data aggregation when the overhead of the sensor nodes is low. Numerous nature-inspired optimization techniques aim to achieve a balance between the quantity of messages delivered, the number of hops, the transmission distance, and the best trusted path.

Unmanned underwater vehicle systems (UWVS) are a new technology being used to explore underwater resources [27]. Due to the vulnerability of the UWSNs’ ecosystem to various security assaults, security is a crucial component. SEECR, a secure, energy-efficient, and cooperative routing strategy for UWSNs, is suggested by this study. SEECR is equipped with powerful and energy-efficient defence mechanisms to fend off attacks in an underwater setting. SEECR uses cooperative routing to improve network performance.

To keep SEECR acceptable for underwater environments, minimum computation is used for security implementation when considering the resource-constrained UWSNs' environment. In this study, the performance of SEECR is compared to that of AMCTD, a well-known routing protocol for UWSNs that stands for Adaptive Mobility of Courier Nodes in Threshold-optimised DBR.

Routing protocols (RPs) do not take into account node states during transmissions, such as a node's lifetime or network congestion [28]. Given that each node requires a certain amount of energy to route or transmit information, node lifetime is crucial. However, QoS (Quality of Services) can increase network lifetimes, particularly in multi-path routing information selections. This research suggests the EHO-ETQRP multi-path routing protocol for Internet of Things-based WSNs, which is both energy-efficient and ideal in terms of QoS awareness (Wireless Sensor Networks). The trust and energy QoS factors are the focus of this work's objective function. By calculating costs related to congestion and node lifetimes, the suggested protocol determined an ideal path for routing.

Security and energy consumption are the two main issues that wireless sensor networks (WSNs) face as a result of their characteristics of limited resources and dynamic topology [29]. Although trust-based solutions can now deal with a range of undesirable node behaviours, there are still a number of attacks, nodes that consume a lot of energy, and nodes that have a communication bottleneck. To address these issues, this study suggests a brand-new trust-based secure and energy-efficient routing protocol (TBSEER). Through adaptive direct, indirect, and energy trust values, TBSEER determines the comprehensive trust value, which can withstand attacks from black holes, selective forwarding, sinkholes, and hello floods. Additionally, the malicious nodes are quickly identified using the volatilization factor and adaptive penalty mechanism. Moreover identifiying the malicious node is a challenging need more secure routing protocol for choosing optimizes node for data transfer. Additionally, to further cut down on energy usage from repetitive calculations, the nodes only need to calculate the direct trust value, while the Sink determines the indirect trust value. The cluster heads then use the comprehensive trust value to determine which multihop paths are the safest, actively avoiding wormhole attacks. According to the simulation results, the suggested TBSEER decreases network energy usage, expedites the detection of rogue nodes, and defends against all common assaults.

Due to its extensive use in practical applications, the scientific community is giving the spread of technology in wireless sensor networks a lot of attention [30]. It has become a significant technological advancement with great promise, because it gives users useful data about a particular area with the aid of real-time sensing. Due to their constraints in resources and infrastructure-less deployment, wireless sensor networks present a variety of issues that may affect how well the system operates. For the improvement of WSNs, which is still a herculean endeavour, the most difficult concerns, like energy conservation, Consideration must be given to proper cluster head selection, secure data transit, and network lifetime extension. This research presents the energy-efficient trusted moth flame optimization clustering technique, which is secure and energy conscious. Utilising moth flame optimization, the most deserving, trustworthy head node is selected using the clustered WSN framework. The fitness function in eeTMFO/GA is assessed in accordance with five crucial factors, providing direct trust measures such as average transmission time, elected node residual energy, connected node density, average cluster distance, and packet forwarding progress. Simulation findings have demonstrated a significant improvement in energy conservation and network stability period enhancement for eeTMFO/GA when compared to the present clustering schemes, as well as when compared to the LEACH protocol and the HEED protocol (Table 1).

Challenges in WSN

The main issue with sensor networks is security. Most applications in the real world use wireless sensor networks (WSNs). WSNs are subject to several insider and outsider attack, and it can be difficult to recognise and defend against insider attacks. The clustered WSNs are typically threatened by an insider attack, in which the attackers pick a few received data packets to discard. The unmanaged clustered environments in the network are to blame for this issue. This study suggests a reliable and secure routing system for choosing the node and protecting the data packet for WSNs to solve this issue. Both approaches rely on active trust to defend against various routing-related attacks.

Open Challenges

- The nodes in the network were consumed more energy; maintaining Energy in node is the biggest challenge in wireless sensor networks.
- The PSO's route-generating algorithm only took into account energy-related variables; it ignored node distance.
- The AODV's performance in the static environment was examined. The network's dynamic changes were unable to identify a secure routing path.
- Due to the presence of malicious nodes in the network, the SEAT-average DSR's packet transmission rate was lower. In order to secure the network and improve network performance, malicious nodes need to be detected.

Table 1 Comparative studies for protocol and techniques used in wireless sensor networks

References	Name of the author	Protocols/algorithms	Techniques	Shortcomings
[1]	S. V. N. Santhosh Kumar and Yogesh Palanichamy	S-SELDRIP	Hop to hop secure optimal routing authentication used	Attack identification and energy- efficiency not focused
[2]	Lein Harn, Ching-Fang Hsu, Ou Ruan, andMao-Yuan Zhang	A novel design for securing routing protocol for two communicating end devices	Secure routing path is find using authentication	Energy efficiency not focused
[3]	Sarita Agrawal, Manik Lal Das	TPIV	Node capture attack can be detected using TPIV protocol in an distributed WSN	Energy efficiency and secure path identification not focused
[4]	YongjunSun, Wenxin Dong, and Yahuan Chen	Ant colony algorithm	Minimises the average energy utilisation and prolong the life cycle of the wireless sensor nodes	Secure route identification and attacks not focused
[5]	Mohammad Wazid1 and Ashok Kumar Da	Efficient group-based technique	Multiple black hole attacks can be detected and prevented	Energy efficiency not focused
[6]	Navjot Sidhu Monika Sachdeva	–	Efficient attack detection and prevention	Energy efficiency not focused
[7]	Suyambu Karthick	Trust-distrust protocol	Secure routing pat is determined using Grade points	Energy efficiency not focused
[8]	Deepak C. Mehetre, S. Emalda Roslin, Sanjeev J. Wagh	Trustable and secure routing scheme	Secure routing path is determined	Node attack not focused
[9]	Khalid Haseeb, Kamalrulnizam Abu Bakar, Abdul Hanan Abdullah, Tasneem Darwish	AECR protocol used to improve the energy efficiency	Improves energy conservation	Secureroute identification and attacks not focused
[10]	Huda A. Babaeer and Saad A. Al-Ahmadi	Efficient energy threshold sensitive sensor network protocol	Consumesless energy	Secureroute identification not focused

- However, the SCBRP technique does not analyse under large-scale environment.
- To find the routing path, an optimization algorithm is required.

Conclusion

This study examines the many methods for delivering Energy and Secure Aware Routing Protocol for Wireless Sensor Networks, and also discusses the difficulties and approaches of various methods. The challenges related to various methods that maintain an Energy and Secure Aware Routing Protocol for Wireless Sensor Networks are also explained in this study, which is helpful for researchers. This research does a thorough analysis of energy efficiency and security routing techniques. Additionally, numerous strategies and protocols linked to finding secure routing protocols, optimising energy usage, and methods to examine security-related problems have been explored.

Funding No funding was received from any organization.

Data availability Data regarding the Reseach results are available from the corresponding author at reasonable request.

Declarations

Conflicts of interest On behalf of all the authors, the corresponding author states that there is no conflicts of Interest.

References

1. Kumar SS, Palanichamy Y. Energy efficient and secured distributed data dissemination using hop by hop authentication in WSN. Wireless Netw. 2018;24(4):1343–60.
2. Harn L, Hsu CF, Ruan O, Zhang MY. Novel design of secure end-to-end routing protocol in wireless sensor networks. IEEE Sens J. 2015;16(6):1779–85.
3. Agrawal S, Das ML, Lopez J. Detection of node capture attack in wireless sensor networks. IEEE Syst J. 2018;13(1):238–47.
4. Sun Y, Dong W, Chen Y. An improved routing algorithm based on ant colony optimization in wireless sensor networks. IEEE Commun Lett. 2017;21(6):1317–20.
5. Wazid M, Das AK. A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks. Wireless Pers Commun. 2017;94(3):1165–91.
6. Sidhu N, Sachdeva M. Impact analysis of network layer attacks in real-time wireless sensor network testbed. Int J Adv Comput Sci Appl. 2020;11(8):701–10.
7. Karthick S. TDP: a novel secure and energy aware routing protocol for wireless sensor networks. Int J Intell Eng Syst. 2018;11(2):76–84.
8. Mehetre DC, Roslin SE, Wagh SJ. Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust. Clust Comput. 2019;22(1):1313–28.
9. Haseeb K, Bakar KA, Abdullah AH, Darwish T. Adaptive energy aware cluster-based routing protocol for wireless sensor networks. Wireless Netw. 2017;23(6):1953–66.
10. Babaeer HA, Al-Ahmadi SA. Efficient and secure data transmission and sinkhole detection in a multi-clustering wireless sensor network based on homomorphic encryption and watermarking. IEEE Access. 2020;8:92098–109.
11. Kumar MH, Mohanraj V, Suresh Y, Senthilkumar J, Nagalalli G. Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in WSN. J Ambient Intell Hum Comput. 2020. https://doi.org/10.1007/s12652-020-02007-w.
12. Malik S, Sharma DAK. Detection and isolation technique for blackhole attack in wireless sensor network. Int J Comput Eng Tech. 2018;9(1):66–73.
13. Upadhyay R, Bhatt UR, Tripathi H. DDOS attack aware DSR routing protocol in WSN. Procedia Comput Sci. 2016;78:68–74.
14. Liu Y, Dong M, Ota K, Liu A. ActiveTrust: Secure and trustable routing in wireless sensor networks. IEEE Trans Inf Forensics Secur. 2016;11(9):2013–27.
15. Das AK, Chaki R, Dey KN. Secure energy efficient routing protocol for wireless sensor network. Foundations Comput Decis Sci. 2016;41(1):3–27.
16. Tamilarasi N, Santhi SG. Detection of wormhole attack and secure path selection in wireless sensor network. Wireless Pers Commun. 2020;114(1):329–45.
17. Ahutu OR, El-Ocla H. Centralized routing protocol for detecting wormhole attacks in wireless sensor networks. IEEE Access. 2020;8:63270–82.
18. Aliady WA, Al-Ahmadi SA. Energy preserving secure measure against wormhole attack in wireless sensor networks. IEEE Access. 2019;7:84132–41.
19. Mythili V, Suresh A, Devasagayam MM, Dhanasekaran R. SEAT-DSR: Spatial and energy aware trusted dynamic distance source routing algorithm for secure data communications in wireless sensor networks. Cogn Syst Res. 2019;58:143–55.
20. Pavani M, Rao PT. Adaptive PSO with optimised firefly algorithms for secure cluster-based routing in wireless sensor networks. IET Wireless Sens Syst. 2019;9(5):274–83.
21. SureshKumar K, Vimala P. Energy efficient routing protocol using exponentially- ant lion whale optimization algorithm in wireless sensor networks. Comput Netw. 2021;197(2021):108250 (**Elsevier**).
22. Kalidoss T, Logambigai R, Kulothungan K, Ganapathy S, Arputharaj K. QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks Springer Science+Business Media, LLC, part of Springer Nature; 2019.
23. Bangotra DK, Singh Y, Kumar N, Singh PK, Ojeniyi A. Energy-efficient and secure opportunistic routing protocol for wsn: performance analysis with nature-inspired algorithms and its application in biomedical applications 25 March 2022.
24. Mittal N, Singh S, Singh U, Salgotra R. Trust-aware energy-efficient stable clustering approach using fuzzy type-2 Cuckoo search optimization algorithm for wireless sensor networks. Springer Science+Business Media, LLC, part of Springer Nature; 2020.
25. Basha AR. Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network. IET Wireless Sens Syst. 2020. https://doi.org/10.1049/iet-wss.2019.0178.
26. Anand JV. Trust-value based wireless sensor network using compressed sensing. J Electron Info. 2020;2(2):88–95.
27. Saeed K, Khalil W, Ahmed S, Ahmad I, Naeem M. SEECR: secure energy efficient and cooperative routing protocol for underwater wireless sensor networks. IEEE Access. 2020. https://doi.org/10.1109/ACCESS.2020.3000863.

28. Lavanya R, Shanmugapriya N. Energy efficient with trust and Qos-aware optimal multipath routing protocol based on elephant herding optimization for IOT based wireless sensor networks. Turkish J Comput Math Educ. 2021;12(9):979–90.
29. Hu H, Han Y, Yao M, Song X. Trust based secure and energy efficient routing protocol for wireless sensor networks. IEEE Access. 2021;10:10585–96.
30. Sharma R, Vashisht V, Singh U. eeTMFO/GA: a secure and energy efficient cluster head selection in wireless sensor networks. Telecommun Syst. 2020;74(3):253–68.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.