The Scientific Temper (2024) Vol. 15 (spl): 338-347
Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl.40

E-ISSN: 2231-6396, ISSN: 0976-8653
https://scientifictemper.com/

REVIEW ARTICLE

Trust and security in wireless sensor networks: A literature review of approaches for malicious node detection

A. Rukmani*, **C. Jayanthi**

Abstract

Wireless sensor networks (WSNs) are widely used in various fields such as environmental monitoring, healthcare, military applications, and smart cities. However, due to their decentralized nature, limited resources, and deployment in often hostile environments, WSNs are vulnerable to several security threats, especially malicious node attacks. Malicious nodes can disrupt network operations by dropping packets, injecting false data, or launching attacks such as sinkholes, wormholes, and Sybil attacks. To counter these threats, numerous malicious node detection methods have been proposed, ranging from trust-based models to anomaly detection techniques and clustering-based approaches. In parallel, the design of efficient routing protocols plays a critical role in ensuring energy-efficient and secure data transmission within the network. This review paper presents a comprehensive analysis of existing techniques for malicious node detection and efficient routing in WSNs

Keywords: Wireless sensor network, Malicious node, Clustering approach, Efficient routing protocol.

Introduction

WSNs have become an essential component of contemporary technological advancements, serving a vital function across a diverse range of applications, including environmental monitoring, healthcare, and industrial automation. WSNs are comprised of a collection of diminutive, self-governing devices known as sensor nodes. These nodes are equipped with sensors, microcontrollers, and wireless communication capabilities. The aforementioned nodes engage in cooperative efforts to gather, analyze, and send data originating from the tangible realm to a central hub or other interconnected nodes within the network.

PG and Research Department of Computer Science, Government Arts College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli – 24), Karur – 5, Tamil Nadu, India.

***Corresponding Author:** Author, PG and Research Department of Computer Science, Government Arts College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli – 24), Karur – 5, Tamil Nadu, India, E-Mail: eswarruby@gmail.com

How to cite this article: Rukmani, A., Jayanthi, C. (2024). Trust and security in wireless sensor networks: A literature review of approaches for malicious node detection. The Scientific Temper, **15**(spl):338-347.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl.40

Source of support: Nil

Conflict of interest: None.

The origins of WSNs may be traced back to the early 1980s, during which wireless sensor systems were initially created by the U.S. military for the purpose of battlefield monitoring. During the latter part of the 1990s, WSNs garnered considerable interest within academic and scientific circles, resulting in notable progress and developments in the field. The proliferation of low-power microcontrollers and wireless communication technologies, such as Zigbee and Bluetooth, expedited the advancement of WSNs during the 2000s.

background study

WSNs consist of several key components that work together to enable the collection, processing, and transmission of data from the physical world to a central point or other nodes within the network.

WSN key components

The key components work together to form a functional WSN, allowing data to be collected from various sensors distributed across a geographical area, processed locally, and transmitted to a central point or external systems for further analysis and decision-making. The design and optimization of these components are critical to the overall performance, energy efficiency, and longevity of the WSN.

Sensor nodes

Sensor nodes serve as the core components of a WSN. Every sensor node is a compact, self-governing device that is outfitted with a diverse range of sensors for the purpose

© *The Scientific Temper. 2024*

Received: 08/09/2024 **Accepted:** 18/09/2024 **Published**: 16/10/2024

of gathering data from the surrounding environment. The sensors have the capability to quantify many characteristics such as temperature, humidity, light intensity, sound levels, motion, and more variables. Sensor nodes exhibit a range of dimensions and intricacies, spanning from rudimentary, economical nodes to sophisticated counterparts equipped with several sensors and processing functionalities.

Microcontrollers (MCUs) or processors

Microcontrollers are embedded computing units within sensor nodes that provide the necessary processing power. They are responsible for collecting data from sensors, performing computations, making decisions based on the collected data, and managing node operation. Low-power microcontrollers are commonly used in WSNs to conserve energy and extend the node's operational lifetime.

Wireless communication module

The wireless communication module enables sensor nodes to transmit and receive data wirelessly within the network. Various wireless communication technologies are used in WSNs, including Zigbee, Bluetooth, Wi-Fi, LoRa (Long Range), and cellular communication.

The choice of communication technology depends on factors such as range, data rate, energy efficiency, and deployment requirements.

Power sources

Sensor nodes in WSNs require a power source to operate. Common power sources include batteries, energy harvesting systems, and energy scavenging mechanisms. Batteries are the most straightforward power source but may need periodic replacement or recharging, making energy-efficient operation crucial in WSN design. Energy harvesting systems capture energy from the environment, such as solar panels, piezoelectric generators, or thermoelectric generators, to power the nodes. Energy scavenging involves harvesting small amounts of energy from sources like radiofrequency signals or vibrations.

Data processing and storage

Sensor nodes frequently possess restricted processing and storage capacities as a result of their physical dimensions and energy limitations. Data processing on nodes can include filtering, aggregation, and compression of sensor data to reduce communication overhead and conserve energy. Onboard memory is used for storing collected data, configuration settings, and temporary storage before data transmission.

Gateway or sink node

The gateway or sink node acts as a central point in the WSN where data from multiple sensor nodes is collected, aggregated, and forwarded to an external network. It typically has more resources than sensor nodes, including greater processing power, storage capacity, and a more reliable power source. The gateway may also serve as a bridge between the WSN and the internet or other communication networks.

Architectures of WSN

WSN architecture plays a critical role in defining how sensor nodes communicate, collaborate, and achieve the network's objectives.

Flat architecture

In a flat architecture, all sensor nodes communicate directly with a central node, often referred to as the sink or base station. Simple and easy to implement. Suitable for small-scale networks or applications with low traffic. Minimal communication overhead as data flows directly to the sink. Low complexity, making it cost-effective for simple applications. Limited scalability as the sink node can become a bottleneck in large networks. Vulnerable to node failures, as losing the sink node can disrupt the entire network.

Hierarchical architecture

In a hierarchical architecture, sensor nodes are organized into a hierarchy with different levels or tiers, often referred to as clusters. Nodes are grouped into clusters, each with a leader or cluster head. Cluster heads communicate with a higher-level coordinator or sink node. Improved scalability as nodes communicate with their cluster heads rather than directly with the sink. Energy efficiency can be enhanced as cluster heads perform data aggregation and can enter sleep modes. Complex to manage and maintain, as it requires cluster formation, cluster head selection, and routing protocols. Overhead is associated with communication between cluster heads and the sink.

Mesh architecture

In a mesh architecture, sensor nodes can communicate with multiple neighboring nodes, forming a self-organizing, multi-hop network. Each node may act as a relay, forwarding data to other nodes in the network. Nodes can dynamically adjust their routes based on network conditions. Robust and fault-tolerant, as multiple communication paths exist. Scalable for large networks with proper routing protocols. Increased communication overhead due to multi-hop routing. Complexity in managing routing algorithms and addressing.

Data-Centric Architecture

Data-centric architectures focus on the efficient retrieval of specific data types rather than node-centric communication. Data is given a specific name or attribute. Nodes advertise their data, and other nodes request data by specifying attributes. Energy-efficient, as only relevant data is transmitted. Supports in-network data processing and aggregation. Requires a naming and discovery mechanism, which adds complexity. May not be suitable for all types of applications.

Mobile WSN architecture

In mobile WSNs, sensor nodes are attached to mobile platforms, such as robots or drones. Mobility adds a dynamic element to network topology. Nodes can adapt to changing environmental conditions or target areas of interest. Enhanced coverage and adaptability for monitoring and data collection. Suitable for applications like search and rescue, precision agriculture, and surveillance. Increased energy consumption due to mobility. Complex path planning and coordination are required.

Communication Protocols of WSN

Communication protocols are essential in WSNs to facilitate efficient and reliable data exchange among sensor nodes. These protocols govern how data is transmitted, received, and managed within the network.

Medium access control (MAC) protocols

MAC protocols regulate access to the shared wireless medium and coordinate when nodes can transmit data.

- Carrier sense multiple access with collision avoidance (CSMA/CA): Nodes listen for a clear channel before attempting to transmit, reducing collisions.
- Time division multiple access (TDMA): Nodes are assigned specific time slots for data transmission to avoid interference.
- Slotted ALOHA: Nodes transmit data within predefined time slots to minimize collisions. The choice of MAC protocol depends on factors like network size, traffic patterns, and energy efficiency requirements.

Routing protocols

Routing protocols play a crucial role in the identification of the optimal path for transmitting data packets from the source nodes to the destination nodes within a specified network. Proactive protocols, which are alternatively referred to as table-driven protocols, include the establishment and upkeep of routing tables within individual nodes. In the absence of data transfer, it is important to perform periodic changes of the routing tables in order to comply with these protocols. Two examples of proactive protocols commonly used in networking are optimized link state routing (OLSR) and destination-sequenced distance vector (DSDV). Reactive protocols, alternatively referred to as on-demand protocols, utilize a route discovery technique that is activated solely when there is a requirement to transfer data. The utilization of this approach successfully mitigates the control overhead that is typically associated with protocols such as AODV and DSR. Hybrid protocols are strategically devised to attain an equilibrium between control overhead and route stability through the incorporation of elements derived from both proactive and reactive procedures. Routing protocols consider multiple factors, such as energy efficiency, variations in network topology, and route reliability, among others.

Transport layer protocols

Transport layer protocols ensure reliable end-to-end data delivery in WSNs.

- *User datagram protocol (UDP)*

Lightweight, connectionless protocol suitable for applications where some data loss is acceptable (e.g., real-time data streaming).

- *Transmission control protocol (TCP)*

Reliable, connection-oriented protocol that ensures data integrity and order (rarely used in WSNs due to overhead).

- *Real-time transport protocol (RTP)*

Used for real-time multimedia streaming applications. The choice of transport layer protocol depends on the application's reliability and latency requirements.

Application layer protocols

Application layer protocols define how applications interact with the network and exchange data.

- *Message queuing telemetry transport (MQTT)*

Publish-subscribe protocol for efficient communication between sensors and applications.

- *Constrained application protocol (CoAP)*

Designed for resource-constrained devices, enabling RESTful communication over the Internet.

- *Hypertext transfer protocol (HTTP)*

Used for web-based communication with WSNs. Application layer protocols facilitate data retrieval, command execution, and interaction with external systems.

Security protocols

Security protocols protect WSNs from unauthorized access, data tampering, and eavesdropping. Security mechanisms in WSNs include encryption, authentication, and intrusion detection. Key management protocols help distribute encryption keys securely. Security in WSNs is crucial, especially in applications like healthcare, military, and industrial control systems.

Time-synchronization protocols

Time-synchronization protocols ensure that sensor nodes maintain a consistent sense of time, which is critical for tasks like data fusion and event coordination. Protocols like flooding time synchronization protocol (FTSP) and reference broadcast synchronization (RBS) synchronize nodes' clocks efficiently.

Literature Review of WSNS

The authors put forth a novel routing method that leverages blockchain technology and reinforcement learning algorithms in order to enhance the security and efficiency of routing in WSNs. The present study presents a viable routing system that is designed to acquire routing information of routing nodes on the blockchain. This method ensures that the routing information remains traceable and resistant to any type of tampering. The utilization of reinforcement learning models facilitates the dynamic selection of routing links by routing nodes, with the aim of enhancing trustworthiness and efficiency. Based on the empirical findings, the researchers observed that the routing scheme exhibits favorable delay performance in a routing environment containing 50% malevolent nodes when compared to alternative routing algorithms Yang, J., *et al*. (2019).

The author has put forth a novel secure routing protocol for WSNs in the context of the existence of malicious nodes. The protocol takes into account relevant information, such as the trust value and status, for each relay node along the route. The trust value is determined by the likelihood of a node being targeted by an attack based on its past packet-forwarding behaviors. On the other hand, the status metric is a combination of the remaining energy level and the distance to the sink node. Hence, the route produced by the protocol exhibits resistance against malevolent attacks and is globally optimal based on the relevant information. The researchers employed an enhanced iteration of the Dijkstra algorithm to compute the secure path for WSNs when confronted with the existence of malevolent nodes Shi, Q., *et al*. (2019).

The present study proposes a revolutionary secure routing protocol based on multi-objective ant-colony-optimization (SRPMA) that is specifically tailored for WSNs. The ant colony method has been modified to operate as a multi-objective routing algorithm. This enhancement considers two optimization targets, namely, the residual energy of nodes and the trust value of a route path. The method constructs a route path by incorporating multiple pheromone information and multiple heuristic information, both of which consist of two-goal functions. The node trust evaluation model is established by employing an upgraded D-S evidence theory and confliction preprocessing techniques to evaluate the level of confidence in nodes, Sun, Z., *et al*. (2019).

The authors introduced a novel routing algorithm, referred to as the energy aware trust based secure routing algorithm. The algorithm incorporates trust score evaluation to efficiently identify malicious users within WSNs, Selvi, M., *et al*. (2019).

Underwater wireless sensor networks (UWSNs). UWSNs are vulnerable to many security threats and malicious attacks due to the constraints imposed by the open acoustic channel, the harsh underwater environment, and the distinctive characteristics of these networks. This paper provides a comprehensive examination of the hazards, challenges, and security concerns associated with UWSNs. Moreover, the present study aims to investigate the challenges and security concerns associated with UWSNs by an analysis of prior research and established security methodologies. Moreover, this study investigates and analyzes the current state of security researchers and their methodologies, Yang, G., *et al*. (2019).

The study introduced a novel technique called the ant colony optimization based QoS aware energy balancing secure routing (QEBSR) algorithm, designed specifically for WSNs. This study introduces improved algorithms for calculating the end-to-end delay of transmission and assessing the reliability of nodes along the routing path, Rathee, M., *et al*. (2019).

The authors presented a routing approach for WSNs that ensures security, trustworthiness, and energy efficiency. The suggested methodology uses fuzzy logic as a means to derive trust values for the routes. Subsequently, the selection of the quickest path from the source to the destination was made, taking into account factors related to trustworthiness and security, Beheshtiasl, A., & Ghaffari, A. (2019).

The authors introduced a novel secure cluster-based routing protocol (SCBRP) that integrates adaptive particle swarm optimization (PSO) with enhanced firefly algorithms. This protocol aims to enhance the efficiency of data transfer inside a WSN while ensuring security, Pavani, M., & Rao, P. T. (2019).

This research presented a novel WSN framework, referred to as E2SDRSNF, comprising three distinct components that have been proposed. algorithm 1, as presented, generates a minimum connected dominating Set (MCDS) that serves as the foundation for constructing a virtual backbone to facilitate energy-efficient inter-cluster routing. The transmission of data occurs through the identified virtual backbone nodes to the base station, facilitated by cluster heads that are determined using the suggested algorithm 2. The signcryption technique that has been presented is employed for the purpose of ensuring secure communication within WSNs, Maitra, T., Barman, S., & Giri, D. (2019).

The domains of study pertaining to energy consumption and secure transmission in WSN applications are currently experiencing significant growth. The utilization of heterogeneous WSNs is a very effective network approach wherein sensor nodes possess varying levels of processing capabilities, memory capacities, and transmission capacities. To ensure efficient transmission within this network, the implementation of clustering in conjunction with secure routing enables the secure transit of data packets to their intended destination. The process of data collection and clustering plays a crucial role in effectively organizing network elements and managing the transmission overhead associated with data transfer. The utilization of a hybridization approach, combining the K-means clustering algorithm with the ant lion optimizer, is employed to achieve improved energy efficiency through the grouping of nodes and optimal selection of cluster heads. Therefore, the integration of miscegenation of ant lion optimizer into the K-means algorithm for clustering and the proposed concept involves the utilization of a spherical grid framework to facilitate the representation and analysis of several interconnected curves. The MALOKSER protocol is designed to facilitate efficient clustering and safe routing of data packets in a timely manner to the base station, utilizing elliptic curve cryptography. The primary objective of this study is to improve network security and energy efficiency in wireless network communication systems. The utilization of elliptic curve cryptography in conjunction with spherical grid multi-tier routing ensures the attainment of safe transmission by employing the encryption of messages using two distinct keys and afterward forwarding the packets in a spherical structure, Dhand, G., & Tyagi, S. S. (2019).

The proposed approach is formulated based on the authentication and encryption model (ATE). The eligibility weight function (EWF) is employed to identify the sensor guard nodes, which are subsequently concealed using a complicated symmetric key technique. A determination has been reached to undertake the development of a secure hybrid routing protocol by incorporating the attributes of both multipath optimized link state routing (OLSR) and Ad hoc on-demand multipath distance vector (AOMDV) protocols, Deebak, B. D., & Al-Turjman, F. (2020).

In this research, a novel routing protocol named secured quality of service (QoS) aware energy-efficient routing protocol is introduced. This protocol is developed with a focus on trust and energy modeling in order to enhance the security of WSNs and optimize energy utilization. The trust modeling employed in this study utilizes an authentication technique that incorporates a key-based security mechanism to generate trust scores. Furthermore, this study calculates three distinct trust scores, specifically direct trust score, indirect trust score, and overall trust score, with the aim of improving the security of communication. Furthermore, this study introduces a safe routing method that operates on a cluster-based approach. The selection of the cluster head is determined by evaluating QoS metrics and trust ratings, ensuring secure routing within the cluster, Kalidoss, T., *et al*. (2020).

The author presented a technique called adaptive source location privacy preservation technique utilizing randomized routes (ASLPP-RR) in order to improve routing mechanisms. The execution of the secure data aggregation based on the principle component analysis (SDA-PCA) method is carried out with a focus on maintaining end-to-end security and integrity. In order to get more effective results in comparison to existing approaches, a thorough evaluation of the protection of sensitive information is undertaken, Babu, M. V., *et al*. (2021).

A proposed routing system is presented that integrates deep blockchain with Markov decision processes (MDPs) to improve the security and efficiency of routing in WSNs. The suggested methodology employs a proof of authority (PoA) method within the blockchain network to verify the transmission of the node. The selection of the validation group required for the process of proofing is accomplished by the utilization of a deep learning approach that prioritizes the examination of the characteristics associated with each individual node. Markov decision processes (MDPs) are subsequently employed to select the optimal next hop, which serves as a forwarding node with the ability to transmit messages in a straightforward and secure manner, Abd El-Moghith, I. A., & Darwish, S. M. (2021).

In this study, a trust management scheme known as the lightweight trust management scheme (LTMS) is introduced. The LTMS is designed to mitigate internal threats and is based on the principles of binomial distribution. The proposed research introduces a multidimensional secure clustered routing (MSCR) method in hierarchical WSNs, Fang, W., *et al*. (2021).

The objective of this research paper is to introduce a routing protocol for WSNs called secure and energy-aware heuristic-based routing (SEHR). The primary goal of SEHR is to enhance the security of WSNs by detecting and preventing the compromise of data while also ensuring efficient performance. The proposed procedure utilizes a heuristic analysis based on artificial intelligence to establish a dependable and intellectually rigorous learning framework. Furthermore, it serves the purpose of safeguarding transmissions from potential adversaries, hence ensuring security while minimizing complexity. Additionally, the technique for maintaining routes is accomplished by the utilization of traffic exploration in order to mitigate link failures and network dis-connectivity, Haseeb, K., *et al*. (2020).

The proposed protocol is SEECR, which stands for Secure Energy Efficient and Cooperative Routing, designed specifically for UWSNs. The SEECR system is composed of energy-efficient components and a robust defense mechanism designed to effectively counteract attacks in underwater environments. The SEECR framework leverages cooperative routing techniques to improve network performance. In the resource-constrained context of UWSNs, the implementation of security measures must prioritize minimal computation. This ensures that the secure and energy-efficient communication protocol for underwater environments (SEECR) remains acceptable for use in these conditions. This study aims to assess the efficacy of SEECR by conducting a comparative analysis of its performance against AMCTD, a widely recognized routing protocol for the UWSN environment, Saeed, K., *et al*. (2020).

The author devised a highly effective routing algorithm that utilizes multiple attributes to ensure secure information transmission in WSNs. The research presented in this study aims to improve the energy efficiency and performance of network systems compared to existing routing algorithms, such as the multi-attribute pheromone ant secure routing algorithm based on reputation value and ant-colony optimization algorithm. The present study aims to enhance the security of the network environment by employing advanced detection approaches that use nodes' heightened coincidence rates. These techniques are utilized to identify and mitigate hostile behavior through the application of a trust calculation algorithm. The technique incorporates several QoS parameters, including the dependability rate, the elapsed time required to identify impersonation attempts and the stability rate for trust-related attacks. These parameters are used to execute a proficient assessment of the trustworthiness of the nodes involved in communication, Feroz Khan, A. B., & Anandharaj, G. (2021).

The proposal introduces a unique routing system called the trust-based secure intelligent opportunistic Routing system (TBSIOP). The protocol being examined leverages three distinct characteristics of WSNs to compute the probability (Pm) of a node being identified as malicious. The trust computation involves the utilization of attributes such as sincerity in data packet forwarding (Fs), sincerity in acknowledgment (ACKs), and energy depletion (Ed). The relay selection mechanism employed in the proposed protocol demonstrates a proficient approach in mitigating the selection of malicious nodes as relay nodes, as evidenced by the computation of the trust factor. The protocol being examined is deployed on the list of forwarder nodes that is generated by the Intelligent Opportunistic Routing Protocol, Bangotra, D. K., *et al*. (2022).

The authors put forth a complete trust management system (GDTMS) for F-IWSN, which is based on a Gaussian distribution. The suggested trade-off entails the efficient selection of a relay node that is both secure and robust. Specifically, this involves the implementation of a secure routing method based on trust management. Furthermore, the offered strategies can also be employed to mitigate the impact of defamatory attacks, Fang, W., *et al*. (2020).

The author has introduced a novel routing protocol, known as trust-based secure and energy efficient routing (TBSEER), as a potential solution to address the aforementioned issues. The TBSEER algorithm computes the complete trust value by incorporating adaptive direct trust value, indirect trust value, and energy trust value. This approach effectively mitigates the energy consumption associated with iterative computations. Ultimately, the cluster heads ascertain the most secure multi-hop pathways by utilizing the comprehensive trust value, so effectively circumventing any wormhole attacks, Hu, H., *et al*. (2021).

The authors focused on the design and simulation of the AODV routing hardware chip, utilizing the VHDL programming language in the Xilinx integrated synthesis environment (ISE) 14.7 software. The investigation focuses on evaluating the chip's performance by analyzing several hardware characteristics of the field-programmable gate array (FPGA), including slices, lookup tables (LUTs), input/output blocks (IOB), flip-flops, and memory. This analysis is conducted for different network configurations, denoted as N = 10, 20,..., 100. The estimation of delay and frequency is also performed on the Virtex-5 FPGA, Gupta, N., *et al*. (2022).

The authors presented a secure routing approach that draws inspiration from biological systems, namely utilizing bee algorithms. The routing system being proposed encompasses two significant metrics, namely, the primary scout bee and the secondary scout bee. These metrics are responsible for facilitating the routing and security mechanisms. In numerous cases, it offers enhanced data efficiency along with security. In this study, three types of routing attacks, including flood attack, spoof attack, and Sybil attack, are employed to assess the effectiveness of the suggested approach. The ultimate decision about the implementation of this technology is to establish a safe routing path for transmitting messages within a WSN setting, Raghav, R. S., Thirugnansambandam, K., & Anguraj, D. K. (2020).

In this study, a novel hierarchical routing protocol called LEACH-TM is introduced. This protocol is designed to enhance trust management and energy efficiency in wireless networks. In order to mitigate internal assaults, the LEACH-TM protocol has a trust management strategy, Fang, W., *et al*. (2021).

The author has put out a proposition for a monitoring and routing protocol that integrates Artificial Intelligence into an Authentication and Encryption Model. The analysis conducted on the proposed work demonstrates its superior efficiency in comparison to alternative routing and monitoring approaches, Bhalaji, N. (2020).

The authors introduced a novel algorithm, known as the particle-based spider monkey optimization (P-SMO), which aims to efficiently determine the ideal route for secure communication management in WSNs. Consequently, the network is simulated and the selection of cluster heads (CHs) is determined by the efficient learning automata-based cell clustering algorithm (ELACCA), resulting in the establishment of the routing path based on the selected CHs, Khot, P. S., & Naik, U. L. (2022).

The authors introduced a system known as realisable secure aware routing (RSAR) in order to tackle the aforementioned concern. The RSAR methodology was implemented as a method to address this particular difficulty. The RSAR procedure is initiated by calculating the trust factor for each individual sensor node. The values are calculated using an optimal trust inference model that employs the conditional tug-of-war optimization technique. The practice of data aggregation facilitates the decrease of immediate data transmission from individual nodes to multi-hop networks. The process involves the deliberate selection and retention of pertinent data, which is then delivered to the recipient as consolidated information, Raja Basha, A. (2020).

The authors introduced a novel algorithm named energy-aware trust and opportunity-based routing (ETOR), which integrates a distinctive hybrid fitness function. The algorithm consists of two main stages: The initial stage entails the selection of secure nodes utilizing a tolerance constant, while the subsequent stage entails the selection of opportunistic nodes from the secure nodes for routing purposes, Hajiee, M., Fartash, M., & Eraghi, N. O. (2021).

The authors presented a novel approach, referred to as the distributed secure unequal cluster-based multipath routing protocol (USCDRP), which aims to promote energy efficiency, security, and reliability in routing protocols. The USCDRP, which is an improved version of the SCMRP, offers a certain level of security. The technology given in this study demonstrates a high level of reliability, energy efficiency, and an extended operational lifespan. In addition, a standalone clustering technique is offered to eliminate isolated nodes and a cluster maintenance plan is implemented to improve the longevity of the network, Vijayalakshmi, V., & Senthilkumar, A. (2020).

In this study, a safe routing algorithm called particle-water wave optimization (P-WWO) is proposed as an efficient and optimal method for routing data packets over secure paths. The P-WWO algorithm is formulated by the integration of particle swarm optimization (PSO) and water wave optimization (WWO) techniques, Khot, P. S., & Naik, U. (2021).

The authors introduced a novel lightweight multi-hop routing protocol designed specifically for 802.15.4 WSNs. The primary objectives of this protocol are to minimize energy usage and effectively detect wormhole attacks. The superiority of the MAC centralized routing protocol (MCRP) over other comparable protocols has been demonstrated through simulation results, Ahutu, O. R., & El-Ocla, H. (2020).

The research community has addressed the challenges and limitations in the design of mobile WSNs (MWSNs) by proposing efficient routing protocols. These protocols aim to optimize specific performance metrics, including residual energy utilization, mobility, topology, scalability, localization, data collection routing, and quality of service (QoS). Furthermore, the incorporation of mobility in WSNs has presented novel complexities pertaining to routing protocols, network stability, security mechanisms, and overall system reliability. Hence, this study presents a thorough and detailed examination of the routing protocols and security concerns within the framework of MWSNs, which have emerged in recent years, Al-Nasser, A., Almesaeed, R., & Al-Junaid, H. (2021).

The author presented a novel protocol, namely the secure load-balanced routing (SLBR) protocol, which utilizes WSNs to facilitate efficient routing in the context of disaster management. The protocol under consideration comprises a logical clustering methodology and a streamlined key management mechanism, Palani, U., Amuthavalli, G., & Alamelumangai, V. (2020).

The proposed solution entails the utilization of a hybrid star and tree structure to provide secure data aggregation. In this scenario, the network is partitioned into four distinct geographical segments, each of which exhibits a stable star configuration. The SHSDA approach employs a secure hybrid structure for data aggregation, wherein each node is allocated a parent node to facilitate data transmission. In order to enhance data security, the implementation of lightweight symmetric encryption is employed, whereby a key is distributed between every parent node and its respective offspring. The encrypted data is transmitted from the leaf nodes to the parent nodes, and subsequently propagates towards the root node in a star-shaped architecture, Naghibi, M., & Barati, H. (2021).

The proposed methodology presented a hierarchical routing and data aggregation strategy for WSNs. The proposed methodology entails the application of network clustering, whereby specific nodes are assigned as cluster heads. The creation of a tree structure among the backbone-tree nodes occurs when establishing a rendezvous zone and selecting backbone nodes. The aggregated data is delivered to the sink through the utilization of backbone-tree nodes and cluster heads. Within the present framework, there are two discernible modalities of data transmission: Sharifi, S. S., & Barati, H. (2021).

The integration of Monarch butterfly optimization in cat swarm optimization, known as Monarch-cat swarm optimization (M-CSO), was presented as a hybrid optimization technique for WSNs. The framework functions based on two fundamental elements: the first involves the identification of secure nodes, while the second entails the selection of opportunistic nodes from the pool of safe nodes. The process of selecting secure nodes using the tolerance constant relies on the evaluation of trust, connection, and QoS characteristics. The initial two criteria are of a direct nature, but for QoS, the factors taken into account to define it are link life time and latency. Furthermore, the selection of opportunistic nodes is efficiently carried out using the suggested multi-objective crow search optimization

(M-CSO) algorithm, which takes into consideration the fitness characteristics of trust, distance, latency, and connection, Patil, P. A., Deshpande, R. S., & Mane, P. B. (2020).

The authors presented a proposed trust-aware secure routing protocol (TSRP) for WSN, designed to mitigate various types of attacks. Initially, it is imperative for each node to compute the comprehensive trust values of its neighboring nodes. This computation is based on various factors, including the direct trust value, indirect trust value, volatilization factor, and residual energy. The purpose of this computation is to provide a robust defense mechanism against potential attacks such as black hole attacks, selective forwarding attacks, wormhole attacks, hello flood attacks, and sinkhole attacks. Furthermore, in a multipath mode, each source node that requires data transmission initiates the forwarding of a routing request packet to its neighboring nodes. This process is repeated until the packet reaches the sink node at the termination point. Ultimately, the sink determines the most favorable route by evaluating the trustworthiness of the path, the distance of transmission, and the number of intermediate hops through an analysis of the received packets, Hu, H., *et al*. (2021).

In this study, a novel energy optimization safe routing strategy is proposed for Internet of Things (IoT) applications in heterogeneous WSNs. The suggested strategy aims to build a secure routing mechanism for the transmission of secret data in the IoT environment, Nagaraju R., *et al*. (2022).

This study offered a comprehensive overview of the WSN infrastructure and the associated security concerns it encounters, so serving as a valuable resource for researchers and practitioners in the field. The text also examines the potential advantages of employing machine learning algorithms to mitigate the security expenses associated with WSN across various domains. Furthermore, it addresses the obstacles encountered and suggests potential remedies for enhancing the sensors' capacity to detect threats, attacks, risks, and malicious nodes by leveraging machine learning algorithms for autonomous learning and development, Ahmad, R., Wazirali, R., & Abu-Ain, T. (2022).

The present study provided a description of Diffusion approaches for safe routing, a data-centric internet-based protocol. This protocol represents a new routing protocol that has been developed with the aim of mitigating potential threats and attacks within the routing infrastructure. Consequently, it is being examined from a security perspective to identify any associated vulnerabilities or concerns. The protocol in question is implemented within wireless sensor nodes, namely within the context of WSN. The present study focuses on the use of the interest distribution mechanism, examining three distinct categories of attacks: denial of service attacks, routing information alteration and spoofing, and data dumping or selective forwarding. The implementation of link layer encryption can potentially limit external assaults, while preventing compromised nodes within the network presents a more challenging task. The researchers reached the conclusion that manipulating or falsifying the data, as necessary, will provide a resolution to the aforementioned dilemma. The direct diffusion (DD) routing protocol facilitates communication between sink and source nodes in networks characterized by random and mesh topologies. The routing protocol employed in this context adopts a data-centric approach, wherein intermediate nodes perform data aggregation and thereafter transmit the aggregated data to a designated sink node, Ganesh, E. N. (2022).

Future Research

- *Hybrid trust models for robust security*

Future research can explore the integration of trust-based models with advanced machine learning techniques, such as reinforcement learning or deep learning, to enhance the detection of malicious nodes WSNs. Hybrid trust models can improve the accuracy and adaptability of trust-based routing protocols, such as the trust-aware secure routing Protocol (TSRP). By leveraging real-time data and historical patterns, these models can be more efficient in mitigating attacks like black hole, wormhole, and sinkhole attacks, especially in dynamic and large-scale networks.

- *Energy-efficient and secure routing protocols*

Designing energy-efficient routing protocols for heterogeneous WSNs in IoT environments remains a key challenge. Future studies should focus on multi-objective optimization techniques that balance energy consumption, security, and data transmission efficiency. Routing protocols can incorporate energy harvesting technologies and adaptive routing strategies to extend the lifetime of WSNs while ensuring secure data transmission.

- *Machine learning-enhanced intrusion detection systems (IDS)*

Research can further investigate the application of lightweight machine learning algorithms in intrusion detection systems. The use of advanced algorithms like ADASYN with CNNs or feature selection methods like CSA-IDS can enhance the detection rate of intrusion systems. Developing IDS that are resource-efficient and scalable for large WSNs, particularly in IoT applications, will be a key focus.

REFERENCES

Abd El-Moghith, I. A., & Darwish, S. M. (2021). Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach. *IEEE Access*, 9, 103822–103834. https://doi.org/10.1109/ACCESS.2021.3100265

Ahmad, R., Wazirali, R., & Abu-Ain, T. (2022). Machine learning for wireless sensor networks security: An overview of challenges and issues. *Sensors*, 22(13), 4730. https://doi.org/10.3390/

s22134730

Ahutu, O. R., & El-Ocla, H. (2020). Centralized routing protocol for detecting wormhole attacks in wireless sensor networks. *IEEE Access*, 8, 63270–63282. https://doi.org/10.1109/ACCESS.2020.2984169

Al-Nasser, A., Almesaeed, R., & Al-Junaid, H. (2021). A comprehensive survey on routing and security in mobile wireless sensor networks. *International Journal of Electronics and Telecommunications*, 67(4), 483–496. https://doi.org/10.24425/ijet.2021.135953

Babu, M. V., et al. (2021). An improved IDAF-FIT clustering based ASLPP-RR routing with secure data aggregation in wireless sensor network. *Mobile Networks and Applications*, 26, 1059–1067. https://doi.org/10.1007/s11036-020-01636-8

Bangotra, D. K., et al. (2022). A trust based secure intelligent opportunistic routing protocol for wireless sensor networks. *Wireless Personal Communications*, 127(2), 1045–1066. https://doi.org/10.1007/s11277-022-09314-0

Beheshtiasl, A., & Ghaffari, A. (2019). Secure and trust-aware routing scheme in wireless sensor networks. *Wireless Personal Communications*, 107, 1799–1814. https://doi.org/10.1007/s11277-019-06466-7

Bhalaji, N. (2020). A novel hybrid routing algorithm with two fish approach in wireless sensor networks. *Journal of Trends in Computer Science and Smart Technology (TCSST)*, 2(3), 134–140. https://doi.org/10.32604/tcsst.2020.021131

Deebak, B. D., & Al-Turjman, F. (2020). A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks. *Ad Hoc Networks*, 97, 102022. https://doi.org/10.1016/j.adhoc.2019.102022

Dhand, G., & Tyagi, S. S. (2019). SMEER: Secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks. *Wireless Personal Communications*, 105, 17–35. https://doi.org/10.1007/s11277-019-06139-5

Fang, W., et al. (2020). TMSRS: Trust management-based secure routing scheme in industrial wireless sensor network with fog computing. *Wireless Networks*, 26, 3169–3182. https://doi.org/10.1007/s11276-019-02236-2.

Fang, W., et al. (2021). MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, 2021(1), 1–20. https://doi.org/10.1186/s13638-021-01954-5

Fang, W., et al. (2021). Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. *Digital Communications and Networks*, 7(4), 470–478. https://doi.org/10.1016/j.dcan.2021.01.001

Feroz Khan, A. B., & Anandharaj, G. (2021). A cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT. *Wireless Personal Communications*, 119(4), 3149–3159. https://doi.org/10.1007/s11277-021-08482-1

Ganesh, E. N. (2022). Analysis of wireless sensor networks through secure routing protocols using directed diffusion methods. *International Journal of Wireless Network Security*, 7(1), 28–35. https://doi.org/10.26483/ijw.2022.0301

Gupta, N., et al. (2022). Performance analysis of AODV routing for wireless sensor network in FPGA hardware. *Computer Systems Science & Engineering*, 40(3), 303–310. https://doi.org/10.32604/csse.2022.019332

Hajiee, M., Fartash, M., & Eraghi, N. O. (2021). An energy-aware trust and opportunity based routing algorithm in wireless sensor networks using multipath routes technique. *Neural Processing Letters*, 53(4), 2829–2852. https://doi.org/10.1007/s11063-020-10421-1

Haseeb, K., et al. (2020). Secure and energy-aware heuristic routing protocol for wireless sensor network. *IEEE Access*, 8, 163962–163974. https://doi.org/10.1109/ACCESS.2020.3019535

Hu, H., et al. (2021). Trust based secure and energy efficient routing protocol for wireless sensor networks. *IEEE Access*, 10, 10585–10596. https://doi.org/10.1109/ACCESS.2021.3050736

Hu, H., et al. (2021). Trust-aware secure routing protocol for wireless sensor networks. *ETRI Journal*, 43(4), 674–683. https://doi.org/10.4218/etrij.2020-0097

Kalidoss, T., et al. (2020). QoS aware trust based routing algorithm for wireless sensor networks. *Wireless Personal Communications*, 110, 1637–1658. https://doi.org/10.1007/s11277-019-06885-4

Khot, P. S., & Naik, U. (2021). Particle-water wave optimization for secure routing in wireless sensor network using cluster head selection. *Wireless Personal Communications*, 119, 2405–2429. https://doi.org/10.1007/s11277-021-08486-x

Khot, P. S., & Naik, U. L. (2022). Cellular automata-based optimised routing for secure data transmission in wireless sensor networks. *Journal of Experimental & Theoretical Artificial Intelligence*, 34(3), 431–449. https://doi.org/10.1080/0952813X.2021.1983409

Maitra, T., Barman, S., & Giri, D. (2019). Cluster-based energy efficient secure routing in wireless sensor networks. In Information Technology and Applied Mathematics: ICITAM 2017 (pp. 25–35). *Springer Singapore*. https://doi.org/10.1007/978-981-13-1645-3_3

Nagaraju, R., et al. (2022). Secure routing-based energy optimization for IoT application with heterogeneous wireless sensor networks. *Energies*, 15(13), 4777. https://doi.org/10.3390/en15134777

Naghibi, M., & Barati, H. (2021). SHSDA: Secure hybrid structure data aggregation method in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, 12(12), 10769–10788. https://doi.org/10.1007/s12652-021-03161-y

Palani, U., Amuthavalli, G., & Alamelumangai, V. (2020). Secure and load-balanced routing protocol in wireless sensor network for disaster management. *IET Information Security*, 14(5), 513–520. https://doi.org/10.1049/iet-ifs.2020.0014

Patil, P. A., Deshpande, R. S., & Mane, P. B. (2020). Trust and opportunity based routing framework in wireless sensor network using hybrid optimization algorithm. *Wireless Personal Communications*, 115, 415–437. https://doi.org/10.1007/s11277-020-07455-x

Pavani, M., & Rao, P. T. (2019). Adaptive PSO with optimised firefly algorithms for secure cluster-based routing in wireless sensor networks. *IET Wireless Sensor Systems*, 9(5), 274–283. https://doi.org/10.1049/iet-wss.2018.5088

Raghav, R. S., Thirugnansambandam, K., & Anguraj, D. K. (2020). Beeware routing scheme for detecting network layer attacks in wireless sensor networks. *Wireless Personal Communications*, 112(4), 2439–2459. https://doi.org/10.1007/s11277-020-07328-3

Raja Basha, A. (2020). Energy efficient aggregation technique-based realisable secure aware routing protocol for wireless sensor network. *IET Wireless Sensor Systems*, 10(4), 166–174. https://doi.org/10.1049/iet-wss.2019.0244

Rathee, M., et al. (2019). Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. *IEEE Transactions on Engineering Management*, 68(1), 170–182. https://doi.org/10.1109/TEM.2019.2931455

Saeed, K., et al. (2020). SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks. *IEEE Access*, 8, 107419–107433. https://doi.org/10.1109/ACCESS.2020.3000584

Selvi, M., et al. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wireless Personal Communications*, 105, 1475–1490. https://doi.org/10.1007/s11277-019-06116-0

Sharifi, S. S., & Barati, H. (2021). A method for routing and data aggregating in cluster-based wireless sensor networks. *International Journal of Communication Systems*, 34(7), e4754. https://doi.org/10.1002/dac.4754

Shi, Q., et al. (2019). Information-aware secure routing in wireless sensor networks. *Sensors*, 20(1), 165. https://doi.org/10.3390/s20010165

Sun, Z., et al. (2019). Secure routing protocol based on multi-objective ant-colony optimization for wireless sensor networks. *Applied Soft Computing*, 77, 366–375. https://doi.org/10.1016/j.asoc.2019.01.017

Vijayalakshmi, V., & Senthilkumar, A. (2020). USCDRP: Unequal secure cluster-based distributed routing protocol for wireless sensor networks. *The Journal of Supercomputing*, 76, 989–1004. https://doi.org/10.1007/s11227-019-03076-7

Yang, G., et al. (2019). Challenges and security issues in underwater wireless sensor networks. *Procedia Computer Science*, 147, 210–216. https://doi.org/10.1016/j.procs.2019.01.218

Yang, J., et al. (2019). A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. *Sensors*, 19(4), 970. https://doi.org/10.3390/s19040970.