IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 4 March 2025, accepted 15 March 2025, date of publication 27 March 2025, date of current version 4 April 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3555280

SURVEY

Recent Trends in Localization, Routing, and Security for Wireless Sensor Networks

H. N. VISHWAS[1] AND T. K. RAMESH[2]
[1]Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Bengaluru 560035, India
[2]Department of Electronics and Communication Engineering, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru 560035, India
Corresponding author: H. N. Vishwas (hn_vishwas@blr.amrita.edu)

ABSTRACT Wireless sensor networks (WSN) are an essential component of modern systems that enable ubiquitous sensing and data collection in a wide range of contexts, including healthcare, smart cities, and environmental monitoring. This article thoroughly covers the three pillars of WSNs i.e. localization, routing, and security along with the integration of WSN with IoT. Localization methods impact the accuracy of data and applications, which in turn influence the determination of the geographical coordinates of sensor nodes. Localization methods, such as range-based and range-free systems, influence data accuracy and energy conservation. This article will also discuss about Routing protocols, which primarily establish energy-efficient and resource-optimal communication paths between nodes in WSNs and popular routing methods like flat, hierarchical, and location-based protocols. It also measures how well they work. In addition to localization and routing, our study delves deep into the most recent security protocols and policies to secure WSNs. Data interception, network interruption, and node penetration are just a few of the many attacks that WSNs are vulnerable to, making security a top priority. Methods like authentication, encryption, and intrusion detection are the main focus points. Similarly, 6TiSCH protocols and their impact in WSN-IoT systems is also discussed. This study highlights the continuous need of improving the security, efficiency, and reliability of WSNs for IoT applications. The detailed survey on three pillars of WSN provides an insight into the existing research gaps which has to be addressed.

INDEX TERMS WSN, localization, routing, security, IoT.

I. INTRODUCTION

The proliferation of wireless communication technologies and microelectronics system has simplified the making of low-cost and energy efficient smart sensor devices. These devices are capable of monitoring air quality in, humidity, temperature, pressure, noise, vibration and motion. The information collected is then organized from the autonomous, mobile and moving sensing devices for future analysis and processing. Sensor nodes self-arrange in a network topology and have the ability to self-configure and communicate in a short range and wirelessly. A WSN is often deployed in a designated area, containing numerous such sensor nodes, which perform the data capturing and converting the information into intelligence [1]. These small devices have been incorporated into many sectors including healthcare, environmental monitoring, smart homes, and military use. With the evolution in communication technologies, the integration of sensor networks has been a key part of what is currently known as the Internet of Things (IoT). A number of different types of sensors have been embedded in IoT systems to check for environmental conditions such as light, sound, humidity, and temperature. These days, IoT paradigm is a cutting-edge innovation that allows for smart communication between everyday physical objects and autonomous gadgets. In essence, the IoT has facilitated automatic communication and collaboration among various devices, thereby enabling them to provide ubiquitous services. IoT relies heavily on sensing objects, but the technology isn't without its flaws. These include problems with power consumption, storage space, processing capacity, data management, and sharing resources. asset sharing. These constraints impede

The associate editor coordinating the review of this manuscript and approving it for publication was Ghufran Ahmed.

the development of innovative applications and intelligent systems. Therefore, people perceive effectively managing complex systems as a challenging task.

A. INTERNET OF THINGS

The IoT is a network of physical objects equipped with sensors, software, and other technologies built into them. These objects connect to each other and share data with other gadgets and systems via the global web. [2], [3]. Embedded systems, commodity sensors, real-time analytics, and machine learning have all contributed to the evolution of the situation [4]. Embedded systems, control systems, automation (including home and building automation), WSNs, and other traditional fields all play a role in making the IoT possible. IoT systems are most commonly associated in consumer markets with smart home products. These products include lighting, thermostats, security systems, cameras, and other home appliances that are elements of one or more shared ecosystems and could be remotely operated through devices which are also part of that ecosystem, like smart speakers and smartphones.

Many researchers have taken an interest in the IoT because it has evolved as a powerful paradigm for communication in the modern world [5], [6]. It can link sensors, cars, homes, and appliances to the web to share data, information, and resources. The IoT has emerged as an essential tool for healthcare and environmental monitoring. For instance, we can monitor ambient variables by deploying wireless sensors in different locations [7], and we can assess the participants' physiological status by attaching wearable sensors to their bodies [6]. Using a cloud architecture, it is possible to receive this data and display it to the appropriate individuals. Similarly, an emerging area gaining significant attention in industrial IoT applications is the 6TiSCH (IPv6 over the TSCH mode of IEEE 802.15.4e) network, which is designed for low-power, reliable communication. 6TiSCH networks leverage time-synchronized mechanisms to achieve deterministic communication, making them suitable for critical industrial environments. They integrate the Time Slotted Channel Hopping (TSCH) mode defined in IEEE 802.15.4e, which enhances reliability and security by minimizing interference and mitigating multipath fading.

In addition to providing robust routing and security features, 6TiSCH networks enable efficient scheduling and resource allocation, ensuring low latency and high reliability in data transmission. These capabilities address the limitations of conventional WSN in terms of scalability, energy efficiency, and security, making 6TiSCH a promising solution for industrial IoT deployments.

B. WIRELESS SENSOR NETWORKS(WSN)

WSN are ubiquitous in nature and provide a wireless combination or interconnection of numerous sensors. The main reason for the establishment of WSN systems is that most processors are already located in appliances, cars, and machinery in factories, rather than in traditional computer systems like desktops and laptops [8]. We have already covered how the IoT is a driving force behind this. The creation of ubiquitous networks—which would include connecting the billions of embedded computer devices—with dependable wireless communications and sensing functions could open up enormous prospects in this context. In this sense, distributed WSN stand for networks of interconnected embedded sensor devices [9]. Nodes in WSNs are sensors. These days, sensors built on cutting-edge microelectromechanical system (MEMS) technology are springing up all over the place, including inexpensive multi-purpose sensors. In addition to a wireless transmitter, memory, a central processing unit, and a battery, sensors often include these components [10], [11]. There are constraints on the amount of power, data storage, processing speed, transmission distance, and bandwidth that sensors can handle. Their performance, utility, and price are defined by their features in relation to the aforementioned attributes. There are usually hundreds, if not thousands, of sensor nodes in a WSN system or network [12]. The WSN end user receives data transmitted from the network's sensor nodes, which are responsible for collecting data about the surrounding environment. Thus, WSN offers a plethora of benefits over standalone sensors, including improved accuracy, a broader range of sensing capabilities, automation of the monitoring process, and many more. This led to a wide variety of uses for these sensor nodes.

Typically, we disperse these sensors at random around the target monitoring area, instruct them to gather data, and then employ a routing mechanism to send the information to a previously established base station. However, other communication devices can access these routing channels when used for public applications like temperature monitoring. Nevertheless, it is not an effortless process to share important information through these means. Consequently, one of the most important aspects of these networks is ensuring safe data transmission and exchange. Although these networks have value in a variety of contexts, our primary concerns are precision agriculture and improving farmers' ability to keep track of and control their farms. Similarly, we utilize WSN-IoT models to monitor endangered species.

Further, we provide an overview of the commonly used protocol stack in WSN, highlighting the specific layers responsible for routing and security. Additionally, it explores emerging security techniques, such as Physical Unclonable Function (PUF)-based encryption, to address evolving security challenges in WSN.

- **Protocol Stack in WSNs:** The WSN protocol stack is typically organized into five layers: Application, Transport, Network, Data Link, and Physical Layer. Each layer serves a distinct purpose, contributing to the overall functionality and security of the network:

  ✓ **Application Layer:** Facilitates interaction with end-users by providing application-specific services

such as data formatting, processing, and network management.

- ✓ **Transport Layer:** Ensures reliable data transmission between nodes, employing protocols like UDP and TCP for end-to-end communication.
- ✓ **Network Layer:** Responsible for routing data packets across the network. In WSN, routing is a critical function due to resource constraints such as limited energy and processing power.
- ✓ **Data Link Layer:** Manages error detection, data framing, and medium access control. Protocols at this layer enhance communication reliability and energy efficiency.
- ✓ **Physical Layer:** Deals with the transmission and reception of raw data bits over wireless communication channels, ensuring signal modulation and frequency selection.

- **Routing in WSN:**Routing is primarily implemented at the Network Layer, where energy efficiency, scalability, and reliability are key considerations. One of the most widely used routing protocols in WSN is the Routing Protocol for Low-Power and Lossy Networks (RPL).
  - ✓ **RPL (Routing Protocol for Low-Power and Lossy Networks):** Operating at the Network Layer, RPL is designed for IPv6-based low-power networks, making it suitable for IoT and WSN environments. It constructs Destination Oriented Directed Acyclic Graphs (DODAGs) to establish optimal routing paths based on metrics such as link quality and energy consumption. RPL supports multiple routing topologies, including point-to-point, point-to-multipoint, and multipoint-to-point communication.
  - ✓ **6TiSCH and IEEE 802.15.4e:** In industrial IoT applications, 6TiSCH networks integrate RPL with the TSCH mode of IEEE 802.15.4e, offering time-synchronized, deterministic communication. TSCH enhances reliability by reducing interference and mitigating multipath fading, making 6TiSCH suitable for critical industrial environments.

- **Security in WSN**

Security in WSN is implemented across multiple layers, with a focus on authentication, data integrity, confidentiality, and availability. Traditional security mechanisms are often constrained by the resource limitations of sensor nodes, necessitating lightweight and efficient encryption techniques.

- ✓ **Network Layer Security:** Ensures secure routing through authentication and integrity checks, preventing attacks like sinkholes and wormholes.
- ✓ **Data Link Layer Security:** Provides data encryption and authentication mechanisms to protect against eavesdropping and tampering.
- ✓ **Physical Layer Security:** Implements techniques such as frequency hopping and spread spectrum to safeguard communication channels against jamming and interference.

In order to address emerging security challenges in WSN, Physical Unclonable Function (PUF)-based encryption is gaining attention. PUFs leverage the inherent physical variations in hardware components to generate unique cryptographic keys, offering several advantages:

- ✓ **Lightweight and Efficient:** PUF-based encryption is resource-efficient, suitable for WSN with limited computational and power capabilities.
- ✓ **High Security and Uniqueness:** Since PUFs are based on hardware-level physical characteristics, they are inherentlyresistant to cloning and tampering.
- ✓ **Enhanced Authentication:** PUFs provide robust device authentication, preventing impersonation and unauthorized access.

C. APPLICATIONS SCENARIOS TO BE ADDRESSED

1) PRECISION AGRICULTURE

WSN and IoT technologies are essential in precision agriculture because they significantly increase production and efficiency. Farmers can more precisely map nutrient levels across their fields using localization techniques, such as placing soil nutrient sensors in a precise grid pattern. This allows for targeted fertilization, which enhances crop yields and reduces expenses. In a similar vein, sensors positioned in crucial areas improve pest detection by identifying infestations' precise positions, allowing for more precise pesticide administration. In order to assist farmers in making rapid decisions, Zigbee and other routing technologies transmit weather information from remote weather stations to a central controller without decrease. Mosquito Networks help not only with the optimal allocation of resources and planning of the harvest, but also provide reliable communication of a large number of sensors to a central system which takes care of yield assessment. The protection of the data related to the agricultural activity is of great importance and is guaranteed by the use of security such as cryptography and network security to ensure no alteration is made to the sensor data. Role-based permissions and strong authentication and authorization policy controls specified on the network restrict the number of people with access to the network and thus prevent criminals and saboteurs from accessing IoT networks.

2) ENDANGERED OR INDICATOR SPECIES MONITORING

WSN and IoT technologies play an invaluable role in tracking and conserving endangered species or monitoring indicator species. The GPS collars are used to track the behaviour patterns of animals, providing data on their movements that is critical for managing ecosystems. Through strategically distributed sensors that monitor environmental conditions inside habitats, this data will be captured for the determination of robust protection plans in the habitat. This provides conservationists with information about habitat needs and threats. Multi-hop communication protocols allow data to

TABLE 1. Methods for localization and how they function.

Type	Technique	Working operation	Hardware Requirement	Attenuation	Cost
Range Based	RSSI	Measurement of signal strength	No special hardware required	High	Low
	AoA	Angle measurement	Desired	Medium	High
	ToA	Measurement of time of arrival	Desired	Low	Med
	TDoA	Time difference in propagation at different points	Required	Low	Med
Range Free	DV Hop	Sensing nodes (Heterogeneous nature) and anchor nodes	No special hardware required	High	Low
	Centroid	Transmit beaconing	No special hardware required	High	Low
	Amorphous	Computes hop distance instead of measuring linear distance	No special hardware required	High	Low

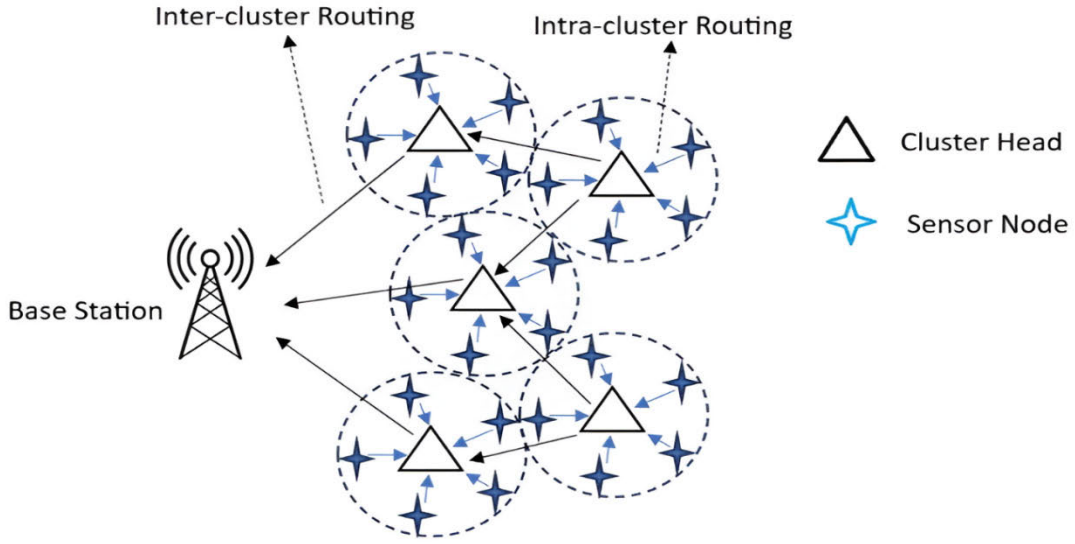

FIGURE 1. Routing in WSN.

be transmitted from remote sensors to central stations by constantly monitoring and operationally improving wildlife corridors. In order to save endangered species, poaching detection systems make use of low-latency routing protocols, which allow for the real-time sending of notifications. It is crucial to use thorough encryption methods to prevent any interceptions or misuse of data related to animal movements and habitat conditions in these monitoring systems. Intrusion detection systems ensure the constant and dependable operation of monitoring networks by monitoring for unusual activity.

Enhancing WSN and IoT applications for precision agriculture, endangered species protection and monitoring indicator species with geolocation, routing, and security features improves data accuracy, communication reliability, and information safety. These developments result in more efficient conservation efforts for endangered species and improved agricultural resource management. This study focuses on the three primary aspects of sensor networks—localization of sensor nodes, routing of these networks, and secure communication within these networks. The study is not limited to the above discussed applications. There are wide range of applications which can be benefited from this study.

D. MOTIVATION AND CONTRIBUTION

The rapid growth of the IoT has led to the widespread deployment of WSN in diverse applications, such as precision agriculture, environmental monitoring, and healthcare. However, IoT-enabled WSN face significant challenges in terms of network reliability, energy efficiency, security, and scalability. The limited computational and storage capabilities of sensor nodes, coupled with the need for low-latency data transmission, further exacerbate these issues.

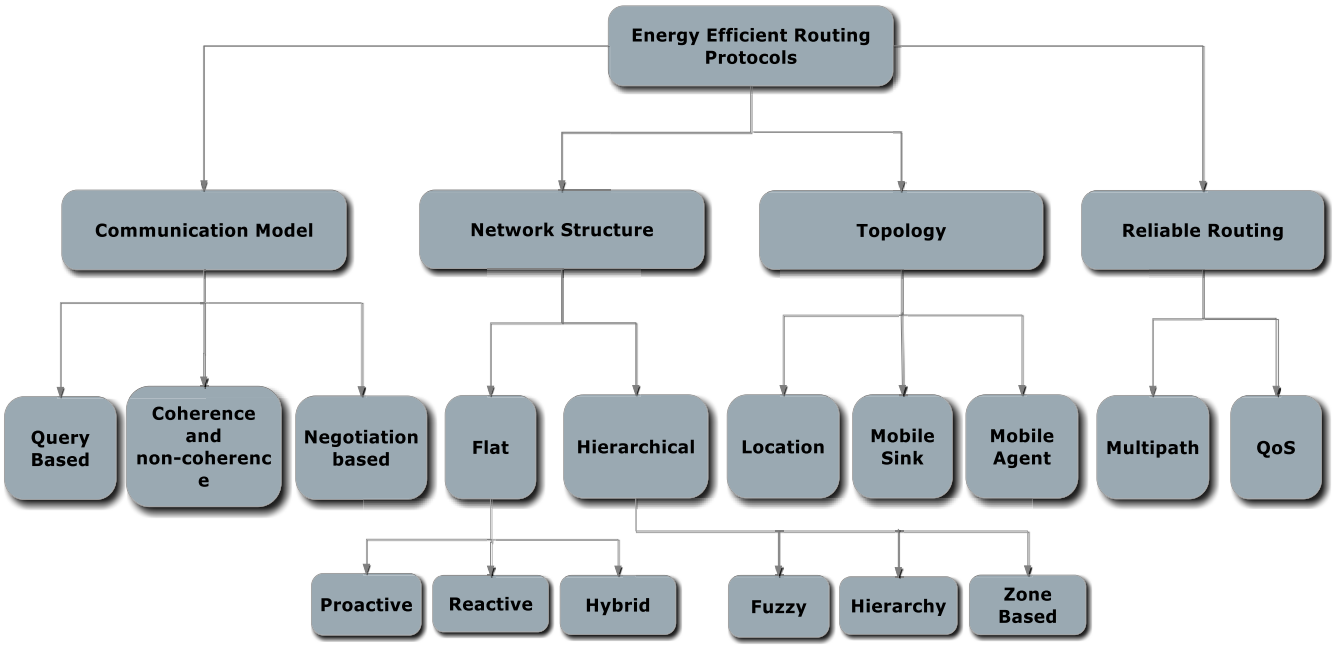

FIGURE 2. Energy aware routing protocol classification.

Moreover, conventional WSN architectures struggle to support the increasing demand for real-time data processing and decision-making, particularly in large-scale IoT deployments. The integration of cloud computing has been explored as a potential solution, but it introduces challenges related to latency, bandwidth constraints, and security vulnerabilities. This necessitates the development of novel frameworks that leverage edge computing and hybrid cloud-edge architectures to enhance the performance of IoT-enabled WSN. In this study, we focus on exploring the existing approaches of localization, routing and security enhancement in sensor networks.

E. ARTICLE ORGANIZATION

The rest of the article is organized as follows: section II presents the discussion about importance/ role of localization, routing and security aspects in WSN, section III presents literature review for localization, routing and security aspects in WSN-IoT domain, section IV presents the challenges and open issues and finally section V presents the concluding remarks.

II. ROLE OF LOCALIZATION, ROUTING AND SECURITY IN WSN

A. LOCALIZATION: OVERVIEW, IMPORTANCE AND CURRENT PROGRESS

Many of these applications depend on the precise placement of sensor nodes. This is essential for making sense of and reacting to the world around us [9]. Consider a program that the military uses to keep tabs on civilians. Here, an aircraft, such as a drone or helicopter, drops a sensor node at the target position to construct a WSN. These sensor-equipped nodes relay information about enemy movements to distant bases [10]. This analysis can inform the base station's next steps. Building a WSN entails positioning sensor nodes along a roadway, much like an intelligent transportation system. The traffic control system monitors congestion levels and modifies traffic patterns appropriately using nodes that function as sensors. The collected data can only serve the goals described above if the precise whereabouts of the events under observation are known. Accurate location data allows for automated responses to hazards like hostile vehicles or traffic jams. Nevertheless, due to the dispersed nature of sensor nodes in such systems, their precise whereabouts remain a mystery. Placing the sensors in specific locations becomes challenging in large-scale applications with challenging and difficult-to-reach areas of interest [11]. One way to find sensor nodes spread out over large networks is to employ Global Positioning Systems (GPS) [12]. Incorporating these technologies into every single sensor node raises their power consumption, physical footprint, and overall cost. The location estimations provided by these technologies are imprecise, even in heavily populated urban areas. This led to the development of several methods for localizing sensor nodes.

Only a GPS [12] module can provide the precise location data required for finding the sensor node. A GPS module's high cost and power consumption make it impossible for any sensor node to attach one. Finding the position of a node without a GPS module has been challenging. These days, there are a plethora of methods that can pinpoint the exact location of each sensor node in a WSN [13]. Two broad categories of localization algorithms exist: those that rely on range and those that do not. Some localization methods, using distance-based positioning algorithms, can infer the

TABLE 2. Routing algorithms comparison.

Routing	Classification	Data aggregation	Query based	Data delivery model	Overhead	Power usage	Scalability
SPIN	Flat	✓	✓	Event based	Minimal	Restricted	Restricted
DD	Flat	✓	✓	Demand based	Minimal	Restricted	Restricted
RR	Flat	✓	✓	Demand based	Minimal	Minimal	Favorable
GBR	Flat	✓	✓	Hybrid	Minimal	Minimal	Restricted
CADR	Flat	✓	✓	Continuous	Minimal	Restricted	Restricted
COUGAR	Flat	✓	✓	Query based	Moderate	Restricted	Restricted
ACQUIRE	Flat	✓	✓	Complex Query	Minimal	Minimal	Limited
LEACH	Hierarchical	✓	×	CH	Moderate	Moderate High	Favorable
TEEN	Hierarchical	✓	×	Active threshold	Minimal	Moderate High	Favorable
PEGASIS	Hierarchical	×	×	Chain based	Moderate	Max	Favorable
VGA	Hierarchical	✓	×	Good	High	Low	Favorable
SOP	Hierarchical	×	×	Continuous	High	Low	Favorable
GAF	Location	×	×	Virtual grid	Moderate	Restricted	Favorable
SPAN	Location	✓	×	Continuous	Moderate High	Restricted	Restricted
GEAR	Location	×	×	Demand Driven	Moderate High	Restricted	Restricted
SAR	Data centric	✓	✓	Continuous	Moderate High	High	Restricted
SPEED	Location	×	✓	Geographic	Less	Minimal	Restricted

location of unknown nodes (those without GPS modules) using physical data such as the signal strength indicator received (RSSI) [12], [13], [14], the Time of Arrival (ToA) [15], [16], and the Angle of Arrival (AoA) [12]. Implementing the range-based positioning algorithm is more expensive and energy-intensive than other methods because it requires a specific module and has better accuracy. Wi-Fi distance measuring can enhance indoor location accuracy [16]. However, there are algorithms that can generate a decent approximation as to where unknown nodes are located using only the WSN connection information. The algorithms utilized for range-free localization include the Approximation Point in Triangulation test (APIT) [19], distance vector-hop [18], and centroid [17]. You can see the inner workings of some widely used localization methods in Table 1.

B. ROUTING IN WSN

Through node-to-node communication, WSN rely on cluster heads (CH) to enable data transfer between sensors and sink nodes. After the sensor nodes get data from the CH node, BS processes the information [20]. Several sensors, smart devices, and (CHs) communicate data with a sink node, also called a data server, as seen in Figure 1. Most important is finding the best data transfer method. Changing the batteries of distant sensor nodes during emergencies is a particularly challenging task. Turning off a large number of nodes increases scheduling difficulty due to high energy usage.

In spite of their numerous advantages, WSN do have some drawbacks, including congestion, connectivity loss, security risks, and reduced QoS [21]. It is well known that the most notable drawback of WSN is the short lifespan of sensor nodes, caused by their severe energy constraints. The batteries that run sensors can never be recharged or replaced. Due to the low energy supplies of the sensor nodes, the operational lifespan of WSN quickly decreases. This has led to the disablement of the sensor node. Energy conservation is crucial for WSN to operate properly [22]. As a result, the five tiers of the sensor protocol stack necessitate less energy waste. Sensor nodes, on the other hand, mostly require power for wireless transmission, with very little power going into sensing and processing data. By improving data transfer and route design between sensors and the BS, we may reduce energy depletion in the protocol stack's network layer. Consequently, WSNs incorporate energy-saving measures into their routing algorithms to keep sensor nodes up for longer. The ability of WSN routing algorithms to detect and remove duplicate data is crucial, as neighboring sensor nodes can

TABLE 3. Network attacks and characteristics.

Attack	Characteristics	Example
Active attack	• Internal or external • Can disturb network operation	Data tampering, jamming, imposter, message replay
Passive attack	• Doesn't affect the working of network to obtain the information • Detection complexity	Traffic analysis, traffic monitoring, eavesdropping

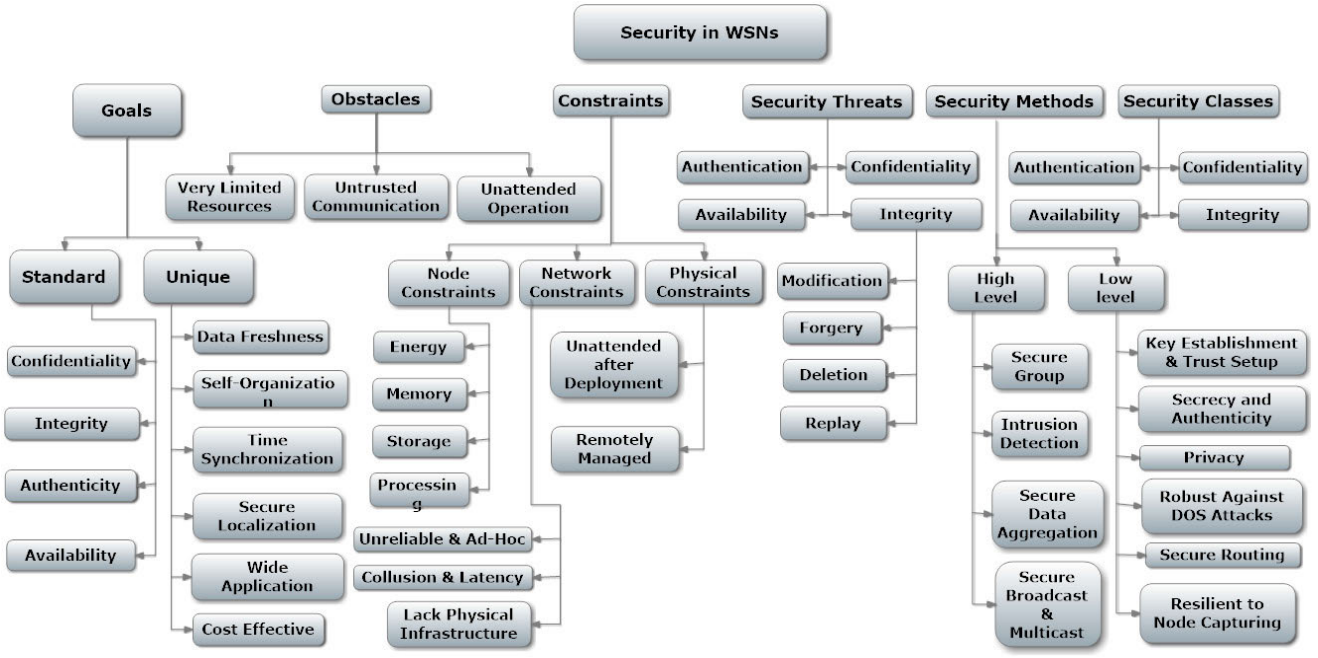

FIGURE 3. Key Components of WSN Security.

TABLE 4. Attacks on different layers of network.

Layer	Work of layer	Attacks
Application	Application interface	Worms, Trojan, Repudiation, DOS, malicious codes
Transport	End-to-end communication	Session hijacking, Flooding, DOS
Network	Routing, logical/IP addressing	Modification, flooding, Sybil, Black-hole, Grey-hole, Byzantine, sink hole, location disclosure
Data link	Flow control, error control	Traffic monitoring, DOS
Physical	Raw bit transmission	Signal jamming, interception, eavesdropping

generate comparable sensing results. WSN centralize data flow, and the absence of an IP-based structure constrains the storage and processing power of sensor nodes. Protocols that govern the routing of wired networks disregard these factors. One thing that matters to them more than anything else is QoS [23]. Hence, we advise against using them in WSN. Due to the aforementioned factors, researchers have created numerous energy-efficient routing algorithms, especially for WSNs, throughout the past 20 years [25]. Figure 2 illustrates the categorization of various energy-aware routing systems.

The challenges associated with routing in WSN have led to the development of a number of methods. These include SPIN, direct diffusion, random routing, gateway-based routing (GBR), COUGAR, ACQIRE, LEACH, TEEN-APTEEN,

TABLE 5. Attacks and their effects.

Attack/criteria	Definition of Attack	Attack techniques	Attack effects
Node outage	When nodes in a WSN fail or are compromised, it disrupts the network and all of its parts.	Physically; Logical	Node's function can be stopped; It may compromise the network and can control over entire network; It can cause several other attacks.
Link layer jamming	The link layer function is disturbed and jammed by data packets.	Estimates the probability distribution of the packets and analyze them to find the attack suitability; It can affect S-MAC, B-MAC and L-MAC protocols [1];	Packet collision occurs; Inappropriate use of resources.
Collision	Nodes communicate at the same frequency and exchange the data; Collisions are classified as Environment and probabilistic.	Modify the field of packets; Modify the ACK packet; Environmental & Probabilistic collision; Verifying and isolate radio transmissions.	Interferences; Modified packets or falsified packets; Drops the packets; Energy utilization.
Resource Exhaustion	Repeated collisions and continuous retransmission until the sensor node death.	Continuously retransmission; Interrogation attack (RTS/CTS); Message modification; Ack corruption/change;	Resources hungry; Node Compromise.
Traffic manipulation	Monitors regular transmissions but as attack occurs it modifies the traffic data, it works as MITM attack.	Analyses the communication and other related information; Misusing of WSN information; Inappropriate use of resources; Not following the communication rules of MAC; Prolonged collisions and unfairness;	Increased packet collisions; Increase in contention Reducing the network availability Increased channel resources utilization Breaches the rules of communication protocol. Inefficient use of bandwidth; Traffic distortion; Confusion.
Unfairness	It a type of Partial DoS attack where it performs other attacks such as collision and extreme resource utilization.	Sporadic use of Collison, and resource exhaustion; The improper or abusive use of a cooperative MAC-layer priority mechanism; persistent requests for channel access.	Reduced network efficiency; Unnecessary request for channel access; Decreased channel capacity.
Acknowledge spoofing	A malicious party can forge packets' link layer acknowledgements (ACKs) [10].	ACKs modification.	Inaccurate information; Selective forwarding; Packet drop.

TABLE 5. *(Continued.)* **Attacks and their effects.**

Sinkhole	A special type of selective forwarding attack; however, computational complexity is high; directing all conceivable network traffic to a hacked node by positioning an evil node closer to the base station [12] and enabling selective forwarding; diverting traffic towards the faulty node. detection complexity is very high;	Node compromise. Selective forwarding, affecting the data packet and packet drop; Altering the traffic information; Short term identity spoofing; Use of communication pattern to perform the attack.	Attracting the traffic in false direction; Inducing black hole, wormhole, eavesdropping etc. Usurp the base station's position; Message tampering; Packet drop and tampering the information; Message suppression Falsified routing information; Excessive resource utilization
Eavesdropping	Eavesdropping conversations or making attempts to access data to learn the communication packet.	Interception; Misuse of WSN transmission; Using significant support and technologies, such as effective transmitters and robust processors.	Causing other attacks such as wormhole; Access to the secret information; Reducing the confidentiality.
Impersonation	A malicious node poses as the cluster leader to trick nodes into moving to the incorrect direction; Posing as a node in the direction of the attacker's desired data flow by altering routing information or suggesting itself to other nodes as a reliable communication partner;	Reconfiguration; Access the encryption keys; Man-in-the-middle attack; Node replication [22]; False node attack; Sybil attacks; Modifying routing information; Convincing nodes;	Modify the actual routing; Inaccurate sensor reading; Network congestion Hacking secret keys Generation of false messages; Resources hungry; Degrading the network performance;

PEGASIS, and VGA. Table 2 provides a side-by-side comparison of different routing techniques. Sensors can be set up to make the most efficient use of their energy and storage capacity. Sensors do use some power at first, but that power gradually decreases as long as nodes continue exchanging data. Most of the time, people abandon the monitored area, making it impossible to repair or restore sensor nodes [26]. The failure of even a single node might render the entire network inoperable [24]. After that, we'll redistribute the data and redraw the network topology. Ad hoc WSN sensor networks will not last as long. WSN face two big problems: how to save energy and how long their networks last.

In order to enhance WSN routing, researchers are always looking for new and different approaches. Up until now, it has been challenging to establish a routing system that is energy efficient. Communication between nodes, also known as routers, constructs data transmission paths in a WSN. Several power-efficient protocols in WSN distribute the load among all nodes and minimize power consumption. Data security in the sensor network is also an important concern.

C. SECURITY PROTOCOLS IN WSN

Some of the many real-world applications made feasible by WSN include tracking forest fires, detecting threats in the military, aiding in medical and scientific research, and

TABLE 6. Localization approaches and challenges.

Paper	Algorithm/Approach	Key Features	Advantages	Challenges
Fawad et al. [1]	Enhanced DV-Hop	Uses RSSI for single-hop distance correction, modifies average hop distance, least-squares approach	Improved accuracy, reduced energy consumption	Complexity in implementation
Wajgi et al. [2]	Clustering-based Localization	Utilizes clustering for distributed computing and parallel processing	Reduced communication cost, increased throughput	Cluster formation overhead
Alfawaz et al. [3]	Modified Rat Swarm Optimizer (MRSO)	Meta-heuristic algorithm for node localization	Competitive performance, better optimization	Algorithmic complexity
Mani et al. [4]	Iterative Bounding Box with Kalman Filter	Refines position estimates, uses mobile anchor	Extends to 3D positioning, reduces GPS dependence	Requires mobile anchor, computational complexity
Mohapatra et al. [5]	CLOCK-Localization Approach (CLA)	CLOCK pattern-based sensor deployment, dual role CHs	Energy-efficient, reduced overhead	Dependence on initial CH selection
Yu et al. [6]	Modified Seagull Algorithm (DISO)	Multi-strategy optimization, chaotic mapping, levy flight	High precision, improved optimization	Complexity in algorithm design
Yadav et al. [7]	Optimized Localization Learning Algorithm (OLLA)	Combines APIT, LAEP, RANN, SPSO	High accuracy, versatile	Complexity in integrating multiple algorithms
Tagne Fute et al. [8]	FPSOTS (Improved PSO)	Uses tabu search, RSSI method, trilateration	High accuracy, fast convergence	Algorithmic and computational complexity
Tripathy et al. [9]	PSO-based Amorphous Algorithm	Reduces average hop size, localization error	Simple, cost-effective	High localization error in certain scenarios
Achroufene et al. [10]	DV + DML, DMLDV	Combines DV-hop and RSSI-based multilateration	Cost-effective, improved accuracy	Imperfections in RSSI measurements
Lee et al. [11]	PSO with RSSI	Uses RSSI for indoor localization and tracking	High accuracy for TOA, TDOA, AOA	Expensive hardware, high computational complexity
Kumar et al. [12]	Enhanced RSSI-based Technique	Dynamic correlation between distance and RSSI	Accurate, application-specific	Requires optimal communication range determination

even improving their own daily lives. In contrast, wireless networks are susceptible to attacks due to their reliance on a broadcast channel and absence of tamper resistance. As a result, a hacker can potentially exploit a sensor node, replay past messages, inject malicious packets, or intercept all traffic [27]. Protecting user privacy and authenticating nodes are the primary issues with sensor networks. Ensuring data confidentiality and facilitating safe network connectivity between sensor nodes and the base station are two primary goals of privacy-preserving security methods. It is crucial to have a strong authentication scheme in place so that unauthorized nodes cannot join WSN and get critical information [28]. Researchers have therefore devised numerous strategies for protecting WSN broadcasts. Assailants cause harm through

both passive and active means. Here are some examples and features of different types of assaults, as shown in Table 3.

Figure 3 illustrates the key components of WSN security. This includes not only the security goals, but also the problems, risks, difficulties, security approaches, and taxonomies of different secure transmission mechanisms.

Table 4 provides a hierarchical breakdown of common types of network assaults, broken down by layer: application, transport, data connection, and physical.

In addition, we provide a concise comparison of different attacks according to their definition, methodology, and effects. Table 5 summarizes this comparison analysis.

III. LITERATURE REVIEW

This section provides a high-level summary of the current approaches to WSN routing, security, and localization. The first section provides a synopsis of current localization approaches; the second section covers activities connected to routing; and the third section addresses secure communication models.

A. LOCALIZATION

Fawad et al. [1] suggested an improved DV-Hop algorithm that uses less power while still providing accurate localization, solving the problems of DV-Hop-based localization in static WSN. First, the suggested method uses the RSSI value for a specific radius to correct the single-hop distance. Then, it uses the difference between the actual and estimated distances to modify the average hop distance between unknown nodes and anchors. Lastly, it estimates the location of each unknown node using the least-squares approach.

Wajgi and Tembhurne [2] laid out the WSN and WMSN localization algorithms that rely on clustering. By arranging sensor nodes into smaller, autonomous groups, clustering provides distributed computing and parallel processing in WSN and wireless multimedia sensor networks. If clustering methods could enhance the conventional localization process, it would be a huge boon. Clustering reduces overall communication costs by dividing the network into autonomous parts. Distributed computing, another benefit of clustering, boosts network throughput.

As per Alfawaz et al. [3] finding the positions of unknown nodes using the coordinates of anchor nodes is the goal of sensor node localization, which is a major obstacle in WSN. The inadequacy of conventional localization algorithms (like GPS) for use in WSN led to the development of new localization strategies. When it comes to WSN optimization, there are a number of different meta-heuristic techniques at your disposal. A newly created algorithm, Rat Swarm Optimizer (RSO), outperforms prior meta-heuristic algorithms and produces results that are notably distinct from their predecessors. They laid out a strategy for solving the node localization issue in WSN using a modified rat swarm optimizer (MRSO).

To improve the predicted position of the unknown node, Mani et al. [4] proposed an iterative bounding box approach supplemented with a Kalman filter. Since 3D positioning is more practical and more reflective of reality, there are really several research projects underway to expand the 2D positioning algorithm in WSN to 3D. They then swapped out a lot of GPS-equipped anchors for a single mobile anchor. They considered a particular kind of wirelessly connected range-free sensor network.

Mohapatra et al. [5] created the CLOCK-Localization Approach (CLA), a topological localization method that uses less energy and makes sure that WSN will last a long time by getting rid of iterative CH selection and recurrent re-clustering. In CLA's sensor deployment approach, which is based on the CLOCK pattern, the chosen CHs serve as both CHs and vice-CHs. Lowering energy consumption and operating expenses is one of its benefits.

Yu et al. [6] They suggested a multi-strategy modified seagull algorithm as a way to improve the DV-Hop mapping algorithm (DISO) so that the non-range-ranging localization method in WSN would work better. Primarily, the technique enhances the phases that generate positioning mistakes in the standard non-ranging locating algorithm, DV-Hop. Algorithmically, the approach partitions the communication region of anchor nodes into several radii to mitigate the effect of distance on hop number. Because the distribution of the nodes is completely random, they chose the mean square error as their estimate rather than an unbiased one. They also assigned more weight to the average jump distance to mitigate the impact of the nodes' random distribution on the inaccuracy. Their second move was to use the modified seagull optimization algorithm for iterative optimization, displacing the trilateral measurement with the objective function optimization method. To fix the algorithm's flaws, they finally tweaked the seagull optimization. They seeded the seagull population with more diverse individuals via chaotic mapping. Flying seagulls, both good and bad, updating their positions, and an algorithm that can identify the optimal solution by combining levy flying and the T distribution variation technique are all for the better.

Yadav et al. [7] shown a logical interest in the localization challenge in WSN. The researchers achieved accurate node localization by employing a variety of optimization and learning strategies. They created a new algorithm called the Optimized Localization Learning Algorithm (OLLA) and tested it against several popular localization-based learning algorithms, such as APIT, LAEP, RANN, and SPSO.

Tagne Fute et al. [8] put forward an optimization-based solution to the indoor localization issue in WSN. The proposed method enhanced the effectiveness of particle swarm optimization (PSO). To speed up its convergence towards a better solution, each particle was enhanced version of PSO employs a tabu search technique to determine which local neighbor is the best. The PSO method, on the other hand, now has performance checks and limits that keep it to improving particles from the search space created by constraint analysis around a first trilateration-found solution. In order to determine the distances between sensors, the FPSOTS algorithm used the RSSI technique. In a simulation test, they compared

the FPSOTS method to existing optimization-based localization systems and assessed its convergence performance and localization accuracy.

Tripathy and Khilar [9] said that Amorphous localization is the most recommended localization algorithm in many application domains because it is easy to implement, has a low cost, and doesn't require any additional hardware. To determine a dumb node's location, the Amorphous algorithm considers three distinct real-world scenarios: when the node is in range of an anchor node, when it faces the opposite direction of the anchor node, and when it is not in range of an anchor node at all. Nevertheless, the amorphous method produces significant localization errors. To address these flaws, they proposed a PSO-based amorphous algorithm. The suggested technique lowers both the average hop size and localization inaccuracy of anchor nodes.

Achroufene [10] used two most common localization algorithms for determining a node's location are range-based and range-free. Unfortunately, range-based localization algorithms tend to be on the pricier side when it comes to hardware needs. Although range-free localization algorithms have lower hardware costs, they do a poor job of accurately localizing in real-world scenarios. They employed two algorithms—the more expensive range-based technique, which involves measurements of the received signal strength indicator (RSSI)—and the more straightforward range-free DV-hop algorithm to locate unknown nodes in WSN. To start, they expanded the popular multilateration algorithm with a novel localization method based on RSSI called disk-based multilateration (DML). A distance interval was actually assigned to each RSSI score. Discs indicating different distances are defined by the locations of the signal's transmitter nodes define the discs indicating different distances. Then, to make use of both forms of localization, they suggested two further algorithms, DV + DML and DMLDV, which merge the DV-hop and DML methods.

As per Lee et al. [11] to better localize targets, TOA, TDOA, and AOA outperform RSS. Nevertheless, the TOA, TDOA, and AOA all necessitate more costly instruments compared to the RSS. Moreover, the computing requirements for TOA, TDOA, and AOA are more complex than those for RSS. They used a particle swarm optimization (PSO) technique to localize and track targets indoors using the received signal strength index (RSSI) channel model.

Kumar et al. [12] improved received signal strength indicator (RSSI) method for locating unlocalized nodes with the help of anchor nodes. Among the many areas that find widespread use of WSN are environmental monitoring, healthcare, and industrial automation. Precise sensor node localization is crucial for this type of WSN application. Examining the relationship between the communication distance and the RSSI as it changed across the localization process allowed them to determine the optimal communication range for the application. Distance determination and computation are the two separate phases that make up the enhanced RSSI-based node localization approach that they suggest in their study.

B. ROUTING

Current routing strategies in this area of sensor networks are summarized in this section. The introduction section covered the classification of these routing strategies into different subcategories.

Kooshari et al. [13] devised a way to optimize the routing of WSN in order to reduce their energy consumption. Discovering the best ways to send packets while keeping sensor nodes' power consumption to a minimum is the main challenge in routing. Using Water Strider algorithms (WSA), the initial step is to group wireless sensor nodes into clusters and then choose a CH to direct the data flow. Second, after the CH transmit their packets, a mobile sink gathers them and relays them to the base station. For the mobile sink to take the shortest route between the cluster nodes, it employed ant colony optimization (ACO) techniques. In an effort to cut down on power usage, they have presented a discrete variant of the WSA method for choosing CH. They provided a more comprehensive objective function for clustering network nodes that considers error rate, energy consumption, PDR rate, and Euclidean distance. They contributed by applying energy-saving variants of the ACO algorithm to CH traversal and by creating CH traversal coding that is comparable to the TSP problem. They extended the WSN lifespan, reduced energy usage, and decreased packet error rates.

Sharma et al. [14] introduced a protocol known as ML-HSOR, an acronym for multi-level hierarchical secure and optimal routing. Optimal routing, registration, clustering, and authentication make up the four phases of the suggested ML-HSOR protocol. The base station (BS) assigns distinct identifiers to each new sensor node as part of the registration process. The base station (BS) employed adaptive weighting and a Markov model to select the optimal node to serve as the cluster head (CH) during the clustering stage. This enhanced both the lifespan and performance of the network. In order to identify potentially dangerous nodes, the authentication process employs a multi-level trust evaluation. Prior to selecting the most efficient data transmission route, they encrypted the combined message and timestamp using the PL-COA technique, which is based on polarity learning.

Vellela and Balamanigandan [15] came up with a number of routing protocols to determine the shortest path in the WSN and reduce energy usage. However, issues related to energy use and delays hampered their progress. In light of these drawbacks, they came out with a new hybrid Chimp-based Clustering Flat Routing Protocol (CbCFRP). In this concept, the chimpanzee fitness function determines the optimal data transmission method. The result was a reduction in both energy use and waiting time. In order to discover the shortest path, the clustering process first determined all the available routes.

Pedditi and Debasis [16] implied a model for a forest fire detection WSN that is energy-aware and uses an efficient clustering and routing technique. The model is based on the IoT. They have proposed a model known as the Energy Efficient Routing Protocol (EERP). In order to reduce power consumption in sensor nodes, the model reduced cluster heads' idle listening. In addition to reducing redundant data transmission, EERP limited event reporting to sensor nodes in close proximity to the source. And the model made sure that low-energy sensor nodes wouldn't become cluster leaders. EERP was able to transmit data from source nodes to the base station over multi-hop paths.

Prabhu et al. [17] demonstrated a reinforcement learning (RL)-inspired routing algorithm for WSN that takes network state into account when framing routes. They found ideal routes that minimized transmission time and increased reliability through the use of reward functions. Recognizing the significance of reward functions, they settled on three reliable ones to calculate the Q-value.

As per Gunjan et al. [18] to prevent energy holes or hot spots from forming, uneven clustering is the most energy-efficient data transmission mechanism in WSN. It adjusts the cluster size depending on the CH distance from the base station (BS). Their new protocol for WSN, GA-UCR, stands for "Genetic Algorithm-Based Unequal Clustering and Routing." CH was selected using a genetic algorithm (GA) that incorporates three fitness functions—the distance between clusters, the residual energy of CH nodes, and the distance between CH and BS/sink. They employ GA for inter-cluster multi-hopping to direct the data towards BS, taking into account three fitness functions: the distance from the CH to the next hop node, the number of hops, and the residual or remaining energy of the following hop nodes.

Sheeja et al. [19] described the biggest issue with WSN is their increased energy consumption and shorter network lifetime. However, in order to transmit data to the base station (BS), the nodes use vast quantities of energy. But WSN short battery life is a problem for the network's durability. They accomplished data forwarding using an efficient routing protocol, which not only reduced energy usage but also extended the network's life. The main objective was to study a new way of routing data that uses a combination of the Black Hole algorithm (BHO) and Tuna Swarm Optimization (TSO) techniques to save energy. It handled routing in WSN well by looking at things like the number of restarts, link quality, node degree, centrality, path loss, packet drop ratio (PDR), delay, distance between sensor nodes and the CH, and the amount of energy left in the CH. The selection of CHs based on multiple objectives helped to optimize network lifetime and performance.

Sharma et al. [20] demonstrated the MHSEER protocol, which stands for safe and energy-efficient routing based on meta-heuristics. The protocol learns to forward packets depending on factors such as remaining energy, connection integrity characteristics, and the number of hops. In addition to using standard encryption methods, the protocol further encrypted the data using counter-encryption mode (CEM). In order to achieve trustworthy learning, the proposed protocol used a meta-heuristics study. There are two parts to the protocol. First, a heuristic method enhanced the choice for trustworthy data routing. They safeguarded the subsequent phase by using a computationally straightforward and arbitrary CEM.

Yang et al. [21] came up with WOAD3QN-RP, a novel intelligent routing system that mixes deep reinforcement learning with swarm intelligence techniques. Routing decisions made by conventional WSN protocols do not fully leverage all available information. This led to long communication delays, an inability to respond to changes in network topology, and a limited network lifespan. In addition to reducing delay, the WOAD3QN-RP balances energy consumption, adapts to changes in network topology, and determines the ideal multi-hop routing simultaneously, thereby extending the network's lifespan. Firstly, they used the whale optimization method (WOA) via the WOAD3QN-RP method to identify the optimal CHs. Nodes' remaining energy, distance from each other, and communication time are among the many significant parameters considered by the algorithm while choosing CHs. Because of this, the procedure was considerably more precise and efficient, which improved energy distribution and network performance. The second thing is that WOAD3QN-RP found the best multi-hop path using a dueling double deep network (D3QN). Through environmental interaction, neural networks teach smart agents how to develop energy-efficient routing policies that can adjust to changing network topologies, improve multi-hop routing performance, and maintain energy balance.

Xue et al. [22] developed k-medoids and a routing protocol for WSN called CL-HHO, which is based on the cross-layer Harris-Hawkins optimization algorithm. K-IABC, an upgraded artificial bee colony, uses less power while still facilitating good device clustering, K-IABC is an upgraded artificial bee colony. Optimizing routing and clustering in a wired network is the primary concern. To address the issue of power asymmetry in WSN, they suggested an efficient routing strategy based on many layers.

Mishra and Yadav [23] reduced power consumption per round and extended the network's lifespan. They employed nature-inspired mechanisms to minimize the network's power consumption. The Butterfly Optimization Algorithm (BOA) selects the optimal number of CH from the dense nodes that are available. Node centrality, node degree, distance from base station, distance from other nodes in the network, and node remaining power are all factors that need to be taken into account while choosing the CH. The CH was formed by choosing specific characteristics, such as the distance between the CH and the base station (BS), using particle swarm optimization (PSO). That decision is made using the Ant Colony Optimization (ACO) method. Optimizing the path is dependent on the distance, node degree, and remaining power.

Sreevidya and Supriya [24] identifies ample of attacks and recommended a multi-layer data security approach to control change of data, dropping of data by the compromised nodes. Trust Based Routing (TBR) is recommended where forwarding node is selected on the basis of highest trust value and thus reduces malicious/ compromised nodes from participating in the routing procedure. The trust factor is computed by figuring the number of packets dropped, packets rejected, and the node's remaining energy. The idea of TBR is improved by adding the concept of past trust and trust of node towards a specific destination and this is called as Extended Trust Based Routing (ETBR). This idea is further improved by adding Direct Trust, Indirect Trust and Energy Trust concepts and referred as Consolidated Trust Estimation – Trust Based Routing (CTE-TBR). Network Simulator NS2 is used to simulate the recommended schemes. The result reflects the impact of the recommended data security scheme in terms of energy efficiency and Packet Delivery ratio (PDR).

Tewari and Tripathi [25] introduced NFEER, a neuro-fuzzy method for energy-efficient routing, for WSN that can be enabled by the Internet of Things. Novel to the existing algorithms is those that take into account the CH's residual energy, cluster size, and distance to the sink as routing parameters in IoT-enabled WSN. Using these parameters, they were able to determine the best route through the network, which helped reduce the impact of the hotspot problem. The NFEER used energy thresholds during the process to limit the set of potential nodes to only those with energies higher than a certain threshold, as long as the requirement is met.

Kumar et al. [26] works with a deployment to surveillance a landslide prone zone, which consists nodes to sense geological attributes essential for early warning. The deployment area is a hilly region where we can find different demographic characteristics. Demonstrating network connectivity in this deployment site for real-time casting of sensor data works with dealing of site-specific challenges such as dynamic network conditions due to rough weather, asymmetric links, network fail-over and re-connection problem, inadequate solar power etc.

C. SECURE COMMUNICATION

Karthikeyan et al. [27] reported that it applies machine learning and the Firefly Algorithm together to make IoT and WSN security better than it is now. They made two significant contributions. The proposed FA-ML approach significantly enhanced the precision of intrusion detection in the WSN-IoT setting. Second, security-oriented optimization techniques gained a new dimension with the integration of machine learning and the Firefly algorithm. Safeguarding the integrity of networked systems is of crucial importance in several areas, including critical infrastructure protection, industrial automation, and beyond. The ramifications of this are far-reaching. Integrating state-of-the-art machine learning with algorithms inspired by biology was a watershed moment in developing intelligent security measures for the ever-changing world of IoT technology. The FA-ML approach groups objects using an SVM model. The parameters were adjusted, and intrusions into the WSN-IoT were detected using a Grey Wolf Optimizer (GWO) algorithm.

Meenakshi and Karunkuzhali [28] discussed the common WSN assaults that can swiftly damage the system include black holes, gray holes, flooding, and scheduling. There is a number of drawbacks to WSN, including increased false alarms, high computing overhead, and low identification rates, despite their intrusion detection systems, improved network data correlation, and substantial redundancy. Collecting information from WSN-DS was the first stage. During the pre-processing phase, we removed duplicate data and missing values and reinstated under color Wiener filtering (CWF). The Tasmanian Devil Optimization (TDO) algorithm selected the best features during the feature selection step. Using the best attributes, SAPVAGAN divides WSN data intrusions into normal and anomalous categories. So, to improve SAPVAGAN's WSN intrusion detection accuracy, they suggested the honey badger algorithm (HBA).

Msolli et al. [29] suggested a new system for managing keys, the Key Management Scheme, which would use pool-hash to create different kinds of keys. By contrasting the original plan with the revised one, they were able to showcase the several steps involved in key management. The discovery and path key phases define new session keys transferred between sensor nodes as a result of modifications that disclosed a new key pool that contains original keys and other hashing that admitted the same identities. The protocol then formalizes and specifies, using a mathematical notion, the probability of connectivity and resilience against node capture.

Dener and Orman [30] utilized a private blockchain to create sensor nodes, cluster nodes, base stations, and blockchain networks to implement the study's system concept. Authentication in WSNs ensures that both data and resources are legitimate. The node in a WSN can verify the data's authenticity and prevent its modification through authentication. But current authentication protocols have some security holes, like those that allow ID spoofing attacks. Furthermore, blockchain, a new technology, has proven to be highly effective in security-related domains. Cryptographically secure, immutable, non-repudiable, irrevocable, auditable, and verifiable are some of the security-related features of the blockchain. Their use of blockchain technology extended to WSN. They came up with an innovative authentication technique for WSN that relies on blockchain technology.

Muhajjar et al. [31] introduced a key management hierarchy as a means of protecting heterogeneous WSN using HEED routing. The Bloom scheme handled key management, while a PRNG efficiently generated keys to preserve sensor resources. Furthermore, this system accomplished cryptographic objectives like secrecy by employing cipher block chaining, specifically Rivest cipher 5 (CBC-RC5).

Anitha et al. [32] suggested a plan to reduce energy consumption and increase the network's lifetime called NTM-LEACH-RSA, which combines a cryptographic RSA method

with a new approach to trust management. The proposed methodology includes two components to enhance WSN security. Initially, they used the proposed NTM-LEACH method to build clusters and elect CHs. They chose the cluster's head based on the trust value, the density and distance between neighbouring nodes, and the threshold function value. They estimated the threshold function value using two domains: energy and distance. To ensure data integrity and secure transmission, they used RSA cryptography technology in the second step.

Iqbal and Sujatha [33] discovered a newer way to create cluster and routing with less energy consumption, which they suggest as an improvement for Hierarchical-EIDS algorithm in HWSN. In the process, they first implemented efficient clustering to reduce electric power consumption by choosing CHs based on a fuzzy transient search algorithm (FTSA). In the next stage, they used an adaptive aquila optimization (AAO) to devise a highly optimized path as best way for data relocation. To meet the final CAP theorem, we saw that ZKP was problematic, which required a special form of mutual authentication between two parties and something like hierarchical EIDS. In the HE (homomorphic equilibrium) approaches a key was formed for each single sensor node.

Kumar et al. [34] cited that the chances of attacks on traditional authentication schemes developed the need for more authenticated procedures. To overcome this vulnerability, they have proposed a new mechanism toward authentication of users in multi-gateway IoT-enabled WSNs, which allowed secure and efficient data transfer. Biometric data, hashing, and XOR operations-the ones that reduce computational overheads-being the backbone, they have proposed a new approach. They keep the communication forward and backward a secret by securely updating biometric information, session keys, and passwords.

Yesodha et al. [35] proposed a trust- and encryption-based SRP for the routing in WSN. Among the features are ACO-oriented SRP, clustering, ECC, confidence modeling with intrusion detection, and fuzzy rules. They suggested building an intrusion detection-based trust model using the enlarged convolutional neural network, particle swarm optimization, and the Schrodinger equation. Herein, the Intrusion Detection-based authentication of node's trust and evaluation proposes a secure protocol, namely TECC-ACO-SRP (Trust and ECC encryption-based ACO-SRP); the ECC encryption algorithm transmits the data only after encryption. They employed the dominant set clustering along with fuzzy criteria for forming clusters including members of similar node types.

Revanesh et al. [36] proposed authentication scheme with ECC, having three-factor authentication combined with key agreement in order to improve the security of WSN. Present schemes, which have many security flaws and vulnerabilities, cannot avail forward security and also fail to meet requirements about anonymity, thus becoming easy targets for security attacks related to MITT attacks, user disguising, internal privileges, and password guessing. The scheme sends authentication across users, gateways, and sensors by using a challenge-response system. It negotiates a secure session key and incorporates biometrics, smart card, and password authentication technologies, all of which are based on the ECC protocol. Burrows, Abadi, and Needham's formal security analysis and the informal study of several known assaults validate the scheme's correctness and security, demonstrating its robustness against diverse attacks.

Fatima et al. [37] unveiled a three-factor authentication protocol that is both lightweight and thorough; it provides adaptive privacy preservation and diverse security criteria, making it perfect for user-friendly scenarios in WLAN environments. They often use complex cryptographic security structures that take a lot of time, and lightweight systems don't always provide important security features like perfect forward secrecy and protection against ephemeral secret leakage (ESL) attacks. Their solution considered the dynamic security needs of users, utilized lightweight cryptographic primitives, and closely monitored potential protocol flaws. They did this by eliminating any cryptographic structures that weren't strictly required.

Khalid et al. [38] have developed a number of authentication methods, but the vast majority of them are either overly complicated or poorly protected. When it comes to tiny sensor nodes, traditional security solutions just won't cut it. Public key cryptography is efficient but resource-intensive, making it unsuitable for wireless networks; symmetric cryptography, on the other hand, uses more energy. Crucial problems with symmetric cryptosystem administration exist. They came up with a more sophisticated and lightweight solution to strengthen network security while using fewer resources. They put out BUAKA, a protocol for biometric user authentication and key agreement that uses one-way hash functions and a fuzzy extractor to authenticate sensor nodes. Initialization, registration, authentication, and password renewal are the four stages that make up the suggested scheme. The suggested scheme's secure authentication mechanism and outstanding resilience against multiple attacks addressed the complexity issues.

Chen et al. [39] proposed protocols for two-factor authentication across multiple gateways are extensive. But they discovered that practically every protocol out there was vulnerable. In particular, no current two-factor multi-gateway authentication method can withstand an attack that uses both a smart card loss and a password or ID guessing component. Using smart cards and passwords, they introduced a new authentication protocol for multi-gateway WSN. Discrete elliptic curve encryption underpins key negotiation, safeguarding the protocol against sensor capture attacks and ensuring forward security. The next step was to use BAN-logic to ensure authentication and session key negotiation. Furthermore, by incorporating the game sequence into the Random Oracle model (RO model), they formalized the new protocol's security proof.

TABLE 7. Routing problems and proposed solutions.

Paper	Key Problem	Proposed Solution	Main Contributions	Goals
Kooshari et al. [13]	Finding optimal paths for sending packets to reduce energy consumption.	WSA for clustering and ACO for mobile sink path optimization.	Discrete WSA for CH selection, comprehensive objective function for clustering, ACO for CH traversal, CH traversal coding like TSP.	Reduce energy consumption, error rate, and increase WSN lifetime.
Sharma et al. [14]	Secure and optimal routing in WSN.	ML-HSOR protocol with four stages: registration, clustering, authentication, and optimal routing.	Markov model for CH selection, multi-level trust evaluation for authentication, PL-COA for optimal data transmission path.	Enhance network lifespan, performance, and security.
Vellela et al. [15]	Minimize energy consumption and delay in WSN routing.	Hybrid Chimp-based Clustering Flat Routing Protocol (CbCFRP).	Chimp fitness function for optimal route, clustering protocol for shortest route.	Minimize energy consumption and delay.
Pedditi et al. [16]	Energy-efficient WSN model for forest fire detection.	Energy Efficient Routing Protocol (EERP).	Minimize idle listening in CHs, reduce redundant data transmission, prevent low energy nodes from becoming CHs, multi-hop routes.	Reduce energy utilization, extend network lifetime.
Prabhu et al. [17]	Optimal route detection with minimal delay.	RL-based routing algorithm.	Uses three reward functions for Q-value computation, detects optimal routes by considering current network status.	Minimize transmission delay, increase reliability.
Gunjan, Sharma et al. [18]	Energy-saving unequal clustering and routing.	Genetic Algorithm based Unequal Clustering and Routing Protocol (GA-UCR).	GA for CH election and multi-hopping, three fitness functions for CH election and routing.	Save energy, prevent energy holes/hot-spots.
Sheeja et al. [19]	High energy consumption and short network lifetime.	Adaptive Black hole Tuna Swarm Optimization (ABTSO) for routing.	Integration of BHO and TSO techniques, multi-functional derivation for CH selection (considering factors like link quality, node centrality, path loss, PDR, delay, distance, and residual energy).	Reduce energy consumption, increase network lifetime.
Sharma et al. [20]	Secure and energy-efficient routing in WSN-IIoT.	MHSEER	Uses meta-heuristics for routing decisions, counter-encryption mode (CEM) for data security, heuristics method for reliable data routing.	Improve security, enhance energy efficiency.
Yang et al. [21]	Adaptability to network topology changes, high	Intelligent routing algorithm (WOAD3QN-RP)	WOA for CH selection (considering residual energy, node distance, communication	Reduce delay, balance energy consumption, extend network lifetime.

TABLE 7. *(Continued.)* **Routing problems and proposed solutions.**

	delays, short lifetimes.	combining WOA and D3QN.	delay), D3QN for multi-hop path optimization.	
Xue et al. [22]	Efficient clustering and routing with better QoS.	K-IABC for clustering and CL-HHO for routing.	K-medoids with improved artificial-bee-colony for clustering, cross-layer routing to reduce delay and power consumption.	Enhance QoS, decrease network-transmission delay and power consumption.
Mishra et al. [23]	Minimize power utilization and elevate network lifespan.	Butterfly Optimization Algorithm (BOA) for CH selection and PSO for clustering and routing.	BOA for optimal CH quantity, PSO for clustering and route optimization (considering distance, node degree, remaining power).	Minimize power utilization, increase network lifespan.
Sreevidya et al. [24]	A new attempt for Data Security in WSN for applications where data security is critical.	An alternate mechanism is employed to route the packet as against the conventional hop count or delay.	A mathematical model for Trust Computation is devised for routing.	Optimization of energy in the nodes of WSN.
Tewari et al. [25]	Energy-efficient routing with hotspot mitigation.	Neuro-fuzzy approach to energy-efficient routing (NFEER).	Uses multiple parameters for routing (CH distance to sink, cluster size, residual energy), relies on energy thresholds for candidate nodes.	Minimize power consumption, mitigate hotspot issue.
Kumar et al. [26]	Positioning to surveillance of a landslide prone zone where the nodes sense geological attributes essential for early warning.	Positioning of few relay nodes few relay nodes for connecting the WSN to a field management center through an IoT gateway.	The field management center makes use of multiple fault-tolerant WAN networks to relay the data to a remote central data management center for deep data analysis and for generating early warnings prior to a catastrophic event.	Heterogeneous sensors are handled by a gateway software which are capable of readings at a rate up-to 1700/s within a latency of 10 s while delivering the data to the data center.

Nagaraja et al. [40] implemented a lightweight communication protocol that guarantees a reasonable compromise between power consumption and the highest levels of security. They pioneered a synchronized framework that employs unique public-key encryption to enable the involvement of genuine on-field sensors in PA, which is different from any previous method. On the other hand, they show an algorithm for energy efficiency that addresses a novel routing structure for aggregator nodes. On the other hand, the security algorithm uses a parallel validation technique to perform secure data aggregation in a unique, progressive, and nonitterative manner.

Mittal et al. [41] aimed to reduce power consumption to a level feasible for sustained operation using harvested energy alone. They presented an infrastructure that is robust, energy-efficient, and spectrum-aware to support the Internet-of-Things (IoT) system deployed in precision agriculture. They laid out a method for optimizing the IoT using system modeling, which they then used to make ULP systems more practical to implement. For ULP infrastructure parts like a wake-up radio and a ULP received signal strength detector, the amount of power they use is in the nano-watt range when using 65-nm CMOS technology. They also suggested a small countermeasure for energy depletion attacks in IoT networks

TABLE 8. Referred article for WSN, IoT and 6TiSCH (year-wise).

Year	Number of Publications	Topics Covered
2020	1	WSN connectivity for remote monitoring
2023	19	Localization, routing, security, energy efficiency, blockchain-based authentication, key management, IoT-WSN integration
2024	16	Localization, routing, security, energy-efficient protocols, machine learning for security, IoT-WSN security

based on energy detection. Additionally, they proposed methods for IoT sensor nodes to manage in increasingly crowded device networks, all the while taking advantage of opportunities to improve their energy systems and maybe even run autonomously.

Srinivasan et al. [42] explore techniques to improve the quality and reliability of WSN systems, focusing on minimizing delay, extending node life, and optimizing routing. While there has been limited research on assessing the safety integrity levels of WSN systems, this gap is addressed through the development of a QoS metric-based safety integrity assessment for end-to-end industrial WSN systems. To effectively monitor safety integrity levels, a 4-step mapping methodology is introduced, linking relevant QoS metrics with communication defenses and safety mechanisms.

Kumaran et al. [43] innovatively proposes a deep learning-based generative adversarial networks and machine learning-based isolation forests approach to identify software piracy. Our cybersecurity GAN-IF model performs its task by training a Generator network to mimic the behavior of legitimate software applications. This model outperforms traditional methods of detection to provide subtle evidence of software piracy by incorporating GANs with Isolation Forests.

Hong et al. [44] reported that increasing adoption of electronic health records (EHRs) has improved medical diagnosis and treatment efficiency but also poses significant privacy risks, necessitating enhanced access control mechanisms. Current regulatory practices are often reactive, addressing medical malpractice only after incidents occur. In order to overcome these issues, a blockchain-based system is proposed that enables patient-centric, fine-grained access control for EHRs. This system integrates attribute-based encryption with blockchain, allowing proactive regulation by medical authorities. Unlike traditional approaches, it uses blank EHRs as intermediaries, enhancing privacy and security. The design reduces storage costs by employing a chameleon hash function for file storage in the interplanetary file system (IPFS). It also enhances telemedicine security and efficiency through single sign-on and improves EHR authorization using proxy re-encryption. Similarly, in [45] authors focused on enhancing the security in the online car-hailing industry where sharing of car location data holds significant value. Existing selective disclosure schemes, such as those based on Merkle trees, become costly when managing numerous data items. In order to address these challenges, a blockchain-based framework is proposed to facilitate the secure sharing of car location data while safeguarding passenger privacy through selective disclosure. The framework combines homomorphic encryption with probabilistic verification, enabling faster batch data verification compared to other blockchain-based solutions and ensuring the authenticity of data on the blockchain.

D. 6TISCH PROTOCOLS

WSN play a crucial role in IoT applications, where the IETF 6TiSCH protocol is widely adopted due to its low power consumption, high reliability, and precise timing. However, security, energy efficiency, and network performance remain key challenges that require innovative solutions.

Aydin et al. [46] proposed a lightweight authentication and session key agreement protocol for 6TiSCH networks, utilizing XOR operations, personal passwords, and hash functions to ensure secure node authentication and link-layer communication. The protocol reduces energy consumption by 25%, shortens authentication time by 20%, and decreases transmitted bits by 15% compared to existing methods. Its implementation in Contiki OS using the COOJA simulator validates its efficiency and scalability for IIoT applications.

Van Leemput et al. [47] addressed energy limitations in battery-less 6TiSCH routers by developing an energy-aware adaptive scheduling mechanism. The approach integrates energy consumption and storage prediction to dynamically adjust scheduling and routing, reducing energy use while maintaining network reliability. The solution is particularly effective in non-critical industrial automation scenarios.

Kim and Chung [48] focus on enhancing route management for mobile nodes in 6TiSCH networks. Since traditional TSCH and RPL protocols are optimized for static nodes, they propose a method that allocates dedicated control cells to reduce collisions and improve network recovery. Their approach enhances overhead efficiency by 2.5 times and improves mobile node participation time by 33%.

Kulcu et al. [49] integrated steerable smart antennas with the 6TiSCH protocol to enhance network capacity and reliability. Their modifications to the MAC layer and scheduling mechanisms enable the seamless operation of smart antennas in IoT networks, particularly in high-density environments. The results demonstrate superior data delivery performance compared to conventional 6TiSCH implementations.

Kim et al. [50] introduced Quick6TiSCH, an approach designed to accelerate 6TiSCH network formation. By prioritizing control messages and diversifying their transmission times, Quick6TiSCH reduces network formation time by 62.6% while maintaining a similar transmission overhead to

TABLE 9. Secure approaches and challenges.

Paper	Algorithm/Approach	Key Features	Advantages	Challenges
Karthikeyan et al. [27]	FA-ML Technique	Combines Firefly Algorithm and SVM with Grey Wolf Optimizer for parameter tuning	High intrusion detection accuracy, novel security-oriented optimization techniques	Implementation complexity, computational overhead
Meenakshi et al. [28]	HBA-optimized SAPVAGAN	Uses CWF for pre-processing, TDO for feature selection, and HBA to optimize SAPVAGAN	Accurate intrusion detection, reduces data redundancy and missing values	High computation overhead, managing feature selection and optimization together
Msolli et al. [29]	Key Management Scheme (Pool-Hash)	New key types establishment with original keys and hashed identities, formalized using mathematical model	Improved resilience against node capture, secure key transmission	Complexity in protocol design and formalization, overhead in key management phases
Dener et al. [30]	Blockchain-based Authentication	Uses private blockchain for secure data authentication	High security, immutable and verifiable data	High computational and energy requirements, blockchain implementation challenges
Muhajjar et al. [31]	HEED with CBC-RC5	Bloom scheme for key management, PRNG for efficient key generation	Efficient key management, achieved cryptographic goals like confidentiality	Complexity in hierarchical key management, overhead in cryptographic operations
Anitha et al. [32]	NTM-LEACH-RSA	LEACH protocol with trust management and RSA for secure data transmission	Extends network lifetime, consumes less energy, ensures data integrity	Complexity in CH election and trust management
Iqbal et al. [33]	Hierarchical-EIDS Algorithm	Fuzzy transient search algorithm for clustering, AAO for routing, EIDS for authentication	Energy-efficient, optimal routing, secure data transmission	Complexity in integrating multiple algorithms, overhead in clustering and routing phases
Kumar et al. [34]	Bio-information-based Authentication	Uses biological information, hash, and XOR operations for secure data communication	Reduced computational costs, maintains forward and backward secrecy	Complexity in managing and updating biometric information and session keys
Yesodha et al. [35]	TECC-ACO-SRP	ECC encryption, ACO for secure routing, intrusion detection-based trust modeling	High security, efficient clustering and routing, resistant to various attacks	Complexity in combining ECC, ACO, and intrusion detection techniques

TABLE 9. *(Continued.)* **Secure approaches and challenges.**

Revanesh et al. [36]	ECC-based Authentication	Combines ECC with biometrics, smart card, and password authentication	High security, resistant to various attacks, formal security analysis	Implementation complexity, overhead in managing multiple authentication factors
Fatima et al. [37]	Lightweight Three-factor Authentication	Uses lightweight cryptographic primitives, adaptive privacy preservation	High security, user-friendly, resistant to ephemeral secret leakage attacks	Complexity in protocol design, ensuring adaptive privacy preservation
Khalid et al. [38]	BUAKA	Biometric-based authentication, fuzzy extractor, one-way hash functions	Secure authentication, resilience against various attacks, resolves complexity issues	Complexity in biometric data management, overhead in multiple authentication phases
Chen et al. [39]	Two-factor Multi-gateway Authentication	Uses password and smart card with fuzzy-verifier and honeywords technique	High security, resistant to password and identity guessing attacks, formal security proof	Complexity in managing multi-gateway authentication, overhead in implementing fuzzy-verifier and honeywords
Nagaraja et al. [40]	Lightweight Communication Protocol	Public-key encryption, unique structural management of routing, non-iterative security mechanism	Energy-efficient, secure data aggregation, facilitates legitimate sensor participation in PA	Complexity in balancing energy efficiency and security, overhead in unique structural management of routing
Mittal et al. [41]	Energy-efficient IoT Infrastructure	ULP received signal strength detector, wake-up radio, lightweight energy-detection countermeasure	Ultra-low power consumption, supports sustained operation using harvested energy	Implementation complexity, ensuring sustained operation in congested device networks
Srinivasan et al. [42]	QoS metric-based safety integrity assessment.	Address this gap by introducing a QoS metric-based safety integrity assessment for end-to-end industrial WSN systems.	Develop a 4-step mapping methodology that connects QoS metrics with communication defenses and safety mechanisms.	Improve safety integrity levels of industrial WSN systems
Kumaran et al. [43]	DL based Generative Adversarial Networks (GANs) and ML based Isolation Forest (IF) for detecting software piracies.	The GAN-IF-based cybersecurity model operates by training a Generator network to replicate the behavior of legitimate software applications.	Facilitates efficient learning and adaptation to piracy challenges, making it highly effective against previously known threats.	Creating lightweight and efficient security solutions designed to address the needs of resource-constrained IoT devices.

baseline methods. The strategy effectively mitigates collision issues during the bootstrapping phase.

Hou et al. [51] proposed a hybrid ECC-AES encryption scheme to enhance security in 6TiSCH networks. Their method employs ECC-based key negotiation and dynamic AES session keys, improving encryption security while optimizing key generation speeds through a regular window algorithm.

Collectively, these studies provide valuable advancements in 6TiSCH networks, addressing key concerns in security, energy efficiency, mobility support, and network formation. These improvements contribute to the development of more robust and scalable IoT solutions.

The above given table shows the total referred article in literature review for WSN, IoT and 6TiSCH networks.

IV. CHALLENGES AND OPEN ISSUES

A. WSN LOCALIZATION RELATED CHALLENGES AND ISSUES.

Some of the challenges in localization in WSN and IoT are energy efficiency, scalability, security, mobility, and heterogeneity. Energy efficiency is a critical factor because IoT devices depend on batteries and most processes regarding the process of localization require frequent communications, which deplete energy rapidly. Scalability is still an open area of research: finding a solution for large network size, since for large network size, traditional localization algorithms may not work properly. However, environmental complexities, such as noise, interference of signals, and physical obstruction, may degrade the accuracy of localization. It needs the development of secure localization protocols that could estimate threats and neutrality in order to keep the accuracy intact. Hybrid methods have also emerged that use both range-based and range-free techniques, yet the integration of such remains a challenge. In addition, mobility adds complications into localization, especially in those applications involving moving nodes. It forms a vital basis for applications ranging from drone navigation and underwater sensor networks to indoor positioning. Multi-hop localization-very often inevitable in large networks-presents its problems, such as error accumulation over multiple hops. Limited processing power and memory of IoT devices impose further restrictions on the complexity of the localization algorithm. Development of standardized methods for localization in WSN-IoT systems is highly essential.

Generally, the Range-based localization techniques, such as ToA and RSSI, require continuous signal exchanges, which consume significant energy. In order to overcome this issue, incorporating energy-harvesting mechanisms (e.g., solar or vibration energy) to extend the lifetime of sensor nodes can play significant role to enhance the lifetime. Moreover, as WSN scale to thousands of nodes, traditional localization algorithms face challenges in maintaining accuracy and efficiency due to increased communication overhead and computational complexity. In order to overcome this, implementation of hierarchical approaches to localize nodes in clusters, reducing the complexity of large-scale networks can be considered as a promising solution.

B. WSN ROUTING RELATED CHALLENGES AND ISSUES

Several characteristics inherent with resource limitations, dynamic topologies, and scalability requirements make up the challenges WSN faces in routing. Under these conditions, energy efficiency remains an important aspect of concern because sensor nodes usually operate on batteries, and the enhancement of routing protocols is very necessary for better energy usage to prolong the lifetimes of the networks. Another challenge is scalability since WSNs can be highly populated with nodes, and conventional protocols may be inefficient in handling communication and overhead latency. Their dynamic nature also makes them challenging to handle because protocols need to act swiftly while retaining low overhead. Security issues are also very valid since WSNs are highly susceptible to node tampering and data manipulation attacks. While routing protocols may enable efficient in-network data aggregation to reduce redundancy, this too is fairly challenging to achieve without trading off some data quality. QoS requirements also vary depending on the application of WSN, and protocols should consider node heterogeneity and mobility.

Fault tolerance is a required characteristic in WSN-nodes can fail due to environmental conditions, battery depletion, or hardware failures. Load balancing enables uniform energy consumption without some nodes acting as hot spots for communication due to uneven depletion. Geographic routing also has its problems, which include, but are not limited to, the accurate calculation of node positions. Cross-layer design is embodied with challenges whereby different network layers need to coordinate with one another, hence more complexity.

Moreover, the routing protocols must minimize energy consumption to prolong network lifetime, as sensor nodes operate on limited battery power. For example, in environmental monitoring, where nodes remain unattended for long periods, energy-efficient routing is critical to ensure continuous data transmission. Therefore, incorporating energy-aware routing protocols can play significant role in improving the performance.

C. SECURITY RELATED CHALLENGES AND ISSUES

IoT-based WSN present serious security challenges owing to their broad applications in critical domains such as smart cities, healthcare, and industrial automation. In most deployment environments, these networks are deployed with minimum physical security; hence, node tampering, eavesdropping, and DoS attacks present very high threats. Security protocols, including encryption and authentication, need to be developed considering the above constraints with little or no impact on the performance or network lifetime. Add the diversity of the various IoT devices to this and the need for security solutions that will be able to handle this diversity with a minimum level of vulnerability. The dynamic nature of

WSN, where a lot of nodes join and leave, requires effective security management, which is rather a challenge. A continuous research area is in developing secure and efficient routing protocols. Privacy is another key concern, especially when sensitive data is being manipulated-for instance, in healthcare or smart home systems. This integration of cloud and edge computing complicates it further, especially when the securing of data in transmission and storage across distributed infrastructures gets more complicated. These are security concerns that can barely be tackled in an isolationist approach but need an in-depth approach toward advancement in cryptography, lightweight protocols for security, machine learning-driven threat detection, and standardization of security frameworks. Moreover, inadequate physical security makes sensor nodes vulnerable to tampering, compromising network integrity. Therefore, PUF-based Authentication can be utilized to introduce tamper-resistant device authentication.

V. CONCLUSION

This study encompasses all the features that define IoT, WSNs, and associated localization, routing, and security features. Localization algorithms would be kings in data quality and reliability of WSN concerning location pinpointing of sensor node locations. Energy efficiency or adaptation to varying settings featured alongside advancements of range-based and range-free localization methods. Different routing protocols are necessary to have maximum resource efficiency, extend network lifetime, and create efficient communication links between sensor nodes. Different routing algorithms, their performance metrics, and their applicability in various applications of WSNs were studied. WSNs are vulnerable to various hostile attacks; hence, robust approaches for data encryption, authentication, and intrusion detection become necessary for WSN. This survey was supposed to report on state-of-the-art security procedures and approaches for the protection from dangers in WSN and ensuring data integrity and confidentiality. This review adds to our understanding of the complexity and challenge involved in installing safe and reliable WSNs for various Internet-of-Things applications by summarizing recent research and development in these areas. These are the core characteristics that, upon improvement, will let researchers continue working towards even more scalable, efficient, and resilient WSN in ever-changing IoT environments. The future work based on these directions will mainly focus on development of an end-to-end protocol for sensor network to enhance the network performance by introducing advanced localization, energy-ware routing and strong secure data exchange protocols.

REFERENCES

[1] M. Fawad, M. Khan, K. Ullah, H. Alasmary, D. Shehzad, and B. Khan, "Enhancing localization efficiency and accuracy in wireless sensor networks," *Sensors*, vol. 23, no. 5, p. 2796, Mar. 2023.

[2] D. W. Wajgi and J. V. Tembhurne, "Localization in wireless sensor networks and wireless multimedia sensor networks using clustering techniques," *Multimedia Tools Appl.*, vol. 83, no. 3, pp. 6829–6879, Jan. 2024.

[3] O. Alfawaz, W. Osamy, M. Saad, and A. M. Khedr, "Modified rat swarm optimization based localization algorithm for wireless sensor networks," *Wireless Pers. Commun.*, vol. 130, no. 3, pp. 1617–1637, Jun. 2023.

[4] R. Mani, A. Rios-Navarro, J.-L. Sevillano-Ramos, and N. Liouane, "Improved 3D localization algorithm for large scale wireless sensor networks," *Wireless Netw.*, vol. 30, no. 6, pp. 5503–5518, Aug. 2024.

[5] H. Mohapatra, A. K. Rath, R. K. Lenka, R. K. Nayak, and R. Tripathy, "Topological localization approach for efficient energy management of WSN," *Evol. Intell.*, vol. 17, no. 2, pp. 717–727, Apr. 2024.

[6] X. Yu, Y. Liu, and Y. Liu, "Optimization of WSN localization algorithm based on improved multi-strategy seagull algorithm," *Telecommun. Syst.*, vol. 86, no. 3, pp. 547–558, Jul. 2024.

[7] P. Yadav, S. C. Sharma, O. Singh, and V. Rishiwal, "Optimized localization learning algorithm for indoor and outdoor localization system in WSNs," *Wireless Pers. Commun.*, vol. 130, no. 1, pp. 651–672, May 2023.

[8] E. Tagne Fute, D.-K. Nyabeye Pangop, and E. Tonye, "A new hybrid localization approach in wireless sensor networks based on particle swarm optimization and Tabu search," *Int. J. Speech Technol.*, vol. 53, no. 7, pp. 7546–7561, Apr. 2023.

[9] P. Tripathy and P. M. Khilar, "PSO based amorphous algorithm to reduce localization error in wireless sensor network," *Pervasive Mobile Comput.*, vol. 100, May 2014, Art. no. 101890.

[10] A. Achroufene, "RSSI-based geometric localization in wireless sensor networks," *J. Supercomput.*, vol. 79, no. 5, pp. 5615–5642, Mar. 2023.

[11] S.-H. Lee, C.-H. Cheng, C.-C. Lin, and Y.-F. Huang, "PSO-based target localization and tracking in wireless sensor networks," *Electronics*, vol. 12, no. 4, p. 905, Feb. 2023.

[12] K. S. Kumar, S. K. Rout, S. K. Panda, P. K. Mohapatra, S. N. Mohanty, and M. I. Khan, "RSSI-based optimization of static and mobile node combinations for dynamic node localization in wireless sensor networks," *Telecommun. Syst.*, vol. 87, no. 1, pp. 137–149, Sep. 2024.

[13] A. Kooshari, M. Fartash, P. Mihannezhad, M. Chahardoli, J. Akbari-Torkestani, and S. Nazari, "An optimization method in wireless sensor network routing and IoT with water strider algorithm and ant colony optimization algorithm," *Evol. Intell.*, vol. 17, no. 3, pp. 1527–1545, Jun. 2024.

[14] V. Sharma, R. Beniwal, and V. Kumar, "Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications," *J. Supercomput.*, vol. 80, no. 8, pp. 11338–11381, May 2024.

[15] S. S. Vellela and R. Balamanigandan, "Optimized clustering routing framework to maintain the optimal energy status in the WSN mobile cloud environment," *Multimedia Tools Appl.*, vol. 83, no. 3, pp. 7919–7938, 2024.

[16] R. B. Pedditi and K. Debasis, "Energy efficient routing protocol for an IoT-based WSN system to detect forest fires," *Appl. Sci.*, vol. 13, no. 5, p. 3026, Feb. 2023.

[17] D. Prabhu, R. Alageswaran, and S. Miruna Joe Amali, "Multiple agent based reinforcement learning for energy efficient routing in WSN," *Wireless Netw.*, vol. 29, no. 4, pp. 1787–1797, May 2023.

[18] Gunjan, A. K. Sharma, and K. Verma, "GA-UCR: Genetic algorithm based unequal clustering and routing protocol for wireless sensor networks," *Wireless Pers. Commun.*, vol. 128, no. 1, pp. 537–558, Jan. 2023.

[19] R. Sheeja, M. M. Iqbal, and C. Sivasankar, "Multi-objective-derived energy efficient routing in wireless sensor network using adaptive black hole-tuna swarm optimization strategy," *Ad Hoc Netw.*, vol. 144, May 2023, Art. no. 103140.

[20] A. Sharma, H. Babbar, S. Rani, D. K. Sah, S. Sehar, and G. Gianini, "MHSEER: A meta-heuristic secure and energy-efficient routing protocol for wireless sensor network-based industrial IoT," *Energies*, vol. 16, no. 10, p. 4198, May 2023.

[21] X. Yang, J. Yan, D. Wang, Y. Xu, and G. Hua, "WOAD3QN-RP: An intelligent routing protocol in wireless sensor networks — A swarm intelligence and deep reinforcement learning based approach," *Expert Syst. Appl.*, vol. 246, Jul. 2024, Art. no. 123089.

[22] X. Xue, R. Shanmugam, S. Palanisamy, O. I. Khalaf, D. Selvaraj, and G. M. Abdulsahib, "A hybrid cross layer with harris-hawk-optimization-based efficient routing for wireless sensor networks," *Symmetry*, vol. 15, no. 2, p. 438, Feb. 2023.

[23] R. Mishra and R. K. Yadav, "Energy efficient cluster-based routing protocol for WSN using nature inspired algorithm," *Wireless Pers. Commun.*, vol. 130, no. 4, pp. 2407–2440, Jun. 2023.

[24] B. Sreevidya and D. M. Supriya, "Trust based routing—A novel approach for data security in WSN based data critical applications," *J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl.*, vol. 15, no. 1, pp. 27–41, Mar. 2024.
[25] P. Tewari and S. Tripathi, "An energy efficient routing scheme in Internet of Things enabled WSN: Neuro-fuzzy approach," *J. Supercomput.*, vol. 79, no. 10, pp. 11134–11158, Jul. 2023.
[26] S. Kumar, S. Duttagupta, V. P. Rangan, and M. V. Ramesh, "Reliable network connectivity in wireless sensor networks for remote monitoring of landslides," *Wireless Netw.*, vol. 26, no. 3, pp. 2137–2152, Apr. 2020.
[27] M. Karthikeyan, D. Manimegalai, and K. RajaGopal, "Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection," *Sci. Rep.*, vol. 14, no. 1, p. 231, Jan. 2024.
[28] B. Meenakshi and D. Karunkuzhali, "Enhancing cyber security in WSN using optimized self-attention-based provisional variational auto-encoder generative adversarial network," *Comput. Standards Interfaces*, vol. 88, Mar. 2024, Art. no. 103802.
[29] A. Msolli, N. Ajmi, A. Helali, A. Gassoumi, H. Maaref, and R. Mghaieth, "New key management scheme based on pool-hash for WSN and IoT," *J. Inf. Secur. Appl.*, vol. 73, Mar. 2023, Art. no. 103415.
[30] M. Dener and A. Orman, "BBAP-WSN: A new blockchain-based authentication protocol for wireless sensor networks," *Appl. Sci.*, vol. 13, no. 3, p. 1526, Jan. 2023.
[31] R. A. Muhajjar, N. A. Flayh, and M. Al-Zubaidie, "A perfect security key management method for hierarchical wireless sensor networks in medical environments," *Electronics*, vol. 12, no. 4, p. 1011, Feb. 2023.
[32] S. Anitha, S. Saravanan, and A. Chandrasekar, "Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission," *Measurement: Sensors*, vol. 29, Oct. 2023, Art. no. 100889.
[33] S. Iqbal and B. R. Sujatha, "Secure authentication and key management based on hierarchical enhanced identity based digital signature in heterogeneous wireless sensor network," *Wireless Netw.*, vol. 31, no. 1, pp. 127–147, Jan. 2025.
[34] R. Kumar, S. Singh, D. Singh, M. Kumar, and S. S. Gill, "A robust and secure user authentication scheme based on multifactor and multi-gateway in IoT enabled sensor networks," *Secur. Privacy*, vol. 7, no. 1, p. e335, Jan. 2024.
[35] K. Yesodha, M. Krishnamurthy, K. Thangaramya, and A. Kannan, "Elliptic curve encryption-based energy-efficient secured ACO routing protocol for wireless sensor networks," *J. Supercomput.*, vol. 80, no. 13, pp. 18866–18899, Sep. 2024.
[36] R. M., J. M. Acken, and V. Sridhar, "DAG block: Trust aware load balanced routing and lightweight authentication encryption in WSN," *Future Gener. Comput. Syst.*, vol. 140, pp. 402–421, Mar. 2023.
[37] M. N. Fatima, M. S. Obaidat, K. Mahmood, S. Shamshad, M. A. Saleem, and M. F. Ayub, "Privacy-preserving three-factor authentication protocol for wireless sensor networks deployed in agricultural field," *ACM Trans. Sensor Netw.*, Jul. 2023.
[38] B. Khalid, K. N. Qureshi, K. Z. Ghafoor, and G. Jeon, "An improved biometric based user authentication and key agreement scheme for intelligent sensor based wireless communication," *Microprocessors Microsystems*, vol. 96, Feb. 2023, Art. no. 104722.
[39] C. Chen, H. Guo, Y. Wu, Y. Gao, and J. Liu, "A novel two-factor multi-gateway authentication protocol for WSNs," *Ad Hoc Netw.*, vol. 141, Mar. 2023, Art. no. 103089.
[40] G. S. Nagaraja, K. Vanishree, and F. Azam, "Novel framework for secure data aggregation in precision agriculture with extensive energy efficiency," *J. Comput. Netw. Commun.*, vol. 2023, pp. 1–11, Feb. 2023.
[41] A. Mittal, Z. Xu, and A. Shrivastava, "Energy-efficient, secure, and spectrum-aware ultra-low power Internet-of-Things system infrastructure for precision agriculture," *IEEE Trans. AgriFood Electron.*, vol. 2, no. 2, pp. 198–208, Sep. 2024.
[42] S. Srinivasan, T. K. Ramesh, R. Paccapeli, and L. Fanucci, "Industrial functional safety assessment for WSN using QoS metrics," *Heliyon*, vol. 8, no. 11, Nov. 2022, Art. no. e11255.
[43] U. Kumaran, S. Thangam, T. N. Prabhakar, J. Selvaganesan, and H. N. Vishwas, "Adversarial defense: A GAN-IF based cyber-security model for intrusion detection in software piracy," *J. Wireless Mobile Netw., Ubiquitous Comput., Dependable Appl.*, vol. 14, no. 4, pp. 96–114, Dec. 2023.
[44] Y. Hong, L. Yang, W. Liang, and A. Xie, "Secure access control for electronic health records in blockchain-enabled consumer Internet of Medical Things," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 4574–4584, Feb. 2024.
[45] Y. Hong, L. Yang, Z. Xiong, S. S. Kanhere, and H. Jiang, "OCHJRNChain: A blockchain-based security data sharing framework for online car-hailing journey," *IEEE Trans. Intell. Transp. Syst.*, vol. 25, no. 6, pp. 5299–5311, Jun. 2024.
[46] H. Aydin, B. Aydin, and S. Gormus, "Lightweight three-factor sensor and user authentication for RPL-based 6TiSCH networks," *IEEE Sensors J.*, vol. 24, no. 17, pp. 28196–28209, Sep. 2024.
[47] D. van Leemput, J. Famaey, J. Hoebeke, and E. de Poorter, "Energy-aware adaptive scheduling for battery-less 6TiSCH routers in industrial wireless sensor networks," *IEEE Access*, vol. 12, pp. 180034–180047, 2024.
[48] M.-J. Kim and S.-H. Chung, "Efficient route management method for mobile nodes in 6TiSCH network," *Sensors*, vol. 21, no. 9, p. 3074, Apr. 2021.
[49] S. Kulcu, S. Gormus, and Y. Jin, "Integration of steerable smart antennas to IETF 6TiSCH protocol for high reliability wireless IoT networks," *IEEE Access*, vol. 9, pp. 147780–147790, 2021.
[50] H. Kim, G. Lee, J. Shin, J. Paek, and S. Bahk, "Quick6TiSCH: Accelerating formation of 6TiSCH networks with TSCH and RPL," in *Proc. IEEE 21st Int. Conf. Mobile Ad-Hoc Smart Syst. (MASS)*, Sep. 2024, pp. 66–74.
[51] C. Hou, W. Yang, Z. Zhang, Q. Liu, and J. Xiao, "Secure communication for 6TiSCH wireless networks based on hybrid ECC and AES algorithms," in *Proc. Int. Conf. Mobile Netw. Manag.* Cham, Switzerland: Springer, Oct. 2022, pp. 306–315.

H. N. VISHWAS received the B.E. and M.Tech. degrees. He is currently an Assistant Professor (Senior Grade) with the Amrita School of Computing, Amrita Vishwa Vidyapeetham, Bengaluru, India. He has more than ten years of teaching experience and five years of research experience in the domain of computer science and engineering. He has an additional designation as an Instructor with the Cisco Networking Academy, Amrita, Bengaluru Campus. He also has published his research works in 23 reputed international conferences/journals. His research interests include the Internet of Things, cybersecurity, WSN, switching and routing, and machine learning.

T. K. RAMESH received the Ph.D. degree in optical networks from Amrita Vishwa Vidyapeetham, India, in 2012. He is currently a Professor with the Department of Electronics and Communication Engineering, Amrita School of Engineering, Bengaluru, India. He has 28 years of teaching experience and has published over 100 research publications in various journals and conferences. His research interests include wired and wireless network communications and applications, network-on-chip, embedded systems, and electronic circuits and design.