Review Paper

A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks

Amit Kumar Gautam[1] · Rakesh Kumar[1]

Received: 9 May 2020 / Accepted: 28 December 2020 / Published online: 9 January 2021

Abstract

Wireless sensor networks (WSN) are the new speed-accelerating technologies worldwide and are used continuously in a range of critical applications. Any damage or compromise to data security could have physical and direct effects on network efficiency and safety. One of the active areas of research is key management, authentication, and trust management in wireless sensor networks (WSN). Since researchers have provided many protection schemes, it is difficult to select which key management or trust management schemes in a specific WSN application suit best. We did a detailed survey in our paper on how the properties of various trust management, authentication, and key management schemes can be used for specific applications. Based on this review, we present the methodologies, advantages, and limitations of the previously proposed key management, authentication, and trust management scheme in WSN. The goal of this thorough analysis is to compare and find the correct security solution that successfully meets the requirements of the application. Moreover, the strength, weaknesses, and open problems are added that can extend more frontiers to get the best security solutions in the future.s

Keywords WSN security · Key distribution · Security attacks · Protocols · Direct trust · Indirect trust

1 Introduction

Wireless sensor networks (WSN) are worldwide emerging at accelerating speed. Several kinds of research on WSN technology and standards are publishing annually, both patented and open standards. Recently botnet attacks, combined with the Internet of Things (IoT), have affected many internet name servers and web service providers. Many IoT device inventors, call-backs all the IoT devices which are affected by botnet attacks. Therefore, in today's scenario, security and trustworthiness are observed as a necessity in WSN and IoT [1].

A wireless sensor network depicted in Fig. 1 is a collection of randomly deployed small sensors that are cooperating with each other. The characteristics of the sensor network are condensed placement, random deployment, variant topology, limited bandwidth, movable or stilled sensors, self-configurable sensor nodes [2, 3]. In today's scenario, the world uses these data collected by sensors from inaccessible environments. These data do not necessarily contain errors and does not alter during transmission. WSN has various opportunities for opponents to compromise the network. Due to the broadcast nature anc vcd mobility, it always attracts many threats towards the network. Therefore, the Internet Integrated Sensor Network (IISN) should be able to provide defense, integrity, privacy, and security against various threats and attacks. As for connectivity between the Internet, sensors and smart devices increases, companies providing security services have a good opportunity.

In recent times, International Business Machines (IBM) launched a product called IoT Solutions Practice. This IBM product provides various security services using this security bundle [4] IBM has also launched a product named

✉ Amit Kumar Gautam, gautam.biet@gmail.com | [1]Department of CSE, M. M. M, University of Technology, Gorakhpur 273010, India.

SN Applied Sciences (2021) 3:50 | https://doi.org/10.1007/s42452-020-04089-9

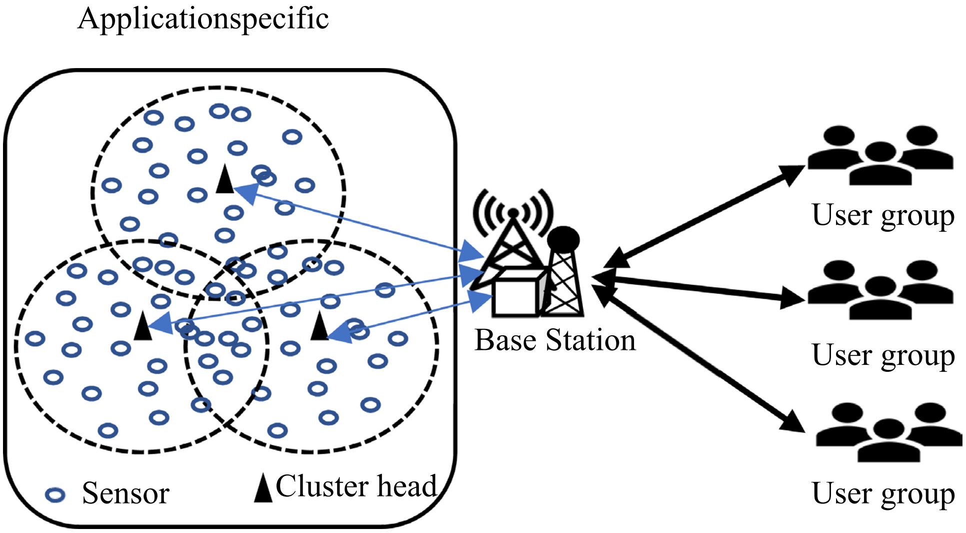


Fig. 1 Wireless sensor network

Watson IoT platform which is a collection of Application Programming Interfaces (APIs) which provides security services such as authentication, block chaining, integrity, scanning, and many other security services. The security solution provided by many cryptographic protocols such as RSA (Rivest–Shamir–Adleman) and Diffie-Hellman suffer from

timing attacks [5]. Therefore, security service providers need to go beyond these timing attacks and provide effective security in IISN architecture [6]. The forecast by IDTechEx [7] about IP-addressed sensor device that it has growth $48 billion in 2025 from $0.68 billion in 2015, the forty-seven percent gross yearly increasing rate as shown in Fig. 2. By 2020 the internet connecting device has more than 50 billion predicted by the Cisco system. The internet connecting devices have included numerous sensors (i.e. heat, pressure, moisture, radiation sensors), IoT devices, actuators, smoke, gas, surveillance equipment, and many communication devices. As the growth rate of connecting devices increases the data is also bounces exponentially.

Contribution and organization

In the related work, the security-based on key management, trust management, and authentication schemes systematically examined and reviewed. We consider the

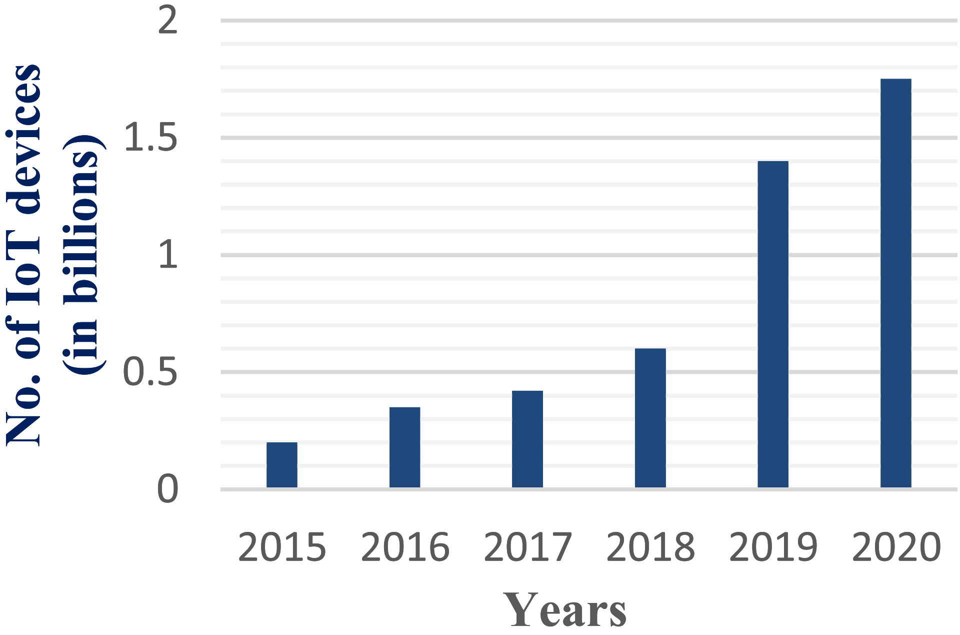


Fig. 2 Communicating devices predicted by IDTechEx [7]

basics of security in wireless sensor networks and summarizes various solutions. This manuscript describes briefly research progress on WSN network security based on key management, trust management, and authentication schemes, three aspects, by summarizing and observing these results, their pros and cons, also pointed limitation future research direction to search new security solutions.

The major contributions of our paper are as follows:

- We present an overview of the basic terminologies of the sensor network, applications, security requirements, security th reats, and security solutions based on keys, trust, and authentication.
- We provide a systematic review of security solutions in the wireless sensor network. The security solutions are summarizing and observing these results, their advantages and disadvantages, also pointed out limitations in previous work.
- Divide the key management schemes in random key distribution, master key-based, location-based, tree-based, and polynomials-based schemes. We also highlight the key generation and distribution approaches with their salient features.
- Divide the authentication schemes into lightweight authentication, Identity (ID)-based, Medium access control (MAC)-based broadcast, and timestamp-based schemes. These authentication schemes are evaluated based on features of network security such as less work and data load, less power consumption, strong security, efficient use of resources like storage, bandwidth, and energy.
- The trust management schemes are classified in distributed trust management and centralized trust management. These schemes are evaluated based on trust attributes.
- We also present a summary of open research challenges and problems about the key management, authentication, and trust management schemes in wireless sensor networks.
- The rest of this review paper is organized as follows. Section 2 described basics of wireless sensor network security. Section 3 has given a brief description of various security solutions based on key management, authentication schemes, and trust management. Section 4 described the discussion and future direction. Section 5 concludes the paper.

2 Background

The wireless network is based on infrastructure-based and infrastructure-less architecture. The infrastructure-based network requires a fixed base station such as WSN whereas infrastructure-less does not require any fixed base station such as the Flying Adhoc network (FANET). WSN is featured by dynamic network topology due to the fixed or mobile nature of the nodes. The resources like storage, energy, and processing speed available to Mobile Adhoc network (MANET) is also limited. Therefore, the security of the sensor network is difficult to perform in comparison to wired networks. Some basics about wireless sensor network security are depicted in Fig. 3.

2.1 Application of wireless sensor network

The variety of sensors such as light, pressure, humidity, air quality, heat, speed are used in many life-changing applications such as healthcare, nuclear field, electric boiler, air quality monitoring, disaster relief application, military application, and house automation devices [8]. Fig. 4 also depicted the application area of WSN. The recent applications of WSN can be explained below:

1. *Monitoring insect's life cycle*

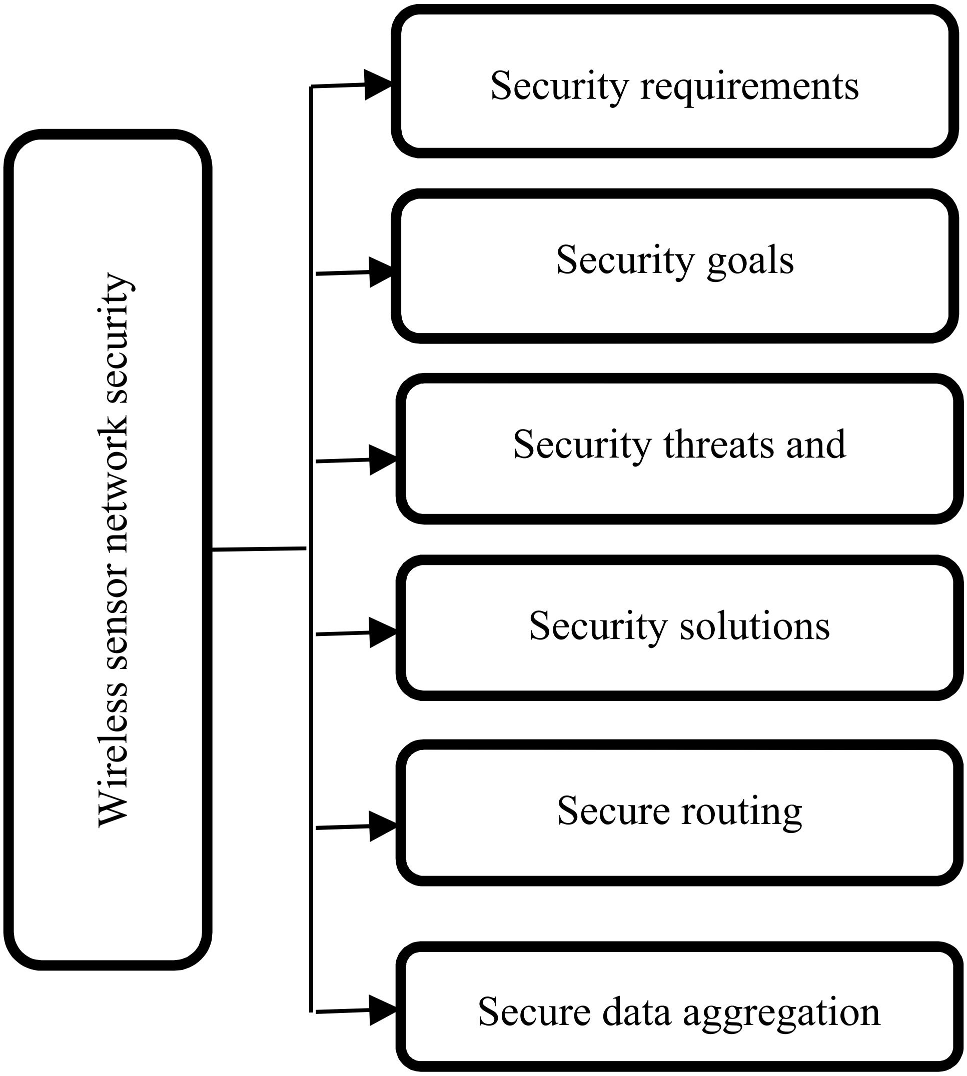
   The monitoring of the insect life cycle can reduce the use of excessive pesticides and reduce the expenditure of farmers. Initially, with the help of different types of sensors users monitor the population growth of insects at different stages of the life cycle. With the help of Carbon diaoxide (CO2) sensors identify the population density of insects at different stages. It is also detected the location and positioning of insects can be communicated by mobile phone via Global System for Mobile Communication and Global Packet Radio Service modules [9].
2. *Monitoring water quality*

   According to the report, more than a hundred million patients registered every year by water pollutant disease, and millions of deaths happened every year worldwide. So, with the help of WSN, we can monitor pH value, acidity, electrical conductivity, oxidation-reduction potential, and Turbidity of water. Therefore, we reduce the toxicity of water and help people to get affected by harmful water [10].
3. *Monitoring greenhouse gases*

   The environment monitoring can help to increase the production of crops with the help of greenhouse gas monitoring which is slowly changing. Zigbee and LoRaare used to monitor greenhouse monitoring. The greenhouse data can be collected and classified with the help of different techniques and produce a predictive model that analyzed the effect of the greenhouse on the environment [11].

Some other applications are WSN is also used in alarm detection and monitor technique in the manufacturing

Fig. 3 Security elements wireless sensor networks



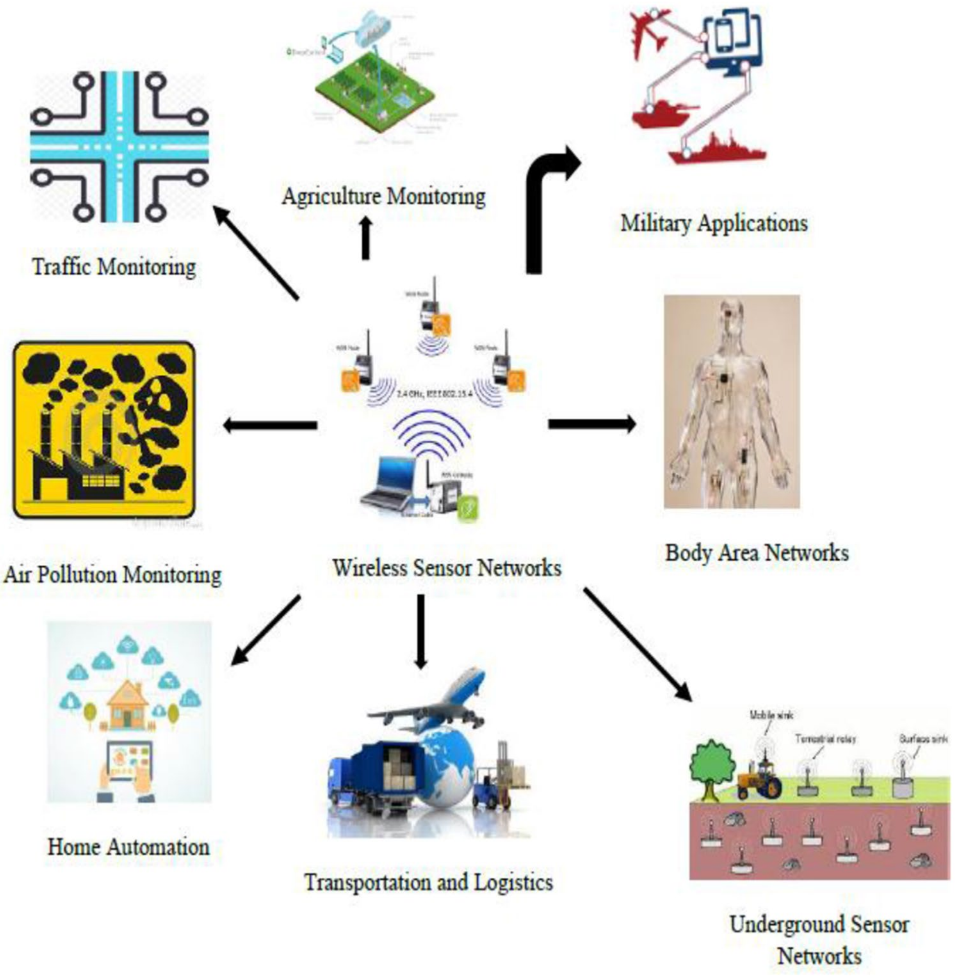
companies. Any abnormal event can harm production and also dangerous to human life. WSN networks can easily detect abnormal events and also fault alarm. The pest control system is also managed by the wireless sensor network. The Pest management system is the application of WSN in agriculture [96].

2.2 Issues and challenges in the security of wireless sensor network

The poor security measures can result in the loss of important, private, sensible data of various applications of the sensor network. It is also causing a loss of customer or user confidence towards WSN. In a worst-case scenario, uncoverable damages can happen due to loss or altered data and information. The other effects of poor security measures such as high network congestion and busy server, loss of trust by the user, and high recovering cost. Design and propose a secure solution for WSN have various issues and challenges [1] [12].

- *Reliability* It is negotiated by the deployment strategy of network, radio connection, power failure, hacking, and various security attacks.
- *Low power WSN* This type of network can be achieving by developing low power microcontroller, lightweight encryption, and decryption algorithms. The battery-powered devices have hibernated and lower consumption modes can help to make low power WSN. Quantum key distribution used in cryptography can also make ultra-low- power WSN.
- *Hacking attacks* The study says that 40% of smart devices are vulnerable to security attacks in 2016. The home security system uses a smart device called Comcast which is using Zigbee standard which can be hackable by a radio jamming device. In 2017, the Distributed Denial of Services (DDoS) attack can be triggered

Fig. 4 Application of WSN



by a worm named Mirai can be affected by around 2.5 million IoT devices. Another worm called Reaper has infected around 1 million smart devices.

- *Vulnerabilities of networking devices* There are more than 500 million smart devices connected every month using IoT technologies. The main security threats for these sensor-based devices are privacy, authentication issue, mobility, physical capture, security configurability, design faults, and cloud interface security.
- *Data integrity* The transmission of data from source to destination safely by using cryptography. For successful data transmission, it can use checksums, timestamps, and hashing techniques.
- *Limited Resources* A sensor/node is a small device which has less amount of memory. To propose an effective security solution, it is always considering the size of the algorithm. Some commonly used sensors have commonly used 10Kb of random access memory, 1024Kb of flash memory, and 48kb for program memory. Also, embedded operating and software are taking a small amount of memory.
- *Power Limitation* Power Limitation is the main restriction to these sensor devices. We consider that, after the deployment of sensors in the target area, it cannot easily replaceable and rechargeable. To propose an effective security solution, the security algorithm must use low power cryptographic function, encryption, decryption, cryptographic keys, and digital signatures.
- *Unreliable Communication* Unreliable communication is also dangerous for WSN security. The algorithm must consider factors such as latency, conflict, etc. to defend against unreliable communication. Unreliable communication is caused by broadcast communication where packets are transferred through the unsecured channel. It may cause damage or loss of the packets due to some channel errors. If there is no proper error handling technique, then it is possible to lose secure packets. There is a confliction that, if there is a secure channel then also a chance to lose some packets due to the dense nature of sensor deployment and wireless communication. Also, latency is a great challenge in unreliable communication. Network congestion can cause large latency in the

network which causes difficult synchronization in the sensor network.

2.3 Security requirements

WSN is an important kind of network. Security solutions must fulfill the following requirements. These requirements are unique and well suited for the WSN network [12].

2.3.1 Data confidentiality

Data confidentiality is a very significant requirement in network security. In any kind of network, the security solution for communication devices considers this requirement first. Confidentiality of any WSN must consider as following [13].

- The sensors must not reveal the observed data to its neighbors or any other node. In some applications the data are highly confidential and secure so, revealing data must fail the purposes of the entire network.
- In several applications nodes transfer very sensitive information, e.g., secure keys, distribution, hence it is very important to make channels secure in WSN.
- Some information related to the sensor such that identities, public keys, and other cryptographic information stored in sensors in encrypted form. It can be protected from passive attackers and traffic analysis.

2.3.2 Data integrity

If data packets are secured by encryption techniques and secure keys, then the adversaries cannot be able to read or steal data but still, it can add some bogus data or any dangerous script with data. a malevolent node might add some trashes or change the data in the information packets. These modified data are not able to use for the network and it can be harmful for network communication. Therefore, data integrity guarantees that any received data has not changed during transmission.

2.3.3 Data freshness

As data confidentiality and integrity have importance in data security similar way the data freshness is also needful for network communication. The data freshness recommends that old data is not used and data must be recent. The cryptographic keys must be refreshes, renew, and changed with time. The data freshness can able to prevent a replay attack. Timestamps and nonce are used to solve these issues.

2.3.4 Availability

We must design a lightweight and reusable secure solution for WSN. Because the addition of some extra features in security algorithms can consume more energy. If sensor nodes are dead early then the availability of data will also reduce. This feature of the security requirement is availability. The data must be available during the lifetime WSN.

2.3.5 Self-organization

A WSN is a typical wireless network, which needs all sensor nodes are self-regulating and flexible enough recoverable, self-organizing and self-healing conferring to diverse situations. Due to dynamic infrastructure, network management in WSN the sensor must be self-organizeed according to the need for a secure network. If self-organization is missing in WSN, the loss resulting from security threats in a dangerous environment may be disturbing.

2.3.6 Time synchronization

Some of the application of WSN needs time synchronization. The sensors just need to turn off when it is not required. It must be turned on whenever required. The time synchronization has saved more energy and useful for WSN security.

2.3.7 Secure localization

Any adversaries can easily manipulate the information of non-secure located sensors. If an adversary can manipulate the data by false signal strength or replaying signals to non-secure located sensors. So, the localization of sensors must be secure and accurate.

2.3.8 Authentication

Authentication is an important attribute of communication security. This property assures that any data comes from a trustable source. If there is communication between two nodes, then the sender node wants to assure that it is the legitimate node of the network and the provided data are valid. In other nodes verify that data or message comes from an authenticated and trustable source.

2.3.9 Accountability

Accountability requires that the behavior of an individual must be attributed solely to that entity. Accountability is becoming critical for problems such as non-repudiation, fault isolation, intrusion detection and avoidance, rehabilitation after action and legal action.

2.3.10 Survivability

Although security concerns are focused on avoiding attacks on information infrastructure, the longevity of the system is concerned with the resistance, detection, and recovery of failures or attacks. Survival is characterised as the ability of a system to perform its task promptly in the face of threats, disruptions, or incidents. Survival shares priorities with defense and improved security will boost the overall potential of the device to survive attacks. Besides survival includes functionality that go beyond security concerns.

2.4 Security attacks

The security solutions must adopt the new techniques and methods to provide security against adversaries, several security threats, intruders, sniffers, malevolent devices, hackers, ransomware, and active/passive attacks. The spoofing attack is countered by an event-driven control strategy. There are various security attacks at each layer of WSN which are given in Table 1[14][15]. Some threats are classifying as following.

- *Tampering* The sensors are made to works in outside environments. Therefore, it is highly vulnerable to a physical attack like node capturing. The attacker can capture the node and temper its cryptographic information which can be compromised the whole network.
- *Blackhole* A node is falsifying the pathfinding operation and it could advertise that some false route is the best past and efficient path for communication. Therefore, it can attract all packets towards itself. Sometimes it is dropping all the packets which are difficult to recover.
- *DoS attacks* A denial of service (DoS) attack is harmful to WSN which causes network capacity decrement and blocked various services. Many key management schemes offer a unique node ID assignment where every node gets its ID by using a secure public-key cryptographic approach. So, by this approach, no sensor node required any buffer to store messages and prevent false message injection in the network
- *Node capturing attack* The nodes are physically attacked and capture information stored in it. The attacker can compromise the node's information such as cryptographic keys, identity, and other important information.
- *Selective forwarding* This type of attack consists of a malicious node that behaves like a router as depicted in Fig. 5. In this attack, the malicious node drops some packets and may deny forwarding those packets or messages.
- *Eavesdropping* This refers that any unauthorized user or malicious node can observe the traffic of communication. The main aim of this threat is to observe the factors (routing information, frequency, etc.) of traffic, communication contents, and finding the information's about the nodes.
- *Sybil attack* In the Sybil attack, any adversary node has multiple IDs in the network. In our proposed ID assignment scheme every node ID has a combination of an initial ID and the public key of the node, which is signed by the cluster head and sanctioned by the known node. Therefore, the adversary node can't generate the Sybil ID without compromising the known node and cluster head. Sybil nodes are also identified by monitoring the consumption of residual energy.
- *HELLO flood attack* A lot of routing protocols use the topology of the network by using the "HELLO" packets. The advisory node sends a flood of "HELLO" packet and blocks the communication among nodes in the network.
- *Jamming* The radio communication is used in transferring packets between nodes is disturbed by the adversaries. A strong jamming device can have blocked the signals or create noise in the signal by disrupting communication.
- *Exhaustion*: A adversaries' node can transmit lots of bogus packets. By processing, calculating, and validating these packets the sensors lose lots of power.
- *Wormhole attack* In this type of security attack any malicious node could be placed at the different ends of the network. The majority of the packets could be accessed and replays.
- *Identity replication attack* Adversaries can copy or clone the nodes in the network. So, it can able to access the majority of the traffic. This is a legitimate ID of any node which are assigned to a fake node.

Table 1 – Security attacks

Layer	Attacks
Application layer	Data Repudiation, Data corruption
Transport layer	Session Hijacking, flooding
Network layer	Wormhole, Blackhole, Flooding, Resource Consumption, Location Disclosure attack
Data Link layer	Traffic Analysis, Monitoring
Physical layer	Jamming, Eavesdropping
Multilayer attacks	Man-in-middle attack, Denial of Service

2.5 Security constraints

When we proposing any solution for security problems in WSN then we need to consider the following constraints [16].

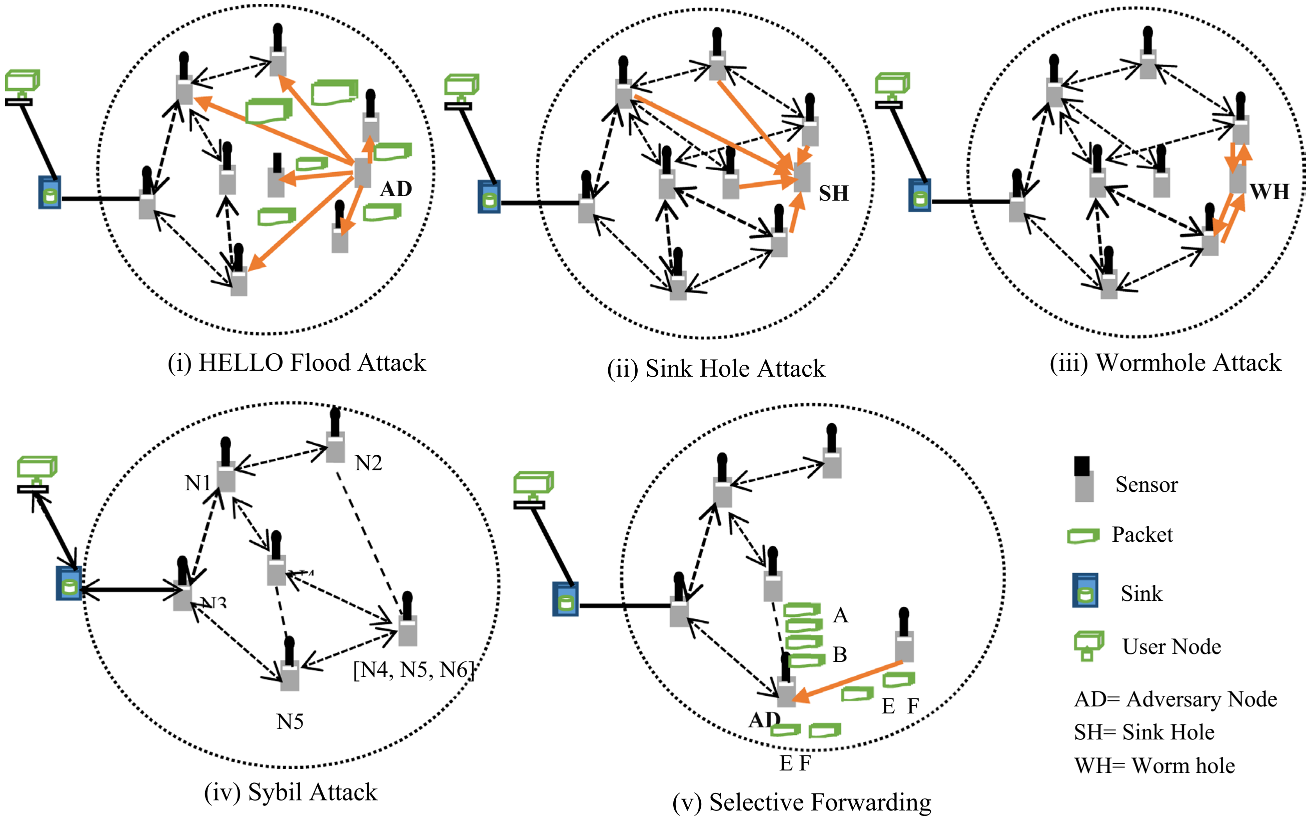


Fig. 5 Security attacks in WSN

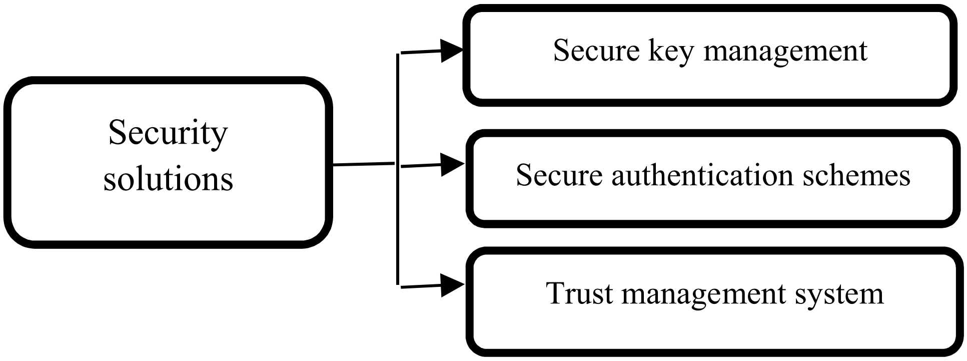
- Lightweight: Due to the resource constraint environment of the sensor network, the security algorithm must take minimal operations and resources. The security algorithm or solutions and all its services are energy efficient, computationally easy so-called lightweight solutions.
- Decentralized: All the sensors are connected so, at any point in time any node will compromise then compromises the whole network. Therefore, we must design our security solutions is decentralized. If any part of the security algorithm will have failed, then it will not affect the other part of the network.
- Reactive: The security solution must react to changes made in the network. The sensor networks are dynamic in nature and work in also real-time environments, Therefore, the solutions must adopt these environments and positively reply to spontaneously and unannounced security threats.
- Fault-Tolerant: The medium where the sensor nodes communicate is unsafe and unreliable. Wireless mediums must-have the capability to detects and recover from these faults. The security solution must take these faults seriously and must include them.

3 Security solutions

As the services provided by IISN increases rapidly therefore the opportunities for security services providers also increase. There is a decent chance for the WSN security companies to launch payable security services to gain profit. These technological companies like IBM launch a security services bundle called IoT solutions practice which bundles security algorithms and security solutions. IBM added the groups of APIs with several safety facilities such as authenticity, scanning, blockchain technology, and other safety solutions in a bundle called the Watson IoT platform. Here we consider trust management, key management and authentication methods (Fig. 6) are the main approaches to provide solutions against various security threats. Some security methods are deliberated to confirm that the security vulnerabilities shall be prevented in an intelligent transportation system.

The recently emerged blockchain technology can provide a secure method to offer authentication in WSN and IoT, because of its cryptographic attributes

Fig. 6 Security attacks in WSN



and decentralized property. Blockchain protocol was proposed for exchanging cryptocurrency bitcoin. The blockchain features can be improvised trustworthiness, unforgeability, reliability, and fault tolerance make a blockchain method is a powerful approach for authentication. Blockchain provides incorporation of smart contracts that gives access control method for communicating devices. Blockchain technology provides a good platform to create and manage distributed and decentralized authentication system for WSN and IoT systems [97].

According to the author, they are the first to use a key management approach for sensor network based on blockchain technology. Blockchain technology can be overcome many limitations of the traditional key management system. Blockchain has many advantages such as decentralization, energy consumption, temper proofing, and deployment. They proposed blockchain-based key management which has less dependency on the base station. This method provides trustworthiness, security, and reliability [98].

3.1 Key management schemes

To be responsible for secure communication, the messages are encrypted by secure keys and provide authentication for the sender node. The single key-based key management schemes are very efficient and less complex, but the adversary can easily detect the key compromise in the whole network.

Therefore, sensor networks use more than one keys based scheme to secure the network. Several key distribution techniques are used in WSN. Some key schemes are depicted in Table 2 [17].

Key pre-distribution distribution distributes the key before the placement of nodes in the working field. So, nodes may communicate by using these secret keys [18]. The keys are pre-distributed and work in three phases: key generation and initialization, key discovery, and establishing of path key [13]. A secret path is created when nodes distribute common keys and communicate via these links. In the key pre-distribution method, the keys are choosing randomly from the key pool [14].

Last few years, different researchers have proposed several key generation and distribution approaches [18–20] for sensor networks. These approaches have used both

Table 2 Key distribution scheme in WSN

Key distribution schemes	Description	Advantages	Limitations
Single network wise key	Each network has only one key to use for encryption and decryption of messages.	It is simple, less complex, scalable, data aggregation and able to organize	It is easy to compromise and lack robustness.
Pair-wise key	In any network, every pair of nodes uses one key for encryption and decryption of the message.	Provide authentication, scalable, maintainable, and robust	High complexity, costly, not scalable, and not easy to organize
Hybrid keys	This type of key distribution method network has been divided into several groups. For a group to group communication, it uses a network wise key, and inside every group it uses a pairwise key.	It provides scalability, easy to organize, multicast, and robustness	Storage is high, need cluster management algorithm

symmetric and asymmetric key management schemes based on various parameters such as computation complexity and power consumption. Many techniques have been proposed for the establishment of key distribution and secure key management. Figure 6 depicts a taxonomy of various key management schemes. In the following, we highlight the key generation and distribution approaches into families and designates the most relative content.

3.1.1 Random key distribution based schemes

Eschenauer et al. [21] proposed an initial key management scheme for WSN. This key management scheme comprises three phases, first is key pre-distribution, sharing keys, and path-key formation. It considers that a node has a fixed set of keys called key ring which is selected arbitrarily without replacement from a set of an enormous number of keys called key pool. In the key ring, each key has linked with the ID of sensor nodes. This information must be stored in a controller node. This controller node is trusted by the network. Chan et al. [22] proposed a Q-Composite key management scheme that gives random key pre-distribution and multipath key reinforcement. It is also called a random pairwise key distribution approach. Q-Composite has a different kind of trade-off. The Q-Composite scheme is a powerful solution for security under little threat and it also detects high-level attacks. Du et al. [23] proposed a matrix-based random key management scheme. The matrix-based scheme maintains a matrix where c number of keys randomly selected from a large set of keys called a key ring. Pairwise keys are selected which are common in the key ring. This scheme provides authentication and also consume less energy. It supports robustness in the network.

3.1.2 Master key-based key management schemes

Another key management scheme that enhanced the security of keys is based on the master key of the Diffie-Hellman algorithm. Gandino et al. [24] proposed a master key-based key generation and distribution scheme to manage symmetric keys. With the help of master keys and global puzzle or secret to initialize and produce pairwise keys. By these keys, a secure communication environment for WSN is formed. Zhu. et al. [25] have given a key management scheme called Localized Encryption and Authentication Protocol (LEAP+). The LEAP+ scheme is to produce keys by using the transitory key. The transitory key is the combination of the master key and ID of the nodes. This key helps to adopt different types of keys according to the messages. Mainly, the pairwise key generation is the core of this scheme. The above schemes provide more security against clone attacks and reduce initial key setup time. The main threat is that when the master key is compromised then the security of the network is at high risk.

3.1.3 Location-based key management schemes

Younies and Eltowieissy [26] proposed a location-Aware combinatorial key generation and distribution scheme. This method uses a location and Exclusion Based System (EBS) for key generation. Based on location, the generated keys are pairwise, randomized, and unique. It is also called SHELL because SHELL stands for scalability, hierarchy, efficiency, location, and lightweight. This scheme offers regeneration of keys and improves the network safety against several threats such as node hijack and node compromise. The key management responsibility is distributed among all the nodes so, the computation complexity and storage overhead are reduced. The overload of the central node or base station is also avoided. In this scheme, the location is the key element to compute the pairwise key between nodes. The SHELL provides defense against the collusion attack. These key management schemes support the change of network size which means node addition or deletion and also refresh the key by factoring the geographic location of nodes. Choi et al. [27] had given key generation and distribution techniques based on location. This approach uses grid-based coordinates to generate keys for the network. It is used nine data coordinates and eight neighbors coordinated. With the help of these coordinated the pairwise keys are established in two phases of the network. It also uses the sequence number of each packet sent by nodes. This method provides security against various insider and outsider threats.

3.1.4 Tree-based key management

Qin et al. [28] proposed an Elliptic Curve Cryptography (ECC) and Adelson-Velsky and Landis (AVL) tree-based key management approach to secure the sensor network. The AVL tree is used to the public key of each node and their ID of a neighbor node. This key management approach is efficient in terms of energy, computation time, storage cost, and communication cost. This approach also uses Elliptic Curve Paillieer Encryption (ECPE) cryptographic technique to defense against various security threats. This approach included another feature where keys are updated frequently. Yao et al. [29] have given a key distribution approach called Local Key Hierarchy (LKH++) for a cluster-based sensor network. In LKH++, keys are maintained and saved in a tree data structure. These keys are used for cluster or group. The tree can be maintained by the sink node. This scheme regenerates and rekeying the keys when required for the network. LKH++ improves network security and robustness against node capture attacks in the sensor network. Swaminathan et al. [30] proposed a scheme where the structure of the wireless network is developing with a combination of Distributed Spanning Tree Structure (DSTs) and effective low-cost key generation method. The Low-cost Key Management Model (ELWKM) is more effective in terms of energy cost, time, and storage. Chen et al. [31] gave an effective public key cryptography-based scheme which is an aggregation of several encryption/decryption methods, Bloom filter, and the Merkle hash tree. The elliptic curve discrete logarithm problem uses to establish a key management scheme by using key threshold theory.

The tree-based key management schemes give better performance on storage, computation, and communication overhead. It also provides perfect scalability where the network gives the same performance during node addition and removal.

3.1.5 Polynomials based key management schemes

There are several polynomial based key distribution approaches proposed by research fraternity in recent years. Shamir [32] introduced the first polynomial based scheme in their paper to implement threshold secret sharing. To certify safe inter-group communication, Lu et al. [33] proposed a unified framework using classes of nodes and the degree of a polynomial for a distributed key management approach in heterogeneous WSN. In this framework, they generated a random bivariate polynomials pool to establish a key between sensor nodes. This framework also considered various parameters of heterogeneity in the network. Fan et al. [34] proposed a key management method based on lightweight polynomial for distributed WSN. This protocol mitigated common security attacks and also provided secure communications via one to one and many to one using polynomial based keys (pairwise key, cluster key, and group key) and also provided authentication using a probabilistic local broadcast authentication protocol among neighboring nodes.

Wang et al. [35] proposed a polynomial - inspired key management scheme to offer the security of personal key shares. It uses p-degree polynomial F(x) for secure inter and intra class communication. Consider a network having two groups of sensors, the first group called G1 and the second group called G2. If P(v) is a key used by a member of group G1 to encrypt the multicast message to members of group G2. To decrypt this message using key P(x) by members of group G2 received by members of group G1, the group controller assigns a polynomial to each member of G1 and G2. In this key distribution scheme, a revocation polynomial and a particular one-way hash function are used to defend against the collusion attack. The broadcast communication is updated by revocation polynomial which is generated by a one-way hash chain utilization method. This scheme shortened the communication overhead and removes the collusion attack.

Suganthi et al. [36] calculated the keys (individual keys and the pair-wise keys) during initialization using polynomial functions. In their approach, the base station shared the individual key and the neighbor nodes shared the pairwise keys. The other nodes shared the group keys. So, by this method, the communication overhead is reduced. Anita et al. [37] had given Q-composite random scheme based on polynomial, which generates a triple key for communicating among the sensor nodes. This is the polynomial pool-based method to establish secure communication between them. Sun et al. [38] have proposed a key management scheme based on polynomials by self-heal keys. The improved polynomials and broadcast authentication scheme can provide secure communication and collision resistance. It is using a group of sliding-window and improved polynomials to produce pairwise keys among the controller node and other sensor nodes. The two unique approaches Sch-I and Sch-II were also proposed. The Sch-I method proposes the idea that pairwise keys are established and shared between the controller node and other sensors. Sch-I can be updated dynamically according to the network. Sch-I declines the vulnerability as other nodes do not have any information about this polynomial. The forward security is provided by a one-way hash function while backward security by using the modified polynomial. Sch-II removes the hash chain and strengthens security. In this method, they improved the collision resistance and avoided the flaws of acceding polynomials. Zhou et al. [39] proposed a unique, effective, and dynamic key management approach for sensor networks. There is a combination of ECC, p-degree, and trivariate symmetric polynomials that were combined to generate efficient keys. The time slice mechanism is used to update the key dynamically. The one-way hash chain technique was designed to lower the cost for communication in the key generation and update process.

Ramkumar et al. [40] have given a novel approach in key management using Chebyshev polynomials to generate keys for ad hoc networks. They used properties of Chebyshev polynomials to secure communications. Jing et al. [41] have proposed a symmetric polynomial which is based on a calculation-based algorithm. By using the homomorphism encrypted mechanism, it generated pairwise keys. By this approach, the network is protected from node capture attacks. Due to the properties of an asymmetric polynomial, these pairwise keys are unique, random, and strong which fulfills the requirements of a good key management scheme. Zhan et al. [42] proposed a system of an equation-based key management scheme to produce pairwise keys among sensor nodes. By these pairwise keys, the sensor network communicated and transmitted messages secretly. The system of equations has properties that all the equations have only one solution. So, the established keys are lightweight, efficient, and secure. The cutting point of linear equations is used to generate secret shared keys. These pairwise keys are used to protect the network from various attacks in sensor networks. The keys are generated by the equations called the associated key. Due to the complexity of polynomial equations, this method uses linear equations that have only two variables and Exclusion Basis System (EBS) to generate keys and implement the key management in that network. The advantage of this approach is that it provides a good key establishment in comparison to other ordinary key schemes and also other performance metrics are unaffected.

Dinker et al. [43] proposed a multivariate symmetric polynomial and matrix-based key management scheme. This scheme uses polynomial and matrix to generate keys between the sink node and the cluster head. The protocol can make a secure network for future communications. It can maintain the matrices at the sink node, multicast control node, and cluster head node. When any node is updated, then due to multivariate symmetrical polynomial, matrices are also updated. In this method, the key management and authentication effectively work with sensor nodes and also give efficient results when nodes are updated frequently.In the IoT platform, scalability is a major issue to provide security because of the heterogeneous and dynamic nature of devices.

There are certain criteria by which key management schemes are evaluated to provide secrecy against various attacks. The key management technique must fulfill certain criteria for the efficient transfer of the message and secrecy of data. The key management schemes are needed according to the application of the network. The comparative study of key management schemes is summarized in Table 3.

3.2 Authentication schemes

The primary aim of authentication is that it provides the authenticity of the source node.

Authentication schemes can provide some features of network security such as less work and data load, less power consumption, strong security, efficient use of resources like storage, bandwidth, and energy. There are several lightweight authentication schemes based on direct and indirect trusts, XOR operation, hash function, ECC, public-key encryption, and many more method. Figures 7 and 8 shows the classification of previously proposed authentication schemes in WSN [44]. (Table 4)

3.2.1 Lightweight authentication scheme

As much as fewer resources utilize by any authentication schemes come in this category. To uphold secrecy at lightweight attributes, the two-factor authentication scheme played a key role. The enhanced scheme of the two-factor authentication scheme is a three-factor authentication scheme. Several versions of the three-factor authentication scheme are proposed by authors. Das et al. [45] proposed asymmetric keys based three-factor authentication scheme. This temporary credit-based scheme is secure and robust. It is using biometric authentication and smart card-based security. This method is efficient in terms of computational and energy. This three-phase authentication scheme has limitations such as not resilient against the desynchronization attack which was removed by Wu et al. [46]. It also gives improved schemes of three-factor authentication schemes. This scheme provided a mutual authentication scheme that secure data transferred among sensors, cluster head, and sink node. The security verification is proved by the Proverif tool. Jiang et al. [47] proposed an advanced version of three factor-authentication and removed flaws in other three-factor authentication are based schemes. These lightweight authentication schemes based on Rabin cryptology. The typical attributes Rabin cryptosystem is a computational anomaly. The verification operation of the local password by using fuzzy verification. Timestamps are also used to protect against session, internal and external attacks. Shim et al. [48] had given an authentication approach that had given services which are message retrieval. The random oracle model is used to provide security. This scheme is named BASIS(multi-user broadcast authentication scheme) which uses multipurpose identification. An identity-based scheme is also used in this approach and it is simulated on MICAz and Tmote Sky WSN platforms.

Xue et al. [49] proposed a password-based authentication scheme. The author realized that the gateway node has worked as a firewall between the outside and inside the network. So, this approach provided a temporary credibility point to every node by the gateway. This temporary credit value connects with the identification of the node.

Based on this we decided the authenticity of the node. XOR operations and hash value used in this approach make it lightweight. Delgado–mohatar et al. [50] had proposed an authentication scheme by using some cryptology primitive in WSN. This scheme provides a lightweight encryption and decryption algorithm to authenticate any honest node in WSN. The proposed approach consumes less energy and communication cost. Shah et al. [51] proposed a secure scheme based on the Chinese remainder theorem and Fermat number transformation to provide authentication. This authentication uses cryptographic

Table 3 Comparison between several key management schemes

Key management schemes	Type of structure	Security agent	Authentication	Advantages	Limitations
Eschenauer et al. [21]	pairwise	Key pool and key ring	No	Uses less storage adjustable, robust least storage cost, simple and implementable	Less accessibility, not supported group based structure
Chan et al. [22]	pairwise	Q-Composite key management	No	Multipath reinforcement, defense against high-level attacks	Complex, less scalable
Du et al. [23]	Pairwise and network wise key	Matrix	Yes	Simple and adjustable, Energy cost remains reasonable. robust	More complex, not supported group-based network and less accessible
Gandino et al. [24]	Symmetric and pairwise	Master key	Yes	Scalable, energy-efficient	Storage complexity is high, Take more time to initial setup
Zhu. et al. [25]	Group-based, pairwise	Transitory key	Yes	Reasonable complexity and scalability	Initially weak security, high storage cost
Younies and Eltowieissy [26]	Pairwise and randomize	Location and Exclusion Based System	Yes	Scalable, efficient and light-weight	Complex and storage cost is high
Choi et al. [27]	Pairwise	Location and grid data	No	Secure against several threats, unique, self-adjustable	Not scalable and robust
Qin et al. [28]	Public key based	AVL tree and Elliptic Curve Paillieer Encryption	Yes	efficient in terms of energy, computation time, storage cost and communication cost	More complex in nature
Yao et al. [29]	Cluster based	Tree structure	No	Rekeying and refreshing. Secure against node compromised attack	Complexity and communication cost is high
Swaminathan et al. [30]	Cluster based	Distributed Spanning Tree Structure	No	Low cost	Storage and computation is high
Chen et al. [31]	Public key	Bloom filter and the Merkle hash tree	Yes	Fast, energy efficient, secure against various attacks	More complex in nature, scalability is low
Lu et al. [33]	Asymmetric pre-distribution	Pre-configured keys	No	Perform well in the heterogeneous model and perform in terms of connectivity, reliability, and resilience	Higher cryptographic overhead
Wang et al. [35]	Group key distribution	Special one-way hash key chain	Yes	Strong collusion attack resistance capability	Difficult to set up securely group management
Suganthi et al. [36]	Pairwise keys and group keys	Pseudorandom function, ID	Yes	Low overhead in computation, communication, and storage	Issues are large scale key distribution, authentication of mobile nodes
Anita et al. [37]	Triple key structure	Polynomial based Q composite random function	No	Resilience against node capture attacks	Nonadjustable security strength
Sun et al. [38]	Hierarchical	Modified access polynomial, entropy, Hash function	Yes	Enhanced forward security, backward security, and collusion resistance capability	Some nodes may not be reachableLow accessibility

Table 3 (continued)

Key management schemes	Type of structure	Security agent	Authentication	Advantages	Limitations
Zhou et al. [39]	Hierarchical	t-degree			
trivariate symmetric polynomial	No	Resilience against node capture and reduced communication overhead	Does not address key revocation or node addition		
Jing et al. [41]	Static	Two element symmetrical polynomials	No	Resist the large-scale node capture a ttack	Partial keys may not be strong enough against analysis by widely available highcomputational platforms
Zhan et al. [42]	Group, pairwise	Elliptic curve discrete logarithm problem (ECDLP)	No	Mutually trusted key generation center (KGC)	Complex and high complexity
Dinker et al. [43]	Symmetric	Polynomial and matrix	Yes	Multicast, key regeneration	Higher cryptographic overhead

techniques and fulfills the requirements of authentication. According to the author, this scheme protectsthe network against DoS attacks, replay and clone attack, the man in the middle attack, and secure communication. Shen et al. [52] proposed a source authentication of the source node in the wireless healthcare network. This protocol has castoff one too many and non-interactive authentication approaches which give confrontation against several threats. Some other authentication techniques [53], [53] also provides a lightweight solution to authenticate the source node.

3.2.2 ID based authentication

In this type of authentication, identity behaves as a key element to provide defense against various security threats in mobile ad hoc networks, vehicular networks, grid networks, smart cards, and different WSN applications. This type of protocol supports to create of a secure, reliable, scalable, resource proficient, low computation, and suitable protocol for WSN. Li et al. [55] give an authentication approach that is based on certificate-less cryptography. In this paper, the author points out some problems related to ID-based authentication such as key escrow problems and problems related to certification. These problems can detect and solved by using conditional preserving authenticity. Therefore, this authentication scheme provides resilience against many threats. Farah S. et al. [56] provide secure authentication among the base station and all sensor nodes.

This scheme has used in a cluster or hierarchical WSN where a node is selected as cluster head and the rest of the nodes are called cluster members. So, all cluster members have an identity and in their public key, identity plays an important role. The public key drive by the identity of the nodes. The energy consumes during certification and identity-based authentication is the same. This protocol works in two-part. The first part deals with the delivery of private keys and in the second step transferring data securely. Zhu et al. [57] proposed ID based authentication scheme where the number theorem research unit lattice and rejection sampling method are used. This scheme protects against random oracle attacks and quantum computer attacks.

3.2.3 Broadcast authentication

Broadcast authentication techniques are useful in hostile and remote areas. This approach is beneficial for the isolated, remote, and inaccessible field. This approach must fulfill the evaluation criteria such as low computation overhead, instant verification, time synchronization, and defense against several security threats. Based on broadcast authentication generation, i

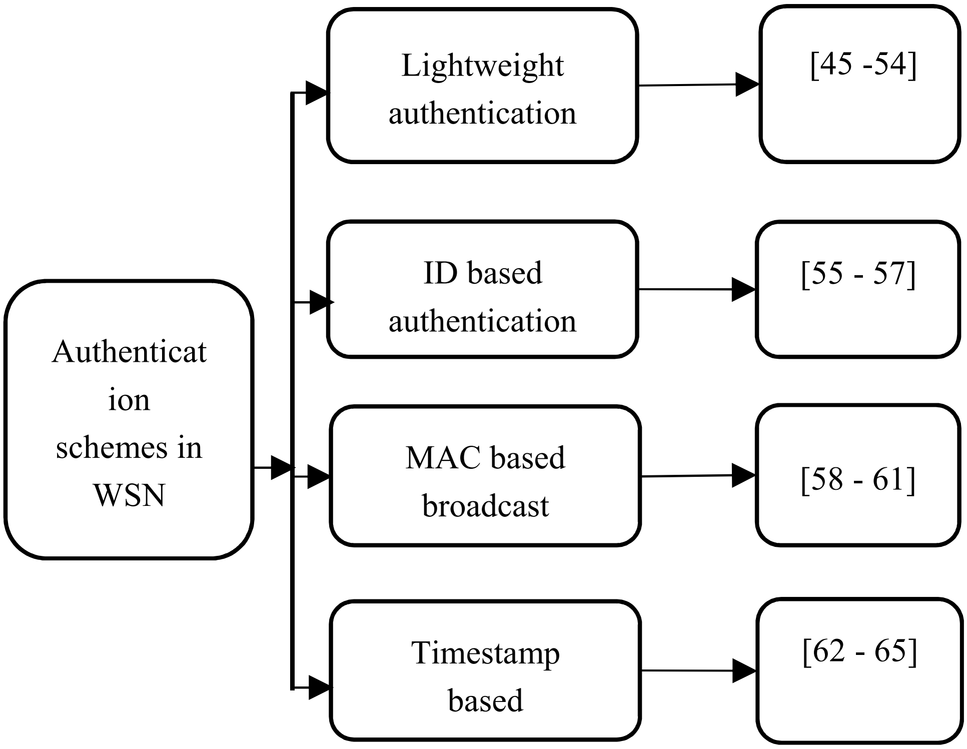


Fig. 7 Classification of the authentication scheme in WSN

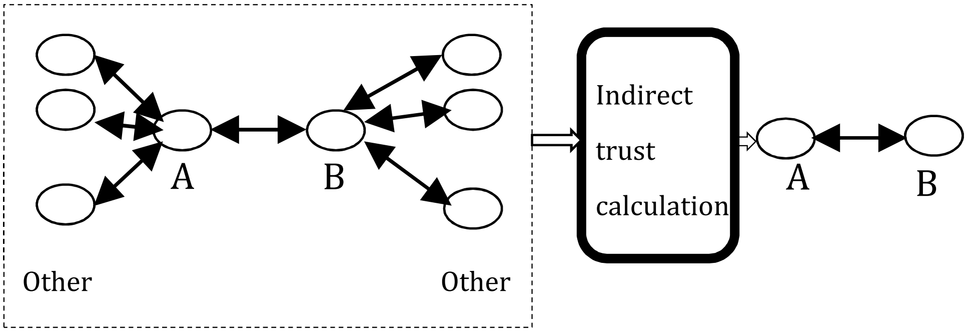


Fig. 8 Indirect trust calculation model

It has mainly two categories, first is authentication using signature and μTesla. The first approach which using signature can establish asymmetric properties by using crypto primitives. There are some issues identified by Chang et al. [58] which are as follows:

•Using the large key size
•In some broadcast authentication schemes only, few messages are authenticated but not all messages.

It authenticated the messages by issuing public and private keys by using their personal information the cryptographic keys are generated and verified. This approach has many benefits over an earlier approach like reducing the number of buffers, synchronization of time, and instant authentication.

Shim et al. [59] proposed an authentication scheme called an efficient identity-based broadcast authentication scheme (EIBAS) for a huge density of nodes and not the mobile base station. This approach contained four stages: the first system initializes, the second cryptographic key mining, the third creation of signature, and the fourth broadcast authentication. The random number and hash function are used to create a prime generator and the current timestamp is used to generate the signature. After that broadcast that message so, every node can verify that message. Chowdhary et al. [60] use a one-way hash algorithm for authentication called A lightweight one-way cryptographic hash algorithm (LOCHA). First, convert the normal message into American Standard Code for Information Interchange (ASCII) form then it breaks the message into packets of

Table 4 Comparison of several authentication schemes

Authentication protocols	Type of authentication scheme	Methodology used	Security agent	Advantages	Limitation
Das et al. [45]	Lightweight	Three-factor authentication using biometric and smart card-sbased security	Biometric information	This scheme secure and robust	Not resilience against desynchronization attacks
Jiang et al. [47]	Lightweight	Advances three-factor authentication using local password by using fuzzy verification	Rabin cryptology	Protect against session, internal and external attacks	The complex structure of the security parameter
Shim et al. [48]	Lightweight	A private key generator is liable to generate private keys for users.	Random oracle model	Provides message integrity, and reduction ofcommunication overhead	limited storage capacity
Xue et al. [49]	Lightweight	Password-based authentication scheme using adaptive gateway node	Credit value assigned by the gateway node. XOR and hash operations	Supports Data integrity, Immediate authentication Time synchronization Communication	Cloning for credit value, Faulty credit value
Shah et al. [51]	Lightweight	This scheme utilizes Fermat NumberTransform (FNT) and Chinese RemainderTheorem (CRT) for authentication	Chinese Remainder Theorem (CRT)	Achieve security requirements efficiently and data freshness	High complexity
Li et al. [55]	ID-based	This authentication method uses a reprogramming approach	Re-clustering, certificate-less cryptography	Less execution time and minimum number of verification	Challenge against dense network
Farah et al. [56]	ID-based	The public key and identity-based authentication scheme	Identity and public key	energy consumes during certification and identity-based authentication is less	Challenges against node compromised and identity theft attack
Chang et al. [58]	Broadcast	Secure keys generation and verification	Personal information	reducing storage, synchronization of time and instant authentication	Time complexity is high
Shim et al. [59]	Broadcast	Broadcast based authentication by keys mining and verification	Random oracle model	Provides message integrity, and reduction ofcommunication overhead	limited storage capacity
Chowdhary et al. [60]	Broadcast	Convert normal message in ASCII format and breaks into some different chunks	the one-way cryptographic hash algorithm	levels it maintains uniformity and minimizes storage and communication overhead	High complexity
Moinet et al. [62]	Timestamp	Combination of load and header is used as a block and used in blockchain algorithm	Blockchain	Fast, storage efficiency, availability, and scalability	Contain only initial information to calculate a trust-based score
Indra et al. [63]	Timestamp	ECC based public-key cryptography and timestamp	timestamp	Session-based attack resistant	Complex nature and high cost
Ren et al. [64]	Timestamp	A public key and signature are used to generate certificate by Certificate Authority (CA) which are used for authentication	Bloom Filters, Merkle tree	Secure against various active and passive attack	Computational cost, Tree maintain cost

Table 4 (continued)

Authentication protocols	Type of authentication scheme	Methodology used	Security agent	Advantages	Limitation
Sharif et al. [65]	Timestamp	It has produce comparatively less number of keys to achieve security for nodes before deployment and reduces the communication overhead	timestamp	Less computational, communication requirements and overhead	Maintainability issue
Subhasish et al. [68]	Lightweight	Energy-efficient re-authentication techniques	XOR operation and hash function	Resilience against DoS attack, tracking attack, data leak attack, and identity theft attack	Not resilience against desynchronization attack

size 512. This packet again breaks and nested of size 8 bit, 64 bits 128 bits and 256 bits. Therefore, swapping and transforming among levels maintains uniformity and minimizes storage and communication overhead. Another broadcast authentication technique [61] uses a signature approach to validate messages which are broadcasted. Consider k block of message, each block can authenticate by previous block authenticator and it will verify up to verify k messages. No time synchronization is needed and provides high security.

3.2.4 Timestamp based authentication

The linked chained authentication technique used by Moinet et al. [62] provides trust-based security in WSN. Here the combination of load and header is used as a block. The load is generated by the authority when any sensor node is added to the group. These payloads contain the public key and cryptographic information. So, the credential payload helps to verify that the block is valid. Here the problem is that it can contain only initial information to calculate the trust-based score. Indra et al. [63] have given an authentication approach for mobile ad hoc networks by using a timestamp and ECC based cryptography to validate the message. It is a mutual authentication scheme using time synchronization. The ECC is lightweight, fast, and contented with the dense environment. This approach efficiently manages the session and provide defense against many external and internal attacks.

Another security method [64] has two stages. First, it is used by Bloom Filters, and second, it is using Hybrid Certification Scheme (HAS). This scheme certifies the nodes of WSN by using the Merkle tree. A public key and signature are used to generate a certificate by Certificate Authority (CA) for any sensor node. Cryptographic keys are also a grouping of identification (ID) and an authentication certificate of any node. After broadcasting, they use flooding and authenticate the incoming message. Sharifi et al. [65] proposed an authentication scheme for nodes that reduces cryptographic keys by using the regeneration of keys. This scheme runs over other schemes. This can reduce complexity and supports scalable network and communication overhead. There are some communications overheads in the schemes des

cribed above, so there is a necessity to propose a new authentication plan that uses fewer resources to provide higher protection. In ECC, scalar multiplication time takes about 80% of the total time of major key generation in WSN. Some research in the literature proposed that an algorithm is used based on 1, s complement subtraction rather than scalar multiplication, which can reduce computational complexity by reducing less hamming weight.

3.2.5 Recent authentication techniques

Recently some authentication schemes were proposed by authors to provide security in WSN. A lightweight three-factor authentication approach [66] which support key management scheme. This scheme fulfills the security requirements of WSN by using XOR and hash functions. The BAN (Burrows–Abadi–Needham) logic and random oracle model is used for proof of this approach. This approach can give guarantee the safety of the secret key, session key, and protect from tracking attack, data leak attack, and identity theft attack.

Mobile wireless sensor network has one biggest challenge is their mobility. Due to mobility, authentication needs to frequently re-authenticate itself. However, the author identified the problems which are unconditional forwarding, absence of high-compromise resilience, and DoS attack in the previously proposed compared method. The proposed energy-efficient re-authentication techniques [67] with key generation. In this approach, the authentication key has changes when the cluster head moves from one location to a foreign location. Subhasish et al. [68] point out the various problem in password and keys based authentication and gives beneficial fact to use biometric information for authentication. The author has used high entropy-based information to shows the biometric authentication is better than the traditional authentication approach. The biometric keys are not easy to reproduce, guessed, stolen, lost, distribute, and misremembered. Another timestamp cryptographic algorithm which helps to protect against jamming attack. Rose and Jayasree [69] had proposed a new clustering of sensor nodes in WSN and generate a timestamp from one sensor node to another.

After that calculate the timestamp value at the receiver end. If the difference between timestamp is greater than an acceptable amount of time, then this message comes from a malicious node and discard this message. This algorithm is less complex and gives an effective result.

3.3 Trust management

Trust is the level of belief and evaluation of the significance between two nodes in WSN. It can be evaluated from direct or indirect and feedback based interactions. Direct trust is the observation of belief between the source node and the target node. Direct trust has more influence than indirect trust.

The source node needs to calculate the direct confidence, where each node is evaluated by the neighboring node. Indirect trust evaluation is based on feedbacks. The feedbacks are provided by neighbors of the target node.

This feedbacks are collected in trust records which are saved in cluster head [70], [70]. The trusted WSN has the attribute like dynamic, subjective, reflexive, intransitive, asymmetric, not absolute, trust is linked with risk, mutual causality, autocatalysis, and cooperative. There are mainly two types of trust management schemes in wireless sensor networks. The first is called Distributed trust management and the second is called centralized trust management. Figure 9 depicted the category of trust management.

3.3.1 Distributed trust management

Some trust management schemes such as [72], [72] are designed for common networks such as peer-to-peer networks while classical trust methods [74–76] were developed for wireless ad-hoc networks. So these trust methods are not eligible for WSN as they are less efficient in terms of memory and

power. Some trust methods (e.g., RFSN [77], PLUS [78], and ATRM [79]) are specifically designed for WSNs due to memory and power efficiency. Sun et al. [80] proposed a trust framework that applies to a hierarchical network. In the setup phase of the scheme, neighbor relationships

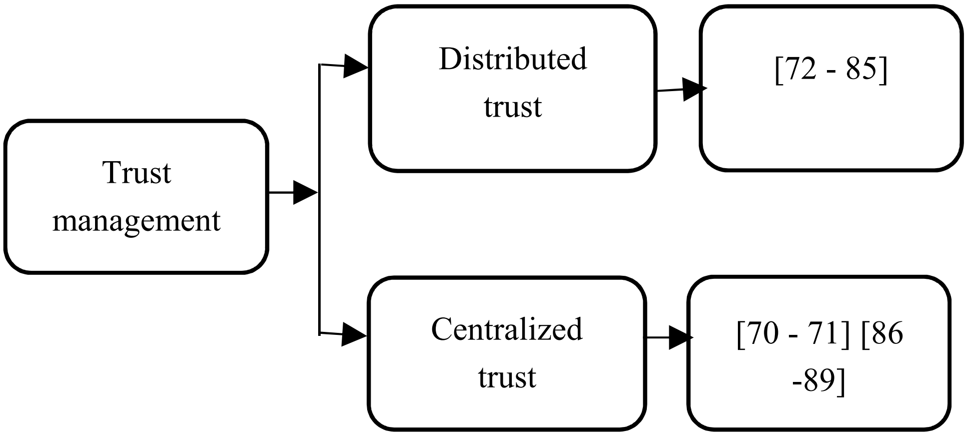


Fig. 9 Types of trust management in WSN

and distances are used to calculate trust. This secure framework uses distance and adjacency relationships during the setup phase of the network. This scheme often uses a modified sliding time window to minimize faulty nodes. This method results in inefficient routing, maintenance, and performance. Also, it gives better efficiency in terms of energy and storage.

Sahoo et al. [81] have used a honey bee optimization approach to develop an energy-efficient trust management model in WSN. The honey bee approach is based on a herd-based model. This method had proposed for clustered WSNs where nodes are treated as one group. The author develops a model where network performance and efficiency are optimized. This method maintains the lifetime of the WSN by isolating faulty behavior nodes to be a candidate for cluster head. It has given better performance when compared to the LEACH (Low-energy adaptive clustering hierarchy) protocol on parameters such as storage, lifetime time, and load.

Distributed systems are more suitable for WSN. So a distributed reputation-based framework sensor network (RFSN) was proposed by Ganeriwal et al. [77]. This framework investigates a generalized and integrated approach to exact extractions in sensor networks. In RFSN, the author develops a trusted community between sensor nodes. This structure has two parts. RFSN monitoring and reputation. The RFSN watchdog can monitor the behavior of neighboring nodes. The watchdog holds a buffer when the source node transmits data to neighboring nodes. The buffer contains all copies of the transmitted packets until the neighbors forward these packets. The reputation system maintained the node's reputation using Bayesian and Beta trust models.

Yao et al. [78] proposed a trust-based scheme for distributed systems, called Parameterized and Localized Trust Management (PLUS). This scheme uses individual recommendations and references to maintain trust between nodes. This method relies on small devices that are implanted into common objects that are cleverly received, moved, and communicated in dynamic infrastructure. PLUS is mainly used in changing environments and provides real-time security. Su et al. [82] proposed the PBTrust model to select the service available on the SOA architecture. The PBTrust Framework uses third-party evaluation, past performance, and reflects preferences for calculating trust by the consumer. The reputation of a service depends on the response of third parties based on the timestamp. The PBTrust model had updated the trust to the service provider without considering the central node. Trust and reputation values are stored in a matrix. So it is beneficial for dynamic environments. Renubala et al. [83] proposed a trust scheme that calculates trust using a fuzzy approach.

Li et al. [84] proposed a reliable evaluation method to identify malicious nodes. The numeric value of trust is calculated by the history of transactions, recommendations, and the response comes from neighbor nodes inside the cluster. It assumes that initially, a new node is trusted when it joins the network. The reliable value of a node varies between 1 and 10. So, the new node assigns the value 5 and updates the value according to the recommendations. The value is represented by using 4-bit memory space therefore it takes less memory.

Reddy et al. [85] proposed a trust management scheme based on Hysteresis Curve for WSN. This scheme provides security against various security threats which includes the wrong decision also. This scheme uses a mathematical function and differential equation for direct trust calculation and hysteresis curve and cos function to calculate indirect trust value. This trust management scheme can minimize the traffic of the network and increases reliability.

3.3.2 Centralized trust management schemes

Shaikh et al. [86] proposed a Group-based Trust Management Scheme (GTMS) for a centralized and hierarchical structure of the network. GTMS make a group of a node is trustable rather than any single node trustable. By using the broadcast strategy, it collects reputation-based trust value for nodes and taking less storage and communication overhead. GTMS are effective against collusion and Sybil attacks.

Zhang et al. [87] were proposed a scheme called Trust Management Architecture (TMA) which works as a decomposing trust calculation method. In this scheme, the trust values which are calculated recently have more weight rather than older observations. In this trust management scheme, the author uses multiple attributes and the certificate method to establish trust between nodes. TMA provides secure and efficient computation of trust without punishment of untrustworthy recommendations. (Tables 5, 6 and 7)

Hao et al. [88] proposed a combined trust organization scheme for a centralized sensor network by inserting the forward and backward joint checking scheme. This scheme had used the local and global trust interchange method. The local trust is calculated based on only a single path trust value.

Global trust is calculated based on the whole cluster's trust value collected by the cluster head from all path values. In this protocol, the trust value depends upon only successful packet transfer. Bao et al. [89] proposed Hierarchical dynamic Trust Management Protocol (HTMP) centralized sensor networks. There are two parts to HTMP schemes. First is intragroup trust calculation and intergroup trust calculation which are distributed

Table 5 Comparison between distributed trust management schemes

Trust scheme	Methodology	Structure	Security Agent	Advantages	Limitation
Sun et al. [80]	Distance and adjacency relationships are used for trust setup	Distributed	Sliding time window	Efficient routing and maintenance	Efficiency in terms of energy and storage
Ganeriwal et al. [77]	Reputation-based framework sensor network and watchdog method	Distributed	Reputation and buffer. Also, reputation using Bayesian and Beta trust models	Good performance, security attack detection, and energy-efficient	Not proven the system robustness
Yao et al. [78]	Direct and indirect trust calculation locally	Distributed	Recommendation and personal reference	Efficiency in the detection of faulty nodes. It also provides real-time security.	Trust estimation and convergence time is high
Li et al. [84]	Weighted value for transaction and recommendation	Centralized and distributed	History of transactions, recommendation	Complexity is minimum	A weighted coefficient is vulnerable for attacks
Reddy et al. [85]	Differential method and hysteresis curve for indirect trust	Distributed	Hysteresis curve	Reliability and reduces traffic	Misleading by several attacks like node compromised attack

manner. It calculates mainly two types of trusts called social trust and quality of service based trust. HTMP elaborates a probabilistic method that uses the stochastic petri net method to estimate the efficiency of this scheme which verifies the result. It is a complex method but it can defend from many security attacks.

A novel and secure trust management approach [70] is proposed for scalable WSN. In this method, we had proposed a trust management method by using the time-lapses function. The time lapses function is used to give more weight to recent communication than older communication. By implementing this scheme, a dependability-enhanced trust assessing scheme with a head node in cluster based network. Direct trust is evaluated by lightweight mathematical functions where it takes fewer resources. The trust has updated dynamically and has more weight on recent transactions. The calculation of trust has depended upon the packet transaction among nodes. We assume the environmental factor is constant during the transaction.

Khan et al. [71] proposed a trust estimate method for a bulky sensor network. WSN retain grouping to recover cooperativeness, honesty, and security by detecting faulty nodes and reduce resource consumption. The author believes that they provide a unique id for sensors to protect sensors from external attacks. It follows the distributed and centralized sensor network for the intercluster and intracluster network to find the trust between nodes. A timing gap analysis is used to find out the successful or unsuccessful transaction. In this work author not considers weight, frequency of fault trust, on-off attack, DoS attacks, and collusion attacks and plan to cover these limitations in the future. Table 7 represents the comparison between trust management schemes on security metrics.

4 Related review papers

Mohamed-Lamine Messai et al. [90] have proposed a Deterministic key management approach and a Probabilistic key management approach. In the Deterministic approach, the node has a probability of 1 to share a minimum of one key between 2 nodes. The pairwise key distribution approach will play a major role in this type of approach. The key connectivity is more an important feature of this approach. In the probabilistic key management approach, the shared key has predefined probabilities and key connectivity depends upon some keys which are selecting from a key pool. So, there is no shared key between two adjacent nodes. The authors divided the key management scheme into four parts which are set of keys scheme, mathematics based scheme, compromise based scheme and public keys scheme. Their proposed key management scheme is lightweight and named as sequence based key management scheme. Pre-process is the distribution of sensor nodes in this method and applies a recursive formula for numerical computation. This method ensured the establishment of keys for each node with an adjacent node after numerical computation deployment. The study of the proposed approach shows the reliability of system success and the author stated that the proposed key management system is more efficient in terms of safe route setting for secure communication and also provides high durability relative to current methods against adversary nodes. In nearly all WSN programs, the protection

Table 6 Comparison between centralized trust management schemes

Trust scheme	Methodology	Structure	Security agent	Advantages	Limitation
Shaikh et al. [86]	Multilevel trust calculation at three levels such as sensor, cluster head, and sink node level	Cluster-based, centralized and distributed	Time window	Less computation and storage overhead	Not effective against on-off attack and not fit in real-time applications
Zhang et al. [87]	Bayesian-based trust management function	Centralized	Attenuation function, reward and penalty factor	Robustness, Defense against malicious nodes	Performance
Hao et al. [88].	forward and backward joint checking scheme	Centralized	Local and global trust interchange method	fast and energy-efficient	Not considers the unsuccessful packet transfer
Bao et al. [89]	The probabilistic method uses stochastic petri net method	Centralized	Social trust and quality of service based trust	Defend against many security attacks	Complex
Gautam et al. [70]	Direct trust with time lapses function and indirect trust with recommendation and reputation of the node	Centralized and distributed	Time lapses function	Robust, fast and energy-efficient	Not tested in a real-time environment
Khan et al.[71]	Calculate the trust of the node to node, cluster head to cluster head, and node to cluster head.	Distributed approach and centralized	Direct and feedback	Fast, energy-efficient and low computation overhead	Vulnerability against DoS attack and several security attacks

cap is the greatest obstacle. There will be several security threats on the network due to the absence of security facilities such as integrity, confidentiality, and authentication. The implementation of cryptographic techniques where sensor nodes require a series of secret keys routinely offers certain services. Therefore, by taking into account this kind of challenge for potential WSNs,

Yousefpoor et al. [91] have proposed an excellent classification of the existing security protocols. Owing to resource constraint systems, there are many security challenges in the wireless sensor structure, such as hardware exploitation, eavesdropping, insertion of false signals, etc., so more effective security measures are distributed to the network that complies with relevant WSN features. Symmetric cryptography is the most common encryption method which can provide security features. In such authentication protocols, they use a shared key for the encryption and decryption process when two nodes try to connect. To provide message protection and authentication, this symmetric key has already been chosen and exchanged by the nodes. Mohammad Sadegh et al. defined hierarchical key management scheme and peer to peer key management scheme based on the network model. The systemic vision and the practical interaction of the sensor nodes are represented in these models. The nodes are organized as a tree like structure in the Hierarchical model and the keys are used from the leaves into the node. The sum of message propagation is minimized as the nodes are organized as layers. The nodes in the network are spread in a peer-to-peer model and the sensor nodes interact directly with their neighbors. (Table 8)

That is, correspondence between the nodes takes place directly without any intermediary, and all nodes are distributed with the same public key. The private person key is used for encryption during peer-to-peer contact along with the public key. Some features of this scheme are as follows.

Pourghebleh et al. [92] have presented a structured analysis study in the field of trust management in IoT using a systematic approach. Previous articles have been divided into four groups, including forecast-based, recommendation-based, reputation-based, and policy-based. Besides, the researchers examined selected papers considering several key factors such as adaptability, heterogeneity, affordability, precision, safety, scalability, and honesty. Finally, several potential road maps have been offered. However, their analysis does not take into account our key subject, trust management for utilities, as well as other previous surveys. Using a comprehensive approach, the authors [92] have given a structured analysis analysis in the field of trust management in IoT. Previous documents have been divided into four groups, including prediction-based, recommendation-based, reputation-based and

Table 7 Comparison between trust management schemes on security metrics

Paper	Accuracy	Availability	Integrity	Privacy	Reliability	Scalability
Sun et al. [80]	High	High	Medium	Medium	High	Low
Ganeriwal et al. [77]	Low	Medium	High	High	Medium	Low
Yao et al. [78]	Medium	Low	Medium	High	Low	Medium
Li et al. [84]	Medium	Low	High	High	High	Medium
Reddy et al. [85]	Medium	Low	Low	Low	High	Medium
Shaikh et al. [86]	Medium	Medium	High	High	Low	High
Zhang et al. [87]	Medium	Medium	Medium	Medium	Medium	High
Hao et al. [88].	Medium	Low	Medium	Medium	Medium	Low
Bao et al. [89]	Low	High	Medium	Medium	Medium	Medium
Gautam et al. [70]	High	Low	Medium	Low	Low	High
Khan et al.[71]	High	Medium	Medium	Medium	High	High

Table 8 Features of Mohammad Sadegh et al scheme

Type of classification	Network key, pairwise key, public key and group key
Scalability	Medium
Minimum number of keys	Two or three
Security	Medium
Storage consumption	Minimum

Table 9 Discussion areas of Ferrag et al. [93] survey paper

Paper	Ferrag et al.	
Discussion areas	Trust	Discussed
	Security	Discussed
	Privacy	Discussed
	Blockchain	Partially discussed
	Machine learning	Partially discussed

policy-based. Besides, the researchers analyzed the chosen documents, taking into consideration some key factors such as adaptability, heterogeneity, affordability, precision, privacy, scalability, and honesty. They have finally offered some potential roadmaps. Our key priority, trust management for utilities, as well as other former review documents, is not considered in their study, however.

Within the context of the IoT, it is unlikely for such central authority to be accessible. (i) it may reflect a single point of weakness, a performance bottleneck, and a point of weakness in the overall infrastructure; (ii) it may not be feasible for a single organization to own the overall infrastructure and it may struggle to decide which institution may resolve the central authority.

This method may not have the same disadvantages as having a centralized authority, but it does have additional ones (i) it is possible to exchange multiple messages to use more resources, (ii) the confidence measurement can be contradictory, with nodes estimating a diverging trust value for the same person, (iii) it is simpler to target and undermine the solution. Recently, by integrating these two contrasting strategies, when many special nodes are installed within the infrastructure, different methods, all from the same view of the stored confidence degree and approached by IoT nodes to recover and change these values. It is simple to show why such a federated method fixes the drawbacks of the two previous solutions, yet needs a way to achieve data continuity across the Internet between several replicas.

A detailed survey on authentication protocols in the IoT setting was proposed by Ferrag et al. [93] in four directions: Machine to Machine Communications (M2M), Internet of Vehicles (IoV), Internet of Energy (IoE), and Internet of Sensors (IoS). They studied the main authentication protocol risks, countermeasures, and structured access verification mechanisms. In addition, several potential research directions were identified, including the topic of authentication and safety, accounting for the method of detecting and preventing attacks, as well as developing authentication protocols for overhead communication and computation. They also proposed an authentication model. To achieve shared authentication, user anonymity, privacy protection, and perfect forward confidentiality, the authentication paradigm uses three types of cryptosystems, namely: symmetric cryptosystems, asymmetric cryptosystems, and hybrid cryptosystems. Symmetric cryptosystem-based protocols, however, needless processing power to store all the symmetric keys used in a network at the expense of high memory usage. However, the reliability of the protocols based on the symmetric-cryptosystem succeeds in the approaches based on the asymmetric-cryptosystem.

Tables 9 and 10 depicted the discussion areas and security aspects of Ferrag et al.[93] survey paper.

Table 10 Security aspects of this research work

Paper	Ferrag et al.	
Security aspects	Authentication	Supported
	Encryption	Not supported
	Access control	Not supported
	Detection	Not supported
	Privacy	Not supported

In [94], the author's analysis that the attack can be reasonably damaging to many of the sensor network's critical functions, including routing, distribution of resources, identification of wrongdoing, etc. The authors create a hierarchy of the various types of Sybil attacks, which helps us to better understand the threats faced by each type and to design better countermeasures against each type. Most data-centered sensor networks demand that data safety, honesty, and confidentiality be maintained because most of the data carried by these sensors if hacked, could lead to industrial/national spying or even life threats.

Din et al.[95] have surveyed various trust management techniques for IoT networks along with their strengths and limitations. Their work aims to identify the most applicable trust management approach with a consistent definition of device collaboration without examining various criteria. Furthermore, the authors refrain from addressing the problems posed by the implementation of IDSs on real platforms. In comparison, the paper does not take account of the consideration of work performed in related network styles. Table 11 represents the summary of this paper.

5 Discussions and open issues

There are various key management systems or protocols are proposed by researchers earlier. They have solved many of the security issues alarmed by many application of a sensor network. But when the technology is upgraded then security threats are also increasing. Several issues still need to an efficient solution and remain to be solved. The key management schemes are mainly three types, network wise key, pairwise and hybrid keys. If there is a small organization and used this communication in a limited area then network wise keys are work efficiently. The network wise keys are simple to implement, taking fewer resources and low cost. But if the deployment area and transmission medium are not under control then pairwise keys are the best solution. Robustness is the key feature of pairwise keys. It is costly in terms of resources but provides a robust solution. Hybrid keys are the combination of both and provide secure key management schemes for the hierarchical based network.

The classification of key management schemes based on a key element which is random, master key, location, tree, and polynomial. The polynomial based approach has many advantages over simple random number generator, master key-based, and matrix based in terms of scalability, key connectivity, resilience, storage complexity, processing complexity, and communication complexity. In general, attacks affecting WSN are usually eavesdropping, active and passive adversaries. A passive adversary obtains some data by analyzing traffic without any physical access, and active adversaries obtain data and information by capturing a packet or node.

The main goal of the authentication scheme proposed by researchers is that it takes less computing load, decreases energy consumption, high security, efficient utilization of resources such as memory, bandwidth, and power. There is plenty of lightweight authentication scheme which are lightweight by using a trust, XOR operation, key hash function, Elliptic curve cryptography, and forward secrecy. The lightweight authentication schemes must take fewer resources. In mobile WSN such as ad hoc network, flying ad hoc networks and vehicular network are using an ID. Therefore, ID based authentication techniques are used in WSN with mobility. The deployment area of WSN is random, dynamic, and hostile then that type of WSN uses a broadcast-based authentication scheme.

Establishing trust in WSN has developed a motivating and interesting issue for the research group due to requirements in various applications of WSN. In the

Table 11 Summary of this survey paper

Paper	Din et al.
Description	Extensive analysis of trust management techniques along with their advantages and disadvantages
Trust management applications	Not discussed
Trust management phases and issues	Not discussed
Advantages and disadvantages	Fully discussed
Trust management schemes	Partially discussed
Trust management research challenges	Partially discussed

existing trust management schemes, some are complete and emphasis on basic security requirements of WSN. Regrettably, many basic security requirements namely resource efficiency, reliability and are not getting much attention from research communities. Many trust management schemes for large scale WSN are not successful because of low cooperation, higher communication, and memory overheads.

The node will fail to perform due to hardware failure, battery depletion, security attacks, and overloading. Mobility is also key issues of the node in any specific application such as cattle monitoring, patient monitoring of WSN. Key management with mobility is considering in many previous works. In IoT applications, secure communications between sensors and servers is a major problem.

Some open issues for proposing a better key management system are as follows

- The lightweight security solution is needed because of small scale, low power, low capacity, and low resources in sensors. It can fulfill the trust and key management requirements.
- The privacy preservation of nodes can enhance the anonymity of the node and increases public confidence. The trust-based solution must consider these issues and secure the location of the mobile node.
- The heterogeneous nature of communication devices in many applications of WSN can create a compatibility issue. So, the solution based on trust and key management can consider the heterogeneous nature of nodes.
- Scalability is an important issue that handles increasing or decreasing the number of communication nodes or resources while possession of their interoperability and evade any per
- The adoption of topology by a new node is also a key challenge for security solutions based on trust and key management.
- Availability and reliability is another major concern to defined security solution which are based on key management, authentication, and trust management.
- As the application area of WSN is increasing, the demand for security solutions against many newborn attacks also increasing. Therefore, the security solution must be flexible in terms of adaptability.
- The key management system must include extensibility, self-organize, and resilience properties.
- Every key management approach must have key refreshing, key revocation, and renewal policy.
- Every network has some situation where some new node added or some node deleted. In both cases, the newly added node and deleted node are dangerous for the network. Therefore, proposing a secure algorithm for a new node joining and updating keys after the deletion of any node is needed for a secure network.
- Several applications, environments, and deployment strategies need different key management and distribution techniques.
- The scalability of key management protocols is extremely dependent on their specific modes of function.
- Public key cryptography suffered from slow speed and expensive in resource constraint environment.
- Speed is an important parameter where sensor nodes essentially establish a secure channel in a very short amount of time.
- Finding techniques to endure the absence of physical security, maybe through redundancy or information about the physical environment, will continue to the overall challenge.
- Cryptography requires a performance cost for extra computation that often increases packet size.
- Some of the limitations of the key management approach have overhead from generating and distributing keys after some delay, possible message delay.
- The flexibility of a public-key scheme is open issues with constraints faster, limited storage, computation, and communication capacity.

6 Future research direction

1.Identify malicious behavior communication overhead and effective research utilization is always better to research direction in the field of security in wireless sensor networks.

2.There are issues with scalability, stabilities, and overhead analysis are key issues in security.

3.Intelligent intrusion detection, mitigation of on-off attacks, collusion attacks, DoS attacks, grey hole attacks, node compromised attacks, and Sybil attacks.

4.In many life changing application environments, to achieving anonymity. It is difficult to achieve the trust management system for the anonymous nodes WSN environment.

5.Storage issues at the node for saving the trust and reputation values in their design and validation.

6.Giving trust based solution for all attacks are not possible. It also suffers from a higher cost.

7.Applying the trust management scheme in an insecure environment is ineffective. Therefore, designing trust management in an unsecured environment is complex and difficult.

7 Conclusion

This paper has concisely presented wireless sensor networks and the issues related to organizing and positioning them in unknown environments. This work presented the security challenges, obstacles, threats, and security solution constraints in WSN. Key management, authentication, and trust management are sometimes used interchangeably to define a protected network. Most of the studies reviewed in literature use keys and trust as a foreign component in an existing sensor network and intention to improve security in these types of networks. There are many key management schemes categorized as probabilities, ID based, master key, location, and polynomial equation based keys distribution scheme. The survey contains the major aspects of the existing key management scheme and provided comparison table 4. which helps in the selection of appropriate protocol according to their WSN application. Trust is an important factor that influences the security in WSN. Trust has, indeed, played a foundational role in security over quite a long ago. Trust is characterized by subjectivity, dynamicity, asymmetry, context-dependency, and incomplete transitivity. Trust is either distributed and centralized. Moreover, applications-based node trust can be designed and secure the network. Authentication is a feature of security where it is guaranteed that the message is to from authenticated to the source. There is various authentication scheme such as lightweight, Id based, MAC based and timestamp-based are proposed by authors takes less computing load, decreases energy consumption, high security, efficient utilization of resources such as memory, bandwidth, and power.

Acknowledgement This paper is funded by the University Grant Commission (UGC), India under Junior Research Fellowship (UGC NET-JRF) vide letter no. 3331/(SC)(NET-JUNE2015). Authors are also thankful to Director, IMS engineering college, Ghaziabad for his constant encouragement and motivation.

Compliance with ethical standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest

References

1. Akyildiz F, Su W, Sankarasubramaniam Y, Cayirci E (2002) Wireless sensor networks: a survey. Comput Netw 38(4):393–422
2. R. Grace Sensor-enabled nodes support the IoT for smart buildings and smart transport. IoT Technologies and Applications Symposium, May 21, San Jose
3. M. Rouvala White paper: security and WSN. New Nordic Engineering. Nov 2017
4. Gilbert EP, Kaliaperumal B, Rajsingh EB (2012) Research issues in wireless sensor networkapplications: a survey. Int J Inform Electron Eng 2(5):702
5. P.C Kocher Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems In proceeding of Annual International Cryptology Conference, pp. 104-113. 1996 Aug 18Springer, Berlin, Heidelberg
6. M. Al-Rakhami and S. Almowuena Wireless Sensor Networks Security: State of the Art. arXiv preprint . 2018 Aug 15
7. R. Grace Sensor-enabled nodes support the IoT for smart buildings and smart transport IoT Technologies and Applications Symposium, May 21, San Jose
8. Sohraby K, Minoli D, Znati, T (2007) Wireless sensor networks: technology, protocols, and applications. Wiley, pp 15–18. ISBN 978-0-471-74300-2
9. Saleh Y, Yahya MS, Dalyop IA, Hussain R (2018) Wireless sensor network (WSN) in insect monitoring: acoustic technique in insect monitoring a review/survey. Int J Eng Technol 7(3):121–126
10. Pule M, Yahya A, Chuma J (2017) Wireless sensor networks: a survey on monitoring water quality. J Appl Res Technol 15(6):562–570
11. Kochhar A, Kumar N (2019) Wireless sensor networks for greenhouses: an end-to-end review. Comput Electron Agric 163:104877
12. Walters JP, Liang Z, Shi W, Chaudhary V (2007) Wireless sensor network security: a survey. Secur Distrib Grid Mob Pervasive Comput 1:367
13. Carman DW, Krus PS, Matt BJ (2000) "Constraints and approaches for distributed sensor network security, " Technical Report 00–010. NAI Labs, Network Associates Inc, Glenwood, MD
14. J. Sen, "Security in wireless sensor networks. Wireless Sensor Networks: Current Status and Future Trends, 407, p. 408
15. M. Al-Rakhami and S. Almowuena (2018) Wireless Sensor Networks Security: State of the Art, ". arXiv preprint
16. Kavitha T, Sridharan D (2010) Security vulnerabilities in wireless sensor networks: a survey. J Inform Assur Secur 5(1):31–44
17. Camtepe SA, Yener B (2005) "Key distribution mechanisms for wireless sensor networks: a survey, " Rensselaer Polytechnic Institute. Troy, New York, Technical Report, pp 05–07
18. Moara-Nkwe K, Shi Q, Lee GM, Eiza MH (2018) A novel physical layer secure key generation and refreshment scheme for wireless sensor networks. IEEE Access 6:11374–1138
19. U. Iqbal, and S. Shafi (2019) A provable and secure key exchange protocol based on the elliptical curve diffe–hellman for WSN. In Advances in Big Data and Cloud Computing, 363-372
20. B. Cui, Z. Wang, B. Zhao, X. Liang and Y. Ding (2015) Enhanced key management protocols for wireless sensor networks. Mobile Information Systems
21. L. Eschenauer, and V. D. Gligor (2002) A key-management scheme for distributed sensor networks, In Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41-47

22. H. Chan, A. Perrig, and D. Song (2003) Random key predistribution schemes for sensor networks, "In Proceeding of Security and Privacy Symposium, pp. 197-213
23. Du W, Deng J, Han YS, Varshney PK, Katz J, Khalili A (2005) A pairwise key predistribution scheme for wireless sensor networks. ACM Trans Inform Syst Secur (TISSEC) 8(2):228–258
24. Gandino F, Montrucchio B, Rebaudengo M (2009) Key management for static wireless sensor networks with node adding. IEEE Trans Ind Inform 10(2):1133–1143
25. Zhu S, Setia S, Jajodia S (2006) LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Trans Sens Netw (TOSN). 2(4):500–528
26. Younis MF, Ghumman K, Eltoweissy M (2006) Location-aware combinatorial key management scheme for clustered sensor networks. IEEE Trans Parallel Distrib Syst 17(8):865–882
27. Choi J, Bang J, Kim L, Ahn M, Kwon T (2015) Location-based key management strong against insider threats in wireless sensor networks. IEEE Syst J 11(2):494–502
28. Qin Z, Zhang X, Feng K, Zhang Q, Huang J (2015) An efficient key management scheme based on ECC and AVL tree for large scale wireless sensor networks. Int J Distrib Sens Netw 11(9):691498
29. Yao W, Han S, Li X (2015) LKH++ based group key management scheme for wireless sensor network. Wirel Pers Commun 83(4):3057–3073
30. Swaminathan A, Vivekanandan P (2017) An effective lightweight key management (ELWKM) model for wireless sensor networks using distributed spanning tree structure. Asian J Res Soc Sci Human 7(2):749–770
31. H. C. Chen and A. Christiana (2017) A role-based RSA key management approach in a hierarchy scheme, "In Proceeding of Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 258-264
32. Shamir A (1979) How to share a secret. Commun ACM 22(11):612–613
33. Lu K, Qian Y, Guizani M, Chen HH (2008) A framework for a distributed key management scheme in heterogeneous wireless sensor networks. IEEE Trans Wirel Commun 7(2):639–647
34. X. Fan and G. Gong (2015) LPKM: A lightweight polynomial-based key management protocol for distributed wireless sensor networks," In proceeding of International Conference on Ad Hoc Networks, pp. 180-195
35. Wang Q, Chen H, Xie L, Wang K (2013) One-way hash chain-based self-healing group key distribution scheme with collusion resistance capability in wireless sensor networks. Ad Hoc Netw 11(8):2500–2511
36. Suganthi N, Vembu S (2014) Energy-efficient key management scheme for wireless sensor networks. Int J Comput Commun Control 9(1):71–78
37. Anita EM, Geetha R, Kannan E (2015) A novel hybrid key management scheme for establishing secure communication in wireless sensor networks. Wirel Pers Commun 82(3):1419–1433
38. Sun X, Wu X, Huang C, Xu Z, Zhong J (2016) Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks. Ad Hoc Netw 37:324–336
39. R. Zhou and H. Yang (2011) A hybrid key management scheme for heterogeneous wireless sensor networks based on ECC and trivariate symmetric polynomial, "In Proceeding of International Conference on Uncertainty Reasoning and Knowledge Engineering (URKE) 1: 251-255
40. Ramkumar KR, Singh R (2017) Key management using Chebyshev polynomials for mobile ad hoc networks. China Commun 14(11):237–246
41. Z. Jing, M. Chen and F. Hongbo (2017) WSN key management scheme based on fully bomomorphic encryption, "In proceeding of Control And Decision Conference (CCDC), 2017 29th Chinese, pp. 7304-7309
42. Zhan F, Yao N, Gao Z, Tan G (2017) A novel key generation method for wireless sensor networks based on system of equations. J Netw Comput Appl 82:114–127
43. Dinker AG, Sharma V (2019) Polynomial and matrix-based key management security scheme in wireless sensor networks. J Discret Math Sci Cryptography 22(8):1563–1575
44. Rajeswari SR, Seenivasagam V (2016) Comparative study on various authentication protocols in wireless sensor networks. Sci World J 2016:1–16
45. Das AK (2016) A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. Peer-to-peer Netw Appl 9(1):223–244
46. Wu F, Xu L, Kumari S, Li X (2018) An improved and provably secure three-factor user authentication scheme for wireless sensor networks. Peer-to-Peer Netw Appl 11(1):1–20
47. Jiang Q, Zeadally S, Ma J, He D (2017) Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access 5:3376–3392
48. Shim KA (2017) "BASIS: a practical multi-user broadcast authentication scheme in wireless sensor networks. IEEE Trans Inform Forensic Secur 12(7):1545–1554
49. Xue K, Ma C, Hong P, Ding R (2013) A temporal-credential-based authentication and key agreement scheme for wireless sensor networks. J Netw Comput Appl 36(1):316–23
50. Delgado-Mohatar O, Fúster-Sabater A, Sierra JM (2011) A lightweight authentication scheme for wireless sensor networks. Ad Hoc Netw 9(5):727–735
51. M. D. Shah, S. N. Gala and N. M. Shekokar (2014) Lightweight authentication protocol used in wireless sensor network. In proceeding of International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), pp. 138-143
52. Shen J, Chang S, Shen J, Liu Q, Sun X (2018) A lightweight multilayer authentication protocol for wireless body area networks. Future Gener Comput Syst 78:956–963
53. Luo H, Wen G, Su J (2018) Lightweight three factor scheme for real-time data access in wireless sensor networks. Wirel Netw 26(2):955–970
54. Gope P, Hwang T (2014) A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. IEEE Trans Ind Electron 63(11):7124–7132
55. Li C, Zhang X, Wang H, Li D (2018) "An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks. Sensors 18(1):194
56. Ouada FS, Omar M, Bouabdallah A, Tari A (2016) Lightweight identity-based authentication protocol for wireless sensor networks. Int J Inform Comput Secur 8(2):121–138
57. Zhu H, Tan YA, Zhu L, Wang X, Zhang Q, Li Y (2018) An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks. Sensors 18(5):1663
58. S. M. Chang, S. Shieh, W. W. Lin and C. M. Hsieh (2006) An efficient broadcast authentication scheme in wireless sensor networks, "In Proceedings of the 2006 ACM Symposium on Information, computer and communications security, pp. 311-320
59. Shim KA, Lee YR, Park CM (2013) EIBAS: an efficient identity-based broadcast authentication scheme in wireless sensor networks. Ad Hoc Netw 11(1):182–189
60. Chowdhury AR, Chatterjee T, Das S (2014) LOCHA: a light-weight one-way cryptographic hash algorithm for wireless sensor network. Proc Comput Sci 32:497–504
61. Liu Y, Li J, Guizani M (2012) "PKC based broadcast authentication using signature amortization for WSNs. IEEE Trans Wirel Commun 11(6):2106–2115

62. A. Moinet, B. Darties and J. L. Baril (2017) Blockchain based trust & authentication for decentralized sensor networks. 1706 -1730
63. Indra G, Taneja R (2014) "A time stamp-based elliptic curve cryptosystem for wireless ad-hoc sensor networks. IJSSC 4(1):39–54
64. Ren Y, Liu Y, Ji S, Sangaiah AK, Wang J, J, (2018) Incentive mechanism of data storage based on blockchain for wireless sensor networks. Mob Inform Syst 2018:1–10
65. M. Sharifi, S. S. Kashi and S. P. Ardakani (2009) Lap: A lightweight authentication protocol for smart dust wireless sensor networks. In proceeding of International Symposium on Collaborative Technologies and Systems, pp. 258-265
66. Adavoudi-Jolfaei A, Ashouri-Talouki M, Aghili SF (2019) Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks. Peer-to-Peer Netw Appl 12(1):43–59
67. Kim B, Song J (2019) Energy-efficient and secure mobile node reauthentication scheme for mobile wireless sensor networks. EURASIP J Wirel Commun Netw 1:155
68. Banerjee S, Chunka C, Sen S, Goswami RS (2019) An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart card. Wirel Pers Commun 107(1):1–28
69. S. G. H. Rose and T. Jayasree, T (2017) A jamming detection technique for WSN using timestamp, " In proceeding of International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)
70. A. K. Gautam and R. Kumar (2018) A robust trust model for wireless sensor networks, in Proc. 5th IEEE Uttar Pradesh Section Int. Conf. Electr.,Electron. Comput. Eng. (UPCON), pp. 1-5
71. Khan T, Singh K, Abdel-Basset M, Long HV, Singh SP, Manjul M (2019) A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. IEEE Access 7:58221–58240
72. M. Gupta, P. Judge, and M. Ammar (2003) A reputation system for peer-to-peer networks, In Proceedings of the 13th international workshop on Network and operating systems support for digital audio and video, 144-152
73. S. D. Kamvar, M. T. Schlosser, and H Garcia-Molina (2003) The eigentrust algorithm for reputation management in p2p networks. In Proceedings of the 12th international conference on World Wide Web, 640-651
74. Liu Z, Joy AW, Thompson RA (2004) A dynamic trust model for mobile ad hoc network, In Proceedings 10th IEEE international workshop on future trends of distributed computing systems. FTDCS 2004:80–85
75. A. A. Pirzada, and C. McDonald (2004) Establishing trust in pure ad-hoc networks", In Proceedings of the 27th Australasian conference on Computer science, Vol 26 , pp. 47-54. Australian Computer Society, In
76. Ren Y, Zadorozhny VI, Oleshchuk VA, Li FY (2014) A novel approach to trust management in unattended wireless sensor networks. IEEE Trans Mob Comput 13(7):1409–1423
77. Ganeriwal S, Balzano LK, Srivastava MB (2008) Reputation-based framework for high integrity sensor networks. ACM Trans Sens Netw (TOSN) 4(3):15
78. Z. Yao, D. Kim, and Y. Doh (2006) PLUS: Parameterized and localized trust management scheme for sensor networks security", In proceeding of 2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), , pp. 437-446. IEEE
79. Boukerch A, Xu L, K. EL-Khatib, (2007) Trust-based security for wireless ad hoc and sensor networks. Comput Commun 30:2413–2427
80. Sun B, Li D (2017) A comprehensive trust-aware routing protocol with Multi-attributes for WSNs. IEEE Access 6:4725–4741
81. Sahoo RR, Singh M, Sahoo BM, Majumder K, Ray S, Sarkar SK (2013) A light weight trust based secure and energy efficient clustering in wireless sensor network: honey bee mating intelligence approach. Proc Technol 10:515–523
82. Su X, Zhang M, Mu Y, Bai Q (2013) A robust trust model for service-oriented systems. J Comput Syst Sci 79(5):596–608
83. S. Renubala, and K. S. Dhanalakshmi (2014) Trust based secure routing protocol using fuzzy logic in wireless sensor networks", In proceeding of 2014 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1-5. IEEE
84. Li X, Zhou F, Du J (2013) LDTS: A lightweight and dependable trust system for clustered wireless sensor networks. IEEE Trans Inf Foren Secur 8(6):924–935
85. V. B. Reddy, A. Negi, and S. Venkataraman (2018) Trust computation model using hysteresis curve for wireless sensor networks," in Proc. IEEE SENSORS, pp. 1-4
86. Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S, Song Y-J (2009) Group-based trust management scheme for clustered wireless sensor networks. IEEE Tran Parallel Distrib Syst 20(11):1698–1712
87. J. Zhang, R. Shankaran, M. A. Orgun, V. Varadharajan and A. Sattar (2010) A trust management architecture for hierarchical wireless sensor networks. IEEE conference on local computer networks (LCN'10), 264–267
88. D. Hao, A. Adhikari and K. Sakurai (2011) Mixed-strategy game based trust management for clustered wireless sensor networks, "In Proceedings of the third international conference on trusted systems (INTRUST'11) , pp. 239–257
89. Bao F, Chen IR, Chang M, Cho J (2014) Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans Netw Serv Manag 9(2):169–183
90. Messai ML, Seba H (2016) A survey of key management schemes in multi-phase wireless sensor networks. Comput Netw 105:60–74
91. Yousefpoor MS, Barati H (2019) Dynamic key management algorithms in wireless sensor networks: a survey. Comput Commun 134:52–69
92. Pourghebleh B, Wakil K, Navimipour NJ (2019) A comprehensive study on the trust management techniques in the internet of things. IEEE Internet Th J 6(6):9326–9337
93. M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu. (2017) Authentication protocols for internet of things: a comprehensive survey. Security and Communication Networks
94. A. Karakaya, and S. Akleylek. (2018) A survey on security threats and authentication approaches in wireless sensor networks." In 2018 6th international symposium on digital forensic and security (ISDFS), pp. 1-4. IEEE
95. Din IU, Guizani M, Kim BS, Hassan S, Khan MK (2018) Trust management techniques for the Internet of Things: a survey. IEEE Access 7:29763–29787
96. Parsons L, Ross R, Robert K (2020) A survey on wireless sensor network technologies in pest management applications. SN Appl Sci 2(1):28
97. U. Khalid, Md. Asim, T. Baker, P. C. K. Hung, Md. A. Tariq, and L. Rafferty (2020) A decentralized lightweight blockchain-based authentication mechanism for IoT systems." Cluster Computing, 23(3): 2067-2087
98. Y. Tian, Z. Wang, J. Xiong, and J. Ma. (2020) A Blockchain-Based Secure Key Management Scheme with Trustworthiness in DWSNs." IEEE Transactions on Industrial Informatics

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