# An Analysis and Comparison of Security Protocols on Wireless Sensor Networks (WSN)

**Ranjit Kumar, Sachin Tripathi and Rajeev Agrawal**

**Abstract** With increasing several applications of WSN, the provision of securing sensitive information of the entire network should be made for which sensor networks and ad hoc networks are introduced for the routing protocol. Many protocols as an opponent can disrupt the network or exploit precious data from the network which is not with the purpose of security. Large number of nodes, limited battery power, and their data-centric nature in routing WSN make routing a challenging problem in WSN. Therefore, security solutions should be properly formed because they have had a strong collision on large presentation. In this work, we mainly concentrate on security issues, security requirements, and we have also analyzed and discussed some key management protocols for secure transmission of data and comparing them on the basis of performance. This work has provided a detailed description of the WSN-related information to extremely understand the concept of the network.

**Keywords** Wireless sensor network (WSN) · Security · Cryptography · Key management protocols

R. Kumar (✉) · S. Tripathi
Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines) Dhanbad, Dhanbad 826004, Jharkhand, India
e-mail: ranjit_kumaruitbu@yahoo.co.in

S. Tripathi
e-mail: var_1285@yahoo.com

R. Agrawal
Department of Computer Science and Engineering, GL BAJAJ Institute of Technology & Management, Greater Noida 201301, India
e-mail: rajkecd@gmail.com

S. K. Das et al. (eds.), *Design Frameworks for Wireless Networks*,
Lecture Notes in Networks and Systems 82,
https://doi.org/10.1007/978-981-13-9574-1_1

## 1 Introduction

WSN has hundreds or thousands of little gadgets with detecting, preparing, and correspondence abilities for certifiable ecological observing [1, 2]. Sooner rather than later, from significant military checking applications to forest flame observing and security checking, they have been appointed to play important roles in different areas. Sometimes, WSN works with infrastructure based or infrastructure less as like wireless ad hoc networks [3–8]. Because it is rapidly used in different real-life applications. In this network, the smart sensor nodes (SSN) are equipped with one or more sensors, one processor, memory, one power supply, one radio, and low-power equipment, an actuator. The sensor's execution is to screen the physical and natural conditions, for example, dampness, weight, sound, and temperature. After their surveillance, they send information to their main place. The sensor network comprises collection of sensor hubs which are deployed in the scenario (Fig. 1).

The WSN network which does not interfere with the use of current security approaches does not have a resource in the different architectural layers, such as the inter-node status of communication and application level, focusing on the level of a node. For example, there are many barriers to limited resources for limited assets, unpredictable statement, and non-permissible functioning. The main motivation of the work is to briefly explain the concept of WSN. There are various issues related to the security of the information used in the wireless network [9]. It provides a detailed description regarding the security protocols.

This work is sorted out when pursues: inside Sect. 2, requirements and security threat models are discussed. Areas 3 talk about different conventions for WSN. Segment 5 illustrates the analysis and comparison of the WSN protocols. At last, the paper has been finishing up in Sect. 6 with conclusion.

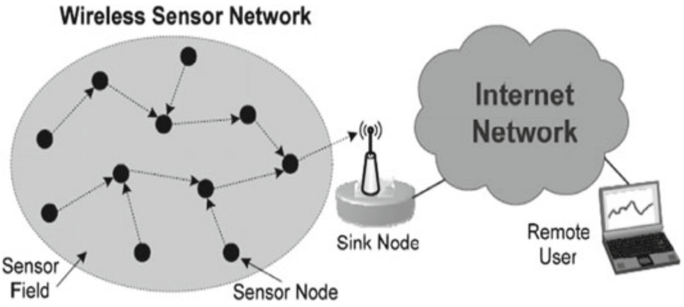

**Fig. 1** Wireless sensor network

## 2 Literature Survey

Bletsas et al. [10] in this work have given different clustering approaches in WSN. First, we separate the protocol used in the WSN in the forms of protocol operation (PO), network structure (NS), and path estimate (PE). Second, we have provided a broad overview of the cluster-based routing protocol used in the block cluster, chain cluster, and grid cluster which forms the WSN, and we have discussed various issues in routing protocols and compared various clustering routing protocols based on various attributes

Priyadarshini et al. [11] discuss the conference which relies on session key foundation and open key cryptography for outside operator verification. An outside administrator passes on through an open key encryption framework with a BS, which talks with sensor center points through the sharing of a private key. The technique for this tradition is isolated into three phases: selection, affirmation, and session key establishment (SKE).

Biagioni et al. [12] proposed an effective cryptographic methodology for information security in WSNs utilizing the Modern Encryption Standard Version-II. The symmetric key encryption is introduced by MES V-II and the JSA and DJSA calculations are utilized and randomized technique by a calculation which is made by Nath et al. In this approach, a summed up and altered Vernam figure methodology is used with different square sizes and keys for each square. As an additional security reason for this count, info is furthermore added to this method. After the quick stage encryption is done, the entire record is divided into two exchanged parts and the balanced Vernam figure method with info and another key will be reiterated. Repeating this entire action, various events result in a system that is significantly secure.

Akyildiz et al. [13] in this essay proposed a multi-level security system which is introduced using a data-oriented random number generator to encrypt a tag of frames. The first level will be started using the interlacing method. Second, the suite-random number generator's value is the seed. Third, the bank will first distribute a numeral. Final status starts when the number is applied to the bank.

Wong et al. [14] proposed the method which introduces a flood dependency based on data sources in the river. The main idea behind this node is that each node can be considered as a data source, which sends the actual data after an event has been detected on a non-node; dummy data is available on all ion nodes in this node. This approach is difficult to distinguish between the opponent's original packet and dummy, which leads to dirt traffic and energy consumption. A new solution is suggested by using variable-sized dummy packets. Dummy patterns vary from actual packages, so energy conservation occured. However, an expert will still find it difficult to distinguish dummy real packages.

Collins et al. [15] proposed the capacity to investigate for security shortcomings, mishaps, and infringement appearing on a honeypot system for WSNs. This is a recommended way to deal with a model that needs more examinations to assess its adequacy as a total framework for recognizing system attacks and different attacks. The opposite side of this innovation has been connected to control utilization by honeypot sensor hubs. This strategy does not have any significant bearing to other security issues and should, accordingly, be joined with different arrangements.

# 3 Security in Wireless Sensor Networks (WSN)

The sanctuary has been used largely as a word that features the characteristics of affirmation, decency, assurance, non-replay, and threatening to playback [16]. More dependence on the information given by the framework has been comprehensive, the further vital the threat of protected diffusion of information on the framework is extended. For the protected transmission of various sorts of information on the framework, various cryptographic, stenographic, and distinctive strategies are used which are remarkable. In this section, we talk about the structure security prerequisites and issues and how the frameworks are proposed for remote sensor frameworks.

## *3.1 Sanctuary Requirements in WSN*

I. Data privacy: The safety methods have the assurance that no communication in the structure is comprehended by anyone aside from the expected receiver. In a WSN, issue of secrecy must address the accompanying prerequisites [17, 18]:

   (i) An SN is not allowed to read its readings to its neighbors, and if such recognition exists,
   (ii) The key distribution method (i.e., Diffie–Hellman) must be amazingly strong,
   (iii) Open data, for example, public keys and sensor characters of the nodes ought to likewise be scrambled in specific bodies of evidence to secure against traffic analysis attacks.

II. Data integrity: Make sure that an organization cannot send a message when it passes to the beneficiary from the sender.

III. Availability: These demands ensure that WSN's rulers are accessible both in and out of the way in the event of attacks, such as the service attack (DoS). Analysts tend to divide the methods of dividing this goal. If one of the systems uses the corresponding correspondence between the nodes, others utilize the use of a middle control framework to effectively distribute each message to its beneficiaries.

IV. Data Authentication (DA): Authentication guarantees the unwavering quality of the message by recognizing its starting point. In a WSN, the issue of validation ought to attend to the accompanying necessities:

(i) Communicating point is the one that it professes to be used among the two nodes for the transferring of the data.

(ii) The recipient ought to check that the acknowledged packets have verifiably originated since the real SN.

For confirmation to be accomplished, the two families could share a secret part to calculate message authentication code (MAC) of all imparted information. The collector will confirm the authentication of the got message by utilizing the MAC key.

V. Non-repudiation: It intends to assurance that the message exchanged has been sent and got by the parties professing to have sent and got the message.

VI. Availability: Availability means to ensure that the data resource is available for legitimate user [19]. It says data ought to be accessible dependably to the legitimate clients all through the system regardless of whether there are inner or outer failures, faults, errors, or attacks [20].

VII. Data Freshness: It guarantees that the intimation got amid trade is crude without any trace of reused data. In wireless sensor network, the data's may not be transmitted inside the given time interim, so we should ensure that it is new. To accomplish this, the time stamp is utilized. It comprises two sorts, for example, frail freshness gives a little request to the information's so delay cannot be determined, while solid freshness gives a general request and permits the count of delays [20].

VIII. Self-organization (SO): WSN is usually an ad-hoc network (AHN), where each SN should be autonomous and sufficiently adaptable to be SO and self-healing (SH) in any situations. There is no permanent framework accessible for the system supervision, so nodes should adjust themselves for the organization strategy [19].

## *3.2 Constraints in WSN*

I. Resource constraints: Low computational power, small memory, low remote control data transmission, restrained as a range, no battery-operated string.

II. Small message size (SMS): The communication in SN has a little size contrasted and the existing networks generally for the most part. Therefore, there is normally no understanding of division in many applications in WSN.

III. Addressing proposals: Appropriate to a generally expansive number of sensor nodes, it is beyond the realm of imagination to expect to manufacture worldwide tending to plans for sending of countless SN as the visual projection of uniqueness preservation is elevated.

IV. Sensor location (SL) and idleness of data: Location responsiveness of SN is significant since information gathering is usually found on position. Likewise, there could be regular wonders together information, it is therefore very likely that this data has some recursion.

### 3.3 Security Threat Models

As indicated by Karlof et al. [21], terrorization in WSN may be ordered into the accompanying classes:

a. Insider attacks (IA) versus outsider: It happens when there are authentic points of a WSN Act in unexpected or unrecognized path. The invader may have incomplete key metric and other SN. IN are very difficult to recognize. Outdoor attacks can be considered as an attack on nodes with no WSN space. The outside invader does not have the most cryptographic materials on the SN.
b. Active versus passive attacks: Latent attacks are in listening stealthily on, or checking of parcels exchanged inside a WSN; the dynamic attacks incorporate a couple of changes of the information stream and the generation of a bogus stream in a WSN.
c. Laptop-class versus Mote-class attack: In laptop-class attacks, all competitors like a rival PC can be used, and it would be damaging a system more than a deadly sensor. In mote-class attacks, a WSN attacked by nodes with relatively powerful nodes, such as network nodes (NN).

Attacks against the WSN are categorized as critically or not. Navigation attacks, usually, side channel attacks include, for example, power-, timing-, or frequency-based attacks. For example, WSN's obvious distribution of clear side attacks, for instance, has many problems with other established frameworks, for example, MAC generation or encryption time can be used with time sensors using sensor nodes.

1. MAC generation: The cryptographic systems are designed to perform complicated encryption and the creation of message authentication becomes challenging in spite of various attacks from adversaries. Many protocols are designed based on the assumption that the host's posses a secret random string known as key and it is conveniently taken for granted that the entire key is kept secret from an adversary. There might be a possibility that an adversary may detect a part or entire key which is called as key exposure problem and it has significant practical interests.
2. Encryption time: This is generally the time required during the generation of keys, encrypted text, and decrypted text. The algorithm having less time for each of the processes is considered to be better algorithm.

Violent attacks are very common; most of them are portrayed in the following sections. Some attacks on sensor networks are as follows:

Attack on protocol layer (PL):

(1) Physical layer: This tile and associates adds:

I. JAMMING: Transmission of a signal to an attacker on base stations at the same frequency of the transmitter. This interrupts the radio conversations.

**Defensive measures**: It is the use of communicating with each other, i.e., the frequency hopping spread spectrum (FHSS) that makes the frequency hoop. This shows the swap of the bus data between different frequency channels [22].

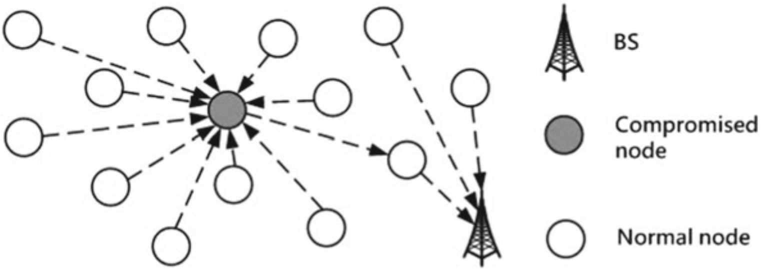

**Fig. 2** Tampering attack

II. Tampering: The attacker is trying to go to a mechanical assembly such as chips. The treatment of bits also receives confidential data from the SN (Fig. 2).

**Defensive measures**: It also helps in containing secret data between the microcontroller and external memory chip. This process is known as eavesdropping.

(2) Data link layer (DLL): This tile and associates adds:

I. Collision/pileup: When an attacker finds the message that a message sends out, he removes his own signals to intervene. This causes conflicts when multiple nodes pass on the same frequency and data velocity. The packet can change the information to be considered worthless.

**Defensive measures**: Steps to deal with this attack can be prevented.

II. Exhaustion/collapse: Aggressor sends ease of data or demand in a channel that promotes deprivation. The origin of the attack is a PC or laptop.

**DM**: It may claim to reduce the MAC sending rate to avoid excess demand from the sensor network. As long as the sensor node enables us to transfer data over time, on these lines, the MAC channel for nodes has long been connected. [22]

(3) Network layer (NL): This layer contains attacks:

I. Selective forwarding (SF): SF is an approach to impact system interchange by trusting to the entire the taking contributing hubs in network are dependable to advance the information. In fixed-sent attacks, some malicious messages (MNs) provide some messages against sending a message (DCM). MN or attacking nodes may won’t route definite messages and leave them. If that they leave every one of the packets during them, at that point it’s known as a BHA. Be that as it may, on the off chance that they specifically forward packets, at that point it is termed as selective forwarding. The embarkation of this occurrence depends on two factors. First, the position of the malicious party, which is much higher than the BS, it will pull off more. The second is the quality of the dropdown messages. Special exchange of this is where a stronger point is to capture all of the nude nodes while most messages are excluded.

**Defensive measures**: Multipath routing could be used to counterattack. This lessens the likelihood of an attack by an enemy. To regulate the framework guard dog can be utilized.

II. Acknowledge spoofing (AS): An attacker can associate with environmental light air conditioner consent. Wrong error messages are created by the attacker. Making routing links. Thus, latency will be terminated and the organization will be assigned (Fig. 3).

**Defensive measures**: Each packet must be broken for a rival.

III. BHA (Black hole attack): In this attack, an MN sensor goes like a black hole [21] to drag for all traffic on the network. Especially in a flood-founded convention, he is listening to answers to the answers to the high-caliber or lowest goal–goal nodes for the BS. If you have a capable device capable of containing malicious nodes (for example, sink and SN), you can do it with packets that go between them. This attack can be influenced even by the nodes of significant means from basic stations. Figure 4 demonstrated the vision applied to a black hole/sinkhole attack.

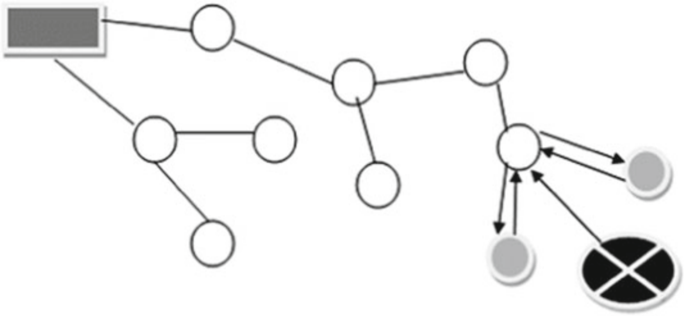

**Fig. 3** Acknowledge spoofing

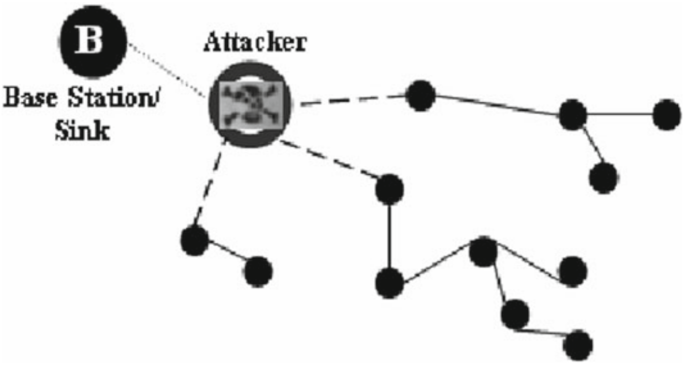

**Fig. 4** Black hole attack

**Defensive measures (DM)**: An arrangement ought to be executed, so one of the hubs on the system must be perceived by translate rate information disseminated through invalid hubs. Cryptographic procedures can be utilized.

IV. Wormhole attack (WHA): It sends offensive record bits to one place in the system at one place and sends them to the other places in the tunnel. Wormhole, WSN is a major threat to the child's tanning or rearrangement choices; there is no need to compromise a sensor in this network for such an attack, it can be done at the beginning of the stage when the sensor starts searching for the neighboring information (Fig. 5) [23].

**DM**: A four-way handshaking messaging system is used to counterattack. The private channel can likewise be utilized for security.

V. Sybil: According to [24], a self-trickery belonging is appended with a hub that keeps nearest node in various locations. Outsiders focus on these numerous areas and cause issues in dispersed capacity to get to multipath routing and bending in topology (Fig. 6).

**Defensive measures**: Validation procedure necessity is utilized to counterattack.

VI. Hello flood (HF): Attacker transmits hello packets starting with one node then onto the next. Attacker publicizes modest routes which lead to sending of communication to assailant [25].

**Defensive measure (DM)**: Using the profile evaluation convention, you can oppose the HELLO FLOW.

According to nature, protocols named Proactive, Active, and Hybrid:

(a) Proactive Routing Protocol: These protocols are additionally called as table-driven routing protocols since they keep up the routing data even before expecting of this data. Every single hub keeps up directing data to each other hub in

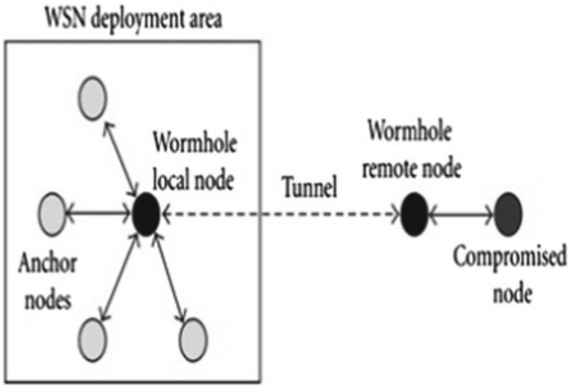

**Fig. 5** Wormhole attack

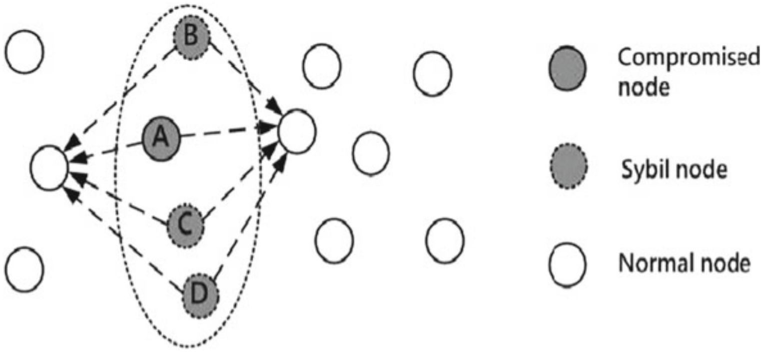

**Fig. 6** Sybil attack

the system. Courses data is commonly kept in the steering tables and is intermittently refreshed as the system topology changes. The protocols under this classification keep up various numbers of tables. Moreover, they are not appropriate for extensive systems, as they have to keep up sections for every hub in the steering table.

(b) Reactive Routing Protocol: These protocols are likewise called as on-demand routing protocol as in these sort of routing protocols hub looks for course on-request, i.e., at whatever point a hub needs to send information it scans course for goal hub and builds up the association.

(c) Hybrid Routing Protocol: The combination of both above protocols is identified as hybrid routing protocols.

### *3.4 Security Solutions in WSN*

WSN are exceptionally defenseless against attacks, it is imperative to embrace a few methods that can shield the system from a wide range of attacks it must be a guarantee that the framework is secured previously, amid and after any sort of attack [26]. Security guards and safety are the main tools for recovery. These locomotives have public key cryptography (PKC), semantic key encryption (SKE), and hash functions (HF) [27]. The SKE and HF are building blocks that make up the required infrastructure of the data stream. This is a confirmation of the classification and reliability of this channel. PKC guarantees assurance from the interest of outside substances and furthermore disposes of the issue of a malicious insider which attempts to utilize added one personality.

PKC guarantees by permitting confirmation of friends associated with the data trade. In light of the natives, it is conceivable to make superior system administrations. It is likewise similarly vital to have a key administration framework by building a safe key base.

Security is a widely used feature of authenticity, integrity, privacy, discontent, and anti-playbacks. The risk of secure transmission of information for the network, increasing the reliability of the information provided to the network. In this section, we discuss network security finances and technology for WSN.

(a) Encryption:

This system is opposed to inactivity, such as a candle. The sensor network is mostly wireless channels operating in public or wild areas. It is therefore uncommon to transfer emails from a device or add messages to the network. The traditional key of this problem is the three primary methods: the authentication codes, the similar key encryption schemes, and the public key cryptography.

(b) Symmetric encryption:

In this paper, the capacity to investigate security shortcomings, mishaps, and infringement has appeared on a honeypot system for WSNs. This is a recommended way to deal with a model that needs more examinations to assess its adequacy as a total framework for recognizing system attacks and different attacks. The opposite side of this innovation has been connected to control utilization by honeypot sensor hubs. This strategy does not have any significant bearing to other security issues and should, accordingly, be joined with different arrangements.

(c) Asymmetric encryption:

This is also known as public key cryptography. It uses two keys: The public key used by encryption, private key, and only the user of the key used to decryption it. Public–private keys are interconnected with any mathematical means. In other words, encrypted data with a public key can only be encrypted using its corresponding key.

(d) Cryptography:

Cryptography is of prime importance, the basic attitudes that make sure the essential elements, honesty, and confidentiality. Elliptic curve cryptography (ECC) is recognized as a practical approach for WSN. A good alternative is the ECC for RSA-based algorithms, as the size of the standard ECC keys, if it is too small for security [28].

## 4 Key Management Systems

In the wake of watching the imperatives and restrictions of sensor systems, obviously, these sorts of environment require trivial cryptography to accomplishing the abnormal state of security [29]. So as to give a protected security arrangement, all sensors need to concur between the costs, the death penalty, and security. Be that as it may, in the meantime, it is hard to accomplish three arrangement objectives. In such a circumstance, engineers are making gifts to the economy utilizing successful viable budgetary arrangements that are not authentic for key appropriation [29].

Accordingly, WSN requires various systems to enhance movement on the fundamental appropriation of the system, which is how they are utilized on verified settled systems.

## 4.1 Protocols and Methods Classification

Mainly techniques dependent on asymmetric or symmetric and hybrid frameworks tackle issue of the key foundation during a pre-distribution stage. The pre-distribution of encoding keys in a WSN is the reality of putting away these keys in the MN previous to exploitation. In literature, we discover a few characterizations of cryptographic key administration frameworks, for example, papers in [30–32]. A few classifications strategies depend on key participation, two nodes (pairwise) or more nodes (group restrictions) and more, abusing the possibility of joint testing. We made a classification and all major governments and distribution models were included in two larger families. The primary classification includes (i) symmetric projects (ii) and asymmetrical projects.

In connivance, the main model of writing will be examined by us as follows:

(i) Symmetric plans (SP): The plans of this segment utilize unbalanced to build up an open key between two hubs in a WSN. It's done in three stages which are given below:

I. Key Pre-circulation: Keys set in memory before conveying are a hub key hub. You can make a typical key between two hubs.
II. Shared-key discovery: Two general keys are easier to find after communicating with the protocol. On deployment, neighboring sensor nodes begin the discovery process to find out whether they share a common key, if they do, they establish a secure link. There could be many modes for the discovery phase, such as broadcasting the list of identifiers existing in their key ring in clear text or through a challenge-response mechanism.
III. Path key establishment (PKE): In the event that there is no open key between the two hubs you need to impart, you should locate a protected way between them. This way goes through a lot of hubs that as of now have secure connections. Two ways are utilized to verify correspondence when this way is set up. A key pre-distribution scheme called PIKE (peer intermediaries for key establishment) is used to achieve the path key establishment. PIKE can guarantee that any two nodes in a network always share a key with an intermediary node. This intermediary node is then used to establish a path key between the two nodes. But this approach makes a large fraction of neighboring sensor pairs that do not share preloaded keys, and thus they need to establish path keys.

Some security protocols are examined beneath:

3. SPINS: This is a suite of security and security hinders that are given by Prig and various different creators. It is advanced for asset restricted conditions and remote correspondences [33]. Twists have two secure squares: SNEP, μTESLA.

   I. SNEP utilizes a common counter between two interchanges gatherings and the counter is utilized to compute a message validation code (MAC) to give semantic security, information uprightness, decodialization, information classification, answer assurance, and refreshing frail messages. What's more, since protocol has lower communications systems, on the off chance that the quantity of controls is dependent on each counter, the convention will just offer up to 8 bytes for each message. For a solid new reason, the sender will make an irregular sound (anticipated 64-bit esteem) and will be incorporated into the beneficiary's demand message. Resister creates reaction messages and incorporates non-MAC processing.
   II. μTESLA produces authentic broadcasts broadcasting from symmetric premises but is presented with delayed key opening and single-function key chains. SPINS also accepts the certified routing application and security back key agreement with μTESLA and SNEP, along with minimum storage, calculation, and communications expenditure. Though few issues still report by SPINS, it will not be regarded as a possible source of DOS risk; SPINS depend on the station-based station because the pair's rear distribution key uses the security protocols; the communication key's update will not be considered. A practical key updating system is needed to prepare for security. Hidden channel leak, spins cannot solve a node problem.

4. LEAP: The LEAP (nearby encryption, validation convention) is a noteworthy administration convention for sensors that help in organize preparing utilizing the fundamental system to control the security impact of a hub that has been undermined for moment arrange neighborhoods. The possibility of the Leap+ was propelled by this intriguing perception that distinctive kinds of messages were exchanged between the sensor hubs. This perception has achieved the decision that an alternate enemy of bunch framework is insufficient for these diverse security prerequisites [34–36]. Backing for the foundation of four keys per node:

   I. Pairwise key: shared with different SN.
   II. Individual key: Shared amid a BS.
   III. Global key: All nodes shared on the network.
   IV. Cluster key: Shared through several neighboring points.

   Packages that have been exchanged for each node in the sensor network are categorized into several categories, for example, different criteria:

   I. Queries or commands sensor readings,
   II. Broadcast Packets versus Unix Packets,
   III. Manage packets, manage data packets, etc.

The security prerequisite for every parcel relies upon the particular classification. Most bundles need to confirm, at times, just the bundles are the codename. This shows that a solitary key framework isn't suitable for every safe correspondence important in sensor systems.

5. Tinysec: Karlof et al. [37] TinySec convention forward and complete activity of secure structure in WSN's information connect layer. This execution underpins two security alternatives: authenticity of messages without message verification and information encryption (TinySec-Auth) with data encryption (TinySec-EA). TinySec utilizes normal cryptographic calculations to guarantee protection and security value checking. The Skyjack calculation [38] for WSN is greatly improved than the two combination revelations found in RC5 (calculation utilized in spines). TinySec validation is determined utilizing RC5 Pre-key utilizing 104 bytes. Utilizing TinySec CBC encryption mode (cipher blockchain) utilizes CTR (utilizing SPINS). The CD will furnish a similar bundle encryption with similar arbitrary numbers. Basically, these numbers are used to generate the encryption, an important section defames it through recursion by the security modules of its repetition and then helps the opponents find the content of the messages. TinySec is actualizing a noteworthy conveyance venture, coming up to finish a noteworthy circulation framework for the all-encompassing system. Two centers have two fundamental symmetric keys shared to pass on. The first is used as scramble messages, and second to determine MAC messages.

6. Micro-PKI: Munivel et al. [39] a straightforward variant of conventional PKI, small-scale PKI propose a technique that is known as an open key foundation. The base station (BS) has an open key and another private. People in general key are utilized for verification of the BSand the private station (PS) is utilized to decode information sent from the hubs. Before conveying, the BS open key is put away in all hubs. Creators give two kinds of handhelds. First sort validation between the interface hub and base station the hub makes a symmetry session key and encodes it utilizing the general population key of the BS. To guarantee the respectability of messages, each message is proposed to coordinate with a MAC (code) utilizing a similar encryption key. For new hubs to join the system, people in general key of the BS is put away on these hubs previously sending.
7. TinyPK: Watro et al. [40] A strategy known as TinyPK dependent on the utilization of open keys and the guideline of Diffie–Hellman proposed establishing a mystery key between the two hubs in WSN. TinyPK utilizes reliable specialist to sign hubs and open keys. Prior to deployment, the CA key is distributed before all keys, so the key can be verified by deploying. Time and energy of the RSA algorithm selection nodes for encryption are of great use. This basic functionality can be about a dozen seconds long, which reduces the time within the network, reducing the effectiveness of reaction.
8. PKKE and CBKE: The two conventions as shown by Zigbee utilizing the recognizable proof of hubs in the key expansion. This is to utilize these personalities to create a solitary sharing key between each pair of hubs on a system. Be that as it may, a common key is created through shared associations between the two hubs.

**Table 1** Comparison among security protocols

| Protocols | Encryption | Freshness (CTR) | Overhead (Bytes) | MAC used | Key agreement |
|---|---|---|---|---|---|
| SPIN | Yes | Yes | 8 | Yes | Symmetric delayed |
| LEAP | Yes | No | Variable | Yes | Pre-deployed |
| TINY SEC | Yes | No | 4 | Yes | Any |
| MICRO-PKI | Yes | Yes | Variable | Yes | Open key foundation |
| TINY PK | Yes | No | 16 | No | Pre-deployed |
| PKKE and CBKE | Yes | No | 8 | No | Noninteractive key distribution scheme |
| C4W | Yes | Yes | 4 | No | Pre-deployed |

This means that you need to send and receive more than one message before creating the key. To protect the power nodes you wish to share with a secret and such intermediate node, there are a number of ways to remove this mutual exchange. These methods are called field ID-NIKDS [41] (a noninteractive key distribution scheme based on identity) in cryptography.

9. C4 W: Jing et al. [42] proposed a methodology known as C4 W based on identifying nodes to estimate open keys. Nodes can calculate other nodes' public keys. What might supplant the jobs of a testament? Before sending, hubs and base stations will be stacked with their very individual keys (private/open key ECC) and general data on system hubs. C4 W technique setting up a solitary sharing key in two hubs utilizing the standard of Diffie–Hellman key exchange is to use without testaments. In Table 1, there is a comparison performed on the basis of different parameters.

# 5 Analysis and Discussion

## *5.1 Analysis Method*

A few criteria are considered so as to look at changed techniques for key administration. We have exhibited in the standard models shown in Fig. 5. We begin with the hub's asset limits. The key management method necessitates that the hubs be conveyed to gather data. They need their memory space to keep their information and vitality inserted so as to guarantee their application job. The arrangement ought to likewise be adaptable and dynamic, and adaptability can go. Another basis to be regarded is the deficiency of viciousness. For example, when capturing nodes, an opponent may use information that can be used to perform other attacks, network management, and storage. Key management should identify the noncompatible nodes (NCN) and authenticate network nodes (ANN) before allocating keys. Final criteria are the upgrade and cancelation of the keys. We can give importance to the consequence of significant distribution that must be dismissed by an obsolete key or an opponent. Keys must be renewed with secure links as well and the node's guarantee that the network's connectivity has more ways to throw its information. The technique of key network allotment should be proficient of ensuring excellent network connectivity. The departure or a node capture can limit the connectivity of other nodes on the set of connections. This mechanism should consider the distribution method by suggesting new safe steps.

## *5.2 Discussion*

WSN studied various types of distribution and key organization. Merely the dimension of the keys hoarded in the memory storage nodes in table is evaluated and the coding algorithm is not the cryptographic primary scope. Stars in the list represent a quality. We placed three or two black stars in the "connectivity" range to indicate high degrees, medium or low connectivity, respectively. In the column "Resistance to attacks," we have created three, two, and one star. The pictures are really high and middle class and resistance to counteract attacks. On the other hand, the circle in the list must provide a default. There are three or two black circles in "resources at cost savings" that indicate that the dialogs use high-, middle-, and low-cost consumption, respectively.

Experts' keys utilizing SPINS and LEAPs additionally decrease the capacity of keys in the memory of the hubs. Be that as it may, the opposition of the attacks is low. The ace key can be undermined any longer and can be undermined with the keys after the arrangement. It is the most appropriate and fastest way they can be computed through a symmetry group method. The secret keys are used to transfer other secret keys, the references to the redesign, and revocation of the equations (obviously). The issue in the asymmetric diary is very simple as the public keys don't have to be confidential. Chan et al. show probability illustration low-power consumption doesn't require a large amount of computing capability. Anyway, the key size ring accumulated in memory nodes is one of the most expensive simmers on the size of this snail memory. Type physical nodes cannot resist captures. Better connectivity between network nodes is provided by PIKE scheme, except low presentation on scalability. In the form of the schema, Tiny is ideal for the PBC asymmetries. It is defensive for the most harasses in the RCSF. The fact that setting up a special key that is shared between the two nodes aided to decrease the larger storage ability in memory. In addition, this key generates energy between the nodes that protect the time when these interventions are calculated as a result. The diagrams used by the principles of certificates and PKI are mainly cost-effective in computation and energy consumption. The difference between symmetries and inequality may vary relying on the required intensity of the network. Let's see if the equations can be resistant to their contemporary and inequitable diagrams.

## 6 Conclusions

This paper presented different security threat models and security requirement along with various protocol discussions. To face those attacks, we have presented a synthesis of cryptography systems and mechanisms that can secure the WSN. The lack of infrastructure such as PKI in the WSN has compelled the nodes to not have confidence in network and to create secure paths from the source of the data to the BS. Works like [42] have used the identities of the nodes and the principle of coupling in order to reduce, or even eliminate, the interactions between nodes to counter a maximum of attacks. However, to date there are no complete and dynamic solutions easily adaptable to WSN. Present routing protocols, such as SPINS and LEAP, are maturing in steering behavior. With the model of safe routing protocols, we can offer a good research method for the extension of original protocol if we can achieve security requirements through a minor change in SRD, INTRSN, etc. This provides the overall description of the protocols and their features and also explains various security-related concerns. In addition, for the future, these researches provide us a direction.

## References

1. Akyildiz, F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *IEEE Communications Magazine, 40*(80), 102–114.
2. Binh, H. T. T., & Dey, N. (Eds.). (2018). *Soft computing in wireless sensor networks*. Boca Raton: CRC Press.
3. Das, S. K., Yadav, A. K., & Tripathi, S. (2017). IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network. *Peer-to-Peer Networking and Applications, 10*(3), 670–687. https://doi.org/10.1007/s12083-016-0532-6.
4. Yadav, A. K., Das, S. K., & Tripathi, S. (2017). EFMMRP: Design of efficient fuzzy based multi-constraint multicast routing protocol for wireless ad-hoc network. *Computer Networks, 118,* 15–23.
5. Das, S. K., & Tripathi, S. (2018). Intelligent energy-aware efficient routing for MANET. *Wireless Networks, 24*(4), 1139–1159. https://doi.org/10.1007/s11276-016-1388-7. Springer.
6. Das, S. K., & Tripathi, S. (2019). Energy efficient routing formation algorithm for hybrid ad-hoc network: A geometric programming approach. *Peer-to-Peer Networking and Applications, 12*(1), 102–128. https://doi.org/10.1007/s12083-018-0643-3. Springer.
7. Das, S. K., & Tripathi, S. (2018). Adaptive and intelligent energy efficient rout-ing for transparent heterogeneous ad-hoc network by fusion of game theory and linear programming. *Applied Intelligence, 48*(7), 1825–1845. https://doi.org/10.1007/s10489-017-1061-6.
8. Das, S. K., & Tripathi, S. (2017). Energy efficient routing formation technique for hybrid ad hoc network using fusion of artificial intelligence techniques. *International Journal of Communication Systems, 30*(16). https://doi.org/10.1002/dac.3340.

9. Pradhan, C., Das, H., Naik, B., & Dey, N. (Eds.). (2018). *Handbook of research on information security in biomedical signal processing*. Hershey: IGI Global.
10. Bletsas, A., & Lippman, A. (2005). Spontaneous synchronization in multi-hop embedded sensor networks: Demonstration of a server-free approach. In *IEEE* (pp. 331–341).
11. Priyadarshini, V. M., Muthukumar, N., & Natarajan, M. (2011). Cellular architecture sensor for WSNs. *IJRRSE, 01*(02), 47–51.
12. Biagioni, E., & Chen, S. H. (2004). A reliability layer for ad-hoc wireless sensor network routing. In *Proceedings of the 37th Hawaii International Conference on System Sciences* (pp. 1–8). IEEE.
13. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2001). *Wireless sensor networks: A survey* (pp. 393–422). Electrical and Computer Engineering, Georgia Institute of Technology.
14. Wong, K. H., Zheng, Y., Cao, J., & Wang, S. (2006). A dynamic user authentication scheme for wireless sensor networks. In *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, Trustworthy Computing* (pp. 244–251). IEEE Computer Society.
15. Collins, M., Dobson, S., & Nixon, P. (2010). A lightweight secure architecture for wireless sensor networks. *Internet Technology and Secured Transactions, 2*(1/2), 12–136.
16. Aftab, M. U., Ashraf, O., Irfa, M., Majid, M., Nisar, A., & Habib, M. A. (2015). A review study of wireless sensor networks and its security. *Communications and Network*, 172–179.
17. Men, X., Shi, X., Wang, Z., Wu, S., & Li, C. (2016). *A grid-based reliable routing protocol for wireless sensor networks with randomly distributed clusters* (pp. 41–61). International School of Software, Wuhan University.
18. Undercoffer, J., Avancha, S., Joshi, A., & Pinkston, J. (2002). Security for sensor networks. In *CADIP Research Symposium*, 1–51. http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf.
19. Carman, D. W., Krus, P. S., & Matt. B. J. (2000). *Constraints and approaches for distributed sensor network security* (pp. 1–126). Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, USA.
20. Perrig, A., Szewczyk, R., Wen, V., Culler, D. E., & Tygar, J. D. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks, 8*(5), 521–534.
21. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, 113–127.
22. Saxena, A., Pal, O., & Saquib, Z. (2011). Public key cryptography based approach for securing SCADA communications. *Computer Networks & Information Technologies*, 56–62.
23. Fatema, N., & Brad, R. (2013). Attacks and counterattacks on wireless sensor networks. *International Journal of Ad Hoc and Ubiquitous Computing, 4*(6), 1–15.
24. Culpepper, B. J., & Tseng, H. C. (2004). Sinkhole intrusion indicators in DSR MANETs. In *Proceedings of the First International Conference on Broad band Networks* (pp. 681–688).
25. Hu, Y.-C., Perrig, A., & Johnson, D. B. (2003) Packet leashes: A defense against wormhole attacks in wireless networks. In *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*. IEEE INFOCOM 2003, 30 March–3 April 2003, vol. 3, pp. 1976–1986.
26. Padmavathi, G., & Shanmugapriya, D. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security, 4*(1 & 2), 1–9.
27. Xiong, N. N., Cheng, H., Hussain, S., Qu, Y. (2013). Fault tolerant and ubiquotous computing in sensor networks. *International Journal of Distributed Sensor Networks*, 1–2. Article ID 524547.
28. Huang, A. (2005, October). *Security primitives for ultra-low power sensor nodes in wireless sensor networks*. Faculty of Engineering, the Built Environment and Information Technology, University of Pretoria.
29. Gaubatz, G., Kaps, J., & Sunar, B. *Public key cryptography in sensor networks—Revisited* (pp. 1–17). Department of Electrical & Computer Engineering Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609, USA.

30. Szczechowiak, Piotr. (2010). *Cryptographic key distribution in wireless sensor networks using bilinear pairings*. PhD dissertation, Dublin City University.
31. Hegland, M., Winjum, E., Mjolsnes, S. F., Rong, C., Kure, O., & Spilling, P. (2006). A survey of key management in ad hoc networks. *IEEE Communications Surveys & Tutorials., 8*(3), 48–66.
32. Camtepe, S. A., & Yener, B. (2005). *Key distribution mechanisms for wireless sensor networks: A survey* (pp. 1–27).
33. Ruj, S., Nayak, A., & Stojmenovic, I. (2011). Key predistribution in wireless sensor networks when sensors are within communication range. In S. Nikoletseas & J. D. P. Rolim (Eds.), *Theoretical aspects of distributed computing in sensor networks* (pp. 787–832). Berlin: Springer.
34. Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002, September). SPINS: Security protocols for sensor networks. *Wireless Networks, 8*(5), 521–534.
35. Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks, 2*(4), 500–528.
36. Celozzi, C., Gandino, F., & Rebaudengo, M. (2013). *Improving key negotiation in transitory master key schemes for wireless sensor networks*. Politecnico di Torino, lecture notes of the institute for computer sciences, social informatics and telecommunications engineering (vol. 122, pp. 1–16). Cham: Springer.
37. Karlof, C., Sastry, N., & Wagner, D. (2004). TinySec: A link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems* (pp. 162–175). New York, NY, USA: ACM.
38. Brickell, E. F. (1993). The SKIPJACK algorithm, July, vol. 28, pp. 1–7.
39. Munivel, E., & Ajit, G. M. (2010). Efficient public key infrastructure implementation in wireless sensor networks. In *International Conference on Wireless Communication and Sensor Computing* (pp. 1–6).
40. Sakai, R., Ohgishi, K., & Kasahara, M. (2000). Cryptosystems based on pairing. In *Symposium on Cryptography and Information Security (SCIS'00)* (pp. 26–28). Japan.
41. Jing, Q., Hu, J., & Chen, Z. (2006). C4W: An energy efficient public key cryptosystem for large-scale wireless sensor networks. In *2006 IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)* (pp. 827–832).
42. Oliveira, L. B., Aranha, D. F., Gouvêa, C. P. L., Scott, M., Câmara, D. F., López, J., & Dahab, R. (2011). TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. *Computer Communications, 34*(3), 485–493.
43. Devi, C., Dhivya, & Santhi, B. (2013). Study on security protocols in wireless sensor networks. *International Journal of Engineering and Technology, 5*(5), 200–207.