Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7766189

SECURITY ISSUES OF WIRELESS SENOR NETWORK AND OPEN RESEARCH CHALLENGES

Mandar K Mokashi[1] **Dr. Ninad N. More**[2] **Dr.Vinayak G. Kottawar**[3]

[1]Research Scholar, School of Engineering and Technology, D.Y.Patil University Pune-Ambi (India) and Assistant Professor, Department of Information Technology, Vishwakarma Institute of Information Technology, Pune (India)

[2]Supervisor, Department of Computer Engineering, School of Engineering and Technology, D.Y.Patil University Pune-Ambi (India)

[3]Co-Guide, Department of Artificial Intelligence and Data Science, D.Y.Patil College of Engineering, Akurdi, Pune (India)

Abstract

Wireless Sensor Network (WSN) is a rising technology for real-time applications to track and monitor environmental and physical parameters. Due to the properties of sensor nodes such as small size, low cost, wireless communication, processing capability, it is widely used in military and public applications. The WSN system deals with real time data, so it becomes prone to various attacks at each level, such as; jamming, tampering, collision, overwhelm, repudiation, monitoring and eavesdropping, flooding, session hijacking, wormhole, black hole, gray hole, sinkhole, Byzantine, and Sybil attack. The paper aggregates all possible attacks at each layer of the WSN protocol stack. It also briefs the major security issues and the possible attacks on WSN system. Finally, the paper is enveloped with a brief discussion on open research challenges.

Keywords: WSN Security challenges, WSN Protocol stack, Attacks based on layers, open research challenges in WSN Security

1. Introduction

Over the last few years, the research community and industry significantly developed an interest in Wireless Sensor Network (WSN) due to its wide range of real time applications [1][2]. WSN usually comprises a large number of sensor nodes placed uniformly or randomly in the target area. It is highly in demand due to the inventions in sensor nodes in terms of, communication, processing capability, and sensing capability. After the invention of radio communication in WSN, the scope of applications such as rescue & disaster systems, wildlife monitoring, health monitoring, medical diagnosis, agriculture, security applications, etc. have tremendously increased[3][4].

A WSN is communication between sensor nodes and the base station (BS) for data sensing and gathering a wireless communication channel. The sensor node sends sensed data to BS for processing. The processed data by BS is forwarded to the gateway to send it to the internet or satellite [5] [6]. The data is communicated to the end users through the internet or satellite. The sensor nodes may either be homogeneous or heterogeneous depending on the type of application [7] [8]. They are used to monitor physical and environmental conditions like; temperature, humidity, pressure, sound, heat, light, etc. In multimedia WSN applications, sensor nodes are equipped with cameras. As the way of communication in the WSN is merely the exchange of messages among sensor nodes and BS, it leads it to be more applicable in complex and intelligent applications [9][10].

1.1 Architecture of WSN

There are mainly two types of WSN architectures [11] [12].

- Flat based architecture WSN architecture
- Cluster based WSN architecture

1.1.1 Flat based WSN architecture

In the flat based WSN system, BS is generally located at the center of the network as shown in figure 1. All the sensor nodes are in the communication range of BS and send sensed data to it. The flat based WSN architecture. It is more suitable for applications where the target is area is small in size. Whereas for large target areas sensor nodes are not able to communicate with BS directly, then they can be routed through the neighbor nodes to BS [11].

Many design issues have to be taken into consideration such as field environments, network topologies, connectivity of nodes, types of nodes, localization of sensor nodes, data transmissions, energy consumptions, security mechanisms, etc. to design and implement a flat based system.

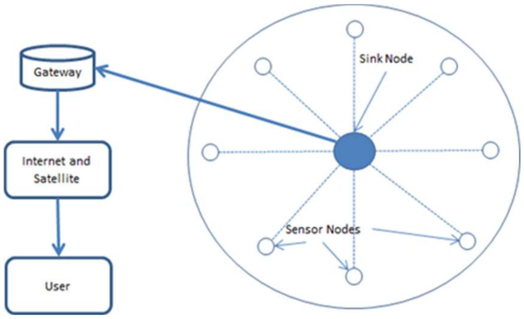

Figure 1 Flat based WSN system

1.1.2 Cluster based WSN architecture

In the cluster based WSN system, the target field is divided into a several groups, and each group is termed a cluster as shown in figure 2. Each of these clusters works as a flat based WSN system and select CH from among the sensor nodes, instead of BS. Sensor nodes send their sensed data to CH. CH collects the data and aggregates it and transfers it to the BS through other CH if it is not in the communication range of BS [12]. For transmission static or dynamic route is selected. All sensor nodes should be in the communication range of BS is not a must.

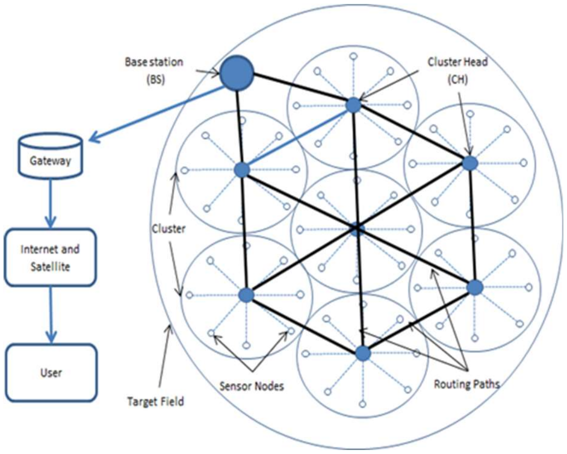

Figure 2 cluster based WSN system

WSN systems are prone to attackers due to wireless communication. The attackers can monitor the traffic, modify the data packets by inserting malicious data, and insert older data in the packet. Attackers can compromise sensor devices too. It also affects the aggregation process, receiving, and transmission of data. There are a lot of security issues, but, major are confidentiality, authentication, integrity, authorization, the ones that affect more on the working of the system. In the literature, major work focuses on the security approaches for data routing. Some cryptographic solutions are provided with symmetric and asymmetric keys. Some of them have proposed hashing functions. Sensor nodes are generally physically insecure once deployed as they are unattended and located in remote area. WSN systems are always vulnerable to physical attacks.

2. Paper Structure

The paper is mainly focused on the Security issues of WSN system and finally open research challenges are discussed. The structure of paper is shown in figure 3.

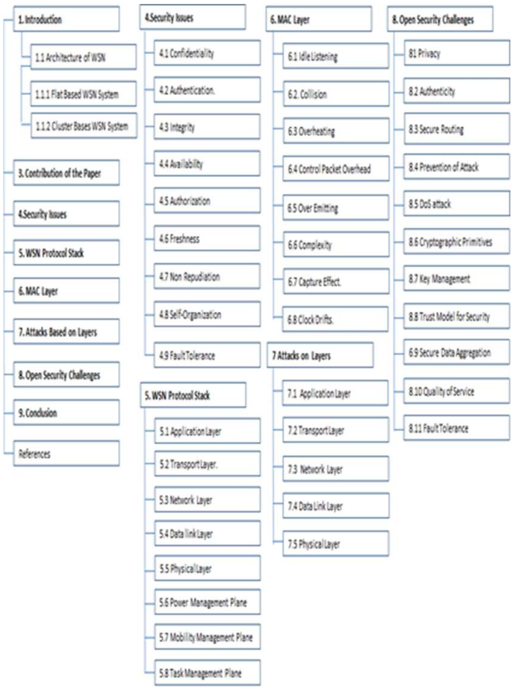

Figure 3 Paper Structure

3. Contribution of the Paper

The primary objective of this paper is to provide a brief overview of the security issues of traditional and cluster-based WSN to novice or inexperienced researchers. All relevant security literature had been critically examined, and the author had identified all potential security issues. The WSN system's current difficulties are highlighted in the paper. Last but not least, the WSN system's open challenges are mentioned and may serve as research objectives.

4. Security Issues

Designing a secure WSN system is a challenging task due to its computing power, memory size, less energy, wireless communication, hazard area and other environmental factors. Because the sensor nodes are positioned in an open area, the system is open to attack, replacement of the node or an intruder can easily cause an attack the network. In the WSN system, for authentication and communication, keys are used in between the sensor node, CH and BS. In the cluster system, three types of communications take place.

- Sensor node to CH
- CH to CH (for routing) and
- CH to BS

Symmetric keys and asymmetric keys are used in the network for communication. If the same key is used for the network and it is in the hand of the intruder

then, he will get full access to the network, so the key should be very secure and confidential [13].

While designing the security of the WSN system, various security measures need to be considered. Some of them are given below.

4.1 Confidentiality

The data which are gathered and transmitted must be in the protected form and should not be easily available to others. Generally, data leakages are in the communication channel due to malicious nodes or intruders. To avoid the misuse of confidential data, keys which are used for encryption must be in the encrypted and compressed form and not readable to others [13[14]. It is an open issue, a challenge to design an effective cryptographic technique which produces unreadable data and which is for the attackers hard to retrieve.

4.2 Authentication

There should be a specific protocol to include a new network node. Generally, malicious nodes try to get added to the network and behave as if they are a part of the existing network. While transmitting data, it should not get to illegal nodes. There should be a strong communication protocol which should verify the authenticity of the node. There should be some mechanism to verify and detect the malicious nodes [14].

4.3 Integrity

The main aim of data routing is to transfer the same information from transmitter to receiver, i.e. from source CH to BS through other CHs. Due to the wireless communication, electromagnetic signals affect transferring of the data, for example, signal diffraction, scattering, noise, reflections of the signal and fading, etc. [15].

The data may get altered by malicious nodes, which are in the network. If malicious nodes are a part of the routing path, they alter the received data and send it to the next hop. It is a big challenge to find such nodes.

4.4 Availability

Availability of a node is a major parameter to keep the WSN system alive and functional. Availability of node is affected by three parameters viz; battery power, failure of node and failure of communication channel. There is a need to design energy-efficient communication and routing strategies to enhance the life of the battery. Once any node fails due to electronic circuitry or other reasons, it should be replaced immediately or the relay nodes should take its place. There are some situations where the node works adequately but, is not able to send data due to the shortage of the communication range. Generally, it happens in Mobile Sensor Node (MSN), as it is moving it may move out of the communication range. There should be some mechanism so that it comes back in the communication range of the receivers [15].

Failure of the communication channel also effects on the availability of the network. The data will not be transmitted to BS if any node from the route or the communication channel between the two nodes fails and, due to less memory and flooding of the incoming data, it cannot store it for a long time. It has to discard it. So availability does not exist.

4.5 Authorization

In general, in most of the low budget systems authorization process is not implemented. The nodes which are taking part in communication and transmission must be authorized nodes. It protects from unauthorized malicious nodes transmission in the network. Even though it requires memory and energy for processing but some novel optimized techniques need to find in authorization of nodes before communication and transmission data [16].

4.6 Freshness

The network should take guarantee that the generated and transmitted data is fresh. Because it may happen that in dynamic routing if any route node is busy or fails due to some reason, then the new route is searched and data is routed through a new route. But if the old path is recovered and transmission is started, then old data may reach after some time. At the receiving end (BS), data should be sorted out as per the time stamps [15].

Generally, the old data is generated and sent by reply attach. It should be identified and find some remedial actions to stop it.

4.7 Non Repudiation

Non-repudiation is helpful for detecting and isolating the compromised nodes. It insures that the message's source cannot be denied. from message sent. At the receiver end, if it receives an erroneous message, then it should convey to all the other nodes that, the sender node is compromised and, not to transfer its messages. So, nonrepudiation secures system from malicious nodes activities [13].

4.8 Self-Organization

WSN systems are deployed in hazardous areas so, it is difficult to go and, find the faults and maintain the system. The deployed nodes should be autonomous, be able to self-organize and, self-heal [13].

In the network, if any node fails or drains then, the data should be routed through other possible nodes and, a new path should be searched. Each routing node should have this self-organizing capacity so, the network will not fail.

4.9 Fault tolerance

The main aim of the WSN system is to send data to BS in the worst condition also. WSN systems may face some failures in the battery, processor, transceiver, power depletion, radio interference, asymmetric communication links, dislocation of node and collision. To cope up with these issues the WSN system, should have fault tolerant mechanism, to minimize the impact of the failure. It should find alternatives to overcome the existing failure and try to make the system in a working state [16].

5. WSN Protocol Stack

The protocol stack promotes power efficient performance and path routing with minimum cost. Through a wireless medium, it integrates information with networking protocols and, provides co-operative efforts of the sensor nodes. It consists of the application layer, transport layer, network layer, data link layer, and the physical layer. It also consists of three planes; task management plane, mobility/connection management plane and, power management plane [13]. The protocol stack of WSN is shown in figure 4.

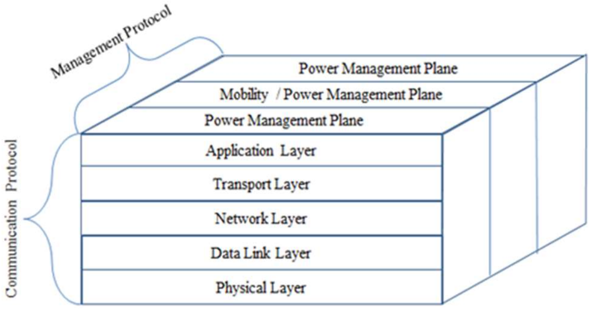

Figure 4 Protocol stack for WSN

Working and functionalities of protocol stack layers-

5.1 Application Layer

- Application deployment
- User communication
- Node localization
- Time synchronization
- Network security
- Database queries
- Sensor network management
- Sensor Query and Tasking Language (SQTL) provides a sensor programming language and implement middleware of WSN
- Uses protocol- Sensor Management Protocol (SMP)

5.2 Transport Layer

- Preserving flow of data
- Congestion control
- End to end connection management
- Data delivery
- Multi-hop transmission
- Upstream and downstream data management
- End to end security
- Authentication
- Encryption
- Data integrity
- Energy and resource efficient Protocol- Transport Control Protocol (TCP)

5.3 Network Layer

- Data routing
- Data centric nodes
- Power efficiency
- Data aggregation (optional)
- Attribute based addressing
- Location awareness

5.4 Data Link Layer

- Energy management
- Collision avoidance
- Multiplexing of data streams
- Data frame creations and detections
- Error control
- Medium access
- MAC (Medium Access Control) for network throughput
- Delivery latency and energy consumption

5.5 Physical Layer

- Modulation
- Data reception and transmission

- Converting bit streams to signal for transmission over communication medium
- Transmission medium and frequency selection
- Signal modulation and detection
- Data encryption
- Design of hardware and various electrical and mechanical interfaces

5.6 Power Management Plane

- If the energy of the sensor node is low, it communicates with the other nodes in the network, broadcasting that it is low in energy and, cannot take part in the communication. It handles /manages/copes by power management plane
- Manages energy level of sensor node, processing, transmission and reception

5.7 Mobility/Connection Management Plane

- It keeps track of the movement of the sensor nodes and its neighbours.
- Configuration and reconfiguration of sensor nodes to maintain connectivity in the network
- Topology change management due to node failure, node addition or node movement

5.8 Task Management Plane

- It schedules and balances the sensing activity of sensors to a specific location. At an instance not all sensors sense data.
- Task distribution among sensor nodes to improve overall network lifetime.

6. MAC Layer

Data link layer in protocol stack of WSN has two sub layers-

- Logical Link Layer (LLC)
- MAC (Medium Access Control) layer

LLC controls medium access, link management, and flow and error control. Whereas MAC has different functionalities and responsibilities which are as follows.

- Idle Listening, collision, overhearing, control packet overhead, over emitting, complexity, capture effect, Clock drifts.

6.1 Idle Listening

It is the state in which radio of the node is switched off. Most of the energy is required for radio communication of the node. In the low traffic application, it is a wastage of energy, so the node sets the radio in idle listening mode. It can be switched on at a specific time slot or in the occurrence of any event [13].

6.2 Collision

In high traffic applications, collision of frames may take place. If collision occurs, then frames are discarded and new frames are transmitted, this requires a lot of energy [17].

6.3 Overhearing

Broadcasted messages are sent to all nodes of the network. To verify whether it is related to itself or not, it requires processing power and energy. If more number of broadcasted messages are in the network, it keeps the nodes busy and, drains more energy even though it is not related to that specific node. If the broadcasted message is for one node then (n-1) node wastes their energy and processing power [18].

6.4 Control packet overhead

Control packets are required to communicate in the network but, more number of packets and, large size packets creates overhead to the nodes. It decreases the channel capacity, so a balanced approach is required [19] [20].

6.5 Over emitting

When receiving node is not ready to accept the packets, then over emitting problem occurs. It consumes channel bandwidth unnecessarily [20] [21].

6.6 Complexity

Complexity of MAC algorithm affects the processing and energy of overall network. But to perform complex functions like; clustering, data aggregation, dynamic path selection, node failure detection, diverting traffic, change in topology, etc. MAC algorithm needs to consider all these functionalities [18]. While designing it should be energy efficient.

6.7 Capture Effect

The receiver receives only high amplitude signals when two signals, with different amplitudes, are transmitted to it. Capturing should be balanced so that, retransmission will be avoided [18].

6.8 Clock drifts

Generally, quartz oscillators are used in networking equipment and, it is affected by age, magnetic fields, mechanical vibrations and, temperatures. Due to the time variations it is called as clock drift [18]

MAC layer protocol must be energy efficient for the lifetime of overall network. It also overlooks addition of node, death of working node and, noise of communication channel.

7. Attacks based on layers of Network

In WSN protocol stack there are five layers and all are prone to attack with regard to their functionalities. The layer wise attacks are given below.

7.1 Application Layer

Application layer plays a major role in the application hosting and, user interactions. It also specifies the data which is requested and sent in the network for interaction with the sensor nodes, BS and, end user.

Application layer is more prone to attacks because it contains aggregated user data which is sensed by the sensors. Attackers get ready-made information to misuse. Normally many vulnerable protocols are used in the application layer like; HTTP, SMTP, TELNET, FTP, etc. which provides accessing loopholes for the attackers [17].

The different types of attacks on the application layer are discussed below [17] [21].

7.1.1 Malicious code attack

Spywares, viruses, Trojan viruses can affect the system and cause it to slow down.

7.1.2 Base station path DoS /Overwhelm attack

In this, the attacker sends several same or, different packets to BS and keeps it busy. It wastes the network bandwidth and, energy.

7.1.3 Repudiation attack

Repudiation is to refuse to participate in partial communications or all the communications even though they can perform. It can be verified by the logs or the audit report.

7.1.4 Data corruption attack

When the data is received from other sensors to BS at the time of transmitting, malicious code is inserted into the packet. At BS the aggregation process is applied to make a useful and, compact data, which should be transferred. While aggregating, malicious code executes and complete data may be altered or deleted.

7.1.5 Monitoring and a Eavesdropping

While data transmission occurs snooping of data can be done by the intruder.

7.2 Transport Layer

Transport layer thrives to maintain data flow in the network. It establishes an end to end communication for reliable delivery of packets. It also performs conjunction control to avoid retransmission of data. Sometimes in the network receiving of packets is delayed so, the sender assumes that the packet has not reached the destination and, it retransmits it. Generally, UDP (User Datagram Protocol) and TCP (Transmission Control Protocol) are used in the transport layer but, it is more vulnerable to SYN flooding attack [17] [22] [23].

The attacks that may affect the transport layer are as follows:-

7.2.1 SYN Flooding

It is the same kind of Denial of Service (DoS) attack. The malicious node sends a large number of SYN packets to the victim node. But, before establishing connection both the nodes should share three handshake signals to start the communication. The malicious node never sends an ACK signal to the victim node to complete the first established connection. Likewise, victim's buffer and get overloaded with pending packets that it will not receive any further packets [25].

7.2.2 Session Hijacking

Generally, communication is protected at the time of session setup. The session hijacking attack gets the victim's address and, the sequence number which is expected by the victim. It then sends the data continuously to the victim and hijacks the victim's activities.

7.3 Network Layer

Network layer is responsible for routing of data in the network. The invader diverts the routing traffic to an unexpected path by attacking the routing protocol. The attacker absorbs the complete or, partial routed packets. By modifying routing table conjunction may occur [17] [24] [25].

In the literature several possible attacks on the network layer are mentioned. Some of these attacks are explained.

7.3.1 Flooding(Hello/RREQ/ACK) attack

Flooding attack is a mischievous activity wherein an attacker sends a large number of packets to the intend node so that it will be busy and, drain more energy to process them. Hello, RREQ and ACK are such messages, sent continuously in the network to keep it busy [15].

7.3.2 Wormhole Attack

Wormhole attack is the activity of the intruder node, which creates a new path from source to destination by using dummy nodes or compromised nodes. It sends packets through its generated path so that, it can misuse the data, but it is difficult to detect this attack as the packets are receiving it at the destination [26] [27] [28] [29].

There are three types of wormhole attacks

- Open wormhole attack

Attacker gets inside the sender and receiver and, sends data through its new false path.

- Half Open wormhole attack

During the transmission of data, intruders transmit the data through a false path.

- Closed wormhole attack

It creates a false path in the hidden node without inserting into the sender and receiver node which is shown in figure 5.

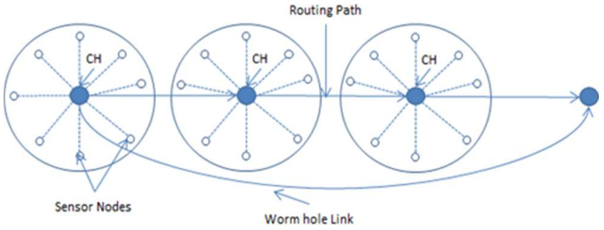

Figure 5 Routing path created by Wormhole attack

7.3.3 Black hole Attack

During transmission of data, sender node sends route REQest (RREQ) to its neighboring nodes including the malicious node to get the shortest path. After receiving RREQ request, harmful node sends Route Reply (RREP) message that the shortest path is available through it. The sender then transmits the data to the malicious node and it drops the packets. Figure 6 shows working of black hole attack [30] [31].

Attacks of this nature are extremely challenging as the sender gets the acknowledgement from the malicious node and the data is received successfully.

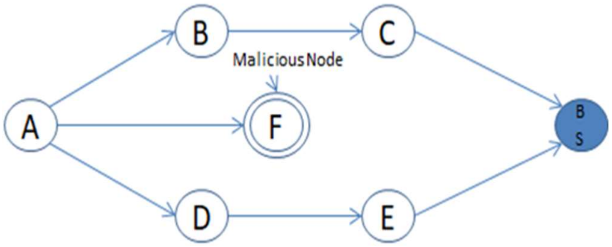

Figure 6 Black hole attack

7.3.4 Gray hole Attack

Gray hole attack is similar to black hole attack which shows that through this node, the shortest path is available. When a black hole attack is launched, all packets from the sender are destroyed once received but, in gray hole attack, malicious node drop some packets and, rest of the packets are forwarded to the receiver. The dropping of packets may be time driven. It means only for a specific time it drops the packet and the rest of the time it forwards the packets as shown in figure 7. In some cases, for certain specific nodes, it drops some of the packets and the others, it forwards to the receiver. So, it is difficult to detect [30].

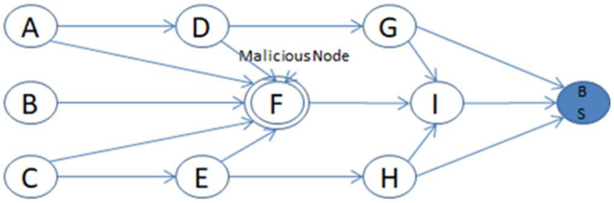

Figure 7 Gray hole attack

7.3.5 Sinkhole Attack

It also works like black hole and gray hole attack, but attacker chooses its location near to the BS or, the sink node. When the node of BS sends RREQ request signal to the neighboring nodes, the malicious nodes send RREP signal that the shortest path to reach the BS is through it. So, it sends data to the malicious node. Hence, the maximum data which was expected to reach to the BS is got by the malicious node [31]. The sinkhole attack is shown in figure 8.

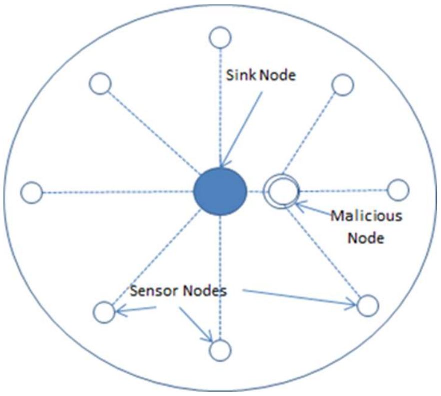

Figure 8 Sinkhole attack

7.3.6 Byzantine Attack

In the network, an intermediate single compromised node or a set of compromised nodes transmits packets through a non-optimized path or creates routing loops. It also drops selectively packets selectively to degrade the performance of the system. This activity is referred to as the byzantine attack [14] [21]. This is the Byzantine attack.

7.3.7 Sybil Attack

In this attack, the compromised node or the malicious node generates multiple nodes, identities and, behaves like it is similar to all the nodes. It creates redundancy in the routing protocol. So, ultimately it affects the routing mechanism and the data security of the network. Cybil node communicates with the neighbor node with, its original ID or, another ID's so, it confuses to the network and the network collapses [26] [32] which is shown in figure 9.

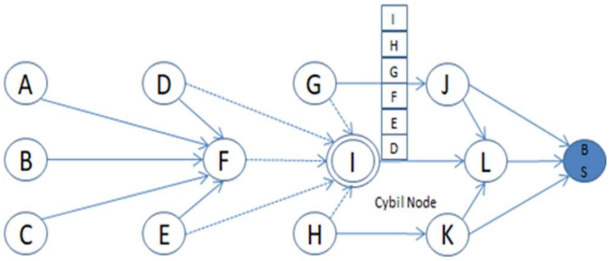

Figure 9 Cybil Attack (Cybil Node H shows identities of Node D,E,F,G,H,I)

7.3.8 ID address Spoofing Attack

This type of attack comes under the Denial of Service (DoS) attack. Generally, in the message, the senders and the receiver's addresses are is written. The malicious node sends the packet to the receiver with another node's address as a sender. It hides its identity to misbehave in the network. Even though at the receiver side, it identifies that it is a false packet that is received, the remedial action, will be taken on the node whose address is stored in the packet, and its legal incoming packets may get rejected. The malicious node sends the random address of the legal nodes which are available in the network [21].

Sometimes, the malicious node sends a request to send me huge data. So, according to the request the receiver sends data to the node whose spoofed address is written in the packet. The node receives unnecessary data which was not requested, becomes busy to process it and ultimately drain its energy. The ID address spoofing is shown in figure 10.

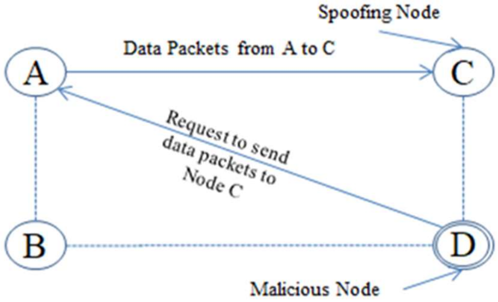

Figure 10 ID Address Spoofing (Malicious node D sends request to send data to Node A, Node D writes destination address as Node C, Node A sends data to spoofed Node C)

7.3.9 Replayed routing information Attack

The intruder steals the data from an authentic node and forwards the same message or a modified message after some duration to the destination. If it is not the current data then it is not useful for processing. This is called the replay attack [16].

Objective of replay attack is to drain the energy of other nodes and disturb the processing at the receiver end. Replay attack can be avoided by using strong digital signatures.

7.3.10 Eavesdropping Attack

It is the prerequisite for other types of attacks. Eavesdropping is the activity that is listening to the transmission of the message carried out to steal the data. Following are the two types of eavesdropping [21] [30].

- Passive eavesdropping
- Active eavesdropping

In passive eavesdropping, the intruder gets the data from the message transmission in the network and, in active eavesdropping through the malicious node the data will be grabbed by sending the request messages to the friendly nodes.

It listens to the network communication and extracts the security keys, node identification number, routing updates, receiver's identification number, etc. to use for further malfunctions.

7.4 Data link Layer

Data link layer observes the data frame detection, medium access, multiple access streams and, error control. It also observes the reliability of point-to-point and point-to-multipoint connections [17] [26] [27].

The possible data link layer attacks are; collisions, resource exhaustion and unfairness.

7.4.1 Collusions

When two nodes simultaneously send their packets to the receiver, collusion of packets results into a change in their checksum mismatch. Such mismatched checksum packets are discarded. Discarded packets need to retransmit [33] [34].

To overcome discarding error, correction codes work good, but again it requires processing power and energy. An efficient technique needs to be developed for collisions.

7.4.2 Resource Exhaustion

The attacker purposefully sends multiple data packets to the receiver and multiple collisions occur. So, the resources are utilized unnecessarily and cause the drain of energy and processing power [14] [16].

To solve this issue some researchers have suggested the Time Division Multiplexing Access (TDMA) technique.

7.4.3 Unfairness

It can be considered as a weak DoS attack, to cause unfairness, the attacker can make collisions of the data packets. It keeps the MAC protocol busy so that it can miss the deadline to provide service to others. The attacker can capture the communication channel by reducing the amount of time. Unfair attack reduces the efficiency [16].

7.5 Physical layer

Role of this layer is modulation, transmission, reception, frequency selection, carrier frequency generation, signal detection and, data encryption. As WSN communication is broadcasted by nature and the Radio channel it may easily face jamming attack [17]

The possible attacks of physical layer are physical attack, jamming attack and, tampering attack.

7.5.1 Physical attack

The WSNs are deployed in remote location in some applications. It is very difficult to protect it from the attackers, animals or environmental factors like flood, temperature, storm, rain etc. Physical attack damages the sensor nodes externally. Sometimes nodes become isolated and are not be able to communicate with the network. While deploying the nodes, care should be taken to protect the network from such physical attacks [16] [35].

7.5.2 Jamming attack

Jamming attack interferes with the existing radio frequency used by the network. Some jamming sources are less powerful, which affect a small part of the network. And some are more powerful and capable to disturb the complete network by adding random noise and pulses. Jamming affects the communication of the network and the message also gets corrupted or lost [21].

7.5.3 Tampering attack

The attacker replaces the working node with the malicious node and extracts the sensitive information like cryptographic keys, nodes identity, routing information and other security majors applied in the network that can be used to hijack the complete network. Physical access of the intruder should be avoided in the network field [14] [16].

7.5.4 Multi-layer attacks

There are some attacks which can affect the multiple layers which are DoS, replay, Cybil and, Eavesdropping.

8. Open security challenges

A great deal of study has been done on the security of WSN but, as it is an emerging technology and, the scope of the applications is increasing, more security challenges need to be faced. Some of them are listed below.

8.1 Privacy

The WSN systems are now days used in IoT and other applications as support systems, hence privacy of profiling and tracking location is essential. It is also required to maintain the privacy for the data transmission. WSN systems are prone to attacks of monitoring and eavesdropping, traffic analysis and camouflages adversaries. Hence providing privacy mechanism is still an open challenge for research to the researcher.

8.2 Authenticity

There are two entities where authentication is required.

8.2.1 Data Authentication

The intruders can change the data packets while routing of packets to BS. Hence the receiver needs to verify whether it is original packet or it is modified by the malicious node.

8.2.2 Sender Authentication

At the receiving end, sender's identity needs to be verified to decide whether the data is sent by the authorized node or the malicious node.

Hence the proper authentication technique needs to develop to identify the intruders.

8.3 Secure Routing

Receiving and forwarding the data packets is one of the major task in the WSN systems. If the data is routing through any false node, it may get modified. So, it is essential to discover a secure path and identify the false nodes. Considering the limitations of the WSN, effective and fine -grained solutions over routing activities are expected.

8.4 Prevention of Attack

There should be a mechanism which checks the security measures periodically before the attack happens. It should find and track the malicious activities in the network.

8.5 DoS (Denial of Service) Attack Detection

In the existing literature, there are many solutions suggested for the DoS attack. But still some lightweight techniques are required to find the origin of the attack and disinfect the network automatically.

8.6 Cryptographic Primitive attacks

Poor implementation of the security measures leads the system to be more vulnerable to cryptographic primitives such as, pseudorandom number attack, digital signature attack and, key management vulnerability that affect the system. Authentication technique and key exchange technique used in the system are majorly targeted by malicious behavior too.

Hence the cryptographic primitives are more challenging and need to be more focused.

8.7 Key Management

Symmetric key and asymmetric key systems both are well elaborated in the literature. Both have their pros and cons. But asymmetric key systems are more suitable for the WSN systems in terms of management & security keys. Hence, more optimal and lightweight techniques need to develop so that it can be more suitable for the WSN systems and consume less energy.

8.8 Trust Model for security

To build the trust model between different entities of the WSN is a great challenge for the researchers. It will definitely reduce the communication overhead between the different entities of the WSN system. Due to the reduction of the overhead communication the network efficiency will improve.

8.9 Secure data aggregation

The location of data aggregation depends upon the architecture of the WSN system. The collected data from the cluster nodes are aggregated at the cluster head. Generally, at the moment of aggregation, various nodes send their data packets. Sender may be a malicious node and it can also send false or modified data. So, the malicious nodes should be identified for aggregating false data.

8.10 Quality of service

The parameters of quality of service are unreliable communication links, failure of nodes, the delay in packet transmission, throughput of data transfer, communication and transmission errors, packet loss during transmission and, correctness of data received at the receiver. As the WSN has limitations such as; battery power, memory and computation power, the overall performance is affected and, it is difficult to achieve the quality of service. so there is a need to work on each of these parameters to improve the quality of service.

8.11 Fault tolerance

Generally, a fault occurs in the communication channel, sensing device, computation, data aggregation, transferring and receiving data packets, topology change, battery failures, draining of battery due to DoS attacks, false data transmission due to intruders, and software & hardware bugs. It is expected that the system works continuously even though any device or parameter fails. Faults can be detected by self-diagnosis techniques and the fault recovery can be processed by passive replication and service distribution. Some more novel techniques need to develop to achieve complete fault diagnosis and its recovery in the WSN system.

9. Conclusion

Now a days, WSN is the most demanding technology for real time applications as it is widely used in various applications, so its security has become a major concern. The major security issues are mainly focused and briefly discussed in the paper. The possible attacks on all layers of WSN and the existing solutions of researchers are explained in depth. Finally, the current open research challenges are highlighted which will prove helpful to the researchers to carry on their work and find a novel and generic solution to improve the security of the WSN.

References:

[1] Khalid M. A., Peer A. S. , Khalid I., Saira G., Waqas A., and Yunyoung N., “Review Article Underwater Wireless Sensor Networks: A Review of Recent Issues and Challenges”, Wireless Communications and Mobile Computing , Hindawi, pp. 1-20, 2019.

[2] Beom-Su Kim, Kyong Hoon Kim, Ki-Il Kim, “A Survey on Mobility Support in Wireless Body Area Networks” Sensor 2017, vol-17, pp. 1-18, 2017.

[3] Nighot M, Ghatol A, Thakare V, “Self-organized hybrid wireless sensor network for finding randomly moving target in unknown environment”, International Journal of Interactive Multimedia and Artificial Intelligence (IJIMAI), 05(01):16–28, 2018.

[4] S. Wagh and R. Prasad “Energy Optimization in Wireless Sensor Network trhough Natural Science Computing: A Survey”, Journal of Green Engineering, River Publication, Vol. 3 pg. no. 383-402, 2013.

[5] Nighot M, Ghatol A, “GPS Based Distributed Communication Protocol for Static Sensor Network (GDCP)”, Procedia Computer Science, Elsevier, 78, 530–536, 2016.

[6] S. Wagh, R. Prasad, “Maximizing lifetime of wireless sensor networks using genetic approach”, Advance Computing Conference (IACC), 2014 IEEE International, 2014

[7] Nighot M, Ghatol A, Thakare V, “Energy aware – Bio-inspired Hybrid WSN for Area Surveillance (E-BHAS)”, Indian Journal of Science and Technology, Vol. 11, pp. 17, 2018.

[8] Song, Y. , He, X. and Binsack, “Energy Aware Routing Protocol for Cognitive Radio Networks”, Wireless Sensor Network, Vol. 9,pp. 103-115, 2017.

[9] Hassan E., Khalid B., Mohammed O., “A Survey on Flat Routing Protocols in Wireless Sensor Networks”, Conference Proceedings of UNET’15, 2015

[10] M. Chu, H. Haussecker, and F. Zhao, “Scalable Information-Driven Sensor Querying and Routing for ad hoc Heterogeneous Sensor Networks", The International Journal of High Performance Computing Applications, Vol. 16, No. 3, August 2002.

[11] Bilal J., Haleem F., Huma J., Bartolomeo M, Murad K., Shaukat A. “Review Article Energy Efficient Hierarchical Clustering Approaches in Wireless Sensor Networks: A Survey”, Wireless Communications and Mobile Computing, pp. 1-14, 2017.

[12] D N. Sabor, S. Sasaki, M.Abo-Zahhad, and S.M.Ahmed, “Acomprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: review, taxonomy, and future directions,” Wireless Communications and Mobile Computing, vol. 2017, Article ID 2818542, 23 pages, 2017.

[13] [18]C.P. Gupta and Arun Kumar, “Wireless Sensor Networks: A Review”, International Journal of Sensors, Wireless Communications and Control, 3, 25-36, 2013.

[14] [16]S. Raja Rajeswari and V. Seenivasagam, “Review Article Comparative Study on Various Authentication Protocols in Wireless Sensor Networks”, Hindawi Publishing Corporation The Scientific World Journal, 16 pages, 2016.

[15] [28]Umer Farooq, “Wireless Sensor Network Challenges and Solutions”, https://www.researchgate.net/publication/331299729, 2019

[16] [31]A.K. Nuristani, Jawahar Thakur, “ Security Issues and Comparative Analysis of Security Protocols in Wireless Sensor Networks: A Review”, International Journal of Computer Sciences and Engineering, Vol.6, Issue.10, PP. 436-444, 2018.

[17] [37]Yong Wang, “A Survey of Security Issues In Wireless Sensor Networks”, CSE Journal Articles, pp.1-23, 2006.

[18] [38]TEODOR-GRIGORE LUPU, “Main Types of Attacks in Wireless Sensor Networks”, Recent Advances in Signals and Systems, pp. 180-185.

[19] [39] Muhammad Noman Riaz, Attaullah Buriro, Athar Mahboob, “Classification of Attacks on Wireless Sensor Networks: A Survey”, I.J. Wireless and Microwave Technologies, 2018, 6, pp.15-39 2018.

[20] [40]Parvathy. K, “Security Attacks on Network Layer in Wireless Sensor Networks-An Overview”, International Journal for Research in Applied Science & Engineering Technology, Volume 5 Issue,pp. 1038-1043, 2017

[21] [41]Pradip Jawandiya, “A Survey of Mobile Ad Hoc Network Attacks”, International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-4071, 2010.

[22] [42] [21]Sufian Hameed, Faraz Idris Khan and Bilal Hameed, “Review Article Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review”, Article ID 9629381, 14 pages, 2019.

[23] [44]Muawia A. Elsadig, Abdulrahman Altigani, Mohammed Abuelaila Ali Baraka, “Security Issues and Challenges on Wireless Sensor Networks”, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, No.4, 2019

[24] [45]Vikhyath K. B, Brahmanand S. H, “Wireless sensor networks security issues and challenges: A survey”, International Journal of Engineering & Technology, vol. 7, pp. 89-94, 2018.

[25] I. F. Akyildiz et al., “A Survey on Sensor Setworks,” IEEE Commun. Mag., vol. 40, no. 8, , pp. 102–114, 2008.

[26] Rasheed, “Security Schemes for Wireless Sensor Network with Mobile Sink” Ph.D Thesis, http://repository.tamu.edu/bitstream/handle/1969.1/ETD-TAMU-2010-05-7844/rasheed- dissertation.pdf? sequence=3.

[27] Y. C. Hu, A. Perrig, and D.B. Johnson, “Packet leashes: A defense against wormhole attacks in wireless networks”, in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM ’03), vol. 3, San Francisco, CA, Mar. 2003, pp. 1976-1986.

[28] Y.C. Hu, A. Perrig, and D.B.Johnson, “Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Network,” Proc. 22nd Annual Joint Conf. IEEE Computer and Communication Societies San Francisco, CA, April 2003.

[29] F. Nait-Abdesselam, B. Bensaou, and T. Taleb.“Detecting and Avoinding Wormhole Attack in Wireless Ad hoc Networks”, IEEE Communicat Magaz, Vol 46, no. 4, pp.127-33, Apr. 2003.

[30] Kahina Chelli, “Security Issues in Wireless Sensor Networks: Attacks and Countermeasures”, Proceedings of the World Congress on Engineering, London, U.K. (Vol. 1, pp. 1-3, 2015

[31] David Martins and Herve Guyennet, “Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey”, pp. 313-320, 2010

[32] J.R.Douceur, “The Sybil Attack,” in Proc. of 1st International Workshop on Peer-to-Peer Systems, Pages 251-260, March 2002, LNCS 2429.

[33] X. Sun, X.Wu, C. Huang, Z. Xu, and J. Zhong, “Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks,” Ad Hoc Networks, vol. 37, pp. 324–336, 2016.

[34] S. Murphy, “Routing Protocol Threat Analysis,” Internet Draft, draft-murphy-threat-00.txt, Octomber 2002.

[35] Murat Dener, “Security Analysis in Wireless Sensor Networks”, Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Vol.10, No.10, pp.303501, 2014.