THE ATTACKS ON SENSOR NETWORKS AND THE METHODS USED TO ATTACK THEM

#1REVELLI KISHOR KUMAR Assistant Professor,

Department of Computer Science and Engineering

#2BODA SWATHI, Assistant Professor,

Department of Computer Science and Engineering,

MOTHER THERESA COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TS.

ABSTRACT: Wireless sensor networks (WSNs) have many exploitable vulnerabilities. These issues stem from unsecure sensor nodes. This makes the network vulnerable to physical attacks. Malicious actors can easily send and receive data inside the network's communication range, which raises concerns about sensor node connection. This page discusses Wireless Sensor Networks (WSNs) security services, threats, and research-validated trust-based solutions. This research offers innovative attack prevention and reduction methods. We also present a new taxonomy of Wireless Sensor Network (WSN) attacks based on attack attributes. Finding similar assaults might help WSN security researchers.

***Keywords*:** Wireless sensor networks; WSN possible attacks; WSN attacks' detecting features; WSN securityservices;WSNtrustbasedsolutions;WSNattacksmitigationtechniques;WSNattackavoidancetechniques

1. INTRODUCTION

Wireless technology improves many ordinary tasks. Often, WSNs and other wireless networks manage sensitive and confidential data. WSNs are essential for smart city environmental monitoring. Network security and integrity require strong attack and intrusion defense. It's also difficult. Military wireless sensor networks (WSNs) monitor troop movements and enemy capabilities. Cameras are also employed to monitor low-level radiation sources, highway traffic, wildlife and birds, railroad bridge trains, fires, landslides, earthquakes, and agricultural practice improvement.

Hackers can spread false information, damage network nodes, cut network segments, and cripple the network. Many apps handle sensitive personal data, thus hacker security is crucial. Network security requires external access restriction and early node deactivation. Wireless networks have minimal power sources and limit long-distance communication between nodes, making asymmetric cryptography unsuitable for deployment. Innovative node isolation and identification methods are essential. These methods were classified as intrusion detection system misuse and others. Every attack could have a pre-detection signal. The detecting system seeks signature behaviors. studying non-traditional ways to find unauthorized access. These solutions assume the invader operates differently from other network nodes. Every node will monitor its neighbors for unusual activity.

2. WSN SECURITY SERVICES

Security measures must be taken to reduce assaults and incursions to allow data to transit securely between nodes. The OSI model and transmission requirements define the services. Secure data exchange routes incorporate many security measures:

- The authentication system offers two service tiers.
- For message verification, recipients favor network node verification over sender node verification.

- Receivers verify data transfer within a network node via data authentication.
- Access control prevents network node misuse.
- Data confidentiality limits unauthorized access to sent data, reducing data abuse and exploitation.
- Data integrity prevents unauthorized data packet alteration, making it crucial to information security.
- Limiting authorized parties' access to data packet sender and recipient information protects user data.
- Timely data ensures the base station receives new data and not duplicates.
- A node that acknowledges its activity can transmit and receive data packets without fraudulently claiming ownership under the non-repudiation principle.
- Data availability determines information availability.
- Self-organization separates vulnerable network nodes.
- Time synchronization synchronizes network time.
- Survivability is an entity or system's ability to resist and persist. This makes the network resistant to external security threats.
- Signals conveying network node position data are relayed precisely via secure localization.

3. WSN POSSIBLE ATTACKS

This section discusses Wireless Sensor Network (WSN) invasions.

Bad Mouthing Attack: Hackers lower benign node reputation scores using this method. In network analysis, lower-quality nodes (A) often criticize higher-quality nodes (B). Because other sensor nodes are having trouble sending data to node B, data may be missed. Because connected nodes can reciprocal network attacks, more nodes may be spared. This issue hinders network connectivity.

Good Mouthing attack: To trick base stations and cluster leaders, attackers modify troubled nodes' reputation rankings. This statement is not defamatory. Despite their unfavorable features, node A respects node B. In this attack, the network is offline.

Whitewashing Attack: A malicious node rejoins the network under a new name to mislead the system and change trust values. This attack begins when the system disconnects an unfriendly node.

Energy Drain Attack: A hostile node that re-enters the network disguises itself to change trust values. When the system loses its malicious node connection, the attack begins.

Exhaustion Attack: An attacker searches for superfluous data. Rogue nodes can communicate over long distances. Transmission of unwanted control or data is possible using this feature. This assault aims to crash the network quickly.

Homing Attack: Homing attacks detect base stations and cluster leaders using network data. An attacker can stop a network by targeting strategic points if they know how it functions.

Node Replication Attack: This approach replicates the node's ID. Malicious nodes steal data by stealing another node's identity. Current methods consider node identifier-based node position estimation incorrect. Figure 1 shows how the laws add two nodes with the same address to the network.

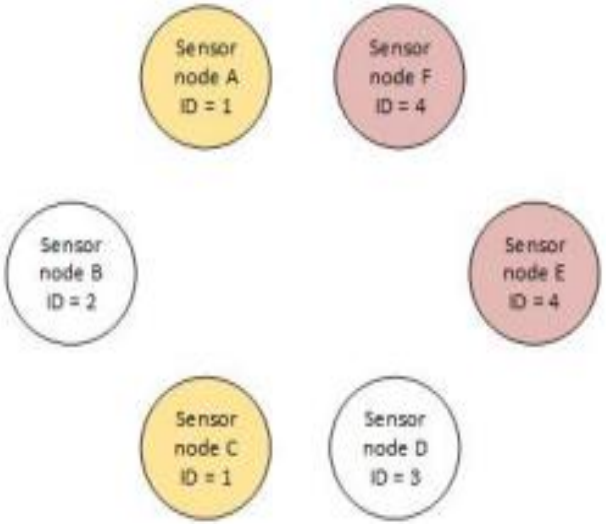


Figure1. This subject discusses Attack on Node Replication

Sybil Attack: This attack involves a hostile node employing multiple network IDs. Like the node duplication attack, this method precisely identifies the rogue node. Figure 2 demonstrates the probability of a Sybil attack in networks with malicious nodes A, B, and C. X, Y, and Z are conventional nodes with distinct IDs. This hinders data collection.

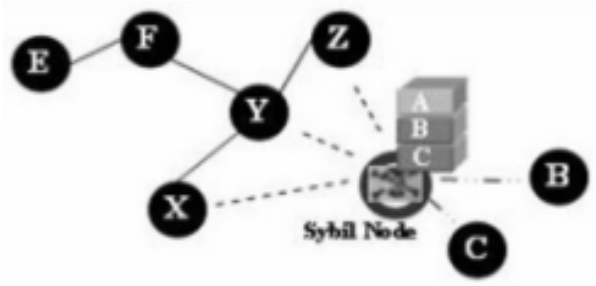


Figure2. A Sybil attack involves a malicious actor creating a fake user on a computer network.

Sinkhole Attack: Malicious nodes impersonate stations near the base station to monitor network activity and block transmissions. Figure 3 shows sinkhole attack consequences on network activity. Orange centralized node hinders most network communications to base station. This attack prevents base stations from sending packets. The intruder is active, energy-efficient, and computationally powerful. The subject's social personality comes from its many neighbors and contacts. Sinkhole creation and harm

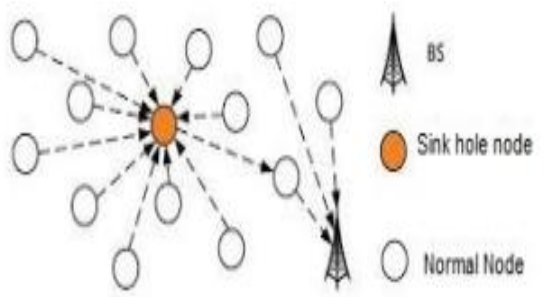
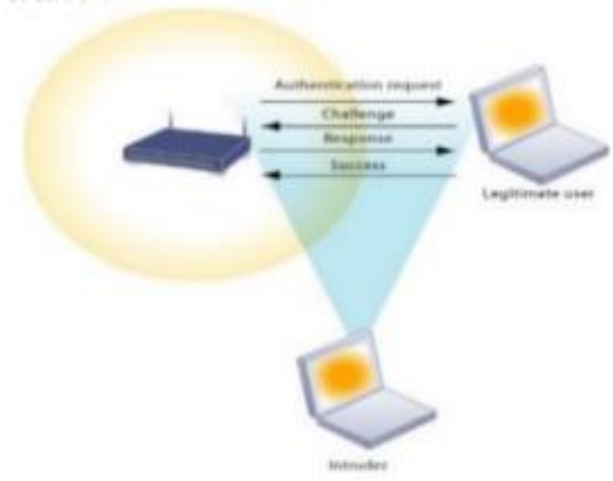


Figure3.Attacking sinkhole

Sniffing Attack: Snooper nodes steal confidential computer network data covertly. No delay or decrease in network efficacy occurs with a rogue node. Instead, the malicious node monitors messages and steals information. Military field service programs that process sensitive data may be attacked. Figure 4 shows that rogue sniffer nodes can communicate indefinitely. A visible communication channel between two nodes or a sensor node and the base station. Monitoring could be used for espionage



.

Figure4.assault for spying

Neglect and Greed Attack: Defective nodes deliver signals to the wrong node, causing multi-hopping. Malicious nodes communicate data quickly. Figure 5 indicates that Node (X) must send data to Node (D). Data arrives at Node D after passing through several intermediary nodes, diminishing node strength along the intended path and worsening network failure. Avarice and stupidity: ideas.

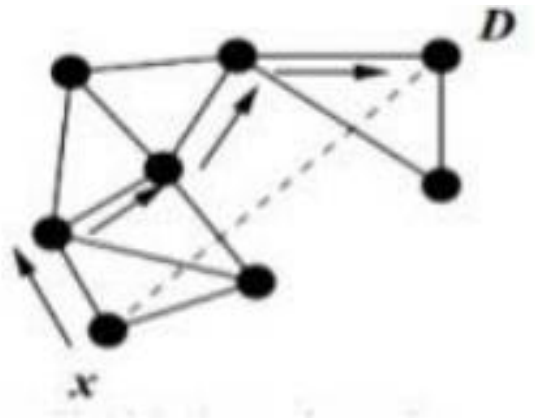


Figure5.Greed and Ignore

Grey-hole Attack: Gray hole sinkhole algorithms do not drop packets randomly. An opponent actively deletes or leaves communications. Discard the package instead. Figure 6 shows nodes 3 and 5 sending data to network nodes while ignoring packets for node 6. Without detection, these acts succeed. Increased fissure attacks were noticeable.

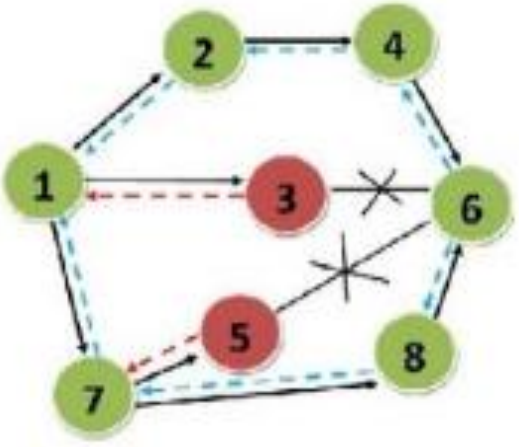


Figure6. During a grey-hole attack, a hostile actor may interrupt or modify network connections to disrupt communication.

Hello Flood Attack: The Energy Drain attack includes hostile nodes sending HELLO signals to neighbors. Figure 7 shows the hello deluge attack. Intrusion perpetrator has vast power but utilizes it rarely. Data is sent and received in large amounts. Many people live there and communication is widespread. This overloads the network with superfluous data packets and drains node energy.

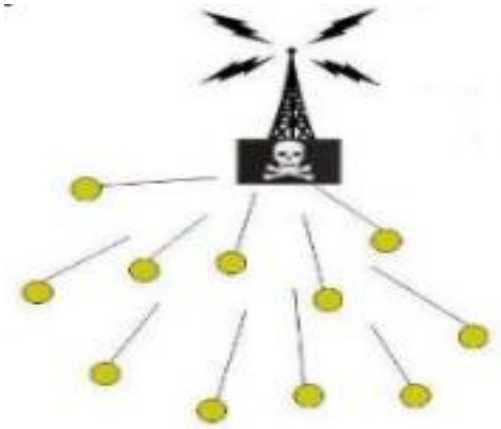


Figure7. I wish to discuss flood attacks.

Node outage: An attacker, possibly the cluster leader, disables and sleeps active nodes. Errant node controlled cluster for a long time. By switching cluster leaders, the assault can be averted. Malicious nodes' unlimited energy supply is used in the prior attack.

Garnished Attack: Garnished Attack shows the malicious node's cleverness and malice. Environmental factors and human traits affect malevolent node activity. Malicious (A) nodes reject incoming packets before and after a set time. However, these nodes send and receive packets regularly. Node B can adjust or transmit temperature, humidity, pressure, and luminance packets except pressure. to avoid detection.

Replay Attack: Replay attacks intentionally capture and retransmit data packets, unlike authorized detection, collection, and sharing. We wish to change base station query responses by lying. Figure 8 shows a hacker listening to the network, recording it, and sending data packets. Actual data makes intrusion detection harder.

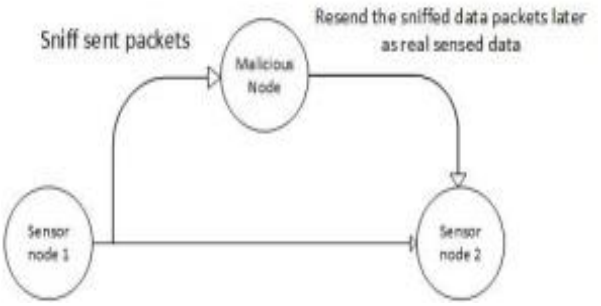


Figure8. The main topic is return to attack.

DoS Attack: DDoS assaults disable network devices and base stations. DoS attacks can occur at any network architectural layer, including medium access, application, and network. Malicious nodes use bandwidth, CPU, and other resources. Due to this vulnerability, the attacker's node may perform dual functions. Initially, the communication may overrun the sender's buffer and impede receiving. The second type includes malicious nodes that transmit many packets that need a lot of processing time and resources.

Stealthy Attack: During this attack, malicious actors inject bogus or nonexistent data into the network. This vulnerability initiates or delays network warnings.

Wormholes: In this type of hacking, two unauthorized nodes swiftly link network segments. Bad nodes build a network tunnel to improve performance and efficiency. Figure 9 demonstrates how the tunnel between malicious nodes S2 and S9 deviated from its planned course, which comprised S9, S8, S6, S5, and S2. Tunnels fool trustworthy nodes into thinking they got a data packet, while erroneous ones delete it. When the originator must lie, malicious nodes send bogus acknowledgment packets.

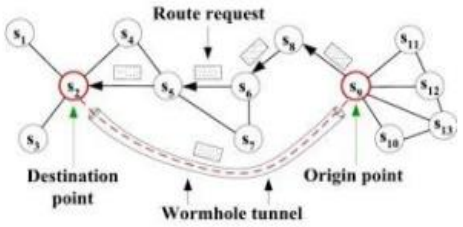


Figure9. Wormhole attacks are hostile acts in network communication systems with openings.

Jamming:

This assault targets the WSN physical layer to cause harm. Jamming affects the entire network, unlike DoS assaults, which target individual nodes. A hostile node sends massive packets to bring down the network. Network nodes must communicate to fix collisions, raising communication costs. This cost comes from trashing every sent packet and requesting each node deliver its contents again. Repeated actions reduce node collision resolution. Physical and medium access assaults lower service quality.

Acknowledgment Spoofing:

The user's work sounds academic. Spoofing creates an acknowledgment spoofer by synthesizing nearby packet acknowledgments without rewriting. As seen in Figure 10, malicious node (AD) acknowledges while node (E) delivers data to C. Transmission can cause data loss.

Unlike malicious node C, node AD confirmed receiving the data. This fooled the sender into thinking the data was received.

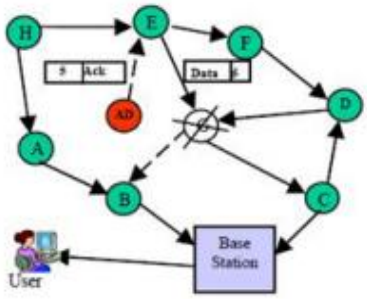


Figure10. Using recognition to attack. Most people call information manipulation spoofing.

Intelligent Attack: The attacker is smart enough to avoid harmful nodes. The perpetrator would follow the steps until the network's dependability became dangerous, then launch another attack. Due of its difficulty, this hit may take time to identify. Table1. Wireless Sensor Network attacks are shown in the first publication. It also has security issue detection and remediation tools.

Attack	Detecting Features	Attack	Detecting Features
Bad or Good Mouthing [24][21] Whitewashing [16][19]	1. Nodes' historical trust value 2. Nodes' current trust value 3. Path trust value	*DoS Attack [35][36] Node outage [23][24]*	1. Nodes' sleeping time 2. Cluster head lifetime 3. Power consumption rate 4. Remaining power
Energy Drain [22][23][42] Exhaustion Attack [24][25]	1. Power consumption rate 2. Remaining power 3. Uptime 4. Sent packets rate 5. Received packets rate 6. Power utilization threshold 7. Nodes' performance 8. Nodes' memory access rate	*Jamming[43]*	1. Collision ratio 2. Communication Range 3. Power consumption rate 4. Remaining power 5. Uptime 6. Sent packets rate 7. Received packets rate 8. Nodes' performance 9. Nodes' memory access rate
Homing Attack [25]	1. Number of initialization packets 2. Number of sent location packets 3. Communication Range 4. Power consumption rate 5. Remaining power 6. Power consumption rate	*Stealthy Attack[37]*	1. Nodes' reputation 2. Nodes' performance
Hello flood [34]	1. Communication Range 2. Power consumption rate 3. Remaining power 4. Power consumption rate 5. Number of sent initialization packets 6. Route Quality 7. Nodes' sent packets rate	*Acknowledgment Spoofing[41]*	1. Base stations' received packets 2. One node has huge connections number 3. Nodes' lost packets 4. Node's Link costs to the base station 5. Power consumption rate 6. Remaining power 7. Distance to the base station
Sinkhole Attack [30][31][32] Wormholes[38] [39][40]	1. Base stations' received packets 2. One node has huge connections number 3. Nodes' lost packets 4. Link costs to base station 5. Power consumption rate 6. Remaining power 7. Distance to the base station	*Intelligent Attack [18]*	1. Nodes' reputation 2. Communication Range 3. Power consumption rate 4. Remaining power 5. Base stations' received packets 6. One node has huge connections number 7. Nodes' sent\lost packets
Suffing[20]	1. Nodes' high receive traffic 2. Nodes' low transmit traffic	*Garnished Attack [16]*	1. Nodes' reputation
Neglect and Greed [20]	1. One node has huge connections number 2. Nodes' sent\lost packets 3. Nodes' high receive traffic 4. Nodes 'low transmit traffic	*Replay Attack[16]*	1. Nodes' reputation 2. Communication Range 3. Power consumption rate 4. Remaining power
Grey-hole Attack [32][33]	1. Nodes' reputation 2. Freshness of the route 3. Base stations' received packets 4. One node has huge connections number 5. Nodes' sent\lost packets	*Node Replication [38][20] Sybil Attack [27][28]*	1. Number of lost network packets 2. Number of newly added nodes 3. Nodes in two different locations claim the same ID

4. WSN ATTACKS DETECTION FEATURES

Read on for attack detection features. Attack detection involves locating and identifying attacks. Table 2 shows these traits. Multiple attacks may share traits. The following section discusses these facets. The past and current trust value of a node's data, service, or communication channel affects its adjacent nodes' veracity. This function detects positive, negative, and whitewashing emotions.

The originator's path trust value indicates data transfer path confidence to the destination node. This feature shows sarcasm, flattery, apathy, and avarice. Sensor nodes remain overpowered. This function may be hampered by fatigue and energy depletion. Time a node operates without slumber cycles. Formula for

calculating availability:

$$uptime = \sum(Wakeup_{tttme} - Sleep_{tttme}) \quad (1)$$

Active nodes with unlimited energy can be found via power consumption rate analysis. Equation (2) calculates characteristic.

$$consum_{rate} = (100 - Remaing \quad PoPPer)/uptime \quad (2)$$

Power consumption, remaining power, and up time can indicate exhaustion, homing, sinkhole, hello flood, node outage, replay, DoS, wormhole, jamming, acknowledgment spoofing, and creative attacks. Nodes with high network traffic send and receive packets faster. High-traffic nodes speed packet reception and transmission. Hostile nodes smell, jam, inundate, fatigue, and deplete energy. Computations can estimate packet delivery and reception rates.

$$sent_{rate} = sent_{packets}/tRRme \quad (3)$$

$$received_{rate} = receRRved_{packets}/tRRme \quad (4)$$

These metrics evaluate data, initialization, control, and localization packets.

The statistic shows how many data packets the base station received during acknowledgment spoofing, fatigue, sinkhole, grey-hole, and wormhole assaults. The absence of this characteristic indicates a major network issue such isolation, data transmission failure, or sensor node power concerns.

This attribute tracks node beginning packet transmission. Homecoming or flood attacks are possible with this node's high score.

The Number of sent location packets, which measures the number of packets identifying a place, is included in sent and received packet rates. This system detects hostile nodes trying to find sensor nodes during homing assaults.

ID nodes can compromise network security through Sybil attacks and replication. One node might have two IDs or two can share one. Duplicate concatenated identities are found in clustered network node identification numbers and cluster leader responses. When two system nodes share an identity, they have redundant concatenated identifiers. Ask the node's position and ID. This displays if two unique nodes in different locations have the same ID or two different IDs.

Network nodes have been added. The indicator increases significantly at deployment or when most nodes fail and must be replaced. If the network starts with a large increase in location packets but no new nodes, a malicious node may be present. The missing packet phenomena is tied to node data loss anxiety. A high metric indicates a rogue node causes packet loss or collisions. Detect sinkhole attacks, worm holes, and acknowledgment manipulation. Formula for calculating this characteristic:

$$lost_{packets} = lost_{data}/tRRme \quad (5)$$

Formula 6 calculates the data packet loss percentage for a node, or the ratio of sent to lost packets.

$$data\_lost_{rattto} = sent_{data}/lost_{data} \quad (6)$$

This attribute can identify complex attacks, avarice, carelessness, and susceptibility in grey areas. CPU utilization indicates a node's processing power and efficiency. By assigning themselves recursive work, malicious nodes can spread computer resources. Over time, unnecessary processing drains sensor nodes.

Memory access speed also affects sensor node performance. High CPU and memory usage may indicate fatigue. The most socially interactive network node is identified by this attribute. Nodes with low power usage, high residual power, and extensive communication range are highly vulnerable to hostility. Multiple connections indicate social sensor nodes. Spoofing, sinkhole, neglect and avarice, grey-hole, wormhole, and intelligent attacks can be detected by this function.

Base station link cost depends on node power, route count, and trust. Sinkhole, wormhole, and greyhole assaults intercept and manipulate data transmissions before deletion or change, making them the most cost-effective base station approach. Low-cost advertising helps malicious nodes expand their social media following and reach more people.

Measurements of base station distance help detect sinkhole, wormhole, and gray hole attacks. The amount of steps and base station distance

determine the connection fee.

Route freshness is the percentage of freshly added nodes along a base station path. Sensor nodes should avoid the newly established path due to malicious or untrustworthy nodes. This method finds greyhole and whitewashing assaults.

Malicious nodes fight for resources. Measure the number of retransmissions during a specific time period to evaluate this statistic. The interference attack must be detected using this skill.

To save energy, malicious nodes can put another node to sleep. This statistic alerts users if a node's sleep duration exceeds a threshold. The system detects node failures and DoS attacks.

Even with some cancerous lymph nodes, cluster heads should be rotated. This method has been used to supervise cluster heads for a long time since they can constitute a threat to the cluster or trash data packets.

This document highlights the major aspects of assault detection systems and the potential attack scenarios for each component to facilitate comprehension and analysis.

Feature	Possible attacks to be detected	Feature	Possible attacks to be detected
Node's current/historical trust value	• Bad mouthing, • Good mouthing, • Whitewashing	*Node's sent/lost packets ratio*	• Neglect and Greed, • Grey-hole Attack, • Selective forwarding, • Intelligent Attack
Path trust value	• Bad mouthing, • Good mouthing	*Route Freshness*	• Grey-hole Attack
Uptime (lifetime), Remaining power, Power consumption rate	• Energy Drain, • Exhaustion Attack, • Homing Attack, • Sinkhole Attack, • Hello flood, • Node outage, • Replay Attack, • DoS Attack, • Wormholes, • Jamming, • Acknowledgment Spoofing, • Intelligent Attack	*Nodes' performance Nodes' memory access rate, Power consumption rate*	• Energy Drain, • Exhaustion Attack, • Jamming
Uptime (lifetime) Sent and Received packets rate	• Energy Drain, • Exhaustion Attack, • Hello flood, • Jamming	*Communication Range*	• Homing Attack, • Hello flood, • Replay Attack, • Jamming, • Intelligent Attack
Base stations' received packets	• Sinkhole Attack, • Grey-hole Attack, • Selective forwarding, • Wormholes, • Acknowledgment Spoofing, • Intelligent Attack	*Number of connections*	• Sinkhole Attack, • Neglect and Greed, • Grey-hole Attack, • Selective forwarding, • Wormholes, • Acknowledgment Spoofing, • Intelligent Attack
Number of sent initialization packets	• Homing Attack, • Hello flood	*Link costs to the Base station, Distance to the base station*	• Sinkhole Attack, • Wormholes, • Acknowledgment Spoofing
Number of sent location packets	• Homing Attack	*Collision ratio*	• Jamming
Nodes in two different locations claim the same ID, Number of newly added nodes to the network	• Node Replication, • Sybil Attack	*Nodes' sleeping time, Cluster head lifetime*	• Node outage, • DoS Attack
Nodes' lost packets	• Sinkhole Attack, • Wormholes, • Acknowledgment Spoofing		

Table2. Several traits distinguish attacks.

5. ATTACKS AVOID ANCE TECHNIQUES

Attacks can be actively prevented by networks, not merely mitigated. Avoiding preserves network resources from harmful nodes. Many researchers have developed cutting-edge network attack prevention technologies. Network collisions are reduced via the CSMA/CA protocol's link layer. Avoiding collisions decreases fatigue, congestion, and DDoS attacks.

Deng et al. suggested CSMA/CA adaptive detection and a dynamic threshold. Felix suggested hacking the remote control network, monitoring network data, and shutting it down to defend against DDoS attacks in another study. This method disconnects harmful nodes from the

perpetrator.

The Delphi method by Kumar et al. monitors and reroutes problematic nodes to change routing patterns. No clock synchronization, position data, or hardware is needed for this route-finding method. No one can identify the perpetrator.

Freiling et al. suggested adding a maximum transmission distance property to packets to verify that the destination address is within the authorized range from the source node. Kaushal et al. suggested network node time synchronization. Determine when the delivery will reach the target node. Senders may be adversaries if recipients observe a significant transmission timing variation from the anticipated time.

Another approach to avoid wormholes is network node distance.The researchers measured round-trip signal duration and speed to calculate node distance. The most reliable and efficient path will be communicated to all network components.

Singh's three-level hierarchical aggregation approach for wormhole defense is shown in Figure 15. Each hierarchical network node has a unique address.

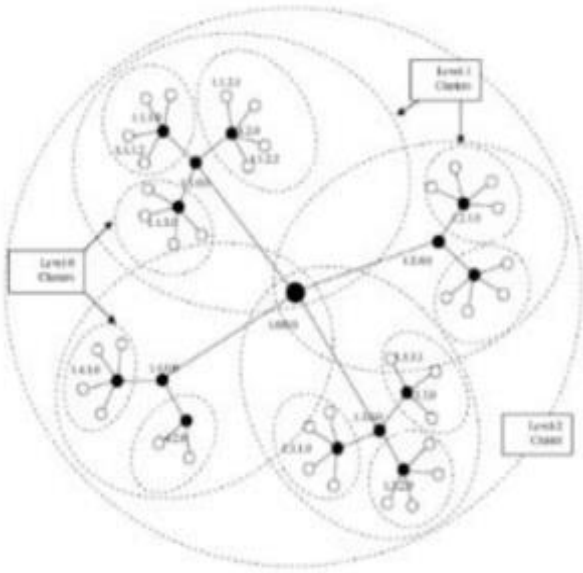


Figure11. Triple-level grouping divides items, concepts, and data into three tiers. That

A predetermined address schema helps a network node find the best way to another node. Thus, nodes indicate improper packet routes from source to destination. This method does not require hardware or network node clock synchronization. Node statistics are unnecessary.

6. OPEN RESEARCH ISSUES

Many security weaknesses exist despite WSN attack prevention measures. This session will examine several development issues. Minimal memory, processing, and energy are available to sensor nodes. The cost of cryptography makes Wireless Sensor Network (WSN) algorithms complex, especially for private key operations.

WSN security is compromised by sensor mobility. WSNs can incorporate mobile sensors and sink nodes. Only stationary WSNs are used in the current routing strategy. Mobile wireless sensor network (WSN) security initiatives are rare since they target specific dangers or general ad hoc networks with unique features.

Many academic and commercial contexts use hundreds to thousands of Wireless Sensor Network (WSN) nodes. This behavior affects big node scalability and requires a security protocol.

Security techniques like TESLA and its child do not require node or sink node synchronization, unlike protocols.

Most security solutions today detect isolated incidents, but wireless sensor networks (WSNs) employ audio and video data streams. When developing new Wireless Sensor Network security measures, the data stream must be examined. Quality of service and security are closely related. Effectiveness requires premium wireless sensor network (WSN) services. Wireless Sensor Networks' QoS is another security issue.

7. CONCLUSION

Due to their mission-critical applications, sensor networks require extensive security research. Reduced sensor network and node capacity makes assault prevention and response difficult. Current sensor network attacks are examined here. Additional material on new mitigating measures is evaluated. This study describes attack traits and elements, which is crucial. The concerns raised by this study will improve sensor network trust model research.

REFERENCES

1. Qabulio, M. (2016). A Framework for Securing Mobile Wireless Sensor Networks against Physical Attacks. In 2016InternationalConferenceonEmergingTechnologies (ICET).
2. Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS : Security Protocols for SensorNetworks. Wireless Networks,8(5),521–534.
3. Hu,Y.,Perrig,A.,&Johnson,D.B.(2006).WormholeAttacksinWirelessNetworks.IEEEJournalonSelectedAreasin Communications ,24(2),1–11.
4. Schaller, P., Lafourcade, P., Basin, D., Capkun, S., &Hubaux, J. (2008). . Security in Mobile Ad Hoc and SensorNetwok and Secure Neighborhood Discovery : A Fundamental Element for Mobile Ad Hoc Networking. Security inMobileAdHocandSensor Netwoks,(February), 132–139.
5. Ko, B. J., Lu, C., Srivastava, M. B., Stankovic, J. A., Ieee, F., Terzis, A., & Welsh, M. (2010). Wireless SensorNetworksforHealthcare. ProceedingsoftheIEEE,98(11).https://doi.org/10.1016/j.comnet.2010.05.003
6. NouhaSghaier, AbdelhamidMellouk, Brice Augustin, YacineAmirat, Jean Marty, Mohamed El Amine Khoussa,Amine Abid, and R. Z. (2011). Wireless Sensor Networks for medical care services. In 7TH International WirelessCommunicationsandMobileComputingConfrence(IWCMC).
7. Banerjee, S., &Majumder, K. (2014). Wormhole AttakMitigtion in MANET : A. International Journal of ComputerNetworks&Communications (IJCNC),6(1),45–60.
8. Barbagli, B., Bencini, L., Magrini, I., Manes, G., Marta, S., & Manes, A. (2011). A Real-Time Traffic MonitoringBased onWirelessSensor NetworkTechnologies.InProc.7th IWCMC (pp.820–825).