Security Analysis with respect to Wireless Sensor Network – Review
K. Sethu Selvam¹, Dr. S. P. Rajagopalan²
¹Research Scholar, Vels University,
Pallavaram, Chennai, India
sedu.devi@gmail.com
²Professor, G.K.M College of Engineering and Technology,
Perungalathur, Chennai, India

Abstract: Security or Privacy is the most important challenges in network. These challenges and issues are mostly affected in Wireless than Wired network because medium is open and less limited resources. Sensor is a tiny and low cost device. Wireless Sensor Network (WSN) is operated remotely and can be used in various fields like military surveillance, environmental monitoring, traffic monitoring, health monitoring and etc. In this paper, analysis of various security attacks and security techniques of WSN was done.


1. Introduction
Wireless sensor networks (WSN) are collection of nodes where each node has its own sensor, processor, transmitter and receiver. Sensor is a Tiny and low cost device that performs a specific type of sensing task. It deployed densely throughout the area to monitor specific event. It mostly operates in public and uncontrolled area.

Wireless Sensor Architecture: WSN contains the following network components [22]
- Field devices are used to route the packets. It controls process or process equipment.
- Gateway is used to communicate between Host application and field devices.
- Network manager is used to configure the entire network which includes scheduling communication between devices, management of the routing tables and monitoring and reporting the health of the network.
- Security manager is used to generate, store and management of keys.

Wireless Sensor Characteristics
- Ability to work in harsh environment.
- Manage when node is failure
- Heterogeneity of nodes
- Ease of use
- Cross-layer design
- Low cost
- Power consumption constraints using batteries.

WSN Application: Some of the applications harshly used in WSN are as follows [22]
- Nuclear reactor control
- Traffic monitoring
- Fire detection
- Contaminant Transport.
- Environmental/Habitat monitoring.
- Acoustic detection.
- Military surveillance
- Medical monitoring.

Security Limitation in WSN [22]
- a. Wireless Medium
- b. Limited Storage space and Memory
- c. Power Limitation
- d. Exposure to physical attack
- e. Managed Remotely
- f. No Central Management point

Security Goals

Data Integrity: The message has not been altered during transmission.

Data Freshness: The message is recent, and it make sure that no old messages have been replayed.

Data Availability: checks whether a node has able to use resources/to communicate with network or not.

Data Confidentiality: ensures that receiver only can understand the message not by attacker.

Self Organization: It specifies that every node be independent and flexible enough to be self-organizing and self-healing according to different situations.
**Authentication**: make sure that communication between nodes is trusted.

![Image of Security Goals in WSN](image)

**II. SECURITY ATTACKS IN WSN**

Security attacks are categorized in two types. These are [5]

- **Passive Attack**
  An adversary is monitoring and listening of the communication channel. This attack is also known as Attacks against Privacy.

- **Active Attack**
  During data transmission, Intruders senses packet and modify message is known as active attacks. The attacks may be given as below:

  1. **Routing attacks**: The attacks which acts on the network layer are called routing attacks. The following are the attacks that happen while routing the messages[22]
     - **Spoofed, Altered, or Replayed Routing Information**: In order to disturb traffic, an attacker may spoof, alter or replay routing information in the network.
     - **Selective Forwarding**: A node should forward only certain messages and simply drop others.

- **Monitor and Eavesdropping**: An unauthorized person can easily find out information while transmissions.

- **Traffic Analysis**: while transmission information is in encrypted means it may be damaged.

- **Camouflage Adversaries**: A node which is inserted by Intruder acts as normal node in the network to attract the packets.

**2. Denial of service attacks**: Sudden failure of the nodes in the sensor networks.

**3. Node Subversion**: An attacker node can capture normal node and it may disclose its important security information and affects the entire security mechanism of the WSN.

**4. Node Outage**: When node stopped function, WSN protocols must be to manage this node outage problem by using some other route

**5. Physical Attacks**: WSN works in an open or harsh environment, it is risk of physical attack.

**6. Node Replication Attacks**: An attacker inserts malicious node in the sensor network by copying the node-id of a normal sensor node.

**7. Passive Information Gathering**: An attacker can easily gather information which not encrypted during data transmission.

**8. False Node**: An attacker inserts malicious node in the network then it sends malicious data in the network.

- **Sybil Attacks**: The fault tolerant schemes like multipath routing, topology maintenance and distributed storage are affected in this attack.

- **Wormholes Attacks**: An attacker collect packet of information at one particular place in the network, transfers them to some other location, and then resend them into the network.

- **HELLO flood attacks**: A malicious node sends or re-plays HELLO packets from one node to another with more power.

- **Sinkhole Attack**: When the whole traffic is attracted at a specific node then it is called as sinkhole attack.

- **Black-hole Attack**: When path finding process, malicious node suggests the incorrect paths as good paths to the destination node.

- **Acknowledgement Spoofing**: An attacker can spoof the acknowledgements of overheard packets destined for particular nodes for providing false information to the neighboring nodes[5].

- **Misdirection**: A malicious node sends the packets in wrong direction where the destination is unreachable.

- **Internet Smurf Attack**: The attacker may fake the network and the address of victim and broadcasts multiple messages in the network to flood a victim with hundreds of responses for every request.

- **Homing**: An attacker targets cluster head nodes and key manager nodes to accomplish DoS by destroying these keys.
1. Physical Layer: This defines on the transmission media between sending and receiving nodes, the data rate, signal strength, frequency types are also addressed in this layer [5].

1.1 Jamming: This disrupts the accessibility of transmission media.

1.2 Tampering: The simplest way to attack is to damage or modify sensors physically and stop their services. The attack is also to capture sensors and extract sensitive information from them.

2. Data Link Layer: This layer is responsible for the data frame detection, medium access and multiplexing of data and includes collisions, exhaustion and unfairness attacks [5].

2.1 Collisions: An attacker may cause collision of packets transmitted on the same frequency and the packets will then be discarded[5].

2.2 Exhaustion: Repeated collision of attacks can cause resource exhaustion which will deplete the energy of surrounding nodes and transmitting nodes[5].

2.3 Unfairness: This is considered as the weak form of a DoS attack. Repeated application of these exhaustion or collision based MAC layer attacks can lead into unfairness[5].

3. Network and Routing Layer: The attacks occurred in the network layer they are referred as routing attacks. There are various attacks occurred at the network layer - Spoofed, altered and replayed routing information, Sinkhole attack, Black-hole attack, Wormholes etc. All these attacks are explained above under routing attacks [5].

5. Transport Layer: This layer is used for external networks and to manage the end to end connections. It includes two attacks flooding and desynchronization [5].

1. Flooding: An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach the maximum limit[5].

2. Desynchronization: An attacker may repeatedly spoof messages to an end host, causing disruption of an existing connection and missed frames[5].

6. Application Layer: This layer is responsible of data collection, management and processing of the data by using the application software to obtain trustworthy consequences[5].

1. Overwhelm attack: This attack consumes network bandwidth and drains node energy by overwhelming the nodes causing the network to forward large traffic to the base station[5].

2. Path-Based DoS attack: This attack can starve the network of legitimate traffic, because it consumes resources on the path to the base station, thus preventing other nodes from sending data to the base station[5].

3. Deluge (Reprogram) attack: If the reprogramming process isn’t secure, an intruder can hijack this process and take control of large portions of a network[5].

III. Related Work:
Various security methods are applied in WSN. In this paper, we classified widely used security techniques. They may be

1. Cryptographic Algorithm
   a. Key Management
   b. Authentication
   c. Key Agreement and Authentication

2. Non–Cryptographic Algorithm
   a. Signal Strength Based
   b. Genetic Algorithm
   c. Firefly Algorithm
   d. Evolution game theory
   e. Stochastic Geometric

Woo Kwon Koo et al.[30] implemented cryptographic algorithm name as HIGHT which recommended for TinySec. This algorithm provided better security solution than Skipjack and RC5.

Virendra Pal Singh et al. [29] implemented Signal strength based system which to detect and prevent Hello Flood attack. Based on signal strength, this method detect whether a node is friend node or stranger.
A.M.Riad et al. [21] implemented Artificial Intelligence (AI) based routing protocol. It reduced communication overhead by removing data redundancy from the network. Energy consumption is achieved by this method.

Sung Jin Choi et al.[27] proposed an Energy-Efficient Key Predistribution Scheme using Eigenvector. Values are used in this vector as Generated pool of random key.

Zhiling Tang et al. [36] proposed technique as Epidemic model based security analysis of Firefly clock Synchronization. It is implemented in MAC layer.

Mohamed Elhoseny et al. [15] proposed technique which is combination of Genetic Algorithm and new cryptography scheme based on Elliptic Curve Cryptography(ECC). In this method, first phase is related to constructing the network structure that minimizes energy exhaustion using GASONEC algorithm. Then the proposed encryption scheme is applied to guarantee secure data routing from sensor nodes to the BS. It prevented passive attack and improved network performance of time.

Udaya Suriya Raj Kumar Dhamodharan et al. [28] proposed technique compare match position (CAM) verification method based on message authentication passing (MAP). CAM-PVM algorithm is used to check the node information from base station iNodeInfo table during data transmission. After verification of node details ID, timestamp and current location of node compared with initial information when the node are registered. The result of this algorithm can provide only trusted nodes in the route to ensure secured data transmission. It is used to prevent Sybil attack.

M. Rajalakshmi et al. [19] implemented Energy Efficient Cryptographic (EECA) algorithm. It provided data confidentiality, authenticity and data integrity. It reduced processing time and memory capacity than RSA, AES and DES.

Mohammad Mozumdar et al.[17] proposed Security proposed technique is Zero Knowledge Protocol (ZKP). It is an authentication technique which provided high security solution with minimal usage of resources and high throughput.

Ayaz Hassan Moona et al.[3] implemented a technique which is based Elliptical Curve Digital Signature Algorithm (ECDS). It is mutual authentication technique with the help of computationally low signature scheme.

Kashif Saleem et al. [12] implemented technique as Enhanced biology-inspired self-organized secure autonomous routing protocol (E-BIOSARP). It is based on Artificial Immune system which is used to gain knowledge for neighboring node It This method is used to countermeasures against selective forwarding, spoofing, eavesdropping, replaying or altering of routing information, Hello flood attack and Sybil.

YoHan Park et al. [33] implemented technique as Bio-metric based user authentication and key agreement. It is based on ECC. It provided better functionalities of mobile services in WSN.

Shital Patil [25], author implemented a security method which is based on Bio-metric and private key. In this method, Smart phone is used to capture biometric input data (finger print).

Lavinia Mihaela Dinca et al. [14] proposed implications of spoofing biometric data for retrieving the derived key. They demonstrated that spoofed biometrics could yield the same key, which in turn will lead an attacker to obtain the private key. Smart phone is used to capture biometric input data. Fingerprint and iris is used in biometrics and the fuzzy extractor for biometric key extraction. This method defined a biometric PKI scenario and an in depth security analysis for it.

Alireza Ahadipour et al.[2] implemented a Location-based Probabilistic Key Pre-distribution Scheme (LKPK). In this method, nodes are represented same region and used graph coloring technique to efficiently assign the random keys. This method is better performance than existing random key pre-distribution schemes.
### Table 1: Comparative table for various Security Technique applied by various authors

<table>
<thead>
<tr>
<th>No</th>
<th>Title</th>
<th>Year</th>
<th>Author</th>
<th>Method</th>
<th>Advantage</th>
</tr>
</thead>
</table>
  • Better security solution than previous method skipjack and RC5 algorithm |
| 2  | Hello Flood Attack and its Countermeasures in Wireless Sensor Networks [29] | 2010 | Virendra Pal Singh et al.     | Signal Strength based                       | • Based on signal strength, it is considered node as a friend or a stranger. |
  • Enhanced energy consumption. |
| 4  | Secure Routing in Wireless sensor network: A state of the Art [21]   | 2013 | A.M.Riad et al.               | AI based routing protocol                   | • Reduced communication overhead by removing data redundancy from the network |
| 5  | An Energy-Efficient Key Predistribution Scheme for Secure Wireless Sensor Networks Using Eigenvector [27] | 2013 | Sung Jin Choi et al.          | Key predistribution scheme                  | • It is a scheme based on Eigenvector which having matrix includes eigenvalues in generating a pool of random key. |
| 6  | A Provably-Secure ECC-Based Authentication Scheme for Wireless Sensor Networks [10] | 2014 | Junghyun Nam et al.           | Smart card based user authentication        | • Based on elliptic curve cryptography (ECC)  
  • Achieves both authentication key exchange and user anonymity. |
  • Efficient because of less computation and communication cost. |
  • Perfect forward secrecy  
  • Key agreement between user and sensor |
<p>| 9  | An Efficient Identity-Based Key Management Scheme                   | 2014 | Zhongyuan Qin et al.          | Identity-Based Key Management (IBKM)        | • Using Bloom filter to authenticate the |</p>
<table>
<thead>
<tr>
<th>No.</th>
<th>Title</th>
<th>Year</th>
<th>Authors</th>
<th>Method/Algorithm</th>
<th>Features</th>
</tr>
</thead>
</table>
• Better WSN lifetime longer than pair-wise key establishment                                                                   |
• The scheme has lowered the power consumption at least 40% without sacrifice in safety and efficiency.                        |
| 12  | Epidemic model based security analysis of Firefly clock Synchronization in Wireless Sensor Networks [36] | 2015 | Zhiling Tang et al.             | Firefly Algorithm                                       | • It is implemented in the MAC layer of WSNs  
• Safe because the number of nodes which are out of synchronization decrease with time.                                           |
| 13  | A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic Encryption [15] | 2015 | Mohamed Elhoseny et al.         | GASONeC                                               | • It is based on Elliptic Curve Cryptography(ECC) algorithm  
• It prevents passive attack, CH compromised attack, and brute force attack.  
• Improved network performance.                                                                                                      |
• It is used to prevent Sybil attack.                                                                                                  |
<p>| 17  | Advanced Cryptographic Algorithm to Secure the Sensor Node Data in WSN                          | 2016 | Rajalakshmi et al.              | Energy Efficient Cryptographic (EECA) algorithm         | • It provided confidentiality, authenticity                                                                                           |</p>
<table>
<thead>
<tr>
<th>Article Number</th>
<th>Title</th>
<th>Year</th>
<th>Authors</th>
<th>Method/Protocol/Approach</th>
<th>Contribution</th>
</tr>
</thead>
</table>
- Increasing no. of sinks improves both average secrecy rate between access point and associated sink                                                                                                                                                                                                                               |
- High packet delivery ratio and low delay.                                                                                                                                                                                                                                                                                                 |
- High security to the network with minimal overhead, minimal energy consumption, and good throughput.                                                                                                                                                                                                                                      |
| 21            | A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities [9] | 2016 | Jun Wu et al. | User Control (UCON) Technology                                                        | - It is framework proposed in which Low - level attack detection with simple rule and high-level attack detection with complex rules is performed in sinks and at the base station  
- Better resource consumption and attack detection rate.                                                                                                                                                                                                                                                                                   |
- It improves the network performance                                                                                                                                                                                                                                                                                                      |
| 23            | A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks [4] | 2016 | Danyang Qin et al. | Light Authentication and Key Management Scheme (AKMS)                                 | - Provide more efficient security with less energy consumption, control overhead, and packet loss rate than other typical schemes  
- Provide message confidentiality and authenticity                                                                                                                                                                                                                                                                                        |
- Low-cost functions  
- One-way hash function                                                                                                                                                                                                                                                                                                          |
<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Year</th>
<th>Authors</th>
<th>Reference</th>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>An Anonymous User Authentication and Key Agreement Scheme Based on a Symmetric Cryptosystem in Wireless Sensor Networks [7]</td>
<td>2016</td>
<td>Jaewook Jung et al.</td>
<td></td>
<td>• Improves the level of security, and is also more efficient relative to other related scheme</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Achieves both stronger security and higher efficiency</td>
</tr>
<tr>
<td>27</td>
<td>A Novel Secure IoT-Based Smart Home Automation System Using aWireless Sensor Network [23]</td>
<td>2016</td>
<td>Sandeep Pirbhulal et al.</td>
<td></td>
<td>• Efficient key generation procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Integrates low power Wi-Fi</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Better performance than AES and DES</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Is countermeasures against selective forwarding, spoofing, eavesdropping, replaying or altering of routing information, Hello flood attack and Sybil.</td>
</tr>
<tr>
<td>29</td>
<td>Three-Factor User Authentication and Key Agreement Using Elliptic Curve Cryptosystem in Wireless Sensor Networks [33]</td>
<td>2016</td>
<td>YoHan Park et al.</td>
<td></td>
<td>• Better security functionalities for mobile services in WSN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• It is based on ECC</td>
</tr>
<tr>
<td>30</td>
<td>Location Privacy Based Security Enhancement In Wireless Sensor Network Using LFPM And PPM [24]</td>
<td>2016</td>
<td>S. Saravanan et al.</td>
<td></td>
<td>• To trace back in to the source node location, then the source node used to another path or another server for data request and data response in the network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Better network performance</td>
</tr>
<tr>
<td>31</td>
<td>Early Detection of DDoS Attack in WSN [11]</td>
<td>2016</td>
<td>Kanchan Kaushal et al.</td>
<td></td>
<td>• Detect the attack on early stages so that data loss can be prevented and more energy can be reserved</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Based on Round Trip Time (RTT)</td>
</tr>
<tr>
<td>33</td>
<td>DoS attack prevention</td>
<td>2016</td>
<td>Shital Patil</td>
<td></td>
<td>• To prevent DoS attacks</td>
</tr>
<tr>
<td>Page</td>
<td>Technique</td>
<td>Authors</td>
<td>Year</td>
<td>Details</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>---------</td>
<td>------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| 34   | User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks [14] | Lavinia Mihaela et al. | 2017 | • Reduces the false alarm rate
| 35   | LPKP: Location-based Probabilistic Key Predistribution Scheme for Large-Scale WSN Using Graph Coloring [2] | Alireza Ahadipour et al. | 2017 | • This model is based on Bio-metric and private key.
• Smart phone is used to capture biometric input data (Finger Print)
• It can randomly pre-distribute keys based on the location of the nodes
Table 2: Comparative various Security Technique with Resource Constraints

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Energy Consumption</th>
<th>Memory</th>
<th>Computation</th>
<th>Processing Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>EECA</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GASONeC</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDSA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>AKMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIGHT</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Signal Strength Based</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Light Weight Kerberos &amp; ECMQV</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>User Authentication</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAM-PVM</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>ZKP</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

IV. Conclusion

In this paper, analysis of various active and passive security attacks was done. This survey is useful for the future researchers to come up with light smarter security mechanism with less energy consumption, less memory and less computation and make safe network for wireless sensor.

References:


DOI: 10.18535/ijecs/v6i4.46


[37]. Zhongyuan Qin, Xinshuai Zhang, Kerong Feng, Qunfang Zhang and Jie Huang, An Efficient Identity-Based Key Management Scheme for Wireless Sensor Networks Using the Bloom Filter, Sensors 2014, 14, 17937-17951; doi:10.3390/s141017937.