A Survey - Security Challenges and Schemes on Wireless Sensor Network

Princy S†1, P.K. Sasikumar*2
†1ME-Computer Science and Engineering
Tamilnadu College Of Engineering, Coimbatore, India

*2Assistant Professor
Tamilnadu College Of Engineering, Coimbatore, India

Abstract—Wireless sensor network (WSN) is one of the emerging technologies to attract the researchers with its research challenges and can be applied on various domains. Now a day WSN applications are used on environmental detection, monitoring system, medical system, military and industrial is monitoring for transforming human life to different aspects. Depending on the applications used on the WSN, Security is one of the greatest challenges in WSNs and it is the essential part before designing the WSNs. In this paper a survey is taken related to the security on the wireless sensor network (WSN).

Keywords—WSN, security, challenges, survey

I. INTRODUCTION

Wireless sensor networks grow as one of the popular and widely used, but security becomes a greater serious concern. Users do not want for revealing the data by the unauthorized people as it disclosed information for the malicious purposes. These concerns are most relevant to the wireless environment in which anyone can overhead the message sent. Therefore for the convenient system may appeal to the users if it is not secure. To address these conflicts, researches in WSN have been implemented serval Security protocols needs to be used on the sensor network. Examples of such protocols are TinySec [1] and TinyECC [2].

In general security is considered to be more expensive. Its cost more in WSNs because of the limited resources in the sensor nodes. Thus in need to provide a sufficient level to security. Meanwhile it should be properly utilizing by the available resources. For Example [3] if a sensor device hasn’t avail with the enough memory to run the particular algorithm that requires on the lessor memory but that may also be less secure. There are more way to secure in WSNs than by using just an encryption algorithms. Modes of operation introduced to ensure the encrypting plaintext with the same key multiple times and could deliver the different cipher text.

Message Authentication Code (MAC) algorithm is used for providing guarantee to the authentication and integrity of data. We conform that all three- encryption algorithm, operation modes and MAC algorithms are mainly takes part on the security in WSNs as shown in fig 1. In survey papers [5], [6], the symmetric key and hash based algorithm techniques are processed on WSNs. In these algorithms, every symmetric authentication key are to be share by the cluster on the sensor nodes. An intruder comprises the key with the capture on the single sensor node. Therefore these techniques are not adapted to the node compromise attacks. A secret polynomial depends message authentication techniques were discussed on [7]. This method presents the information on the theoretic security with the ideas on the threshold secret sharing, in which the threshold is calculated by the degree in the polynomial. While the number of messages transformed as the lower threshold the techniques applies the intermediate nodes to authenticity the message through the polynomial evaluation. Wherever the number of messages transmitted is larger than the threshold, the polynomial must fully improve and thereby the system will completely damage. To boost up the threshold and the complexity among the intruder for reconstruction the secret polynomial, a random noise which is also called as perturbation factor, was developed to the polynomial in [8] from counting the coefficient of the polynomial.

Hence the added perturbation factor can entirely erased by using error correcting code schemes [13]. By using the public key based ap techniques, messages are transmitted through the sender private key together with the digital signature of the message given. The upgraded development on elliptic curve cryptography (ECC) depends on the term public key schemes which are more benefit on the memory usage; message complexity and security because public key based techniques have a simple and neat key management.

II. LITERATURE REVIEW

Wireless sensor network leads on the traditional networks in many ways like as large scale, autonomous nature and intense deployment [1] [14]. It also improves the fault tolerance since a sensor node fails others can gather the
data. Hence it develops more attractive on the particular application likewise syndrome surveillance, military, environmental observation, fire detection, supply chain management, energy automation, vision enabling, gaming, building administration, health and other commercial and home applications [15-28].

Thereby the extensive deployments of WSN used on the multi-faceted applications security are developing concern. For example on a battle ground, a military communication network applied to susceptible information exchange may be hacked on adversaries because of the WSN’s security hole leads to stern loss of the life and machineries. Thus security of WSN is the greatest task because of its limited resources likewise power supplies, energy, computation, small memory and communication capability [29][30][31][14][33]. Cryptographic algorithm plays a major role in the security and resource conservation of the wireless sensor network (WSN) [33] [34].

OVERVIEW ON WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSN) is an interconnection to the large number of nodes that are deployed to monitor the system which means the measurement to its parameters. Recent research on wireless sensor networks that led for various new protocols that based particularly on the designed sensor networks. To design these networks, the factor needs to be considered under the coverage area, mobility, power consumption, communication capabilities etc. Wireless Sensor Architecture is shown and described below in the fig 2.

**A. Characteristics of a WSN include:**
- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures
- Mobility of nodes
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Cross-layer design

**B. Summary of various Security Schemes for Wireless Sensor Networks**

<table>
<thead>
<tr>
<th>Security Schemes</th>
<th>Attacks</th>
<th>Deterred Network Architecture</th>
<th>Major Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAM [38]</td>
<td>DoS Attack (Jamming)</td>
<td>Traditional wireless sensor network</td>
<td>Avoidance of jammed region by using coalesced neighbor nodes</td>
</tr>
<tr>
<td>Wormhole based [39]</td>
<td>DoS Attack (Jamming)</td>
<td>Hybrid (mainly wireless partly wired) sensor network</td>
<td>Uses wormholes to avoid jamming</td>
</tr>
<tr>
<td>Statistical En-Route Filtering [33]</td>
<td>Information Spoofing</td>
<td>Large number of sensors, highly dense wireless sensor network</td>
<td>Detects and drops false reports during forwarding process</td>
</tr>
<tr>
<td>Bidirectional Verification, Multi-path multi-base station routing [40]</td>
<td>Hello Flood Attack</td>
<td>Traditional wireless sensor network</td>
<td>Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing</td>
</tr>
<tr>
<td>On Communication Security [32]</td>
<td>Information or Data Spoofing</td>
<td>Traditional wireless sensor network</td>
<td>Efficient resource management, Protects the network even if part of the network is compromised</td>
</tr>
<tr>
<td>TIK [27]</td>
<td>Wormhole Attack, Information or Data Spoofing</td>
<td>Traditional wireless sensor network</td>
<td>Based on symmetric cryptography, Requires accurate time synchronization between all communicating parties, implements temporal leashes</td>
</tr>
<tr>
<td>Random Key Predistribution [29], [30],[41]</td>
<td>Data and information spoofing, Attacks in information in Transit</td>
<td>Traditional wireless sensor network</td>
<td>Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes</td>
</tr>
</tbody>
</table>

![Fig-2. Wireless sensor network architecture](image)
III. CONCLUSION

This paper discusses the security challenges and schemes in Wireless Sensor Network (WSN). Many among the attackers are against the security in Wireless sensor networks which are caused due to the insertion of fake information on the compromised nodes within the network. According to the false information on the compromised node, a mean is needs for detecting false reports. Thus the security schemes would help us for secure transmit of data among the sensor nodes.

REFERENCES


