International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Study on Vulnerabilities, Attack and Security Controls on Wireless Sensor Networks

Dr. C. Umarani[1], R P Shruti[2]

[1]Assistance Professor, [2]Student,
[1,2]Masters in Computer Applications, Jain (Deemed-to-be) University, Bangalore, Karnataka, India

ABSTRACT

In this fast evolving world of technology where security plays a major role, the threats to security is also increasing rapidly. The world aims to go wireless in all the fields, and the wireless sensor networks is also one such major field. The sensors which can sense its environment based on the functions allocated. It retrieves the data of its surrounding and sends it to the authorized location for further analysis. But as technology grows, the attacks on the system also increases due to the vulnerabilities in the system. Hence security plays a major role in the evolution of technology. This paper mainly concentrates on the vulnerabilities, the attacks possible due to vulnerabilities in the system and the counter measures to be taken to overcome the vulnerabilities.

KEYWORDS: *WSN, Wireless sensor networks, keying, SPINS protocol, Tiny-Sec protocol, LEAP protocol*

How to cite this paper: Dr. C. Umarani | R P Shruti "Study on Vulnerabilities, Attack and Security Controls on Wireless Sensor Networks" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.1681-1683, URL: www.ijtsrd.com/papers/ijtsrd35738.pdf

IJTSRD35738

I. INTRODUCTION

Basically, a wireless sensor network is the one which senses its environment and stores the collected information and send sit to the central location where the information is further processed. For instance, a sensor is placed in the tsunami prone area, then based on the data which is sent, they detect the changes in the environment and take actions. The data which is stored need to be observed at all times. Many attacks can be possible on the wireless sensor networks due to the vulnerabilities. Based on the type of attack, the mitigation techniques are suggested in the form of papers and projects. Therefore, this paper mainly concentrates on the vulnerabilities, attacks and security measures on WSN.

A sensor is a device which measures or detects its environment and indicates, records or responds according to the task given to it. Whereas, a wireless sensor network is a combination or collection of many nodes placed in a particular physical location for recording and monitoring. It further sends the collected data to the far away central location for observation and processing.

II. Objectives

This paper mainly concentrates on,

- The vulnerabilities in the wireless sensor networks.
- The attacks possible due to the vulnerabilities in the system.
- Some of the security controls suggested and published for wireless sensor networks.

III. Vulnerabilities and attacks in the wireless sensor networks

As we know, all kind of networks are vulnerable to many kind of attacks, may it be wired or wireless. WSN's are more vulnerable as they are prone to different kind of attacks as they are the wireless medium and also some of the nodes have resource constraints with respect to computation. They have limited battery power, so the energy consumption and the memory is very less.

The data in WSN can be altered or dropped maliciously. The nodes can be compromised or it may also malfunction. So, some of the effective measures must be taken to overcome these challenges.

There are 3 keying schemes available in WSN are,

- Network keying: It uses only one key for the whole network. It does not consume too much resources. So there is no need of key management techniques. But it is not so robust.
- Pair-wise keying: One key is used for every pair of sensor nodes. Therefore, for instance, if the number of nodes are N, then the required number of keys are N-1. It is robust.
- Group keying: It is hybrid, i.e., the combination of both network keying and pair-wise keying mechanisms. A single key is used for network communication and different keys are used between every pair of sensor nodes. This is also robust.

The wireless sensor networks have resource constraints, they are small sized, and they have limited processing power and limited bandwidth. Because of these limitations in WSN, they cannot be used directly in traditional cryptographic algorithms.

Limitations in WSN

- Unpredictable communication: It uses connectionless communication. Due to which it suffers from reflection, scattering and fading. By this, it produces very high bit errors and produces huge amount of data loss.
- Delay in communication: Due to the presence of some intermediate nodes between the nodes, packet transmission between the nodes can be delayed.
- Remote sites and unattended setup of WSN's: Most of the time, the nodes are employed in remote locations. Therefore, they are more prone to attacks. Even these kind of attacks are difficult to predict and detect.

IV. Security requirements in WSN

- **Data integrity**: This is about the trustworthy of data i.e. the data should not be modified or changed during transmission. The data obtained by the sensor nodes and which is in transit over the network should not be modified by any third party. Malicious nodes may modify the data. So, the tampered data should be transmitted to actual source. And the data should be verified from time to time.
- **Data confidentiality:** Only the authorized user should get access to the data. The key distribution should be secured enough for the data to remain between the intended users. This means, a secure channel must be generated. And without the permission of the intended users, the data should not be read or accessed by nearby users.
- **Self-organization**: Wireless sensor network is a kind of ad-hoc network. In WSN each sensor node is flexible and self-organizing. Hence, applying the traditional cryptographic algorithm like RSA is difficult. And as the sensor nodes behave dynamically, sharing key between nodes is difficult before deployment if the symmetric key is used. Here, the topologies (physical and logical topologies) may also change in the self- organizing network.
- **Data newness**: The data should be sent only once. That means the old data which is already sent, should not be sent again and again. If so replay attack can be possible. To ensure the freshness of data, a time stamp or a time specific counter can be added. If the shared key is used, it is mandatory to update data overtime.
- **Data authentication**: The data inflow must be from an authenticated source. Authenticating the source is very much important. We should make sure that no third party is acting like an authenticated user. It can be done through MAC (Message Authentication Code).
- **Time synchronization**: Since WSN uses distributed environment, the different entities or nodes participating must be time synchronized.
- **Secure localization**: It is all about understanding the location of various sensor nodes. In sensor network, the data which is sent to the central location is geo-tagged. I.e., the geographical location of node is also embedded with that data. If the node is not secured properly, attacker can deliver false location and also reply to the messages.
- **Data availability**: This makes sure that no authorized user is prevented from using services privileged to him. WSN should always be available to the legitimate users. To ensure that the data is accessible to the legitimate user, one common technique to be used is to use extra nodes for communication.
- **Denial-of-sleep attack**: It is a kind of denial-of-service attack where, lot of unwanted or garbage packets will be sent to the network. So, the nodes will always be kept busy and active. Therefore they will not go to the sleep state and consume all the resources. So it is a type of attack.

V. Security protocols for WSN

There are many security measures proposed for wireless sensor networks. Some of the mare,

- SPINS protocol.
- Tiny Sec protocol.
- LEAP protocol (Localized Encryption and Authentication Protocol).

SPINS Protocol: Sensor Protocol for Information via Negotiation is a group of security protocols which will take care of issues related to confidentiality and integrity. SPINS protocol basically has two blocks, one is SNEP which fulfils the requirement of confidentiality, integrity, privacy and newness and is employed as peer connection between the nodes. The other is microtesla which offers authentication and produces key for MAC authentication scheme. It uses the mechanism of broadcasting.

Tiny Sec: It is a lightweight data link layer security protocol. It offers privacy, Authentication and newness to the nodes. There are two types of approach, one is authentication approach and the other is authentication and encryption approach.

LEAP protocol: It is abbreviated as Localized Encryption and Authentication Protocol. It is a key management protocol. Instead of using only one key, it generates four type of keys.

- A collection of keys: This key is shared to all the members of WSN.
- Arrangement in clusters: Set of nodes arranged in the form of clusters.
- Arrangement in peers: A key is shared between the nodes of each peer.
- Single key: Only one single key is shared with the base station.

VI. Conclusion

Wireless sensor network is a major topic of interest for research. Each of the development in the technology may lead to much vulnerability. Hence, the security should also be implemented strongly when it comes to the wireless networks. The sensor networks helps monitoring day to day activities. If the security can be implemented strongly in these nodes using the protocols, the sesensors nodes can be implemented effectively. So, we should work more on implementing security more efficiently.

References:

[1] https://books.google.co.in/books?hl=en&lr=&id=4zyDBwAAQBAJ&oi=fnd&pg=PA21&dq=Wireless+sensor+networks&ots=6jtCbzfC4C&sig=byC54m6jnBRW8shk-

37pApnQwdA&redir_esc=y#v=onepage&q=Wireless%20sensor%20networks&f=false

[2] https://www.sciencedirect.com/science/article/abs/pii/S1389128601003024

[3] https://dl.acm.org/doi/abs/10.1145/570738.570751

[4] http://webstaff.itn.liu.se/~jinzh29/TNE090/LectureNote4in1/TNE090_Letcure_1_4in1.pdf

[5] https://www.sciencedirect.com/science/article/abs/pii/S1570870503000088

[6] https://dl.acm.org/doi/fullHtml/10.1145/990680.990707

[7] https://www.researchgate.net/profile/D_Sridharan/publication/266591710_Security_Vulnerabilities_In_Wireless_Sensor_Networks_A_Survey/links/544629e30cf2f14fb80f26ce/Security-Vulnerabilities-In-Wireless-Sensor-Networks-A-Survey.pdf

[8] https://ieeexplore.ieee.org/abstract/document/5636116

[9] https://www.researchgate.net/profile/Robert_Rittenhouse/publication/261324361_Sinkhole_Vulnerabilities_in_Wireless_Sensor_Networks/links/0deec533e47c7ac7c2000000.pdf