Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) - May 2016
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Security Problems and Defies in Wireless Network

J.Usha[#1], S.Lakshmi Devi[#2]
[1]*Master of Computer Applications, S.A. Engineering college, Chennai-77.*
Ushajayaraman954@gmail.com
[2]*Asst Prof., Department of Computer Applications, S.A. Engineering College, Chennai-77.*

Abstract— The threats and attacks beside security in wireless sensor networks are almost similar to their wired computers corresponding part while some are improved with the inclusion of wireless connectivity. The concept of this paper is to consider the security related issues and challenges in wireless network. Now project an adaptive routing protocol is an advanced and scanned which minimizes the drive cost per bit of information by using the channel material to choose the best approach to route information. In this approach, the source join will switch between direct and imparted message based on the value of the link and will use the relay only if the control quality is underneath a certain inception.

Keywords— Security; Challenges; WSN

1. Introduction

Security aspect of multi-hop wireless networks such as WSNs are fast securities of examiners as there are still numerous unclear issues which needed to be addresses earlier large scale improvement take place. The same time, we cannot manage the security individual of WSNs as medical monitoring, industrial automation and military applications highlight the must to address the security sensor networks. Data integrity is typically helpless on the primary routing protocols. The use of wireless knowledge is fast suitable the most in style way to associate to a network. Passive attacks are very challenging to detect as they are still in nature and do not harm the network [1].

A classification is necessary to understand the issues in each condition. The essential design of sensor network is to divide miniature intelligences policies; which are accomplished of perceiving some alters of issues and interactive with other apparatus, over a precise geographic region for a few precise reason different aim patching, assessment, ecological observing etc. Security in wireless networks is still a employed development, segment 6 chats one of the latest proposals to develop current safety criteria, a protocol called PANA (Protocol for carrying Authentication for Network Access).

Wireless networks contain of a number of nodes which connect with each other over a wireless frequency which have different types of networks: antenna network, ad hoc mobile network, cellular networks and dependency networks. Wireless sensor network contain of small nodes with detecting, addition and wireless communications capabilities. Data integrity confirms that the packets are traditional by the receiver in the same organization and arrangement as sent by the sender; at this point the purpose is to keep the attackers away from packets changes, revision, distraction and interest.

1.1 Application Of Wireless Antenna Networks

Wireless sensor nodes are used in infinite range. Here we complete main area of the request of Wireless Sensor Networks.

A. The Military Application

The military application of sensor nodes includes battle ground following the monitoring, guiding systems of intelligent military hardware and finding of attack by ordnances of build destruction.

B. The Medical Application

Sensors can be particularly useful in easy going identification and monitoring. Patients can uniform small sensor devices that monitor their physiological data such as heart rate or family stress.

C. Industrial Applications

It includes business detecting and diagnostics. For example employments, industrial unit, stream cables etc.

1.2 Security Goals For Wireless Network

A. Availability

It ensures survivability even with Denial of Service (DOS) attacks. The physical and media access power layer attacker can use jamming methods to interfere with communication on physical network. On network layer the attacker can dislocate the routing protocol. [5]

B. Confidentiality

Ensures confident information is never disclosed to unauthorized entities. It is an decent duty, privacy is a right

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

rooted in common law. Accepting the difference between these two conditions can unused you a lot of confusion when signing contracts, establishing a client advocate relationship, and generally meaningful your rights in a given situation.

C. Integrity

Message being diffused is never corrupted. It refers to the overall wholeness, correctness and reliability of data [2]. Data integrity must be executed when sending data through a network. This can be completed by using error testing and correction protocols.

2. Existing System

Wireless Network requisite for cooperation and interactive using extra nodes and cooperation between nodes to relay material to the base is connected with the single-chip. The main impartial of this average is to make available connectivity between low-power wearable and implanted strategies while supportive high data rates (up to 10Mbps) as well as quality of service [1].
Disadvantage: It consumer more energy. Decrease the network lifetime.

3. Proposed System

Propose an adaptive routing protocol is established and planned which reduces the energy cost per bit of information by using the occurrence information to choose the best approach to route data[3]. In this methodology, a receiver achieves information on the network through a statement and selects whether to use an alternative relay frequency to produce redundancy.
Advantage: Reduce the energy consumption. Increase the network lifetime.

4. Methodology

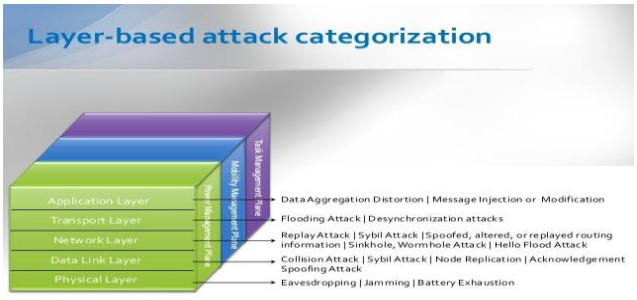

Fig.1: Layerd based attack categorization

This protocol stack combines control and routing alertness. There are five basic categorization. They are Physical, Data Link, Network, Transport and Application.

4.1 Attacks in wireless networks

Attacks compared to wireless networks could be normally considered from two different levels of views

A. Physical layer attack

Physical layer outbreaks to eavesdropping are secretly listening to the private discussion of others without their authorization, as *definite* by Black's Law Dictionary. Jamming is the process of presenting a strong source of noise authoritative enough to importantly decrease the signal to noise ratio (fig.2).

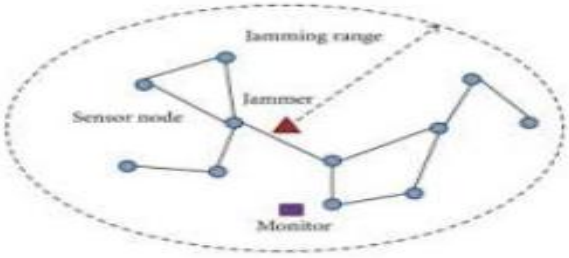

Fig.2: Jamming

B. Data Link Layer Attack: Sybil Attack

In many cases, the sensors in a wireless sensor network might need to work together to achieve a task, hence the use distribution of subtasks and redundancy of material (fig.3). This type of attack everywhere a node forges the identity of further than one node is the Sybil attack.

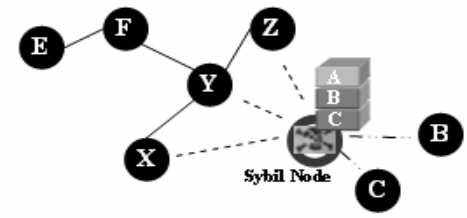

Fig.3: Syblic attack

C. Network Layer Attack: Black hole/Sinkhole Attack

The attack is a malicious node action as a black hole to attract all the traffic in the antenna network. Principally in a drowning based protocol, the attacker listens to requests for routes then responses to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious machine has been able to introduce itself between the connecting nodes (for example, sink and sensor node), it is able to do something with the packets fleeting connecting them (fig.4) shows the conceptual view of a black hole/sinkhole attack.

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

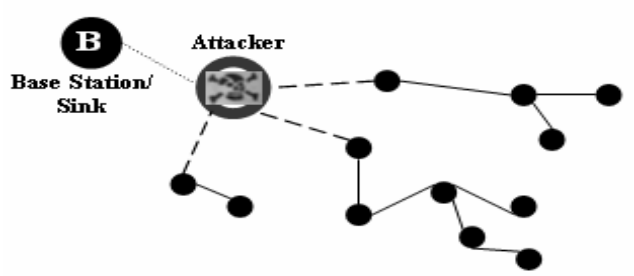

Fig.4: Conceptual view of black hole attack

D. Transport Layer Attack:Wormhole Attack

Wormhole attack is a serious attack in which the enemy records the packets (or bits) at one location in the network and tunnels persons to an additional position. The tunnelling or retransmitting of bits might be done selectively. Wormhole attack is a significant danger to wireless sensor networks.

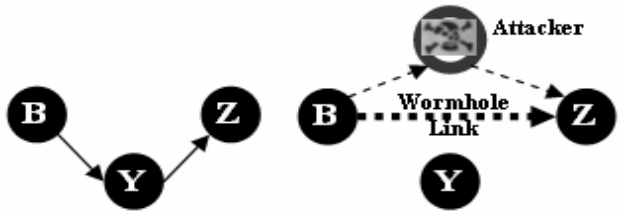

Fig.5: Wormhole attack

E. Application Layer Attack

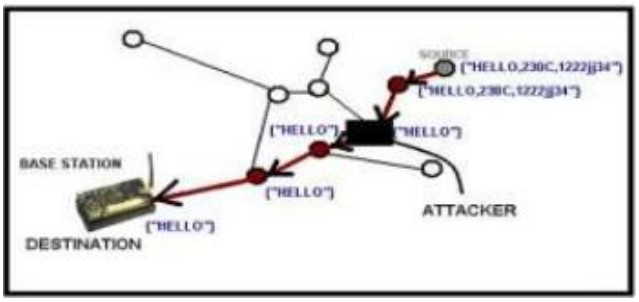

Fig.6: Application attacks

When routers or gateways act as partisans between client and base station, there is an increased possible of security vulnerabilities, as the routers that live between base station and client are presentable and disposed to attacks (fig 6).

4.2 WSN Security Challenges

Advanced anti jamming techniques are improbable due to its composite design and high energy ingestion. Most current ordinary security protocols do not scale to a big number of participants. Encryption involves extra processing, memory and battery power [4]. A Protected asymmetric key requirements in additional measurement, Even though sensors site information are indispensable most recent applications are apposite for motionless WSNs.

5. Result

Application Layer Security for fixed substructure networks comparable notions of wired network. Require Light-weight sand boxing mechanisms. Key management resolutions may not work due to real-time voice data.

- If key management is used dynamics and storing become issues
- Need a different way of control records.

6. Conclusion

Wireless Network requires high level of security due to its testing environment. This leads to intense security and persistence requirements in attacks of different types and incomplete resources of sensors and makes a huge security challenges in wireless networks. The challenges are resolved and many haven't determined yet or under reviewing is a real need for such security instruments which are projected and designed protection in view the limitations and challenges of wireless networks.

7. Future Enhancement

Future enhancement is a power effectual adaptive routing protocol for the performance of force competence procedure. It has been illustrates that in single-hop method, the lump with highest distance from the drop will be weak out energy faster, while in the multichip case the relay nodes earlier to the drop have much advanced energy ingesting due to the traffic they carry.

References

[1] Tahir Naeem, Kok-Keong Loo, "Common Security Issues and Challenges in Wireless Sensor network and IEEE 802.11", Wireless mash network, Vol.8, No. 7, July 2008, pp.1-6.
[2] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong , "Security in Wireless Sensor network: Issues and Challenges", ICACT2006, Feb. 20-22, 2006, pp.544.
[3] Kishore Kothapalli Bruhadeshwar Bezawada, "Security Issues and Challenges in Wireless network", Center for Security, Theory and Algorithmic Research , SPAA 2005, pp.116-125.
[4] Gurveen K. Sandhu, Gurpreet Singh Mann, Raj deep Kaur, "Benefit and Security Issues in Wireless Technologies: Wi-Fi and WiMax" International Journal of Innovative Research in Computer and message Engineering , Vol. 1, Issue 4, June 2013, pp.322-329.
[5] Jamshed Hasan "security Issues of IEEE 802.16 (WiMAX)" Australia, 5th December, 2006, pp.890-898.
[8] U.Revathi, "Attack Detection Using Intrusion Detection System in Wireless Sensor Network", Special Issue of Engineering and Scientific International Journal, Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College, May 2015, pp.28-31.