УДК 004.4

Bah Ibrahima,
Student,
Department "Big Data Analytics and Video Analysis Methods",
Engineering School of Information Technologies,
Telecommunications and Control Systems,
Ural Federal University named after the first President of Russia B.N. Yeltsin
Yekaterinburg, Russian Federation

WIRELESS SENSOR NETWORKS AREA: SECURITY AND CHALLENGES

Abstract:
Wireless Sensor Network (WSN) is a high potential and emerging technology with a multitude of important applications such as remote environmental monitoring and target tracking. They are used in crisis or critical situations (military use) and have commercial applications such as construction, also in traffic, as well as the surveillance of homes and smart homes and in many other situations. Wireless sensor networks are a major security problem these days. This level of security has been made weak or rendered obsolete by the possibility of some sort of attack; the innate power and recall limit of the sensor nodes win the usual impractical security solutions. Wireless interface team, they communicate with each other forming a network. This article sheds light on security issues in WSN networks, discuss the know-how of sensor network security research and also future research angles.

Keywords:
Wireless sensor networks, security attack, investigation, security.

Introduction

Wireless communication has been the engine of development prowess in the advancement of low-power, low-cost electronic and multifunction sensor nodes [1].

There has been a clear evolution from the conventional sensor network cable to the use of small sensor nodes, which detect, process and constitute the communicating parts. WSNs superlatively facilitate the design and process of operating the system in their wireless environment. For example: observation of a contaminated environment. The security of sensor networks is not negligible [2]. They perform a variety of tasks that need security. Leakage of prepared male sensitive information leads to incorrect results due to inadequate or misuse of the information.

The main problems of the WSN security are discussed in this work based on [2-6].

Architecture WSN

The network devices that make up a typical WSN can be cited as follows (Fig. 1):

Sensor nodes (field devices);

Gateway or access points;

Network manager;

Interfacing with the sensors and a power source;

Security Manager.

Base stations are one or more distinguished components of the WSN with much more computing, power and communication resources. They act as a gateway between the sensor nodes and the end user, as they typically transfer data from the WSN to a server. The other special components of routing-based networks are routers, which are designed to calculate, compute, and distribute routing tables. Many of the techniques are used to connect to the outside world, including mobile phone networks, satellite phones, radio modems, high power Wi-Fi links, etc.

Under normal conditions, most security services like: non-repudiation, confidentiality, availability, integrity, authenticity, front and back secrecy, freshness must be provided.

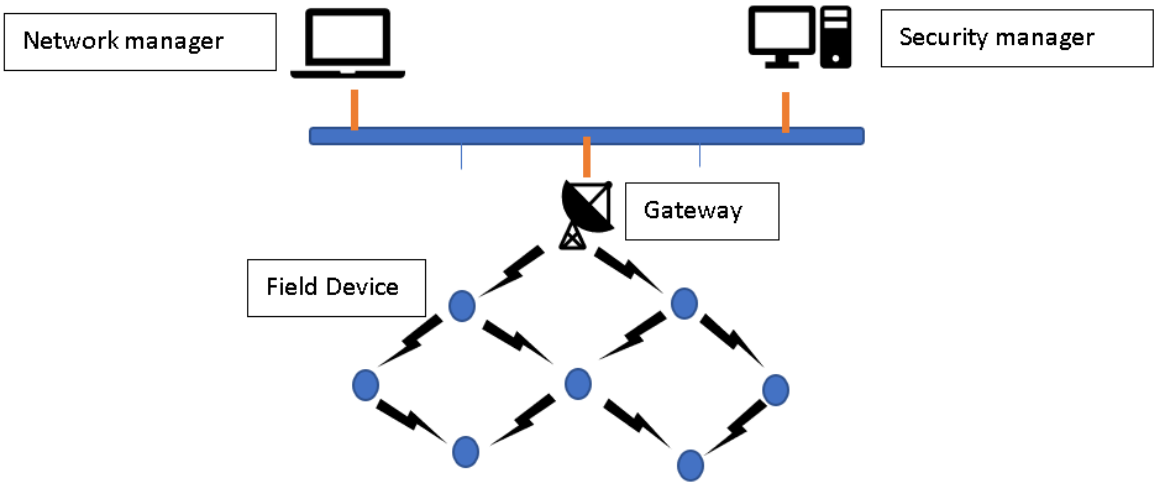

Figure 1 – Architecture of WSN

The restrictions of the WSNs sometimes make it difficult to apply the formal security technique. Routine security algorithms in WSNs must be optimized, for this to be possible, attention to restrictions is essential. The most obvious constraint for WSNs is energy limitation.

Several security proposals at different layers of the protocol stack are considered below.

Challenge of Wireless Sensor Network (WSN)

– Supporting trust is difficult in WSNs. Without adequate protection, communication of privacy over civilian wireless sensor networks is considered inappropriate.

– Portable equipment with limited resources is untrained for intensive calculations and communication overload.

– The need for aggregate results helps preserve random results from inappropriate algorithms.

– Dedicated infrastructure for data collection is not credible on wireless sensor networks.

– The repercussions of aggregating data without security of its integrity is unreliable.

Security objectives in Wireless Sensor Network (WSN)

The security objectives can be divided into two sections. Primaries are known as standard security objectives such as confidentiality, integrity, authentication, and availability. The secondary objectives are data freshness, self-organization, time synchronization and secure location.

Primary objectives

Data confidentiality: Under no circumstances should a sensor node be able to reveal its information to neighbors. It is one of the most important concerns in network security.

Data authentication: By identifying the origin of the message, it guarantees its reliability through authentication.

Data integrity: To have confidence in the reliability of data, data integrity is essential. It has the ability to confirm that the message has not been altered, tempered and changed.

Data availability: it specifies the network availability for the messages to be communicated and also the ability of a node to use the resources.

Secondary objectives

The freshness of the data ensures that the data is recent and that no old messages have been re-read. To remedy this problem, another time counter can be added to the packet.

Time synchronization: the majority of sensor network applications obey some form of time synchronization. It allows the sensors to evaluate the delay from one end-to-end packet as it moves between two sensors per pair.

Self-organization: In general, a wireless sensor network is an ad hoc network which is characterized by the sufficient and flexible independence of each sensor node to self-organize and self-repair under different scenarios. Post-attack damage can be devastating if self-organization is obsolete in a network of sensors.

Secure location: the ability to locate automatically and accurately determines the utility of a network to locate the location of a fault.

Attacks against wireless sensor networks

Attacks against Wireless Sensor Network (WSN) can be listed as active attacks and passive attacks. Active attacks: It is structured as follows: the flow of data in the communication channel is called an active attack, it is monitored, listened to and modified by attackers.

Attacks on information in transit: Any attacker can monitor the flow of traffic as wireless communication is vulnerable to eavesdropping and act to cut, modify, intercept or build packets to ultimately deliver false information to sinks and base stations.

Black hole / sinkhole attack: the nodes act like a black hole to attract all traffic from the sensor network. And it can extend to nodes considerably far from base stations (Fig, 2).

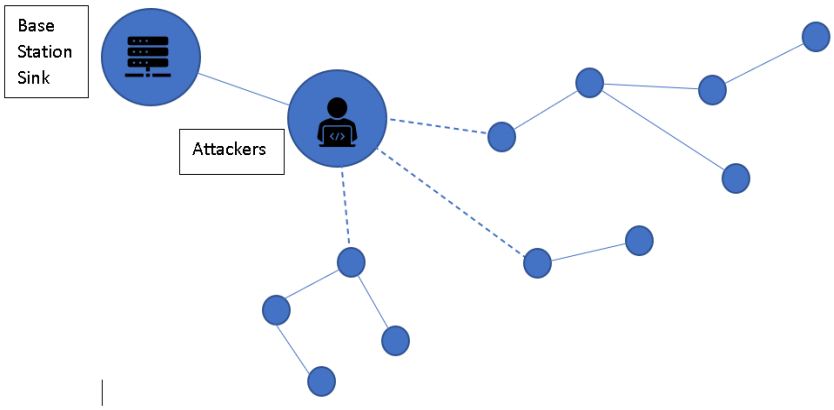

Figure 2 – Black hole attack conceptual view

Worm hole attacks (Fig. 3): it is an extreme attack. It consists of recording the packets in one location and driving them to another.

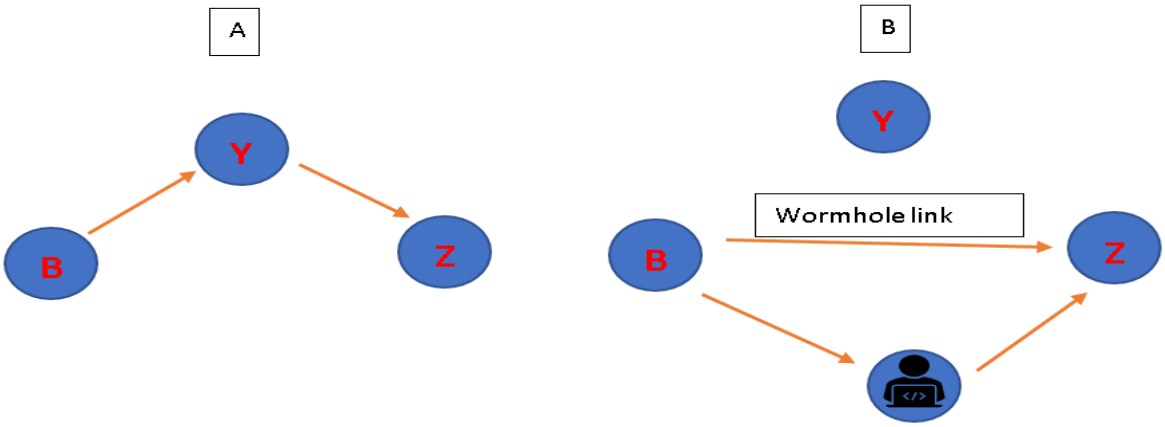

Figure 3 – Worm hole attack simulation

Diagram A and B simulates a situation where a wormhole attack is taking place. When a node B shares the routing request packet, it is picked up by the attacker who plays it back in its neighborhood. Each of the nodes that pick up this packet will mark it as its parent, because it will consider it to be in the range of node B. In this case the attacker convinces them that B is only one

jump away from them even when the victim nodes are several jumps apart from B thus creating a wormhole.

HELLO flood attacks: it consists in sending packets of a HELLO routing protocol replayed by an attacker from one node to another with more energy.

Denial of service: several types of DoS attacks can be carried out in different layers of the network. It can be voluntary (malicious action) or just be a failure: Node subversion, Node malfunction, Node outage, Message corruption, Passive collection of information, Physical attacks, Node replication attacks, False node.

Passive attacks unauthorized listening and monitoring of the communication channel by an attacker is called an attack. The most common attacks that breach privacy are: Monitor and eavesdropping, Traffic analysis, Camouflage adversaries.

Conclusion

The WSN network is multi-hop wireless networks with limitations and challenges. Open wireless support, multi-hop architecture, power restrictions, etc. are such features that impose many security challenges on them. Security challenges can be physical threats like jamming and jamming, risks from routing attacks like black hole, wormhole and sleep deprivation attacks to drain energy resources. Spread spectrum, frequency hopping, or cognitive radios can be considered to prevent jamming attacks, but these techniques are not suitable for WSN due to the simplicity and low power of the sensor nodes. Routing attacks due to multi-hop architectural complexity can be addressed by secure routing protocols for WSN. The intrusion detection system may be a good candidate to consider for these wireless networks, however, such a mechanism may not be more feasible for WSN; as such a mechanism can increase the complexity of sensor node design, however, it can be studied for sensor gateways. it is clear with bitterness that there is a gap in the level of wireless sensor networks.

References:

1. Römer and Mattern, The Design Space of Wireless Sensor Networks. IEEE Wireless Communications, 2004.
2. X. Du, and H-H. Chen, Security in Wireless Sensor Networks, IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp.60-66.
3. B. Krishnamashari, D. Estrin and S. Wicker, Impact of Data Aggregation in Wireless Sensor Networks, Proc. 22nd International Conference Distrib. Comp. Systems, Jul. 2002.
4. H. Luo, Y. Lin and S. K. Das, Routing Correlated Data in Wireless Sensor Networks: A Survey, IEEE Network, vol. 21, no.6, Nov/Dec. 2007, pp. 40-47.
5. Yun Zhou, Yuguang Fang, Yanchao Zhang, Securing Wireless Sensor Networks: A Survey, IEEE Communications Surveys & Tutorials, year 2008
6. Y. Wang, G. Attebury, and B. Ramamurthy, A Survey of Security Issues in Wireless Sensor Networks, IEEE Commun. Surveys Tutorials, vol. 8, pp. 2– 23, year 2006.