Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 9, Issue, 11, pp.61286-61289, November, 2017

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

SECURITY THREATS AND THEIR DEFENSE METRICS FOR WIRELESS SENSORS

***Mr. Sk Khasim, Mr. B. Jayaram and Mrs. Ismatha Begum**

Asst Professor, Dept of CSE-GNITC, Hyderabad-India

ARTICLE INFO

Article History:
Received 17th August, 2017
Received in revised form
30th September, 2017
Accepted 29th October, 2017
Published online 30th November, 2017

Key words:
Base station,
Sink,
Suspected,
Sensitive data,
investigate,
Countermeasures,
Threats.

ABSTRACT

Wireless Sensor Network consists of distributed autonomous sensor nodes to monitor physical and environmental conditions, Such as temperature, sound, vibration, pressure, motion and to collectively pass their data through the network to a main location known as Base station or Sink. Wireless sensor consist of huge number of nodes spread over diverse locations having characteristics like low processing power, low storage capacity and limited battery life. That means sensor networks are battery powered. As a sensor network grows it is more suspected to attacks. Sensor nodes will communicate highly sensitive data among various nodes, so it is most important to construct a secure channel for a wireless sensor network. They are mostly used in applications, such as military monitoring, health care as well as civilian applications. The main aim of this paper is to investigate the security related issues in wireless sensor networks .This paper categories various security threats and their classification that can occur in wireless sensor networks and providing probable Countermeasures (defenses) against the attacks.

Citation: Mr. Sk Khasim, Mr. B. Jayaram and Mrs. Ismatha Begum. 2017. "Position of mandibular third molar to inferior alveolar canal using cone beam computed tomography: a new classification", *International Journal of Current Research*, 9, (11), 61286-61289.

INTRODUCTION

Wireless sensor network (WSN) is the collection of spatially distributed and dedicated sensors used to monitor physical or environmental conditions such as temperature, pressure, etc. and transferring the collected data to a base station (sink). The primary goal of wireless sensor networks is collecting the information from the physical world. The wireless nodes with sensing capability will sensor various physical and environmental conditions with low. Processing power and wireless communication are vulnerable to attacks. As sensor network grows, the need for more effective security mechanisms is also increasing. The security must be addressed from the beginning of designing of the system as sensor networks interact with sensitive data and usually operate in hostile diverse locations.

Types of Wireless Networks: There are five types of wireless networks available:

- Wireless Personal area network(PAN)
- Wireless Local area Network(LAN)
- Wireless Metropolitan area network(MAN)
- Wireless Wide area network(WAN)
- Global Area Network(GAN) (David Clark)

The Wireless sensor network is a collection of "nodes" from a few to several hundreds or even thousands, where each node is connected to one sensor and collect sensitive data which altogether is sent to a base station or sink.

Components of sensor network: Each sensor network node has several parts:

- A radio transceiver with an internal antenna or connection to an external antenna.
- A microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

The WSN architecture consist of

- Data acquisition network(sensing)
- Data aggregation network(network processing)
- Data Dissemination network

Characteristics of wireless sensor network: The main characteristics of a WSN include the following:

****Corresponding author:*** **Mr. Sk Khasim,**
Asst Professor, Dept of CSE-GNITC, Hyderabad-India.

- Sensor nodes are battery powered that means they are limited with Power consumption constraints.

Constraints of Sensor Nodes

- The bandwidth of powerful Sensor node is 250kbps
- Processors with low computing power of 8-bit or 16-bit
- Storage capability is less
- Low power transmitter with ISM-industrial scientific medical Bands, GPSK, BFSK, GFSK.
- The Ability to cope with node failures (resilience)
- mobility of nodes
- sensor nodes are Heterogeneous nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use

Security issues in wireless sensor networks

This section of the paper categories various issues related with the security of WSNs.

Limitations of wireless sensor networks

Sensor networks are often used in mission critical environments such as in military and healthcare applications. These environments have demanding security requirements that must be addressed at the initial phase of design, in an attempt to focus on a spherical security strategy that will cover as many security problems as possible.

Hostile Environment

Sensor networks can be deployed in remote or hostile environments such as battlefields. In these cases, the nodes cannot be protected from physical attacks, since anyone could have access to the location where they are deployed. An adversary could capture a sensor node or even introduce his own malicious nodes inside the network. If the latter is the case, the adversary's aim is to trick the network into accepting his nodes as legitimates. In both cases, the adversary can compromise sensitive information, which is either stored on the compromised nodes or is forwarded through the adversary's nodes to the next hop; the sensitive information that is collected could be used for illegal purposes. The challenge here for researchers and developers is to design resilient security protocols and solutions offering security, even if a subset of sensor node is compromised. It is important to ensure that, if a node is compromised, sensitive information stored on the node cannot be taken off with ease.

Dynamic Network topology

Deploying a sensor network in a hostile environment is done by random distribution, i.e. from an airplane. Therefore, it is difficult to know the topology of sensor networks a priori. In these situations, it is hard to store various encryption keys on nodes in order to establish encryption among a group of neighbors, since the neighborhood cannot be known a priori. The challenge is to design key agreement protocols that do not require certain nodes to be neighbors of some other nodes, and also do not require encryption keys to be stored on sensors before deployment.

Appropriate key distribution algorithms must be designed along a flexible WSN architecture to securely provide encryption keys in real time.

Limited Resources

Power restrictions

The power restrictions of sensor nodes are raised due to their small physical size and lack of wires. Since the absence of wires results in lack of a constant power supply, not many power options exist. Sensor nodes are typically battery-driven. However, because a sensor network contains hundreds to thousands of nodes, and because often WSN are deployed in remote or hostile environments, it is difficult to replace or recharge batteries. The power is used for various operations in each node, such as running the sensors, processing the information gathered and data communication. Keep in mind that communication between sensor nodes consumes most of the available power, much more than sensing and computation. Power limitations greatly affect security, since encryption algorithms introduce a communication overhead between the nodes; more messages must be exchanged, i.e. for key management purposes, but also messages become larger as authentication, initialization and encryption data must be included.

Limited Computational power

In the case of computational power, computations are linked with the available amount of power. As you may understand, since there is a limited amount of power, computations are constrained also. Although it is acknowledged that sensors are not expected to have the computing power of workstations or even mobile handheld devices, researchers and developers are greatly concerned with the issue. More power is used for communication than computations. Therefore, since the power for computations is even more constrained than the total quantity of power, complex security solutions are prohibited. The limitation of computational power limits the adoption of strong cryptographic algorithms such as the RSA public key algorithm, which is computationally expensive.

Instead, symmetric encryption algorithms are used to secure sensor nodes' communication, since symmetric encryption doesn't have as demanding computational requirements as asymmetric encryption. However, with asymmetric encryption, features like digital signatures are not supported. Therefore, another challenge for researchers and developers is to design appropriate algorithms to establish and verify trust among the nodes participating in a communication. Furthermore, other security solutions must be adopted to cover the weaknesses of symmetric encryption; when an adversary compromises a node, he could retrieve the shared key used to encrypt the messages and then compromise the entire communication of the sensor network.

Storage Restrictions

The limited capability for storage affects the storage of cryptographic keys as well. According to the encryption scheme used, each sensor node may need to know a number of keys for each other node in the network to secure communication, and thus store the keys in the nodes' storage space.

However, the large number of sensor nodes requires a lot of memory, which may not be provided. As I mentioned previously, having a single encryption key common to all nodes allows an adversary to compromise the whole network by compromising only a single node. The challenge of storage restriction is for researchers to design security protocols in a way that a minimum number of encryption keys must be used to provide adequate protection to the network.

Design challenges

- **Scalable and flexible architecture.** The network should be scalable and flexible to the enlargement of the network's size. The communication protocols must be designed in such a way that deploying more nodes in the network does not affect routing and clustering. Rather, the protocols must be adapted to the new topology and behave as expected.
- **Error-prone wireless medium.** Since sensor networks can be deployed in different situations, the requirements of each different application may vary significantly. Researchers must take into consideration that the wireless medium can be greatly affected by noisy environments, and thus the signal attenuates in regard to the noise.
- **Fault tolerance and adaptability.** If a sensor node fails due to a technical problem or consumption of its battery, the rest of the network must continue its operation without a problem.

Wireless sensor network security requirements

In this section, standard security requirements for the wireless sensor network are discussed.

Data Confidentiality

In sensor networks, the confidentiality relates to the following (Carman *et al*., 2000; Perrig *et al*., 2002)

- A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
- In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensornetwork.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

Data integrity & Authentication

The summarized information sent to base station must be accurate without any changes done by intruders. It ensures integrity of information collected. Data integrity ensures that any received data has not been altered in transit.

Data availability

Some Approaches weaken the availability of a sensor and sensor network for the following reasons:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.
- A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network

Data Availability ensures availability of network at all times. However, it is extremely difficult to ensuring network availability due to limited ability of individual sensor nodes to detect between threats and failures.

Data Freshness

The data must be recent one without any old data being used. Data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. Data freshness implies that the available data is recent, and it also ensures that any old messages are not replayed by adversary.

Non repudiation

The summarized information once deployed to a base station by the sink (aggregator) could not be denying them back.

Attacks in wireless sensor networks & probable defenses

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways.

DOS (Denial of Service) Attacks

These attacks cause not only jamming of sensor communication channel but also create severe sophisticated attack to violate some protocols & some other layers of wireless network. Types of Denial of Service attacks: There are several DOS attacks that can occur at different layers. a) DOS attacks at Physical Layer: Jamming and Tampering. Jamming is simply the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network.

Defenses for jamming: Spread Spectrum, Priority messages, Lower duty cycle, Region mapping and Node change. Defenses for physical Tampering: Tamper proof hardware & Node hiding

DOS attacks at Data Link layer: Collision & Exhaustion
Defenses: Rate limiting

DOS attacks at Network layer: False Routing (Very dangerous to TinyOS beaconing), Selective forwarding (Neglect & greedy) , Black hole(Malicious node refuses to Forward every packet) & IP Spoofing

Defenses: Multipath routing

In WSN there is no IP Address Concept. The other possible attacks at Network layer includes. Sinkhole Attack(Black hole (or sinkhole attack) is the black hole attack is also termed as sink hole occurring at the network layer, where the attacker

builds a covenant node that seems to very attractive in the sense that it promotes zero cost routes to neighboring nodes with respect to the routing algorithm (Aashima single and ratikasachdeva, 2013).Sybil Attack (malicious device illegitimately taking on multiple identities"(Newsome *et al*., 2004). Worm hole attack (In wormhole attack, a pair of awful nodes creates a wormhole tunnel to replay the packets. Malicious node receives the packet in one section of the network and sends them to another section of the network (Aashima single and ratikasachdeva, 2013). Hello flood attack DOS attacks at Transport Layer: Synchronization -flood attack, De-synchronization attack

Common security mechanisms for wsn

Security mechanism is actually used to detect, prevent and recover from the security attacks. A wide variety of security schemes can be invented to counter malicious attacks and these can be categorized as high-level (secure group management, intrusion detection, secure data aggregation) and low-level mechanism (key establishment, secrecy, privacy, secure routing and resilience to node capture)(5)

- Symmetric key cryptography
- Public key
- Digital signatures
- Message authentication codes
- Anti replay protection

Conclusion and future scope

The Wireless sensor networks are widely used in many applications and WSNs continue to grow as more and more sensor node added to the network. As WSNs grows the need will arise for maintaining its security. However WSN suffers from many constraints like limited energy, processing capability, storage capability, as well as unreliable communication and unattended operation. Most of the Security attacks are caused by the injection of false information into the network while aggregating the data. Hence Security has become the main issue in providing confidentiality to data in the sensor network.

This paper categorizes the threats and probable defense metrics. And we have also listed various types of attacks in wsn. We presented the common security mechanisms that should be taken into considerations and researchers should work in these areas to obtain security of wireless sensor networks.

REFERENCES

Aashima single and ratikasachdeva, "Review on security issue and attacks in wireless sensor network, IJARCSSE, vol. 3, April-2013.

Carman, D. W., Krus, P. S. and Matt. B. J. 2000. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD.

Newsome, J., Shi, E., Song, D. and Perrig. A. 2004. The sybil attack in sensor networks:analysis & defenses. In roceedings of the third international symposium on Information processing in sensor networks, pages 259–268. ACM Press.

Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V. and Culler. D. E. 2002. Spins: security protocols for sensor networks. Wireless Networking , 8(5):521–534.

Wireless Networking Complete The Morgan Kaufmann Series in Networking Series Editor , David Clark, M.I.T., Pei Zheng, Feng Zhao, David Tipper, Jinmei Tatuya, Keiichi Shima, Yi Qian, Larry Peterson, Lionel Ni, D. Manjunath, Qing Li, Joy Kuri, Anurag Kumar, Prashant Krishnamurthy.

Yogesh Kumar, Rajiv Munjal, Krishan Kumar, 2011. "Wireless Sensor Networks and Security Challenges", IJCA.

****