ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Security Challenges for Wireless Sensor Network

N. Vijayarani[1], G.Nandhakumar[2]

Assistant Professor Department of Computer Science, Selvamm Arts and Science College (Autonomous), Namakkal, India[1]

M.Phil Scholar, Department of Computer Science, Selvamm Arts and Science College (Autonomous), Namakkal, India[2]

ABSTRACT: Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. WSN are playing a great role in the controlling and managing environments in different situations and has become important part of research area. WSN research is usually classified into three categories i.e. hardware & software of the sensors nodes, application area, and communication & security. Due to limited resources of computation power, battery, communication range, WSN are vulnerable to different types of attacks and providing security of WSN is really a great challenge. In this paper we first discuss various security issues concern with the security of WSNs; next we describe various security requirements of WSNs and in the en end of the paper we discuss research issues that are concern with WSNs.

One of the major challenges wireless sensor networks face today is security. While the deployment of sensor nodes in an unattended environment makes the networks vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor nodes makes conventional security solutions unfeasible. The sensing technology combined with processing power and wireless communication makes it profitable for being exploited in great quantity in future.

KEYWORDS: "Wireless sensor network"

I. INTRODUCTION

In spite of the diverse applications, sensor networks pose a number of unique technical challenges due to the following factors:

Ad hoc deployment: Most sensor nodes are deployed in regions which have no infrastructure at all. A typical way of deployment in a forest would be tossing the sensor nodes from an aeroplane. In such a situation, it is up to the nodes to identify its connectivity and distribution.

Unattended operation: In most cases, once deployed, sensor networks have no human intervention. Hence the nodes themselves are responsible for reconfiguration in case of any changes.

Untethered: The sensor nodes are not connected to any energy source. There is only a finite source of energy, which must be optimally used for processing and communication. An interesting fact is that communication dominates processing in energy consumption. Thus, in order to make optimal use of energy, communication should be minimized as much as possible. **Dynamic changes**: It is required that a sensor network system be adaptable to changing connectivity (for e.g., due to addition of more nodes, failure of nodes etc.) as well as changing environmental stimuli. Thus, unlike traditional networks, where the focus is on maximizing channel throughput or minimizing node deployment, the major consideration in a sensor network is to extend the system lifetime as well as the system robustness.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

II. WIRELESS SENSOR NETWORK ARCHITECTURE

The characteristics of a sensor network and the requirements of different applications, have a decisive impact on the network design. Some of the factors that influence the network design are fault tolerance, scalability, production costs, operating environment, sensor network topology, hardware constraints, transmission media and power consumption.

Fault tolerance is the ability of the network to continue its function, even if some nodes fail or block. Sensor nodes are prone to failure due to harsh environment conditions, lack of power, etc. This shouldn't affect the overall function of the network.

In WSNs, the number of nodes may be in order of tens, hundreds or thousands. Therefore, the protocols designed for these networks should be able to handle the new schemes efficiently.

Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers and cannot be reused, it is important to reduce the cost of sensor nodes so that the cost of the whole network is reduced.

In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.

Sensor nodes have limited processing and storage capacities, and thus can only perform limited computational functionalities. These hardware constraints present many challenges in software development and network protocol design for sensor networks.

WSN topology

WSNs use four basic networking topologies: point-to-point (peer-to-peer), star (point-to-multipoint), tree and mesh.

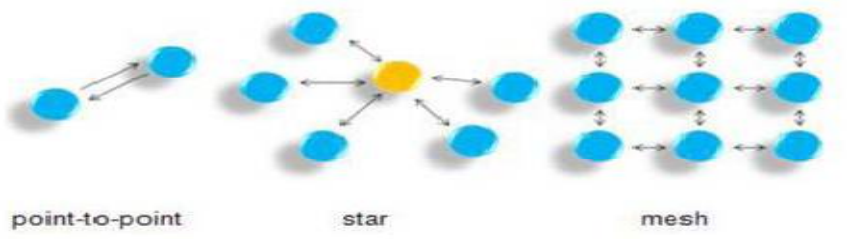


Figure 1.1 Basic WSN topologies

In point-to-point networks, each node is allowed to communicate with other nodes of the network, without having to go through a centralized node (the sink). Each node is able to function either as "client" or a "server" to the other nodes of the network.

In star networks, the sensor nodes cannot communicate directly with each other. Communication must be routed through the centralized node, which acts as the server, whereas all the other nodes are the clients. The main flaw of star topology is that if the sink fails, the entire network fails.

A lot of central nodes linked with each other, can form an extended star network, called tree network. A tree network can be considered as a hybrid of both point-to-point and star networks.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Figure 1.2 Tree topology

In mesh topology, each node can choose between many pathways, in order to route the data to the desired location. Mesh topology is more flexible and allows the network to self-heal, in case of nodes failure. On the other hand, power and processing requirements at each node are much higher.

Communication in a WSN

To send data to the sink, each sensor node can transmit its data directly using a single hop. However, when the sensor network covers a large geographical area, long-distance transmission could be very costly in terms of power consumption. Therefore, it is essential to reduce the transmission distance, in order to increase power savings and prolong the network lifetime.

For this purpose, multi-hop short-distance communication is preferred. In multi-hop communication, each node transmits its sensed data to the sink, via one or more intermediate nodes. This way, the communication energy consumption is sufficiently reduced.

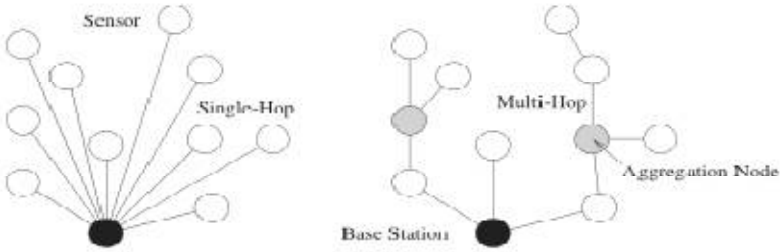


Figure 1.4 Single-hop versus multi-hop communication in sensor networks

Hardware Specifications

A sensor node consists of four basic components : a sensing unit, a processing unit, a radio transceiver and a power unit. Additional components may include location finding systems like GPS, mobilizers and power generators. Sensing unit contains a sensor and an analog to digital converter (ADC). The analog signals measured by the sensors are converted to digital by the ADC. Afterwards, they are used as input for the processing unit, which manages procedures that allow the nodes to collaborate with each other. The transceiver is used to connect the node to the device.

The power unit is the most important component of the sensor node because it implicitly determines the lifetime of the entire network. Power is a resource hard to maintain, basically for two reasons: a) because of the size limitations of the nodes and b) because of the possible harsh conditions of the observed phenomenon, that make the nodes inaccessible. On the other hand, it is possible to extend the lifetime of the sensor network by energy scavenging, e.g. using solar cells.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

III. APPLICATIONS

Area monitoring Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.
Health care monitoring The medical applications can be of two types: wearable and implanted. Wearable devices are used on the body surface of a human or just at close proximity of the user. The implantable medical devices are those that are inserted inside human body. There are many other applications too e.g. body position measurement and location of the person, overall monitoring of ill patients in hospitals and at homes. Body-area networks can collect information about an individual's health, fitness, and energy expenditure.
Environmental/Earth sensing There are many applications in monitoring environmental parameters,examples of which are given below. They share the extra challenges of harsh environments and reduced power supply.
Air pollution monitoring Wireless sensor networks have been deployed in several cities (Stockholm, London, and Brisbane) to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas.
Forest fire detectionA network of Sensor Nodes can be installed in a forest to detect when a fire has started. The nodes can be equipped with sensors to measure temperature, humidity and gases which are produced by fire in the trees or vegetation. The early detection is crucial for a successful action of the firefighters; thanks to Wireless Sensor Networks, the fire brigade will be able to know when a fire is started and how it is spreading.
Landslide detectionA landslide detection system makes use of a wireless sensor network to detect the slight movements of soil and changes in various parameters that may occur before or during a landslide. Through the data gathered it may be possible to know the occurrence of landslides long before it actually happens.
Water quality monitoring Water quality monitoring involves analyzing water properties in dams, rivers, lakes & oceans, as well as underground water reserves. The use of many wireless distributed sensors enables the creation of a more accurate map of the water status, and allows the permanent deployment of monitoring stations in locations of difficult access, without the need of manual data retrieval.
Natural disaster prevention Wireless sensor networks can effectively act to prevent the consequences of natural disasters, like floods. Wireless nodes have successfully been deployed in rivers where changes of the water levels have to be monitored in real time.
Industrial monitoring
Machine health monitoring Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionality.
Data logging Wireless sensor networks are also used for the collection of data for monitoring of environmental information, this can be as simple as the monitoring of the temperature in a fridge to the level of water in overflow tanks in nuclear power plants. The statistical information can then be used to show how systems have been working. The advantage of WSNs over conventional loggers is the "live" data feed that is possible.
Water/Waste water monitoring Monitoring the quality and level of water includes many activities such as checking the quality of underground or surface water and ensuring a country's water infrastructure for the benefit of both human and animal. It may be used to protect the wastage of water.
Structural health monitoring Wireless sensor networks can be used to monitor the condition of civil infrastructure and related geo-physical processes close to real time, and over long periods through data logging, using appropriately interfaced sensors.
Wine production

Wireless sensor networks are used to monitor wine production, both in the field and the cellar.

IV. CHARACTERISTICS

The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures (resilience)
- Some mobility of nodes (for highly mobile nodes see MWSNs)

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Cross-layer design

Cross-layer is becoming an important studying area for wireless communications. In addition, the traditional layered approach presents three main problems:

1. Traditional layered approach cannot share different information among different layers , which leads to each layer not having complete information. The traditional layered approach cannot guarantee the optimization of the entire network.
2. The traditional layered approach does not have the ability to adapt to the environmental change.
3. Because of the interference between the different users, access conflicts, fading, and the change of environment in the wireless sensor networks, traditional layered approach for wired networks is not applicable to wireless networks.

So the cross-layer can be used to make the optimal modulation to improve the transmission performance, such as data rate, energy efficiency, QoS (Quality of Service), etc.. Sensor nodes can be imagined as small computers which are extremely basic in terms of their interfaces and their components. They usually consist of a processing unit with limited computational power and limited memory, sensors or MEMS (including specific conditioning circuitry), a communication device (usually radio transceivers or alternativelyoptical), and a power source usually in the form of a battery. Other possible inclusions are energy harvesting modules,[11] secondary ASICs, and possibly secondary communication interface (e.g. RS-232 or USB).

V. LITERATURE SURVEY

The **KirtiRaj Bhatele, et al.,** presented hybrid security protocol for better security using a combination of both symmetric and asymmetric cryptographic algorithms. In this hash value of the decrypted message using AES algorithm is calculated using MD5 algorithm. This hash value has been encrypted with dual RSA and the encrypted message of this hash value also sent to destination. Now at the receiving end, hash value of decrypted plaintext is calculated with MD5 and then it is compared with the hash value of original plaintext which is calculated at the sending end for its integrity. By this we are able to know whether the original text being altered or not during transmission in the communication medium.

Arash Habibi Lashkari, et al., presented a survey on wireless security protocols (WEP, WPA and WPA2/802.11i). Here WEP protocol types, weaknesses and enhancements, WPA protocol types, WPA improvements such as cryptographic message integrity code or MIC, new IV sequencing discipline, per packet key mixing function and rekeying mechanism. They also explained major problems on WPA that happened on PSK part of algorithm. Finally paper explained third generation of wireless security protocol as WPA2/802.11i.

Gamal Selim, et al., explained various types of security attacks modification, fabrication, interception, brute force, maintainability and static placement of MIC. They surveyed currently available security protocols i.e. WEP, WEP2, WPA and WPA2. They also proposed a new mechanism called multiple slot system (MSS). MSS makes use of the key selector, slot selector and MIC shuffle selector. MSS uses one of four encryption algorithm RC4, RSA, Blowfish and AES.

Hyung-Woo Lee, et al., explained various issues and challenges in wireless sensor network. Paper explained two types of wireless security attacks – one is the attack against the security mechanisms and another is against the basic mechanisms like routing mechanism. Major attacks explained are denial of service attack, attacks on information in transit, sybil attack, hello flood attack, wormhole attack, blackhole/sinkhole attack. Paper also explained the various security schemes for wireless sensor networks like wormhole based, statistical en-route filtering, random key and tinysec. Holistic view of security in wireless sensor networks is also described.

Lifeng Sang, et al., proposed shared secret free security infrastructure for wireless networks based on two physical primitives: cooperative jamming and spatial signal enforcement. Cooperative jamming is for confidential wireless communication and spatial signal enforcement is for message authenticity. Proposed infrastructure

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

International Journal of Future Generation Communication and Networking Vol.7, No.4 (2014) 32 Copyright ⓒ 2014 SERSC provides confidentiality, identity authentication, message authentication, integrity, sender non-repudiation, receiver non repudiation and anonymity.

Andrew Gin, et al., compared the performance analysis of evolving wireless 802.11 security architecture. Paper explained wireless network security methods. Paper explained security layers like WEP shared key authentication and 40 bit encryption, WEP shared key authentication and 104 bit encryption, WPA with PSK authentication and RC4 encryption, WPA with EAP-TLS authentication and RC4 encryption, WPA2 with PSK authentication and AES encryption and WPA2 with EAP-TLS authentication and AES encryption. Effects on throughput are also discussed.

VI. METHODOLOGY

Security Threats and Issues in Wireless Sensor Networks

Most of the threats and attacks against security in wireless networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. In fact, wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In most of the cases various security issues and threats related to those we consider for wireless ad hoc networks are also applicable for wireless sensor networks. These issues are well-enumerated in some past researches and also a number of security schemes are already been proposed to fight against them. However, the security mechanisms devised for wireless ad hoc networks could not be applied directly for wireless sensor networks because of the architectural disparity of the two networks.

While ad hoc networks are self-organizing, dynamic topology, peer to peer networks formed by a collection of mobile nodes and the centralized entity is absent ; the wireless sensor networks could have a command node or a base station (centralized entity, sometimes termed as sink). The architectural aspect of wireless sensor network could make the employment of a security schemes little bit easier as the base stations or the centralized entities could be used extensively in this case. Nevertheless, the major challenge is induced by the constraint of resources of the tiny sensors.

Attacks in Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here we point out the major attacks in wireless sensor networks.

Denial of Service Denial of Service (DoS)

DoS is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

Attacks on Information in transit

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks.

Sybil Attack

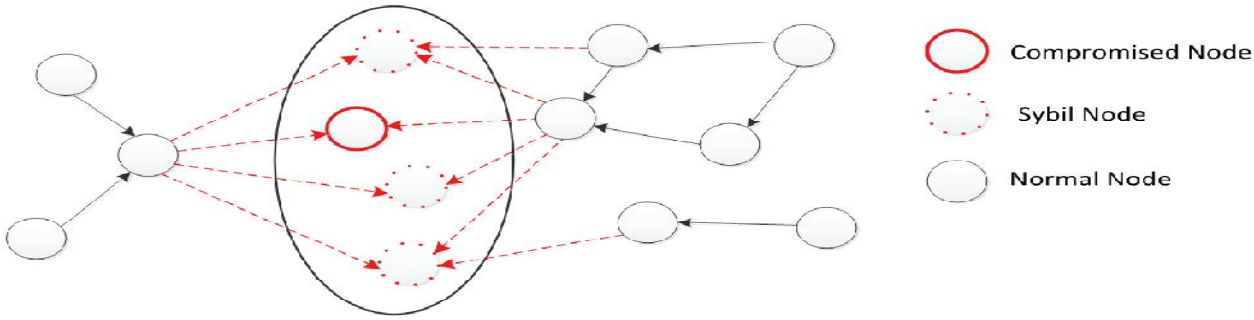
In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016



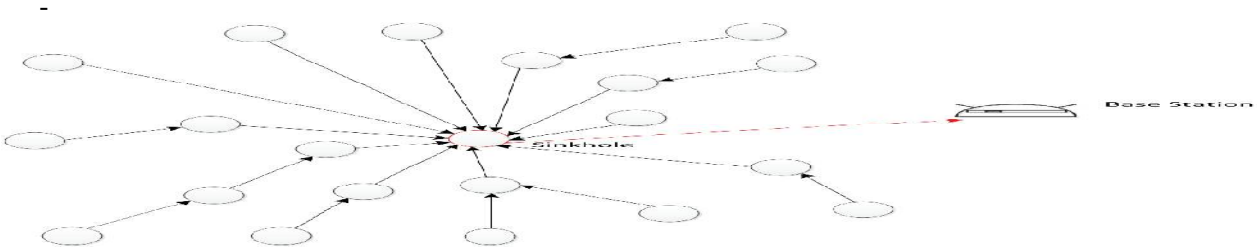
Sybil attack

This type of attack where a node forges the identities of more than one node is the Sybil attack.Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection . Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols. Douceur showed that, without a logically centralized authority, sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities.

Blackhole/Sinkhole Attack

In this attack, a malicious node acts as a blackhole to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station.

-



Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations.

Hello Flood Attack

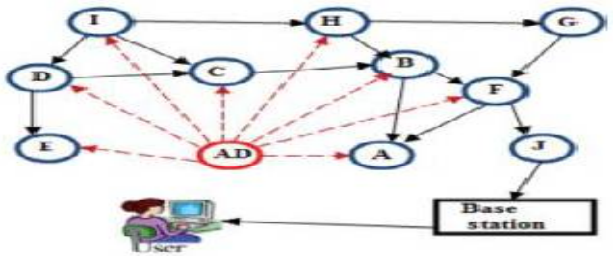
Hello Flood Attack is introduced in This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission (termed as a laptop-class attacker in) range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

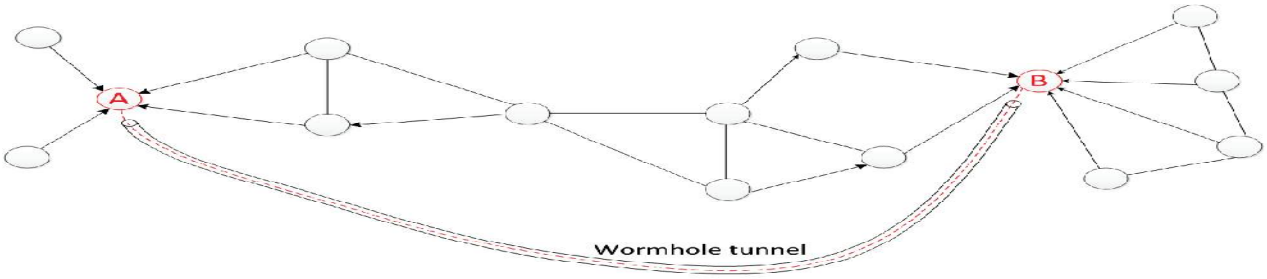
(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016



Wormhole Attack

Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information. When a node B (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent. Hence, even if the victim nodes are multihop apart from B, attacker in this case



Wormhole attack

Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically attacks are classified as active attacks and passive attacks.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

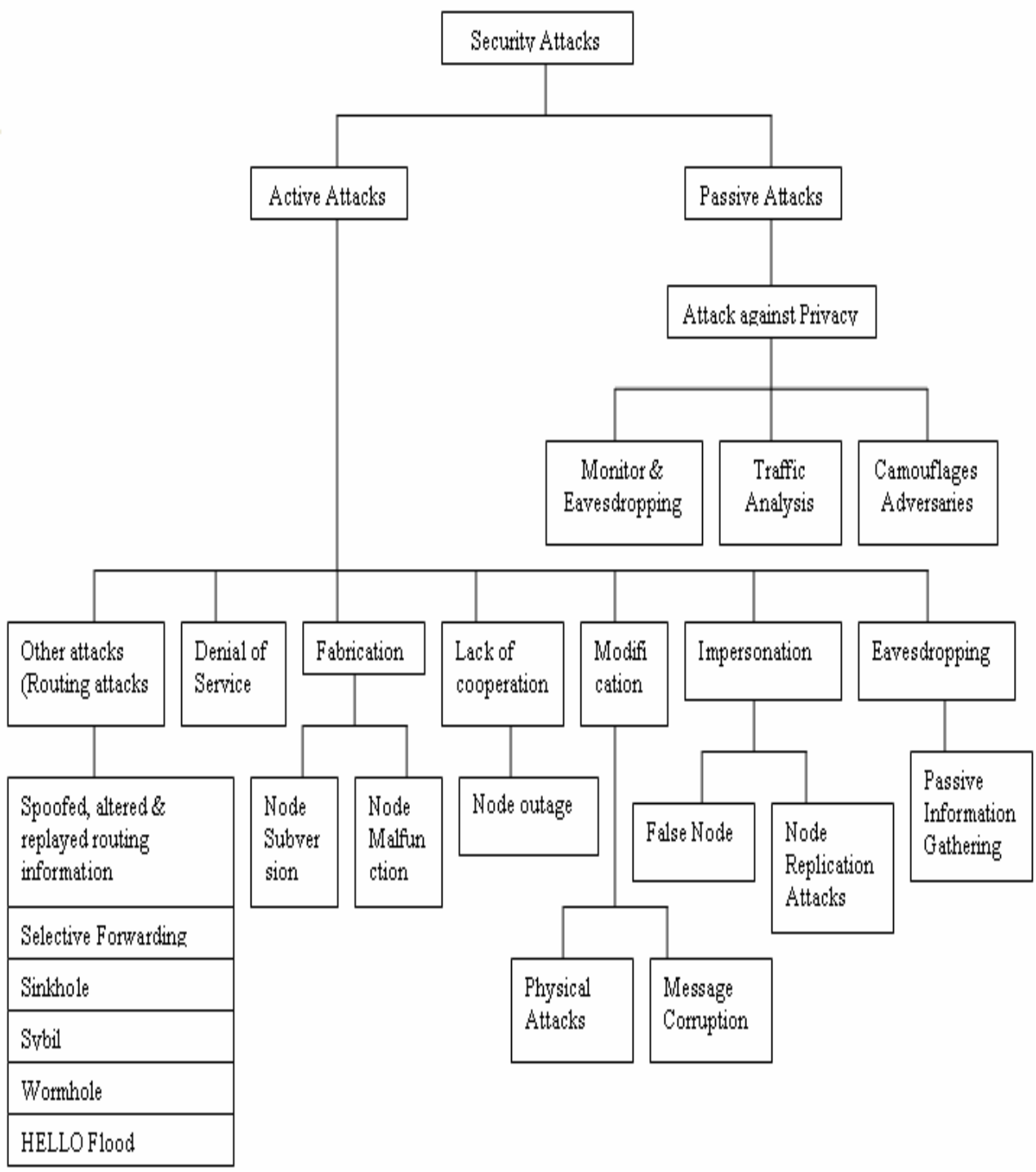


Figure 3.3 General Classification of Security Attacks

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

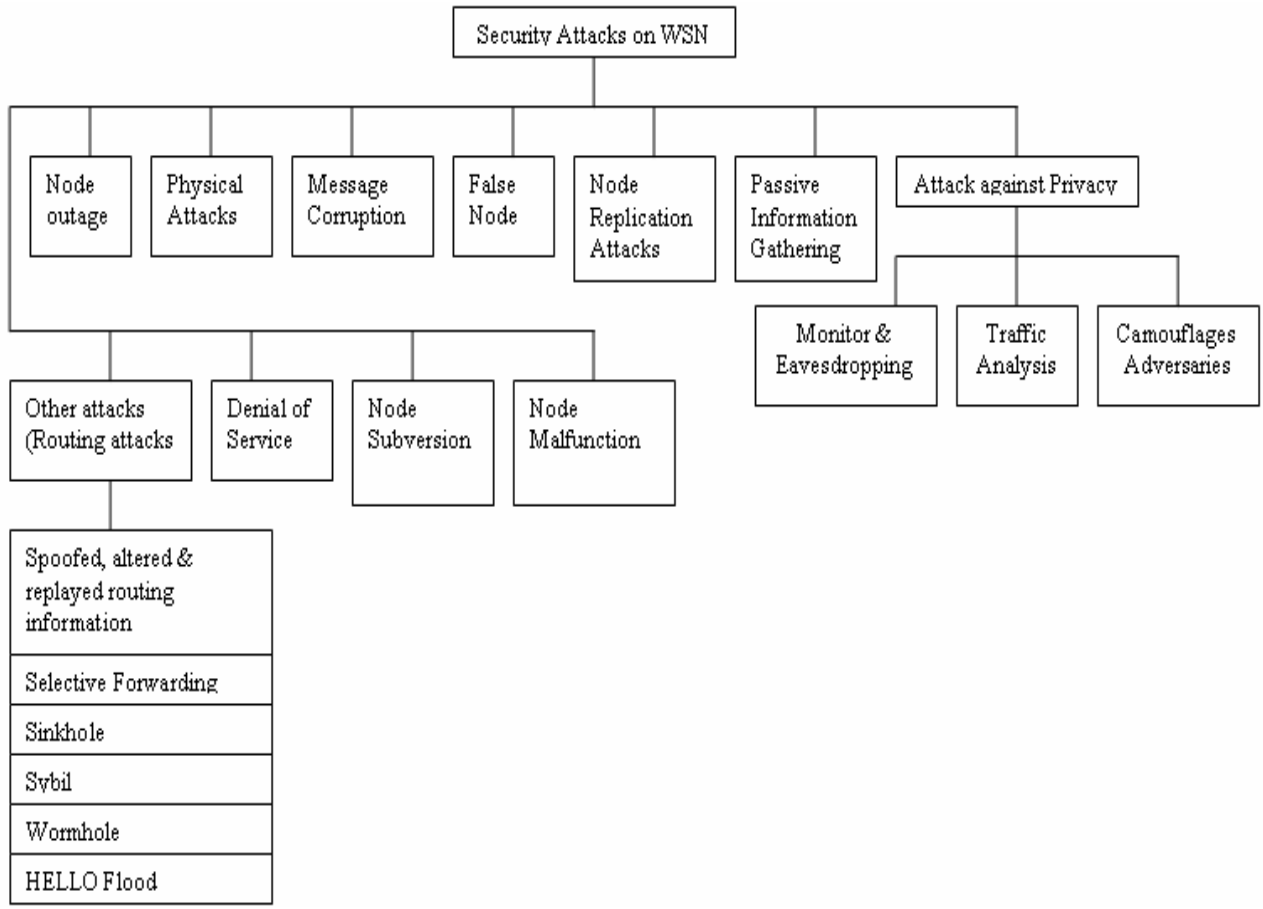


Figure 3.4 Classification of Security Attacks on WSN

Passive Attacks The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.

Attacks against Privacy The main privacy problem is not that sensor networks enable the collection of information. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner. Some of the more common attacks against sensor privacy are:

Monitor and Eavesdropping When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

Traffic Analysis Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns.

Camouflage Adversaries One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

Active Attacks The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature. Routing Attacks in Sensor Networks, Denial of Service Attacks, Node Subversion, Node Malfunction, Node Outage, Physical Attacks, Message Corruption, False Node, Node Replication Attacks, Passive Information Gathering etc.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

VII. CONCLUSION AND FUTURE WORK

Due to continue growth of wireless sensor networks, the need for more effective security mechanisms is also increasing. The security concerns of the sensor network should be addressed from the beginning of designing of the system as sensor networks interact with sensitive data and usually operate in hostile unattended environments. A detailed understanding of the capabilities and limitations of each of the underlying technology is required for secure working of wireless sensor networks. In the paper we tried to discuss various issues concern with the security of WSNs along with WSNs requirements and research challenges. In the future work, various attacks on WSNs will be studied along the various countermeasures proposed in the literature to tackle with these attacks. Novel techniques will be proposed in the future for countermeasure to various attacks in order to make WSNs more secure and reliable for their extensions in other fields.

REFERENCES

[1] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, "Sensor Network Security: More Interesting Than You Think", In Proc. of the 1st USENIX HotSec, 2006.
[2] M. Anand, Z. Ives, and I. Lee. "Quantifying Eavesdropping Vulnerability in Sensor Networks", In Proc. of the 2nd International VLDB Workshop on Data Mgnt. for Sensor Networks (DMSN), 2005
[4] Stamatios and V. Kartalopoulos, Editors, "Differentiating Data security and Network Security", IEEE International Conference on Communications, (2008) May 19-23, Beijing.
[5] S. D. Kanawat and P. S. Parihar, Editors, "Attacks in Wireless Networks", International Journal of Smart Sensors and Adhoc Networks, (2011) May 18-23.
[6] Y. X. Lim and T. Schmoyer, Editors, "Wireless Intrusion detection and response", IEEE Information Assurance Workshop, (2003) June 18-20, Westpoint, Newyork.
[7] K. Bhatele, A. Sinhal and M. Pathak, Editors, "A Novel Approach to the Design of New Hybrid Security Protocol Architecture", IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), (2012) August 23-25, Ramanathapuram. International Journal of Future Generation Communication and Networking Vol.7, No.4 (2014) Copyright ⓒ 2014 SERSC 33