International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

TAXONOMY FOR WSN SECURITY-A SURVEY

Ms.Kshitija A.Chaple,

Assistant Professor, KJEI's Trinity college of engineering and Research ,Pune.

k.chaple@gmail.com

ABSTRACT: WSN is one of the dominant and emerging technology that shows great promise for various application in military, ecological and health related areas.WSN is highly vulnerable to attacks and inclusion of wireless communication technology incurs various types of security threats.WSN requires security measures due to sensitive data and as sensor may operate in hostile unattended environment.WSN suffer from constraints like low computational capability, small memory limited energy resources physical capture susceptibility and insecure wireless communication channel. These create security a challenge in WSN. In this article we provide a survey of security in WSN.We provide an outline with constraints and security requirement and attacks with their counter measures in WSN.

KEYWORDS: Wireless Sensor Networks (WSNs), Security, Threats, Attacks,

1. INTRODUCTION

Wirless sensor networks (WSN) are emerging to solve many problems related to networking ,security and social factors. Idea behind sensor network is to distribute sensor devices in an area to sense any change related to different parameter and communicate those changes or incident to other devices. In WSN transreceivers are used for communicating between sensors.

As WSN is progressing, security factor related to WSN is becoming crucial and new challenges are introduced in WSN day-by- day. Sensor data can be attacked externally and internally. Sensor can be captured physically and data can easily modify or new message can be transmitted or message can be leaked/used .WSN is more susceptible to Dos(Denial-of-service) attack.Dos attack is performed not only for disturbing or destroying network but also to create problem in service providing.

2. SECURITY THREATS AND ATTACKS IN WSN

Threat is a circumstance or event with the potential to adversely impact a system through a security breach and the probability that an attacker will exploit a particular vulnerability causing harm to a system asset is known as risk

Categories of threats

- Passive information gathering
- Subversion of node/insertion of a false node
- Node malfunction
- Node outage
- Message corruption
- Denial of service
- Traffic analysis

Threats in WSN can be classified

- External Vs internal attack
- Passive Vs active attack
- Mote class Vs Laptop class

2.1 WSN Security

WSNs provide unique opportunities of interaction between computing devices and their environment. The adhoc nature and wireless vulnerability make WSN a soft target for security attacks. In order to understand the security aspects of WSN, we provide a brief description of the different attacks and then present the possible solutions. First, we find out the requirements of WSN security. Then we present some of the typical attacks on WSN security and lastly we describe some well-known mechanisms for preventing some the attacks.

2.2 WSN Attacks

WSNs are vulnerable to various types of attacks. These attacks can be broadly categorized as passive and active. Passive attacks do not disrupt the operation of the network. In this case the attacker snoops the data exchanged inside the network without modifying it. Detection of passive attacks is very difficult since the operation does not get affected. Where as in active attacks, data is altered and thus disturbing the normal network activities.

2.3 WSN Requirements

WSN can be considered as a highly distributed database with wireless links. Security goals for distributed databases are very well studied. The data should be accessible only to authorized users (confidentiality), the data should be genuine (integrity), and the data should be always available on the request of an authorized user (availability). All these requirements also apply to WSNs and their users. Data confidentiality is the most important issue in network security. The

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

objective of confidentiality is required in sensors environment to protect information travelling among the sensor nodes of the network or between the sensors and the base station from disclosure. With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe.

The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit. Authentication in sensor networks is essential for each sensor node and base station to have the ability to verify that the data received was really sent by a trusted sender or not.

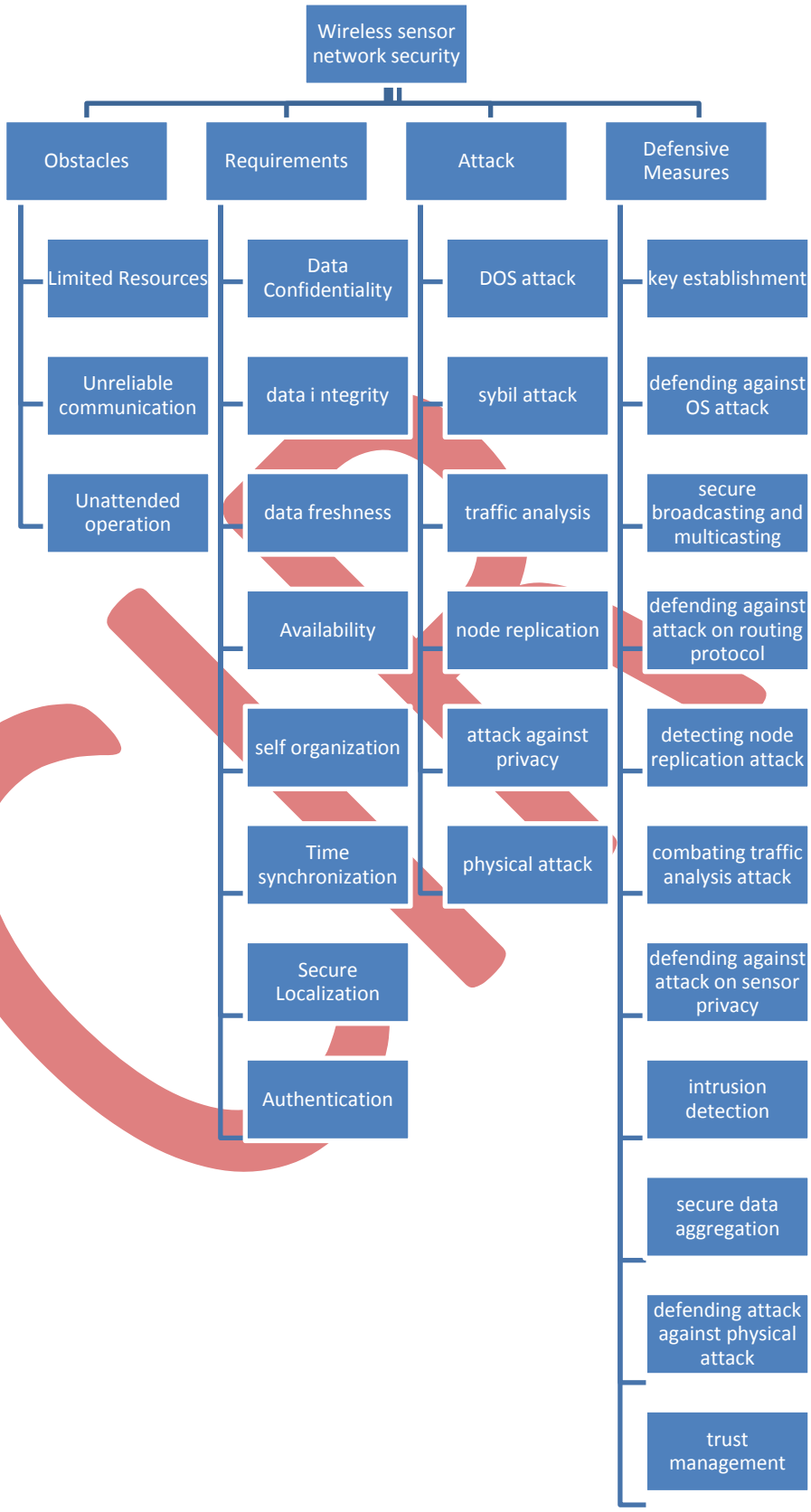
This authentication is needed during the clustering of sensor node in WSN. We can trust the data sent by the nodes in that group after clustering. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications such as pollution and healthcare monitoring rely on the integrity of the information to function with accurate outcomes. Secure management is needed at base station, clustered nodes, and protocol layer in WSN. Because security issues like key distribution to sensor nodes in order to establish encryption and routing information need secure management. Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time. Another important issue is the availability factor of the nodes or the transmission media. The network should remain operational all the time. It must have some redundancy to counter link failures and have the capability to survive against different attacks

3.SECURITY MECHANISMS

3.1 Secrecy and Authentication

Most of the sensor network applications require protection against eavesdropping, injection, and modification of packets. Cryptography is the standard defense. Remarkable system trade-offs arise when incorporating cryptography into sensor networks. For point-to-point communication[11],end-to-end cryptography achieves a high level of security but requires that keys be set up among all end points and be incompatible with passive participation and local broadcast. Link-layer cryptography with a network wide shared key simplifies key setup and supports passive participation and local broadcast, but intermediate nodes might eavesdrop or alter messages. The earliest sensor networks are likely to use link layer cryptography, because this approach provides the greatest ease of deployment among currently available network

cryptographic approaches.



International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

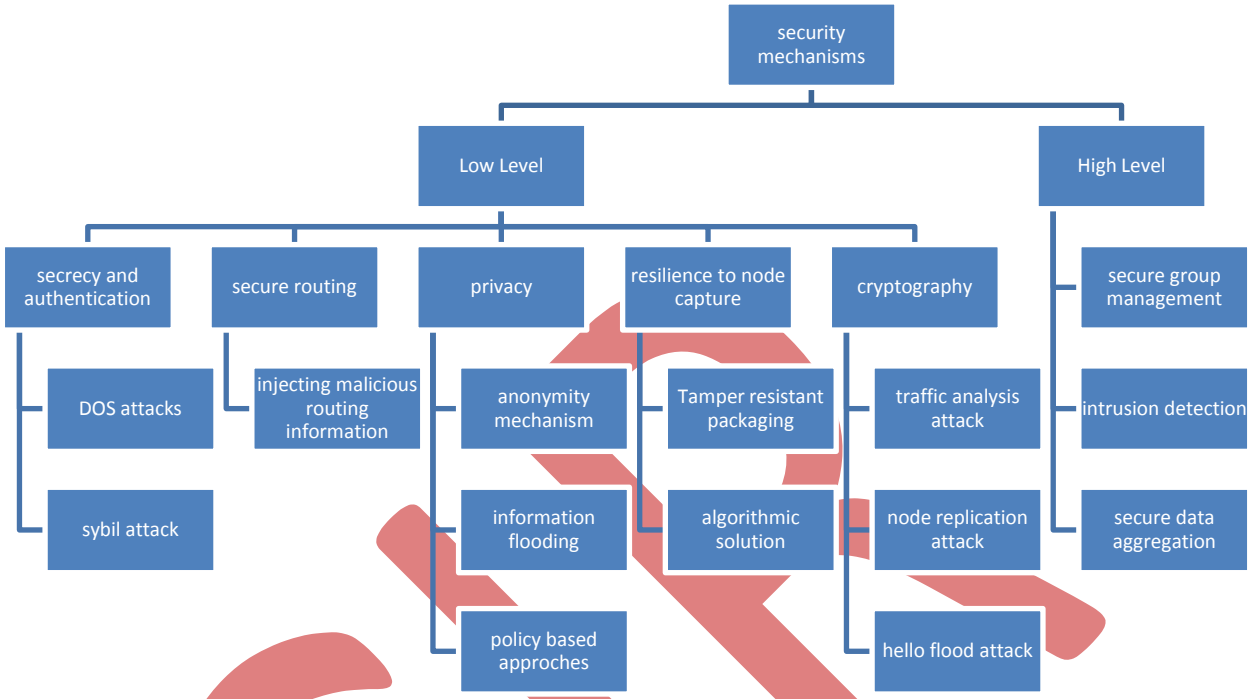


Fig 1:WSN Security Classification

Fig 2:Security Mechanisms

Routing security Energy efficient scheme Cryptography eavesdropping and tampering	Secure Localization Sinkhole Wormhole Selective forwarding Sybil Black hole
Data security Trust and reputation	Key management DOS

Altered spoofed replayed

Hello flood attack

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

Fig 3: Taxonomy for security Mechanisms

3.1.1 Denial of Service

Denial of Service (DoS) is produced by the unintentional failure of nodes or malicious action. 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 and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification

3.1.2 Sybil Attacks

A single node duplicates itself and presented in the multiple locations. The Sybil attack targets fault tolerant schemes such as distributed storage, multipath routing and topology maintenance. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network of traffic.

3.2 Secure Routing

Routing and data forwarding is a crucial service for enabling communication in sensor networks. Unfortunately, current routing protocols suffer from many security vulnerabilities. For example, an attacker might launch denial of- service attacks on the routing protocol, preventing communication. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Simple authentication might guard

3.3 Privacy

Like other traditional networks, the sensor networks have also force privacy concerns. Initially the sensor networks are deployed for legitimate purpose might subsequently be used in unanticipated ways. Providing awareness of the presence of sensor nodes and data acquisition is particularly important.

3.3.1 Anonymity mechanisms

Precise location information enables accurate identification of a user. This is a serious threat to privacy. One way to handle this problem is to make data source anonymous. An anonymity mechanism depersonalizes the data before it is released from the source. Since ensuring total anonymity is almost an impossible proposition, in almost all practical scenarios, a tradeoff is to be made between anonymity and disclosure of public information in most of the privacy protection mechanisms.

Four approaches have been proposed by researchers in this direction for WSNs. These approaches are: (i) decentralization of storage of sensitive data, (ii) establishment of secure channel for communication, (iii) changing the pattern of data traffic, and (iv) exploiting mobility of the nodes. The sensitive location data is to be stored in a spanning tree of nodes so that no single node holds a complete view of the location information. Communication using secure protocols such as SPINS will make eavesdropping and active attack on a WSN extremely difficult. The data traffic pattern may be changed by selectively inserting some bogus data in the network traffic so that traffic analysis by an external entity will not be successful. Mobile sensor nodes make attack on location privacy very difficult. The Cricket system is a location support system for in-building, mobile, location dependent applications. It allows applications running on mobile and static nodes to learn their physical location from a set of listeners. The listeners hear and analyze information from beacons in a building.

3.3.2 Information flooding

Various modifications to WSN routing protocols are proposed for protecting the location information of a source node. In particular, a set of flooding protocols are proposed. The randomized data routing and phantom traffic generation mechanism are used so that it is difficult for an adversary to track any data source

3.3.3 Policy-based approaches

In policy-based defense mechanisms the access control decisions and authentication techniques are made on the basis of a specified set of privacy policies**.**

3.4 Resilience to node capture

One of the most challenging issues in sensor networks is resiliency against node capture attacks. In most applications, sensor nodes are likely to be placed in locations easily accessible to attackers. Such exposure raises the possibility that an attacker might capture sensor nodes, extract cryptographic secrets, modify their programming, or replace them with malicious nodes under the control of the attacker. Tamper-resistant packaging may be one defense, but it's expensive, since current technology does not provide a high level of security. Algorithmic solutions to the problem of node capture are preferable [10].

3.5 CRYPTOGRAPHY

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

Selecting the most appropriate cryptographic method is vital in WSNs as all security services are ensured by cryptography. Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated by code size, data size, processing time, and power consumption. In this section, we focus on the selection of cryptography in WSNs.[2]

3.5.1Traffic Analysis

Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

3.5.2 Node Replication Attacks

Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether [10].

3.5.3 HELLO flood attacks

An attacker sends or replays a routing protocol's HELLO packets from one node to another with more energy. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes that are isolated in a large area within a WSN.[6] The sensors are thus influenced that the adversary is their neighbor. As a result, 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.

4. HIGH LEVEL MECHANISMS

High-level security mechanisms for securing sensor networks, includes secure group management, intrusion detection, and secure data aggregation.

4.1 Secure group management

Each and every node in a wireless sensor network is limited in its computing and communication capabilities. However, interesting in-network data aggregation and analysis can be performed by groups of nodes. For example, a group of nodes might be responsible for jointly tracking a vehicle through the network. The actual nodes comprising the group may change continuously and quickly. Many other key services in wireless sensor networks are also performed by groups. Consequently, secure protocols for group management are required, securely admitting new group members and supporting secure group communication. The outcome of the group key computation is normally transmitted to a base station. The output must be authenticated to ensure it comes from a valid group.

4.2 Intrusion Detection

Wireless sensor networks are susceptible to many forms of intrusion. Wireless sensor networks require a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements. The use of secure groups may be a promising approach for decentralized intrusion detection.

4.3 Secure Data Aggregation

One advantage of a wireless sensor network is the fine grain sensing that large and dense sets of nodes can provide. The sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station. For example, the system may average the temperature of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending on the architecture of the wireless sensor network, aggregation may take place in many places in the network. All aggregation locations must be secured.

ACKNOWLEDGEMENT

I would like to express my greatest gratitude to the people who have helped & supported me throughout my survey.

REFERENCES

[1].Dr. G. Padmavathi, Mrs. D. Shanmugapriya, 2009, A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2.

International Journal of Computers & Technology
Volume 4 No. 2, March-April, 2013, ISSN 2277-3061

[2].Jaydip Sen , 2009, A Survey on Wireless Sensor Network Security International Journal of Communication Networks and Information Security (IJCNIS) Vol. 1, No. 2.

[3]. K. Sharma and M. K. Ghose; 2010, Wireless Sensor Networks: An Overview on its Security Threats; IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs; CSE Department, SMIT, Sikkim, India.

[4].Kai Xing, Shyaam Sundhar Rajamadam Srinivasan, Manny Rivera, Jiang Li, Xiuzhen Cheng, 2005 Springer, Attacks and Countermeasures in Sensor Networks: A Survey NETWORK SECURITY .

[5].Shio Kumar Singh , M P Singh and D K Singh 2011 ,A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks International Journal of Computer Trends and Technology- May to June Issue ISSN: 2231-2803 1 IJCTT.

[6]. Dr. Banta Singh Jangra, Vijeta Kumawat 2012, A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 3.

[7].John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary,2006, Wireless Sensor Network Security: A Survey. Auerbach Publications, CRC Press.

[8]. Adrian Perrig, John Stankovic, David Wagner, 2004, "Security in Wireless Sensor Networks" communications of the ACM, Page53-57.

[9]. Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, 2006, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT).

[10].Adrian Perrig, John Stankovic, David Wagner, 2004 "Security in Wireless Sensor Networks" Communications of the ACM.

[11] H. Zhu, F. Bao, R. H. Deng, and K. Kim. 2004,Computing of trust in wireless networks. In Proceedings of 60th IEEE Vehicular Technology Conference, Los Angles, California.

Author' biography with Photo

Prof.Kshitija A.Chaple is a Assistant Professor in Information Technology department at KJEI's Trinity college of engineering, Pune.

CIR