Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.432 – 443

RESEARCH ARTICLE

Communication Layer, Attacks and Security Mechanisms of Wireless Sensor Network

Ku. Trupti D. Kadu
Student
Dept. of Computer Science, & Engineering,
Sant Gadge Baba Amaravati University,
Amaravati, India.
Kadutrupti9@gmail.com

Mr. D. C. Dhanawani
Assistant professor
Dept. Of Computer Science & Engineering
Sant. Gadge Baba Amaravati University,
Amaravati, India,
Deepak.c.dhanwani@gmail.com

Abstract: ***Wireless Sensor Networks (WSN) is a recent advanced technology of computer networks and electronics. The WSN increasingly becoming more practicable solution to many challenging applications. The sensor networks depend upon the sensed data, which may depend upon the application. One of the major applications of the sensor networks is in military. So security is the greatest concern to deploy sensor network such hostile unattended environments, monitoring real world applications. Wireless Sensor Networks (WSN) are a most challenging and emerging technology for the research due to their vital scope in the field coupled with their low processing power and associated low energy. Today wireless sensor networks are broadly used in environmental control, surveillance tasks, monitoring, tracking and controlling etc. On the top of all this the wireless sensor networks need very secure communication in wake of they being in open field and being based on broadcasting technology.***

Keywords- wireless sensor network (wsn); communication protocol; attack; security.

I. Introduction

One of fundamental goals for Wireless Sensor Networks (WSNs) is to collect information from the physical world. Comparing to existing infrastructure – based networks, wireless sensor networks can virtually work in any environment, especially those where wired connections are not possible. WSNs are often deployed to sense, process and disseminate information of targeted physical environments.

Today Intrusion Detection Systems (IDS) are widely used as a security solution in a wired network in the form of software/ hardware by which one can detect unwanted services going on the system by way of enhanced/abnormal network activity and identify suspicious patterns that may indicate whether the network/system is under attack? For WSN several schemes were proposed but they have limited features like only concern to attacks on a particular layer. Some others have also proposed a theoretical framework that is not suitable at deployment time [16, 17].

In general, WSNs consist of battery- operated sensor devices with computing, data processing, and communicating components. The ways the sensors are deployed can either be in a controlled environment where monitoring and surveillance are critical or in an uncontrolled environment. In the uncontrolled environments, security for sensor networks becomes extremely important.

A. WSN Architecture

In a typical WSN we see following network components – Sensor nodes (Field devices) – Each sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for -

a) Interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

b) Gateway or Access points – A Gateway enables communication between Host application and field devices.

c) Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.

d) Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

The base stations are one or more distinguished components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. Other special components in

routing based networks are routers, designed to compute, calculate and distribute the routing tables. Many techniques are used to connect to the outside world including mobile phone networks, satellite phones, radio modems, high power Wi-Fi links etc. Figure 1-1 shows the architecture of WSN.

II. COMMUNICATION PROTOCOLS

Wireless sensor networks use layered architecture like wired network architecture. Characteristics and functions of their each layer is given below in figure 2.

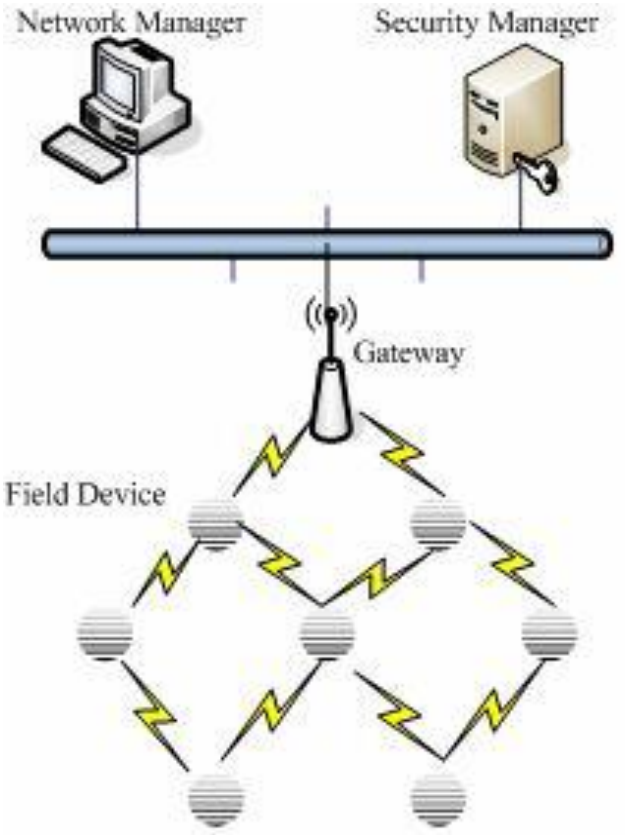


Figure 1. Architecture of WSN.

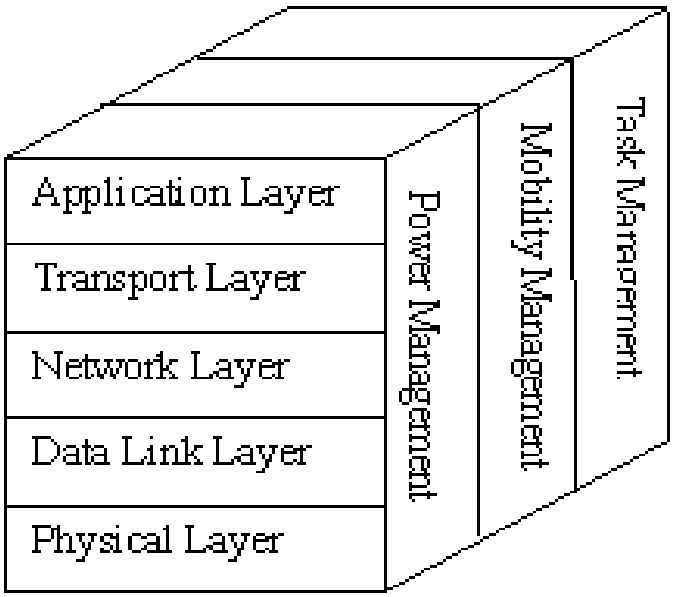


Figure 2. Layered Architecture of WSN

A. Physical Layer

The objective of physical layer is to increase the reliability by reducing path loss effect and shadowing. This layer is responsible for established connection, data rate, modulation, data encryption, signal detection, frequency generation and signal detection.

B. Data Link Layer

The objective of Data link layer is to insure interoperability amongst communication between nodes to nodes. This layer is responsible for error detection, multiplexing. Prevention of Collision of packets, repeated transmission etc. To secure data link layer, Karlof et al [2] proposed a link layer security architecture "TinySec" for wireless sensor networks. Naveen Sastry et al[4] proposed Zigbee or the 802.15.4 standard for hardware based symmetric key encryption. Some researches also proposed the possible use of public key cryptography [3, 9], secure code distribution [10] to create secure key during network deployment and maintenance.

C. Network Layer

The objective of Network layer is to find best path for efficient routing mechanism. This layer is responsible for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa. The LEACH and PEGASIS are the protocols which describe the techniques to save the energy consumption (power of sensor) so as to improve the life of sensors. LEACH gives cluster based

transmission while PEGASIS is chain protocol [5, 6, 15]. WSN use ID based protocols and data centric protocols for routing mechanism. In WSN, each node in the network acts as a router (because they use broadcast mechanism), so as to create secure routing protocol. Encryption and decryption techniques are used for secure routing [8, 13, 14].

D. Transport Layer

The objective of Transport Layer is to establish communication for external networks i.e. sensor network connected to the internet. This is most challenging issue in wireless sensor networks.

E. Application Layer

The objective of Application Layer is to present final output by ensuring smooth information flow to lower layers. This layer is responsible for data collection, management and processing of the data through the application software for getting reliable results.

III. ATTACKS ON WSN

The security breaches occur primarily in the form of Interruption (breakdown of communication links), Interception (unauthorized access of WSN), Modification (Change of data by unauthorized access) and fabrication (Addition of false data by unauthorized accesses) [13, 25, 26].

A. Denial of service

This type of attack results into making unavailable the resources to their intended users. As an example node „A" sends request to node „B" for communication and node „B" sends acknowledge to node „A" but „A" keeps on sending request to „B" continuously. As a result „B" is not able to communicate with any other nodes and thus becomes unavailable to all of them.

Denial of service attack may also occur at physical layer by jamming (by broadcasting mechanism) and/or tampering (modification or fabrication) of the packet. In Link Layer it is by producing collision data, exhaustion of resources and unfairness in use of networks. In network layer, it occurs by way of neglecting and the greediness of packets resulting into path failure. In transport layer, DOS attack occurs due to flooding and de-synchronization. Most of denial of service attacks may be prevented by powerful authentication and identification mechanisms.

B. Attack of information in transit

In case of wireless sensor networks usually each node reports changes to a cluster head or base station only for data above some threshold. Information in transit may be altered, spoofed, replayed again or vanished. In this type of attack attacker has high processing power and large communication range. This type of attack may be prevented by data aggregation and authentication techniques.

C. Sybil attack

In this attack the attacker gets illegally multiple identities on one node. By this, the attacker mostly affects the routing mechanism. Sybil attacks are generally prevented by validation techniques.

D. Blackhole/ Sinkhole Attack:

In this type of attack, attacker places himself in a network with high capability resources (high processing power and high band width) by which it always creates shortest path. As a result, all data passes through attacker‟s node.

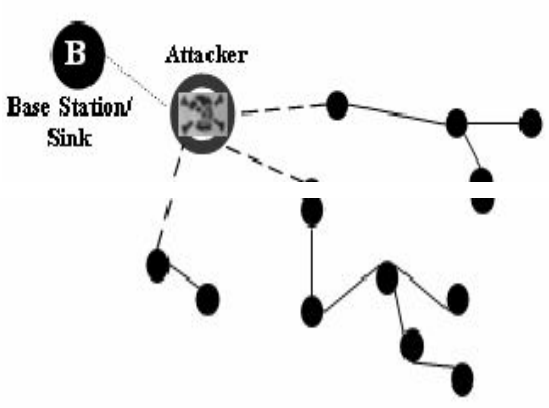


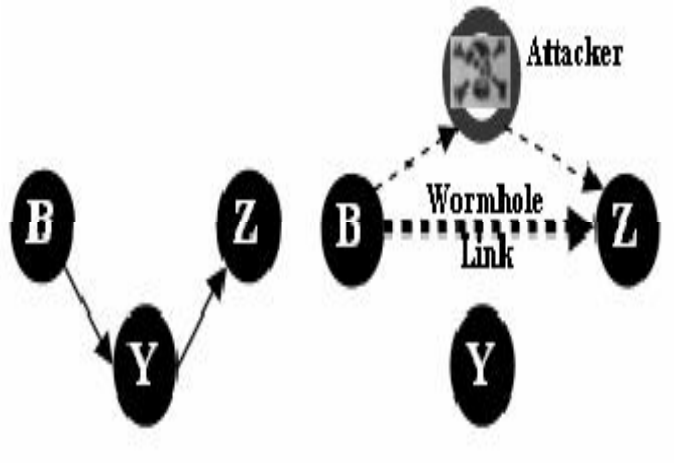
Figure 3: Conceptual view of Black hole Attack

E. 'Hello flood' Attack

This is one of the simplest attack in wireless sensor networks in which attacker broadcasts HELLO packets with high transmission power to sender or receiver. The nodes receiving the messages assume that the sender node is nearest to them and sends packets by this node. By this attack congestion occurs in the network. This is a specific type of DOS. Blocking techniques are used to prevent Hello Flood attacks.

F. 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.



(a) **(b)**

Figure 4: Wormhole Attack

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 multi-hop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole.

IV. SECURITY MECHANISM

The security mechanisms are 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 and low-level. Figure 3 shows the order of security mechanisms.

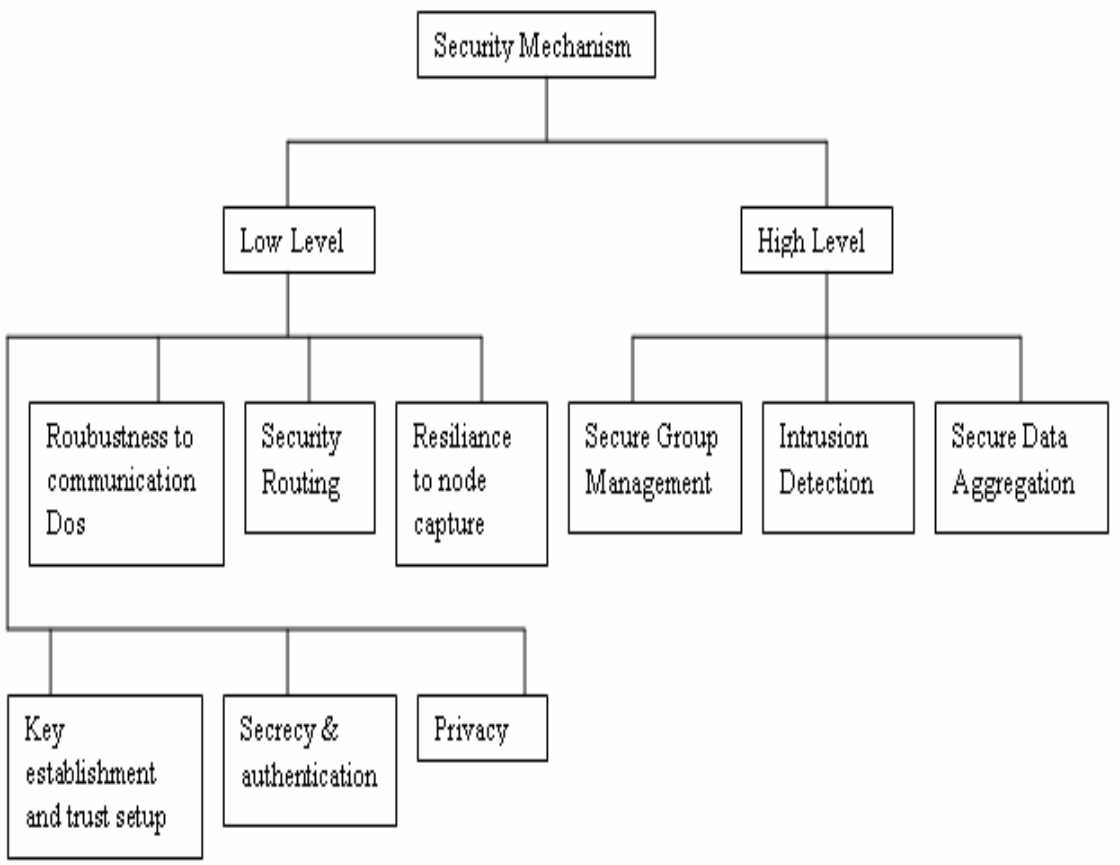


Figure 5: Security mechanisms

A. **Low-Level Mechanism**

Low-level security primitives for securing sensor networks includes,

1. Key establishment and trust setup
2. Secrecy and authentication
3. Privacy
4. Robustness to communication denial of service
5. Secure routing
6. Resilience to node capture

1) Key establishment and trust setup

The primary requirement of setting up the sensor network is the establishment of cryptographic keys. Generally the sensor devices have limited computational power and the public key cryptographic primitives are too expensive to follow. Key-establishment techniques need to scale to networks with hundreds or thousands of nodes. In addition, the communication patterns of sensor networks differ from traditional networks; sensor nodes may need to set up keys with their neighbors and with data aggregation nodes. The disadvantage of this approach is that attackers who compromised sufficiently and many nodes could also reconstruct the complete key pool and break the scheme.[1]

2) 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[12],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.[6]

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. [1]

4) Robustness to communication denial of service

An adversary attempts to disrupt the network's operation by broadcasting a high-energy signal. If the transmission is powerful enough, the entire system's communication could be jammed. More sophisticated attacks are also possible; the adversary might inhibit communication by violating the 802.11 medium access control (MAC) protocol by, say, transmitting while a neighbor is also transmitting or by continuously requesting channel access with a request-to send signal.[1]

5) 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 against injection attacks, but some routing protocols are susceptible to replay by the attacker of legitimate routing messages. [6]

6) 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.[1]

B. High-Level Mechanism

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

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. [1]

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.[1]

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.[6]

V. Conclusion

The deployment of sensor nodes in an unattended environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. This paper summarizes the attacks and their classifications in wireless sensor networks and also an attempt has been made to explore the security mechanism widely used to handle those attacks.

REFERENCES

[1] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004

[2] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", International conference on Advanced Computing Technologies, Page1043-1045, year 2006

[3] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003

[4] A. Perrig, R. Szewczyk, V. Wen, D. culler, and J. Tygar. "SPINS: Security Protocols for Sensor Networks." In Seventh Annual ACM International Conference on Mobile Computing and Networks(Mobicom 2001), Rome Italy, July 2001.

[5] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti."Secure pebblenets." In Proceedings of the 2001 ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 156-163. ACM Press, October 2001.

[6] S. Rajasegarar, C. Leckie, and M. Palansiwami, "Anomaly detection in wireless sensor networks", IEEE Wireless Communications, vol. 15, no. 4, Aug. 2008, pp. 34-40.

[7] Yun Zhou, Yuguang Fang, Yanchao Zhang, Securing Wireless Sensor Networks: A Survey, IEEE Communications Surveys & Tutorials, year 2008

[8]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.

[9] Malan D. J., Welsh M., and Smith M. D.," A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography" In First IEEE International Conference on Sensor and Ad Hoc Communications and Networks SECON04, 2004.

[10] Wen Hu, Peter Corke, Wen Chan, et al., "secFleck: A Public Key Technology Platform for Wireless Sensor Networks.", EWSN,

