A COMPARATIVE STUDY OF PHYSICAL ATTACKS ON WIRELESS SENSOR NETWORKS

Rina Bhattacharya

Department of Computer Science, CMJ University, Shillong, Meghalaya, INDIA, ***rinikolkata@gmail.com***

Abstract

Wireless Sensor Networks (WSN) have many potential applications and challenges They consists of hundreds or thousands of low power, low cost sensor nodes which have limited computing resources. WSNs are susceptible to many types of physical attacks due to wireless and shared nature of communication channel, un-trusted transmissions, deployment in open environments, unattended nature and limited resources. So security is a vital requirement for these networks. However wireless micro-sensor networks pose numerous design challenges. This challenge is especially difficult due to the energy constrained nature of the devices. In this paper we focus a wide variety of physical attacks and a comparison on them which enable s us to identify the purpose and capabilities of the attackers. Also this paper discusses known approaches of security detection and defensive mechanisms against the physical attacks effectively.

Keywords*- Communication channel, Open environment, Physical attacks, Sensor nodes, Wireless Sensor Networks,*

---*****---

1. INTRODUCTION

In recent years, the idea of wireless sensor networks has garnered a great deal of attention by researchers, including those in the field of mobile computing and communications [1,2]. WSN's have many potential applications and unique challenges. They usually are heterogeneous systems contain many small devices, called sensor nodes, that monitoring different environments in cooperative i.e, sensors cooperate to each others and compose their local data to reach a global view of the environments. In WSN's there are two other components, called "aggregation" and "base station'. Aggregation points collect information from there nearby sensors, integrate them and then forward to the base stations to process gathered data [7,8,9]. Also WSN's are vulnerable to many types of attacks such as physical attacks, they are one of the most malicious and harmful attacks on WSN's. due to unprotected and unsafe nature of the communication channel, untrusted and broadcast transmission media, deployment in hostile environments, automated nature and limited resources, the most of security techniques of traditional networks are impossible in WSN's, therefore security is a vital requirements for these networks especially against the physical attacks. The objective of this paper is to design an appropriate security mechanism for these networks that should cover different security dimensions of WSN's include confidentiality, integrity, availability and authenticity. The main purpose is presenting an overview of different physical attacks on WSN's and comparing them together and also focus on their goals, effects, possible detection and defensive mechanisms.

2. OVERVIEW OF WSN'S

A WSN is a heterogeneous system consisting of hundreds or thousands low cost and low power tiny sensors to monitoring and gathering information from deployment environment in real time. Common functions of WSN's are including broadcast and multicast, routing, forwarding and route maintenance. The sensors components are: sensor unit, processing unit, storage/memory unit, power supply unit and wireless radio transceiver, which are communicating each other.

3. SECURITY IN WSN'S

Security attack is a concern for wireless sensor networks because:

- Usage of minimal capacity devices in parts of the system.
- Physical accessibility to sensor and actuator devices.
- Wireless communication of the system devices.

In spite of these drawbacks or security attacks, WSN can still function effectively. These security threats can be handled using structured network security architecture, which includes modifications to traditional security services such as confidentiality, integrity and authenticity to the wireless domain.

4. SECURITY ISSUES IN WSN'S

A. Availability

Ensure that the desired network services are available even in the presence of denial of service attacks.

B. Confidentiality

Confidentiality means restricting data access to authorized personnel. The data should not be leaked across adjacent sensor networks. For this purpose, the message is sent on the channel in encrypted form.

C. Authenticity

Authentication is important application in sensor networks. Adversary can easily inject messages, the receiver need to ensure that data used in any decision making process originate from trusted sources. Authentication allows sender node and receiver must be sure that they talking really to the node to which they want to communicate.

D. Integrity

Data integrity ensures that the receiver receives unaltered data in transit by any unauthorized personnel.

E. Data f reshness

Data freshness ensures that the recent data is available without any reply of old messages by unauthorized personnel.

F. Robustness and Survivability

Sensor network should be robust against the various attacks and if an attack succeeds, the impact should be minimized.

G. Self-Organization

Nodes should be flexible enough to be self-organizing and self-healing.

H. Time Synchronization

These protocols should not be manipulated to produce incorrect data.

5 DEFINITIONS, STRATEGIES AND EFFECTS OF PHYSICAL ATTACKS ON WSN'S

WSN's are designed in layered form; this layered architecture makes these networks susceptible and lead to damage against many kinds of attacks. The following table presents the physical attacks based on their strategies and effects.

Attacks	**Attack definition**	**Attack techniques**	**Attack effects**
Signal/radio jamming	The adversary tries to transit radio signals emitted by the sensors to the receiving antenna at the same transmitter.	Constant jamming, deceptive jamming, random jamming, reactive jamming.	Radio interference, resource exhaustion.
Device tampering attack, node capturing attack	Direct physical access, captured and replace nodes,	Invasive attacks, non-invasive attacks, eavesdropping on wireless medium.	Damage or modify physically stop/alter node's services, take complete control over the captured node, software vulnerabilities.
Path-Based DOS	Typical combinational attacks include jamming attacks	Sending a large number of packets to the base station	Nodes battery exhaustion, network disruption, reducing WSN's availability
Node outage	Stopping the functionality of WSN's components.	Physically, logical	Stop nodes services, impossibility reading gathered information, launching a variety of other attacks.
Eavesdropping	Detecting the contents of communication by overhearing attempt to data	Interception, abusing of wireless nature of WSN's transmission medium	Launching other attacks, extracting sensitive WSN information, delete the privacy protection and reducing data confidentiality
DOS attacks	A general attack includes several types of other attacks in different layer of WSN's. reducing WSN's availability.	Physical layer, link layer, routing layer, transport layer, application layer attacks techniques.	Effects of physical layer, link layer, routing layer, transport layer and application layer attacks.

6. PHYSICAL ATTACKS CLASSIFICATION BASED ON THREAT MODEL

The physical attacks of WSN's based on attacks nature and effects, attacker's nature and capabilities, and WSN's threat model are shown in the following table.

Attacks	**Security Class**	**Attack threat**	**Threat model**
Signal/radio jamming	Modification	Availability, integrity	External and active
Device tampering	Interception, modification, fabrication	Availability, integrity, confidentiality, authenticity	External and active

Node capture	Interruption, interception, modification, fabrication	Availability, integrity, confidentiality, authenticity	External and active
Path-Based DOS	Modification, fabrication	Availability, authenticity	External and active
Node outage	Modification	Availability, integrity	External and active
Eavesdropping	Interception	Confidentiality	External and passive
DOS attacks	Interruption, interception, modification, fabrication	Availability, integrity, confidentiality, authenticity	Active

7. DETECTION AND DEFENSIVE STRATEGIES OF WSN's PHYSICAL ATTACKS

In the following tablr a classification and comparison of detection defensive techniques on WSN's physical attacks is presented.

Attacks/ criteria	Detection methods	Defensive mechanisms

Signal/radio jamming	Statistical information;
	Channel utility degradation than a threshold;
	Detecting background noise;
	Misbehavior detection techniques
		Access restriction;
		Encryption;
		Error-correction;
		Mode change;
		Lower duty cycle;
		Reporting attacks to base Station;
		Buffering;
		Mapping protocol

Device tampering attack or node capture attack(physical layer) or node subversion attack (routing layer) or node cloning attack(application layer)	Node disconnection/ absence from the network;
	Regular Monitoring;
	Existence interference in functionality of node; Node destruction;
	Using key management protocol;
	Misbehavior detection techniques
		Optimizing and using crypto-processors or physically secure processors;
		Applying standard precautions;
		Hardware/software alerter;
		Access restriction;
		Physical protection;
		Data integrity protection;
		Data confidentiality protection;
		Malicious node detection Techniques;
		Local removing or exclude the capture

CONCLUSIONS

Security is a vital requirement and complex feature to deploy and extend WSN's in different application domain. The most security physical attacks are targeting WSN security dimensions such as integrity, confidentiality, authenticity and availability. In this paper, the different dimensions of WSN's security is analyzed and presented a wide variety of WSN's physical attacks and classify them. The approach is to classify and compare the WSN's physical attacks, their properties such as threat model of WSN's physical attacks nature, goals and results, their strategies and effects and finally their associated detection and defensive techniques against these attacks to handle them independently and comprehensively.

REFERENCES

[1] K. Chris, W. David, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California, Berkeley.

[2] K. H. Kumar, A. Kar, "Wireless Sensor Network Security Analysis", Proceedings of International Journal of Next-generation Networks, Vol. 1, No. 1, December 2009, pp 1-9.

[3] P. Kumari, M. Kumar, R. Rishi, "Study of Security in Wireless Sensor Networks", Proceedings of International Journal of Computer Science and Technology, Vol.1, No. 5, pp 347-354.

[4] V.C. Manju, "Study of Security Issues in Wireless Sensor Network", Proceedings of International Journal of Engineering Science and Technology (IJEST), Vol. 3, No.10, October 2011, pp 7347-7351.

[5] N. Rajani, "Energy Efficient Reliable Routing Protocol for Wireless Sensor Networks", Indian Institute of Technology, Kanpur, June 2008.

[6] K. Sharma, M.K. Ghosh, D. Kumar et al, "A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks", Proceedings of International Journal of Advanced Science and Technology", Vol. 17, April 2010, pp 31-37.

[7] R. Sharma, Y. Chaba, Y. Singh, "Analysis of Security Protocols in Wireless Sensor Network", Proceedings of International Journal of Advanced Networking and Application, Vol. 2, No. 3, 2010, pp 707-713.

[8] E. Shih, H.S. Cho, N. Ickes, R. Min, A. Sinha, A. Wang, A. Chandrakasan, "Physical Layer Driven Protocol and Algorithms Design for Energy-Efficient Wireless Sensor Networks", Proceedings of MOBICOM'01, July 2001, Rome, Italy.

[9] S. K. Singh, M. P. Singh, D.K. Singh, "Routing Protocols in Wireless Sensor Networks - A Survey", Proceedings of International Journal of Computer Science & Engineering Survey (IJCSES), Vol.1, No. 2, November 2010.

[10] S. Singh, H. K. Verma, "Security for Wireless Sensor Network", Proceedings of International Journal on computer Science and Engineering (IJCSE), Vol. 3, No. 6, June 2011, pp 2393-2396.

[11] K. Ssu, C. Chou, H. C. Jiau, W.T. Hu, "Detection and diagnosis of data inconsistency failures in Wireless Sensor Networks", Proceedings of Elsevier Journal of Computer Networks, No. 50, 2006, pp 1247-1260.

[12] K. Sophia, "Security Models for Wireless Sensor Networks", Proceedings of, March 2006, pp 6-8.