EUROPEAN ACADEMIC RESEARCH
Vol. IV, Issue 12/ March 2017

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

A Paper Critique on Network Security and Attack Defense Mechanism for Wireless Sensor Networks

ALLYSA ASHLEY M. PALAMING
College of Computer Studies
Masters in Information Technology (MIT)
Tarlac State University

Abstract:

In this report the authors discussed the severe constraints and demanding deployment environments of wireless sensor networks make security for these systems more challenging than for conventional networks. However, several properties of sensor networks may help address the challenge of building secure networks. The unique aspects of sensor networks may allow novel defenses not available in conventional networks. Further, the authors investigate the security related issues and challenges in wireless sensor networks. It identifies the security threats, and review proposed security mechanisms for wireless sensor networks.

It was explained the concept of LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network. Mote-class versus laptop-class attacks - in moteclass (sensor-class) attacks, an adversary attacks a WSN by using a few nodes with similar capabilities as that of network nodes. There can be many potential threats to WSNs; the categories of the threats could be (a) passive information gathering, (b) subversion of node or insertion of a false node, (c) node malfunction, (d) node outage, (e) message corruption, (f) denial of service, or (g) traffic analysis. In this type of attack an attacker with a high radio transmission range (termed as a laptop-

class attacker) and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. Wireless sensor network (WSN) is a heterogeneous system combining thousands to millions of tiny, inexpensive sensor nodes with several distinguishing characteristics.

Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted a lot of attention in the recent years. The salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads. In this paper, we have introduced some security issues, threats, and attacks in WSNs and some of the solutions. Network security for WSNs is still a very fruitful research direction to be further explored.

Key words: network security, attack, network management, wireless sensor, network

I. INTRODUCTION

In this report the authors discussed the severe constraints and demanding deployment environments of wireless sensor networks make security for these systems more challenging than for conventional networks. However, several properties of sensor networks may help address the challenge of building secure networks. The unique aspects of sensor networks may allow novel defenses not available in conventional networks.

Further, the authors investigate the security related issues and challenges in wireless sensor networks. It identifies the security threats, and review proposed security mechanisms for wireless sensor networks.

II. REVIEW AND ANALYSIS

Wireless sensor network (WSN) is a heterogeneous system combining thousands to millions of tiny, inexpensive sensor nodes with several distinguishing characteristics. It has very low processing power and radio ranges, permitting very low energy consumption in the sensor nodes, and performing limited and specific sensing and monitoring functions designing security protocols is a challenging task for a WSN because of the following unique characteristics:

1. Wireless channels are open to everyone and has a radio interface configured at the same frequency band. Most protocols for WSNs do not consider necessary security mechanisms at their design stage. Attackers can easily launch attacks by exploiting security holes in those protocols.
2. The constrained resources in sensor nodes make it very difficult to implement strong security algorithms on a sensor platform due to their complexity.
3. A stronger security protocol costs more resources in sensor nodes, which can lead to the performance degradation of applications.
4. A WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment.

Therefore, it may face various potential attacks. In this paper, the authors discussed the most common security services for WSNs. The paper was structured as follows. Then it focuses on the critical security issues in WSN. After that, it explores various threats and attacks compromising the availability of network services. Finally, it reviews the related works and proposed schemes concerning security in WSN. The security issues in WSN of a wireless sensor network can be classified as follows:

A. Data Confidentiality in networking is most challenging task in network security. The major problem is that radio spectrum is an open resource and can be used by anyone equipped with proper radio transceivers.

B. Data Authenticity is an assurance of the identities of communicating nodes. WSN communicates sensitive data to help in many important decisions making. Thus, it is very important for every node to know that a received packet comes from a real sender.

C. Data Integrity is to ensure that information is not changed in transit, either due to malicious intent or by accident. Thus, integrity is an assurance that packets are not modified in transmission. This is a basic requirement for communications because the receiver needs to know exactly what the sender wants her to know.

D. Data Freshness all information describes a temporary status of an object and thus is valid in only a limited time interval. Therefore, when a node receives a packet, it needs to be assured that the packet is fresh. Otherwise, the packet is useless because the information conveyed in it is invalid. Packet replaying is a major threat to the freshness requirement in network communications.

E. Availability is an assurance of the ability to provide expected services as they are designed in advance. It is a very comprehensive concept in the sense that it is related to almost every aspect of a network. The standard approach for keeping confidentiality is through the use of selective forwarding, multipath routing, etc. It was also explained the security threats and attacks in WSN:

A. Security Threats a 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. There can be many potential threats to WSNs; the categories of the threats could be (a) passive information gathering, (b) subversion of node or insertion of a false node, (c) node malfunction, (d) node outage, (e) message corruption, (f) denial of service, or (g) traffic analysis.

According to Karlof, threats in wireless sensor network can be classified into the following categories:

1. External versus internal attacks - the external (outsider) attacks is from nodes which do not belong to a WSN. An external attacker has no access to most cryptographic materials in sensor network.
2. Passive versus active attacks - passive attacks are in the nature of eavesdropping on, or monitoring of packets exchanged within a WSN. The active attacks involve some modifications of the data steam or the creation of a false stream in a WSN.
3. Mote-class versus laptop-class attacks - in moteclass (sensor-class) attacks, an adversary attacks a WSN by using a few nodes with similar capabilities as that of network nodes. In laptop-class attacks, an adversary can use more powerful devices like laptop, etc. and can do much more harm to a network than a malicious sensor node.

B. Attacks - wireless networks are more vulnerable to security attacks than wired networks, due to the broadcast nature of the transmission medium. These attacks are normally due to one or more vulnerabilities at the various layers in the network.

Attackers, intruders or the adversaries are the originator of an attack. The weakness in a system security design, implementation, configuration or limitations that could be exploited by attackers is known as vulnerability or flaw.

Interruption is an attack on the availability of the network, for example physical capturing of the nodes, message corruption, insertion of malicious code etc. Interception is an attack on confidentiality.

Modification means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted or causing a denial of service attack such as flooding the network with bogus data.

Fabrication is an attack on authentication. In fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed. Some of the critical attacks are categorized as follows:

1. Denial of Service (DoS) - is produced by the unintentional failure of nodes or malicious action. This attack is a pervasive threat to most networks.

2. Sybil - attack is defined as a malicious device illegitimately taking on multiple identities. In Sybil attack, an adversary can appear to be in multiple places at the same time. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve.

3. Sinkhole (Blackhole) - in sinkhole attacks, a malicious node acts as a blackhole to attract all the traffic in the sensor network through a compromised node creating a metaphorical sinkhole with the adversary at the center. The main reason for the sensor networks susceptible to sinkhole attacks is due to their specialized communication pattern.

4. Hello flood - 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 (termed as a laptop-class attacker) and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. In a HELLO flood attack, every node thinks that the attacker is within one-hop radio communication range.

5. 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. In the wormhole attack, an adversary (malicious nodes) eavesdrop the packet and can tunnel messages received in one part of the network over a low latency link and retransmit them in a different part.

There are also related works and security solution in WSN as reviewed by the authors some of the popular security solutions and combat some of the threats to the sensor networks are:

A. Security protocols for sensor networks (SPIN) was proposed by Adrian Perrig in which security building blocks optimized for resource constrained environments and wireless communication. SPINs has two secure building blocks: (a) sensor network encryption protocol (SNEP) and (b) µTESLA.

SNEP provides data confidentiality, two-party data authentication, and data freshness. µTESLA provides authenticated broadcast for severely resource-constrained environments. SNEP uses encryption to achieve confidentiality and message authentication code (MAC) to achieve two-party authentication and data integrity. µTesla is a new protocol which provides authenticated broadcast for severely resource-constrained environments.

In a broadcast medium such as sensor network, asymmetric digital signatures are impractical for the authentication, as they require long signatures with high communication overhead. µTESLA solves the following inadequacies of TESLA in sensor networks:

1. TESLA authenticates the initial packet with a digital signature, which is too expensive for our sensor nodes. µTESLA uses only symmetric mechanisms.

2. Disclosing a key in each packet requires too much energy for sending and receiving. µTESLA discloses the key once per epoch.

3. It is expensive to store a one-way key chain in a sensor node. µTESLA restricts the number of authenticated senders.

B. TINYSEC - TinySec is link layer security architecture for wireless network, which was designed by Karlof. It provides similar services as of SNEP, including authentication, message integrity, confidentiality and replay protection. TinySec provides the basic security properties of message authentication and integrity using MAC, message confidentiality through encryption, semantic security through an Initialization Vector and replay protection. TinySec supports two different security options: authenticated encryption (TinySec- AE) and authentication only (TinySec-Auth).

C. LEAP – a localized encryption and authentication protocol (LEAP) Protocol is a key management protocol for sensor networks. It is designed to support in-network processing and secure communications in sensor networks. LEAP provides the basic security services such as confidentiality and authentication. LEAP supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network. LEAP includes an efficient protocol for inter-node local broadcast authentication based on the use of one-way key chains. Key sharing approach of LEAP supports source authentication without precluding in-network processing and passive participation. It restricts the security impact of a node compromise to the immediate network neighborhood of the compromised node.

V. RECAPITULATION AND CONCLUSION

Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted a lot of attention in the recent years. The salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads. In this paper, we have introduced some security issues, threats, and attacks in WSNs and some of the solutions. Network security for WSNs is still a very fruitful research direction to be further explored.

VI. REFERENCES

1. Jun Zheng and Abbas Jamalipour, “Wireless Sensor Networks: A Networking Perspective”, a book published by A John & Sons, Inc, and IEEEE, 2009.

2. Shio Kumar Singh, M.P. Singh, and D.K. Singh, “A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks”, International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.

3. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks
(IJWMN), Aug. 2010, vol. 2, no. 3, pp. 49-61.

4. Shio Kumar Singh, M.P. Singh, and D.K. Singh, “Applications, Classifications, and Selections of Routing Protocols for Wireless Sensor Networks” International Journal of Advanced Engineering Sciences and Technologies (IJAEST), November 2010, vol. 1, issue no. 2, pp. 85-95.

5. Shio Kumar Singh, M.P. Singh, and D.K. Singh, “Routing Protocols in Wireless Sensor Networks – A Survey” International Journal of Computer Science and Engineering Survey (IJCSES), November 2011, Vol. 1, issue no. 2, pp. 63-83.

6. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Performance Evaluation and Comparison of Energy-efficient Routing Protocols for Wireless Sensor Network", Global Journal of Computer Application and Technology (GJCAT), Jan. 2011, vol. 1, no. 1, pp. 57-65.

7. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy Efficient Transmission Error Recovery for Wireless Sensor Network", International Journal of Grid and Distributed Computing (IJGDC), December 2010, vol. 3, no. 4, pp. 89-104.

8. E. Yoneki and J. Bacon, “A survey of Wireless Sensor Network technologies: research trends and middleware’s role”,

Technical Report, 2005. http://www.cl.cam.ac.uk/TechReports, ISSN 1476-2986.

9. J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security - a survey", Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press, 2007. 10. L.L. Fernandes,"Introduction to Wireless Sensor Networks Report", University of Trento. 2007, http://dit.unitn.it/~fernand/downloads/iwsn.pdf