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. 3, Issue. 7, July 2014, pg.208 – 213

RESEARCH ARTICLE

Comparison of Attacks on Wireless Sensor Networks

Jyotsna[1], Vikram Nandal[2]

[1]M.Tech, CSE Dept., R.N College of Engineering & Management

[2]Assistant Professor, R.N College of Engineering & Management

[1] jyotsnasharma1989@gmail.com, [2] vikramcselive.com

Abstract: Wireless sensor networks consist of individual nodes that are able to interact with the environment by sensing or controlling physical parameters. These nodes have to collaborate to fulfill their tasks. The nodes are interlinked together and by using wireless links each node is able to communicate and collaborate with each other. In this paper, we focus on security issues of WSNs; small survey on the main challenges of these networks, a wide variety of WSNs' attacks and a comparison between them. Also, this paper discusses known approaches of security detection and defensive mechanisms against the link layer attacks; this would enable IT security managers to manage attacks of WSNs more effectively.

Keywords: WSN, ad-hoc networks, security, attacks

I. INTRODUCTION

Wireless sensor network is often deployed in an open environment, even the enemy-occupied domain. As sensor nodes transfer data through wireless communication link, the network can be easily captured and invaded. Due to the lack of foundation infrastructure like wired network, what wireless sensor networks face not only traditional security threats but also some attacks which include the exhaustion attack, selective forwarding-attack, wormhole-attack, collision attack, sinkhole-attack, Sybil attack, hello-flood-attack, etc… Besides, each sensor node has limited energy and processing capability, small storage capacity and low bandwidth, this put forwards a larger challenge for the security of wireless network. Energy consumption has been considered as the single and important design key in sensor networks, hence, the most recent work on medium access control (MAC) protocol for sensor networks focused on energy efficiency, where MAC protocols play a crucial role in controlling the usage of the radio unit [6]. The radio transceiver unit is the major power consumer unit in the sensor node. For most MAC protocols designed for WSNs, it is assumed that the sensor nodes are stationary, which causes performance degradation when these

protocols are applied in mobile environments. Generally, an efficient MAC layer protocol for sensor networks should have the following attributes:

- The protocol should be scalable since most applications of sensor networks involve a large set of sensor nodes.
- Collisions among the transmissions of various nodes should be avoided. Collisions lead to packet drop and thus reduce throughput and cause energy wastage.
- Energy consumed by the radio circuit in idle mode is almost equal to that consumed in active state. Consequently, idle mode of operation and transmission overhearing among sensors should be minimized.
- To limit energy consumption during idle time, the sensors are typically switched to a sleep mode when not in use. However, active to sleep transitions and vice-versa consume considerable amount of energy. Therefore, an efficient protocol should minimize such transitions [4].
- Control packets overhead and active sensing of the medium, typically performed by contention-based protocols, are inefficient in terms of energy consumption. So, the protocol should not be contention-based.
- Packet drop due to limited buffer capacity should be prevented.
- The protocol should adapt to changes in the network topology and all sensors should have a fair chance of transmitting.

The main purpose of this paper is presenting an overview of different link layer attacks on WSNs and comparing them together. In this paper, we focus on security of WSNs, the threat model on WSNs, wide variety of WSN's link layer attacks and comparison of them.

II. SECURITY IN WSNS

Security in WSNs is an important, critical issue, necessary and vital requirement because WSNs are vulnerable against security attacks (broadcast and wireless nature of transmission medium); some issues in WSN can be broadly classified into three groups [6], namely, node system, middleware services, and communication protocols, as shown in Figure 1.

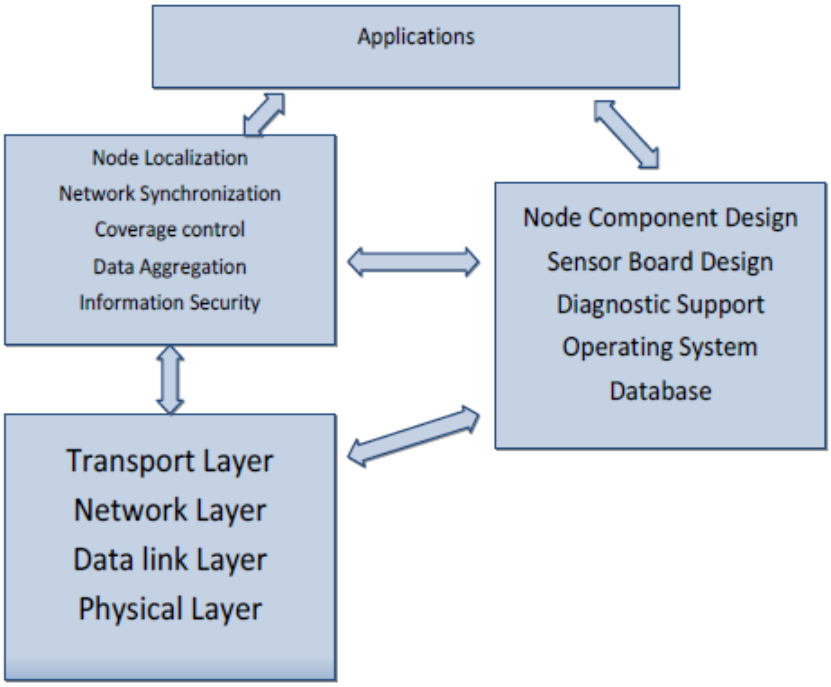

Fig 1: A categorization of key research issues in sensor networks

WSNs are vulnerable to many kinds of attacks; some of the most important reasons are:

- Theft (reengineering, compromising and replicating),
- Limited capabilities (DoS attacks risks, constraint in using encryption),
- Random deployment (hard pre-configuration),
- Unattended nature

Security in WSNs is an important, critical issue, necessary and vital requirement. Intrusion techniques in WSNs are increasing; also there are many methods to disrupt these networks. In WSNs, data accuracy and network health are necessary; because these networks usually use on confidential and sensitive environments. There are three security key points on WSNs, including system (integrity, availability), source (authentication, authorization) and data (integrity, confidentiality). Most common challenges and constraints in WSNs; include:

- Deployment on open/dynamic/hostile environments (physical access, capture and node destruction);
- Insider attacks;
- Inapplicable/unusable traditional security techniques (due to limited devices/resources, deploying in open environments and interaction with physical environment);
- Ad-hoc based deployment (dynamic structure and topology, self-organization);
- Resource scarcity/hungry (low and expensive communication/computation/processing resources);
- Devices with limited capabilities, pervasiveness (privacy worries), wireless (medium) and mobility;
- Unreliable communication (connectionless packet-based routing unreliable transfer, channel broadcast nature conflicts, multi-hop routing and network congestion and node processing Latency);
- Unattended operation (Exposure of physical attacks, managed remotely, no central management point);
- Increased attacks' risks and vulnerabilities, new attacks, increased tiny/embedded devices, multihopping routing (selfish);
- Immense/large scale (high density, scalable security mechanism requirement);
- Redesigning security architectures (distributed and self-organized);

III. ATTACKS ON WSNS

WSNs are vulnerable against many attacks. Therefore, we have to use some techniques to protect data accuracy, network functionality and its availability. As a result, we require establishing security in WSNs with attention to requirements and limitations of these networks. WSNs are designed in layered form; this layered architecture makes these networks susceptible and lead to damage against many kinds of attacks. For each layer, there are some attacks and defensive mechanisms. Thus, WSNs are vulnerable against different attacks, such as DoS attacks, Collision, unfairness and other attacks; WSNs are susceptible to link layer attacks. Attackers can gain access to transmission media, create radio interference, prevent from legitimate sensor nodes to communicate/transmit (access to the communication channel) or launch DoS attacks against link layer. In table 1, we have classified and compared attacks based on strategies and effects.

Attack/criteria	Attack definition	Attack techniques	Attack effects
Collision	• Message transmission by two nodes on a same frequency [1,5], simultaneously; • There are 2 types collision: environmental and probabilistic collision;	• Environmental collision; • Probabilistic collision; • Verifying and isolate radio transmissions; • Change packet's fields; • Alter the ack message;	• Interferences [1]; • Data/control packets corruption/cripple [1]; • Discarding packets; • Energy exhaustion; • Cost effective;
Resource Exhaustion	Repeated collisions and continuous retransmission until the sensor node death;	• Continuously retransmission; • Interrogation attack (RTS/CTS); Message modification;	• Resources exhaustion; • Compromise availability;

		• Ack corruption/change;	
Sinkhole	• A special selective forwarding attack; • More complex than blackhole attack; • Attracting or draw the all possible network traffic to a compromised node by placing a malicious node closer to the base station and enabling selective forwarding; • Centralizing traffic into the malicious node; • Possible designing another attack during this attack;	• Luring or compromising nodes; • Tamper with application data along the packet flow path (selectiveforwarding); • Receiving traffic and altering or fabricating information; • Identity spoofing for a short time; • Using the communication pattern;	• Luring and to attract almost all the traffic; • Triggering other attacks, such as eavesdropping, trivial selectiveforwarding, blackhole and wormhole; • Usurp the base station's position; • Message modification; • Information fabrication and packet dropping; • Suppressed messages in a certain area; • Routing information modification/fake; • Resource exhaustion;
Eavesdroping	Detecting the contents of communication by overhearing/stealthy attempt to data;	• Interception; • Abusing of wireless nature of WSNs' transmission medium; • Using powerful resources and strong devices, such as powerful receivers and well-designed antennas;	• Launching other attacks (wormhole, blackhole); • Extracting sensitive WSN information; • Delete the privacy protection and reducing data confidentiality;
Wormholes	Tunneling and replicating messages from one location to another through alternative low-latency links, that connect two or more points (nodes) of the WSN with fast communication medium (such as Ethernet cable, wireless communication or optical fiber), by colluding two active nodes (laptop-class attackers) in the WSN, by using more powerful communication resources than normal nodes and establishing better real communication channels (tunnel);	• Compromising/luring nodes with false and forged routing information; • An attacker locates between two nodes and forwards messages between them; • Using out-of-band or high-bandwidth fast channel; • Wormholes may be used along with Sybil attack; • This attack may combines with selective forwarding or eavesdropping;	• Routing disruption / disorder (false routes, misdirection and forged routing); • False/forged routing information; • Confusion and WSN disruption; • Enable other attacks; • Exploiting the routing race conditions; • Change the network topology; • Prevention of path detection protocol; • Packet destruction/ alteration by wormhole nodes;
Denial of Service (DoS) attacks	• A general attack includes several types other attacks in different layers of WSN, simultaneously; • Reducing WSN's availability	Physical layer, link layer, routing layer, transport layer and application layer attacks techniques;	Effects of physical layer, link layer, routing layer, transport layer and application layer attacks;
De-synchronization	Disrupting the established connections between two legitimate nodes by re-synchronizing their transmission;	• Sending repeatedly forged or false messages; • Re-synchronizing transmissions;	• Disrupt communication; • Go out the synchronization; • Resource exhaustion;

IV. DETECTION AND DEFENSIVE STRATEGIES OF WSNS

In Table 2 a classification and comparison of detection and defensive techniques on WSNs is presented.

Table 2. Attacks on WSNs (classification based on detection and defensive mechanisms).

Attack/criteria	Detection methods	Defensive mechanisms
Collision	Misbehavior detection techniques;	• All countermeasures of jamming attack; • Error correction codes (such as CRC codes); • Time diversity;
Resource Exhaustion	Misbehavior detection techniques;	• Limiting the MAC admission control rate [1]; • Random back-offs; • Using Time-Division multiplexing; • limiting the extraneous responses; • Protection of WSN ID and other information;
Sinkhole	• False routing information detection; • Cooperating neighboring nodes to each other; • Tree structure and verify by tree; • Verify by Visual Geographical Map;	• Geographical routing protocols; • Learning global map (if nodes are static and at known location); • Scalability; • Probabilistic next hop selection; • leveraging global knowledge; • Verifying and to trust information that advertised of neighbor nodes; • Authentication, link layer encryption and global shared key techniques; • Routing access restriction (R); • Wormhole detection (W); • Key management (K); • Secure routing (S);
Eavesdropping	• Eavesdropping is a passive behavior, thus it is rarely detectable; • Misbehavior detection techniques;	• Access control; • Reduction in sensed data details; • Distributed processing; • Access restriction; • Strong encryption techniques;
Wormholes	• False routing information detection; • Wormhole detection; • Combinational methods; • Packet leashes techniques;	• Packet leach/leashes techniques; • MAD protocol and OLSR protocol; • Directional antennas; • Multi-dimensional scaling algorithm (scalability); • Using local neighborhood information; • DAWWSEN protocol; • Designing proper routing protocols (clustering-based and geographical routing protocols); • leveraging global knowledge; • Verifying information that announce of neighbor nodes; • Graphical Position System; • Ultrasound;

		• Global clock synchronization;
De-synchroniztion	Strong and un-forgeable authentication mechanisms;	• Strong authentication mechanisms; • Time synchronization, cooperatively; • Maintaining proper timing;
Denial of Service (DoS) attacks	Detection methods of physical layer, link layer, routing layer, transport layer and application layer attacks;	Defensive mechanisms of physical layer, link layer, routing layer, transport layer and application layer attacks;

V. CONCLUSION

In this paper, we analyzed different dimensions of WSN's security, presented a wide variety of WSNs' attacks and classified them; and compared the WSN's attacks based on different extracted features of WSN's and attackers' properties and finally their associated detection and defensive techniques against these attacks to handle them. This work makes us enable to identify the purpose and capabilities of the attackers; also the goal, final result and effects of the attacks on the WSNs' functionality. As a result, one can take better and more extensive security mechanisms to design secure WSNs.

REFERENCES

[1] Zhenwei Yu, Jeffrey J.P. Tsai,A Framework of Machine Learning Based Intrusion Detection for Wireless Sensor Networks, IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing,2008.
[2] W. Znaidi, M. Minier and J. P. Babau; An Ontology for Attacks in Wireless Sensor Networks; INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (INRIA); Oct 2008.
[3] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on Its Security Threats," International Journal of Computers and Their Applications, Special Issue on "Mobile Ad-hoc Networks", Vol. 1, 2010, pp. 42-45.
[4] K. Xing, S. S. R. Srinivasan, M. Rivera, J. Li and X. Z. Cheng, "Attacks and Countermeasures in Sensor Networks: A Survey," Network Security, Springer, Berlin, 2010, pp. 251-272. doi:10.1007/978-0-387-73821-5_11.
[5] T. A. Zia, "A Security Framework for Wireless Sensor Networks," PhD Thesis, University of Sydney, Sydney, February 2008.
[6] G. Padmavathi and D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," International Journal of Computer Science and Information Security, Vol. 4, No. 1-2, 2009, pp. 115-119.
[7] T. Kavitha and D. Sridharan, "Security Vulnerabilities in Wireless Sensor Networks: A Survey," Journal of Information Assurance and Security, Vol. 5, 2010, pp. 31-44.
[8] Z. Li and G. Gong, "A Survey on Security in Wireless Sensor Networks," 2011. http://www.cacr.math.uwaterloo.ca/techreports/2008/cacr2008-20.pdf
[9] A. Dimitrievski, V. Pejovska and D. Davcev, "Security Issues and Approaches in WSN," 2011 http://ict-act.org/ICT Innovations.../ictinnovations 2009_submission_21.pdf.
[10] T.V. Dam and K. Langendoen: An adaptive energy-efficient MAC protocol for Wireless Sensor Networks, in SenSys '03. New York, NY, USA: ACM Press, pp. 171–180, 2003.
[11] W. R. Heinzelman, J. Kulik, and H. Balakrishnan. Adapti ve protocols for information dissemination in wireless sensor networks. In Proceedings of MobiCom'99, pp. 174–185, Seattle, WA, USA, August 1999.

