Wireless Sensor Network Security Issues

ANSHU SAGAR1, MISS NAMRATA KASHYAP2

[1]*CCSIT, TEERTHANKER MAHAVEER UNIVERSITY, MORADABAD U.P*

[1]anshusagar1231@gmail.com

namratakshp@gmail.com

Abstract-***This*** **work deals with some security issues over wireless sensor networks (WSNs). A survey of recent trends in general security requirements, typical security treats, intrusion detection system, key distribution schemes and target localization is presented. In order to facilitate applications that require packet delivery from one or more senders to multiple receivers, provisioning security in group communications ispointed out as a critical and challenging goal. Presented issues are crucial for future implementation of WSN.**

Keywords-Sensor, Security, Attack, Holistic, Challenge.

I. INTRODUCTION

NE of fundamental goals for Wireless Sensor Networks (WSNs) is to collect information from the physical world. Although a number of proposals have been reported concerning security in WSNs, provisioning security remains critical and challenging task. WSNs have attracted much attention due to its great potential to be used in various applications. Comparing to existing infrastructure – based networks, wireless sensor networks can virtually work in any environment, especially those where wired connections are not possible. Unlike conventional networks supporting mostly point-to-point or point-to-multipoint data forwarding, WSNs are often deployed to sense, process and disseminate information of targeted physical environments. WSNs are exploited to be deployed for a long period, and the nodes are likely to need software updates during their lifetime in order to support new requirements. In many cases the nodes will be inaccessible or too numerous to be physically accessed. This drives the need for software updates support

II. GENERAL SECURITY REQUIREMENT WIRELESS SENSOR NETWORKS

Because of the nature of wireless communications, resource limitation on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors, it is a challenge to provide security in WSNs. The ultimate security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. To provide secure communications for the WSNs,

WSNs have the general security requirements of availability,integrity,authentication,confidentialiy and non-repudiation. These security requirements can be provided by distribution mechanism with the requirements of scalability, efficiency key connectivity and resilience. Scalability is the ability to support large sensor nodes in the networks. Key distribution mechanism must support large network, and must be flexible against substantial increase in the size of the network even after deployment. Efficiency is the

consideration of storage processing and communications limitations on sensor nodes. Key connectivity is the probability that two or more sensor nodes store the same key or keying material. Enough key connectivity must be provided for a WSN to perform its intended functionality.

III. . TYPICAL SECURITY TREATS AND DEFENSE TECHNIQUES IN WIRELESS SENSOR NETWORK

Communications over wireless channels are, by nature, insecure and easily susceptible to various kinds of treats. A large-scale sensor network consists of huge number of sensor nodes and may be dispersed over a wide area. Typical sensor nodes are small with limited communication and computing capabilities. These small sensor nodes are pervious to several key types of treats.

For a large-scale sensor network, it is impractical to monitor and protect each individual sensor from physical or logical attack. Treats on sensor networks can be classified into attacks on physical, link (MAC), network, transportation, and application layers.

WSNs have the general security requirements of availability, integrity, authentication, confidentiality and nonrepudiation. These security requirements can be provided by distribution mechanism with the

requirements of scalability, efficiency key connectivity and resilience. Scalability is the ability to support large sensor nodes in the networks. Key distribution mechanism must support large network, and must be flexible against substantial increase in the size of the network even after deployment. Efficiency is the consideration of storage processing and communications limitations on sensor nodes. Key connectivity is the probability that two or more sensor nodes store the same key
or keying material. Enough key connectivity must be provided for a WSN to perform its intended functionality. Resilience is about the resistance against node capture.

TABLE I

TYPICAL TREATS IN WSN

Treat	Layer	Defense techniques
Jamming	Physical	Spread-spectrum, lower duty cycle
Tampering		Tamper-proofing, effective key management schemes
Exhausting	Link	Rate limitation
Collision		Error correcting code
Route infor. manipulating	Network	Authentication, encryption
Selective forwarding		Redundancy, probing
Sybil attack		Authentication
Sinkhole		Authentication, monitoring, redundancy
Wormhole		Flexible routing, monitoring
Hallo flood		Two-way authentication, three-way handshake
Flooding	Transport	Limiting connection numbers, client puzzles
Clone attack	Application	Unique pair-wise keys

1) Attacks in Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of One is the attack against the security mechanisms and another is against the basic mechanisms Here we point out the major attacks in wireless sensor networks.

- **Denial of Service**

Denial of Service (DOS) is produced by the unintentional failure of nodes or malicious action. The simplest DOS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. 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, 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 of traffic.

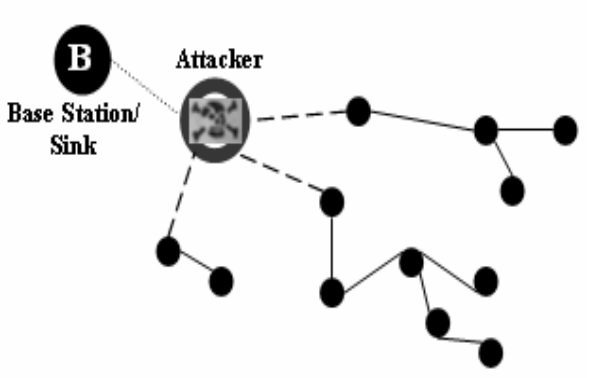
- **Attacks on Information in transit**

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks. As sensor nodes typically have short range of transmission and scarce resource, an attacker with high processing power and larger communication range could attack several sensors at the same time to modify the actual information during transmission.

- **Black hole/Sinkhole Attack**

In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious
is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations. The conceptual view of a blackhole/sinkhole attack.

Conceptual view of Black hole Attack



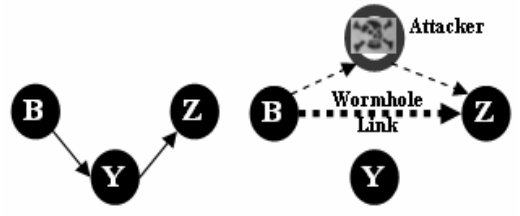
- **Hello Flood Attack**

Hello Flood Attack is introduced in [26]. This attack uses HELLO packets as a weapon to convince the sensors in WSN.

In this sort of attack an attacker with a high radio transmission (termed as a laptop-class attacker in [26]) range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, 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.

- **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. The tunneling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information.



Wormhole Attack

a and b shows a situation where a wormhole attack takes place. When a node B (for example, the base station or any other sensor) broadcasts the routing request 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 multihop 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 I GROUPCOMMUNICATIONS OVER WSNS

over WSNs. Zhu et al., proposed a key management protocol called a localized encryption and authentication protocol (LEAP) for large-scale distributed sensor networks, where each sensor node can establish pair-wise keys with its one-hop neighbor Multi-hop pair-wise key may be require to reach clusters heads and it can be done by each node generating a secret key and finding *m* intermediate nodes. The protocol is designed based on two observations: different packet types exchanged among sensor nodes require different security services, and a single key-management scheme may not be suitable for various security requirements.

authentication of one-hop broadcast communications among nodes with one-way key chains can mitigate the impersonation attack, while a time stamp is used to expire keys to prevent node capture and Sybil attacks.

V. SOFTWARE UPDATING IN WSNS

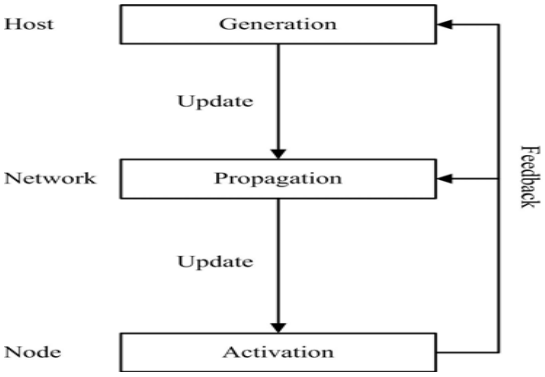
A critical issue in the effective deployment of these networks is the ability to update software after deployment. The WSNs related software include all application specific tasks and functions of the middleware to build up and maintain the network e.g., routing, looking for nodes, discovering services, and self-localization. There are a number of reasons why the software may require updating in a WSN. The Software Engineering Institute (SEI) at Carnegie-Mellon University identifies four categories of software updates for defendable systems, which help to provide an insight into these reasons: maintenance releases, minor releases, major releases (technology refresh), and technology insertion. Embedded wireless sensor systems programmed by specialists are likely to experience higher levels of maintenance than normal. Minor release will be used to improve data collection and performance. As the needs of

WSNs are likely to develop dynamically over time, major releases can be expected in response.
Wireless sensor nodes are characterized by very limited resources and by large-scale deployment Accessing these nodes in the field to perform software updates can be difficult to locate or inaccessible, or the scale of the deployment can preclude individual access.

1) Three key issues are:

- Avoiding interference with data collection while sharing the same communication infrastructure;
- Minimizing the cost of upgrades in terms of the impact on sensor network lifetime;
- Avoiding the loss of part or all of a sensor network due to an upgrade fault.

WSN software update model is shown in Fig. 3. The high level data – flow diagram highlights the interactions between the three key elements of software update functionality: generation, propagation and activation.



Software update model for WSNs

VI. CONCLUSIONS

Security in sensor networks has been an increasingly important issue for both academia and in industry individuals and groups working in this fast growing research area. In a WSN, physical security of wireless links is virtually impossible because of the broadcast nature and resource.

ACKNOWLEDGEMENT

We take this opportunity to express our profound gratitude and deep regards to our guide MISS **NAMRATA KASHYAP, Associate Professor, CCSIT** for his exemplary guidance, monitoring and constant encouragement throughout the course of this project. The blessing help and guidance given by their time to time shall carry me a long way in the journey of life on which we are about to embark.
We also take this opportunity to express a deep sense of gratitude to **Prof. Rakesh Kr. Dwivedi, Principal, CCSIT, TMU** for his cordial support, valuable information and guidance, which helped out in completing this task through various stages.

Lastly, we thank almighty, our parents, brother, sister, and friends for their constant encouragement without which this assignment would not be possible.

REFERENCES

[1] B. Krishnamashari, D. Estrin and S. Wicker, "Impact of Data
[2] Aggregation in Wireless Sensor Networks", Proc. 22nd International Conference Diatribe. Comp. Systems, Jul. 2002,
[3] [2] H. Luo, Y. Lin and S. K. Das, "Routing Correlated Data in Wireless Sensor Network: A Survey", IEEE Network, vol. 21, no.6, Nov/Dec. 2007,
[4] [3] K. Lu et al., "A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks", IEEE Transactions on
[5] Wireless Communications, vol. 7, no. 2, Feb. 2008
[6] [4] X. Du, and H-H. Chen, "Security in Wireless Sensor Networks", IEEE
[7] Wireless Communications, vol. 15, no. 4, Aug. 2008, Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842
[8] [5] Y. W. Law et al., "A Formally Verified Decentralized Key Management for Wireless Sensor Networks", Personal Wireless Communications, ser. Lecture Note in Computer Science, Springer Berlin/Heidelberg, Sept. 2003,
[9] [6] R. Ramen, J. Lopez, S. Gritzalis, "Situation awareness mechanisms for
[10] Wireless sensor networks ", IEEE Communication Magazine, vol. 46, n [7] R. Khanna and H. Lin, "Control Theoretic Approach to Intrusion
[11] Detection Using Distributed Hidden Markov Model", IEEE Wireless Communications, vol. 15, no. 4, Aug.
[12] M. Caddie and J. Wu, "Energy-Efficient Coverage Problems in Wireless Ad Hoc Sensor Networks", Computer Communications, vol. 29, no. 4,Feb. 2006,
[13] [9] B. Wang, et al., "Information Coverage and its Applications in Sensor Networks", IEEE Communications Letters, vol. 9, no.11, Nov. 2005,