Energy Depletion Attacks on Wireless Sensor Networks

FARZANA T
12MCS1004
Guided by: Mrs. Aswathy Babu C.A(Asst.Professor CSE Dept)

December 16, 2013

Abstract

Deployment of sensor network in hostile environment makes it mainly vulnerable to battery drainage attacks because it is impossible to recharge or replace the battery power of sensor nodes. Most of the research on this topic is revolved around security solutions using the layered approach. Here analysis is mainly focused on minimization of energy consumption at MAC layer and routing layer. This survey mainly focused on resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes battery power. These Vampire attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols.

Keywords: Wireless Senser Network, Denial of Service,multi-path routing, opportunistic routing, energy efficiency

1 Introduction

A wireless sensor network consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions such as pressure, temperature, sound, vibration motion or pollutants. WSN is used to locate not only the objects whose area of location is known but also the objects whose location is anticipated to be around a certain domain. Each node in a sensor network is typically equipped with a radio receiver, a small micro controller, energy source usually a battery. Sensor networks can be used for target tracking, system control and chemical and biological detection. Sensor networks are typically characterized by restricted power supplies, low bandwidth, small memory size and limited energy. This leads to a very demanding environment to provide security.

Sensor networks can be pushed to resource consumption attack. This means enemies would send data to drain a node battery and reduce network bandwidth. Sensor network is typically the cluster based and has irregular topology. Clusters are interconnected to the main base station. Each cluster contains a cluster head responsible for routing data from its corresponding cluster to a base station. Sensor networks often have one or more points of centralized control called base station. The wireless sensor node is equipped with a limited power source such as battery, sensor unit, processing unit, storage unit and wireless radio transceiver; these units communicate each other. A base station is typically a gateway to another network, a powerful data processing or storage center or an access point for human interface; communicating nodes are normally linked by a wireless medium such as radio.

2 Literature Survey

Most of the research on this topic is revolved around security solutions using the layered approach. In layered approach the protocol stacks consists of the physical layer, data link layer, network layer,

transport layer and application layer. These five layers and the three planes, i.e., the power management plane, mobility management plane and task management plane jointly forms the wireless layered architecture.Researches are always being conducted to improve the energy efficiency of the wireless Sensor Networks. Some of the approaches are described.

Michael Brownfield[1] discussed the energy resource vulnerabilities at MAC level and proposed a new G-MAC protocol to control the sleep awake pattern of sensor nodes. This scheme performs well in all traffic situations but deals only with MAC layer depletion attack.

Jing Deng, Richard Han, Shivakanth mishra[2] proposed an Intrusion tolerant routing protocol for WSN. INSENS constructs a forwarding table at each node to facilitate communication between sensor nodes and base station. It also provides multi path routing and minimize the communication,storage and computation requirements of sensor node at the expense of increased requirements at base station.

Fatma Bouabdullah, Nizar Bouabdullah,Raouf Bouabdullah [3] proposed a cross layer strategy that considers routing and MAC layers jointly. At routing level they proposed that sending data through multiple paths instead of using a single path, at MAC level limits the retransmission over each wireless links, but this scheme does not considers any attack.

Xufei Mao[4]. focused on selecting and prioritizing forwarder list to minimize energy consumption by all nodes but this method does not consider any attack at routing level.

Tapaliana Bhattasali[5] proposed an frame work based on distributive collaborative mechanism for detecting sleep deprivation attack increased energy efficiency but does not considers routing layer

E.Y Vasserman N. Hopper[6] proposed a new method for resource depletion attack at routing layer(Vampire attack), which permanently disable networks by quickly draining nodes battery power. Vampire attack is defined as the composition and transmission of a message that causes more energy to be consumed by the network than if a honest node transmitted a message of identical size to the same destination although using different packet headers. Here deals with 2 kinds of vampire attacks. They are stretch attack and carousel attack, then employs vampire attacks on an existing routing protocol PLGP during packet transmission phase. PLGPa is the new protocol to avoid this attack. Here a check is made before forwarding any packet to next hop. The node checks whether the hop distance is increasing or not, thus each node validates the path and can avoid the chance of attack.

3 Problem Definition

Since PLGP has 2 phases route discovery phase and packet forwarding phase, PLGPa is not vulnerable to vampire attacks during the forwarding phase,but cannot make the same claim about discovery phase. PLGPa includes path attestation increasing the size of every packet,incurring penalties in terms of bandwidth use, and thus radio power. Adding extra packet verification requirements for intermediate node increases processor utilization. Energy expenditure for cryptographic operations at intermediate hop is much greater than transmit or receive overhead. Only PLGP protocol is considered, how the proposed solution works in other routing protocol is not considered.

3.1 One possible solution

The main problem of PLGPa is overhead, since it use chain of attestations. Inorder to reduce this, change the encryption chain with single encryption.

4 Conclusion

The absence of infrastructure in WSN makes it difficult to detect security threats. Therefore security mechanism have to be designed with efficient resource

utilisation, especially power. The vampire attack discussed here explores the energy consumption attack that use routing protocols to permanently disable the network by depleting node's battery power. These attacks do not depend on particular protocols or implementations but rather expose vulnerabilities in a popular protocol classes. PLGPa, the first sensor network routing protocol that provably bounds damage from vampire attack by verifying that packets consistently make progress toward their destination.

References

[1] Michael Brownfield,Yatharth Gupta, "Wireless Sensor Network Denial of Sleep Attack", *Proceedings of 2005 IEEE workshop on information assurance,June 2005.*

[2] Jing Deng, Richard Han, Shivakanth mishra, "INSENS: Intrusion-Tolerant routing in Wireless Sensor Networks", *University of Colorado,Department of computer science Technical report,June 2006* .

[3] Fatma Bouabdullah, Nizar Bouabdullah,Raouf Bouabdullah "Cross-layer Design for Energy Conservation in Wireless Sensor Networks", *IEEE GLOBECOM 2008,New Orleans,USA,December 2008.*

[4] Xufei Mao,Shaojie Tang, Xiahua Xu, "Energy efficient Oppurtunistic Routing in Wireless Sensor Networks", *IEEE transactions on parellel and distributed systems, VOL. 12, NO. 2, February 2011*

[5] Tapaliana Bhattasali,Rituparna Chaki,Sugata Sanyal "Sleep Deprivation Attack Detection in Wireless Sensor Networks", *International journal of computer applications(0975-8887)vol 40-No: 15,February 2012*

[6] Eugene Y. Vasserman, Nicholas Hopper, " Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", *IEEE transactions on mobile computing, VOL. 12, NO. 2, February 2013*

[7] Yazeed Al-Obaisat,Robin Braun, "On Wireless Sensor Networks: Architectures,Protocols,Applications and Management", *Institute of Information and Communication Technologies,May 2004*

[8] B.Prano, M.Luk, E.Gustad, A.Perrig, "Secur Sensor Network Routing: A Clean-state Approach", *CoNEXT:Proc.ACM CoNEXT Conf.,2006*

[9] D.B. Johnson, D.A Maltz, J.Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Adhoc Networks", *Adhoc Networking, Addison Wesley, 2001*