IJCAT - International Journal of Computing and Technology
Volume 1, Issue 1, February 2014
www.IJCAT.org

Energy Depletion Attacks on Wireless Sensor Networks: A Survey

[1]Farzana T , [2]Aswathy Babu

[1] M.Tech Student in CSE, Calicut University, Kerala, India

[2] Asst. Professor in CSE, Calicut University, Kerala, India

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 and MAC layer, which permanently disable networks by quickly draining nodes battery power.

Keywords **- Wireless Sensor 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 [7].

Wireless sensor network have various applications like habitat monitoring, building monitoring, health monitoring, military surveillance and target tracking. All sensor nodes in the wireless sensor network interact each other or with intermediate nodes. Figure 1 shows the architecture of wireless sensor networks.

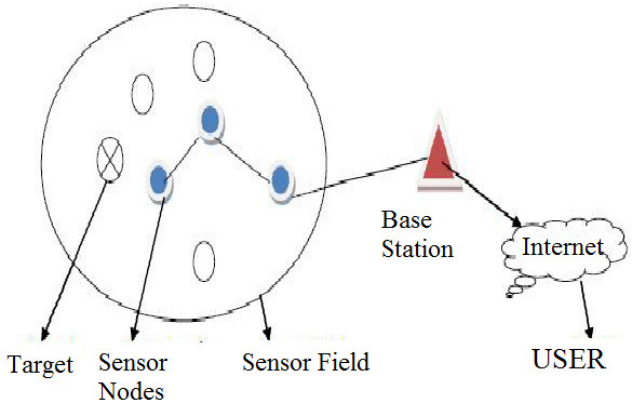

Fig. 1 Wireless Sensor Networks

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. Researchers are always being conducted to improve the energy efficiency of the wireless Sensor Networks. Some of the approaches are described. They are :

i. Wireless Sensor Network Denial of Sleep attack[1]
ii. Intrusion Tolerant routing in Wireless Sensor Network[2]
iii. Cross-Layer Design for Energy Conservation in Wireless Sensor Network[3]
iv. Energy Efficient Opportunistic Routing in Wireless Sensor Network[4]
v. Optimal sleep-wake scheduling for quickest intrusion detection using sensor networks[10]
vi. Sleep Deprivation Attack Detection in Wireless Sensor Network[5]
vii. Vampire Attack: Draining Life from Wireless Sensor Network[6]

2.1 Denial of Sleep Attack

Michael Brownfield [1] discussed the energy resource vulnerabilities at MAC level. Denying sleep effectively attacks each sensor node's critical energy resources and rapidly drains the network's lifetime so proposed a new G-MAC protocol to control the sleep awake pattern of sensor nodes. G-MAC has several energy saving features which not only show promise in extending the network lifetime, but the centralized architecture makes the network more resistant to denial of sleep attacks. This scheme performs well in all traffic situations but deals only with MAC layer depletion attack. G-MAC divides a frame into a collection period and a distribution period as shown in Fig.1.

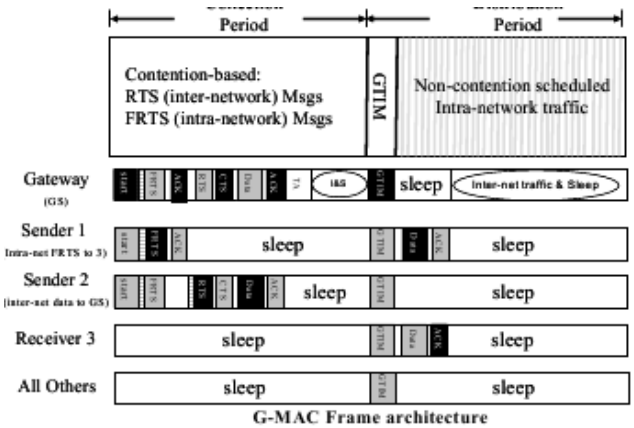

Figure 1 : G-MAC Frame Architecture

2.2 Intrusion Tolerant Routing

The 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. In INSENS each node shares a secret key only with the base station and not with any other nodes.

This has advantage in case a node is compromised that an intruder will only have access to one secret key rather than the secret keys of neighbors and other nodes throughout the network. It also provides multi path routing and minimizes the communication, storage and computation requirements of sensor node at the expense of increased requirements at base station.

2.3 Cross-Layer Design Approach

Fatma Bouabdullah, Nizar Bouabdullah, Raouf Bouabdullah [3] proposed a cross layer strategy that considers routing and MAC layers jointly. A network lifetime is time for the first node in wireless sensor network to fail. An efficient routing protocol would drain energy slowly and uniformly among nodes leading to the death of all nodes nearly at same time.

At routing level they proposed that sending data through multiple paths instead of using a single path so can balancing energy consumption. At MAC level limits the retransmission over each wireless links according to its property and the required packet delivery probability, but this scheme does not considers any attack.

2.4 Opportunistic Routing Method

Xufei Mao,Shaojie Tang, Xiahua Xu & Huadong Ma[4] focused on opportunistic method to minimize energy consumption by all nodes but this method does not consider any attack at routing level.

Opportunistic routing is based on the use of broadcast transmission to expand the potential forwarders that can assist in the retransmission of data packets. By this method nodes in the forwarder list are prioritized and the lower priority forwarder will discard the packet if the packet has been forwarded by a higher priority forwarder.

2.5 Optimal Sleep-Wake Scheduling for Quickest Intrusion Detection

Table 1

Sl no.	Methods	Affected OSI layers
1	Denial of sleep attack	MAC layer
2	Cross layer design	MAC and Routing layer
3	Energy efficient opportunistic routing	MAC layer
4	Optimal sleep-wake method	MAC layer
5	Sleep deprivation attack	MAC layer
6	Vampire attack	Routing layer

K.Premkumar and Anurag Kumar proposed a protocol that uses markov decision process models to identify the malicious nodes quickly with the use of minimal set of sensor nodes in active state. By using a minimal number of sensor devices, it ensures that the energy expenditure for sensing, computation and communication is minimized and so the lifetime of network is maximized.

2.6 Sleep Deprivation Attack

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. Sleep deprivation torture comes in the form of sending useless control traffic and forces the node to forgo their sleep cycles so that they are completely exhausted and hence stop working. Here workload is distributed among components according to their capacity to avoid complete exhaustion of battery power. Packet transmission overhead may high in some cases and its main advantage is it enhances energy efficiency and network scalability.

2.7 Vampire attack

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[8]. 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 distances is increasing or not, thus each node validates the path and can avoid the chance of attack.

3. Performance Analysis

The distribution nature and dynamic topology of wireless sensor networks introduces very special requirements in routing protocols that should be met. The most important feature of a routing protocol in order to be efficient for WSN is the energy consumption and the extension of network's lifetime. Following table shows how the different technique affects different OSI layers.

4. Conclusions

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 parallel 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

[10] K.Premkumar and Anurag Kumar, "Optimal sleep-wake scheduling for quickest intrusion detection using sensor networks ", IEEE explore, February, 2008.

Farzana T received the bachelor's degree in Computer science and engineering from the Calicut University, Kerala in 2008. Presently she is pursuing her M.Tech in the department of Computer Science and Engineering from Calicut University, Kerala. She has teaching experience of three and half years. Her research interests include wireless sensor networks, cryptography and network security, wireless security etc.

Aswathy Babu received bachelor's degree in Information technology from Cochin University of Science & Technology and M-Tech in Information and Communication engineering from Anna University,Chennai..She has a teaching experience of six years..Her research area include cryptography, cloud computing and wireless sensor networks