ENERGY DEPLETION ATTACK ON WIRELESS SENSOR NETWORK : A Survey

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

December 2, 2013

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

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.Some of such innovations are analysed here.

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

3 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.Here analyses the energy resource vulnerabilities of WSN at MAC level.The vampire attack discussed in this survey explores the energy consumption attack at routing layer.

References

[1] Anil K. Jain. Data Clustering : 50 years beyond K-means. *Pattern Recognition Letters Elsevier*, 31(8):651–666, 2010.

[2] Fahim A.M, Salem A.M, Torkey F.A and Ramadan M.A. An efficient enhanced k-means clustering algorithm. *Journal of Zhejiang University SCIENCE A ISSN 1009-3095 (Print); ISSN 1862-1775 (Online),www.springerlink.com*, 7(10), 2006.

[3] K.A.A. Nazeer and M.P. Sebastian. *Clustering Biological Data Using enhanced k-Means Algorithm.* Springer Netherlands, First edition, 2010.

[4] M.P.Sebastian and K.A. Abdul Nazeer. Improving the accuracy and efficiency of the k-means clustering algorithm. In *Proceedings of the World Congress on Engineering 2009* , Vol I July 2009.

[5] M.P.Sebastian, K.A. Abdul Nazeer and S.D.Madhu Kumar. Enhancing the k-means clustering algorithm by using a O(n logn) heuristic method for finding better initial centroids In *Second International Conference on Emerging Applications of Information Technology IEEE* , Feb 2011 pp. 261 –264.

[6] M.P.Sebastian, K.A. Abdul Nazeer and S.D.Madhu Kumar. A Heuristic k-Means Algorithm with Better Accuracy and Efficiency for Clustering Health Informatics Data *American Scientific Publishers Journal of Medical Imaging and Health Informatics* , 1:66–71, 2011.

[7] R.Sumathi and E.Kirubakaran. Enhanced Weighted K-Means Clustering Based Risk Level Prediction for Coronary Heart Disease *European Journal of Scientific Research* ,ISSN 1450-216X 71(4):490–500 2012 .

[8] Murat Erisoglu , Nazif Calis and Sadullah Sakalliogl. A new algorithm for initial cluster centers in k-means algorithm. *Pattern Recognition Letters Elsevier*, 32(14):1701–1705, October 2011.

[9] Damodar Reddya and Prasanta K. Janaa. Initialization for K-means clustering using Voronoi diagram. *Procedia Technology Elsevier*, 4:395–400, October 2012.

[10] T.H Sarma , P. Viswanath and B. Reddy. A hybrid approach to speed-up the k-means clustering method. *nternational Journal of Machine Learning and Cybernetics Springer-Verlag*, pp.1–11, January 2012.