

Applicability and Realization of Security in Leach Protocol in WSNs

Mrs Pooja Preet
Ph.D. Scholar, Department of Computer Application, IFTM University, Moradabad

Dr. Rahul Mishra
Professor, Department of Computer Application, IFTM University, Moradabad

Dr. Rajiv Suman
Assistant Professor, Department of Industrial & Production Engg. GBPUA&T, Pantnagar

Abstract
WSN is a collaborative network of a large number of loosely connected nodes. The intense deployment of such networks over varied topographic regions ranging from a few meters to several hundreds of kilometres is feasible by setting up small, low cost devices which are capable of monitoring the physical world around them by collecting status information and then converting this into radio signals. These signals are then transmitted to a local sink.
Keywords: WSNs, Leach, Noad etc.

1. Introduction

1.1 Wireless Sensor Networks

Since the dawn of the twenty first century, wireless sensor networks (WSNs) have spawned an increase in interest from industrial and research perspectives. WSN can be generally described as a network of nodes that cooperatively sense and may control the environment enabling interaction between persons or computers and the surrounding environment [**Verdone, 2008**]. In order to send the data to external networks such as Internet this local sink has to be connected to a gateway. Eventually the received data undergoes analysis and suitable decision/action is taken depending on the nature of application.

One of the key features of WSN that leads to its popularity is its ability to efficiently coalesce distributed sensing and computing with wireless communication. WSN consists of a number of small individual devices (nodes), which sense their operating environment like temperature, humidity, gas, vibration, illumination, pressure etc. in harsh conditions. Other than this these nodes perform data fusion, make decisions as well as control actuators. They even self-configure and maintain a network topology. Apart from these responsibilities these nodes route requested data to “sink” nodes using multiple short hops which form gateways to other networks or are user interfaces. One of the best advantages of these nodes is that they have a very long battery lifetime (even years)

1.2 Security issues in WSNs

Security in sensor networks is complicated by the constrained capabilities of sensor node hardware and the properties of the deployment [Shi *et al*., 2004], [Sarma*et al*., 2006] and [Zhou *et al.,* 2008]. Following are certain grounds that lead to security issues in WSNs

- The overall outlay of the WSN should be as low as possible.
- Sensor nodes are prone to physical capture but for the reason like their intentioned low cost, the success of tamper-resistant hardware is improbable.
- Sensor nodes employ wireless communication which is predominantly simple to eavesdrop on.
- An adversary can easily inject malicious messages into the wireless network.
- Superior anti-jamming techniques for instance frequency-hopping spread spectrum and physical tamper proofing of nodes are normally impractical in a sensor network due to the prerequisites of greater design complexity and elevated energy consumption.
- Ad-hoc networking topology of WSN facilitates adversaries for various kinds of link attacks ranging from passive eavesdropping to active interfering. Moreover attacks on a WSN can approach from all directions and aim at any node resulting in disclosure of confidential information, snooping of message, impersonating nodes etc.
- Security also requires scaling to large-scale employments. The majority of existing standard security protocols were devised for two-party situations and do not scale to a great number of participants.
- There is a clash of interest between minimization of resource consumption and maximization of security level. A better solution in fact gives a good negotiation between these two.
- Since sensor nodes typically are strictly constrained, asymmetric cryptography are often too superior for several applications. Thus, a promising solution is to utilize more competent symmetric cryptographic options.

- Most security schemes employ symmetric key cryptography. For this use of keys for secure communication is required. Administrating key distribution is not inimitable to WSNs, but again limitations such as little memory capacity make many keying techniques impracticable.

1.3 LEACH

LEACH is one of the most popular clustering algorithms used in WSNs to increase the network lifetime **[Sabar**ish*et al*., 2012].LEACH is an adaptive, self organizing and clustering protocol. The main concept of LEACH protocol is the formation of clusters of the sensor nodes on the basis of the received signal strength. This protocol employs local cluster heads as routers to the sink in order to save energy since only cluster heads (CH) perform the transmissions rather than all sensor nodes. Figure 1 shows LEACH communication hierarchy.

LEACH pioneers the concept of Rounds. These rounds (Figure 2) consist of a setup phase and a steady-state phase and have predetermined duration. Even though there are synchronized clocks, the nodes are aware when each round starts.

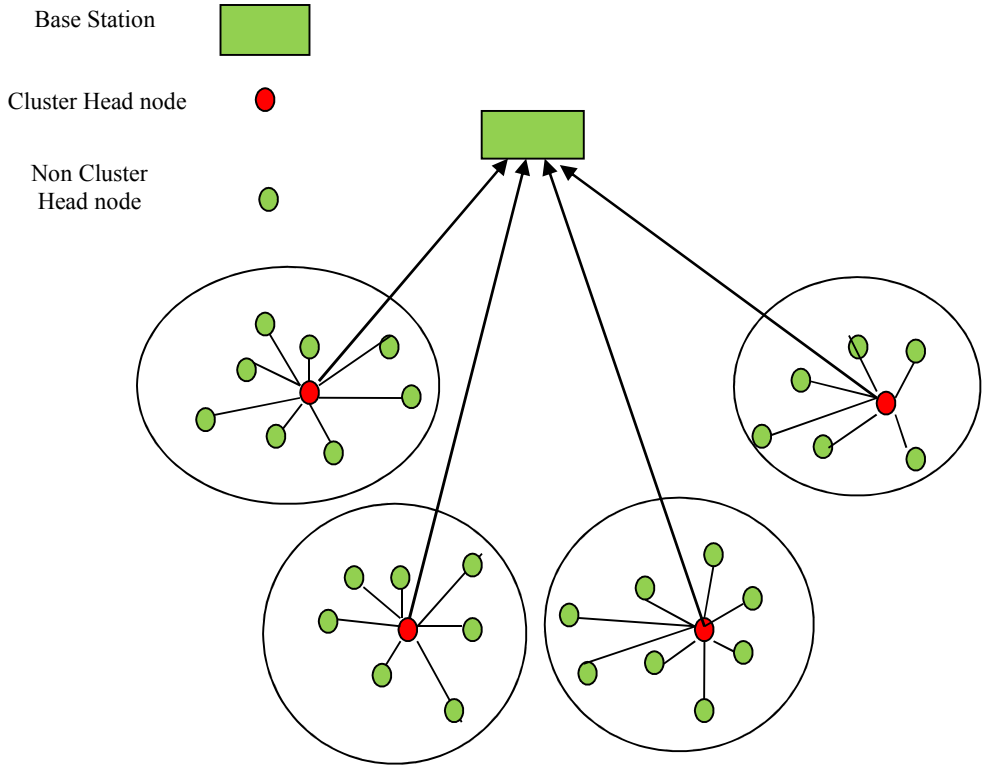

Figure 1: Illustration of LEACH protocol **[Javaid*et al*., 2012]**

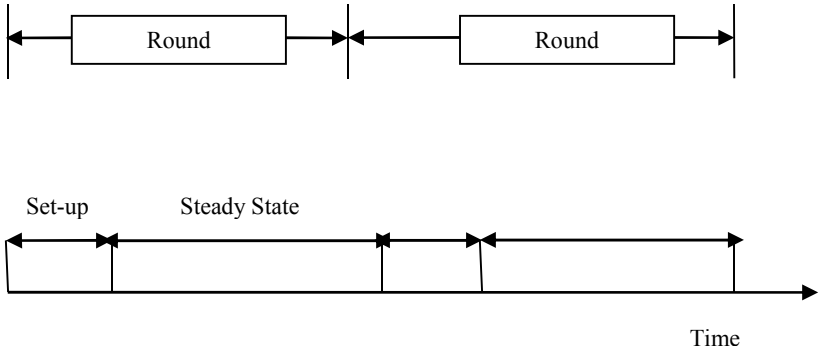

Figure 2: LEACH phases: setup and steady state phase **[Li *et al*., 2006]**

1.4 Motivation

Wireless sensor networks (WSNs) are budding as a technology for supervising different backgrounds of interest and they find relevance ranging from battlefield exploration to environmental protection. When implanted in significant applications, WSNs are most likely to be attacked. Aside from the familiar susceptibilities due to

wireless communication, WSNs lack physical security and are frequently deployed in open, unattended surroundings, which makes them exposed to attacks. It is thus essential to develop security solutions to these networks. The diverse network architectures demonstrate different communication models. Cluster-based organization has been projected for ad hoc networks in general and WSNs in particular. In cluster-based networks, nodes are normally organized into clusters and cluster heads (CHs) transmit messages from regular nodes in the cluster to the base stations (BSs). Clustered WSNs were first proposed for a variety of reasons including scalability and energy efficiency.

LEACH (Low-Energy Adaptive Clustering Hierarchy) is a self-organizing, adaptive clustering protocol that employs randomization to distribute the energy load consistently among the sensors in the network. In LEACH, the nodes arrange themselves into confined clusters, with one node acting as the local cluster-head. If the cluster heads were elected beforehand and fixed over time, it is easy to observe that the ill-fated sensors chosen to be cluster-heads would die quickly hence, ending the functional lifetime of all nodes belonging to those clusters. Thus, LEACH embraces randomized rotation of the high-energy cluster-heads so that it rotates among the different sensors in order to not consume the battery of a single sensor.

LEACH is also appealing in terms of security. This is due to the fact that the CHs which are more prominent targets for adversaries rotate from one node to another sporadically making it tougher for an adversary to recognize the CHs and compromise them. Thus applying security to LEACH protocols is difficult due to dynamic and periodic reorganizing of the network's clustering.

Hence, the project will include a detailed study of the various security approaches that have been proposed for LEACH-like protocols which will give an insight into the advancements that have taken place in the security domain in the field of WSNs. The proposed work will attempt to provide an energy efficient solution to ensure security in LEACH protocol in WSNs.

1.5 Problem Formulation

The characteristics of WSNs such as low-memory, limited energy and large-scale nodes make it unfeasible to employ the majority of the existing secure algorithms that were intended for powerful workstations. For instance, the working memory of a sensor node is inadequate to even hold the sufficient length variables that are required in asymmetric cryptographic algorithms **[Perrig*et al.*, 2002].** Thus, in order to ensure security in a WSN it is necessary to come up with an appropriate solution that provides a good compromise between two major conflicting requirements of resource consumption and security.

1.6 Challenges to deal with:

This includes:

- Security issues in Wireless Sensor Networks.
- Various security approaches in LEACH-like clustering protocols in WSNs.
- An energy efficient security solution (EES-LEACH) that combats blackhole attack in LEACH protocol.

References

1. Cheng Y. and Agrawal D., An improved key distribution mechanism for large-scale hierarchical wireless sensor networks, Ad Hoc Networks (Elsevier), Vol. 5, No. 1, pp. 35–48, 2007.
2. Eschenauer L. and. Gligor V. D, A key management scheme for distributed sensor networks, In Proc. of the 9th ACM conference on Computer and communications security (CCS'02), pp. 41-47, 2002.
3. Ferreira A. C., Vilaca M. A., Oliveira L. B., Habib E., Wong H. C., and Loureiro A. A. F., On the security of cluster-based communication protocols for wireless sensor networks. In 4th IEEE International Conference on Networking (ICN'05), volume 3420 of Lecture Notes in Computer Science, pages 449–458, Reunion Island, April 2005.
4. Gawdan I. S., Chow C. O., Zia T. A., Sarhan Q. I., A Novel Secure Key Management for Hierarchical Wireless Sensor Networks, In Proceeding of 2011 Third Conference on Computational Intelligence, Modeling and Simulation (CIMSiM), pp. 312 - 316, 2011.
5. Ibriq J. and Mahgoub I., A secure hierarchical routing protocol for wireless sensor networks, In: Proc. 10th IEEE International Conference on Communication Systems, pp. 1-6, 2006.
6. Javaid N., Rahim A., Nazir U., Bibi A., Khan Z. A., and Aslam M. S., Survey of extended leach-based clustering routing protocols for wireless sensor networks, Proc. IEEE 14th International Conference on High Performance Computing and Communication & IEEE 9th International Conference on Embedded Software and Systems, pp. 1232-1238, 2012.
7. Kausar F., Masood A. and Hussain S., An Authenticated Key Management Scheme for Hierarchical Wireless Sensor Networks, In Advances in Communication Systems and Electrical Engineering, Lecture Notes in Electrical Engineering, Vol. 4, pp. 85-98, 2008.
8. Lalitha T. and Umarani R., Energy efficient Cluster Based Key Management Technique for Wireless Sensor

Network, International Journal of Advances in Engineering & Technology (IJAET), Vol. 3 No. 1, pp. 186-190, 2012.
9. Li L., Jin S., Liu H. F., Cluster number variability problem in LEACH, in Ubiquitous Intelligence and Computing, Springer Berlin Heidelberg, pp 480-501, 2006.
10. Oliveira L. B., Ferreira A., Vilaca M. A., Wong H. C., Bern M., Dahab R., and Loureiro A. A. F., Secleach-on the security of clustered sensor networks, Signal Processing, Vol. 87, No. 12, pp. 2882–2895, 2007.
11. Perrig A., Szewczyk R., Wen V., Culler D., and Tygar J. D., SPINS: Security Protocols for Sensor Networks, Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.
12. Sabarish B. A., Guru M. S. M., Dhivya M. A., Naveen K. S., and Vaishnavi S., A survey on clustering protocols in wireless sensor networks, International Journal of Advances in Computing and Information technology, vol. 1, no. 2, 2012.
13. Sarma. H., Kar A., Security Threats in Wireless Sensor Networks, IEEE, pp. 243-251, 2006.
14. Shi E. and Perrig A. Designing Secure Sensor Networks, Wireless Commun. Mag., vol. 11, no. 6, pp. 38–43, Dec. 2004.
15. Tubaishat M., Yin J., Panja B., and Madria S., A secure hierarchical model for sensor network, ACM SIGMOD Record, Vol. 33, No. 1, pp. 7–13, 2004.
16. Verdone, R.; Dardari, D.; Mazzini, G.; Conti, A. Wireless Sensor and Actuator Networks; Elsevier:London, UK, 2008.
17. Wu D., Hu G., and Ni G., Research and improve on secure routing protocols in wireless sensor networks, In 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008), pp. 853–856, 2008.
18. Yin J. and Madria S., SecRout: A Secure Routing Protocol for Sensor Network, IEEE 20th International Conference on Advanced information networking and applications, Vol. 1, 2006.
19. Zhang K., Wang C., and Wang C., A secure routing protocol for cluster-based wireless sensor networks using group key management, In Proc. 4th IEEE International conference on Wireless Communications, Networking and Mobile Computing, pp. 1–5, 2008.
20. Zhou Y., Fang Y., Zhang Y. Securing Wireless Sensor Networks: A Survey, IEEE Communications Surveys & Tutorials, vol.10, issue 3, pp. 6 –28, Third Quarter 2008.