Chapter 62
Energy Consumption Analysis of Secure and Clustered Wireless Sensor Network

Ashim Pokharel
University of Turku, Finland

Ethiopia Nigussie
University of Turku, Finland

ABSTRACT

Due to limited energy resources, different design strategies have been proposed in order to achieve better energy efficiency in wireless sensor networks, and organizing sensor nodes into clusters and data aggregation are among such solutions. In this work, secure communication protocol is added to clustered wireless sensor network. Security is a very important requirement that keeps the overall system usable and reliable by protecting the information in the network from attackers. The proposed and implemented AES block cipher provides confidentiality to the communication between nodes and base station. The energy efficiency of LEACH clustered network and with added security is analyzed in detail. In LEACH clustering along with the implemented data aggregation technique 48% energy has been saved compared to not clustered and no aggregation network. The energy consumption overhead of the AES-based security is 9.14%. The implementation is done in Contiki and the simulation is carried out in Cooja emulator using sky motes.

1. INTRODUCTION

Wireless sensor networks are proliferating into our everyday life in the form of different applications, such as eHealth (Ho, ym., 2009; Honeine;Mourad;Kallas;Snoussi;Amoud;& Francis, 2011; Singh;Tiwary;Hoon-Jae;& Chung, 2009), environment and infrastructure monitoring (Yunseop;Evans;& Iversen, 2008), home automation(Langhammer & Kays, 2012; Tudose, ym., 2011; Zhang;Song;Wang;& Meng, 2011), traffic control (Laisheng;Xiaohong;Zhengxia;Bing;& Pengzhi, 2009; Zou;Yang;& Cao, 2009), agriculture (Vijayakumar & Rosario, 2011; Zhang Y., 2011)[29-30], and manufacturing(Bertocco;Gamba;Sona;& Vitturi, 2008;

DOI: 10.4018/978-1-4666-8751-6.ch062

Yamaji;Ishii;Shimamura;& Yamamoto, 2008). Most of wireless sensor networks have unique characteristics, such as the ability to withstand unfavorable environmental conditions, dynamic network topology, communication failures, large scale deployment, node mobility, unattended operation and limited energy resource. As energy is a limited resource in most cases, efforts need to be made to save energy in all operating conditions and network layers(Dargie & Pollebauer, 2010). The type of protocols and the selected parameters at different network layers play a vital role in energy consumption. Different strategies have been proposed in order to achieve better energy efficiency and organizing sensor nodes into clusters is among such solutions (Mamalis; Gavalas;Konstantopoulos;& Pantziou, 2009). The high density of the network may lead to multiple adjacent sensors generating redundant data. In order to solve this issue, data aggregation within clusters can be used to eliminate data redundancy and reduce communication load. Clustering can also reduce the number of nodes responsible for long distance transmission which helps in saving the network's power consumption.

Wireless sensor networks are vulnerable to attacks and the possible security attacks have different degree of impact to the system, such as jamming(Xu;Ma;Trappe;& Zhang, 2006), denial-of-service(Raymond & Midkiff, 2008), node compromise(Lin, 2009), impersonation attacks, and protocol specific attacks. Security can be considered as a non-functional requirement that maintains the overall system usable and reliable by protecting the information and information systems. Thus, security is of paramount importance, the network must be adequately protected against malicious threats that can affect its functionality. Due to the role of wireless sensor networks as sensing and actuating systems, any disturbances in such a network may have consequences in the real world. The communication between the sensor nodes can be secured by implementing energy efficient cryptography.

The main focus of this work is developing a secure communication channel between cluster heads and base station for transmission of aggregated data and analyzing its energy efficiency. In order to accomplish this, first clustering algorithm is implemented in Contiki operating system and the clustered network is simulated in Cooja network emulator to evaluate its energy efficiency. The next step involves developing of a secure architecture for the communication of aggregated data between cluster heads and base station by incorporating Advanced Encryption Standard (AES) protocol on the clustering algorithm. The energy overhead is analyzed after the implementation of encryption protocol and detailed comparisons are carried out.

2. NODES CLUSTERING IN WIRELESS SENSOR NETWORKS

Clusters are formed by putting together neighboring sensor nodes to work as a small team within a large network of wireless sensors. Many such clusters make up the entire network of wireless sensors. Each cluster has a leader usually called as the cluster head (CH). Clusters of wireless sensor nodes are formed in order to achieve sensor network scalability and better energy efficiency. Clusterization also helps to save the overall network energy this in turn prolongs the overall network lifetime in a large scale deployment of wireless sensor nodes. It is possible to gain significant energy saving through clusterization because it makes data fusion and aggregation possible and the cluster head is responsible for these tasks. The sensor nodes transmit the data periodically to their corresponding cluster heads. The cluster head aggregates the data coming from all the nodes in its cluster and then transmits it to the base station either directly or after communicating with other cluster heads in the entire network. In this approach the total number of packets relayed throughout the network is decreased considerably leading to energy conservation. However, since