Work Energy Modelling Link Layer Protocol on TinyOS and TinySec Based Wireless Sensor Networks with LEACH Method

Miftahur Rohman [1,*] Farid Baskoro[1]

[1] *Electrical Engineering State University of Surabaya Surabaya, Indonesia*
[*] *Corresponding author. Email: miftahurrohman@unesa.ac.id*

ABSTRACT
Monitoring the activities of the surrounding area using a wireless sensor network is very important to help support human work such as bridge surveillance, agricultural supervision, and others. Wireless sensor networks work in real time requiring a large amount of power source. In order for the wireless sensor network to work optimally and last, it is necessary to minimize the working energy of communication protocols on wireless sensor networks as in this study is a link layer protocol used for savings in the use of resources in wireless sensor network transmission systems. In large-scale use, wireless sensor networks use multiple nodes. In order to use less energy for the most efficient use of wireless sensor networks with many nodes, the most appropriate way to perform a clustering system that divides nodes into groups with each cluster there is a head cluster that serves as a data aggregation in each node member on their respective clusters. In this study the clustering system used the LEACH protocol. If a wireless sensor network uses multiple nodes, it is vulnerable to attack. To provide security in the wireless sensor network used Tiny Sec protocol based Tiny OS. So in performing energy minimization wireless sensor network protocol can also consider the security aspects of the sensor network. The parameters analyzed in this study are the relationship of the use of working energy with the lifetime of the sensor network. The data found in this study is with the addition of Tiny Sec, the power consumption and data used become minimal and the working energy that is able to survive by using 100 nodes and working energy 2 J then the maximum usage time is about 500 seconds.

Keywords: *Wireless Sensor Network, LEACH, Energy Modeling.*

1. INTRODUCTION

Supervision of area activities is an important thing to develop. Human life certainly affects the surrounding area. Lots of research has been done on the supervision of the surrounding area, one of which is agricultural supervision which is used to evaluate nutrient levels in the soil and soil moisture, supervision in industrial activities such as detection of machine errors and supervision of properties in industry, and monitoring activities. other. In this supervision, sensors are needed to be able to detect the activity of the area. However, in this monitoring, each sensor will communicate with other sensors and also with the access control center that forms a sensor network. In order to make the sensor network more effective in installation, wireless media is needed or what is called a wireless sensor network [1].

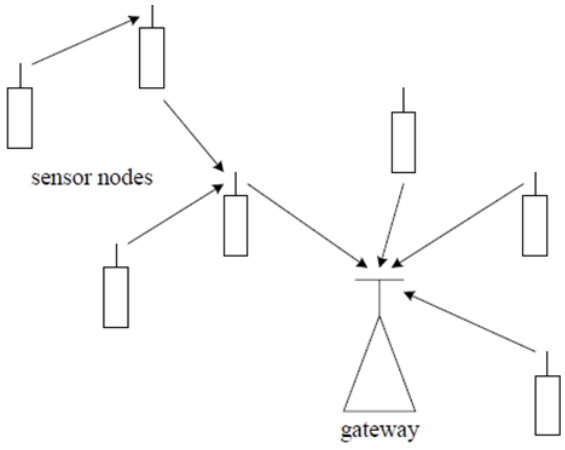


Figure 1 Illustration of a Centralized Wireless Sensor Network at the Gateway[1].

Wireless sensor network (JSN) is a network created specifically to carry out tasks related to area condition detection through wireless communication media. The wireless sensor network is a distributed and distributed sensor system with an integral part of the physical space with several components of the wireless sensor network [2]. The network is made up of two components, namely sensor nodes and sinks. The sensor node is an integral component of the network that gets information from the detection of the area. Sink is a unit that collects information from sensor nodes so that further information processing can be carried out.

There are several forms of sinks, namely sinks can be other sensor nodes in the form of sensors/actuators from the network itself or from other networks. The sink can also be a laptop/computer, a PDA, a smartphone, etc. that is used to interact with the wireless sensor network. Even sinks can be gateways to larger networks such as the internet so that interactions can be carried out over great distances and not directly connected to wireless sensor networks, which can be shown in Figure 1.

In supervising activities in the area, the wireless sensor network will work in real time. To run the wireless sensor network, of course, requires a resource so that the wireless sensor network can work. If the wireless sensor network works continuously, there will be a waste of resource use. In order for the wireless sensor network to work optimally and also last a long time, it is necessary to minimize the wireless sensor network protocol to save on resource use. If a wireless sensor network uses many nodes for certain purposes, then to be able to use energy more efficiently it is necessary to have a clustering system on several groups of nodes using a cluster head. The clustering system uses the LEACH protocol [3]. Wireless sensor networks with multiple nodes are vulnerable to malicious attacks from enemies. Information obtained from nodes is vulnerable to eavesdropping, information theft, changing information from enemies, and others. So to provide security in the wireless sensor network, the TinySec protocol is used [3]. Energy minimization in wireless sensor networks can also extend the life of wireless sensor networks [4].

In this study, we provide some background and models used for the WSN problems we investigate: minimum energy consumption issues, node clustering issues, data security issues and maximum network lifetime issues. In this study, we will demonstrate an energy minimization methodology using the LEACH protocol which divides the nodes into several clusters for energy minimization without regard to the data security system and the TinySec protocol which pays attention to the data security system. We discuss the performance and presentation of simulation results of energy minimization using LEACH and TinySec.

2. LITERATURE

2.1. LEACH Protocol Architecture

The LEACH approach is used to reduce the energy consumption of the wireless sensor network. Remote area monitoring is a typical use case for wireless sensor networks. Individual nodes in wireless sensor networks are typically linked to each other and so redundant information is not needed by the end user, but rather the end user who wants a high-level description of what is happening in the region. We decided to build LEACH on top of the clustering architecture because of the substantial correlation between data signals from nearby nodes. This reduces the amount of data that has to be transmitted to end users by allowing all of the cluster's nodes to analyze the data locally. Furthermore, aggregation techniques may be used to merge numerous linked data signals into a single data set comprising effective data, or the information content of each signal [6]. [7, 8]. It is therefore necessary to convey the real data from the cluster to the basestation (BS).

Based on the network model and sensor nodes, we establish various assumptions for LEACH. We assume that all sensor nodes are capable of transmitting with adequate power to reach the base station. Different MAC protocols may be supported and signal processing operations can be performed on each of a node's processors thanks to power regulation. Because of developments in radio technology and low-power processing, this is a fair assumption. There are nodes that always deliver data to end users, and those positioned near one another correlate data in such networks.

One node serves as the cluster leader in LEACH, which organizes its nodes into local groups. A cluster head node receives data from all member nodes, performs signal processing operations such as aggregation, and transmits data to a distant BS; non-cluster head nodes deliver data to the cluster head.

Being the cluster head node consumes a lot of energy, as opposed to a node that is not a cluster head node A set priority and lifespan for the cluster heads will soon deplete these nodes of their limited energy. When the cluster head runs out of energy, the nodes in the cluster lose their ability to communicate with each other. As a result, LEACH features a random movement of the cluster head's high-energy location between sensors in order to minimize battery drain. As a result, the cluster head's energy consumption is spread out evenly across the nodes.

Operations in LEACH are broken down into "rounds." As illustrated in Figure 2, each cycle begins with a setup phase when the cluster is assembled, followed by a steady state phase where data is transported from nodes to the cluster head and back to the BS. Figure 3 from LEACH shows the technique for selecting cluster

heads and for forming dispersed clusters, as well as the steady state operation. Wireless sensor networks require a strong protocol to grasp the essential characteristics for sensor applications. Adaptive Clusters can be constructed in a variety of ways during the initial set-up phase, and the nature of the sensor network protocol can be studied during the steady state phase [5].

2.1.1. *Ease of Distribution*

There may be large number of nodes in a sensor network and they may need to be put in distant or hazardous regions, enabling users to retrieve knowledge in ways that would otherwise be impossible. There must be a way for nodes to communicate in the absence of a network infrastructure and a fixed location.

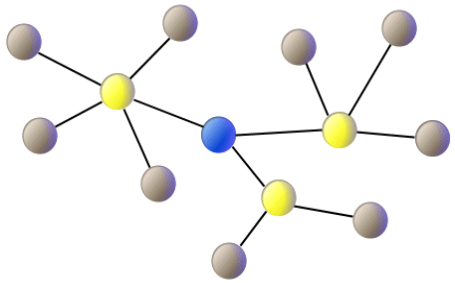


Figure 2 Sensor Network Clustering Network that uses 3 clusters.

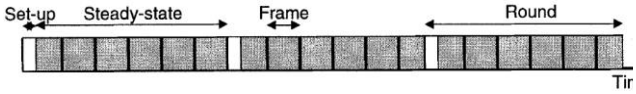


Figure 3 Timeline showing LEACH operations

2.1.2. *Lifetime System*

This network should function as long as possible. The sensor network is not possible to recharge the node battery. Therefore, all aspects of the node, from hardware to protocols, must be designed to be energy efficient.

2.1.3. *Latency*

Data from sensor networks is usually time sensitive, so it is very important to receive data in a timely manner.

2.1.4. *Quality*

It's a big difference between wireless sensor networks and wireless data networks when it comes to the quality of service. Data from surrounding nodes in sensor networks is strongly linked, thus it is unnecessary for end users to see it, and end users are more interested in high-level descriptions of events taking place in the monitored region. The quality of the sensor network depends on the quality of the aggregated data, thus protocols must be developed to maximize the sensor network's quality and specialized applications.

2.2. *Wireless sensor network link layer security protocol*

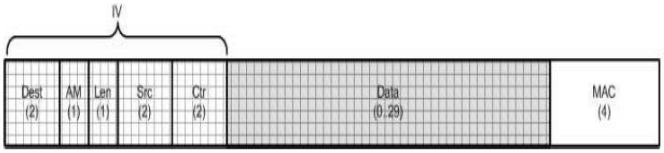
Communication between nodes in a sensor network is regulated by a protocol. Nodes on the network are protected from interference by MAC (Medium Access Control), which is a medium used for sending signals owned by each node without interference. As part of the OSI (Open System Interconnection) layer two, known as the data link layer, MAC serves as a means of transmitting data.

The network card manages the physical layer communication between the connecting systems with error management by encapsulating data into frames and transmitting them across the communication mediums. It also determines the format in which the data bits are arranged into. This level also includes error correction and flow management, as well as hardware addressing (e.g., Media Access Control Address / MAC Address), which govern how network devices such as hubs and bridges work. Split levels in the IEEE 802 standard The Logical Link Control (LLC) layer and the Media Access Control (MAC) layer [7] are the two outcome layers of this layer. There are a number of security protocols in use today, including LiSP [8], SPIN [9], TinySec [10], and others.

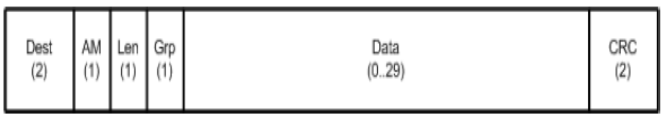
2.3. *TinyOS and TinySec*

Wireless sensor networks benefit from TinyOS, a modular operating system application. TinyOS' major goal is to give operational assistance while consuming the least amount of energy feasible. TinyOS was first developed at the University of California, Berkeley, where it is now being used. The TinyOS Open Technology Alliance, a group of private firms, as well as numerous academic institutions, contributed to the project's growth.

Many software components are included in TinyOS, including FIFO (First In First Out), which is used for radio transmission and other functions. A TinyOS program is not a binary kernel, but rather a collection of software components that are linked together in an efficient binary. TinyOS is also written in NesC [11], a descendant of C.



(a) TinySec AE Format Packet



(B) TinyOS Format Packet

Figure 4 TinySec AE format package and TinyOS package format with byte size of each field.

Many popular sensor node platforms, such as the MSP430, are supported by TinyOS. This has led to an increase in TinyOS's popularity.

Both encryption authentication (TinySec-AE) and authentication alone are supported (TinySec-Auth). When TinySec authenticates packets with MAC encryption, the data payload is encrypted. Encrypted data and packet headers are used to compute MAC. To authenticate a packet, TinySec uses MAC authentication, although the data payload is not encrypted.

SmallSec package format based on TinyOS's package format. Figure 4 shows that TinySec packets and TinyOS packets have distinct characteristics. TCP/IP port numbers are analogous to active message kinds. In order to extract and decode the message, the AM type provides the proper handler function for the recipient. Unencrypted communication is used in this area because it provides more benefits in terms of speed and security than encrypting a message would provide.

After recognizing that the message is not for it, the sensor node can employ initial rejection to switch off the radio. Initial rejection in the AM field can also be used with broadcast messages by nodes. It is not possible to call an initial refusal until the AM address and type have been decoded. If rejection occurs frequently in this situation, there will be energy waste. When using long field encryption, it is possible to determine the message length separately, which provides an additional layer of protection.

Tossim and PowerTOSSIM are incorporated into the TinyOS area, which includes a simulator named TOSSIM (Luo. et al, 2004) and an energy simulator. TOSSIM is a tool for reducing defects in programming, testing and analyzing algorithms in a controlled environment. PowerTOSSIM, which stands for TOSSIM, gives accurate estimations of nodes based on their power usage. Instrumentation of hardware peripherals such as the radio, EEPROM, LED and CPU in PowerTOSSIM provides a trail of each peripheral activity during run-time simulation. An energy model based on the Mica2 sensor node platform is provided by PowerTOSSIM (Heinzelman et al., 2002). For the TinySec project, there are four key goals:

Access management. In order to participate in the network, only nodes with a common group key are allowed.

Integrity. To accept a message, it must not be altered while in route. Attacks in which the adversary deliberately intercepts and alters and retransmits communications are prevented. Confidentiality. The message should not be deciphered by anybody who is not allowed to see it.

It's simple to use. With TinySec's wide range of network sensor users, it isn't difficult to utilize. To meet the needs of the above three reasons, TinySec can provide a set of communication channels.

3. SYSTEM MODEL

Figures Wireless sensor networks are modelled in this chapter by identifying the distribution of nodes, which can be as many as 100 nodes. The nodes are distributed in a random manner over a 100-square-meter region.

A cluster head serves as a gateway or data aggregation point for all nodes in the cluster and serves as a node-to-node communication link amongst the cluster members. The TinySec protocol must be used in the wireless sensor network to ensure the safety of data transmission. The wireless sensor network will next be analyzed in MATLAB and TinyOS. Figure 5 depicts the research process, whereas Table 1 lists the additional software specs employed.

Among the characteristics used to evaluate the wireless sensor network are the network's lifetime resistance to a large number of nodes, data transmission energy consumption, and network area.

The TinySec protocol was implemented and simulated in order to compare the energy usage of each device on the simulated network. The TinyOS system, which is already extensively used to control hardware resources and sensor devices by providing a user interface, is the primary component in this simulation.

TinyOS's TOSSIM and PowerTOSSIM modules, which simulate the network's status and estimate its energy usage, are shown in their fundamental system structure and function in this tutorial. In addition, the comparison approach is utilized to demonstrate the model's outcomes.

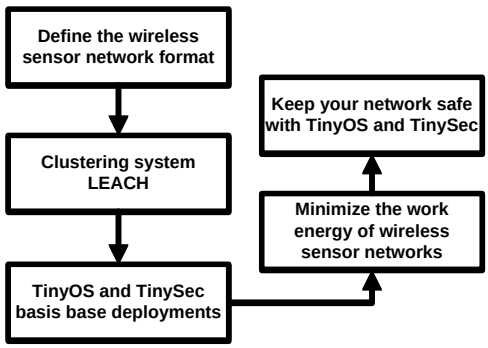


Figure 5 Research methodology.

Table 1 Simulation software specifications.

Software	Versi
Windows XP	SP 3
TinyOS	1.x
TOSSIM	Paket TinyOS 1.x
PowerTOSSIM	Paket TinyOS 1.x
TinySec	1.12 TinyOS

4. ANALYSIS OF SIMULATION RESULTS

From the analysis obtained using the LEACH protocol, it can be seen that with an energy of 2J (minimum energy and the number of nodes as much as 100 assuming a network area of 100×100 meters, the lifetime of the wireless sensor network will decrease in about 500 seconds. And when the network is the sensor will reach 650 seconds, energy will dissipate. Likewise with the combination of the LEACH and TinySec protocols which show that with the addition of security to the LEACH protocol with the TinySec protocol, the energy consumption or lifetime of the sensor network will also decrease when the time comes. 500 seconds and gradually disappears when the time reached is more than 650. Comparative analysis for the LEACH protocol without TinySec which can be shown in Figure 6 and the LEACH protocol with TinySec can be shown in Figure 7.

4.1. Work Energy Consumption

This simulation uses 20 nodes and 60 nodes for 1800 seconds. Simulations without a security algorithm are labeled with the TinyOS name while simulations with additional security use the TinySec label.

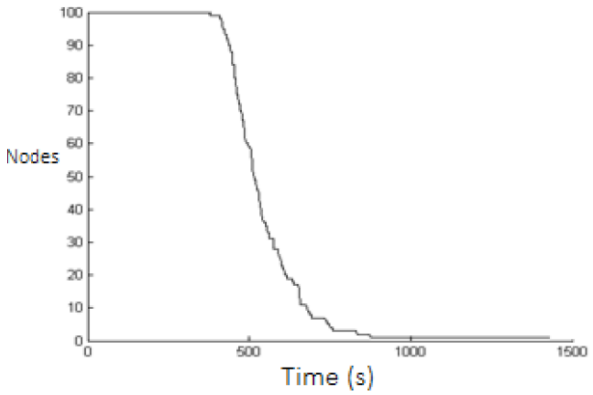


Figure 6 Graphical data of the LEACH protocol simulation with the energy of each node of 2 J.

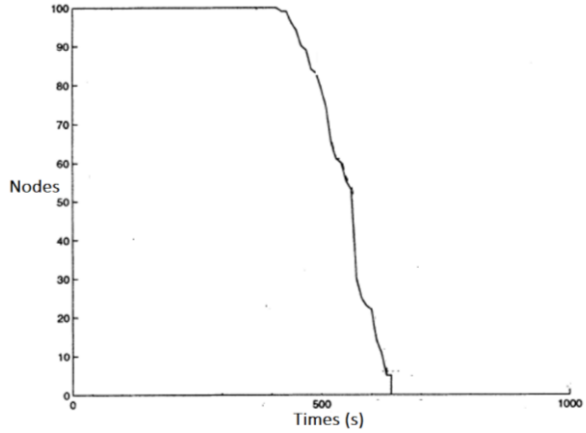


Figure 7 Graphical data of the LEACH protocol simulation using the TinySec protocol with an energy of 2 J for each node.

Figure 8 shows the simulation results of the average energy consumed per node for 1800 seconds. It appears that by using the security algorithm, nodes require an additional energy of 60 and 61 mJ for 20 and 60 nodes, respectively.

Figure 9 shows the total energy of all nodes. For 20 nodes, the energy difference between TinyOS and TinySec is 1.2 J, while for 60 nodes, the total energy difference is 3 Joules.

4.2. Memory Consumption

Based on the simulation results, Figures 10 and 11 show the value of RAM and ROM that must be allocated on the Mica2 platform that a wireless sensor network equipped with the TinySec feature requires larger data nodes and transmissions for node defense.

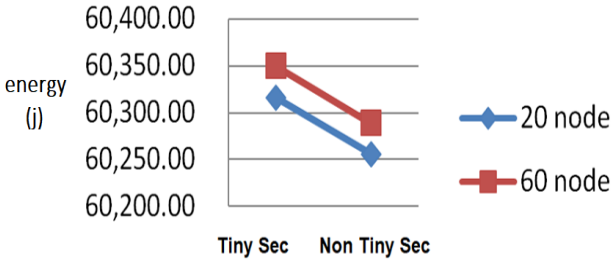


Figure 8 Average energy per node consumed for 1800 seconds.

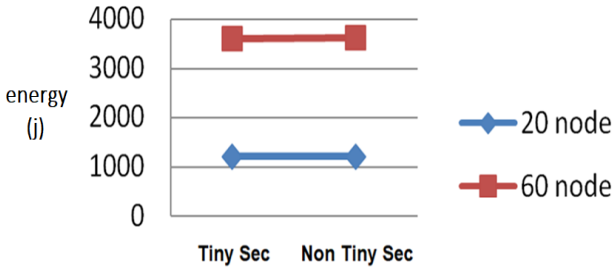


Figure 9 Total energy of all nodes consumed for 1800 seconds.

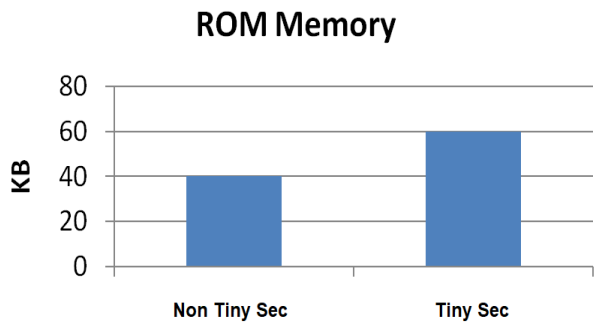


Figure 10 ROM memory allocation required during compilation process in KBytes (Mica2 platform).

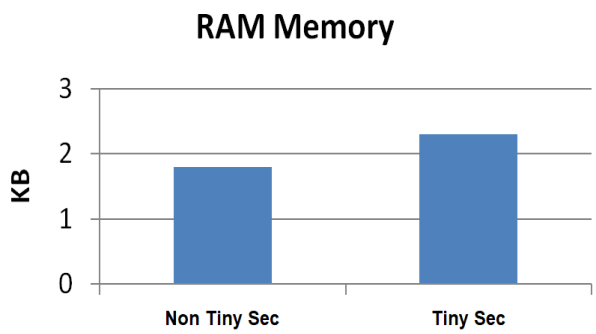


Figure 11 RAM allocation Required memory when compiling in KBytes (Mica2 platform).

5. CONCLUSION AND SUGGESTION

Many planning and operational problems in energy-limited wireless sensor networks must operate in conditions of nodes that are spread out in large numbers with distances between different nodes. The optimal solution used in energy minimization is the use of the LEACH protocol. However, the LEACH protocol still does not pay attention to the security side but is able to provide a more efficient transmission system by dividing a set of scattered nodes into several clusters with each cluster having a cluster head which functions as a data aggregator or data collector from member nodes and then transmitted to base station. This more efficient way can extend the life of the wireless sensor network. The use of the TinySec protocol as a complement to provide transmission system security at nodes in wireless sensor networks that previously used the LEACH protocol. In this paper it is shown that the use of the TinySec protocol for an operational time of 1800 seconds requires an additional energy of about 60 to 61 mJ.

REFERENCES

[1] Akyildiz, W. Su, Y. Sankarasubramaniam and Cayirci E, August 2002 A Survey on Sensor Networks, IEEE Communications Magazine.

[2] Raghavendra C S, Sivalingam K M, dan Znati T, 2006, Wireless Sensor Network, United States of America.

[3] Karlof C, Sastry N, dan Wagner D, 2004, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, Baltimore, Maryland, USA.

[4] Heinzelman W, Chandrakasan A dan Balakarishnan H, January 2000, Energy-Efficient Communication Protocols for Wireless Microsensor Networks, Proceedings of the Hawaaian International Conference on Systems Science.

[5] Heinzelman W, Chandrakasan A P, dan Balakrishnan H, October 2002 , An Application-Specific Protocol Architecture for Wireless Microsensor Networks, IEEE Transactions On Wireless Communications, Vol. 1, No. 4.

[6] Dong M, Yung K, dan Kaiser W, Aug. 1997, Low power signal processing architectures for network microsensors, in Proc. Int. Symp. Low Power Electronics and Design, Monterey, CA, pp. 173–177.

[7] Acharya V, 2006, TCP/IP and Distributed System, Golden House, Daryaganj, New Delhi.

[8] Park T and Shin K G, June 30, 2004, LiSP: A Lightweight Security Protocol for Wireless Sensor Networks, ACM-Transaction.

[9] Perrig A, Szewczyk R, Wen V, Culler D J. dan Tygar D, 2001, SPINS: Security Protocols for Sensor Networks, University of California, Berkeley, USA.

[10] Levis P, Lee N, Welsh M and Culler D, 2003, TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications, Proceedings of the 1st International Conference on Embedded Networked Sensor Systems, pp 126-137.

[11] Luo X, Zheng K, Pan Y, dan Wu Z, 2004 , Encryption Algorithms Comparisons for Wireless Networked Sensors, IEEE International Conference on Systems, Man and Cybernetics, pp 1142-1146.