COMPARISON OF SECURITY PROTOCOL IMPLEMENTATION MINISEC AND LISP ON THE WIRELESS SENSOR NTWORK

I Gusti Agung Gede Arya Kadyanan[1], Ida Bagus Made Mahendra[2], Ida Bagus Gede Dwidasmara[3], I Nengah Aryadi Suputra[4]

Informatics, Faculty of Math and Science, University of Udayana
South Kuta, Badung, Bali, Indonesia
[1]gungde@unud.ac.id
[2]ibm.mahendra@cs.unud.ac.id
[3]dwidasmara@unud.ac.id
[4]aryadisuputra@student.unud.ac.id

Abstract

There are many types of security protocols in wireless sensor networks. This requires a Security Analysis to choose what type of security protocol to apply to the network. Through this research expected to help security analysis in the collection of data and information for comparison of performance levels of both protocols and algorithms used. The system built is an implementation in the form of simulation. The simulation runs on NS3 software on Ubuntu 18.04 Linux Operating System. In this study, a third-party external library crypto++ was embedded to add security features such as encryption and authentication at the simulation stage. Simulation scenarios built for testing are based on two topologies to determine the performance of Minisec and LLSP security protocols. In the first topology used to measure the performance of Confidentiality, Integrity, and Authentication. The second topology is used to measure the energy consumption of both security protocols with the number of 10, 15, and 20 nodes. From the results of the study, it can be concluded that in the aspect of integrity and authentication obtained that both methods used by each security protocol can drop packages, and provide false message information on packages coming from unauthorized nodes. In the confidentiality aspect, both security protocols are able to hide plaintext and can guarantee the confidentiality of data in network simulations. In terms of total energy spent on the Minisec protocol averaged 1226,977 Joules, while the energy consumption of llsp averaged 1227.4067 Joules.

Keywords: *Wireless Sensor Network, Security Protocol, Minisec, LLSP, Confidentiality, Integrity, Authentication, Energy Consumption.*

1. Introduction

Wireless sensor network (WSN) is a technology that is being used lately, which can be used for research and can also facilitate daily life. The market predicts that by 2021, global shipments of wearable computing devices will reach 929 million, which will be a major driver of healthcare devices [1]. In today's era, there are many types of security protocols on wireless sensor networks. This requires a security analysis to select the type of security protocol to be applied to the network. Not only need to find the most secure security protocol, but also to understand the appropriate characteristics between the network and the necessary security protocols. If the network implementation that will be implemented prioritizes data security, then it is best to use security protocols that use authentication algorithms and complex encryption methods so that the data owned is not easily leaked to anyone. However, if the network to be implemented prioritizes battery power, it is better to use a simple security protocol. This is because more energy is usually consumed when more complex security protocols are implemented.

Due to the lack of information related to the wireless sensor network security protocol, and to facilitate security analysis to choose the correct security protocol to be applied in certain situations. In the application, whether it is a large project or a small project, it is necessary to view and analyze the security protocol. Because it relates to the top priorities of the necessary security protocols, such as energy efficiency or security. To compare between security protocols, security requirements are required. Requirements that need to be provided by WSN include integrity, authentication, and confidentiality [2].

2. Research Methods

2.1. Wireless Sensor Network

Wireless Sensor Network (WSN) is a network that connects devices such as node sensors, sinks, and routers. The device is ad-hoc connected, and supports multi-hop communication.

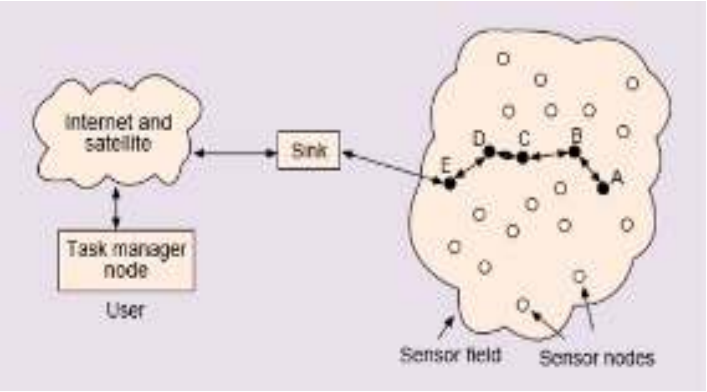

Figure 1. Wireless Sensor Network *[3]*

Sensor nodes are usually scattered on the sensor field as shown in Figure 6.1. Each scattered sensor node has the ability to collect data and route data back to the sink. Data can be redirected back on the sink by the multihop infrastructure architecture via sink. Then sink can communicate with task manager node via internet and satellite [3].

2.2. Security Protocol

Security protocol wireless sensor network is a network security that has the task of protecting information communicated through the network and resources from attacks on sensor nodes. Some Security Requirements of Wireless Sensor Network [4].

2.3. Minisec

MiniSec Security Protocol is a protocol that provides a high level of security, and accompanied by low power consumption. There are three techniques used to achieve this. The first is because of the encryption blocking method used to provide privacy and authentication. Second, vector initialization (or IV) is used as very few bits. Third, the basic gaps used during unicast and broadcast communication. In unicast mode, radio power consumption is reduced by making additional calculations and using synchronized counters. While in broadcast mode, a bloom filter mechanism is used. SkipJack is used as an encryption algorithm and OCB as encryption mode [5].

2.4. LLSP (Link Layer Security Protocol)

Security Protocol LLSP is a development of the TinySec protocol. The design of LLSP aims to be a more cost-effective protocol when it comes to energy consumption than TinySec. LLSP can reduce energy consumption by minimizing security overhead on each package. Similar to TinySec, LLSP also ensures security on authentication, confidentiality and integrity. However, there is one advantage in LLSP is that LLSP has replay protection. Replay Protection can prevent old messages from being sent back, so that the messages received are completely new messages and can maintain freshness data. To deal with confidentiality issues, the Advance Encryption Standard encryption method with chipper block chaining (AES-CBC) is used. As for authentication used MAC method, and for integrity aspect is CBC-MAC. In replay protection, the method used is to maintain a 4-byte counter between sender and receiver. Feedback shift register (FSR) is used to update the 4-byte counter [2].

2.5. Skipjack

Skipjack algorithm is one of the algorithms that can be used for data encryption, so the original data can only be read by someone who knows the encryption key. This algorithm uses the technique of cipher blocks with symmetric keys. Skipjack's algorithm is an algorithm developed by the U.S. National Security Agency (NSA), uses 80-bit keys to encrypt and decrypt 64-bit blocks, and uses Feistel's network structure with a total of 32 rounds.

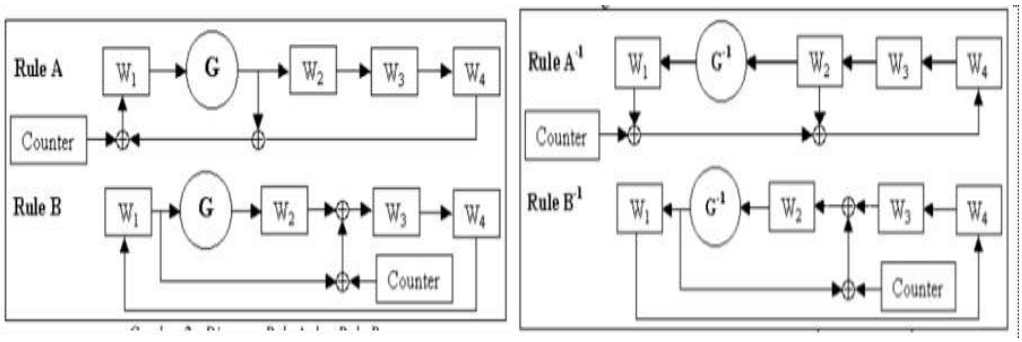

Figure 2. Encrypt skipjack (left) and Decrypt skipjack (right) *[6].*

2.6. AES

Advanced Encryption Standard (AES) is a development of DES (Data Encryption Standard). When DES was deemed to be ineligible for safety standards, NIST (National Institute of Standard Technology) held a competition to find a replacement for DES. Out of the 15 proposals that came in, eventually Rijndael's algorithm was chosen as the AES algorithm. As with DES, AES also uses substitution and permutation functions as well as a number of rounds that each use a different internal key. One of the differences between AES and DES is byte-oriented AES operations, unlike bit-oriented DES.

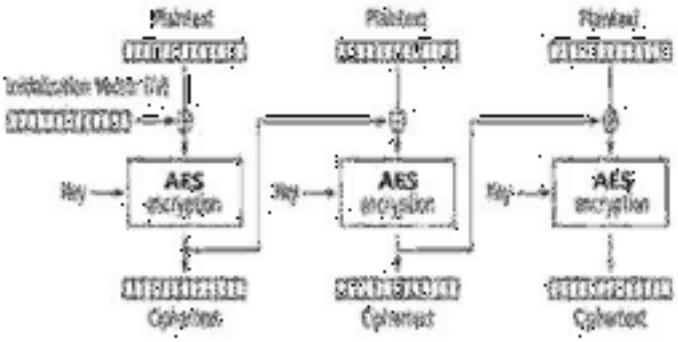

Figure 3. AES-CBC*[7]*

2.7. System Planning

The simulation runs on NS3 software on Ubuntu 18.04 Linux Operating System. The overall performance of the built system is illustrated by the flow diagram below.

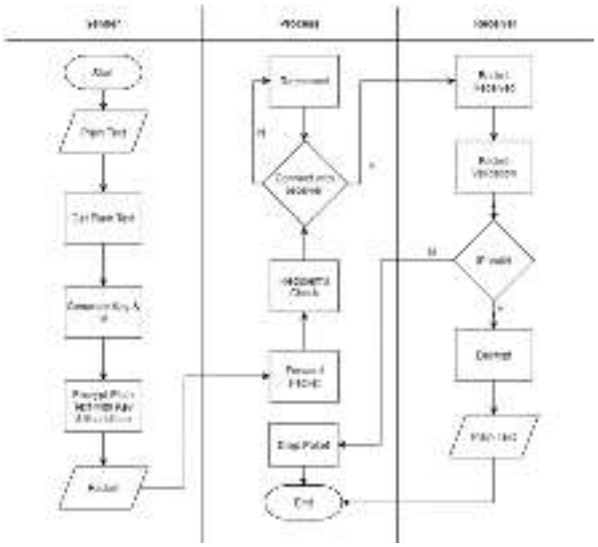

Figure 4. System design diagram flow

In this study, a third-party external library crypto++ was embedded to add security features such as encryption and authentication at the simulation stage. The addition of Crypto++ is due to ns3 having absolutely no security features. Third library embedding causes cryptographic implementations to be unable to be performed inside sensor nodes in simulations so energy and power consumption test results will not be fully accurate, but scaled down.

3. Result and Discussion

In the creation of this simulation program, it is built on the design of simulation stages and flowcharts that have been created before. In NS3 there are already modules and examples of scripts used to assist in the creation of this program. After the simulation of this program is made according to the design, then the simulation is run. After that will be obtained output containing the performance of both security protocols during the simulation run. The output of the simulation is a .xml file, and .pcap, then accompanied by an analysis stage.

Simulation Testing on confidentiality, authentication, and integrity aspects is created using NS-3 applications. Visualizations of the simulation will be shown using the NetAnim application, and the results of the attack process will be shown via a .pcap file. The encryption algorithm used in each security protocol will be implemented

using crypto++ library. In this test used topology as in figure 5. From the image, there are 18 sensor nodes. The blue node is the authorized node (normal node), while the red node is the unauthorized node (the attacker node). As seen in the image of normal nodes or blue ones numbering 15 nodes (0-14), then the attacker nodes or attack nodes numbered 3 nodes (15-17). Below is an exposure to the results of the test based on pre-defined scenarios and aspects of the test.

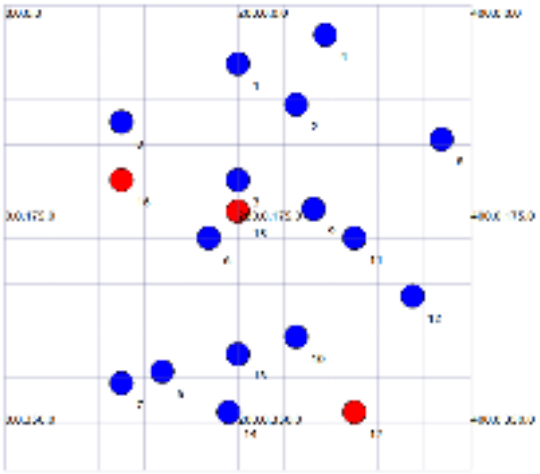

Figure 5. Network topology simulation

3.1. Confidentiality

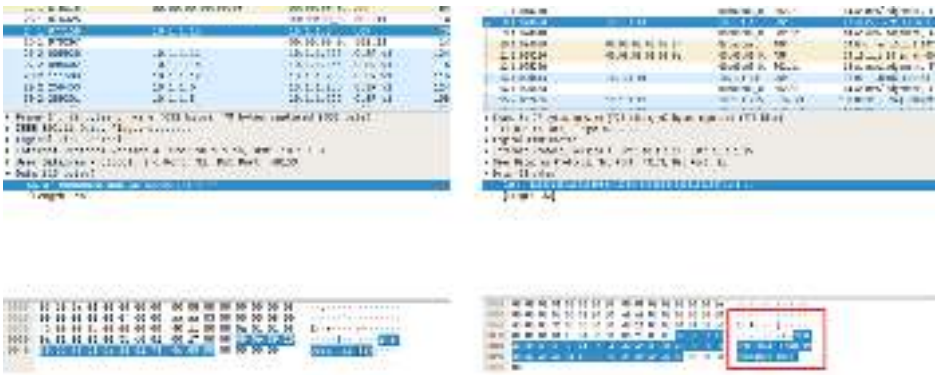

Figure 6. The result of sniffing process without encryption (left) and with LLSP protocol (right).

Based on the results of confidentiality aspect testing, both security protocols are able to hide plaintext and can guarantee the confidentiality of data in network simulations. However, according to Murat Dener's research [8], in high-level applications that require a lot of security, AES algorithms can be preferred over Skipjack algorithms. This is because skipjack algorithms that are 80 bit long, as well as AES algorithms seem more expensive than other algorithms due to the specific methods it uses for encryption. It is also concluded that 64-bit algorithms can be used until 1994, 80-bit algorithms through 2013, and 128-bit algorithms up to 2076 can be used in proportions created knowing that the 56-bit DES algorithm introduced in 1977 was broken in 1982.

3.2. Integrity and Authentication

Figure 7. The results display a fake minisec message (left) and with the LLSP protocol (right).

Based on the results of integrity and authentication aspect testing, it obtained both methods used by each security protocol can drop packages, and provide false message information on packages coming from unauthorized nodes or attack nodes.

Figure 8. Chipertext generated by Minisec (left) LLSP (right)

Figure 8 is obtained from the Follow UDP Stream analysis. This Follow UDP Stream feature is used to view data plan information. Based on the results of integrity and authentication aspect testing, it was obtained that both methods used by each security protocol can drop packages, and provide false message information on packages coming from unauthorized nodes or attack nodes.

3.3. Energy

In terms of energy consumption, a simulation was conducted for 1500 seconds. Testing conducted three times with the number of sensor nodes 10, 15, and 20. Figure 9 shows total energy consumption scenario of 10 nodes.

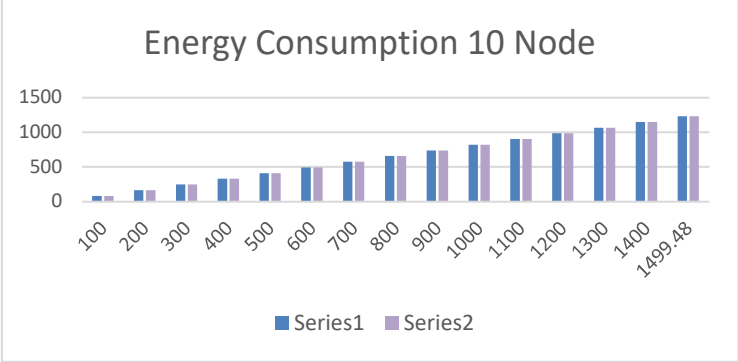

Figure 9. Graph of total energy consumption scenario of 10 nodes

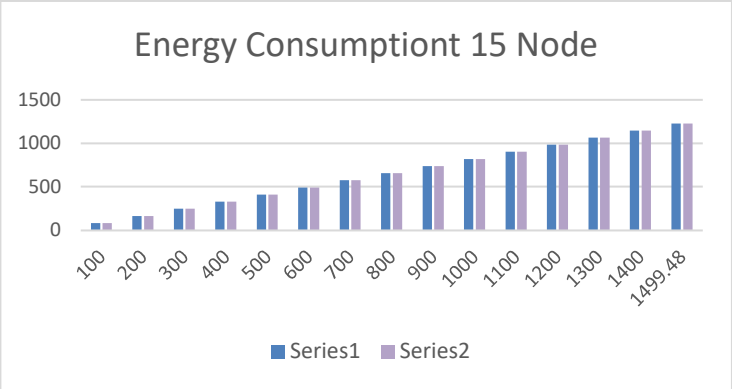

Figure 10. Graph of total energy consumption scenario of 15 nodes

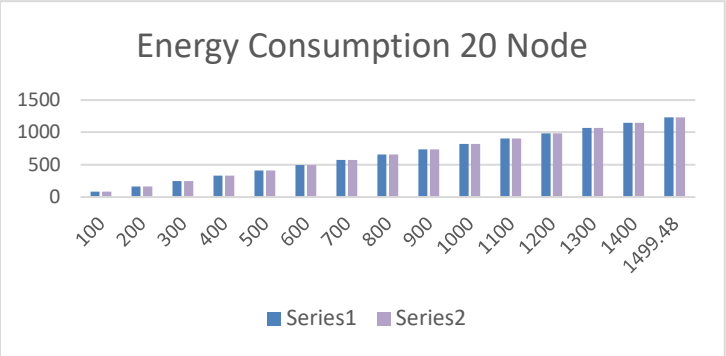

Figure 11. Graph of total energy consumption scenario of 20 nodes

Figures 7, 8, and 9 show the total energy consumption of each security protocol. The X axis represents the duration, and the Y axis represents the total energy in the joule. The blue diagram represents the Minisec security protocol, and the yellow diagram represents the LLSP security protocol. The results showed that through simulations of 10, 15 and 20 nodes, minisec security protocols consume less energy on average than LLSP security protocols. From the data above obtained the results of total energy spent on the Minisec protocol averaged 1226,977 Joules, while the energy consumption of llsp averaged 1227.4067 Joules. Then the average power consumption on minisec security protocol is 0.818444584666W, and LLSP is 0.818731416W.

4. Conclusion

From the research, it can be concluded the aspect of integrity and authentication obtained that both methods used by each security protocol can drop packages, and provide false message information on packages coming from unauthorized nodes. In the confidentiality aspect, both security protocols are able to hide plaintext and can guarantee the confidentiality of data in network simulation. In terms of total energy spent on the Minisec protocol averaged 1226,977 Joules, while the energy consumption of llsp averaged 1227.4067 Joules. Then, the average power consumption on minisec security protocol is 0.818444584666W, and LLSP is 0.818731416W. Minisec security protocol uses less power than LLSP security protocol with AES algorithm. This is because Minisec security protocol with skipjack algorithm can process up to 32 times fewer instructions, and can consume 3.5 times less ROM memory when compared to AES algorithm.

References

[1] C. C. Cheung, A. D. Krahn, and J. G. Andrade, “The Emerging Role of Wearable Technologies in Detection of Arrhythmia,” *Can. J. Cardiol.*, vol. 34, no. 8, pp. 1083–1087, 2018, doi: 10.1016/j.cjca.2018.05.003.

[2] R. Danuansa, F. A. Yulianto, and S. Prabowo, “Analisis Performansi Dan Simulasi Security Protokol Tinysec Dan Llsp Pada Wireless Sensor Network,” *eProceedings Eng.*, vol. 4, no. 1, pp. 1191–1197, 2017, [Online]. Available: file:///C:/Users/BANU/Zotero/storage/34JLNJ3M/3879.html.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–105, 2002, doi: 10.1109/MCOM.2002.1024422.

[4] A. Perrig, J. Stankovic, and D. Wagner, “S Ecurity in W Ireless S Ensor N Etworks ワイヤレスセンサネットワークにおけるセキュ リティ,” pp. 30–36, 2004.

[5] M. Dener, “Security analysis in wireless sensor networks,” *Int. J. Distrib. Sens. Networks*, vol. 2014, 2014, doi: 10.1155/2014/303501.

[6] Hartono, “Aplikasi Pengamanan Data Menggunakan Metode Skipjack,” *Stmik Ibbi*, no. 18, pp. 39–50, 2009.

[7] A. F. Ramdhansya, E. Ariyanto, and H. H. Nuha, “Implementasi Advanced Encryption Standard (Aes) Pada Sistem Kunci Elektronik Kendaraan Berbasis Sistem Operasi Android Dan Mikrokontroler Arduino,” *Semin. Nas. Inform.*, vol. 2014, no. semnasIF, pp. 92–98, 2014.

[8] M. Dener, “Comparison of Encryption Algorithms in Wireless Sensor Networks,” *ITM Web Conf.*, vol. 22, p. 01005, 2018, doi: 10.1051/itmconf/20182201005.