EMITTER International Journal of Engineering Technology
Vol.1, No.1, December 2013
ISSN: 2443-1168

Secure Ubiquitous Sensor Network based on Elliptic Curve MenezesQu Vanstoneas Status Data Supply of EnvironmentinDisaster Management

Ismed Jauhar, Amang Sudarsono,Mike Yuliana

Program Studi Teknik Telekomunikasi Departemen Teknik Elektro
Politeknik Elektronika Negeri Surabaya
Jl. Raya ITS, Sukolilo, Surabaya 60111, Telp:+62-31-5947280, Fax:+62-31-5946114
E-mail: ismed.jauh@gmail.com, amang@eepis-its.edu, mieke@eepis-its.edu

Abstract

Along with the many environmental changes, it enables a disaster either natural or man-made objects. One of the efforts made to prevent disasters from happening is to make a system that is able to provide information about the status of the environment that is around. Many developments in the sensor system makes it possible to load a system that will supply real-time on the status of environmental conditions with a good security system. This study created a supply system status data of environmental conditions, especially on bridges by using Ubiquitous Sensor Network. Sensor used to detect vibrations are using an accelerometer. Supply of data between sensors and servers using ZigBee communication protocol wherein the data communication will be done using the Elliptic Curve Integrated security mechanisms Encryption Scheme and on the use of Elliptic Curve key aggrement Menezes-Qu-Vanstone. Test results show the limitation of distance for communication is as far as 55 meters, with the computation time for encryption and decryption with 97 and 42 seconds extra time for key exchange is done at the beginning of communication .

Keywords: Ubiquitous Sensor Network, Accelerometer, ZigBee, Elliptic Curve Menezes-Qu-Vanstone

1. INTRODUCTION

The Changing of environmental conditions allows a disaster either natural or man-made objects and a bridge without no exception. It takes a monitoring system on a bridge that will supply the bridge condition status data in realtime. To supply the bridge condition data it will need a device that will detect pre-defined parameters. These devices will form a network called the Ubiquitous Sensor Network (USN) to connect between the devices to each other. The term "Ubiquitous" Ubique is derived from the Latin word

meaning "everywhere". USN is a realization in gathering information in real-time, wherever and whenever [1].

USN has a serious security problem because the process is done in a wireless communication device commonly used and should be easily accessible. Cryptographic algorithms are implemented as a security mechanism in Elliptic Curve Cryptography is the USN (ECC). ECC is an efficient security mechanism used on systems with low power[2]. System with guaranteed security and low power is a very reliable system for the communication process is done wirelessly.

In this study, it will be made a prototype system that is used to monitor the state of a bridge, where the system is equipped with a safety mechanism made using ECC. The sensors were placed on the bridge will send the bridge status conditions in real time to a server, so the condition of the bridge can be monitored at any time.

2. RELATED WORKS

In the study titled Bridge Condition Monitoring System using Wireless Network (CDMA and Zigbee)[3] it has been created a monitoring system from the condition of the bridge with the use of multiple sensors in its undertaking to the bridge. For communication between the sensor towards the data center used ZigBee andCDMA. Meanwhile, the study Efficient Implementation of Elliptic Curve Cryptography Using Low-power Digital Signal Processor[4] described the efficient use of Elliptic Curve Cryptography on devices that have low power.

In this study was created a prototype for bridge monitoring system by using a device that has the capability of computing and low energy supply and is equipped with a safety mechanism Elliptic Curve Cryptography .

3. ORIGINALITY

One of the operating system used to build a secure WSN using ECC is TinyOS [5]. Several previous studies have discussed about the low cost implementation on ECC in WSN [2], as well as the manufacture of secure ECC in WSN [1]. In this study, the scheme will be implemented on IEEE802.15.4 WSN security device, namely the Intel Mote2 platform [5] to build the security mechanism Elliptic Curve Integrated Encryption Scheme and on the use of Elliptic Curve key aggrement Menezes-Qu-Vanstone. This security mechanism is used for a supply system status data of environmental conditions, especially on bridges .

4 . DESIGN SYSTEM

4.1 ECC (Elliptic Curve Cryptography)

Elliptic Curve Cryptography (ECC) has emerged as a public-key cryptosistem suitable for mobile or wireless application, including the application of the USN. ECC offers equivalent security level with smaller key sizes, so that the required computing faster with lower power consumption.

In the other words , the ECC offers savings of memory usage and bandwidth or lower the load when transmitting data. Features such as these are very important when used for applications that run in mobile devices generally have a CPU with speed, power and network connectivity to a low [2] [6].

4.2 Elliptic Curve Menezes - Qu - Vanstone

ECMQV a key exchange protocol that is based on the Diffie-Hellman protocol already has on the IEEE P1363 standard [7] [8]. There are some types for key exchange namely one-way, two-way and three -way.

$$\begin{aligned} &A^{(\omega_A,\omega_A)} \overset{R_A}{\rightarrow} B^{(\omega_B,\omega_B)} \\ &S_A = (\gamma_A + \overline{R_A}\omega_A) mod\ n;\ S_B = (\gamma_B + \overline{R_B}\omega_B) mod\ n; \\ &K = hS_A(W_B + \overline{W_B}W_B);\ K = hS_B(W_A + \overline{W_A}W_A) \end{aligned} \quad (1)$$

One-way key exchange will only send one message only. Its use will be very useful in an application where there is only one party that ¬ online while others do not. Exchange is done with the assumption that party A has B's public key is used to obtain the secret key. It is assumed that because the B is considered offline [9].

$$\begin{aligned} &A^{(\omega_A,\omega_B)} \overset{R_A}{\rightarrow} B^{(\omega_A,\omega_B)};\ A^{(\omega_A,\omega_B)} \overset{R_B}{\leftarrow} B^{(\omega_A,\omega_B)} \\ &S_A = (\gamma_A + \overline{R_A}\omega_A) mod\ n;\ S_B = (\gamma_B + \overline{R_B}\omega_B) mod\ n; \\ &K = hS_A(R_B + \overline{R_B}W_B);\ K = hS_B(R_A + \overline{R_A}W_A) \end{aligned} \quad (2)$$

Key two-way exchange of each party will raise $\gamma_A$and $\gamma_B$which is used to calculate the RA and RB. Calculations for RA and RB are $R_A = \gamma_A P$and$R_B = \gamma_B P$. Validation will be performed on RA and RB, if the validation fails then the protocol will immediately fail its implementation. The calculation is continued if the validation correctly, counting s_A and s_B.The calculation will be continued until the K values are known with steps taken above. K value determined the protocol is successful or not, if the value of K = 0 then the protocol is also considered failed and there would be no key exchange is done between the two sides.

$$\begin{aligned} &A^{(\omega_A,\omega_B)} \overset{R_A}{\rightarrow} B^{(\omega_A,\omega_B)}; \\ &A^{(\omega_A,\omega_B)} \overset{MAC_k(2,B,A,R_A,R_B)}{\longleftarrow} B^{(\omega_A,\omega_B)}; \\ &A^{(\omega_A,\omega_B)} \overset{MAC_k(2,B,A,R_A,R_B)}{\longrightarrow} B^{(\omega_A,\omega_B)}; \\ &S_A = (\gamma_A + \overline{R_A}\omega_A) mod\ n;\ S_B = (\gamma_B + \overline{R_B}\omega_B) mod\ n \\ &K = hS_A(R_B + \overline{R_B}W_B);\ K = hS_B(R_A + \overline{R_A}W_A) \\ &k = H_1(z);\ k = H_1(z); \\ &k = H_2(z);\ k = H_2(z); \end{aligned} \quad (3)$$

An additional key that is used to confirm produce a three-way key exchange. The same principle as a two-way exchange with an additional key

that is used to confirm use. Confirmation of this is done with the use of the MAC function. This function makes it possible to determine whether a message sent from the correct parties are invited to communicate or not.

4.3 System Design

Figure 1 shows the block diagram of the sensor system or parts of the transmitter which sends the data to the receiver using the Xbee. In general, the system will retrieve the data by using existing sensors. The data obtained by the sensor will be processed in the microcontroller. Treatment in question is data encryption using ECC that requires public and private key. This is a key part to communicate to the receiver so that it takes a key exchange process. Key exchange is done by ECMQV key exchange protocol. After the process is for the key exchange is complete, the data can be delivered because the recipient has received a key part of which is used for decryption so that the data can be read.

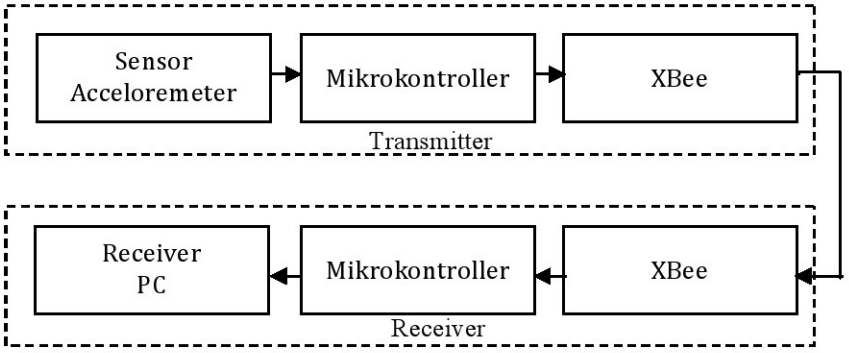

Figure 1. A block diagram of the system consists of a transmitter and receiver

4.3.1 The Transmitter

The sender consists of three devices, namely:

1) Accelerometer Sensor MMA7361

In this study, the accelerometer sensor MMA7361. This sensor is coined 3 axis X, Y, Z and used to detect vibrations that occur on the bridge.

Figure2. Over the crosssection accelerometer sensor MMA7361

MMA7361 is 3-Axis accelerometer sensor second generation . Users can get the value of the acceleration of the axis X, Y, and Z. These sensors can be used to detect collision, vibration, cartwheels, and movement .

2) Microcontroller ATmega128L

AVR is a series of 8-bit CMOS microcontroller Atmel artificial , based on RISC architecture(Reduced Instruction Set Computer). Nearly all instructions executed in one clock cycle. AVR has 32 general-purpose registers, timer/counters flexible with compare modes, interuptinternal and external, serial UART, programmable Watchdog Timer and power saving mode. In-System Programmable have on-chip Flash allows the program memory to be reprogrammed in the system using a serial connection. ATMega 128L microcontroller in the system acts as a regulator in this section. His role is to set the input obtained from sensors and processed to set the format before passing it to the XBee to be delivered at the receiver.

Figure 3.AVR Microcontroller ATmega128L

3) XBee

The role of the XBee here is as a medium of data to the sender to the receiver. The data have been obtained from the microcontroller will be sent to the recipient who also uses the same device to receive data.

Figure 4.XBee module

XBee is a module that allows the AVR ATMega to communicate wirelessly using Zigbee protocol. ZigBee operates in the IEEE 802.15.4 physical radio and operates on unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz. Base MaxStream XBee module comes from. This module enables wireless communication in a range up to 30 meters (indoors) or 100 meters (outdoor) [5].

Overall the sender will make the process as shown in Figure 5.Theprocess starts from a sensor that will read the measured parameters in this case is a vibration. After getting the sensor data, then the data is converted into digital data that is ready to provide protection to the encrypted data to be sent.

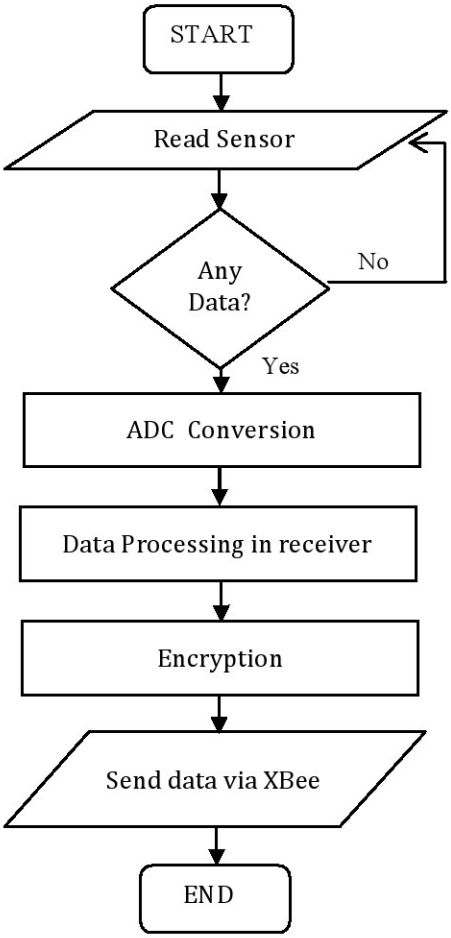

Figure 5. Process flow chart on the sender

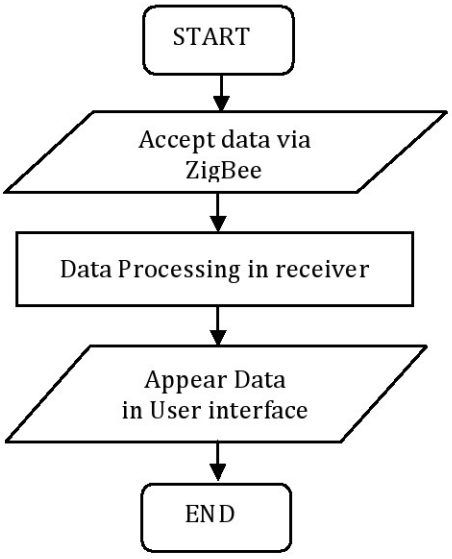

Figure 6. Process flow chart on the sender

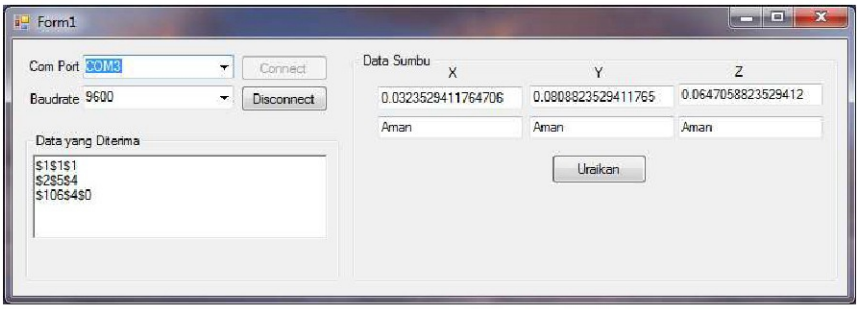

Figure 7. Display of interface on the receiver

4.3.2 The Receiver

At the receiver, there are two devices that compose the XBee is a function to receive data from the transmitter and a PC used to view the results of the incoming data. Overall on the receiver will make the process as shown in Figure 6.

A user interface that is used to see the results of the data that has been received. This interface is made using Visual Basic. Net 2010. The interface is in Figure 7. This display will show the received data and the level of data that contains data about the vibration / shock received by the sensor.

5. EXPERIMENTAND ANALYSIS

A user interface that is used to see the results of the data that has been received. This interface is made using Visual Basic. Net 2010.The interface is in Figure 7. This display will show the received data and the level of data that contains data about the vibration/shock received by the sensor.

Communication between the XBee to send and receive data will be limited to the distance. For it has been tested to determine the maximum distance that can be resolved within the XBee communication. Table 1. shows the results of testing the successful delivery of the XBee. Maximum distance while in the outdoor measurements, the distance is 55 meters. If more than the distance of the receiver will not accept the data even though the transmitter continues to transmit the data.

The process of encryption and decription are done quite time consuming because it is done on devices that have limited capabilities. The computing time will affect the data taken for the data that has been measured to wait their turn to be encrypted before it is sent to the recipient. Table 2 shows the time difference between encryption and decryption process, wherein the difference is due to the encryption process is more complicated than for the decryption process is done so that there is a lapse of time for both. The length of data to be processed also make a difference in time for each process is carried out. Besides the addition of computational time is also caused by the key exchange process. When a key is used for encryption and decription have been obtained on both sides, then the process is not done anymore.

Tabel 1. The results of testing the successful delivery of the Xbee

No	Distance (m)	Packet Loss
1	0	0%
2	1	0%
3	2	0%
4	5	0%
5	10	0%
6	20	0%
7	30	0%
8	40	0%
9	50	0%
10	60	100%
11	70	100%
12	80	100%

Table 2. Computing time encryption and decryption

No	Sent data(ADC)			Received data (ADC)			Time	
	X	Y	Z	X	Y	Z	Enk (s)	Dek (s)
1.	2	0	4	2	0	4	91	42
2.	0	-2	2	0	-2	2	91	42
3.	3	2	5	3	2	5	91	42
4.	3	3	5	3	3	5	91	42
5.	4	2	6	4	2	6	94	42
6.	-4	22	-26	-4	22	-26	102	43
7.	-4	25	-30	-4	25	-30	103	43
8.	0	29	-27	0	29	-27	102	43
9.	13	106	9	13	106	9	104	44
10.	20	114	116	20	114	116	104	43
Average time							97	42

There is a possibility, the data is sent encrypted missing, resulting in the data can not arrive at the receiver and consequently the data will not be obtained when the data is very important.

Table 3 shows the results of testing the successful delivery of the data, which of the test failure occurs ten times as much as 10%. The failureresulted in the receiver section can not decrypt the data so that no data is entered.

Results received on the result of the ADC number but the user interface has been revamped into a vibration unit. The data is also divided into three sections which is the axis of the accelerometer. The data have been divided and converted into units of vibration has also been classified into several categories according to the scale of existing vibrations. Scale used to determine the level of vibration obtained from a predetermined standard.

Table 3. The results of the successful delivery of the data

No	Sent data (ADC)			Received data (ADC)		
	X	Y	Z	X	Y	Z
1.	2	0	4	2	0	4
2.	0	-2	2	0	-2	2
3.	3	2	5	3	2	5
4.	3	3	5	3	3	5
5.	4	2	6	4	2	6
6.	-4	22	-26	-4	22	-26
7.	-4	25	-30	-4	25	-30
8.	0	29	-27	0	29	-27
9.	13	106	9	13	106	9
10.	16	109	14	-	-	-

Figure 8. Display data on the sender

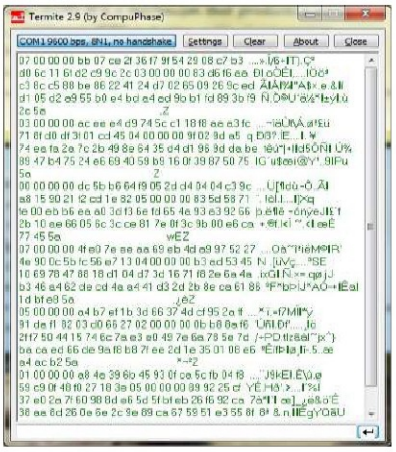

Figure 9. Display the current data into ciphertext

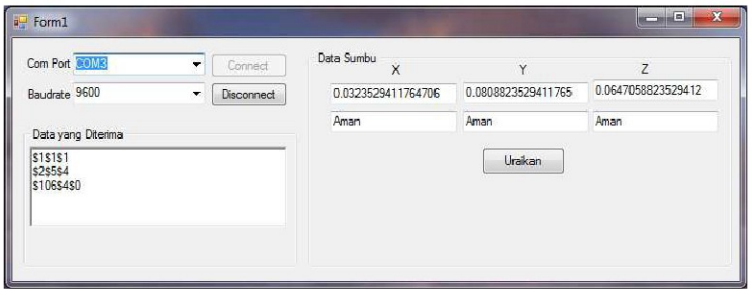

Figure 10. Display data on user interface

6 . CONCLUSION

The test results prove that the data can not be sent to the destination, because it is influenced by technical factors or the distance of the data reception. In this study, the maximum distance that can still transmit data is as far as 55 meters, while the data transmission done can happen without no data reception by 10% in ten attempts. The average computation time of encryption and decryption is for 97 seconds and 42 seconds but this time increased in the early initiation of communications to perform the key exchange protocol.

REFERENCES

[1] **Ubiquitous Sensor Netwoks(USN)**,ITU-T Technology Watch Briefing Report Series, No.4, February 2008.

[2] Darrel Hankerson, Alfred J. Menezes, dan Scott Vanstone, **Guide to Elliptic Curve Cryptography**, Springer, New York [u.a.], 2004.

[3]Chae, M. J, Yoo, H. S.,Kim, J. R., Cho, M. Y., **Bridge Condition Monitoring System Using Wireless Network (CDMA and ZigBee)**, Proceeding of ISARC, Korea,, 2006.

[4]Malik, Muhammad Yasir, **Efficient Implementation of Elliptic Curve Cryptography Using Low-power Digital Signal Processor**, Proceeding of ICACT, Pakistan, 2010.

[5] Ronald Watro, Derrick Kong, Sue Fen Cuti, Charles Gardiner, Charles Lynn, dan Peter Kruus, **TinyPK: Securing Sensor Networks with Public Key Technology**, Dalam SASN '04: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, pages 59–64, New York, NY, USA, 2004. ACM Press.

[6] M. Aydos, B. Sunar, dan C. K. Koc, **An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication**, 2nd International Workshop on Discrete and Methods for Mobile Computing and Communications, Dallas, Texas, 1998.

[7] L. Eschenauerdan V. Gligor, **A Key Management Scheme for Distributed Sensor Networks**, Dalam CCS '02: Proceedings of the 9th ACM Conference on Computer and Communications Security, New York, NY, USA, 2002. ACM Press.

[8] W. Du, J. Deng, Y. Han, dan P. Varshney, **A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks**,Dalam CCS '03: Proceedings of the 10th ACM Conference on Computer and Communications Security.

[9] H. Chan, A. Perrig, dan D. Song, **Random Key Predistribution Schemes for Sensor Networks**,Dalam Proceedings of the IEEE Security and Privacy Symposium 2003.