EMITTER International Journal of Engineering Technology
Vol.1, No.1, December 2013
ISSN: 2355-391X

Secure Ubiquitous Sensor Network based on Elliptic Curve Menezes Qu Vanstone as Status Data Supply of Environment in Disaster 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

Copyright © 2013 EMITTER International Journal of Engineering Technology - Published by EEPIS