Towards an Efficient Certificateless Access Control Scheme for Wireless Body Area Networks

Philemon Kasyoka, Michael Kimwele & Shem Mbandu Angolo

Abstract

Wireless body area networks have become popular due to recent technological developments in sensor technology. A sensor can be used to collect data from different environments of interest, process and communicate the data to other nodes in a network. By its very nature, a sensor node is limited in resource usage. Due to these limitations, numerous security challenges have emerged in their applications, hence the need for more efficient and secure cryptosystems. In this paper, we give an efficient certificateless pairing-free signcryption scheme then design a secure access control scheme that can satisfy both the properties of ciphertext authentication and public verifiability using the signcryption scheme. A formal security proof of our scheme in random oracle model is provided. In addition, we compare the efficiency of our access control scheme with other existing schemes that are based on signcryption scheme. The analysis reveals that our scheme achieves better trade-off for computational and communication cost.

Full text: https://doi.org/10.1007/s11277-020-07621-7