CERTAIN INVESTIGATIONS ON SECURITY ENHANCEMENT AND KEY MANAGEMENT TECHNIQUES IN WIRELESS SENSOR NETWORKS FOR HEALTHCARE APPLICATIONS

ABSTRACT

Submitted by

SIVA BHARATHI K R

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

FACULTY OF INFORMATION AND COMMUNICATION ENGINEERING

ANNA UNIVERSITY

CHENNAI 600 025

NOVEMBER 2021

ABSTRACT

Remote monitoring of patients and elderly people has become mandatory nowadays owing to the growing Covid – 19 Pandemic across the globe. An Engineering approach for the same results in numerous advantages. Switching to Wireless Body Area Networks can be a suitable and well required solution for adopting the same. A wide range of medical monitoring equipment's are available in hospitals but they are not location dependent and mostly difficult to handle due to wired nature of the network. Wireless Body Area Networks can thus be a key technology to overcome this. Wireless Body Area Networks are special type of wireless sensor network used for healthcare applications. This study aims at developing various security framework to overcome the security issues and attacks encountered by Wireless Body Area Networks.

The sensor nodes in the Wireless Body Area Networks are either wearable or implanted in the human body. Thus, Wireless Body Area Networks transport life critical sensitive information and it becomes obligatory to ensure the secure transmission of data in the network. The main objective of the study is to develop a complete security framework for the transmission and reception of medical data in a secure manner. For this, all the possible security attacks in different layers of the OSI model is studied and analyzed. The security protocols and algorithms developed for traditional wireless networks don't fit into Body Area Networks because of the inimitable nature of network. The design of security protocols and models should not only enhance the security but also the performance of the network. In this research work, three different modules are proposed for effective and secure transmission and reception of the medical data, that is, the health information or the sensor parameter from human body.

In the first module, a protocol is designed with the optimal Fair exchange protocol for enhancing the security and authenticity in a three-tier wireless Body Area Network. A third-party auditor (TPA) is involved at all stages in the

network. Attacks are induced externally in the network and the performance is analyzed. It is proved that the performance of the proposed protocol is getting improved with 5-8% in packet delivery with a delay less than an average of 4ms when compared to the existing Light Weight Secure Routing (LWSR) Protocol.

In the next module, an integrated security model is proposed so as to provide a triad level of security to the network. To accomplish this, the biometric authentication is done at the network level, the traditional RSA cryptography is applied as second level to the nodes and Hash based Message Authentication along with SHA – 256 (HMAC SHA – 256) is applied as the third level of security to the data. The performance of a conventional simple clustered BAN and clustered BAN with RSA is compared with the proposed model. It is observed that this method results in a minimum number of deceased nodes with maximum packet transmission and less Energy consumption. The residual energy remains up to 20J after 2000 rounds of simulation.

In the third module, Quantum Key Distribution is considered to attain an unbreakable level of security. The Key generation of the existing B92 protocol is done with a minor improvement. It is observed that the key generation time of the proposed EB92 protocol is a little more than half the key generation time of the existing EBB84. The ideal key generation time of B92 will be half of that of BB84 and a small increase in time is due to the X-OR function performed with the unmatched bits to form the secure key.

All known attacks are possible in traditional cryptanalysis schemes because of the key distribution problem, computational weaknesses and authentication failure. It is concluded that the proposed Key management scheme applying QKD provides security against all the attacks as it uses the quantum key and hence impostors will not be able to predict or catch the secret key, thus providing unbreakable security to the network.