INTERNATIONAL CONFERENCE ON ADVANCED RESEARCH TECHNIQUES IN ENGINEERING, SCIENCE, HUMANITIES AND BUSINESS MANAGEMENT (ICARTESHBM – 2020)
15TH MARCH, VIJAYAWADA, ANDHRA PRADESH, INDIA

CERTIFICATE NO : ICARTESHBM /2020/ C/ C0320102

A STUDY OF FEASIBILITY OF BASIC SECURITY SCHEMES IN WIRELESS SENSOR NETWORKS

CHAVAN SIDRAM NAGNATH

Research Scholar, Ph.D. in Computer Science, Dr. A.P.J. Abdul Kalam University, Indore, M.P.

ABSTRACT

Security is critical for wireless sensor networks (WSN) deployed in hostile environments since many types of attacks could reduce the trust on the global functioning of any WSN. Many solutions have been proposed to secure communications for WSNs and most of them rely on a centralized component which behaves as a certificate authority. We propose in this paper a distributed solution able to ensure authentication of nodes at any time without having any on-line access to a certificate authority. Each node will be equipped with a Trusted Platform Module (TPM) which is able to store keys with security. Each node will have its own public key and private key pair in the TPM and a certificate of the public key. The certificate is issued off-line when setting-up the node. When a node communicates with another, it has to sign the message with its own private key (done securely by the TPM) and sends the message, the signature and the certificate of the public key. The evaluation of the solution has been done using simulation and the overhead added by integrating authentication does not exceed 15% of energy consumption.

Keywords: Wireless Sensor Networks (WSN), Trusted Platform Module (TPM), Secure Communications.