Abstract

These days witness a tremendous development in Wireless Sensor Networks (WSNs). They are used in various fields for different purposes due to their advancements in hardware technology and software skills. The unattended environment where the sensor nodes are deployed along with the unreliable wireless communication offered in WSNs and the peculiar characteristics owned by WSNs pertains security relevant issues to many applications of WSNs. It is essential to ensure security services for the applications of WSNs to achieve all the benefits of applications of WSNs faultlessly. One method of providing security in communications performed between sensor nodes is through cryptographic operations. An open research issue in providing security through cryptographic operation is the distribution of cryptographic keys to the communicating entities in WSNs. Further, when sensor networks are used for applications such as monitoring and continuous tracking in surveillance, it is necessary to report event information securely and accurately in a timely manner to the respective authorities. When WSNs are used for these applications sensor nodes frequently suffer from different types of attacks such as eavesdropping, intercepting, data manipulating, replay attack, impersonation attack and attacks denying the event reports from reaching the Gateway nodes(GWN). Hence it is necessary to design secure communication schemes to get rid of these attacks or to mitigate the impact of this attack on WSNs applications.

The objective of the thesis is to design secure communication schemes for WSNs. The performance of the proposed schemes are compared with already proposed mechanisms ensuring security through secure and reliable data transmission and mechanisms providing anonymous secure communication. In the first study, the proposed protocol is tailored for IoT. In this scheme, the communicating parties establish a common session key which can be used for data sharing over insecure channel without giving raise to any security issues. The proposed scheme could significantly improve the performance of user authentication and key agreement segment. In comparison to other compared schemes, our scheme shows the resiliency against node compromisation and data compromisation.

The second study enforces security for Ad hoc networks, where the multi-gateway based design is utilized to provide the user a secure communication through a secret sharing mechanism. The proposed mechanism offer lightweight energy efficient secure multi-gateway based communication. This scheme provides better security in gateway based WSNs. The secret sharing mechanism securely distributes secret shares among authenticated members over a insecure channel in a secure way such a way that, only the authenticated parties can communicate and get the opted data. The proposed scheme is able to achieve forward as well as backward security. The proposed mechanism ensures

security in communications, when compared to other proposed schemes in the literature.

The third study focuses on achieving security WSNs environment, where the predefined shared secret keys plays a very important role in establishing a secure communication. In designing a secure communication system, there should not be any scope of leakage of these predefined secret keys. We have shown in our work, how essential to preserve these predefined secret keys, otherwise the security of any well designed system can be proven insecure and further cannot be used for practical applications. To avoid such situation, the public key cryptosystem such as Elliptic curve cryptography(ECC) is used in our design for the better communication and easy access. ECC is preferred due to its advantageous over RSA, as it consumes less key size in comparison to RSA. Moreover, ECC is much efficient and can be implemented easily. Along with ECC, collision-resistant hash functions and a symmetric key cryptosystem is used to design our proposed scheme. The proposed scheme is provable secure and can resist many security functionalities. The performance of our proposed scheme also consumes much less time to communicate and its efficiency is shown in terms of computation time, communication and storage capacity.

The main goal of the fourth study is to preserve the privacy of the user's information and data in transit by providing security services to enhance the security strength of the e-medical services performed in Wireless Medical Sensor Networks (WMSNs). The privacy is ensured in this scheme by preventing the disclosure of source and destination information through anonymity. In addition this scheme provides security for the sensed event information through cryptographic operation. The proposed scheme prevents the adversary from knowing about the identity of the user (patient) by eavesdropping on the transmitted messages. This scheme ensures successful e-medical services to the patient by continuously monitoring the opted medical services from WMSNs. Moreover, before initiating the services, the users establish a common secure session key for further communication with the medical-gateway nodes and the sensor nodes. The efficiency of our proposed scheme also consumes much less time to communicate and its efficiency is shown in terms of computation time, communication and storage capacity.

On the whole, the security protocols designed in this dissertation are useful in establishing secure communication to WSNs. This thesis focuses in establishing privacy and security for WSNs by designing a secure user authentication and key agreement protocol in various environments and technologies. The presented mechanisms are very useful in achieving energy efficiency, increasing network lifetime and enhancing resiliency against data compromisation.

Keywords: Authentication; Impersonation; BAN Logic; AVISPA; Anonymity; Smartcard; Privacy.