Abstract

Wireless sensor networks (WSNs) have become popular in the field of information and communications technology, they are increasingly being used in applications such as surveillance systems, patient monitoring, object tracking, forest fire detection and habitat monitoring among others. By its very nature, a WSN provides a resource constrained environment where devices used are limited in resource usage. Due to these limitations, security challenges have emerged in their applications. Hence, the need for computationally efficient but still secure cryptosystems. Traditional cryptographic primitives cannot be directly applied on WSNs due to their resource constrained nature, this has led to the challenge of achieving cryptographic security goals which are important for effective communication of information on WSNs. Recent studies have shown that it is possible to apply public key cryptography such as ECC to resource constrained devices by using the right selection of algorithms and associated parameters, optimization and low power concepts. To address security challenges on WSNs, this thesis proposed an efficient digital signature scheme, a variant of ECDSA that can be applied on WSNs to provide authentication. Further, the variant of ECDSA was used in the design of a signcryption schemes. The signcryption schemes are intended to be efficient enough for use on WSNs and for that reason the research work focused on certificateless cryptography (CLC) for the design of the signcryption scheme with a property of ciphertext authenticity. The research methodology employed was experimental. Major contributions of this research were an efficient variant of ECDSA more efficient in the signing and verification process that does not suffer from the security challenges inherent in the original ECDSA. Out of the proposed digital signature scheme a certificateless pairing free authentication scheme for wireless body area network in healthcare management system and a multi-user broadcast authentication scheme for WSNs were constructed. Three certificateless signcryption schemes were designed, two signcryption schemes were designed from the proposed ECDSA variant and one signcryption was a modification of a scheme by Wei and Ma (2019). A formal security proof for indistinguishability against adaptive chosen ciphertext attack and existential unforgeability against adaptive chosen message attack was provided for the three signcryption schemes in the random oracle model. The signcryption schemes were more efficient with respect to computational cost, communication overhead and energy consumption comparison with other existing related schemes.