Abstract

In recent times, Wireless Sensor Network (WSN) has achieved tremendous applications in various fields like military, commercial, healthcare and detection of volcano eruption. For practical realization of these applications, security is very important. The Key management plays a crucial role in implementation of security as other security primitives depend on it. Sometimes nodes are deployed in hazardous environments such as military battlefield and moreover nodes in WSN have certain constraints due to limitation of energy, storage space, computation and communication capability. Researches have shown that homogeneous sensor networks suffer from performance bottleneck, poor scalability, high communication and computation overhead as well as high storage requirement. Therefore, to overcome these problems, heterogeneous sensor network has been proposed which provides benefits to some extent compared to homogeneous network. Here owing to security requirement and limitations of nodes, we propose a novel key management protocol applying identity based cryptography which uses bilinear pairing on elliptic curves. We have proved the security property of the protocol using Strand Space model. The security analysis and simulation results show that the proposed protocol gives better performance compared to other similar protocols in the literature.

Keywords: Key Management, Heterogeneous Sensor Network, Bilinear Pairing, Identity based cryptography, Elliptic Curve, Strand Space model.