Abstract

Security plays an important role in designing a wireless sensor networks (WSNs). As the medium is wireless in nature which is more vulnerable to adversaries attacks in the network. Key management is used to achieve security in WSNs. If symmetric key is used in the network then one key is more enough to secure the network but the issue is that once the key is compromised, entire network gets compromised. On the other hand, if an individual key is provided to every sensor in the network then sensor to sensor communication is not possible in the network. Therefore sensors are grouped together to form a cluster. Each cluster is assigns a cluster key shared by every cluster member of the group. If this key is fixed then key compromising affects the security principle in the entire group. So to avoid this type of attack, key is updated after a fix interval of time. But if key updating is done by the base station, communication overheads in updating the keys are increased in the network. Therefore resource constrained wireless sensor networks; the concept of key generation is used instead of key distribution. In key generation process, the key is generated by applying a one way hash function on a given secret. But the problem is that if this secret is compromised, all the keys
which are generated in past or to be generated in the future are immediately compromised. In this research paper, we present a LOKS: Low-Overhead Forward and Backward Key Secrecy scheme to secure WSNs. This scheme updates the keys of each cluster in the network with resiliency to attack. Simulation results proves that presented scheme takes less number of communication overheads as compared to existing schemes given in literature to update the group keys for every groups after every round.

References

Keywords

Backward Secrecy, Cluster Head, Forward Secrecy, Key Generation, Key Secrecy, Sensor nodes, WSNs.