Abstract

Wireless sensor networks establish a specific type of wireless data communication networks. WSNs have acknowledged remarkable deliberation in recent years due to probable applications in armed sensing, fitness care, wildlife tracking, traffic investigation, building constructions monitoring, atmosphere monitoring etc. The central of trust route deceits in gaining trust. Conversely, the present-day trust-based route approaches have some challenging concerns. Finding the trust of a sensor node is most difficult, and just how it can be completed is still uncertain. Routing rules of wireless sensor network naturally adjust themselves with the current environments which may vary with high mobility to low mobility in extremes along with high bandwidth. Detection of malicious node and information safety in a wireless sensor network is an essential work in any sensor network. To achieve availability, integrity and reliability routing rules should be robust against malevolent attacks. We proposed a secure trust value which helps authenticate the sensor node and similarly preserve and safe the sensor network from malicious nodes. We also proposed a novel approach to detect the black hole attack and also keep safe the network from malicious nodes. The network lifetime will improve
and energy consumption reduced. Experimental outcomes demonstrate that our scheme is good for wireless sensor network security.

References

Index Terms

Computer Science  Wireless

Keywords