Wireless sensor networks (WSNs) have gained huge popularity in various new fields. The direct use of each of these sensors individually is to detect its surrounding conditions such as temperature, pressure, sound, motion etc. whereas a collection of such nodes finds application in various large scale management systems such as healthcare, disaster and traffic management programs. In most of these systems, the sensors are located at points which are not physically protected and can hence fall prey to several security threats and attacks very easily. The limited memory, power and capacity of such sensors make it more difficult to introduce advanced, heavy-weight algorithms for securing them against such attacks. Further, the criticality of the applications using WSN makes such security threats more dangerous. In this paper, we show the results of combining a novel detection algorithm with the results of a unique resolution technique of the sinkhole attack when the network is routed using Collection Tree Protocol (CTP).
References

2. Government Health Staff, “Internet of Things triggers healthcare security concerns”, Government Health IT, 2015

Index Terms

Computer Science

Algorithms

Keywords

Wireless Sensor Network (WSN), Collection Tree Protocol (CTP), Sinkhole Attack, Base Station (BS), Cluster Head (CH), Sensor, Internet of Things (IoT)