International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)
ISSN(P): 2250-1568; ISSN(E): 2278-9448
Vol. 4, Issue 2, Apr 2014, 115-124

TRANS STELLAR
• Journal Publications • Research Consultancy

APPROACH TOWARDS SAFETY IN WSN: A SURVEY

PADMINI M. S & PRASANNA KUMAR G

The National Institute of Engineering, Mysore, Karnataka, India

ABSTRACT

Wireless sensor networks gaining more popularity and continue to grow in large extent and so there is need for effective security and safety mechanisms. Sensor networks operate in hostile environments and they interact with sensitive data and they do not have any user controlling the individual nodes. Wireless Sensor networks can be used in various areas like battlefields, commercial applications such as Traffic monitoring, Environment monitoring and also in buildings and smart homes and in many other scenarios. So the security concerns need to be addressed from the initial stage of the system design and it is one of the important challenges in wireless sensor networks. Compared to traditional networks, there are lot of security challenges involved in sensor networks due to existing computing and resource constraints. This provides chance for enormous research potential in wireless sensor network security. So the current research in the field of wireless sensor network will be of great benefit to the researchers. So, in this paper we have done the survey of new technologies of wireless sensor network security in different scenarios and the ways of providing security in the sensor networks, classifying different attacks and the defensive measures that can be taken in the sensors networks and also cryptographic strength and analysis of performance of these scenarios. Cloning attack will be identified using this model. Zero knowledge protocol can be applied for verifying the sender sensor nodes. Clone attack can be addressed with attachment of unique fingerprint to each node. We have used the zero knowledge protocol to address the non transmission of crucial cryptographic information in the wireless sensor network. Thus, replay attack and man-in-the middle attack can be prevented.

KEYWORDS: Crucial Cryptographic Information, Cloning attack, Wireless Sensor Networks