

28. GUARENTEED SECURITY IN WIRELESS NETWORK USING IMPROVED KEY MANAGEMENT SCHEME

P. M. Blessey, R. Geetha

PG Scholar, Associate Professor

Department of CSE

S. A. Engineering College, Chennai

blessey.pm@gmail.com ,geetha111@yahoo.com

Wireless sensor networks (WSNs) distribute nodes with the limited capabilities to sense, collect, and distributes information in numerous applications [1]. As sensor networks become pervasive, security is exposed to several attacks such as Sybil attack, network eavesdropping, masquerade attack, etc. For secure communication between the nodes, secret key cryptosystem is used. To deliver data in a secure manner without being compromised by an adversary, WSN provides secure communication and key distribution Key management schemes have been established to achieve security. The tradeoff between the security and the connectivity is explained in each key management scheme. By this survey, it helps us to know the schemes that detect attacks and prevent it. As we recuperate the merits and demerits of the schemes are analyzed. Moreover, the techniques and methods used have been summarized.

Index Terms— Sensor networks, Security, Connectivity Key management schemes, Secure communication.

Journal of Science and Innovative Engineering & Technology