Enhancing security of Wireless Network from External Attacks

[1]Monika Rani, Research Scholar, prachi.Rose14@Gmail.Com
[2]DR. VIKRAM SINGH, vikramsinghkuk@yahoo.com

Abstract: A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks & enterprise (business) installations avoid costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless personal area networks (WPANs) interconnect devices within a relatively small area that is generally within a person's reach. For example, both Bluetooth radio & invisible infrared light provides a WPAN for interconnecting a headset to a laptop. Zig Bee also supports WPAN applications. Wi-Fi PANs are becoming commonplace (2010) as equipment designers start to integrate Wi-Fi into a variety of consumer electronic devices. A hacker is somebody who exploits & seeks weaknesses within a computer network or computer system. A hacker can be motivated by a multitude of reasons, such as profit, challenge or protest. Grouping that has evolved everywhere hackers is often referred to as computer underground & these days they are well known community.

Keyword: transmitter, Communications, Framework, Cryptography, Cellular, telecommunications, equipment

[1] INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks & enterprise (business) installations avoid costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented & administered using radio communication. This implementation takes place at physical level (layer) of OSI model network structure. Examples of wireless networks include cell phone networks, Wi-Fi local networks & terrestrial microwave networks.

Computers are very often connected to networks using wireless links.

[2] LITERATURE REVIEW

Xavier Boyen et al[5] Distributed-password public-key cryptography (DPwPKC) allows members of a group of people, each one holding a small secret password only, to help a leader to perform private operation, associated to a public-key cryptosystem. Abdalla et al. recently defined this tool , with a practical construction. Unfortunately, latter applied to ElGamal decryption only, & relied on DDH assumption, excluding any recent pairing-based cryptosystems.

Note : For Complete paper/article please contact us info@jrps.in

Please don't forget to mention reference number , volume number, issue number, name of the authors and title of the paper