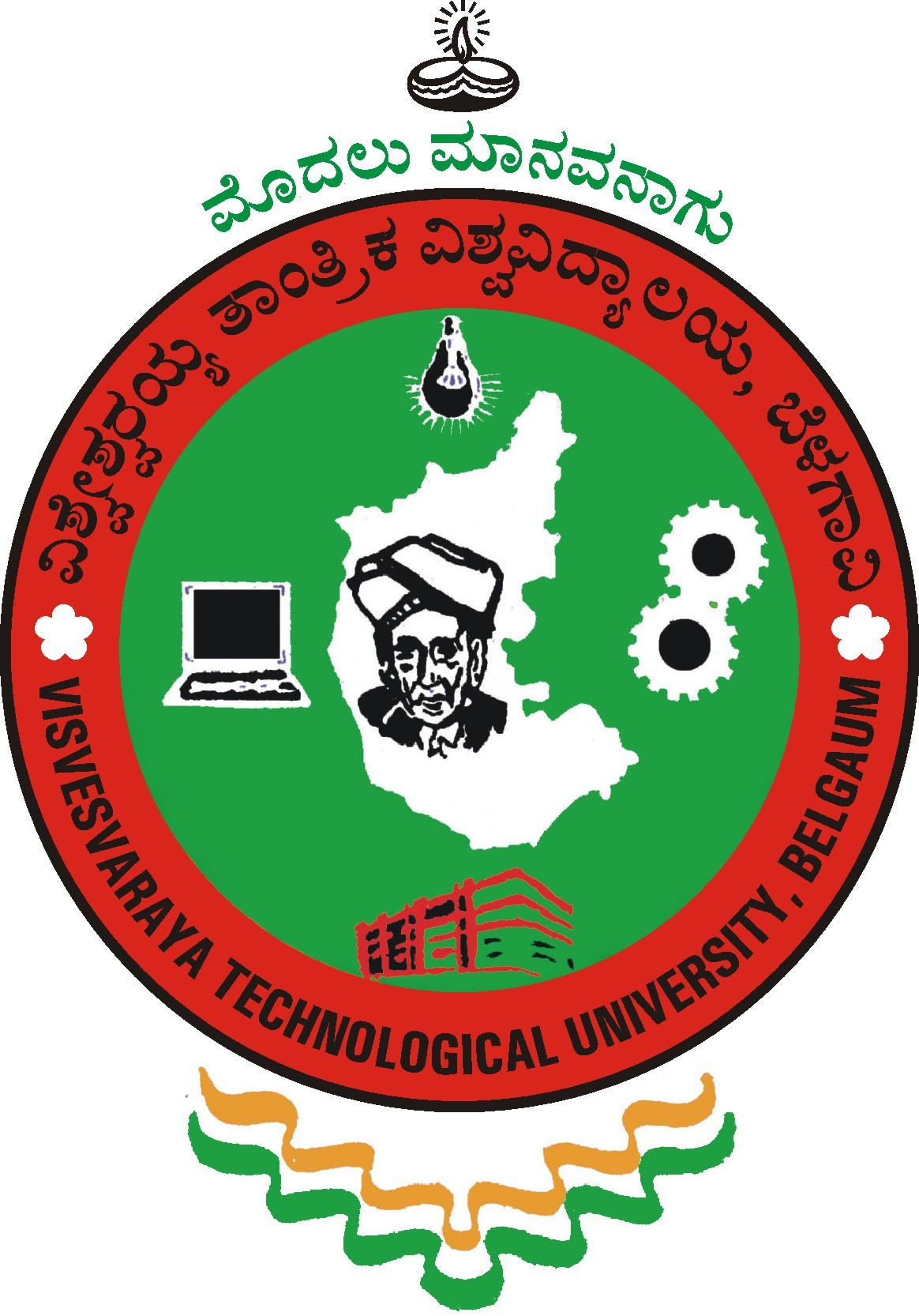
**VISVESVARAYA TECHNOLOGICAL UNIVERSITY**

Jnanasangama, Macche, Santibastwada Road

Belagavi-590018, Karnataka



**A**

**Mini Project Report**

on

**Physical Layer Wired and Wireless Security**

*Submitted in partial fulfillment of the requirement for the degree of*

**Bachelor of Engineering**

*in*

**Electronics & Communication Engineering**

*by*

**USN :** 1DS18EC153 **Tanvi Vijay**

**USN :** 1DS18EC156 **Vishvendra Singh**

**USN :** 1DS18EC143 **Sameer Gautam**

**USN :** 1DS18EC144 **Saurabh Singh**

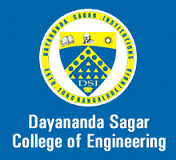
Under the guidance

of

**Prof. Nagachandra MK**

Internal Departmental Project Guide

Designation, ECE Dept., DSCE, Bengaluru



**Department of Electronics & Communication Engineering**

(An Autonomous College affiliated to VTU Belgaum, accredited by NBA & NAAC)

Shavige Malleshwara Hills, Kumaraswamy Layout,

Bengaluru-560078, Karnataka, India

**2020-21**

# Certificate

Certified that the mini project work entitled “Physical Layer Wired and Wireless Security” carried out by Tanvi Vijay (1DS18EC153), Vishvendra Singh (1DS18EC156), Sameer Gautam (1DS18EC143), Saurabh Singh (1DS18EC144) are bona fide students of Dayananda Sagar College of Engineering, Bangalore, Karnataka, India in partial fulfillment for the award of Bachelor of Engineering in Electronics & Communication Engineering of the Visvesvaraya Technological University, Belagavi, Karnataka during the academic year 2020-21. It is certified that all corrections / suggestions indicated for mini project work have been incorporated in the report deposited to the ECE department. This mini project report **(18EC5DMETS)** has been approved as it satisfies the academic requirement in respect of mini project work prescribed for the said degree.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Dept. Mini Project Coordinator Convener Project Guide

Dr. Roopa M Prof. NagachandraMK

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Section Mini-project Co-ordinator Head of the Department

Name Dr. T.C.Manjunath

External Project Viva-Voce

Name of the project examiners :

1 : Signature : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2 : Signature : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Declaration

Certified that the mini project work entitled, “Physical Layer Wired and Wireless Security” is a bona fide work that was carried out by ourselves in partial fulfillment for the award of degree of Bachelor of Engineering in Electronics & Communication Engg. of the Visvesvaraya Technological University, Belagavi, Karnataka during the academic year 2019-20. We, the students of the mini project group/batch no. C-9 hereby declare that the entire project work has been done on our own & we have not copied or duplicated any other’s work. The results embedded in this mini project report have not been submitted elsewhere for the award of any type of degree.

Student Name-1 : Ms. Tanvi Vijay. USN :1DS18EC153

Sign : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Student Name-2 : Mr. Vishvendra Singh USN : 1DS18EC156

Sign : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Student Name-3 : Mr. Sameer Gautam USN : 1DS18EC143

Sign : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Student Name-4 : Mr. Saurabh Singh USN : 1DS18EC144

Sign : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date : 07 / 12 / 2020

Place : Bengaluru -78

**Abstract**

As technology advances in society the need for wired and wireless networking has become essential. Each of these types of networking has their advantages and disadvantages according to security. Wired networking has different hardware requirements and the range and benefits are different. Wireless networking takes into consideration the range, mobility, and the several types of hardware components needed to establish a wireless network.

Wireless networking provides many advantages, but it also coupled with new security threats and alters the organization’s overall information security risk profile. Although implementation of technological solutions is the usual respond to wireless security threats and vulnerabilities, wireless security is primarily a management issue. We are presenting an efficient demonstration to understand and assess the various threats associated with the use of wireless technology. We have also discussed a number of available solutions for countering those threats.

As you read on you will understand different types of configurations of networks and the security measures that need to be taken to ensure a secure network.

# INTRODUCTION

Organizations rely heavily on the ability to share information throughout the organization in an efficient and productive manner. Computer networks have allowed for this technology and are now a part of almost every business. An organization has two options when it comes to setting up a network. They can use a completely wired network, which uses networking cable to connect computers, or they can use a wireless network, which uses radio frequencies to connect computer.

Wireless Networks have a number of benefits including Convenience, Mobility, Productivity, Deployment, Expandability and Cost, therefore, organizations are now using a combination of both wired and wireless networks. In Wireless Networks the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. Wireless Network technology, while replete with the conveniences and advantages described above has its share of downfalls. The disadvantages of using a wireless network are: Security, Range, Reliability, and Speed.

## 

**LITERATURE SURVEY**

* Security policies should not be fixed rather than it should be flexible enough to fulfill the need of an organization as well as it should be capable enough to tackle future security threats while at the same time easily manageable and adoptable.
* The studies showed that a positive secrecy capacity can be achieve if the intended receiver has a better channel than the eavesdropper.
* The studies offers low complexity and it is information-theoretically secure. It circumvents the limitations of the conventional cryptography-based schemes. In particular, the RFF of the transceiver is employed for authenticating the user identity and the wireless channel is exploited to generate cryptographic keys.
* The impact of CSIT uncertainty on the secrecy throughput of multi-user broadcast wiretap channels was studied and examined. The obtained results show that even with a noisy CSIT, a non-zero secrecy rate can still be achieved. Asymptotic analysis at high SNR, perfect, and no-main CSIT were addressed and the results were illustrated for the case of Rayleigh fading channels.
* The asymptotic performance limits of physical layer security were analyzed. Based on these theoretical modellings, channel correlation were then revealed to have constructive effect on the outage secrecy capacity if the asymptotic outage probability is less than 1/2, and have destructive effect otherwise. ­­

**METHODOLOGY**

There are two types of networks employed for data communications, wired and wireless.

A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables. The benefit of a wired network is that bandwidth is very high and that interference is very limited through direct connections.

A wireless network uses high-frequency radio waves rather than wires to communicate between nodes. Wireless networks are being used by individuals and organizations to expand their existing wired network or to go completely wireless. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure (Wi-fi.com). Wireless networks are reliable, but when interfered with it can reduce the range and the quality of the signal.

Methods used for network security:

TAPPING CABLE: COUNTER MEASURES

Physical inspection, physical protection

* + E.g., encase cable in pressurized gas
  + Use faster bitrate

Monitor electrical properties of cable

* + TDR: sort of like a hard-wired radar
  + Power monitoring, spectrum analysis

WILDLIFE: COUNTER MEASURES

Use High Strength Sheath cable

* + PVC wrapping stainless steel sheath
  + Performance studies on cable (gnathodynameter)

Cable wrap

* + Squirrel-proof covers: stainless steel mesh surrounded by PVC sheet

Fill in gaps and holes

* + Silicone adhesive

Use bad-tasting cord

* + PVC infused with irritants
  + Capsaicin: ingredient in pepper spray, irritant
  + Denatonium benzoate: most known bitter compound

WIRELESS COMMUNICATION: COUNTER MEASURES

* The first line of defense is a firewall. A firewall is a number of security schemes that prevents unauthorized users from gaining access to a computer network. Firewalls are very effective at preventing attacks and the cost for a firewall is definitely offset by the benefit and security it provides.
* Organizations can use encryption to transform data into a hard to interpret form. This allows businesses to transmit data over their networks in a secure way and even if a person were to intercept the data they wouldn’t be able to interpret anyway.
* An anti-virus program is a utility that searches a hard disk for viruses and removes any that are found. Examples- Norton Anti-virus, McAfee Anti-virus and AVG virus protection.
* Spyware consists of computer software that gathers and reports information about a computer user without the user's knowledge or consent. This program scans your computer’s hard drive for spyware and deletes them from the system. This is a very effective program along with Spybot Search & Destroy One example is Lavasoft’s AdAware.
* Elimination of rogue access points by using 802.1x on the wired network to authenticate all devices that are plugged into the network.
* Secure Configuration of Authorized Access Points by changing all default settings because they are well-known and can be exploited by attackers.

# BLOCK DIAGRAM AND IMPLEMENTATION

System 2

System 3

System 4

System 1

Physical Taping, Damaged by Wildlife

Noise, Jamming, Information Leakage

Blind physical attacks, Search-based physical attacks

Eavesdropping, Email-Borne viruses, Email Spoofing, DOS, Trojan Horse

…... Wireless Network

Wired Network

This Block Diagram represents communication system having wired and wireless networks and their corresponding possible security attacks.

**RESULTS AND DISCUSSIONS**

Wireless networking provides numerous opportunities to increase productivity and cut costs. It also alters an organization’s overall computer security risk profile. Although it is impossible to totally eliminate all risks associated with networking, it is possible to achieve a reasonable level of overall security by adopting a systematic approach to assessing and managing risk. This report discussed the threats and vulnerabilities associated with each of the basic technology components of wired and wireless networks and it also stressed the importance of training and educating users in safe networking procedures.

In Wired communication, preventive measures can be taken as physical inspection, physical protection (for example, encase cable in pressurized gas), use faster bitrate, monitor electrical properties of cable, TDR: sort of like a hard-wired radar, Power monitoring, spectrum analysis.

In Wireless communication, security can be ensured by use of encryption, anti-virus and anti-spyware software and the firewall, by turning off identifier broadcasting, changing the identifier on your router from the default, change your router pre-set password for administration. Adding to it, allow only specific computers to access your wireless networks, turn off your wireless network when you know you won’t use it and don’t assume that public hotspots are secure.

Users are the basic component of wired and wireless networking, indeed, the importance of training and educating users about secure networking behaviour can be overstated. To be effective, user training and education needs to be repeated periodically.

**CONCLUSION AND FUTURE WORK**

Wired and Wireless networks are very common in the workplace as well as in the home. Technology has been created to store, transmit and receive data through networks at very high rates of speed. Networks have become essential to completing daily business tasks and most business, those who rely heavily on information technologies, would be crippled without their networks.

Advances in networking storage have allowed for organizations to use their networks not only for the sharing of resources but to store large pools of data to be used for data analysis. Companies can now store detailed profile information for customers at a very low cost. In the future, the speed of networks will increase as they have in past years. The cost of networks will continue to decline and using a network will be essential for every organization. As computing technology increases in power, and decreases in size, the price of creating a high-powered full featured network will decrease rapidly.

Some of the future research works which can be undertaken in the field of Physical Layer Security are :

– Accurate fading channel models play a remarkable role in an optimal secure transmission design over 5G. Thus, some efforts have been oriented to propose new more accurate channel models that provide a better fit to field measurements in a variety of new mm-Wave propagation scenarios. Therefore, the performance of Physical Layer Security techniques over these generalized channels is an important topic for further research work.

- Due to the combination of innovative technologies to cover the growing demands of data traffic and emerging services, it is essential to investigate PLS techniques regarding these new network scenarios. Within these networks, the following stand out: Unmanned Aerial Vehicles (UAV), enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low-Latency Communications (URLLC), massive Machine-Type Communications (mMTC), and Vehicle-to-Everything (V2X) networks.

– In the security paradigms, a promising direction of research is the integration of PLS and the classic wireless cryptography. Specifically, the physical layer features of the wireless medium can be exploited for designing new security algorithms to improve the current authentication and key management in higher layers. However, the integration of both approaches has not been properly studied at present. Thus, this topic needs further research.

– An interesting future research direction could be to provide a detailed survey on the main drawbacks and merits of physical layer authentication (PLA) and Secret-Key Generation in 5G. In this sense, a research field, which is not yet investigated extensively in the literature, is the machine learning for intelligent PLA in 5G wireless networks.

**REFERENCES**

For Books –

Mr. Aaron J. Kennelly , “Wireless Networks Security”, April 20, 2005

For websites –

[1]. http://www.researchgate.net

[2]. http://www.amazonaws.com

[3]. http://www.nptel.org

[4]. <http://www.academics.org>

For Journals -

[1] Graham, E., Steinbart, P.J. (2006) Wireless Security

[2] Cisco. (2004). Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, July 19.

[3] CSI. (2004). CSI/FBI Computer Crime and Security Survey.

[4] Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.

International Journal of Multimedia and Ubiquitous Engineering

Vol. 3, No. 3, July, 2008

85

[5] Kelley, D. (2003). The X factor: 802.1x may be just what you need to stop intruders

from accessing your network. Information Security, 6(8), 60-69.

[6] Kennedy, S. (2004). Best practices for wireless network security. Information Systems

Control Journal (3).

[7] McDougall, P. (2004, March 25). Laptop theft puts GMAC customers’data at risk.

Information Week Security Pipeline.

[8] Nokia. (2003). Man-in-the-middle attacks in tunneled authentication protocols.

[9] Paladugu, V., Cherukuru, N., & Pandula, S. (2001). Comparison of security protocols

for wireless communications.

[10] Slashdot. (2002, August 18). Wardriving from 1500ft Up.

[11] Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). Risk management guide for

information technology systems. NIST Special Publication 800-30.

[12] Wailgum, T. (2004, September 15). Living in wireless denial. CIO Magazine.