OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

WIRELESS BUDDY

Shivani Varma[1], Prasad Moze[2], Afraaz Shaikh[3], Atul Rokade[4], Prof. Trupti Suryawanshi[5]

UG Student, Department of Computer Engineering, Keystone School of Engineering, Pune[1,2,3,4]

Assistant Professor, Department of Computer Engineering, Keystone School of Engineering, Pune[5]

shivanimvarma@gmail.com[1], prasad97moze@gmail.com[2], afraazshaikh70@gmail.com[3], atulrokade1427@gmail.com[4], truptisuryawanshi12@gmail.com[5]

ABSTRACT: Now a day's android phones are used for the various applications. We can use android phone for monitor and control the network. It is to control the network when network admin is in admin office but it is difficult to control the network from outside the office. It is integrated software solution that allows a network admin to remotely monitor his LAN network by his Android phone with GUI. The main purpose of this application is to provide all the important details of the network to the admin on their android phone with the help of GPRS or Wi-Fi. We are using data connectivity or Wi-Fi to connect the mobile phone to LAN server. And we also are using password encryption for authentication in phone.

Keywords: Network Security, LAN Monitoring Server, Virtual Network Computing (VNC), GPRS/Wi-Fi, Network/LAN Monitoring.

----------∴∴∴----------

I INTRODUCTION

Numerous studies on measurement and characterization of remote i.e. wireless LAN's (WLANs) have been performed recently. Then, wireless monitoring, the traffic measurement from a wireless vantage point, is additionally generally received in both wireless research and business WLAN management product development. Wireless monitoring technique can give detailed PHY/MAC information on wireless medium. For the network analysis reason (e.g. abnormality detection and security monitoring) such point by point wireless information is more helpful than the data gave by SNMP or wired monitoring.

This project is useful for monitoring the nodes in networks. We can access or monitor the LAN by our mobile device. We can perform number of action on remote PC through the handheld device i.e. Android phone. This system develops an integrated software application that will help network admin to remotely monitor network through android phone. The communication between the client and the android phones is done through the server.

We develop a LAN monitoring System in which the LAN is handled by a Mobile App. Nowadays everything is very easy to handle by Android by a single small Android Device. So, In LAB or in any the client PCs are can be handled by server but we can't handle server from another location. So we plan to access that server i.e. LAN by Android Device wirelessly.

II GOALS AND OBJECTIVES

The main goal of this system is to provide maximum information about the network to the administrator on their android phones when administrator is not present there. Helps in preventing unauthorized use of hardware devices and software.

- Allows administrator to perform various activities like PC shutdown, screenshots, activate/ kill processes etc.
- Provides bidirectional communication between client and admin.
- Platform Dependent
- Extensive in Nature
- Secure
- User-friendly GUI

III LITERATURE SURVEY

The goals of this paper is understanding of wireless user behavior and wireless network performance by comparing and contrasting the workload, to characterize wireless users in terms of a parameterized model for use with analytic and simulation studies involving wireless LAN traffic, and to apply our workload analysis results to better understand issues in wireless network deployment and potential network optimizations. [1]

This paper focuses on the threats posed by denial-of-service (DoS) attacks against 802.11's MAC protocol. Such attacks, which prevent legitimate users from accessing the network, are a vexing problem in all networks, but they are particularly threatening in the wireless context. [2]

This paper describes the use of a novel and efficient discovery method using neighbor graphs and non -overlap graphs. This method reduces the total number of probed channels as well as the total time spent waiting on each channel. The implementation results show that this approach reduces the overall probe time significantly when compared to other approaches. [3]

These papers examine the vulnerabilities of wireless networks and argue that we must include intrusion detection in the security architecture for mobile computing environment. Developed such architecture and evaluated a key mechanism in this architecture, anomaly detection for mobile ad-hoc network, through simulation experiments. [4]

IV PROPOSE SYSTEM

Using the mobile the administrator can perform following actions:

a) Kill Process b) Start Process c) Net view d) Shut down

The server keeps the list updated to check the live hosts working in the network. The server can contact with the particular client using his ID.

The basic flow of the system with MVC is given below:

- Client submits login request to Android Activity.
- Android Activity acts as controller.
- Activity requests DB to verify whether the database is having the same user name and password, if found login operation is successful.
- Controller then gives response back to Android Activity which displays the Android XML file on Mobile.
- It prepares presentation response on to the Mobile.

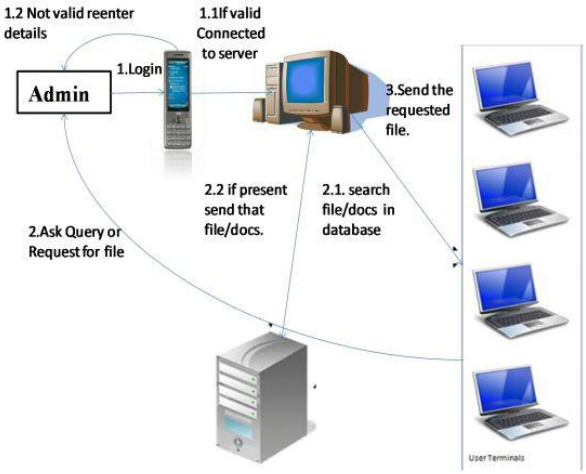

Fig 1: System Architecture

V CONCLUSION

The main purpose of this application is to provide all the important details of the network to the admin on their android phone with the help of GPRS or Wi-Fi. We are using data connectivity or Wi-Fi to connect the mobile phone to LAN server. And we also are using password encryption for authentication in phone.

VI FUTURE SCOPE

- Provide more security
- Provide scalability
- Provide parallelism
- Integration with schools and colleges

REFERENCE

[1] A. Balachandran, G. M. Voelker, P. Bahl, P. V. Rangan, "Characterizing User Behavior and Network Performance in a Public Wireless LAN".

[2] John Bellardo and Stefan Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions".

[3] Minho Shin, Arunesh Mishra, William A. Arbaugh, "Improving the Latency of 802.11 Hand - offs using Neighbor Graphs".

[4] Yongguang Zhang, Wenke Lee, Yi An Huang, "Intrusion Detection Techniques for Mobile Wireless Networks".

[5] Abigail Paradise, Asaf Shabtai, Rami Puzis, Aviad Elyashar, Yuval Elovici, Mehran Roshandel, and Christoph Peylo, "Creation and Management of Social Network Honeypots for Detecting Targeted Cyber Attacks".

[6] Jana Medkova, Martin Husak, Martin Vizvary , Pavel Celeda, "Honeypot Testbed for Network Defence Strategy Evaluation".

[7] leksey A. Egupov , Sergey V. Zareshin , Igor M. Yadikin , Dmitry S. Silnov, "Development and Implementation of a Honeypot Trap".

[8] Ozge Cepheli, Guido Dartmann, Gunes¸ Karabulut Kurt, "An Encryption Aware Physical Layer Security System", 2018.