Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444
Volume 3, Issue 4, April-2016

A Framework for Wireless LAN Monitoring and Its Applications.

Shashank Gawade, Shashank Kubal, Vidyesh Thakoor, Vinay Thakoor

Computer Engineering Department, Dr.D.Y.Patil Collage Of Engineering Ambi Talegaon.

Abstract —Numerous studies on measurement and characterization of remote i.e. wireless LAN's (WLANs) have been performed recently. The majority of these measurements have been conducted from the wired part of the system in based on wired monitoring (e.g. sniffer at some wired point) or SNMP measurements. 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. In this paper we have investigated different issues in implementing the wireless monitoring system for an IEEE 802.11 based wireless network. We distinguish the pitfalls that such system needs to be aware of, and after that give feasible solutions to avoid those pitfalls. We implement a genuine wireless monitoring system and show its effectiveness to characterizing typical computer science WLAN traffic. Our characterization uncovers rich information about the PHY/MAC layers of the IEEE 802.11 protocol, for example, the typical traffic mix of distinctive frame types, their temporal characterization and relationship with the client exercises. Additionally, we distinguish different anomalies in protocol and security of the IEEE 802.11 MAC. With respect to security, we identify malicious utilization of WLAN, for example, email worm and system checking. Our outcomes likewise demonstrate excessive re-transmissions of some management frame types reducing the helpful throughput of the wireless network.

Keywords- *WLAN,LAN ,wireless network ,SNMP.*

I. INTRODUCTION

With the popularity of the IEEE 802.11 based wireless networks ,it has become increasingly important to understand the characteristics of the wireless traffic and the wireless medium itself. It is found that the measurements have been conducted on the wired portion of the network and/or combined with *SNMP* logs. The measurements at such wired vantage points can provide accurate traffic statistics as seen in that portion of the network. However ,practically they do not effectively expose the instantaneous wireless medium characteristics i.e. PHY/MAC in the IEEE 802.1.The reasons are that SNMP exploits the summary data polled periodically in typically between every 1 - 5 minutes1 and wired monitoring completely relies on the information observed at the wired portion.

Instantaneous wireless PHY/MAC data is very important for security observation in the IEEE 802.11 wireless network. It is well known that the IEEE 802.11 WLAN has security vulnerability due to the flaws in the MAC protocol and basic features of wireless networks, such as open medium and mobility. To accurately diagnose such security issues we need to monitor both MAC operations and mobile user activities instantaneously. Therefore ,with such instantaneous wireless PHY/MAC information, security monitoring and surveillance can be effectively performed. To capture such detailed PHY/MAC information, wireless monitoring technique can be used. Recently, wireless monitoring is widely adopted in both wireless research, and commercial WLAN management product development.

II. LITERATURE REVIEW

2.1 Introduction

A literature survey is a discussion of the literature in a given area of the study. It is concise overview of what has been studied, argued and established about a topic, and it is usually organized chronologically or thematically. It is not an annotated bibliography, because it groups related works together and discusses trends and developments rather than focusing on one item at a time. It is not a summary, rather it evaluates previous and current research in regard to how relevant and or useful it is.

2.2 Technology Information

Android:-

Android is an operating system based on Linux with a Java programming interface. The Android Software Development Kit (Android SDK) provides all necessary tools to develop Android applications. This includes a compiler, debugger and a device emulator, as well as its own virtual machine to run Android programs. Android is currently primarily developed by Google. Android allows background processing, provides a rich user interface library, supports 2-D and 3-D graphics using the OpenGL libraries, access to the file system and provides an embedded SQLite database. Android applications consist of different components and re-use components of other applications.

Emulator:-

All Rights Reserved, @IJAREST-2016

A software package that mimics the hardware functionality of a given platform. Used for testing and development of solution applications.

SDK:-

Software Development Kit - A set of development tools that enable a developer to create applications from a pre-designed software framework.

WAP:-

This refers from Remote Monitoring and Control Using Mobile Phones Embedded Wireless Information Servers by Dr. Mikael Sj¨odin WAP [17] (Wireless Applications Protocol) was designed to remedy the problems with using web servers in wireless networks and embedded environments. It builds on the same concepts as the Web and reuses much of techniques and standards for the Web. The WAP standard calls for three different servers to be involved in WAP communication. An ISP (Internet Service Provider), a WAP gateway, and a web server. However, when building embedded information servers, these three can be efficiently combined into a single entity, thus reducing the complexity of implementing WAP, but still gaining its benefits. We call such a combination a WAP server.

JAVA:-

Java[2] is a set of several computer software products and specifications from Sun Microsystems (which has since merged with Oracle Corporation), that together provide a system for developing application software and deploying it in a cross-platform computing environment. Java is used in a wide variety of computing platforms from embedded devices and mobile phones on the low end, to enterprise servers and supercomputers on the high end. While less common, Java applets are sometimes used to provide improved and secure functions while browsing the World Wide Web on desktop computers.

SQLite:-

SQLite, the most popular Open Source SQL database. **SQLite**[21] is a relational database management system contained in a small C programming library. In contrast to other database management systems, SQLite is not a separate process that is accessed from the client application, but an integral part of it.

2.3 Summary

Sr. No.	Parameters	Alternatives		
		WiFi	**WiMAX**	**Wirelss (Proposed System)**
01	**Range**	Upto 100 metres	About 15 kms.	More than WiFi & WiMAX
02	**Boosting of signal**	Limited	Upward of 50 kms.	Great extent
03	**Sort of connection**	Not required	Not required	Not required
04	**Scope**	Good	Better	Best
05	**Frequency**	2.4-5.8 GHZ.	15-16 GHZ.	Great extent

Table 2.1: Comparisons for mediums

All Rights Reserved, @IJAREST-2016

III. SURVEY OF PROPOSED SYSTEM

In our paper, we focus on implementing an effective wireless monitoring system and demonstrating its effectiveness in traffic characterization and network diagnosis like anomaly detection and security monitoring. Mainly, we first focus on some situations phy/mac information. We conduct a number of controlled experiments to identify the pitfalls of wireless monitoring .for the identified pitfalls, we propose feasible solutions and implement them to provide a wireless monitoring system. After showing the effectiveness of the solutions, we apply our wireless monitoring system to a real wlan traffic in computer science department in a university, over a period of two weeks. Then, this system show how the monitored data can be effectively used for both wlan traffic characterization and network diagnosis.

IV. MATHEMATICAL MODEL

Let S be the set of Whole system which consists:

S= {L_User, Client, Server, Administrator }

Where,

1. L_User is the lan user of the system.

   L_User={Ulist,ChatList}.

   Where,
2. Ulist is set of number of users in the system

   Ulist={user1,user2,……..usern}

3. Chatlist is used to get list of online users.

4. Client={Clist, loginId, connection_req, selectpc, a_command}.

5. Clist is the set of number of clients in the system.

6. Clist={client1,client2,……clientn}.

7. loginId is used by users to login and use the product

8. Server is used for sending commands.
   Server{Database, updatedb, connect, register, command ,fetch}.

9. updateddb is used to keep the records of the users.

10. Invite_connection is used to invite a client for chatting.

11. Register = (loginId, password).

12. Execute = used to execute the command.

13. Result = gives the result of the command.

14. Remove_req = request by user to remove himself from the n/w.

All Rights Reserved, @IJAREST-2016

15. Remove = use to remove a user.

IV. SYSTEM ARCHITECTURE

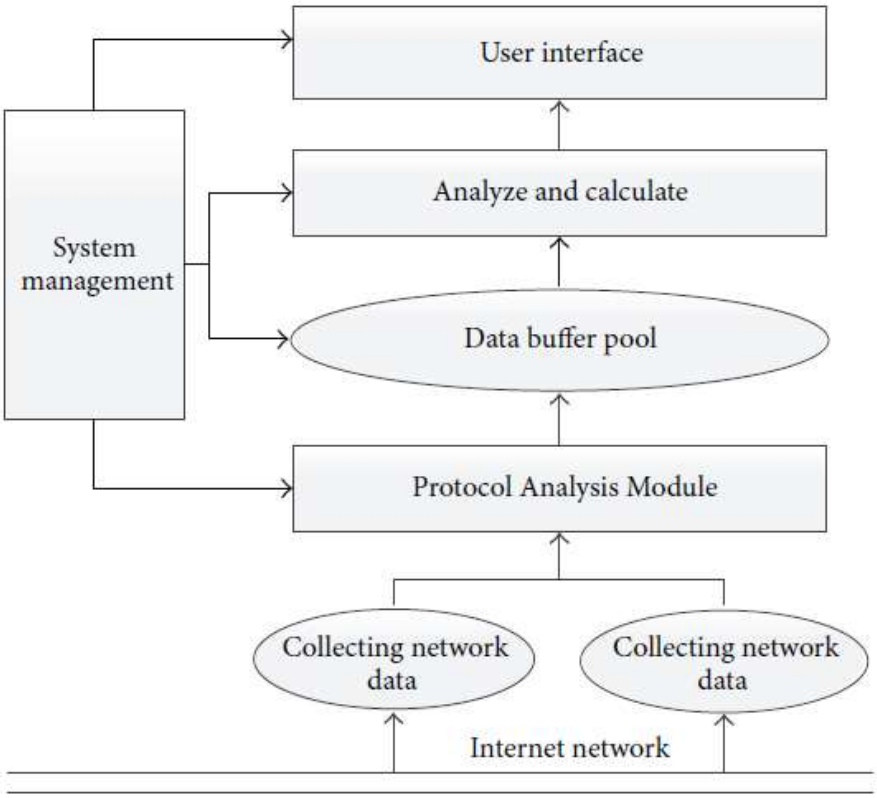

Fig 1:-SYSTEM ARCHITECTURE

V. CONCLUSION AND FUTURE WORK

The available techniques for monitoring and controlling are perfect in themselves. But to improve the accuracy, more efforts need to be taken. In the proposed technique, we have used the Wi-Fi network and LAN. The system will provided a low cost, secure, accessible, remotely monitored and controlled solution for LAN monitoring using wireless media is been introduced. The use of a mobile, wireless media, Server provides exciting possibilities. However as far as the company applications are concerned this can be seen as a low cost, customized wireless LAN monitoring system. Thus this solution can be customized to suit any other company requirement related to monitoring and controlling LAN network. The target to control LAN network remotely using the wireless media for satisfying user needs and requirements. Wireless technology capable solution has proved to be controlled remotely, provide security and is cost-effective as compared to the previously existing systems. Hence we can conclude that the aim and objective of the system is achieve by this proposed system .

VI. ACKNOWLEDGMENTS

We might want to thank the analysts and also distributors for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

VII. REFERENCES

[1] A. Balachandran, G.M. Voelker, P. Bahl and V. Rangan.Characterizing User Behavior and Network Performance in aPublic Wireless LAN In *Proc. ACM SIGMETRICS 2002*,Marina Del Rey, CA, June 2002.

[2] S. Banerjee and A. Agrawala. Estimating Available Capacityof a Network Connection. In *Proceedings of IEEEInternational Conference on Networks*, September 2001.

All Rights Reserved, @IJAREST-2016

[3] J. Bellardo and S. Savage. 802.11 Denial-of-Service Attacks:Real Vulnerabilities and Practical Solutions. In *Proceedingsof the USENIX Security Symposium*, Washington D.C.,August 2003.

[4] B.J. Bennington and C.R. Bartel. Wireless Andrew:Experience building a high speed, campus-wide wireless datanetwork. In *Proceedings of MOBICOM*, September 1997.

[5] N. Borisov, I. Goldberg and D. Wagner. Intercepting MobileCommunications: The Insecurity of 802.11. In *AnnualInternational Conference on Mobile Computing AndNetworking*, Rome, Italy, July 2001.

[6] Computer Associates. Virus Information Center(Win32.Netsky.B Virus)http://www3.ca.com/virusinfo/virus.aspx?ID=38332

[7] D. Eckardt and P. Steenkiste. Measurement and Analysis of the Error Characteristics of an In-Building Wireless Network. In *Proceedings of SIGCOMM*, August 1996.

[8] Enterprise Wireless LAN Security and WLAN Monitoring. http://www.airdefense.net/

[9] S. Fluhrer, I. Mantin and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. In *Lecture Notes in Computer Science*, 2259, 2001.

[10] M. Raya, J-P. Hubaux and I. Aad. DOMINO A System to Detect Greedy Behavior in IEEE 802.11 Hotspots. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services*, Boston, MA, June 2004.

[11] IEEE Computer Society LAN MAN Standards Committee. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Speci_cations. In *IEEE Std 802.11-1999*, 1999.

[12] IEEE Computer Society LAN MAN Standards Committee. IEEE 802.11 Management Information Base In *IEEE Std 802.11-1999*, 1999.

[13] THE IMAP Connection. http://www.imap.org/

[14] D. Kotz and K. Essien. Analysis of a Campus-wide Wireless Network. In *Proc. the Eighth Annual International Conference on Mobile Computing and Networking (MOBICOM 2002)*, Atlanta, GA, September 2002.

[15] P. Kyasanur and N. Vaidya. Sel_sh MAC Layer Misbehaviorin Wireless Networks. In *IEEE Transactions on Mobile Computing*, April, 2004.

All Rights Reserved, @IJAREST-2016