A Perspective on Estimation of Available Capacity in Wireless Networks

H.S. Ramesh Babu[1], Gowrishankar[2], and P.S. Satyanarayana[3]

[1] Department of Information Science and Engineering,
Acharya Institute of Technology,
Bangalore – 560090, Karnataka, India
[2] Department of Computer Science and Engineering,
B.M.S. College of Engineering,
Bangalore – 560019, Karnataka, India
[3] Department of Electronics and Communication Engineering,
B.M.S. College of Engineering,
Bangalore – 560019, Karnataka, India
rameshbabu@acharya.ac.in,
{gowrishankar.cse,pssvittala.ece}@bmsce.ac.in

Abstract. To understand the characteristics of the wireless networks, the network usage data from wireless measurement tools are essential. The data collection is a process of collecting the network time-varying information in standardized formats and from standard interfaces. The characteristics of the wireless networks include, signal propagation, received signal quality, network traffic, active applications and mobility of the MT. The purpose of the measurement is to collect vital data of the wireless network. There are several tools available for this purpose. The most widely used network measurement tools are client side measurement tool, Syslog, Simple Network Management protocol(SNMP), network sniffing, wireless sniffing. This paper discusses the different wireless measurement tools like Syslog, Simple Network Management protocol, network sniffing, wireless sniffing and their benefits and limitations.

Keywords: Wireless networks, Syslog, Simple Network Management protocol, network sniffing, wireless sniffing**.**

1 Introduction

The data collection is a process of collecting the network time-varying information in standardized formats and from standard interfaces. This needs a Portable tool for data collection. The collected data need to be processed effectively without losing the "tail" of the data and identifying holes and cleaning data. In the pre-processing mechanism, the time-varying network parameters are arranged in an order. These time series may have few missing entries, due to the minor flaws in the measurement tools, which are estimated and filled using time series techniques.

There are many implicit differences in wired and wireless medium. Wired medium will have clear points of connection but wireless medium is physically dispersed. The

Y. Cai et al. (Eds.): Mobilware 2010, LNICST 48, pp. 451–461, 2010.

mobility in wireless networks and novel devices used inspires new usage patterns. In this prevailing scenario, the measurement of wireless network information is essential. This strengthens our understanding of user and network behaviours. The better understanding leads to better network models. The improved network models are momentous to improvement in terms of network protocols, distributed algorithms, applications and improved deployment strategy.

The NGWN provides users with a wide range of services across HWNs coexisting with diverse throughput and coverage with a single MT. The existing cellular networks will provide communication services over a wide geographical area but has limited bandwidth to support emerging data services. But the future 3G cellular and 4G systems, such as UMTS, Wi-Max (802.16), have lesser coverage and higher bandwidth when compared to cellular networks. The WLAN (IEEE 802.11a/b/g/n) is able to provide higher data rate but with lesser coverage compared to cellular and 4G systems. Therefore an integration of cellular networks, Wireless Local Area networks (WLAN) and Wi-MAX would result in higher bandwidth, more network coverage and will also help in enhanced user mobility and with choice of new services and enhanced QoS [1]. The Speed v/s Mobility comparison for wireless networks is represented in Figure1. The characteristics of the different wireless networks are depicted in table 1.

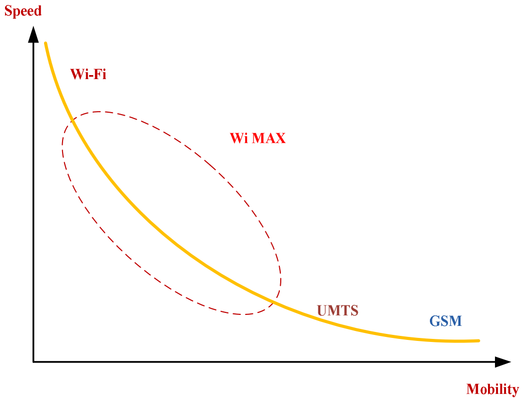


Fig. 1. Speed v/s Mobility comparisons of different wireless networks

The process of network switching will involve the following three phases – network discovery, switching decision and execution [2]. The decision phase will play an important role in balancing network utilization, fulfilling the user requirements and QoS requirements of network applications. Thus, the need of effective decision mechanism is crucial. The decision mechanism is driven by a set of QoS parameters [3-6]. The QoS parameters are bandwidth, BER and cost. The criteria that affect these QoS parameters are wireless link quality and the current network load. The factors that influence link quality are noise and signal fading [7]. The Signal to Noise Ratio (SNR) value of the wireless channel can be considered as the measure of the channel quality in a wireless network. The network load is measured based on the number of active users and their network sessions and is also called as network traffic [8].

The signal fading in a wireless system is common phenomena of the radio channel. They are classified into two types, *Flat fading* and *Frequency selective fading*. In a narrowband wireless channel, the consistency bandwidth of the channel is larger than the bandwidth of the signal. In such channels all frequency components of the signal will experience the same amount of fading. Such a fading is called as *'Flat fading'*. On the other hand, in a wideband wireless channel the coherence bandwidth of the channel is smaller than the bandwidth of the signal. This result in Different frequency components of the signal, experiencing the different amount of fading called as *'frequency selective fading'*. Apart from these two types of fading, when the MT is moving at a high speed, the signal strength varies severely and undergoes deep fading within the small time frame. This type of fading is named as 'Fast fading' [9].

The next generation wireless systems typically have higher bandwidth and support optimal mobility, need to challenge with the frequency selective fading and fast fading. The next generation wireless systems make use of low complexity techniques such as Orthogonal Frequency Division Multiplexing (OFDM) in the physical layer and Orthogonal Frequency Division Multiple Access (OFDMA) mechanisms in the link layer to prevail over the effect of frequency selective fading [10].

2 Wireless Network Measurements

To understand the characteristics of wireless networks, the network usage data from wireless measurement tools are essential. The characteristics include signal propagation, received signal quality, network traffic, active applications and mobility of the MT. The purpose of the measurement is to collect vital data of the wireless network. There are several tools available for this purpose. The most widely used network measurement tools are client side measurement tool, Syslog, Simple Network Management protocol (SNMP), network sniffing, wireless sniffing.

2.1 Client Side Network Management Tools

The wireless measurement tools mentioned above i.e. Syslog, SNMP, and Network sniffing and wireless sniffing tools are intended to monitor the network from the viewpoint of the network. In client side methods the measurement tools are installed in client to measure the activities at the client side. This client side measurement has many advantages.

A client side tool can accurately determine what exactly a client is doing. While Syslog will provide information about set of clients which are associated to the particular AP/BS, a client side tool can list all the APs/BSs that a client can handle, which are useful for mobility tracing. A client side tool can list all the applications that are running on it, rather than just those applications that generate network traffic. Client side tools are extensively used in WMAN and WWAN measurements [11] [12].

Writing a generic client side program, such as *tcpdump, Wireshark* formerly called *Ethereal* and *kismet*, will be a challenging task because it has to run on varieties of operating systems and different device drivers.

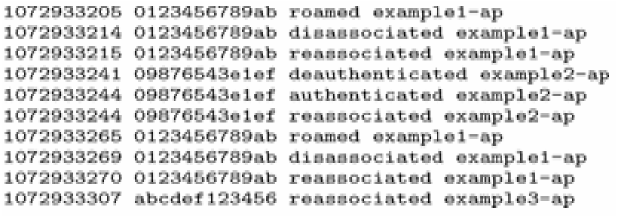
Table 1. Attribute comparisons of Different Wireless Networks

Wireless Network	*Bandwidth (Mbps)*	*Modulation Technique*	*Freq (GHz)*	*Coverage*	
				Indoor Coverage	*Outdoor Coverage*
IEEE802.11a	20	OFDM	5	35 Meters	120 Meters
IEEE802.11b	11	DSSS	2.4	38 Meters	140 Meters
IEEE802.11g	54	OFDM/ DSSS	2.4	38 Meters	140 Meters
IEEE802.11n	600	OFDM	5	70 Meters	250 Meters
HiperLAN2	54	OFDM	5	50 Meters	50 Meters
802.16e	Up to 125	OFDMA	2-6	Up to 35000 Meters (35Kms)	
802.16m	Up to 300	OFDM	Upto6	Up to 50000 Meters (50 Kms)	
EDGE Evolution	9.6- 384	TDMA/ FDD	900/ 1800/1 900 MHz	Up to 40000 Meters (40kms)	
UMTS W-CDMA	2	FDD, TDD	2	Up to 20000 Meters (20kms)	

2.2 Syslog

Syslog records detail steps of association, and have been used effectively for studying user activity patterns [13] [14]. To all intents and purposes Syslog is a standard for sending and receiving of log messages [15]. The wireless APs and BSs can be configured to log appropriate events in the network. The Syslog messages are used to understand the state of an MT in the wireless network. The AP or BS can generate a time stamped message whenever an MT *authenticates, de-authenticates, associates, disassociates or roams* to that AP or BS. By collecting these messages it is possible to determine the state of the MTs on the network. The Syslog messages are stored and analyzed locally in the BS or transmitted across the network for storage and analysis by a dedicated computer.

There is no standard format for Syslog messages. The messages that APs or BSs send can vary in format and amount of information contained. In most of the cases APs and BSs manufactured from same manufacturer will have different Syslog message formats. In certain cases the message formats differ for each version of the same product. In a heterogeneous wireless environment, multiple type of APs and BSs with varieties of Syslog message formats. It is necessary to translate these messages in to an intermediate format prior to the data analysis. In some of the measurement studies [16] [17], the multiple Syslog message formats are translated to general, intermediate parsed format for the purpose of analysis. Figure 2 indicates the parsed Syslog trace data format.



```
1072933205 0123456789ab roamed example1-ap
1072933214 0123456789ab disassociated example1-ap
1072933215 0123456789ab reassociated example1-ap
1072933241 09876543e1ef deauthenticated example2-ap
1072933244 09876543e1ef authenticated example2-ap
1072933244 09876543e1ef reassociated example2-ap
1072933265 0123456789ab roamed example1-ap
1072933269 0123456789ab disassociated example1-ap
1072933270 0123456789ab reassociated example1-ap
1072933307 abcdef123456 reassociated example3-ap
```

Fig. 2. Parsed Syslog Format

2.3 SNMP

The SNMP is a generic tool in measuring and managing a network device, called *'network object'* in the network management terminology [18]. The SNMP provides information on both traffic volume and the number of active users. This makes the SNMP the most suitable technique used for both traffic studies [14] [19] [20] and user mobility studies [21].

A network administrator runs a tool known as *'manager'*, which communicates with SNMP *'agents'*. Agents run on network objects and provide interface between the object and manager. A network object can contain several objects, such as statistics or configuration items, arranged in a database known as *Management Information Base (MIB).* The network statistics are stored in the MIB variables and these variables are represented in a standard format known as Abstract Syntax Notation (ASN) .The manager queries the agent for the purpose of measurement and agent replies by extracting information from the MIB variables. Both request and reply will be in the standard SNMP message format [22]. In the recent version of SNMP few MIB variables, like MAC address, IP address, Signal strength, Power saving mode, Network session length and Traffic of the MT associated with AP or BS, are specific to the wireless network [23].

Some of the advantages of the SNMP are

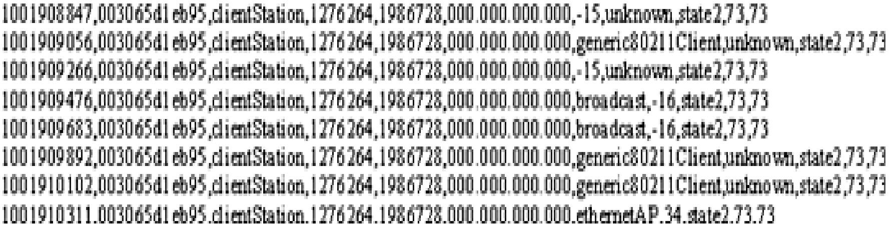
- SNMP messages provide more detailed information about the status of the network than Syslog messages.
- SNMP provides information on both traffic volume and the number of active users. Hence it is suitable to be used for both traffic studies and user mobility studies.
- SNMP messages are generally device independent and are usually available in a standard format.

The drawbacks of SNMP are

- SNMP-based approaches is that they require an interval between SNMP polls (typically every 1–5 minutes), and it has been shown that long poll intervals may miss wireless clients that associate with APs for less than this poll interval [24].
- The SNMP-based approaches may be able to retrieve such detailed wireless MAC/PHY information through the use of a properly defined MIB, the most existing SNMP MIBs for APs (MIB-I (RFC 1066), MIB-II (RFC 1213), and 802.11 MIB (IEEE Std 802.11-1999)) provide very limited visibility into MAC-level behaviour.

2.4 Network Sniffing

The network or packet *sniffing* refers to the process of capturing of the network traffic at the network interface. For the purpose of sniffing, the network interface should be in a promiscuous mode. In this mode the interface will ignore its assigned address and captures all the frames/packets present in the network. There are programs, such as *tcpdump*, *Ethereal* and *kismet,* which will capture and analyze the frame/packet [25] [26] [27].



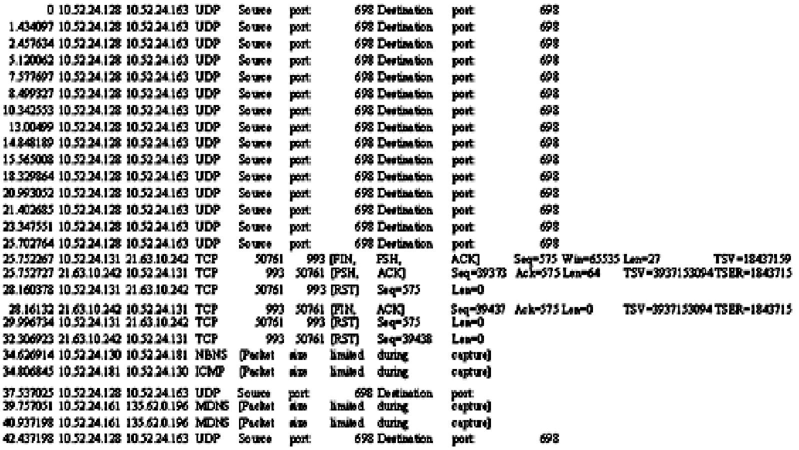
```
1001908847,003065d1eb95,clientStation,1276264,1986728,000.000.000.000,-15,unknown,state2,73,73
1001909056,003065d1eb95,clientStation,1276264,1986728,000.000.000.000,generic80211Client,unknown,state2,73,73
1001909266,003065d1eb95,clientStation,1276264,1986728,000.000.000.000,-15,unknown,state2,73,73
1001909476,003065d1eb95,clientStation,1276264,1986728,000.000.000.000,broadcast,-16,state2,73,73
1001909683,003065d1eb95,clientStation,1276264,1986728,000.000.000.000,broadcast,-16,state2,73,73
1001909892,003065d1eb95,clientStation,1276264,1986728,000.000.000.000,generic80211Client,unknown,state2,73,73
1001910102,003065d1eb95,clientStation,1276264,1986728,000.000.000.000,generic80211Client,unknown,state2,73,73
1001910311.003065d1eb95.clientStation.1276264.1986728.000.000.000.000.ethernetAP.34.state2.73.73
```

Fig. 3. Set of SNMP Messages

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. *Kismet* is good for WLAN surveillance. It is capable to sense the details of all wireless access points (WAPs) and WLAN nodes, showing channels, use of encryption and signal strength.

Ethereal is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. You could think of a network packet analyzer as a measuring device used to examine what's going on inside a network cable. The Ethereal is not an intrusion detection system. It will not warn when someone does strange things on the network that he/she isn't allowed to do. However, if strange things happen, Ethereal might help you figure out what is really going on. Ethereal will not manipulate things on the network, it will only "measure" things from it. Ethereal doesn't send packets on the network or do other active things (except for name resolutions, but even that can be disabled). The trace of an ethereal is shown in figure 4.

The important concern with network sniffing is that the volume of data generated from the sniffing process is much larger than Syslog and SNMP. A typical sniffing of 802.11b wireless network operating at 11 Mbps speed can generate several gigabits of data within few minutes. It is vital to ensure that sufficient disk space is available to store the captured frames/packets in the hard disk. Another major concern in the network sniffing is the privacy of captured information.



```
        0 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
 1.434097 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
 2.457634 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
 5.120062 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
 7.577697 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
 8.499327 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
10.342553 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
 13.00499 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
14.848189 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
15.565008 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
18.329864 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
20.993052 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
21.402685 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
23.347551 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
25.702764 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
25.752267 10.52.24.131 21.63.10.242 TCP     50761      993 [FIN,  PSH,      ACK]     Seq=575 Win=65535 Len=27        TSV=18437159
25.752727 21.63.10.242 10.52.24.131 TCP       993    50761 [PSH,  ACK]      Seq=39373 Ack=575 Len=64   TSV=3937153094 TSER=1843715
28.160378 10.52.24.131 21.63.10.242 TCP     50761      993 [RST]  Seq=575   Len=0
 28.16132 21.63.10.242 10.52.24.131 TCP       993    50761 [FIN,  ACK]      Seq=39437 Ack=575 Len=0    TSV=3937153094 TSER=1843715
29.996734 10.52.24.131 21.63.10.242 TCP     50761      993 [RST]  Seq=575   Len=0
32.306923 21.63.10.242 10.52.24.131 TCP       993    50761 [RST]  Seq=39438 Len=0
34.626914 10.52.24.130 10.52.24.181 NBNS [Packet size  limited during   capture]
34.806845 10.52.24.181 10.52.24.130 ICMP [Packet size  limited during   capture]
37.537025 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port
39.757051 10.52.24.161 135.62.0.196 MDNS [Packet size  limited during   capture]
40.937198 10.52.24.161 135.62.0.196 MDNS [Packet size  limited during   capture]
42.437198 10.52.24.128 10.52.24.163 UDP  Source  port      698 Destination  port       698
```

Fig. 4. Network Sniffing Trace

The frame/packet that is captured through sniffing may contain sensitive data especially when the data within the frame/packet is not encrypted. The issue of privacy may be alleviated by only capturing the header data, which may be sufficient for a network measurement. Even with this, the privacy problem is not completely overcome as some vital information, such as packet size, MAC/IP address, higher layer protocol and inter-arrival time, stand exposed. The result of such a sniffing is referred to as a trace.

2.5 Wireless Sniffing

The wireless sniffing is a WLAN measurement tool [28]. Syslog, SNMP and network sniffing are the generic measurement tools which will be used in measuring all types of wireless as well as wired networks. The wireless sniffing is a measurement tool useful only for a wireless network. It will operate at AP/BS or at a switch that connects wireless network to the wired backbone. The disadvantage of wire side measurement is that not all wireless data observable from the wired network, such as management frames, beacons, retransmissions and collisions, send traffic via wired network. The wireless sniffer is widely used to collect the MAC level frame information in a wireless network. Even though wireless sniffer can be installed on a host under measurement, but in majority of cases, it is installed on an autonomous device. This independent device could be a laptop or any MT or a PDA system. This makes the wireless sniffer to monitor the wireless network in promiscuous mode without interfering with the stations under study/monitoring. Wireless sniffers capture both the data frames as well as management frames. The management frames captured by wireless sniffer includes beacon frames, request to send (RTS) frames, clear to send (CTS) frames and Acknowledgement (ACK) frames. Nevertheless, there is need of special hardware and software in form of drivers is essential for effective working of a wireless sniffer. *Ethereal* and *Kismet* are the most admired wireless sniffer and analyzer software. There are good amount of research works reported on wireless performance using Wireless sniffers .The measurement of streaming media over wireless link using independent sniffers [29][30], measurement of congestion in wireless LAN [31],the network monitor research in [32],a complete wireless sniffer system is implemented and used to characterize a typical computer science department WLAN traffic.

Wireless measurement can be applied to the mobile host. This is accomplished by placing wireless network interface card in a *monitor* mode. In this mode, the wireless card captures all types of frames/packets. These frames/packets may be analyzed similar to those of network sniffing. Since this mode is not a promiscuous mode it limits the wireless sniffer in the mobile host as a simple network monitoring tool. Figure 6 shows an example of wireless sniffing trace.

The advantages and disadvantages of wireless sniffing are as listed below

Advantages of wireless sniffing are:

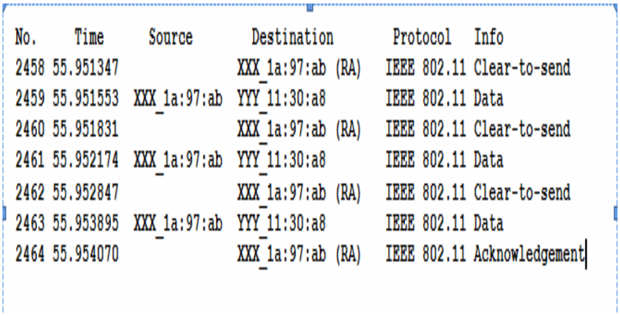
- Wireless Sniffing done be an independent sniffer in a promiscuous mode will not cause any interference with the hosts under test in wireless experiment. Therefore, sniffing can be used to measure these devices, such as the wireless game consoles, which do not provide general accesses for measurement purpose.
- Wireless sniffing can provide frame level information and wireless network conditions, such as the RSSI and sending capacity.
- Wireless sniffers can be used as wireless network diagnostic tools as they are capable to capture wireless management frames, such as RTS, CTS, Authentication/De-authentication frames, and Association/Disassociation frames.

Disadvantages of Wireless sniffers are:

- Wireless sniffers cannot record all the frames that are transmitted over the network [31] [33] since the sniffer is only capturing the frames at its own location this results in non-capturing of the packets lost due to a hidden terminal and packets lost due bit errors.
- The Received Signal Strength Indicator (RSSI) is measured relative to the wireless sniffer installation location. This measurement of received signal strength may not be same as the AP or the clients that are remote from the wireless sniffer installation location.
- The location of the sniffer plays an important role in the wireless sniffing. For example, a location very close to an AP is helpful when studying the AP behaviour, but may miss some traffic sent from a distant client due to signal attenuation and on the other hand the similar effect is experienced when the sniffer is near to the client and away from the AP. This results in ‘Generic losses.

- The wireless sniffing suffers from ‘AP losses due to the firmware incompatibility between AP and monitoring device. These losses can be minimized by using redundant sniffers or sniffers with interface cards having different chipset and using antennas of different gains and positioning the sniffers at strategic places [34].

The sample of wireless sniff trace is shown in figure 5.



```
No.     Time       Source        Destination        Protocol   Info
2458 55.951347                XXX_1a:97:ab (RA)   IEEE 802.11 Clear-to-send
2459 55.951553 XXX_1a:97:ab YYY_11:30:a8          IEEE 802.11 Data
2460 55.951831                XXX_1a:97:ab (RA)   IEEE 802.11 Clear-to-send
2461 55.952174 XXX_1a:97:ab YYY_11:30:a8          IEEE 802.11 Data
2462 55.952847                XXX_1a:97:ab (RA)   IEEE 802.11 Clear-to-send
2463 55.953895 XXX_1a:97:ab YYY_11:30:a8          IEEE 802.11 Data
2464 55.954070                XXX_1a:97:ab (RA)   IEEE 802.11 Acknowledgement
```

Fig. 5. Wireless Sniffing Trace in WLAN

3 Conclusion

The wireless Measurement is an important stage of any study on wireless networks. The data collection phase acts as the building stone of the study of wireless measurements. The various wireless measurements tools used have their own strength and weaknesses. The wireless sniffing is one of the measurement techniques that could be used for effective measurement of wireless network time varying characteristics. The data collection of wireless networks can be supported by standardization of interfaces and format, information from network vendors and archival of the network data. Our future works includes the building up the effective measurement framework and step ahead for predicting the missing values in measurements by applying intelligent techniques.

References

[1] Kuran, M.S., Tugcu, T.: A Survey on Emerging Broadband Wireless Access Technologies. Computer Networks 51(11), 3013–3046 (2007)

[2] Siddiqui, F., Zeadally, S.: Mobility Management across Hybrid Wireless Networks: Trends and Challenges. Computer Communications 29(9), 1363–1385 (2006)

[3] Chen, W., Shu, Y.: Active Application Oriented Vertical Handoff in Next-generation Wireless Networks. IEEE Wireless Communication and Networking Conference 3, 1383–1388 (2005)

[4] Al-Gizawi, T., Peppas, K., Axiotis, D., et al.: Interoperability Criteria, Mechanisms and Evaluation of System Performance for Transparently Interoperating WLAN and UCLIENTS-HSDPA Networks. IEEE Networks 19(1), 66–72 (2005)

[5] Song, Q., Jamalipour, A.: Network Selection in an Integrated Wireless LAN and UCLIENTS Environment using Mathematical Modeling and Computing Techniques. IEEE Wireless Communication Magazine 12(3), 42–48 (2005)

[6] Zhu, F., McNair, J.: Optimization for Vertical Handoff Decision Algorithms. In: IEEE Wireless Communication and Networking Conference, vol. 2, pp. 867–872 (2004)

[7] Zhang, J., Cheng, L., Marsik, I.: Models for Non-intrusive Estimation of Wireless Channel Bandwidth. In: 9th IFIP International Conference on Personal Wireless Communication Conference, pp. 334–348 (2003)

[8] Papadopouli, M., Shen, H., Raftopoulos, E., et al.: Short-term Traffic Forecasting in Campus-wide Wireless Networks. In: 16th IEEE International Symposium on Personal, Indoor and Mobile Wireless Communications, pp. 1446–1452 (2005)

[9] Pahlvan, K., Krishanamurthy, P.: Principles of Wireless Networks - A Unified Approach. Prentice-Hall, Inc., Englewood Cliffs (2002)

[10] Prasad, R.: OFDM for Wireless Communication Systems. Artech House Inc., Boston (2004)

[11] Tang, D., Barker, M.: Analysis of a Metropolitan-Area Wireless Network. Wireless Networks 8, 107–120 (2002)

[12] Claypool, M., Kinicki, R., Lee, W., Li, M., Ratner, G.: Characterization by Measurement of a CDMA 1xEVDO Network. In: 2nd International Workshop on Wireless Internet, p. 2-es (2006)

[13] Chinchilla, F., Lindsey, M., Papadopouli, M.: Analysis of Wireless Information Locality and Association Patterns in a Campus. In: Proceedings of INFOCOM 2004, Hong Kong, China (March 2004)

[14] Kotz, D., Essien, K.: Analysis of a Campus-wide Wireless Network. In: Proceedings of MOBICOM 2002, Atlanta, GA (September 2002)

[15] Lonvik, C.: The BSD Syslog Protocol., IETF RFC 3164 (August 2001)

[16] Henderson, T., Kotz, D., Abyzov, I.: The Changing Usage of Mature Campus-wide Wireless Network. In: 10th ACM International Conference on Mobile Computing and Networking, pp. 187–201 (2004)

[17] Kotz, D., Essien, K.: Analysis of a Campus-wide Wireless Network. Wireless Networks 11(1-2), 115–133 (2005)

[18] Mc Cloghire, K., Perkins, D., Schoenwaelder, J.: Structure of Management Information Version 2 (SMIv2). IETF RFC 2578 (April 1999)

[19] Balachandran, G.M., Voelker, P.B., Rangan, V.: Characterizing User Behavior and Network Performance in a Public Wireless LAN. In: Proceedings of ACM SIGMETRICS 2002, Marina Del Rey, CA (June 2002)

[20] Tang, D., Baker, M.: Analysis of a Local-Area Wireless Network. In: Proceedings of MOBICOM 2000, Boston, MA (August 2000)

[21] Balazinska, M., Castro, P.: Characterizing Mobility and Network Usage in a Corporate Wireless Local-Area Network. In: Proceedings of MOBISYS 2003, San Francisco, CA (May 2003)

[22] Subramanian, M.: Network Management: Principles and Practice. Addison-Wesley, Reading (2000)

[23] Flick, J., Jhonson, J.: Definitions of Managed Objects for Ethernet-like Interface Types. IETF RFC 2665 (August. 1999)

[24] Subramanian, M.: Network management. PearsonEducation, London

[25] Ethereal Protocol Analyzer, http://www.ethrereal.com

[26] Kismet Wireless Sniffing Software, http://www.Kismetwireless.net

[27] Tcpdump packets capture software, http://www.tcpdump.org

[28] Shenoy, R., Ananda, A.L., Chan, M.C., Ooi, W.T. (eds.): Mobile, Wireless and Sensor Networks: Technology, Application and Future Directions. John Wiley & Sons, Chichester (2006)

[29] Kuang, T., Williamson, C.: RealMedia Streaming Performance on an IEEE 802.11b Wireless LAN. In: Proceedings of IASTED Wireless and Optical Communications (WOC), pp. 306–311 (July 2002)

[30] Bai, G., Williamson, C.: The Effects of Mobility on Wireless Media Streaming Performance. In: Proceedings of Wireless Networks and Emerging Technologies (WNET), pp. 596–601 (July 2004)

[31] Jardosh, A.P., Ramachandran, K.N., Almeroth, K.C., Belding-Royer, E.M.: Understanding Congestion in IEEE 802.11b Wireless Networks. In: Proceedings of the Internet Measurement Conference (IMC), Berkeley, CA, USA (October 2005)

[32] Yeo, J., Youssef, M., Agrawala, A.: A framework for wireless lan monitoring and its applications. In: ACM Workshop on Wireless Security (WiSe 2004) in conjunction with ACM MobiCom 2004, Philadelphia, PA, USA (October 2004)

[33] Claypool, M.: On the 802.11 turbulence of nintendo ds and sonypsp hand-held network games. In: Proceedings of the 4th ACM Network and System Support for Games (NetGames), Hawthorne, NY, USA (October 2005)

[34] Yeo, J., Banarjee, S., Agarwaala, A.: Measuring Traffic on the Wireless Medium: Experience and pitfalls., Technical Reports, CS-TR-4421, Department of Computer Science, University of Maryland (December 2002)