An Overview of Link-Level Measurement Techniques for Wide-Area Wireless Networks

Scott Raynel
WAND Network Research Group
Department of Computer Science
University of Waikato
smr26@cs.waikato.ac.nz

Murray Pearson
WAND Network Research Group
Department of Computer Science
University of Waikato
mpearson@cs.waikato.ac.nz

ABSTRACT

By building wireless link-level measurement tools we hope to improve the design, deployment and management of wide-area wireless community networks. This paper identifies existing link-level measurement techniques and discusses the advantages and disadvantages of each in the context of measuring and monitoring such networks. Finally, we make a case for the need for more sophisticated techniques and tools which will assist both day-to-day network operations as well as wireless network research.

Categories and Subject Descriptors

C.2.1.1 [**Computer Systems Organization**]: Network Architecture and Design—*wireless communication*

; C.2.3.b [**Computer Systems Organization**]: Network Operations—*network monitoring*

Keywords

wireless networks, link-level measurement

1. INTRODUCTION

The use of IEEE 802.11[7] in wide-area communications networks has been steadily increasing due to its low cost and low complexity. Many rural and remote community networks such as CRCnet[1] use IEEE 802.11 in a multi-hop, point-to-point fashion to provide Internet access to communities, schools and businesses.

A unique characteristic of community networks is that the end-users of the network play a significant role in the deployment and management of the network. As such, tools to manage the network must be able to identify problems with the network and present solutions that can be carried out by people with only a basic knowledge of networking.

As the popularity of community wireless networks increases the complexity increases. When wireless networks become more densely populated with nodes, interaction between logically separate links increases due to the shared nature of the wireless medium. This interference between links can lead to severe performance degradation and is a major factor in the design of any wireless network.

Presently there is no simple way for a network operator to quantify the effect of such interference from other links on the network. To make matters worse, other co-located networks operated independently may also cause interference. At the same time, wireless network researchers want to be able to ask questions about the performance of wireless link-layer protocols under these conditions.

The goal of our project is to develop a system that allows the instrumentation of an entire wide-area wireless network. This system will give detailed information about the link-level state at each node. The information can then be fed back to a central server for storage or analysis. Tools will be developed to target the end users of the network to provide high-level information about the network, identify problems and propose solutions. Additionally, wireless network researchers can use the information to investigate low-level characteristics of the wireless environment and how performance of network protocols is affected.

One of the major design considerations of such a system is to ensure that it is suitable for use on the low-power systems that are used as wireless routers. These systems generally have slow CPUs, small amounts of RAM and little or no stable storage.

The main contribution of this paper is a discussion of the advantages and disadvantages of several existing wireless link-level measurement techniques in the context of performing measurement and monitoring of an entire wide-area wireless network. We use this discussion to motivate the need for more sophisticated techniques and tools.

2. BACKGROUND

To understand wireless measurement an understanding of some fundamental principles of wireless networking is required. this section presents the background information necessary to understand the context in which the rest of the paper exists and motivate the need for wireless link-layer measurement in general.

NZCSRSC 2008, April 2008, Christchurch, New Zealand.

2.1 Wireless Networks

Wireless networks are used in many different scenarios to provide communication between endpoints where it may not be feasible to use traditional wired networks. IEEE 802.11 was originally designed for home and office networks, with a central Access Point (AP) that clients connect to. This point-to-multipoint topology is the most common implementation of IEEE 802.11, however wide-area networks such as CRCnet may use other link topologies, such as point-to-point and multipoint-to-multipoint. These topologies provide multi-hop connectivity over long distances to rural and remote schools, communities and businesses where suitable high-speed Internet connections may not have been available previously.

Each of the nodes within a wireless network acts as a router and may have several wireless network interfaces. This means that there may be several wireless links terminating at any node on the network. While these links are logically separate, they share the same physical Radio Frequency (RF) space and may interfere with each other (see Figure 1). This interference may manifest as increased ambient noise levels or if the received signal strength is high enough, fully decoded frames from other links may be observed (they may however appear with a higher bit error rate). Because the medium is a shared resource, these erroneous frames lead to performance degradation of the original link. This effect can be mitigated by employing channelisation, however IEEE 802.11b/g only supplies three completely non-overlapping channels. This approach, however, will limit the number of incoming links that a node can support.

The wireless medium presents several challenges over traditional wired networks. As noted previously, logical links share the same physical RF space. This leads to interference between links that does not occur in wired networks where the links are physically separated. As well as this interference, the wireless channel itself is both time and space varying.

The relative positions of receivers to transmitters and sources of noise or interference affect the reception of a frame. As a result of this, the wireless channel is generally described as being "space varying". Various models of path attenuation exist which describe the decrease over distance in received signal power. Noise events occur at the point of reception and do not affect the signal being received elsewhere. Obstacles such as buildings and natural formations can affect the path attenuation of a signal. All of these effects influence the receivers view of the channel and result in a unique channel state.

The wireless channel can be described as "time varying" due to the effects of multipath fading on the received RF signal power over time. Fading is caused by reflected signals taking longer to arrive at the source than the original line of sight signal. The resulting reflected signal is offset in time and is added to the original signal, which can cause destructive interference. A node may experience a "deep fade" during which RF signals are attenuated so severely that they are not detected by the receiver. The physical environment affects the amount of reflections that occur and several models exist to describe fading effects in different physical environments. The Rayleigh fading model[9] describes fading in environments with high rates of reflection, such as urban areas. Rician fading[5] models the case where the line-of-sight signal is significantly stronger than the reflected signals, such as in the case of rural networks.

All of these effects lead to the wireless medium being far more complex than the wired medium. As such, wireless Medium Access Control (MAC) protocols need to be more complex in order to try and mask these issues from the higher layer protocols. It is the interaction between the effects of the wireless medium, the wireless MAC protocols and the higher layer protocols that we are interested in investigating through measurement of the wireless link layer.

2.2 Link-Layer Measurement

Link-layer measurement of wireless networks involves the capture of traffic as it appears on the medium. While the upper network layers may appear to transmit a single frame, this may involve several frames on the wireless medium due to acknowledgements, retransmits, or fragmentation performed by the link-layer. Performing link-layer measurement also allows capture of information specific to the wireless medium, such as RF signal strength, noise levels, frequency and channel modulation.

This is different to traditional end-to-end measurement techniques such as "ping" or "traceroute" which provide a single measurement of an entire path without any knowledge of the underlying network medium. By collecting data at the link-level, we can start to understand how properties of the wireless medium affect higher layer protocols such as TCP.

Link-layer measurement can be useful in different ways. During the day to day operation of a network, link-layer measurement can give feedback about the state of the network. It can highlight links which are performing poorly and closer analysis can determine the cause. For example, link-layer measurement may identify that a particular configuration is causing hidden terminal problems[10]. This may result in physical changes being made to the network topology to overcome interference.

Of more interest is the use of link-layer measurement as a tool for wireless network researchers. In designing new wireless MAC protocols, tools for the measurement of existing network protocols are needed to identify situations where the protocols may be improved. Link-layer measurement can also be used to investigate the MAC protocol's responses to changes in the wireless environment and how this affects the performance of higher layer protocols. This information can aid the design of new protocols and the cycle can begin again.

Link-layer measurement also provides a way to investigate phenomena specific to the wireless medium. For example, researchers may be interested in studying the effect of the wireless error environment. They may want to study how noise, interference, etc, affect the reception of frames or how symbols within frames are affected. This information could be used in the design of new MAC protocols that can adapt to changes in the wireless environement.

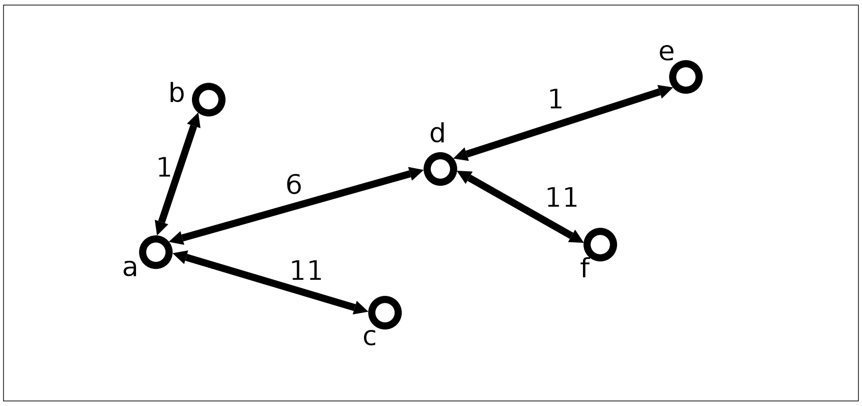

Figure 1: An example multi-hop point-to-point wireless network. Each node (circles) communicates with other nodes via wireless links (arrowed lines). Each link is numbered with its channel in such a way that all incoming links at each node are non-overlapping. However, frames from *a* to *c* may be detected at *f*. This simple example illustrates that even though links are logically separate, the nature of the shared wireless medium allows links to interfere with one another.

2.3 Common Constraints

Community wireless networks involve the community in the design, construction and eventual maintenance of the network. As such, the network must be cheap and easy to deploy and run. Additionally, network management tools must be able to diagnose network problems and present solutions that can be actioned by people without a significant networking knowledge.

Community networks are typically based on low power devices such as the Soekris range of microcomputers[3]. These computers have limited processing power available to them as they are designed to be used solely as wireless routers. They generally have 486-class processors, limited amounts of RAM and little or no usable stable storage. These limitations present constraints on what types of measurement can be performed.

Low-power devices are not fast enough to keep up with full packet capture at line rates. The overhead of copying each frame from kernel to user space is too high for the devices to handle. When measuring wired networks, each frame is captured as it passes a switch or router. Attempting to do this on a wireless node usually brings the device to a standstill, preventing the main task of routing packets from occurring. It is important that measurement tasks do not affect the performance of the network being measured.

The nodes themselves have no stable storage, so collected packets cannot be stored for long periods of time. Data must be transported back to a central server for later processing. However, this introduces network overhead and again it is important that the overhead does not affect the network being measured. It should also be noted that as more network overhead is introduced the probability of measuring measurement traffic increases and this should be kept to a minimum.

In conclusion, the nodes that make up wide-area wireless community networks are not suitable for the same type of data collection performed on wired networks. Full packet capture at line rates is difficult due to the processing overhead involved and large amounts of data is not able to be stored on the nodes. This requires wireless measurement to be performed differently than wired networks.

3. CURRENT TECHNIQUES

In this section we will discuss two types of passive link-layer measurement: indirect and direct capture. A third non-passive technique, active measurement, will also be introduced. Each technique will be described in general and then discussed in the context of their usefulness in link-level measurement and monitoring of a wide-area wireless network.

Much of the early literature surrounding wireless measurement was based on the wired side of the network. For example, Balachandrani, *et al*[4] took packet traces from the wired distribution system and SNMP traces from the wireless APs. By combining this data the authors were able to infer high-level information about the wireless channel. The main disadvantage of this technique was that the SNMP traces contained aggregated information about the wireless medium, so the effect of the wireless medium on the performance of higher layer protocols was not able to be studied in any detail. Frameworks for the monitoring of large heterogeneous wireless networks such as that proposed by Ho, *et al*[6] are also based on polling SNMP information from wireless devices. Such techniques only give insight to the fact that links are performing poorly; little information is gained as to why. Techniques which give link-level information for each frame on the wireless medium are far more powerful.

3.1 Passive Indirect Capture

Passive indirect capture is one of the most common forms of wireless link-layer measurement due to its simplicity. It is sometimes referred to as “vicinity sniffing” as it involves sniffing frames using a passive monitor which is not part of the network being measured. For example, a laptop computer could be used to passively sniff frames from a network operating in the same area. This technique is used extensively by wireless monitoring software systems such as

Kismet[2]. Much of the current literature on wireless network monitoring uses this technique. For example, Yeo[11] and Jardosh[8] use passive indirect capture when characterising indoor WLAN environments.

Using this monitoring technique introduces no overhead to the network that is being monitored. That is, the nodes that are part of the network are doing no extra work to facilitate the measurement. Also, because this is a passive technique, no frames are being injected into the network, so no bandwidth is being used for the measurement.

One of the main advantages of passive indirect capture is that a more powerful machine can be used to perform the capture. Modifications to the existing network infrastructure are not necessary. The constraints of the individual routers are not a factor because the capture node is completely separate from the network. This allows full packet capture to be performed easily. In the case of monitoring a wide-area network, providing a second more powerful machine at each node to perform measurement is seldom a feasible solution given both the cost and power constraints of wireless sites.

Indirect capture provides a view of the channel state from the position of the monitoring node. This could be significantly different from the channel state at the intended receiver. Due to the varying nature of the wireless channel as well as differences in the RF front-end, the monitoring node will receive frames at a different signal power and in a different noise environment than that of the intended receiver. This is significant because the monitoring node may receive frames in error when they were received by the intended receiver without error, or vice versa.

Even with these caveats, passive indirect capture can give a good overview of what is going on at the link-layer. It can be a useful tool for site-surveying to determine which other network nodes can be heard. However, it is not an appropriate technique for use in large scale monitoring of wide-area wireless networks. It is impossible to tell which nodes "heard" a particular frame or which nodes received a frame in error, at what signal strength, etc. The view of the channel state is restricted to that of the monitoring node which may not accurately reflect the channel state of the intended receiver. Additionally, there is no feedback on transmission of a frame. For example, it is difficult to reliably tell how many times a frame was transmitted.

3.2 Passive Direct Capture

Passive direct capture involves instrumenting each wireless node to be measured with a "tap" that provides a copy of each frame as it is seen on the medium. This direct capture at the receiver (rather than indirect capture at a third-party node) provides a much more accurate view of the channel state at the intended receiver.

This method requires extra software on each node however it provides many benefits. It is now possible to see at each node how and when frames are received with an accurate view of the channel state. With this information it is possible to see how each node in range of a transmitter heard a particular frame. With each node instrumented with a direct tap, a picture can be built of the network as a whole, rather than the snapshot of a particular node provided by indirect capture.

Direct capture involves the use of "promiscuous" mode which turns off any hardware address filtering. Usually the Network Interface Card (NIC) will filter frames that are not intended to be processed by the host however in a measurement scenario is is desirable to see all frames on the medium. Disabling receive filtering increases the interrupt load on the system however we have found that this does not adversely affect the systems under normal use and there are other factors that affect performance of the system much more significantly.

Direct capture is much closer to how one would measure a wired network. It provides much more accurate information but it comes at a cost. As well as incurring the cost of an increased interrupt load, the cost of copying each frame from kernel to user space is significant. During testing we found that performing full packet capture overloads the nodes due to the significant cost of copying each frame from kernel to user space. This resulted in a drop in performance of the node as well as an unreliable capture. Only capturing packet headers reduced the load somewhat but the capture process still dropped packets.

Even if a node is capable of capturing each frame without degrading the performance of the system, promiscuous capture generates large amounts of data. Capturing the content of every frame detected on the medium can generate megabytes of data per second. Given that each node has very little stable storage for recording packet traces it is not possible to capture and store each frame for any extended period of time. Transporting full packet traces to a central server in real-time will result in writing each packet back onto the network after it has been captured. Other nodes will repeat this process as they hear packets resulting in saturation of the network with measurement traffic, creating a positive feedback loop.

In the context of monitoring a wide-area network which is constrained by the capabilities of the individual routers, limiting the measurement to capture of meta-data describing each frame rather than capturing the entire frame contents can help. This can be achieved by either capturing only the MAC layer packet headers, or by generating records which describe the frame and include link-level information such as received signal strength, etc. This enables collection of information about a large number of frames without requiring large amounts of storage. Transporting such data to a central server becomes much easier.

This method provides much more detailed and accurate information about the channel state as seen at the intended receiver. If all nodes on the network are instrumented in such a way then a picture can be built describing how each node in the network sees the channel and how changes in the channel state affect reception of packets.

This makes direct capture extremely useful in the context of measurement of wide-area wireless networks, however it is important that measurement tasks do not overwhelm the individual nodes or the network resource itself with measurement traffic. Other techniques for reducing the amount of work done by each node when performing passive direct capture are the subject of continued research. For example, kernel-level packet filtering techniques may be employed such that the measurement software sees a sampling of the packets on the channel, rather than every packet. Moving parts of the measurement software into the kernel itself may also help to reduce the amount of kernel to user transitions.

3.3 Active Measurement

A third technique called active measurement exists whereby known frames are actively injected into the network being measured. The main disadvantage of actively injecting frames is that it consumes network resource. However, it can provide interesting information that is unable to be captured easily using passive techniques.

Active techniques are already widely used in network measurement. Most tools for measurement of end-to-end networks rely on actively probing the network. Tools such as "ping" or "traceroute" are common examples. These tools actively probe the network at the IP layer and analyse the responses generated by hosts. This is slightly different from the way active measurement at the link-layer works. Active measurement at the link-layer involves transmission of a frame from one node and analysis of how that frame is received by each other node.

Injection of frames into the network with known payloads allows for analysis of how those frames were received by each receiver in range. For example, it may reveal that some receivers are receiving a large proportion of frames with a particular set of bits corrupted. Such information is difficult to extract using purely passive techniques. Passive techniques can only provide information about packet error rates. Active techniques, however, allow the study of symbol errors within packets.

The level of control provided by active measurement makes several measurement tasks easier. For example, if each frame is numbered uniquely then receivers can determine statistics about the proportion of packets that they are not receiving at all, possibly due to collisions, deep-fades or other wireless effects.

By marking each frame with the channel or frequency that it was transmitted on, receivers can determine the amount of cross-channel interference that is occurring. That is, the extent to which links that have been placed on separate channels are interfering with one another can be measured.

Using active techniques lends itself nicely to measurement of a wide-area wireless network as it allows injection of known frames and measurement of how those frames are being received at each node. Non injected frames can easily be rejected using kernel-based packet filters so the overhead of receiving such frames is minimal compared to full passive promiscuous capture.

While active measurement provides many benefits, restricting measurement to purely active techniques means that the ability to detect nodes which are not part of the measurement system is lost. For example, the measurement system should be able to detect the presence of other networks in the area and determine how they affect the performance of the network being measured. To do so requires the use of passive techniques due to the fact that the other networks in the area will not be part of the measurement system.

Active techniques require careful consideration of the scalability of the system. Ideally, the system should dynamically scale back the amount of traffic being injected by each node based on the number of nodes within range. As with passive measurement, the system should minimise the amount of network overhead so that the network does not become overwhelmed when the number of nodes increases.

4. SUMMARY

The need for a system to measure and monitor wide-area wireless networks is clear. Such a system would clearly benefit both the day to day operations of such a network and assist wireless researchers in developing new wireless MAC protocols.

Several link-level measurement techniques exist, however alone none are suitable for long term measurement of wide-area wireless networks. Passive indirect capture does not provide an accurate view of the channel state at the intended receiver. Passive direct capture provides an accurate view of the channel state but generates too much data for the low-power nodes to process. Active measurement allows control of what is being measured and hence allows measurement of effects that are difficult to measure using passive techniques. Purely active measurement however lacks the ability to measure the effect of other networks that are not part of the measurement system.

This paper has discussed existing techniques for the measurement and monitoring of wide-area wireless networks. It has shown that each of the existing techniques is not suitable for the required task. It is clear then that further research is needed in the area of measurement and monitoring of wide-area wireless networks.

5. FURTHER WORK

Work on improving the state of wireless link-layer measurement is an on-going project.

By combining passive and active measurement and applying novel techniques to reduce both the processing and network overhead of the measurement system we believe that an acceptable level of measurement precision can be achieved while operating under the constraints of the wireless nodes.

A system is currently under development which uses both passive direct capture and active measurement techniques to provide information about link-layer activity from each node in the network. By combining this information at a central point, we can generate a view of the entire network and how links are affecting other links and start to answer questions about how links are performing or how the wireless protocols react to environmental change.

6. REFERENCES

[1] Connecting Remote Communities (CRCnet) Project. http://www.crc.net.nz, February 2007.

[2] Kismet. http://www.kismetwireless.net, December 2007.

[3] Soekris Engineering. http://www.soekris.com, December 2007.

[4] A. Balachandran, G. M. Voelker, P. Bahl, and P. V. Rangan. Characterizing user behavior and network performance in a public wireless lan. In *SIGMETRICS '02: Proceedings of the 2002 ACM SIGMETRICS international conference on Measurement and modeling of computer systems*, pages 195–205, New York, NY, USA, 2002. ACM.

[5] L. W. Barclay. *Propagation of Radio Waves*, chapter 2, pages 16–24. The Institution of Electrical Engineers, 2nd edition, 2003.

[6] C. C. Ho, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer. A scalable framework for wireless network monitoring. In *WMASH '04: Proceedings of the 2nd ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, pages 93–101, New York, NY, USA, 2004. ACM.

[7] IEEE. *ANSI/IEEE Std 802.11*. Insitute of Electrical and Electronics Engineers, 1999.

[8] A. P. Jardosh, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer. Understanding link-layer behavior in highly congested ieee 802.11b wireless networks. In *E-WIND '05: Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*, pages 11–16, New York, NY, USA, 2005. ACM Press.

[9] B. Sklar. Rayleigh fading channels in mobile digital communication systems .I. Characterization. *Communications Magazine, IEEE*, 35(7):90–100, 1997.

[10] F. Tobagi and L. Kleinrock. Packet Switching in Radio Channels: Part II–The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution. *Communications, IEEE Transactions on*, 23(12):1417–1433, 1975.

[11] J. Yeo, M. Youssef, and A. Agrawala. A framework for wireless lan monitoring and its applications. In *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*, pages 70–79, New York, NY, USA, 2004. ACM.