SWAT: Fingerprinting Your Wireless Network

Kannan Srinivasan, Maria Kazandjieva, Jung Il Choi, Mayank Jain, Edward Kim, and Philip Levis
Computer Science Lab,
Stanford University,
Stanford, California, CA - 94305.
{srikank,mariakaz,punch98,mayjain,edskim}@stanford.edu, pal@cs.stanford.edu

Abstract

The Stanford Wireless Analysis Tool (SWAT) is a software tool for characterizing wireless networks. It runs automated, user-configurable measurement experiments on any given mesh network and collects per-packet and per-node statistics. SWAT distills these statistics into a handful of metrics such as temporal and spatial correlation of packet receptions. These metrics help users understand how different protocols, such as opportunistic routing and network coding, behave in a given network. Understanding why a protocol behaves the way it does will improve future protocol design as well as allow existing protocols to be fine-tuned to a specific environment.

Categories and Subject Descriptors: C.2 [Computer Systems Organization]: Computer-Communication Networks.
General Terms: Measurement, Performance, Design.

1. INTRODUCTION

Wireless protocol design is notoriously difficult. This is especially true with open-spectrum technologies such as 802.11b/g/n, Bluetooth, and 802.15.4, all of which share the 2.4GHz band with cordless phones, microwaves, and other consumer devices. While these technologies are inexpensive and therefore ubiquitous, their RF environments tend to be complex, interference-heavy, and hard to tackle with clean analytical approaches or simulations.

Researchers have addressed this challenge by deploying, testing, and evaluating protocols on indoor and outdoor testbeds [1, 2, 6]. Deployments demonstrate that a protocol can work in practice, but results are difficult to generalize. Protocol comparison is especially subjective to the testbed environment and results are not consistent.

To explain variations, deployment studies typically report high-level network properties such as a connectivity graph, reception ratios, average hop count, and average node degree. This information is valuable but it does not capture many of the changes a network experiences. We believe that measuring and reporting low-level link dynamics along with the high-level properties can help us understand these vagaries in protocol performance.

For example, immediate retransmissions will have different performance on two links that have the same packet reception ratio (PRR) but have different durations of correlated reception. If a link has uncorrelated reception over time, i.e a packet's fate is independent of all other packets' fates, then retransmitting immediately after a failure is fine. However, if another link has the same PRR but highly correlated reception, the immediate retransmission after a failure is also likely to fail. The Stanford Wireless Analysis Tool (SWAT) can measure the high-level PRR metric as well as low-level properties such as reception correlation.

System malfunctions and software misbehaviors do lead to inconsistent protocol performance. The goal of SWAT is not to help identify such bugs. Jigsaw [3] is a network monitoring tool that uses passive radio monitors in a network to provide a global viewpoint to understand network performance inefficiencies. SWAT's purpose is rather to measure environment-specific properties of links and nodes in a network. SWAT uses active experiments on the network to do the measurements and requires no extra equipment. The goals of SWAT and Jigsaw are complementary and can coexist in the same network.

2. SWAT

The Stanford Wireless Analysis Tool (SWAT) allows network researchers to measure and analyze various network characteristics. SWAT works by running packet transactions between all transmit-receive pairs in a network and measuring various link level metrics. Those include packet reception ratio (PRR) distribution, link asymmetry, signal-to-noise-ratio (SNR), node degree, network diameter, and temporal and spatial correlations in packet reception.

SWAT provides a user interface for configuring and running measurements and for visualizing the collected data. SWAT uses a serial or Ethernet back-channel to gather data. Users specify the IP addresses or machine names along with the other experiment configuration parameters such as the number of packets, inter-packet interval, data rate, and transmission power level. The demo release of SWAT will support both 802.11b and 802.15.4.

SWAT for 802.11b is implemented as part of Click [4]. Every node sends broadcast packets and every receiver logs packet statistics locally. As the experiment progresses, SWAT displays, in real-time, which node is transmitting and which nodes are receiving packets. At the end of every node's transmissions, SWAT retrieves these logs from all the receivers and stores them in a database. Upon completion of an experiment, SWAT computes all the metrics from the collected data and generates a report. The report includes a summary of the metrics along with the detailed plots showing the relationship between metrics.

SWAT's experiment and metric calculation modules are open and available for the users to modify and extend. The experimental database can be retrieved for a later study and can be shared with other users.

3. SWAT IMPACT

The metrics that SWAT computes give insights into how protocols perform in a network. In this section, we briefly show how β, reception's temporal correlation metric and ρ, reception's inter-receiver correlation metric tell us how MAC and opportunistic routing protocols perform. Table 1 shows β and ρ values and their meanings.

Figures 1(a) and 1(b) show the complementary cumulative distribution functions (CCDFs) of β for Roofnet, an outdoor 802.11

Metric	Description
β=0	independent reception over time
β >0	positive reception correlation [success (failure) follows success (failure)]
β <0	negative reception correlation [failures follow successes and vice versa]
ρ=0	reception at receivers are independent
ρ >0	positive inter-receiver correlation [success (failure) at one receiver implies likely success (failure) at the other]
ρ <0	negative inter-receiver correlation [success (failure) at one receiver implies likely failure (success) at the other]

Table 1: Understanding β and ρ.

testbed. While about 70% of the 11Mbps roofnet links are highly temporally correlated with a $\beta > 0.8$, less than 10% of the 1Mbps roofnet links are equally correlated. The plot also shows that as the inter-packet interval (IPI) increases, a link's β decreases; packets seperated farther in time are more independent. These plots are representative of other 802.11b data rates and transmission power levels, that are not shown here for brevity.

β has implications to MAC protocols and retransmission policies. On links with highly temporally correlated reception, upon a success, sending more packets back-to-back is more beneficial than sending packets as they arrive. Likewise, immediately retransmitting after a failure is wasteful on highly correlated links. Setting the backoff interval based on β can reduce the average number of transmissions per node by about 15% [7].

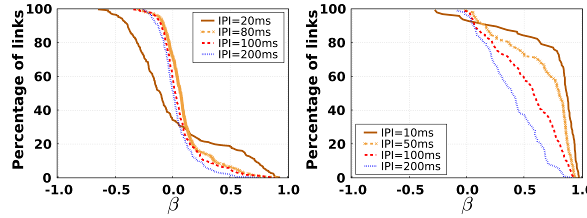
Figures 2(a) and 2(b) show the CCDFs of ρ for the roofnet and SWAN testbeds. The SWAN testbed is an indoor testbed in the Computer Science building of Stanford Univeristy. While 90% of all the roofnet receiver pairs are independent (with $\rho = 0$), only 40% of SWAN receiver pairs are independent.

ρ has implications to opportunistic routing protocols. Opportunistic routing protocols assume inter-receiver reception independence [2, 5]. We use the anypath ETX ratio as a measure of how bad the ETX estimate is when assuming reception independence; an ETX ratio of 0 means that the estimate is same as the actual ETX, > 0 means that the estimate is an under-estimate and < 0 is an over-estimate.

Figures 2(c) and 2(d) plot the anypath ETX ratio against the average of ρ's of all the receiver pairs in the anypath. As the average ρ increases the anypath ETX ratio also increases; when many receivers have correlated reception, path diversity decreases and so opportunistic routing does not benefit from such receivers.

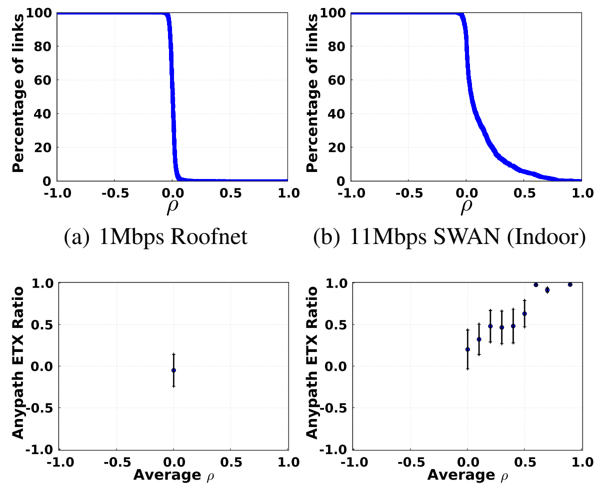
4. DISCUSSION

As shown in Section 3, SWAT metrics give us insight into protocol performance. These metrics also give insights into tuning existing protocols according to the environment to improve protocol efficiency. In addition, SWAT measurements will ensure a common basis for comparing protocols. In the future, we hope that researchers will include SWAT metrics in their protocol evaluations to clearly describe testbed characteristics.



(a) 1Mbps Roofnet (b) 11Mbps Roofnet

Figure 1: β for Roofnet. 1Mbps links have mostly low β's while 11Mbps links have high β's.



(a) 1Mbps Roofnet (b) 11Mbps SWAN (Indoor)

(c) 1Mbps Roofnet (d) 11Mbps SWAN (Indoor)

Figure 2: ρ and opportunistic routing. @1Mbps, none of the Roofnet receivers have reception dependent on reception at other receivers. @11Mbps, about 5% of the SWAN receivers have dependent reception. As the average ρ of all receiver pairs in an anypath increases, the anypath ETX ratio also increases; if many receiver pairs have correlated reception, the anypath ETX estimate (assuming independent receivers) and the actual anypath ETX are very different.

5. REFERENCES

[1] D. Aguayo, J. Bicket, S. Biswas, G. Judd, and R. Morris. Link-level measurements from an 802.11b mesh network. In *SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications*, 2004.

[2] S. Biswas and R. Morris. ExOR: opportunistic multi-hop routing for wireless networks. In *SIGCOMM '05: Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications*, 2005.

[3] Y.-C. Cheng, J. Bellardo, P. Benkö, A. C. Snoeren, G. M. Voelker, and S. Savage. Jigsaw: solving the puzzle of enterprise 802.11 analysis. *SIGCOMM Comput. Commun. Rev.*, 36(4):39–50, 2006.

[4] E. Kohler, R. Morris, B. Chen, J. Jannotti, and M. F. Kaashoek. The Click modular router. *ACM Transactions on Computer Systems*, 18(3):263–297, August 2000.

[5] R. Laufer, H. Dubois-Ferrire, and L. Kleinrock. Multirate anypath routing in wireless mesh networks. In *Proceedings of IEEE Infocom 2009*, Rio de Janeiro, Brazil, April 2009.

[6] K. Srinivasan, P. Dutta, A. Tavakoli, and P. Levis. Some implications of low-power wireless to IP routing. In *Hotnets-V*, Irvine, CA, Nov. 2006.

[7] K. Srinivasan, M. Kazandijieva, S. Agarwal, and P. Levis. The β-factor: Measuring wireless link burstiness. In *Proceedings of the Sixth ACM Conference on Embedded Networked Sensor Systems*, Raleigh, NC, Nov. 2008. To appear.