Is there an optimum in ad-hoc networks?

D Y Polukarov[1] **and P O Chursin**[1]

[1]Samara National Research University, Moskovskoe Shosse 34A, Samara, Russia, 443086

Abstract. One of the most promising modern data transmission technologies is ad-hoc wireless peer-to-peer networks. A distinctive feature of such networks is the absence of a central node, which allows you to create connections "on the fly" with arbitrary connections between nodes. Ad-hoc networks are designed to create mobile computer networks and can be used, for example, to coordinate transport, in search and rescue operations and similar situations in which the use of infrastructure nodes is ineffective. When using Wi-Fi as a transport for self-organising sensor networks, attention should be paid to details. Wi-Fi technology is used in ad-hoc mode in self-organising sensor networks with non-hierarchical nodes. An experiment was conducted to measure the available bandwidth of a segment of the Wi-Fi network. This parameter was measured, and the dependence of the available bandwidth on the segment load was determined. We tried to create a tool for testing the Wi-Fi segment while also testing the tool's own performance in various configurations of the Wi-Fi segment.

1. Introduction

There is a large number of studies devoted to measurements in the Ethernet segment [1]. Also, a lot of work was done on the topic of measuring the parameters of the infrastructural mode of the Wi-Fi segment.

However, there is not enough attention paid to measuring the parameters of the Wi-Fi segment in the ad-hoc mode, yet this mode is important for organising mesh networks and other self-organising networks. Therefore, it makes sense to pay more attention to measuring the ad-hoc parameters of the Wi-Fi segment.

Ad-hoc mode allows network nodes to establish connections directly between devices without using a base station. Such networks are decentralised, and the definition of the node to which you want to send data is dynamic based on the connectivity of the network.

On the other hand, a network in infrastructure mode always consists of at least one access point and several wireless client stations connected to it. At the same time, data exchange between the client stations takes place through their forwarding through the access point.

When testing a network, you can't do without special software tools. There are many free and commercial products that solve this problem [2,3]. The comparative analysis of common tools for testing networks showed that, for all their advantages, the proposed programs have shortcomings that do not allow for fully performed functional testing of computer networks.

2. Related works

Nping [4] is an open source tool for generating network packets, analysing responses and measuring response times. Nping allows users to generate network packets from a wide range of protocols such as TCP, UDP, ICMP, and ARP, allowing them to configure virtually any area of protocol headers. While Nping can be used as a simple ping utility to detect active nodes in the network, it can also be used as generator packages for stress tests of the network stack, sending ARP requests, attacks such as "denial of service", route tracking and other purposes. The program has a command-line interface.

Iperf3 [5] - cross-platform console client-server program-generator of TCP, UDP and SCTP traffic to test network bandwidth. The program allows you to perform load testing of a network segment, has a convenient command line interface, but does not have the ability to configure the package headers. The "iperf3-s"command is used to start the server. There is also a graphical shell called jperf [6].

Ostinato [7] is a multithreaded traffic generator designed to test services that enable the network to run at different levels of the network protocol stack. The user is given the opportunity to create data packages of arbitrary content, defining both the package title and the content of all its fields. In addition to the content of the packages, you can choose the interface and the frequency of traffic generation. Ostinato is a commercial product, though the cost of a single-user license is, however, relatively low. The disadvantage of the product is the heavy weight and lack of command line interface, which prevents it from installing on embedded systems.

Table 1. Comparative analysis of software products.

Feature	Nping	Iperf3	Ostinato	Our software
Protocols	TCP, UDP, ICMP, ARP	TCP, UDP, SCTP	TCP, UDP, ICMP, ARP	UDP
Configure packet headers	partially	no	yes	yes
Setting the packet size	yes	yes	yes	yes
Custom send interval (between packets)	yes	no	yes	yes
Select target speed	no	yes	yes	no
Changing traffic profiles “on the fly”	no	no	yes	yes

3. Features of ad-hoc networks

Wi-Fi segments commonly use CSMA/CA [8] for media access control — modification of pure Carrier Sense Multiple Access (CSMA). CSMA/CA differs from CSMA/CD [9] in that only jam-signals are vulnerable to collisions, but not the data packets. That is what “collision avoidance” stands for.

Collision avoidance is used to improve the performance of the CSMA method by attempting to divide the channel somewhat equally among all transmitting nodes within the collision domain. This functionality is assigned to the «jamming signal». Decrease in collision probability and the number of retransmissions leads to performance improvement, but waiting for the jam signal creates additional delays, thus making other methods able to achieve better results. Collision avoidance is quite useful in situations, when it is impossible to detect collisions in real-time – for example, when using radio transmitters [8].

The hidden node problem occurs when several nodes are visible to an access point (AP), but not to other nodes, communicating with this AP, thus making them unable to physically receive signals from each other (e.g. because of distance, signal spreading conditions, etc.). This leads to difficulties in the media access control sublayer, as the majority of existing client-side methods for accessing digital networks use carrier sensing to detect channel utilisation (CSMA/CD, CSMA/CA, etc.) [10].

4. Measurement of parameters

4.1. Fully connected ad-hoc Wi-Fi segment

The scheme of the experiment is shown in figure 1. The segment of the wireless ad-hoc network consisted of four nodes: two wireless Wi-Fi routers with special software installed and two computers used to measure the available bandwidth.

Wireless routers were used as sources of spurious traffic. Devices ran operating system OpenWRT [11], as well as specially developed software to generate spurious traffic. This software has the ability to change the intensity of generated traffic. Changing the intensity of spurious traffic is achieved by adjusting the time interval between the packets being sent.

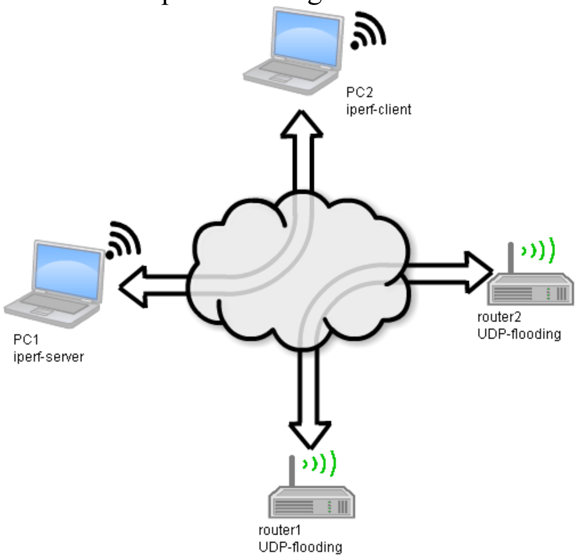

Figure 1. Scheme of the experiment.

Nodes PC1 and PC2 are set up for connection in ad-hoc mode and utilise iperf3 [5] to measure available bandwidth.

The obtained measurement results are presented in Table 2.

Table 2. Results of the experiment.

Delay, µs	Available bandwidth Bav, Mbit/s		
	Packet size V=500 bytes	Packet size V=1000 bytes	Packet size V=1500 bytes
10	2.97	2.35	1.36
500	7.30	6.48	6.30
2000	10.72	9.74	9.94
5000	11.85	11.00	11.34

The results of the measurements are also presented on the graphs shown in Figure 2.

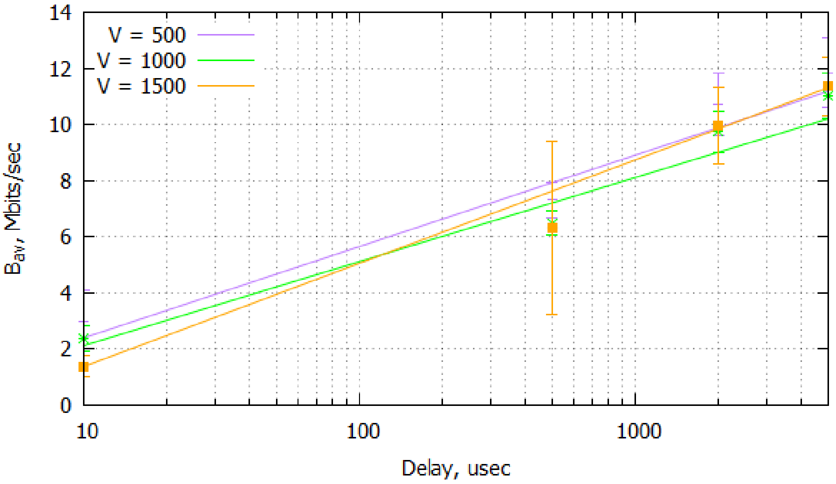

Figure 2. Dependence of bandwidth on segment load.

4.2. Ad-hoc Wi-Fi segment with hidden node problem

Figure 3 shows a diagram of an experiment that implements the hidden node problem. Special waveguides were used to limit the spread of the Wi-Fi signal.

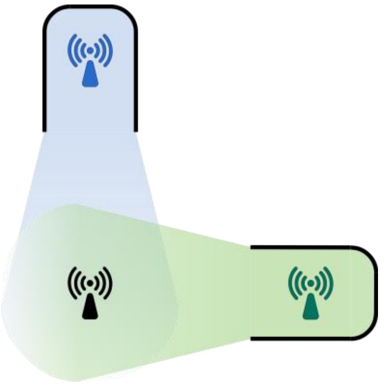

Figure 3. Scheme of the experiment with hidden node problem.

Portable Wi-Fi routers of type TL-MR3020 with an OpenWRT operating system installed on them were used as ad-hoc segment nodes. To prevent spurious signal leakage, the nodes were powered from autonomous power sources.

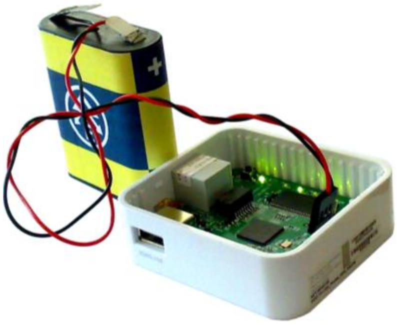

Figure 4. Portable Wi-Fi router TL-MR3020 as ad-hoc segment node.

Special waveguides are cardboard boxes covered with aluminum foil. This allowed for limiting the area of the Wi-Fi signal and significantly reducing the size of the experimental setup.

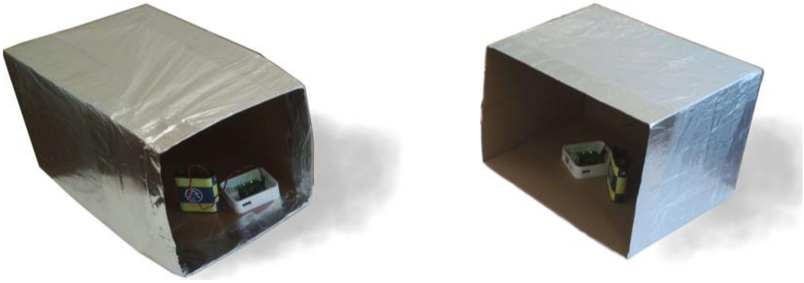

Figure 5. Photo of the experiment with hidden node problem.

Unfortunately, we were unable to capture the noticeable effect of the hidden node. However, this experiment allowed us to test the performance of our software in this mode.

5. Conclusion

In this paper, the bandwidth of the ad-hoc Wi-Fi network segment was measured under various load conditions. The measurements did not reveal a significant qualitative difference in the throughput of the Wi-Fi network segment in the ad-hoc mode from the infrastructure mode. The use of the developed tools allows us to determine the rational mode of operation of the Wi-Fi segment. Also, these results can be used to solve the optimal path problem [12] and other related works [13].

6. References

[1] Boggs D R, Mogul J C and Kent C A 1988 *Measured capacity of an ethernet: Myths and reality* **18(4)** 222-234

[2] Chursin P O and Polukarov D Yu 2017 Some features of the implementation of the source of test traffic *Perspective information technologies* 1033-1035

[3] Chursin P O and Polukarov D Yu 2018 Designing an automated information system for testing the functionality of network interaction *Perspective information technologies* 1154-1155

[4] *Nping - Network packet generation tool* (Access mode: https://nmap.org/nping/) (21.11.2017)

[5] *iPerf - Download iPerf3 and original iPerf pre-compiled binaries* (Access mode: https://iperf.fr/iperf-download.php/) (21.11.2017)

[6] *JPerf – graphical interface wrapper for Iperf* (Access mode: https://www.rarst.net/software/jperf/) (21.11.2017)

[7] *Ostinato Network Traffic Generator* (Access mode: https://ostinato.org/) (21.11.2017)

[8] *Carrier-sense multiple access with collision avoidance* (Access mode: https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_avoidance/) (21.11.2017)

[9] *Carrier-sense multiple access with collision detection* (Access mode: https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_detection/) (21.11.2017)

[10] *Hidden node problem* (Access mode: https://en.wikipedia.org/wiki/Hidden_node_problem/) (21.11.2017)

[11] *OpenWrt Project: Welcome to the OpenWrt Project* (Access mode: https://openwrt.org/) (21.11.2017)

[12] Agafonov A A and Myasnikov V V 2016 Method for the reliable shortest path search in time-dependent stochastic networks and its application to GIS-based traffic control *Computer Optics* **40(2)** 275-283 DOI: 10.18287/2412-6179-2016-40-2-275-283

[13] Nikitin V S, Semenov E I, Solostin A V, Sharov V G and Chayka S V 2016 Modeling the"smartlink connection" performance *Computer Optics* **40(1)** 64-73 DOI: 10.18287/2412-6179-2016-40-1-64-73

Acknowledgements

This work falls within the public tasks allotted to the Ministry of Education and Science of the Russian Federation (2.974.2017/4.6) and was carried out with the support of grant RFBR 16-07-00218a.