# AN INVESTIGATION ON TCP SACK CONGESTION CONTROL ON UNIVERSITY OF NIGERIA LIONET HOTSPOT

<sup>1</sup>Okafor K.C, <sup>2</sup>Udeze C.C, <sup>3</sup>Ugwoke F.N, <sup>4</sup>Ochi Josiah .C, <sup>5</sup>Okwuelu Nnaemeka

<sup>1,2,5</sup>Electronics Development Institute, Awka, Nigeria,

<sup>3</sup>Computer Science, Michael Okpara University Umuahia, Nigeria,

<sup>4</sup>Electronic and Computer Engineering, Nnamdi Azikiwe University Awka,

<sup>1</sup>udezechidiebele@yahoo.com, <sup>2</sup>arissyncline@yahoo.com, <sup>3</sup>azubuikec@yahoo.com, <sup>4</sup>edujosh09@yahoo.com. <sup>5</sup>god4meks@gmail.com

**Abstract**—With the increasing awareness of mobility cloud computing via-a-vis wireless networks, there is an indication that Flow-Aware Wireless LAN (FA-WLAN) will play an important role in future internetworks supporting clouding, virtualization, Smart grids, and 4G LTEs. Congestion management in FA-WLAN considering existing network transport protocols such as TCP and UDP have limitations when fitting into these new technologies as increased heterogeneity and mobility will generate issues and concerns in managing congestion issues. With respect to realistic loads, TCP-SACK cannot handle traffic congestion in a Flow Aware-WLAN for scalable Internet traffic. This work conducted a pilot study in University of Nigeria Nsukka using three sets of APs to carry out measurements and analysed the behaviour of data frame size in traditional TCP- SACK. We used ethereal wireshack in a real time scenario for the data collection. Also, we considered IEEE 802.11 based wireless LAN where the access points is used to connect a fixed number of users to the Web or to a shared file system. The results of our investigation showed that in FA-WLANs, TCP-SACK will scale poorly in this new era of high performance computing (HPC), hence a novel congestion control scheme which will harvest packet size distributions is proposed, layer4 DMF.

Keywords: FA-WLAN, Wireless, Congestion, TCP, SACK, Ethereal, HPC.

### 1. INTRODUCTION

Mobility computing in the context of hotspot networks goes with its associated transport layer challenges. The 802.11a/b/g is the de facto standard for wireless local area networks (WLANs). Which aim at providing wireless connectivity to the Internet, representing a valid alternative to classical Ethernet LANs. Communication in wireless network is quite susceptible to mobility, nodes capacity and power consumption level [1]. These might contributes to the major problem of TCP performance degradation where there are highly potential of packet loss and packet reordering [1].

In particular, it turns out that, due to the extremely high overhead encompassed by the 802.11 TCP protocol which lacks robust explicit duplexing mechanism, this will have an extremely negative effect on packet size distribution metrics. Also, we analyze the impact of the TCP congestion mechanism on frame size window distribution. However, evidence is provided that, under a careful tuning of design of an efficient algorithm as well as setting of some AP parameters, TCP delayed ACK technique scan help in reducing the mean session delay which could affect packet size distribution, thereby enhancing effective throughput.

The paper is organized as follows. Section 2 reports on related works as well as a broad description of a contextual network scenario of the 802.11 MAC protocol. The methodology involving the UNN measurement testbed for TCP SACK frame size distribution analysis for persistent TCP connections is presented in Section 3. The analysis of the limitations of generic TCP SACK is presented in Section 4. Section 5 concludes the paper.

#### 2. RELATED WORKS

The author in [2] carried out an exhaustive investigation into the effects of data frame size distribution on WLANs without understudying the congestion effects of TCP mechanisms. For HTTP traffic in the context of persistent connections, the work in [3] analysed the network performance of an 802.11-based WLAN in the presence of realistic workloads. A derivation of estimates for the TCP throughput in the context of competing persistent connections, for both standard TCP and generalized delayed ACK techniques was presented. This leads to their development of a queuing model.

The work in [4], presented a simulation study on WLANs for http services using OPNET IT Guru. A collective sample of literature on wireless traffic measurement and Internet protocol performance over wireless networks was studied in [5], [6], [7], and [8]. We observed that several studies have utilized measurements from production wireless networks to compute traffic models [10], [11], [12], [13], [14]. The primary focus of these studies has been to either investigate transport and application layer performance through the analysis of traffic captured on the wireline portion of the network, or utilizes SNMP and syslog information from access points to model mobility and association patterns. The effect of congestion on the performance of the various protocol layers has been studied extensively using either simulations or analytical methods. Cen et al. Propose algorithms for distinguishing congestion from wireless network losses [15]. The algorithms provide a basis for optimizing TCP parameters such as back-off intervals and congestion window sizes. Several methods for the optimization of the 802.11 protocol in congested environments have been suggested [16], [17], [18].

The above studies do not offer an experimental evaluation of link-layer performance in heavily utilized and congested wireless networks particularly for TCP SACK vis-a-vis frame size distribution. This research opines that by gaining a deep understanding of the real-world performance of the TCP SACK under congestion scenario, a novel algorithm can now be considered to address packet size distribution in host spot scenarios.

#### 2.1 Contextual Network Scenario

Consider a hotspot WLAN where an access point (AP) provides access to Web or a shared file system to (n....N+1) hosts. At any instant of time, a host is downloading (or, receiving) at most one file via an AP. This file transfer is controlled using TCP SACK. After the completion of a file transfer, a host waits for a random amount of time before initiating another file transfer request. The size of the requested files in successive requests is assumed to be independent and identically distributed. The TCP controlled Data traffic flows in the downlink direction (from the AP to the hosts) while the TCP Acknowledgement traffic flows from the hosts to the AP. The AP and various node s use the IEEE 802.11 MAC protocol for transmission of their data (TCP DATA packets in case of AP and TCP ACK packets in case of nodes).

This work seeks to show the weakness of existing TCP SACK for real time mission critical applications in a flow-Aware hotspot scenario.

Hence, an important issue to address is the impact of congestion via the 802.11 MAC and the closed-loop nature of TCP SACK. This is accomplished in this paper, where we estimate the frame size distribution by TCP SACK in UNN lionet network for concurrent and persistent connections. A natural step in the wireless frame size distribution is to understand the effect of congestion control mechanism on the network.

#### 3. RESEARCH METHODOLOGY

The experimental approach presents a congestion measurement based on TCP SACK vis-à-vis data frame sizes with characterization of a real life testbed in University of Nigeria Nsukka (UNN Lionet). This work will first characterize the lionet WLAN environment for high density user data access with a good experimental technique to derive our evidence which now gave rise to real plots for analysis purposes

#### 3.1 Description of Experimental Environments

This section discussed UNN Lionet wireless network architecture, the congestion monitoring framework and a set of monitoring challenges for heavily utilized wireless networks. The traffic scenarios comprise of heavy database access, email access, file transfers, etc. Fig. 3.1 shows a Sniffer test terminal (in Room A) with the WifiCard for selective TCP SACK filtering of the designated metrics.



#### Fig.3.1: A Sniffer test terminal (in Room A) with the WifiCard

Fig. 3.2 shows a fixed data center for mobility Computing (FA-WLANS) (Source UNN data center, 2012). In this network, the traffic is typically based on TCP SACK. Several applications and services are hosted from this environment which the end users can access.



Fig.3.2: A Fixed Data center for Mobility Computing (FA-WLANS) (Source UNN data center, 2012)

#### 3.1.1 Lionet Wireless Access Point Environment

In this research we structured the wireless network to comprised of 3 Airspace Access Points (Linksys APs) distributed on three adjacent doors cover a vicinity of about 200m for our investigations. Each AP supported the IEEE 802.11a, IEEE 802.11b and IEEE 802.11n protocol standards; however, in this experiment, we assumed the operation of the IEEE 802.11 generic FA-WLAN for the three standards as depicted by the setup in Fig. 3.1.

Fig. 3.3 show the placement of the 3 APs in the rooms where we conducted our measurement and collection data frame during the day and late evening sessions, respectively.

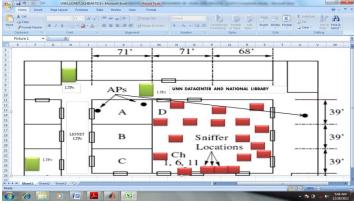


Fig. 3.3: Sniffer locations For Frame Captures.

Fig.3.4 shows the floor Plan of UNN Lionet indicating the positions of the access points. The access points connects to a dynamic hosts configuration server (DHCP) which allocates the respective IP addresses to client machines after a challenge handshake authentication from the network server. In order to optimize network performance, the Airspace APs are designed to support dynamic channel assignment, client load balancing, and transmission power control. The dynamic channel assignment and power transmission controls were enabled. Dynamic channel assignment refers to the technique that switches the AP's operating channel, depending on parameters such as traffic load and the number of users associated with the AP. Client load balancing refers to the technique that controls per-AP user associations via their service set identifiers (SSIDs). The transmission power control regulates the power at which an AP transmits a frame. In our observation, the technical details about these three optimizations are proprietary. Also, the access points were observed to switch channels dynamically to balance the number of users and traffic volume on the three channels.

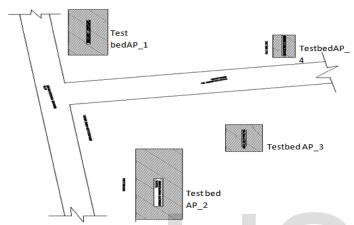


Fig.3.4: Structural diagram of the entire network AP placement

Basically, in heavily utilized FA-WLAN, the wireless portion of the network is a major performance bottleneck. Understanding the behavior of the wireless portion of such networks is critical to ensure their robust operation. This understanding will help us to optimize network performance in our future work.

A quantitative approach was used in carrying out congestion management study using link layer information collected from an operational, medium-scale, and heavily utilized IEEE 802.11 wireless network deployed in our testbed. This work then considered the use of trace file data set define highly congested, moderately congested, and uncongested network states in the context of TCP SACK scheme. This formed the basis for the proposed layer 4DMF which will be compared with other existing congestion control schemes as part of our future work.

#### 3.2 Data Collection Methodology

With the network sniffer, wireshack, measurements were taken on the network described above on each test bed. The attributes (settings) of the access points (Linksys) were first configured and the network sniffer was used to measure the TCP frame sizes, throughput, delay, signal strength, the MAC address, the access point types, the speed, the noise level, vendor etc.

The method used to collect data from the MAC layer is called *vicinity sniffing* [19]. The vicinity sniffing framework consisted of three *sniffers*, Dell Inspiron laptops. Each sniffer was equipped with a Wifi-802.11n radio with WLAN cards. The radios were configured to capture packets in a special

operating mode called the RFMon mode. The RFMon mode enables the capture of regular data frames as well as IEEE 802.11 management frames. In addition, the RFMon mode records information for each captured packet. This information includes the send rate, the channel used for packet transmission, the signal to- noise ratio (SNR) of the received packet, frame number, number of bytes on channel, number of bytes captured and some prism monitor header information which included whether the frame were a wireless LAN management frame or not. Because the Airespace access points were expected to switch between the 802.11 channels 1, 6, and 11, each sniffer was configured to sniff on one of the three different channels for the duration of each session. The packets were captured using the sniffer utility Ethereal wireshack. The snap-length of the captured packets was set to 250 bytes in order to capture only the RFMon, MAC, IP and TCP/UDP headers. The data capturing process was conducted using a placement configuration during the day only.

**i.** Day sessions: The day sessions done between 09:30am and 4:00pm on August 24.08, 2012. The day sessions were split into 1 to 3 parallel tracks and each track was held in one of the several meeting rooms shown in Fig. 3.1. The parallel session tracks were held at three intervals

During the day: 09:30 am to 11:30am, 12:30am to 2:30 pm, and from 2:30pm to 4:00pm. This work chose to place the three sniffers in one of the busiest and largest meeting rooms close to MTN ICT center while picking packets from lionet network. The placement of the three sniffers is shown in Fig. 3.4. Data was collected during the day sessions

#### 3.3 Analysis Data Sets

Wireless network data collected from the Lionet network was arranged into a day session. A trace file of captured real live wireless traffic from UNN wireless Network (LIONET) was used in the analysis considering the congestion scenarios. Wireshark Network Analyzer (Etheral) was used on the various sniffer machines and the traffic data collected. Our collection framework recorded a total of 1.6 million data frames, 1.05 million acknowledgment frames, 40,000 RTS frames, and 17,490 CTS frames during the day and the plenary sessions cumulatively. However, a total of 100000 frames were captured for analysis by progressively analyzing the selected frame captures. The trends of individual frame size types as well as the trend of management and non-management (mostly data) frames were discerned. The use of the RTS.CTS mechanism is generally turned off by default on wireless devices and its use is optional. The data indicates that the use of the RTS.CTS mechanism for channel access by users was average on Table 3.1:

Table 3.1: Trace files Data Set

	Trace mes Data Set		1
Data	Day	Channel	Time
Set			
	August 24, 2012	1	09:30am to 1:30am
Day	August 24, 2012	6	12:30am to 2:30pm
-	August 24, 2012	11	02:30pm to 4:00pm.

However, our sniffer machines satisfy the above requirements. Fig. 3.5 depicts the congestion traffic captured with ethereal Wireshack from varying IP sources as allocated by the DHCP server. Fig. 3.6 depicts the congestion traffic captured with Etheral Wireshack under TCP-SACK and its variants. Fig. 3.7 depicts the Average packets transmitted under congestion scenario. Fig. 3.8 depicts the congestion traffic captured with Etheral Wireshack from varying TCP services. Fig. 3.9 shows the TCP services statistics. Fig. 3.10 shows the congestion traffic captured with Etheral Wireshack from varying TCP Ack feedback packet drop scenario while Fig. 3.11 shows the summary congestion traffic statistics captured with Etheral Wireshack under varying TCP services.

	Ede	Alena	90	Captur	• <u>0</u>	alyze	Statist	ics U	elp													
EX.	- Geol	654		- Had	e	> 0	នា 🔹	e 9		m	9	4	*	80	4	<u>₽</u>				0	a.	
	Reri							-				_	-	+ 0	pressik		200	Jear	1 14	aly		
łu. +		Time		Sour				D	lanitea	ion			Prot	locol	Info							1
		0.000		192	160.	0.2			roade				ARE		Who I	and 1	92.1	60.0	27	Gratur	tour	21
		0.299		192.	168.	0.1			92.14				NBB		Name	quer	Y NE	STAT	**00	IN HOOM	OON HON	\$
		0.299	214	192	160.	0.2		1	92.14	10.Q.	( <b>1</b> )		ICA	P	Dects	00000	OR L	inger 1	tiabl	e (Por	t unr	
		1.025			168.				24.0.				TCP		V3 Me					1.5.1		
		1.048			160						5.250		UDS		Source		dner		E Dese	apte	ion po	13
		1.050			169								DING		STan	and the second	CHART	50	0.01	CHOICE I H	Man COD-1	1
		1.055	05.8		1681				No. 1				1.01.2.0		Source	10 m		3 MOO	Des	TIMATI	on por	
		1.082			168.				92.34				NUM		Regie	trat	100	NII NI	11006	1D:000:		
		1.111			168.				92.14				DN		STAR	fand	quer	YAI	smoory	CONT /S	40004.1	
		1.227			a testing				2201				10.0		11146		<b>TP</b> 1	SYNT		ci Lem-		21
		1.200	282			0. J								_	144.4.14		914			2 m cl m	ACKA	•)
Fr	-	11 (6	2 by:	es or	win	. 62	byter	Cap	tures	17								_				
							byte				Der Der	. Nata		2412	5 19a	(00.1	0915	61241	25.19	•)		
164	hern	ot II	. 50	1 192	.160	.0.2	(00:00	15d1	2010	102		t: Net:						b12d1	75 19	a)		
E.e	hern	et Fr	, Sri	1 192	.160 C: 1	.0.2	(00:00	(192	2010	1102 0.2	. Dat	t: 192.	160	.0.1	(192.	160.	0.1)			a)		
E.e	tern	et Pr	, Sri otocc	1 192 1. Sr	ci 1 Prote	0.2 92.16	(00:00	(192	2010	1102 0.2	. Dat		160	.0.1	(192.	160.	0.1)			a)		
E.e	tern anse Sour	et Pr ssio	, Sri otocc	1 192 1. Sr trol	CI 1: Prote (3196	0.2 92.16 1001,	(00:00	(192	2010	1102 0.2	. Dat	t: 192.	160	.0.1	(192.	160.	0.1)			a)		
E.e	hern Anse Sour Dest	et II et Pr nssio ce pr inati	, Sri otoci n Chi orti	1 192 01, 50 0196 0196	.160 Prote (3196	.0.2 92.16 9001, ) (#0)	(00:0) 8.0.2 See 1	(192 (192	20 ici 160	0.2 6 (1	). Dal	t: 192.	160	.0.1	(192.	160.	0.1)			a)		
Et Ir	Sour Sour Sequ	et II et Pr nssio 'Ce po inati	, Sri otocc n Con orti numb	1 193 01, 5r 0196 0196 0rt: 0	.160 C: 1 Prote (3196 http	.0.2 92.16 9001, ) (#0)	(00:00	(192 (192	20 ici 160	0.2 6 (1	). Dal	t: 192.	160	.0.1	(192.	160.	0.1)			a)		
E.T.	hern Anse Sour Dest Sequ Heat	et II et Pr nesio ce po inati inati inati	, Sri otocc n Con norti numb	1 192 1, 5r 194 196 196 196 196 196 1 28	Ci 1 Prote (3196 http (ytes	.0.2 92.16 9001, ) (#0)	(00:0) 8.0.2 See 1	(192 (192	20 ici 160	0.2 6 (1	). Dal	t: 192.	160	.0.1	(192.	160.	0.1)			a)		
E.T.	hern anse Sour Dest Sequ Heas	et Fr nesto de pe inati ience ler le je: Os	, Sri otocc n Con orti numb numb	1 192 1, 5r 196 196 196 196 196 196 196 196	Ci 1: Prote (3196 http (ytes	.0.2 92.16 9001, ) (#0)	(00:0) 8.0.2 See 1	(192 (192	20 ici 160	0.2 6 (1	). Dal	t: 192.	160	.0.1	(192.	160.	0.1)			a)		
(A)	hern Sour Dest Sequ Heat Flag	et II et Pr nssin ice po inati ience ler le jei Os kow si	, Sro otocc n Co numb numb ngth 0002	11 192 11 192 1196 1196 1196 1196 1196 1196 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1196 11	(J196 (J196 (J196 http (bytes)	.0.2 92.16	(00:0) 6.0.2 Sec 1	(192 (192 AOPE 1	2010 .160 .110	d 102 .0.2 6 (3	), Dst 196), r)	DST P	160	.0.1	(192.	160.	0.1)			a)		
(A)	hern Sour Dest Sequ Heas Wins	et II et Pr nesto inati ience ler le bw si 09 51	s Sri otocc in Con in Con in Con in Con in C	11 192 1, 5r 1196 1196 1196 1196 1196 1196 1196 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1196 119	(J196 (J196 (J196 http (bytes)	0.2 92.16 0001. ) (RO) relat	(00:01 6.0.2 Sec 1	(192 00mt 1 equer	2010 .160. 119	4102 0.2 6 (8 umb-6	00 00	E-W	160	.0.1 http	(192, (80)	160.	0.1)			a)		
E 17	Hern Sour Dest Sequ Heat Wins	et II et Pr nssin insti- insti	, Sri otocc n Chi numb ngth 10002 zei 2d	11 192 1. Sr 1196 1196 1196 1196 1196 1196 1196 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1196 119	()160 ()196 ()196 ()196 ()196 ()196 ()196 ()196 ()196 ()196 ()196 ()196 ()196	0.2 92.16 0001. ) (RO) relat	(00:01 6.0.2 Sec 1	(192 00mt 1 equer	2010 .160. 119	4102 0.2 6 (8 umb-6	00 00		160	.0.1 http	(192. (80)	160.	0.1)			n)		
E T	Sour Dest Sequ Flag	et II et Pr nesto inatione ler le ler le les 0 kow si 09 55 30 10	stores of Con- on to numb numb numb numb numb numb numb numb	11 192 1. Sr 1196 1196 1196 128 1 128 1 128 1 128 1 128 1 128 1 128 1 128 1 128 1 1 1 1 1 1 1 1 1 1 1 1 1	(3196 (3196 (3196 (3196 (3196 (3196 (3196 (3196 (3196 (3196))))))))))))))))))))))))))))))))))))	0.2 92.16 0001, ) (m0) relat	(00:00 6.0.2 Sec 1 1ve e	(192 April 1 equer	20 100 . 160 . 1190 . 1190 	umba	00 00		160	.0.1 http	(192, (80)	160.	0.1)			a)		
E T	Sour Dest Sequ Flag	et II et Pr nesto inatione ler le ler le les 0 kow si 09 55 30 10	stores of Con- on to numb numb numb numb numb numb numb numb	11 192 1. Sr 1196 1196 1196 1196 1196 1196 1196 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1197 1196 119	(3196 (3196 (3196 (3196 (3196 (3196 (3196 (3196 (3196 (3196))))))))))))))))))))))))))))))))))))	0.2 92.16 0001, ) (m0) relat	(00:01 6.0.2 Sec 1	(192 April 1 equer	20 100 . 160 . 1190 . 1190 	umba	00 00		160	.0.1 http	(192, (80)	160.	0.1)			a)		
E 11	hern tern Sour Dest Sequ Heat Flag Wins 00 00 fa	et II et Pr instin ience ler le bow si 09 51 00 100 70 27	, Smootocc n Con numb numb numb numb numb numb numb num	11 192 1. Sr 1196 1196 1196 128 1 128 1 128 1 128 1 128 1 128 1 128 1 128 1 128 1 1 1 1 1 1 1 1 1 1 1 1 1	1.160 c: 1: Prote (3196 http (310) http (310	0.2 92.16 0001, ) (m0) relat	(00:00 6.0.2 Sec 1 1ve e	(192 April 1 equer	20 100 . 160 . 1190 . 1190 	umba	00 00		160	.0.1 http	(192, (80)	160. . Se	0.1) 41 0		11 0	a)		

Image: The second sec		and the second se	Ethernet NIC		rshark 1.6				00000/11							- 0 -
Image: Control (1)         Description (1)         Descri	te Eque Atena Sto															
Type         Source         Decompose         Periodic Length Mile           6 - 113113         50 - 0.6 -0.6 -0.6 -0.6 -0.6 -0.6 -0.6 -0			C++++227		QC	2 Q E		RU 🐻 🕄	36 30							
6 0.11311 0.0.0.5 with the former of the for	iter:			Expression	Ger	Apply	-				_		_			
6 0.13113 10.0.0.18 140,7.241.2 TC 15 10T Data ACX 201 1382 * NTC [ACX See] Add-29803777 Wines800 Level 36.4-2980377 Wines800 Level 36.4-29803	Time	Source	Destination	Protocol 1	enoth 1	Info										_
	7 0.243269 8 0.277528 9 0.277512 10 0.362469 11 0.37032 12 0.170318 13 0.406384 14 0.420138 15 0.462554 16 0.462542 17 0.353166	10.0.0.88 10.0.0.5 149.7.241.26 10.0.0.88 Heel lett41891aC 140.7.241.26 10.0.0.88 10.0.0.2 149.7.241.26 10.0.0.88 149.7.241.26 10.0.0.88 149.7.241.26 10.0.0.88	10.0.0.255 10.0.0.88 149.7.241.26 Broadcast 10.0.0.88 149.7.241.26 255.255.255.255 255.255.255.255 10.0.0.88 149.7.241.26 10.0.0.88 149.7.241.26 10.0.0.88	ТСР NBNS HTTP TCP ARP HTTP TCP MAC-Te1 HTTP TCP HTTP TCP HTTP TCP HTTP	66 92 1494 66 1494 66 133 64 1494 1494 1494	[TCP Di Name qu Continu [TCP Di who has continu [TCP Di 00:0d:1 00:0d:1 00:0d:1 [TCP Di Continu [TCP Di Continu [TCP Di	ation pack in ack in ack	API. YO or non	NTOD.COM HTTP tr: 682 > ht Tell 10. HTTP tr: 682 > ht 00:10:5; 00:10:5; 00:10:5; HTTP tr: 682 > ht HTTP tr: 682 > ht HTTP tr:	M-005 affic ttp [ACK] affic ttp [ACK] affic a122:77:10 affic ttp [ACK] affic ttp [ACK]	Seq=1 Seq=1 9 Direc 9 Direc 9 Direc 1 Seq=1 Seq=1	Ack=42949 Ack=42949 tion: Cli tion: Cli Ack=42949 Ack=42949	55777 wi ent->Ser ent->Ser 55777 wi 55777 wi	In=64800 I In=64800 I In=64800 I In=64800 I	Len=0 SLE : Data : Acknowl Len=0 SLE Len=0 SLE	429495721 429495721 4996 429495721 429495721
	20 0,647667 Ethernet II. Internet Proto transmission	Eycon on wire (119) Fre: Jeom_90:3b:71 ( Scol Version 4, Src: control Protocol, Src	0:50:da:90:1b:71), 149.7.241.26 (149.	Dst: Com	(1105) palin_ 	Ja:04:0	11 03 (00: 0.85 (3	1b:38:34 0.0.0.81	a:04:03) 8)	,	seq=1	ack=12949	55777 w			4.294.997.23
Frame (Iranse), 1494 bytes Packets: 1170 Displayed: 1170 Marked: 0 Profile: Default	20 0.647667 Frame 12 2404 Ethernet II. Internet Prote Transmission e Hypertext Tran 00 00 10 18 10 05 cs 00 0 10 0 cs 00 0 10 0 0 0 0 0 0 10 0 0 0 0 0 0 0	Increase on technol (1995) Free Jenn, 90 19 173, 0 scol Version 4, Sree control Protocol, sree insfer Protocol 4 04 05 00 50 da 00 14 00 05 10 da 00 15 0 da 00 15 0 da 00 05 10 da 00 15 0 da 00	2 Dits), 1494 Dytes 30:50:04:00:10:73), 149.7.241.26 (149, c Port: http (80), 50:07:10:10:10:10:10:10 50:07:10:10:10:10:10 50:07:10:10:10:10:10 50:07:10:10:10:10 50:07:10:10:10:10 50:07:10:10:10:10 50:07:10:10:10:10	Captored Dat: Com 7,241,200 Dost Port:	(1105) palin_ 	Ja:04:0	11 03 (00: 0.85 (3	1b:38:34 0.0.0.81	a:04:03) 8)	,	seq=1	ack=12949	55777 w			4.094.957.23

Fig.3.6: Congestion traffic captured with Etheral Wireshack under TCP-TRONVS.

Wireshark Summary					
file					
Name				C/\Users\NG\AppData\Local\Temp\wireshark_62F1C869-50F9-42C3-8979-147618041587_20128216135645_a04492	
Length:				1305977 bytes	
Format:				Wireshafk/tcpdump/ libpcap Unknown	
Encapsulation: Packet size limit:				Unknown 65535 bytes	
Packet size innic				6333 B/48	
Time					
First packet:				2012-02-16 13:56:45	
Last packet:				2012-02-16 13:58:07	
Elapsedi				80.01.21	
Capture					
Interface				Realtek RTU8139/810x Family Fast Ethernet NEC	
Dropped packets:				unknown	
Capture filten				none	
Display					
Display filten				none	
Ignored packets:				0	
Traffic	<ul> <li>Captured</li> </ul>	• Displaye	d • Marked		
Packets	1699	1699	0		
Between first and last	packet 81.476 sec				
Avg. packets/sec	20.853				
Avg. packet size	752,660 by	tes			
Bytes	1278769				
Avg. bytes/sec	15695.111				
Avp. MBit/sec	0.126				
and and an					
Help					Stose
	-				
	12 🚞	52	~		- □ 10 10 10 10 100 PM
					2/16/2012

Fig.3.7: Average packets transmitted under congestion scenario

Bis Idt Yers &		ca Telephene Tools I-	ranah Malo	rechtere 3.4.3 (Suits Aan 40429 Nove (transled A))
			and the second	
Filter			bornen.	u Chur Apply
No. Tava 6 0.185134 7 0.243269		Destention 169.7.241.26 10.0.0.255	Protocol 1 TCP NSNS	Laugh Mo. 45 [FUE Dap Ack 242] 31882 > http://dxil.36014.Ack-4264955777 win-64800 Lan-0 SLK-429495 45 Water Opency Mil. 473.100006, Com-OD: 142.8 0004 (CONTUNE or Annotation and Acc.
+	10.0.0.84 Hewlett, 42:39:26 149.7.241.26 10.0.0.88 10.0.0.88 10.0.0.3 149.7.241.26 10.0.0.88 149.7.241.26 10.0.0.88 149.7.241.26 10.0.0.88 249.7.241.26 10.0.0.88 bytes on wire (1193	128,7,241,24 #readcast 10,0,0,88 149,7,241,24 255,251,253,255,251 10,0,0,88 149,7,241,26 10,0,0,88 149,7,241,26 149,7,241,26 20103),1494 byte: 20103),1494	TCP ARP HTTP TCP NAC-TQ1 HTTP TCP HTTP TCP HTTP TCP HTTP TCP HTTP TCP CP CP CP CP CP CP CP CP CP CP CP CP C	46 [TTP large 26, 24]; 1883 - 1812 [Cel] Bargh Annal/2481377 straid/861 [thro 516.23847 86 [TTP large 26, 24]; 1883 - 1812 [Cel] Bargh Annal/2481377 straid/861 [thro 516.23847 86 [TTP large 26, 24]; 1880 - 1812 [Lel] Bargh Annal/2481377 straid/861 [thro 516.23847 80 [TTP large 26, 24]; 1880 - 1812 [Lel] Bargh Annal/2481377 straid/861 [thro 516.23847 80 [TTP large 26, 24]; 1880 - 1812 [Lel] Bargh Annal/2481377 straid/861 [thro 516.23847 80 [TTP large 26, 24]; 1880 - 1812 [Lel] Bargh Annal/2483377 straid/861 [thro 516.23847 80 [TTP large 26, 24]; 1880 - 1812 [Lel] Bargh Annal/2483377 straid/861 [thro 516.23847 80 [TTP large 26, 24]; 1880 - 1812 [Lel] Bargh Annal/2483377 straid/861 [thro 516.23478 80 [TTP large 26, 27]; 1883 - 1812 [Le] Bargh Annal/2483377 straid/861 [thro 516.23478 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483377 straid/861 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483377 straid/861 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483377 straid/861 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483377 straid/861 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483377 straid/861 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483377 straid/861 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483377 straid/861 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483377 straid/861 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483378 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483378 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/24833377 straid/861 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/24833377 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/24833378 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [Le] Bargh Annal/2483378 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [thro 516.23478] 80 [TTP large 27]; 1883 - 1812 [thro 516.23478] 80 [TTP la
a Internet Prot	ocol version 4, Srcs concrol Protocol, sr	c Port: hctp (80),	DUE POPEL	

Fig.3.8: Congestion traffic captured with Etheral Wireshack from varying TCP services



Fig.3.9: TCP services statistics

Time	149.7.241.25 10.0.0.88	10.0.0.5 10.0.0.255	Hewlett4a39.ac	Comment	
0.185	Continuation or non			HTTP: Continuation or non-HTTP traffic	
185	TEP Dup ACK 2#215			TCP: [TCP: Dup: ACX 242] 51682 > http: [ACX] Seq=1 Ack+4294955777 Win+64800 Len+0 5LE+4294957217 SRE+4	
0.243		Name query NB APLY		NBNS Name query NB ARLYONTOD.COM+00>	
0.278	Continuation or not			HTTP: Continuation or non-HTTP safe	
0.278	ITCP Dup ACK 28315			TCP: (TCP Dup ACK 240) \$1682 > http: (4CK) Segs1 Acks4294855777 Wine64800 Lens0 \$3,8:s4294957217 \$85:s5	
362			Who has	ARP Who has 1002447 Tel 100317	
.370	Continuation or non			HTTP: Continuation or non-HTTP traffic	
370	ITCP Dup ACK 2=415			TCP: (TCP: Dup: ACX: 244) 51682 > http: (ACX) Seg=1 Ack+4294955777 Win+64800 Len+0 SLE+4294957217 SRE+7	
405	and the second se			MAC-Teinet 00:0d:9d:4ea846 > 00:10:5e2277:b9 Direction: Client->Server Type: Data	
420				MAC-Teinet: 00:00:9:0:4xa5:45 > 00:10:5x2277:09 Direction: Client->Server Type: Acknowledge	
.463	Continuation or nos			HTTP: Continuation or non-HTTP suffic	
0.463	TCP Dup ACK 2=515			TCP (TCP Dup ACK 245) \$1682 > http: (ACK) Seg=1 Ack=4294955777 Win=64800 Lan=0 SLE=4294957217 SRE=8	
555	Continuation or nos			HTTP: Continuation or non-HTTP traffic	
555	TEP Dup ACK 2#615			TCP: (TCP: Dup: ACK 2#6) 51682 > http: (ACK) Seg=1 Ack=4294955777 Win=64800 Len=0 9.E=4294957217 SRE=1	
1548	Continuation or non			HTTP: Continuation or non-HTTP traffic	
0.648	TCP Dup ACK 2#715			TCP: (TCP Dup ACK 247) 51682 > Mtp (ACK) Seg =1 Ack+4294655777 Wine64800 Lenvo 5LE+4294957217 SRE=1	
657	and a second	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		NBNS Nerve query NB WWW GDDGLE COM (00)	
0.740	Continuation or non			HTTP: Continuation or non-HTTP traffic	
740	ITCP Dup ACK 24815			TCP. (TCP. Dup. ACK 246) 51682 > http://ACKi.Sep=1.Acki+4294955777 Win+64800 Len+0 5LE+4294957217 58E+1	
.833	ITCP Retransmission			HTTP: (TCP Retransmission) Continuation or non-HTTP traffic	
823	\$1682 > http [ACK]			TCP: 51/62 > http://4Ck1 Seciel: Arck+12961 Win+64800 Lenv0	
925	Continuation or non			HTTP: Continuation or non-HTTP traffic	
018	Continuation or non			HTTP: Continuation or non-HTTP traffic	
018	S1682 > http://ACKI			TCP: 11652 > Http: (4CK) Segu1 Acku15641 Winu64600 Lenu0	
110	Continuation or not			HTTP: Continuation or non-HTTP traffic	
183	and the second second			TCP: 51649 > http: [5]N: ACK] Seg=1 Ack+1 Win=16278 Lan=0	
1.203	Continuation or non			HTTP: Continuation or non-HTTP traffic	
.203	\$1682 > http://ACK1			TCP S1682 > http: (4CK) Sequil Advail8721 Winad4800 Lenad	
				-	
	* Installing			Dyn	



International Journal of Scientific & Engineering Research, Volume 5, Issue 4, April-2014 ISSN 2229-5518

		ATLANTING Forsity Last			them 3.8.5. Cluffe free #16.79 from (Wash-1#11)	
Image: Control of the state of the	ine for the first	Driven, Workin, Street	es Telephony Loois Ivo			
Description         Description <thdescription< th=""> <thdescription< th=""></thdescription<></thdescription<>		EQXDA	000027	0.00	a a a 🖸 📲 🛛 📲 💥 🗯	
1 3.0000 1.5.7.24.14 1.0.0.6.9 ar 17 1.14 0.0.0.14 1.0.0.7 ar 1.14 0.0.0.14 1.0.0.14 1.0.0.14 1.0.0.14 1.0.0.14 1.0.0.14 1.0.0.14 1.0.0.0.14 1.0.0.0.14 1.0.0.0.14	Stat			Epreson.	Onar Teply	
weight         weight	1 0.00000 2 0.000104 3 0.000104 4 0.000104 5 0.185037 5 0.185037 6 0.185037 6 0.277528 9 0.277547 10 0.362469 11 0.370437 12 0.362469 11 0.370437 12 0.362469 13 0.400386 14 0.420338	149,7,241,28 149,7,241,28 149,7,241,28 149,7,241,28 149,7,241,28 10,0,0,88 10,0,0,88 149,7,241,28 10,0,0,88 149,7,241,24 10,0,0,88 149,7,241,24 10,0,0,88 10,0,0,2	$\begin{array}{c} 10, 0, 0, 68\\ 140, 7, 241, 268\\ 100, 0, 0, 88\\ 140, 7, 241, 268\\ 100, 0, 0, 68\\ 110, 0, 0, 68\\ 110, 0, 0, 0, 235\\ 100, 0, 0, 235\\ 100, 0, 0, 235\\ 100, 0, 0, 84\\ 140, 7, 241, 268\\ 100, 0, 0, 84\\ 140, 7, 241, 268\\ 100, 0, 0, 84\\ 140, 7, 241, 268\\ 100, 0, 255, 255\\ 255, 255, 255\\ 255, 255, 255$	HTTP TCP HTTP TCP HTTP TCP Mdk5 HTTP TCP Mdc-Ta1 Mdc-Ta1	List continuation or non-more carffit and continuation of non-more carffit and con	77 W18-81800 Lan-0 3LL-4291097227 77 W18-84800 Lan-0 5LL-4294997217 77 W18-84800 Lan-0 5LL-4294997217 77 W18-84800 Lan-0 5LL-4294997217 77 W18-84800 Lan-0 5LL-4294997217
	<pre>neader length: Differentiate total compto: Identification #Flags: CAU2 (0 #rapment offs: Time to live: Protocol: IDE Breader checks: Source: 140.7 Destination: I Transfission Com Pypertext Transfi</pre>	4 Services Field. 1 4480 1: Codobe (12774) Son't Fragment) 4: 0 42 (0) am (0.1499 [correct 245.26 (140.7.241, 10.0.0.88 (10.0.0.) fer Frotecol	1] 26) 55) 5 Port: Http (80), 5	Nat Port:	33662 (31682), Seg: 4321, Adki 1, Len: 1440	
	020 00 18 00 50 010 3c 88 90 71 040 01 15 65 27 030 00 99 05 88		97 39 34 08 50 10 43 88 45 45 47 44 50 64 42 43 07 62 77 07 79 63 00 70	X. P N 4 5 9 	· · · · · · · · · · · · · · · · · · ·	Profile Delaut
	💿 🖉 🛛	2 📜 🔛	N 2	1	No. No. of Concession, Name	- 10 No # 41 2/0/PM

Fig.3.11: Summary congestion traffic statistics captured with Etheral Wireshack under varying TCP services.

During the day sessions between 09:30am and 4:00pm, frame propagation under congestion periods as a result of much traffic enabled the capturing of TCP frames at various tracks. Fig.s 3.5 to Fig. 3.11 shows the responses of the combinations of selected frames sizes from the trace file of the scenario data set whose metrics are shown for captures 1, capture 6, capture 13, capture 23, capture 36, capture *N*.

However, this work only focused on TCP SACK traffic captures 1, capture 6, capture 13, capture 23 and capture 36. The metric selected for our study included frame sizes, throughout, latency, sources and destination.

# 4. ANALYSIS OF TCP SACK METRICS

Fig. 3.12 shows an ethereal data collection snapshot showing various parameters such as frame sizes (Bytes/Bits), delays (Secs), throughputs (Bytes/Bits), TCP SACK protocols, sources, destinations.



Fig. 3.12: A Snapshot of Etheral Wireshack Capture Datasets

In Fig 3.13 and Fig. 3.14, congestion analysis in context was based on frame size distributions. As shown in the trends, the frame sizes follow an odd sequence as result of TCP SACK mechanism leading to intermittent packet drops. In Fig. 3.15 and 3.16, the TCP SACK easily gets saturated and once this occurs, a gradual decrease in the throughput response follows suite with time particularly with corresponding increase in the number of users on the network. This is also the case with Fig 3.21. Fig. 3.18 and Fig. 3.19 show a similarity response with Fig. 3.15 and Fig. 3.16.

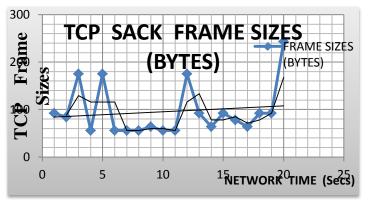


Fig.3.13: Congestion TCP SACK Frame size behaviour (bytes)

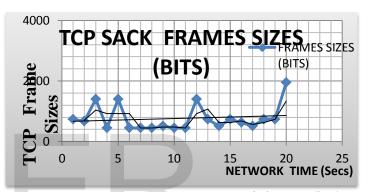


Fig.3.14: Congestion TCP SACK Frame size behaviour (bits)

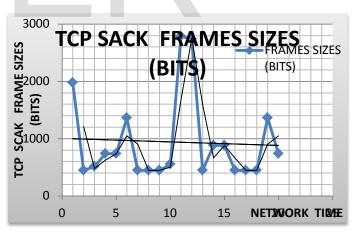


Fig. 3.16: Congestion TCP SACK Throughput behaviour (Bytes/secs)

Fig. 3.17 and Fig. 3.20 show the delay transitions under the influence of TCP SACK congestion. The delay gradually builds from an initial gradient to a maximum of about 1second before switching on the users to the network.

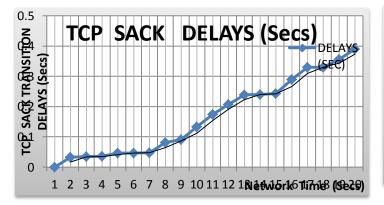


Fig. 3.17: TCP SACK delay transition plot

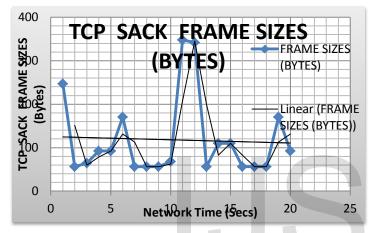


Fig.3.18: Congestion TCP SACK Frame Size behaviour (Bytes)

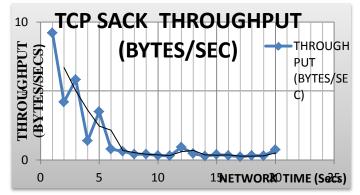


Fig.3.19: Congestion TCP SACK behaviour (Bits) for capture 23

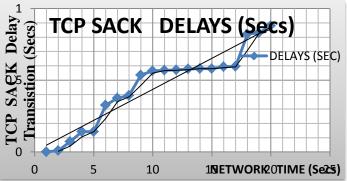


Fig. 3.20: TCP SACK Delay transition behaviour (Secs)

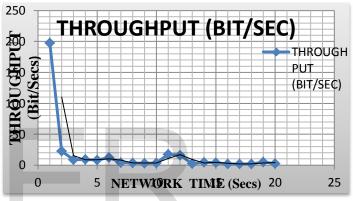


Fig.3.21: Congestion TCP SACK Throughput behaviour (Bits/Secs)

An analysis of the data from the plots of Fig. 3.13 to Fig. 3.21 now led to the following main observations:

- The throughput metrics in TCP SACK scheme is largely unacceptable for FA-WLAN as packet drops at peak times very common.
- The delay time based on TCP SACK is too large for a network intensive service provisioning.
- The use of RTS.CTS by a few nodes in a heavily congested environment (frame size context) prevents those nodes from gaining fair access to the channel.
- The number of frame transmissions at 11Mbps is low while that of 54Mbps are high for all congestion levels. Current rate-adaptation implementations make scarce use of the 2 Mbps and 5.5 Mbps data rates irrespective of the level of congestion.
- At high congestion levels, the time to successfully transmit a large frame sent at 54Mbps is *lower* than for a small frame sent at 11 Mbps.
- At high congestion levels, the delay time consumed by frames transmitted at 54Mbps is only about half the time consumed by frames transmitted at 11Mbps. Yet the number of bytes transmitted at 54Mbps is approximately 300% more than at 11Mbps.

These observations offer important insight into the operation and performance of congested wireless networks. The International Journal of Scientific & Engineering Research, Volume 5, Issue 4, April-2014 ISSN 2229-5518

plots in Fig.s 3.22, 3.23 and 3.24 also present an insight into congestion classification.

#### 4.1 Congestion Classification

This work through the observed trends in the ethereal traffic plots and data set captured, classified FA-WLAN into three classes: uncongested, moderately congested, and highly congested. In context, on the wireless network case study, an uncongested channel is a channel that experiences less than 30% utilization form the capture framed. When the throughput and goodput of the network shows a gradual increase from 30% utilization to 84%, the network is moderately congested (medium throughput). A network is stated to be highly congested when the channel utilization is greater than the 90% threshold ie very low throughput with large packet drops.

#### 4.2 Effects of Congestion

The aggregate effects of effect of the different congestion levels on network characteristics, behavior of the RTS-CTS mechanism, and reception of frames of different frame sizes transmitted at different rates, and acceptance delays for data packets is very large for TCP SACK. These characteristics offer a basis for understanding the operation of the IEEE 802.11 MAC protocol in heavily congested networks. In our experiments to better understand the effects of congestion, we categorize data frames capture into 10 different categories. The categories are defined as a combination of (1) the four possible data rates: 1, 5.5, 11, and 54Mbps, and (2) the four different frame size classes: small, medium, large and extra-large. The frames are split into the four size classes so that the effect of congestion on different sized frames can be derived separately. The four size classes are defined as follows:

- i. Small (S): frame sizes between 1-400 bytes
- ii. Medium (M): frame sizes between 401-800 bytes
- iii. Large (L): frame sizes between 801-1200 bytes
- iv. Extra-large (XL): frame sizes greater than 1200 bytes

The behavior of the small size class is representative of short control frames and data frames generated by voice and audio applications. The medium, large, and extra-large size class represents the frames generated by file transfer applications, SSH, HTTP, and multimedia video applications. Fig. 3.22, Fig. 3.23 and Fig. 3.24 depict these behaviors.



Fig.3.22: Congestion response with frame sizes between 401-800 bytes {Medium (M)}

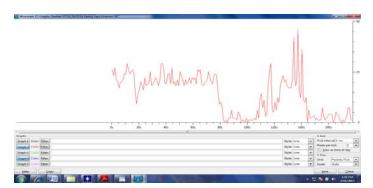


Fig.3.22: Congestion response with frame sizes between 801-1200 bytes {Large (L)}

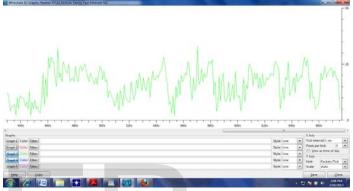


Fig.3.24: Congestion response with frame sizes greater than 1200 bytes (Extra-large (XL))

# 4.3 Channel Utilization, And Throughput Qos

Channel utilization for a set period of time is computed on a real time scale. In this study, we configured the graph plotter in the server to show the channel utilization of TCP SCK as shown in Fig. 3.25 and Fig. 3.26. This work observed that the timing interval is an appropriate granularity for a good analysis. The utilization of a network channel per second is computed by adding (1) the time utilized by the transmission of all data, management, and control frames recorded by the sniffers, and (2) the total number of delay components such as the Distributed Inter-frame Spacing (DIFS) and Short Inter-frame Spacing (SIFS) during the same second. These delays form a part of the channel utilization computation because, during this period, the medium remains unshared between the stations in the network. The communication channel is unshared when no other station in the vicinity of the station that holds the channel can transmit frames for the specified delay time. Congestion was observed at different time tracks as the frame data set kept increasing with time. For TCP SACK, the channel utilization effects as depicted in Fig.s 3.25 and Fig. 3.26 is not reliable for a FA-WLAN.

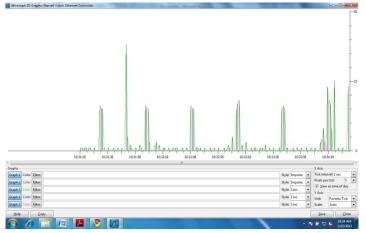


Fig. 3.25: TCP SACK Utilization response for capture 23

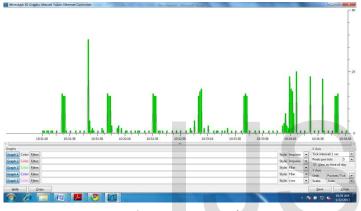


Fig.3.25: TCP SACK Utilization response for capture 6

# 5. DISCUSSION

Based on the observed congestion trends from the study, TCP frame dataset under congestion experiences large data drops, poor throughput while building large queuing lengths in the testbed environment. Under TCP SACK variant, congestion control under realistic loads is really difficult. Also, the quality of service will not be optimized in any intelligent network that uses TCP SACK. Finally, with TCP SACK, optimization of resources in WLAN setups will be expensive and resource consuming.

# 6. CONCLUSION AND FUTURE DIRECTIONS

In investigation on TCP SACK control scheme as well as the analysis of congestion effects on frame size distribution is crucial for the robust operation of efficient networks. An improved congestion control scheme will enhance a reliable user experience on FA-WLANs. To this end, this paper has presented an analysis of a large-scale hotspot wireless network deployed at the University of Nigeria Lionet Hotspot environment. Specially, we have investigated the effect of congestion on frame size distribution, delay, congestion classification and TCP utilization. It is shown that TCP SACK as well as other TCP variants will need to be remodified to address complex network scenarios.

Future work will show how a proposed layer4 –DMF algorithm can improve the overall performance of FA-WLAN in context. A validation criterion will be used to justify our proposal.

# REFERENCES

- Haniza N., Zulkiflee M., Abdul S.Shibghatullah, Shahrin S., " Congestive Loss in Wireless Ad hoc Network Network Performance Analysis" In World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 6, 269-273, 2011.
- [2] Aneke Ogochukwu Joseph, "Effects of data frame size distribution on WLAN"M.Sc thesis, UNN, 2009.
- [3] Salam A. Najim, Ibrahiem M. M. El Emary, and Samir M. Saied, "Performance Evaluation of Wireless IEEE 802.11b used for E-Learning Classroom Network" IAENG International Journal of Computer Science, 34:1, IJCS. August 2007.
- [4] Daniele Miorandi, Arzad A. Kherani, Eitan Altman, " A queuing model for HTTP traffic over IEEE 802.11 WLANs" Elsevier Computer Networks50 (2006) 63–79
- [5] B. Bennington and C. Bartel, "Wireless Andrew: Experience Building a High Speed, Campus-WideWireless Data Network", Proceedings of ACM MOBICOM, Budapest, Hungary, pp. 55-65, September, 1997.
- [6] T. Hansen, P. Yalamanchili and H-W. Braun, "Wireless Measurement and Analysis on HPWREN", Proceedings of Passive and Active Measurement Workshop, For Collins, Co, pp. 222-229, March 2002.
- [7] A. Balachandran, G. Voelker, P. Bahl, and P. Rangan, "Characterizing User Behavior and Network Performance in a Public Wireless LAN", Proceedings of ACM SIGMETRICS, Marina Del Rey, CA, pp. 195- 205, June 2002.
- [8] H. Singh and P. Singh, "Energy Consumption of TCP Reno, TCP NewReno, and SACK in Multihop Wireless Networks", Proceedings of ACM SIGMETRICS, Marina Del Rey, CA, pp.206-216, June 2002.
- [9] D. Tang and M. Baker, "Analysis of a Metropolitan- Area Wireless Network", Proceedings of ACM MOBICOM, Seattle, WA, pp. 13 23, August 1999.
- [10] A. Balachandran, G. M. Voelker, P. Bahl, and P. V. Rangan. Characterizing User Behavior and Network Performance in a Public Wireless LAN. In *Proceedings of ACM SIGMETRICS*, pages 195.205, Marina Del Rey, CA, June 2002.
- [11] T. Henderson, D. Kotz, and I. Abyzov. The Changing Use of a Mature Campus-wide Wireless Network. In *Proceedings of ACM MOBICOM*, Philadelphia, PA, September 2004.
- [12] D. Kotz and K. Essien. Analysis of a Campus-wide Wireless Network. In *Proceedings of ACM MOBICOM*, Atlanta, GA, September, 2002.
- [13] X. Meng, S. Wong, Y. Yuan, and S. Lu. Characterizing Flows in LargeWireless Data Networks. In *Proceedings of ACM MO-BICOM*, Philadelphia, PA, September 2004.
- [14] D. Schwab and R. Bunt. Characterizing the Use of a Campus Wireless Network. In *Proceedings of IEEE INFOCOM*, Hong Kong, March 2004.
- [15] S. Cen, P. C. Cosman, and G. M. Voelker. End-to-end Differenti-

769

ation of Congestion and Wireless Losses. ACM/IEEE Transactions on Networking, 11(5):703–717, October 2003.

- [16] E. Modiano. An Adaptive Algorithm for Optimizing the Packet Size Used inWireless ARQ Protocols. Wireless Networks, 5(4):279.286, July 1999.
- [17] Y. Tay and K. Chua. A Capacity Analysis for the IEEE 802.11 MAC Protocol. Wireless Networks, 7(2):159.171 March 2001.
- [18] M. Torrent-Morenoe, D. Jiang, and H. Hartenstein. Broadcast Reception Rates and Effects of Priority Access in 802.11 Based Vehicular Ad hoc Networks. In *Proceedings of ACM VANET*, Philadelphia, PA, October 2001.
- [19] A. Jardosh, K. Ramachandran, K. Almeroth, and E. Belding-Royer. "Understanding Link-Layer Behavior in Highly Congested IEEE 802.11b Wireless Networks". In *Proceedings of ACM SIGCOMM Workshop E-WIND*, Philadelphia, PA, August 2005.

# IJSER