Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi

Afyon Kocatepe University Journal of Science and Engineering

AKÜ FEMÜBİD **16** (2016) 035101 (592-598) AKU J. Sci. Eng. **16** (2016) 035101 (592-598)
DOI: 10.5578/fmbd.36324

Araştırma Makalesi / Research Article

Security Patrol Control and Data Transfer Performance Analysis of Campus Network Using Wireless Mobile Nodes

Zeydin Pala
Muş Alparslan Üniversitesi, Mühendislik-Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Muş
e-posta: z.pala@alparslan.edu.tr

Geliş Tarihi: 23.06.2016 ; Kabul Tarihi: 22.11.2016

Keywords
Wireless LAN, Mobile Security Station; Campus Security; Wireless LAN Roaming

Abstract

Each method suggested for each solution to simplify our lives brings a perspective towards problems. Wireless solutions are now included in every aspect of our lives. In this study, duties and responsibilities of both campus security and security guards were brought to the forefront and a wireless mobile patrol system was suggested. The aim was to put forth more effective and more controllable model of the efforts. The main theme of the designed network system created in two cases: The first one is a mobile node circulating in orbit that defines the campus environment. The second one is sending the collected information to the target station. While the mobile node was visiting around campus, it took the advantage of all access points and sent collected data to target stations with its roaming feature. Five different scenarios were designed and different transmission standards were used to evaluate delays with data transmission performance. In the network system design, Riverbed Modeler Academic Edition 17.5 PL6 (OPNET) was used. To conclude, both IEEE 802.11g and IEEE 802.11n standard data were successfully transmitted to the central station. As the mobile node went farther away from access points during data transmission, data transfer rates decreased. In the security patrol model suggested here, the obtained analysis results showed that wireless transmission devices arranged in lower speed were more successful.

Kampüs Ağlarında Kablosuz Mobil Düğümler Kullanılarak Güvenlik Devriyesi Kontrol ve Veri Transfer Performans Analizi

Anahtar kelimeler
Kablosuz Ağ; Mobil Güvenlik İstasyonu, Kampüs Güvenliği; Kablosuz Ağ Dolaşımı.

Özet

Hayatımızı kolaylaştıran her bir çözüm, önerilen her bir yöntem, sorunlara bir bakış açısı getirir. Kablosuz çözümler artık hayatımızın her noktasında yer almaktadır. Bu çalışmada hem kampüs güvenliği hem de güvenlikçilerin görev sorumlulukları ön plana çıkarılmış ve mobil kablosuz bir devriye sistemi önerilmiştir. Amaç, daha etkin ve daha kontrol edilebilir bir modelin ortaya konulma çabasıdır. Tasarlanan ağ sisteminin ana temasını iki şey oluşturmaktadır: Bunlardan birincisi, kampüs çevresini tanımlayan yörüngede dolaşan mobil bir düğüm, ikincisi ise toplanan bilgilerin gönderileceği hedef istasyonudur. Mobil düğüm kampüs çevresini gezerken, kablosuz ağ dolaşım özelliği sayesinde, tüm erişim noktalarından faydalanarak, verileri hedef istasyona göndermiştir. Tasarlanan beş ayrı senaryoda, farklı iletim standartları kullanılarak, veri iletim başarımı ile beraber gecikmeler değerlendirilmiştir. Ağ sistemi tasarımında, Riverbed Modeler Academic Edition 17.5 PL6 (OPNET) kullanılmıştır. Böylece hem IEEE 802.11g hem de IEEE 802.11n standardı ile veriler başarılı bir şekilde merkez istasyona iletilmiştir. Veri iletimi esnasında, mobil düğüm her bir erişim noktasından uzaklaştıkça, merkeze iletilen veri hızları da düşmektedir. Bu çalışmada önerilen güvenlik devriyesi modelinde elde edilen analiz sonuçları, düşük hızlarda ayarlanan kablosuz iletim cihazlarının daha iyi başarım sağladığını göstermiştir.

© Afyon Kocatepe Üniversitesi

1. Introduction

Being a product of human thought, technology is developing and offering better solutions to the new problems day after day. As a result of this development, wireless communications continue to be the focus of researchers' attention in solution-oriented sense. In terms of performance, the assessment process using OPNET Modeler is based on certain criteria of the wireless and wired networks in studies conducted in recent years (Abdullah and Mustafa 2016; Jasper 2015; Yi et. al 2013; Sukhroop et. al 2012). Mobile nodes are

widely used in wired and wireless networks. In the literature, there are a variety of studies recently conducted on the energy efficiency and facilitated use of the mobile node (Pal and Dhir 2013).

Thanks to their flexibility, simulation and modeling software continue to be the focus of researchers' attention (Alisa 2013; Jaswal et al. 2014; Khan et al. 2013; Kumar and Velmurugan 2013; Nehra and Singh 2013; Park and Willinger 2000). In network simulation research, OPNET, OMNeT++, NS2, NS3, NETSIM++ Smurphin, comnet3 and Qualnet mostly are used in wired and wireless networks (Sukhroop et. all 2012; Tolani and Mishra 2012; Yiu et. all 2013; Zubairi and Zuber 2000). Riverbed Modeler Academic Edition 17.5 PL6 (OPNET) supports discrete event-driven simulation (DES). DES can ensure to make more accurate and realistic modeling (Leemis and Park 2006).

OPNET modeling software is extensively used both by network researchers and trainers. Modelling flexibility, facilitation of model development, rapid modeling capabilities are only a few features of the OPNET. In OPNET environment, simulations can be run with the changed parameters. (Lu and Yang 2012).

To evaluate network performance, four different methods are used by assessing the network protocols for modeling a system (Leemis and Park 2006):

The first one is analysis and mathematical modeling; the second one is discrete time-based or event-based simulation, the third one is analysis and simulation of hybrid simulation and the last one is the test-bed emulation.

For university campuses, generally large areas are preferred since many new units can be installed in the future. However, this situation makes it difficult for pedestrians to ensure security audit of the patrol.

A mobile patrol system has been suggested to overcome this difficulty. The wireless mobile patrol system, which can send data to the central station, can roam the campus environment. A trajectory is determined to define the campus environment for the mobile node. Using the suggested mobile data collection system, both safety spots and security guards can be controlled. In the design of the mobile patrol system, both Ethernet technology (IEEE 802.3) and WLAN (IEEE 802.11g/n) standards are used together (Gupta and Kaur 2010).

One of the goals of this activity is to enable mobile node to gather information to conduct the plotted trajectory, and the second one is to send the collected data to the destination station via access points. More precisely, the collected data is transmitted to the central unit via wireless access points which are located on four separate locations within the campus network. On campus, the lack of fully functioning of security patrols is a major issue. In this study, the suggested system forced security guards to do their tasks on time. It is also important for security guards to do their own tasks at least until the environmental safety is ensured.

2. Material and Method

In this study, Riverbed Modeler Academic Edition 17.5 PL6 (formerly OPNET) simulation software was used to evaluate the results of the five scenarios. Four of them were carried out using Access Points (APs) having different transmission speeds. In the last scenario, two mobile security nodes were used. In one of them, two different mobile nodes were used at the same time, yet in delay. The second node was moved approximately 450 seconds after the movement of the first node. When the simulation was completed, both of the mobile node sending data performances were analyzed together.

The fundamental difference between four other scenarios is different data transmission speeds of Wi-Fi modules used in both access point and mobile node in the system infrastructure. The speed rates used in the scenarios are as follows; 6.5 Mbps (base)-60 Mbps (max), 26 Mbps(base)-240 Mbps (max), 65 Mbps(base)-600 Mbps (max) and 54 Mbps (for 802.11g), respectively.

The mobile node was initially connected to the access point named Access Point 1 (AP1). Thanks to its roaming feature (Shklyaeva et. al 2006; Alsaif et. all 2014), as it moved on its orbit, the data was transferred to the central station through access points which entered the coverage area.

Using a star topology, 1000Base X type of cable was used in the designed network infrastructure. Prior to the simulation, a trajectory that determined the path to be followed by the mobile node was drawn

Trajectory presented as dashed lines in Figure 1 represents the campus environment. The mobile node was made to follow the trajectory presented in the Figure in all of the simulations. Meanwhile the speed of the mobile node was 20 km/h. The mobile node continued on its way without stopping until the end of the simulation. While determining the direction at certain points, the speed of the mobile node continued to stay in constant way and straight away. To complement the inner perimeter of the campus, total length of the trajectory total length was 5.009 m.

The starting point of the movement of the mobile node was the Aliya Izetbegovic square, in the center of the campus. Movement began in the square, continued down underneath the transformer building. After the sightseeing tour was completed, it returned back to Aliya Izetbegovic square.

In this study, the common parameters used in the scenarios are presented in Table 1. As presented in Figure 2, four access points were capable of communicating wirelessly with the mobile node used in the study. Destination station and access points were connected to the central switch via fiber optic cable.

In the modeled wireless network, the data load to be produced by the mobile node can be calculated as follows:

MN load= ((Mean ON Time)/ (Mean ON Time + Mean OFF Time)) *(Packet size in bits) *(Number of nodes generating traffic)/ (Mean Interarrival Time)
Where a mobile node has the following data load in minimum:
= (900/900) *(1000*8) *1/ (0,005) = 1.6 Mbps

The maximum value is as follows:
= (900/900) *(2000*8) *1/ (0,005) =3.2 Mbps

Table 1. Common parameters used by five scenarios

Parameter Name	Parameter Value
Terrain Size	Campus 10 km X 10 km
Simulation Time (s)	900 s
Trajectory Distance (m)	5.009 m
Trajectory Time (s)	900 s
Mobile Node (MN) Speed	20 km/h
MN Start Time (s)	uniform (0.1,1)
MN-ON State Time (s)	constant (900)
MN-OFF State Time (s)	constant (0)
MN Interarrival Time (s)	0.005
Stop Time (seconds)	Never (for MN node)
MN Packet Size (bytes)	uniform (100,2000)
MN Roaming Capability	Enabled
MN Transmit Power (w)	0.03
Buffer size(bits)	256000
BSS Identifier	MN→(1), ap1→ (1), ap2 →(2), ap3→ (3), ap4→ (4)
MN Physical Characteristics	HT PHY 2.4GHz (802.11n)/Extended Rate PHY (802.11g)
MN and APs Data Rate (bps)	• 6.5 Mbps (base)/ 60 Mbps (max) • 26 Mbps (base)/ 240 Mbps (max) • 65 Mbps (base)/ 600 Mbps (max) • 54 Mbps (for 802.11g scenario)



Figure 1. Trajectory of Mobile Node (MN) node drawn on the campus map

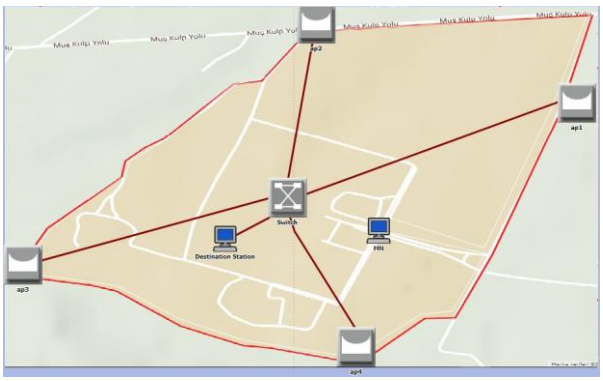


Figure 2. Wireless and wired network model for mobile security patrol

3. Result and Discussion

Wired and wireless system designs for the suggested campus security patrol were performed in 15 minutes and five different scenario simulations. Graphics obtained and analyzed at the end of the simulation are as follows: Figure 3 presents data load on the access point as a result of the roaming feature of the mobile node where the complete 802.11g standard of AP1 (BSS 1), AP2 (BSS 2), AP3 (BSS 3) and AP4 (BSS 4) was used. From the beginning, the first data for 6 minutes passed through AP1 (BSS 1). As mobile nodes progressed, data were transmitted to the destination station through AP1 (BSS1), AP2 (BSS 2), AP3 (BSS 3) and AP4 (BSS 4), respectively. The data collected from the access point were sent to the central station with about 2.6 Mbit /s.
The information was sent to the destination station by the wireless network access points presented in Figure 4. The highest data rate around 8.2 Mbits/s was submitted by 11n_65 Mbps scenario using physical characteristics of the 2.4GHz HT PHY (802.11n). Afterwards, the data transmission rate was realized in order as expected: 54 Mbps, 26 Mbps and 6.5 Mbps. On the other hand, transmission of data to the central station at low speed gave better results. In this case, as clearly presented in Figure 5, the best data transmission was provided by the 11n_6.5 Mbps scenario (around 2.6 Mbits/s).

One of the most important parameters of the wired and wireless networks is delay. Wireless LAN average delay values are given in Figure 6 with the results of the four different scenarios. The largest delay value was obtained starting from the 5th minutes by the 11n_26 Mbps scenario (average value of about 0.7 s). In the same graph, it can be seen that the average ideal values were obtained by the 11n_6.5 scenario. Figure 6 represents the end to end delay of all the data packets received by the wireless campus LAN MAC layers of all the wireless LAN devices in the suggested system.

Throughput of the wireless access devices in different scenarios are presented in Figure 7. The most interesting part of the throughput values are ranked from small to large. The best throughput values were achieved by 11n_6.5 Mbits scenario (about 2.6 Mbits/s). Contrary to expectations, the lowest throughput value was provided by the 11n_65 Mbits scenario. The movement of the two nodes in a scenario is analyzed in Figure 8. Given in the scenario, MN_2 nodes were sent 450 seconds after MN_1 node. This delay can be clearly seen in the graph. MN_2 nodes started to produce data after about the 7th minute. Because, in the relevant scenario for MN_2 nodes, starting Time (second) feature was set to 450 s. Figure 9 presents both the speed data received by the destination station of the mobile node and the collected data collected. Especially after the 5th minute, a lack of communication occurred due to the distance between the three different access points to the mobile node. In this case, the mobile node endeavored to transmit data at higher speeds. In the same chart, the average value of the data sent by the mobile node is shown with green linear lines. Figure 10 presents the Data dropped (Retry Threshold) (bits/sec). Time averages of the data dropped in the wireless network orders are as follows; 11n_65 Mbps, 11g Mbps, 11n_26 Mbps, and 11n_6.5 Mbps, respectively.

In the suggested security patrol model, the results of the analysis clearly show that wireless transmission devices arranged in lower speeds were more successful in contrary to the expectations. Because at high data rates, higher Bit Error Rate (BER) values are encountered. Higher BER values are causing packet loss. Further increases delay and reduces the data transfer rate (Babu and Rao 2011). When evaluated in the simulation results obtained with graphics, mobile patrol system for campus networks said to be in acceptable level in terms of performance.

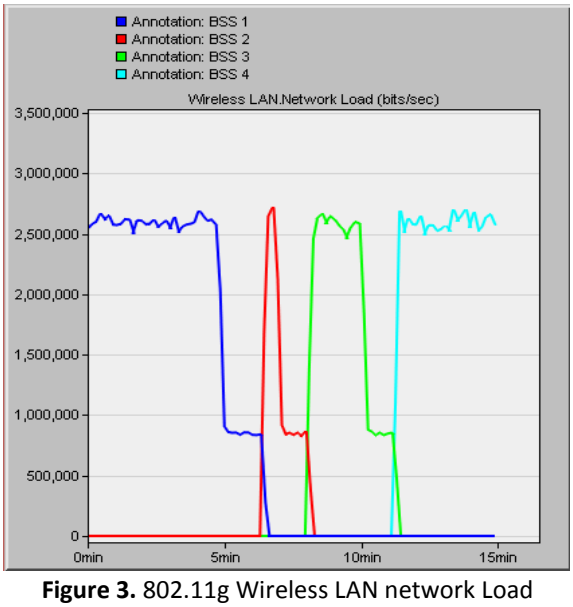


Figure 3. 802.11g Wireless LAN network Load

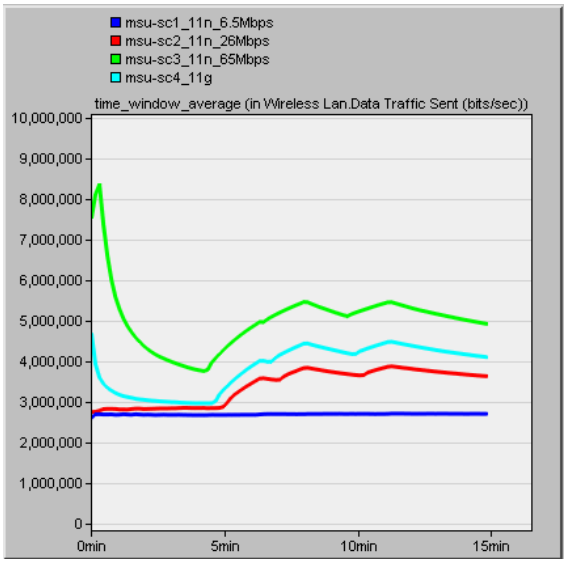


Figure 4. The Sent MN Data Traffic (bits/sec)

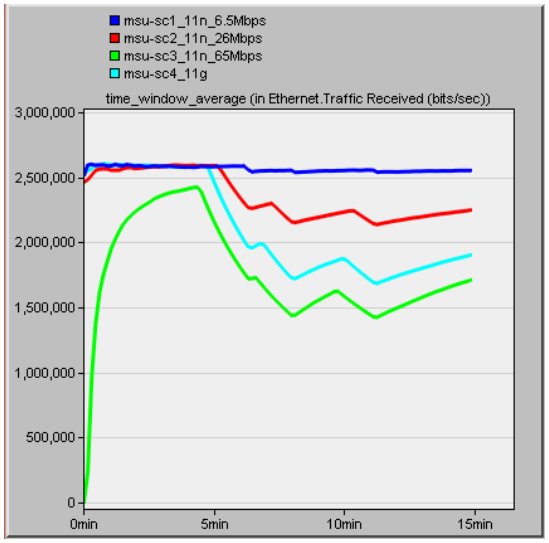


Figure 5. The received target station data traffic (bits/sec)

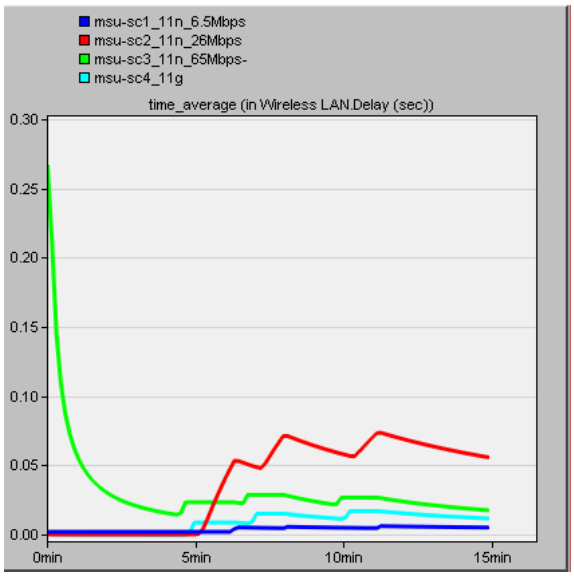


Figure 6. Wireless LAN Delay(sec)

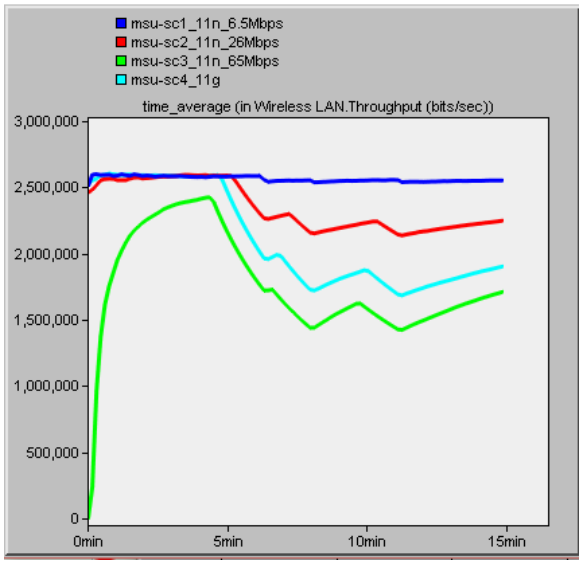


Figure 7. Wireless LAN Throughput (bits/sec)

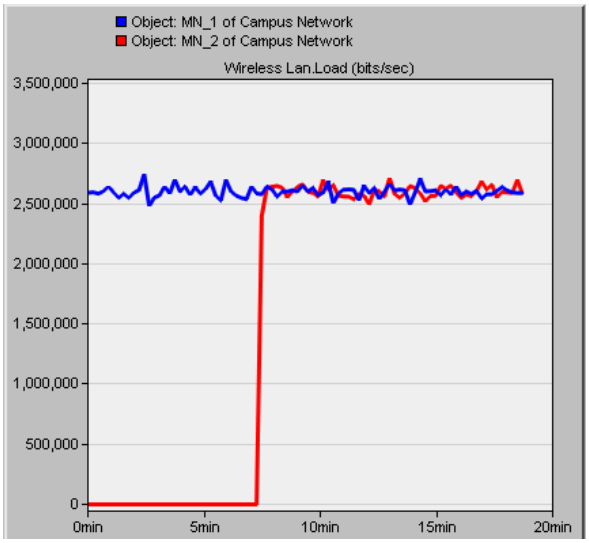


Figure 8. MN_1 and MN_2 Load (bits/sec)

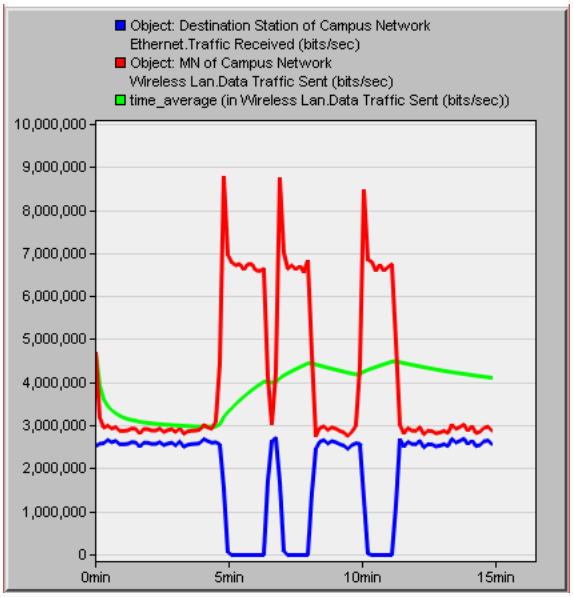


Figure 9. Data sent by MN to the Destination Station (bits/sec)

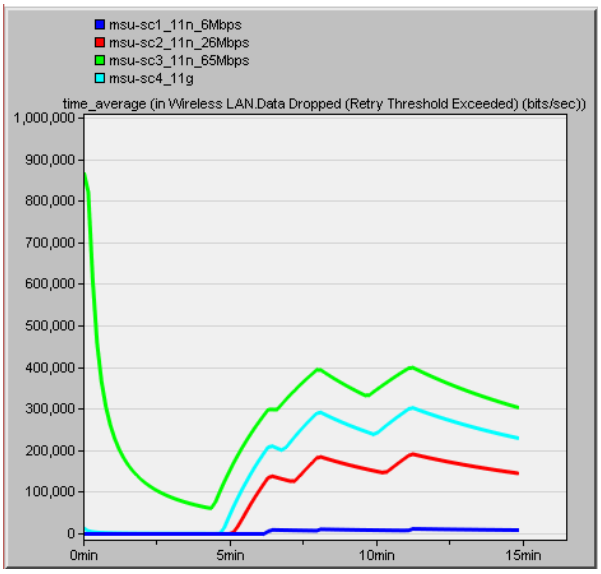


Figure 10. Wireless LAN Data Dropped (bits/sec)

4. Conclusions and Future Work

In this paper, we investigated the potential benefits of utilizing the wireless mobile data collection system which is a new concept of the mobile campus security patrol in the research of data collection system. We analyzed the wireless networks parameters; such as delay, throughput, network load, sent and received data traffic sent and data dropped to evaluate network performance in the wireless mobile networks through Riverbed Model Academic Edition 17.5 PL6 (OPNET) simulation scenarios. While the mobile node moved away from access points during data transmission, data transfer rates to the target station also decreased. In the security patrol model suggested in the present study, the obtained analysis results show that wireless transmission devices arranged in lower speed were more successful.

We conclude that the data, collected by mobile node in the wireless campus network via IEEE 802.11g and IEEE 802.11n standards, were successfully transmitted to the central station.

Further studies can be conducted on the effect of Quality of Service (QoS) in IP-based telephone in campus network via OPNET modeler.

References

Abdullah, I.S.A, Mustafa, A.B., 2016. The Impact of Distance on WLAN and LAN Network Performance, International Journal of Science and Research, **5(3)**, 1063-1065.

Alisa, Z.T., 2013. Evaluating the Performance of Wireless Network using OPNET Modeler, International Journal of Computer Applications, **62(13)**, 22-28.

Alsaif, KI., Saleh, IA., Alsaif, OI., 2014. Design and Analysis WLAN Nodes Performance Based on Roaming Technique, Journal of College of Education for Pure Science, **4**, 228-235.

Babu, AS., Rao, KVS.,2011. Evaluation of BER for AWGN, Rayleigh and Rician Fading Channels under Various Modulation Schemes, International Journal of Computer Applications, 26(9), 23-28.

Gupta, I., Kaur, A., 2010. Comparative Throughput of WiFi & Ethernet LANs using OPNET Modeller, IJCST, **1(2)**, 105-107.

Jasper, A., 2015. Comparison of Local Area Network Technologies: Ethernet (IEEE 802.3), ATM and WLAN/WiFi (IEEE 802.11g), International Journal of Current Engineering and Technology, **5(1)**, 503-506.

Jaswal, K., Jiyoti, Vats, K., 2014. Opnet Based Simulation and Investigation of Wimax Network Using Different QoS, IJRET: International Journal of Research in Engineering and Technology,3, 575-579.

Khan, T, A., Beg, MT., Khan, MA., 2013. Performance Analysis of WLAN Using OPNET, International Journal of Innovative Technology and Exploring Engineering, **2(5)**, 1-4.

Kumar, AS., Velmurugan, S., 2013. Integrating of WLAN / UMTS Network in Hot-Spot Locations Using OPNET, **2**, 1330-1336.

Leemis, L., Park, S., 2006. Discrete Event Simulation: A First Course, Pearson Prentice-Hall.

Lu, Z., Yang H., 2012. Unlocking the Power of OPNET Modeler, Cambridge University Press 2012.

Nehra, E., Singh, J., 2013. Practical Methodology for Expansion of Company's Intranet Using Opnet Modeler, International Journal of Electronics & Communication Technology, **4(3)**, 18-21.

Pal, N., Dhir, R., 2013. Analyze the Impact of Mobility on Performance of Routing Protocols in MANET Using OPNET Modeller, International Journal of Advanced Research in Computer Science and Software Engineering, **3(6)**,768-772.

Park, K., Willinger, W., 2000. Self-Similar Network Traffic and Performance Evaluation,Wiley-Interscience. John Wiley & Sons, Inc. New York, NY, USA.

Shklyaeva A., Novotny V., Abilov A. 2006. Roaming and Quality of Service in WLAN network. Proceedings of Research in Telecommunication Technology,Nove Mesto na Morave, Chech Republic, 2006, pp. 332-336.

Sukhroop, P., Singla, K., Singla, A., 2012. Simulate the Performance Parameters of Wired and Wireless Networks by Soft Computing Technique, International Journal of Engineering Research and Applications, **2(1)**, 25-35.

Tolani, M., Mishra, R., 2012. Effect of Increasing Load on WLAN Analyzed Through OPNET Simulator, International Journal of Computer Applications, **50**, 25-29.

Yi, S., Xu, P., Liu, H., 2013. Performance Analysis of Wireless Sensor Network Based on OPNET, Communications and Network, **5**, 512-516.

Zubairi, J.A., Zuber, M., 2000. SUNY Fredonia Campus Network Simulation and Performance Analysis Using OPNET, 1-3.