INFLUENCE WITH TRAFFIC RATE AND BEACON TIME FOR JAMMING ATTACK ON 802.11B IN MOBILE AD HOC NETWORKS

Jammana Lalu Prasad,
Department of Computer Science & Engineering,
Centurion University, Vizianagaram, AP, INDIA

Kavitha Chekuri
Department of Computer Science & Engineeing.
Raghu Engineering College (A),Vishakapatnam,AP,INDIA

Lakshmana Rao Rowthu
Department of Computer Science & Engineering
Centurion University, Vizianagaram, AP.

Abstract— **MANETs have distinctive characteristics like dynamic topology, wireless radio medium, restricted resources and lack of centralized administration; as a result, they're liable to differing types of attacks in several layers of protocol stack. Every node in a Manet is capable of acting as a router. The need for a secure Manet networks is powerfully tied to the protection and privacy options. This Jamming attacks are one in every of them. These occur by transmittal continuous radio ways in which to inhibit the transmission among sender and receiver. These attacks have an effect on the network by decreasing the network performance with buffer size, beacon amount varied as certained result on mobile ad-hoc network degrade the performance with Jamming attack. This work includes a network with high Mobility IEEE 802.11b with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. FTP with high rate is being generated within the network. For the Simulation purpose we tend to utilized OPNET (Optimized Network Engineering Tool) MODELER 14.5 is employed for simulation. The performance of network is measured with relation to the QoS parameters.**

Keywords— **MANET, SANET, AODV, JAMMING, OPNET, OLSR, MODELER, WLAN, Route Discovery Time, Packet Drop.**

I. INTRODUCTION

Ad-Hoc networks don't have any infrastructure wherever the nodes are liberal to be part of and left the network. The nodes are connected with one another through a wireless link. A node will function a router to forward the info to they don't have any centralized administration. Ad-Hoc networks have The capabilities to handle any haywire within the nodes or any changes that its expertise because of topology changes.

Whenever a node within the network is down or leaves the network that causes the link between alternative nodes is broken. The affected nodes within the network merely request for brand spanking new routes and new links are established Ad-Hoc network are often categorized in to static Ad-Hoc network (SANET) and Mobile Ad-Hoc network (MANET).

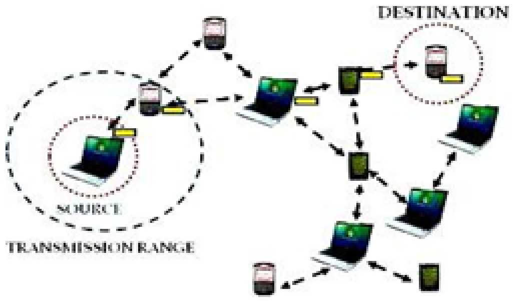


Figure1. Mobile Ad hoc Network

In our analysis work we have a tendency to be up the performance of mobile unintentional networks underneath Jamming attack by mistreatment associate degree integrated approach. The planned work includes a network with high Mobility, using IEEE along g standard with improved AODV (Ad hoc On Demand Distance Vector) routing protocol parameters. FTP and Video conferencing with high rate are being generated within the network.

JAMMING ATTACK

Jamming attack deliberately transmits of radio signals to disrupt the full communications by decreasing the signal- to-noise quantitative relation. The term Jamming is employed to differentiate it from unintentional jamming that known as as interference. In Manet jamming may be a serious threat to its security. Jammers perpetually send.

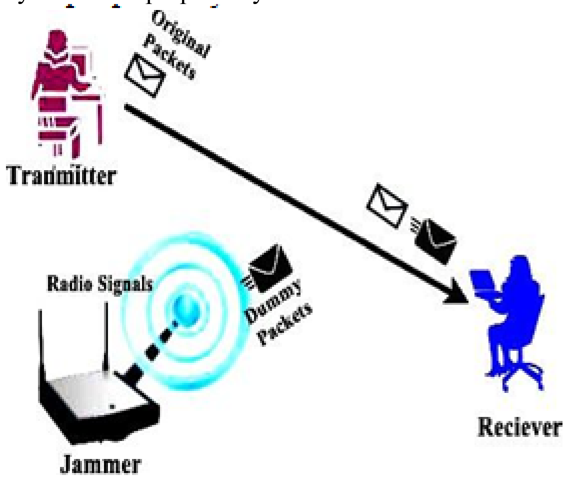


FIGURE 2: JAMMING ATTACK

II .LITERATURE REVIEW

Sisi Liu et al. (2012) addresses the matter of mitigating DoS attacks manifested within the sort of jam. The author thought of a complicated antagonist World Health Organization has data of the protocol specifics and of the science quantities won't to secure network operations. This kind of antagonist can't be prevented by opposing jam techniques that bank unfold spectrum. The author projected a brand new security metrics to quantify the flexibility of the antagonist to deny access to the management channel, and introduced a randomized distributed theme that enables nodes to ascertain and maintain the management channel within the presence of the transmitter. The projected technique is applicable to networks with static or dynamically allotted spectrum.

Moreover, 2 algorithms for distinctive identification of the set of compromised nodes were projected, one for severally acting nodes and one for colluding nodes[19].Dorus.R et al. (2013) proposes a mechanism for preventing jam attacks on wireless networks, examine the detection potency of jam attack and communication overhead of the wireless network exploitation proactive and reactive protocols. RSA formula is employed and analyzed for providing knowledge packets integrity data throughout wireless transmission. Through simulation and performance analysis, the enforced bar mechanism and also the integrity preservation provides higher packet delivery magnitude relation in proactive routing protocol (OLSR) than reactive routing protocol (AODV). Nadeem Sufyan et al. (2013) investigate a multi- modal theme that models totally different jam attacks by discovering the correlation between 3 parameters: packet delivery magnitude relation, signal strength variation, and pulse dimension of the received signal.

III . METHODOLOGY

A. Simulation Tool used:

This section describes the simulation tool used along with the proposed method. OPNET modeller v14.5 is extensive and a very powerful simulation tool with wide variety of possibilities. The entire heterogeneous networks with various routing protocols can be simulated using OPNET. High level of user interface is use in OPNET which is constructed from C and C++ source code blocks.

B. Simulation Setup:

The simulation work focuses on analyzing the performance of Manet below with and without jamming attack. So AN Integrated approach is employed to investigate the network performance below jam attack. This approach includes:

- High **rate** of 54mbps by **victimisation** IEEE 802.11b **normal.**
- Network with high **quality**
- Improved parameter of AODV routing protocol.
- Generation of high resolution FTP traffic.

C. Buffer management Methodology:

As long because the requests hit terribly slow rate the nodes might service the requests. Since the arrivals are freelance of every alternative, all the nodes might request for the service at an equivalent time, a condition of congestion might develop and node might not be ready to service all request. To beat this case it's urged to use buffer to keep up a queue for such unfinished requests and to avoid packet drops.

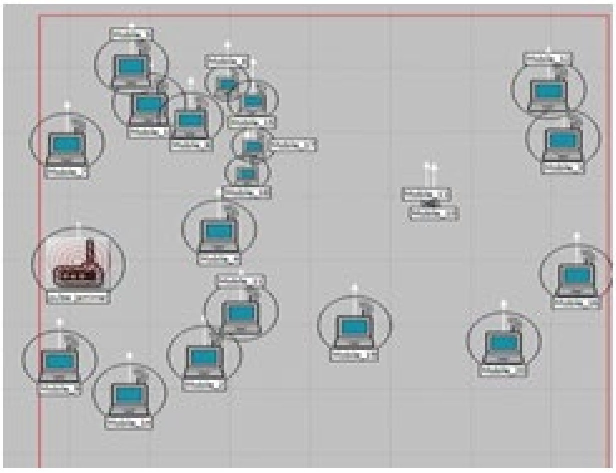


FIGURE 3: with JAMMING ATTACK

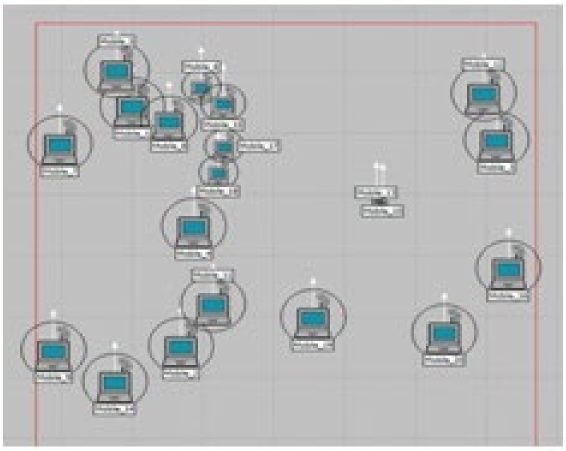
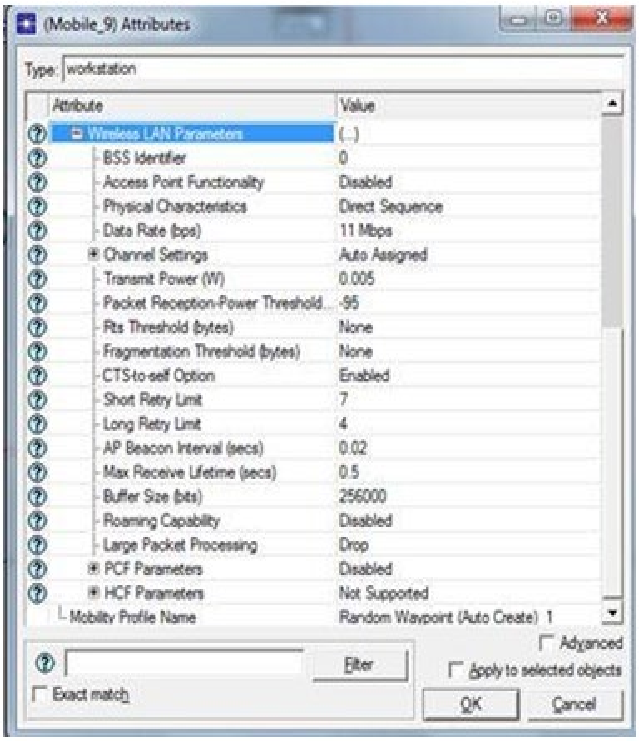


FIGURE 4: without JAMMING ATTACK



(Mobile_9) Attributes

Type: workstation

Attribute	Value
⊟ Wireless LAN Parameters	(...)
BSS Identifier	0
Access Point Functionality	Disabled
Physical Characteristics	Direct Sequence
Data Rate (bps)	11 Mbps
⊞ Channel Settings	Auto Assigned
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop
⊞ PCF Parameters	Disabled
⊞ HCF Parameters	Not Supported
Mobility Profile Name	Random Waypoint (Auto Create) 1

FIGURE 5: Parameter setting for Traffic and Beacon time

Retransmission: Represents the full variety of bits (in bits/sec) forwarded from wireless local area network layers to higher layers altogether Wi-Fi nodes of the network. Retransmission is high for with transmitters once compare with while not jammer for changed Beacon amount. Default Beacon amount is nice in Medium network as seen in Figure 6.

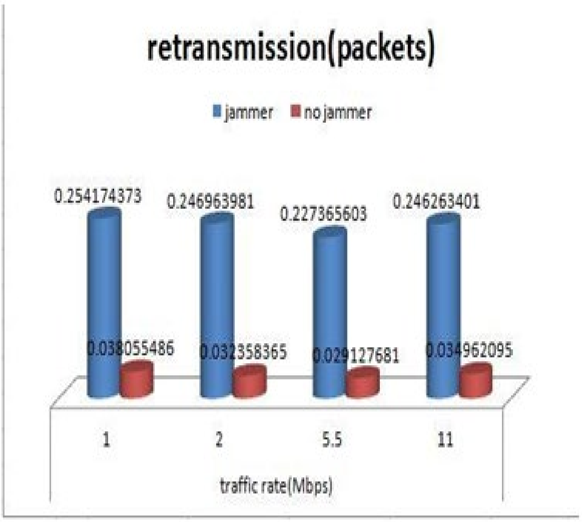


Figure 6: Variation of retransmission with Traffic Rate.

Throughput (bits/sec): Represents the entire variety of bits (in bits/sec) forwarded from wireless local area network layers to higher layers all told WLAN nodes of the network. Throughput is high for with transmitters once compare with while not jammer for changed Beacon amount. Default Beacon amount is sweet in Medium network as seen in Figure 7

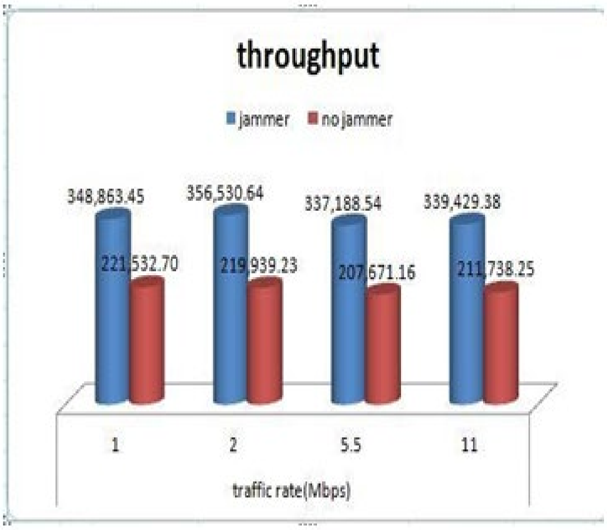


FIGURE 7: Variation of Throughput with Traffic Rate.

Delay (sec): Represents the full range of bits (in bits/sec) forwarded from wireless local area network layers to higher layers altogether wireless fidelity nodes of the network. Delay is high for with senders once compare with while not jammer for changed Beacon amount. Default Beacon amount is nice in Medium network as seen in Figure 8.

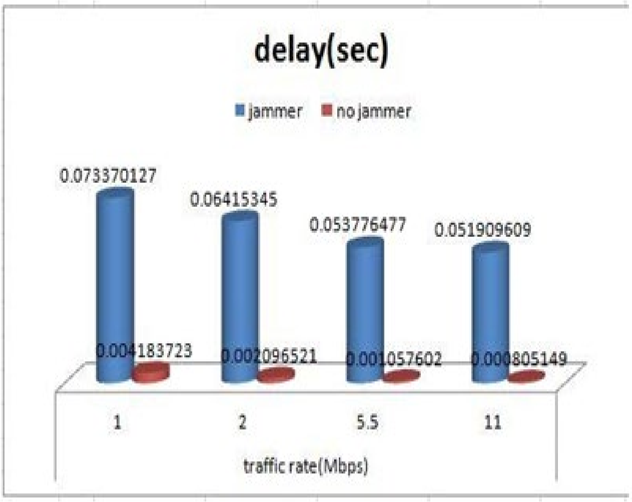


FIGURE 8: Variation of Delay with Traffic Rate.

Route Discovery Time (sec): Represents the overall variety of bits (in bits/sec) forwarded from wireless LAN layers to higher layers altogether Wi-Fi nodes of the network. Route Discovery Time is high for with senders once compare with while not jammer for changed Beacon amount. Default Beacon amount is sweet in Medium network as seen in Figure 9.

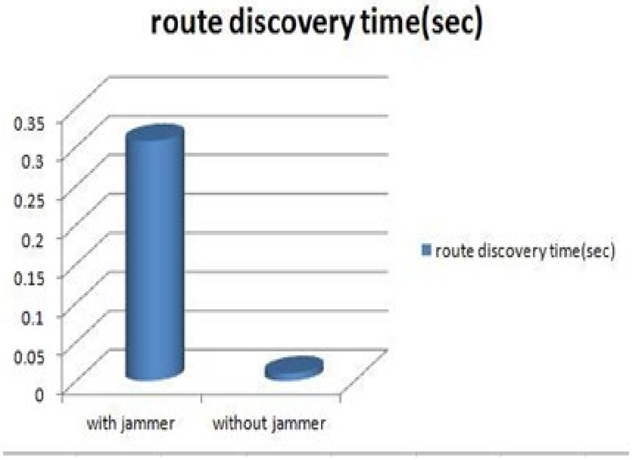


Figure 9: Variation on of route discovery time with Simulation Time

Packet Drop: Represents the entire variety of bits (in bits/sec) forwarded from wireless computer network layers to higher layers altogether Wi-Fi nodes of the network. Packet Drop is high for with transmitters once compare with while not jammer for changed Beacon amount. Default Beacon amount is sweet in Medium network as seen in Figure 10.

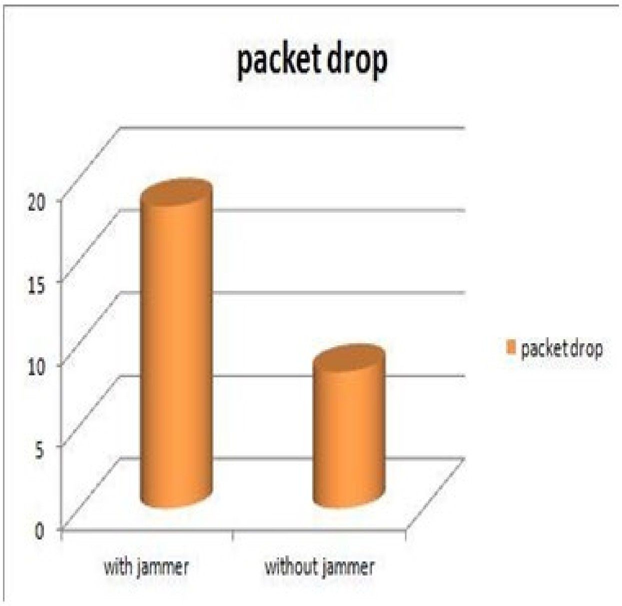


Figure 10: Variation of Packet Drop with Simulation Time.

Total route error send: Represents the whole variety of bits (in bits/sec) forwarded from wireless local area network layers to higher layers all told WLAN nodes of the network. Total route error send is high for with senders once compare with while not jammer for changed Beacon amount. Default Beacon amount is nice in Medium network as seen in Figure 11.

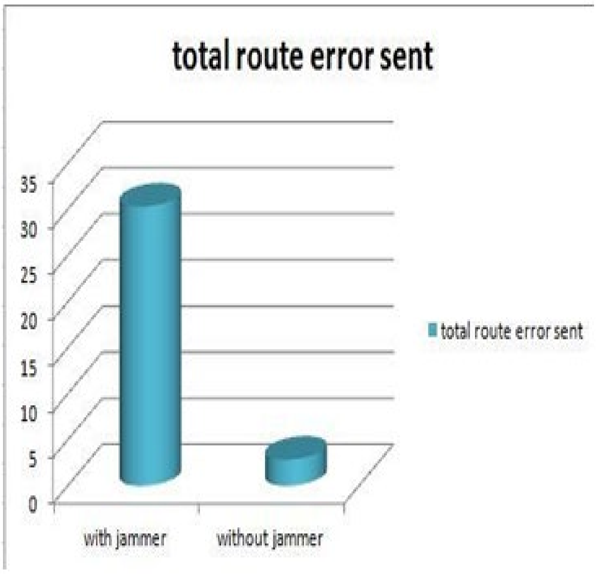


Figure 11: Variation of Total route error sent with Simulation Time

IV.CONCLUSION

Because of the wireless nature of mobile ad-hoc networks, numerous attacks are performed degrade the network performance. Jamming attack is one in every of them thus routing protocols are accustomed increase the network turnout. During this analysis work, Impact of jam Attack in Performance of Mobile improvement Networks.

Jammers attacks can have an impression on network's performance as a result of the jammers interferes with the normal operation of the network. The result of attackers studied during this paper was by increasing delay, knowledge born traffic received and sent and decreasing packer drop quantitative relation of the network. During this analysis work, the network performance beneath jam attack is analyzing by applying integrated approach. This approach includes a network with high quality, IEEE 802.11g customary with Georgia home boy rate; serious traffic like FTP improved AODV parameters and inflated buffer size. In our paper, it absolutely was shown that jam attack reduces the network turnout, retransmission tries and will increase the media access delay.

V. REFERENCE

[1] Fatima Ameza, Nassima Assam and Rachid Beghdad, "Defending AODV Routing Protocol Against the Black Hole Attack", International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112- 117.

[2] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[3] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[4] Hoang Lan Nguyen and Uyen Trang Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149

[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

[6] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.

[7] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.

[8] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, "New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks", 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

[9] Dang Quan Nguyen and Louise Lamont, "A Simple and Efficient Detection of Wormhole Attacks", New Technologies, Mobility and Security, November 2008, pp. 1-5.

[10] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, "Analysis of Wormhole Intrusion Attacks in MANETs", Military Communications Conference, November 2008, pp.1-7.

[11] Gianni A. Di Caro, Frederick Ducatelle, Luca M. Gambardella. "A simulation study of routing performance in realistic urban scenarios for MANETs". In: Proceedings of ANTS 2008, 6th International Workshop on Ant Algorithms and Swarm Intelligence, Brussels, Springer, LNCS 5217, 2008.

[12] Ebrahim Mohamad, Louis Dargin. "Routing Protocols Security." In: Ad Hoc Networks". A Thesis at Oakland University School of Computer Science and Engineering.

[13] Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method." In: International Journal of Network Security, Vol. 5, No.3, pp.338–346, Nov. 2007.

[14] Hao Yang, Haiyun Luo. Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: Challenges and solutions". IEEE Wireless Communications, February 2004.

[15] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kat, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, P.P 338-346, Nov. 2007.

[16] C. E. Perkins, S.R. Das, and E. Royer, "Ad-hoc on Demand Distance Vector (AODV)". March 2000, http://www.ietf.org/internal-drafts/draft-ietf-manet-aodv05.txt.

[17] Ioanna Stamouli, "Real-time Intrusion Detection for Ad hoc Networks" Master's thesis, University of Dublin, September 2003.

[18] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.

[19] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A

Secure On-Demand Routing Protocol for Ad hoc Networks," Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia, September 2002, pp. 12- 23.

[20] Dokurer, Semih."Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, AtılımUniversity, September 2006.