International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-10)

Research Article | **October 2015**

Survey on Detection Mechanism for the Detection of Jamming Attacks under Different Protocols in MANETs

Prof. Shubhangi Sonone
Asst. Prof. D.Y. Patil College of Engg,
Pune, Maharashtra, India

Abstract—

Several studies in the literature have been addressed by the researchers to solve security dilemmas of Mobile Ad-Hoc Networks (MANET). Due to the wireless nature of the channel and specific characteristics of MANETs, the radio interference attacks cannot be mitigated through conventional security mechanisms. These attacks cause a significant degradation on overall network throughput, packet transmission rates and delay on the MAC layer since other nodes step back from the communication. A malicious node can continually transmit a radio signal in order to block any type of legitimate access to the medium and/or infer with reception. This phenomenon is called as jamming and the malicious nodes are termed to as jammers. MANET routing protocols could improve system performance by increasing throughput and data dropped. To minimize the impact of the disruption, it is important to identify its presence. So, in this paper, a meliorated detection mechanism has been proposed in order to detect the physical jamming attacks in Ad Hoc On Demand (AODV) Routing protocol and Dynamic source routing (DSR) protocol thereby increasing the throughput and decrease the delay. The results of the proposed technique are compared under both these protocols with respect to throughput and delay.

Keywords— AODV, defense, delay, DSR, jamming attack.

I. INTRODUCTION

Wireless networks enjoy widespread commercial implementation because of their low cost, ease of use and setup. However, since accessing wireless media is much easier than tapping a wired network, security becomes a serious issue when implementing any wireless network. There are two classifications of Mobile networks: Infrastructure networks and Mobile Ad Hoc Networks (MANET) according to their dependence on fixed infrastructures. In a Mobile Ad Hoc Network, the network may experience rapid and unpredictable topology changes because of the presence of the mobile nodes. Every node in MANET has the responsibility to act as a router and routing paths in MANETs. Due to the wireless nature of the channel and specific characteristics of MANETs, these are easily exploited bye various attacks. A malicious node can continually transmit a radio signal in order to block any type of legitimate access to the medium and/or infer with reception. This phenomenon is called as jamming and the malicious nodes are termed to as jammers. The jamming is categorized as: Physical and Virtual Jamming attacks [10].

The physical jamming is launched by continuous transmissions and/or by ensuring packet collisions at the receiver. Physical or Radio jamming in a wireless medium is a simple but the most disruptive form of DoS attack [5]. The jammers leading to these attacks can deny complete access to the channel by monopolizing the wireless medium. The nodes trying hard to communicate have an unusually large carrier sensing time waiting for the channel to become idle [15].

Virtual Jamming Attacks can be launched at the MAC layer through attacking on the RTS/CTS (Rate to Send/Clear to Send) frames or DATA frames. An advantage of MAC layer jamming is that the attacker node consumes less power in targeting these attacks as compared to the physical radio jamming. Here, we focus on the jamming attacks at the MAC layer resulting in collision of RTS/CTS control frames or the DATA frames. In virtual jamming attack malicious node send RTS packets continuously on the transmission with unlimited period of time. During this entire process, the malicious node effectively jam the transmission with a large amount of transmission on the wireless channel with small expenditure of power [2]. Jamming attack can easily be deployed in wireless network resulting in the degradation of network's throughput and performance. MANET routing protocols could improve system performance by increasing throughput and data dropped. Previous techniques exist, to prevent and mitigate the jamming attacks thereby improving the throughput and resulting in the increased overall performance, but they result in increased network delay. So, the objective of the paper is to propose an efficient approach with least possible delay and increased throughput for the detection of the physical jamming attack in AODV and DSR protocol. The metrics of performance with the proposed approach are Throughput and Delay.

II. LITERATURE REVIEW

Wenyuan Xu et al. (2005) gives a detailed description of the radio interference attacks and diagnosing the critical issue of the presence of the jamming attack. Four different jamming attack models were proposed that can be used by an adversary to disable the operation of a wireless network, and evaluated their effectiveness in terms of how each method affects the ability of a wireless node to send and receive packets to and from the destination. The author also discussed

different measurements that serve as the basis for detecting a jamming attack, and explored different scenarios where each measurement is not enough to reliably classify the presence of a jamming attack. The author observed that signal strength and carrier sensing time are unable to conclusively detect the presence of a jammer. Further, the author observed that although by using packet delivery ratio he may differentiate between congested and jammed scenarios, he was unable to conclude whether poor link utility was due to jamming or the mobility of nodes. To address the need of detecting the presence of jammer, the author proposed two enhanced detection protocols that employ consistency checking. The first scheme employed signal strength measurements as a reactive consistency check for poor packet delivery ratios, while the second scheme employed location information to serve as the consistency check[1]. Mario Strasser et al. (2008) considers the problem of how can two devices that do not share any secrets establish a shared secret key over a wireless radio channel in the presence of a communication jammer. An inherent challenge in solving this problem was that known anti-jamming techniques (e.g., frequency hopping or direct-sequence spread spectrum) which should support device communication during the key establishment required that the devices shared a secret spreading key (or code) prior to the start of their communication. This requirement created a circular dependency between anti jamming spread-spectrum communication and key establishment. The author proposed an Uncoordinated Frequency Hopping (UFH) scheme that breaks the dependency and enables key establishment in the presence of a communication jammer. The author performed a detailed analysis of UFH scheme and showed its feasibility, both in terms of execution time and resource requirements[6]. Ali Hamieh et al. (2009) describes that the military tactical and other security sensitive operations are still the main applications of ad hoc networks. One main challenge in design of these networks is their vulnerability to Denial-of-Service (DoS) attacks. In this paper, the author considers a particular class of DoS attacks called Jamming. A new method of detection of such attack by the measurement of error distribution was proposed. To differentiate the jamming scenario from legitimate scenarios, the author measured the dependence among the periods of error and correct reception times. In order to measure this dependency, auhtor used the Correlation Coefficient which is a statistic measure of relation between two random variables[16]. Zhuo Lu Wenye Wang et al. (2011) aims at modeling and detecting jamming attacks against time-critical traffic. The author introduced a new metric, message invalidation ratio, to quantify the performance of time-critical applications. The author claims that the behavior of a jammer who attempts to disrupt the delivery of a time-critical message can be exactly mapped to the behavior of a gambler who tends to win a gambling game. The author showed via gambling-based modeling and real-time experiments that there exists a phase transition phenomenon for a time-critical application under jamming attacks. As the probability that a packet is jammed increases from 0 to 1, the message invalidation ratio first increases slightly (even negligibly), then increases dramatically to1. Based on analytical and experimental results, the author further designed and implemented the JADE (Jamming Attack Detection based on Estimation) system to achieve efficient and robust jamming detection for time-critical wireless networks[26]. Sisi Liu et al. (2012) addresses the problem of preventing control-channel DoS attacks manifested in the form of jamming. The author considered a sophisticated adversary who has knowledge of the protocol specifics and of the cryptographic quantities used to secure network operations. This type of adversary cannot be prevented by anti-jamming techniques that rely spread spectrum. The author proposed a new security metrics to quantify the ability of the adversary to deny access to the control channel, and introduced a randomized distributed scheme that allows nodes to establish and maintain the control channel in the presence of the jammer. The proposed method is applicable to networks with static or dynamically allocated spectrum. Furthermore, two algorithms for unique identification of the set of compromised nodes were proposed, one for independently acting nodes and one for colluding nodes[19]. Dorus.R et al. (2013) proposes a mechanism for preventing jamming attacks on wireless networks, examine the detection efficiency of jamming attack and communication overhead of the wireless network using proactive and reactive protocols. RSA algorithm is used and analyzed for providing data packets integrity information during wireless transmission. Through simulation and performance analysis, the implemented prevention mechanism and the integrity preservation provides higher packet delivery ratio in proactive routing protocol (OLSR) than reactive routing protocol (AODV)[8][25]. Nadeem Sufyan et al. (2013) investigates a multi-modal scheme that models different jamming attacks by discovering the correlation between three parameters: packet delivery ratio, signal strength variation, and pulse width of the received signal. Based on that, profiles were generated in normal scenarios during training sessions which were then compared with test sessions to detect and classify jamming attacks. The proposed model helps in clearly differentiating the jammed regions for various types of jamming attacks. In addition, it is equally effective for both the protocol-aware and protocol-unaware jammers [3] [24].

III. SYSTEM MODEL

The paper consists of three simulation scenarios:

- Simple scenario with 50 mobile nodes deployed randomly.
- Attack scenario with two jammer nodes.
- Scenario simulated with the proposed technique.

1. Description of the First Scenario

This scenario consists of 50 mobile nodes deployed randomly in the area of 1000 x 1000 m. Nodes move in this area on the basis of random waypoint mobility model with a constant speed of 10 m/s. With the help of this algorithm, random trajectories of the mobile nodes have been set. The ad-hoc routing protocol is changed accordingly as per the requirements of the simulation study in order to analyze the results under a particular protocol i.e. AODV or DSR. Here,

the start time is taken as 10 seconds and the stop time is set to the end of the simulation. The packet inter-arrival time and the packet size is set to 0.03 seconds (exponential) and 2000 (exponential).

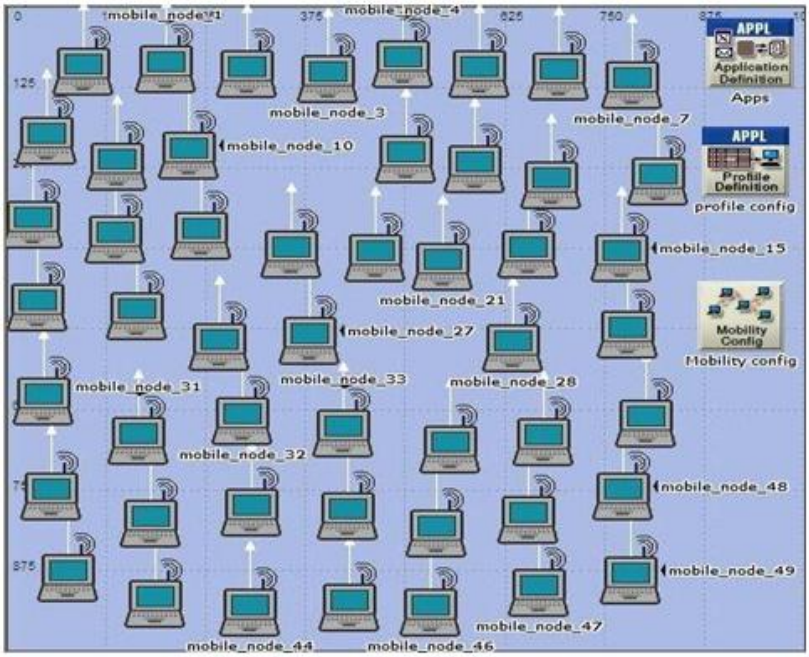

Figure1. Scenario without attack

The scenarios are simulated and analyzed on the basis of two parameters- Throughput and Delay.

- Throughput- Represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to the higher layers in all WLAN nodes of the network.
- Delay- Represents the end to end delay of all the packets received by the wireless LAN Macs of all the WLAN nodes in the network and forwarded to the higher layers.

The simulation was performed for 300 seconds while the number of seeds used were 300 in order to provide 1 hour simulation performance.

Table 1: Parameters for the First Scenario.

Parameters involved	**Value used**
No. Of mobile nodes	50
Area of the network	1000 x 1000
Mobility speed of the mobile nodes	10 (m/s)
Trajectory of the mobile nodes	VECTOR
Ad-hoc routing protocol	AODV/DSR
Start time	10 seconds
Stop time	End of the simulation
Packet inter-arrival time	0.03 seconds (exponential)
Packet size	2000 (exponential)
Simulation time	300 seconds
No. of Seeds	300
Simulation kernel	Optimized

2. Description of the Attack Scenario

Here, we have placed two jammer nodes in order to engage the physical jamming attack in the network. The physical jamming is launched by continuous transmissions and/or by ensuring packet collisions at the receiver. The jammers leading to these attacks can deny complete access to the channel by monopolizing the wireless medium. The nodes trying hard to communicate have an unusually large carrier sensing time waiting for the channel to become idle [5][15]. The jammer used here is mobile pulse jammer. Jammers also need to be configured according to the network's requirements.

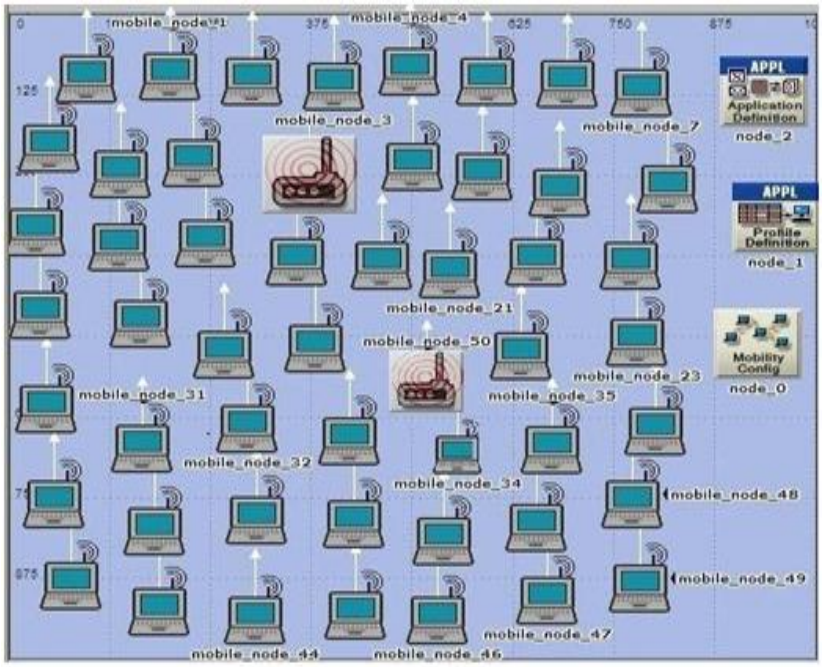

Figure2. Attack Scenario.

Here, the trajectory of the jammer nodes is set to VECTOR. The jammer bandwidth is set to 100000 and the jammer base band frequency is taken as 2402. The pulse width is taken as 2.0. The start time and the stop time is set to 10 seconds and end of the simulation respectively.

TABLE2: JAMMER CHARACTERSTICS.

Parameters involved	**Value used**
Model of the jammer node	Mobile pulse jammer
Trajectory	VECTOR
Jammer bandwidth	100000
Jammer base band frequency	2402
Pulse width	2.0
Start time	10 seconds
Stop time	End of the simulation

3. Description of the Third Scenario

In order to implement the proposed technique for the detection of the physical jamming attack, following detection technique is proposed.

3.1 Proposed Technique

In order to enhance the throughput of the entire network, the presence of the jammer node is very necessary to be stated. Various techniques were opted for the discovery, prevention and mitigation of the jamming attack. In order to enhance the throughput and decrease the delay as compare to the existing approaches, a meliorated detection mechanism is proposed in this dissertation, for the detection of the physical jamming attack.

1. In case, if packet size exceeded to a particular RTS threshold, that packet would have to wait for a particular RTS/CTS interval in order to completely forward that packet to its destination. So, the buffer size is taken as 102400000.
2. Also, high data rate of 54 mbps is taken which was previously 11 mbps during the simple and the attack scenario.
3. The value of the physical characteristics is set to Extended Rate PHY.
   So, apart from performing the modifications in the data rate and buffer size for the prevention of penalties caused by the drawbacks of the existing techniques and in order to improvise the throughput, improved AODV parameters are also adopted. Here, the active route timeout is taken as 30 seconds.

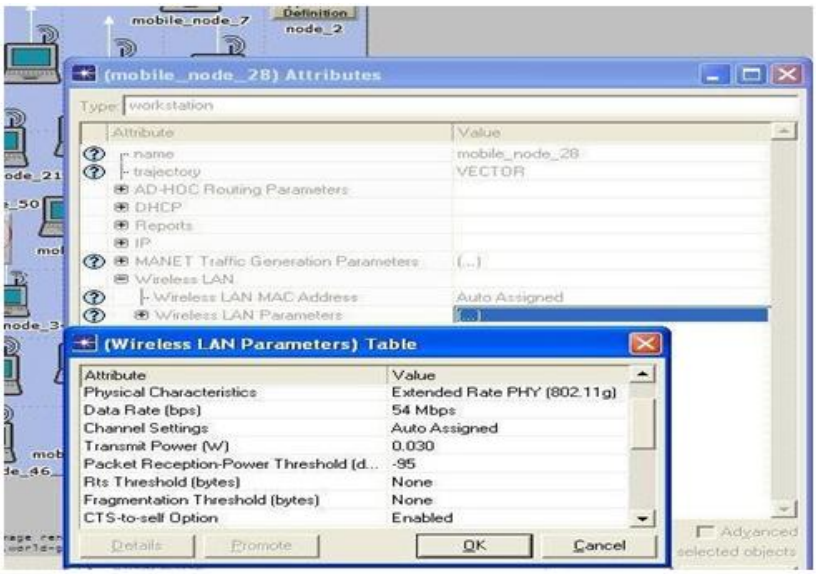

Figure 3: Scenario with the proposed scheme.

IV. PERFORMANCE RESULTS

4.1 Analysis of jamming attack under DSR protocol:

In the scenario with attack, the throughput decreased from the previous scenario. This clearly identifies the presence of the jamming attack. The graphs analysis clearly verifies the discussion.

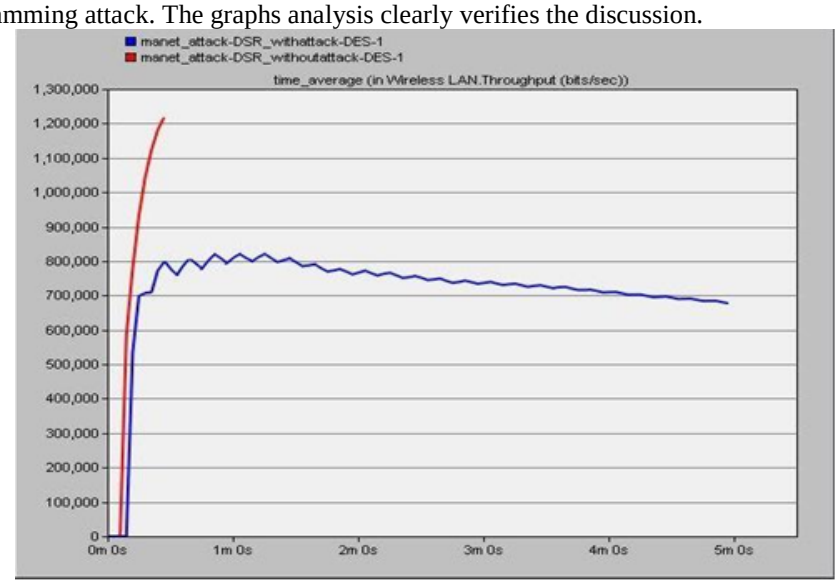

Figure 4. Throughput of the network under DSR protocol

Figure5. Delay of the network under DSR protocol

4.2 Analysis of jamming attack under DSR protocol when the proposed technique was applied:

After the proposed technique was applied under DSR protocol attack scenario, the throughput of the network increased to a promising value and the delay was decreased, but not much. This analysis is clearly visible in the graphs.

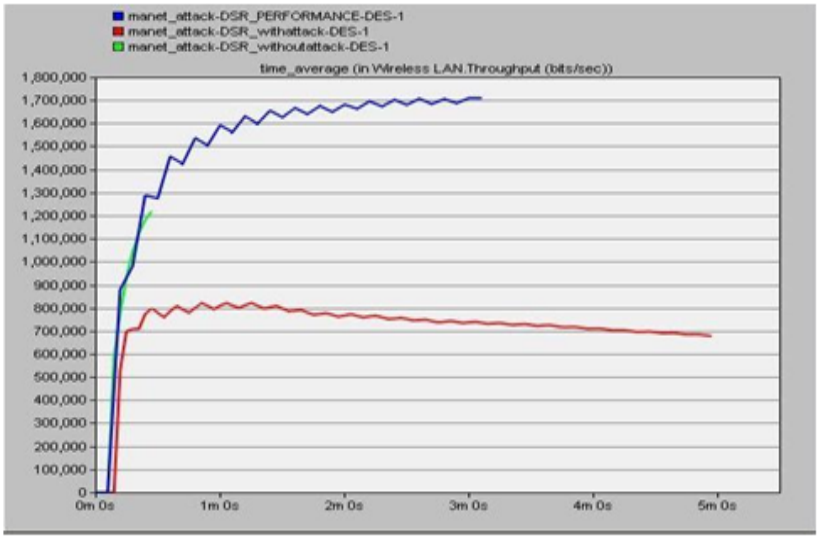

Figure 6. Throughput of proposed approach under DSR protocol

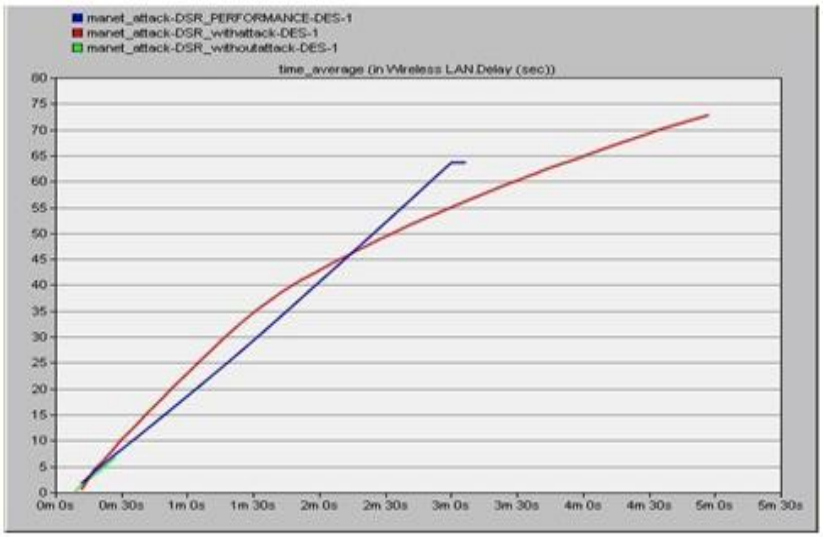

Figure 7. Delay of proposed approach under DSR protocol

4.3 Analysis of jamming attack under AODV protocol:

When the attack nodes were engaged into the network of the mobile nodes under AODV protocol, the throughput of the network decreased, thereby depicting the presence of the physical jamming attack.

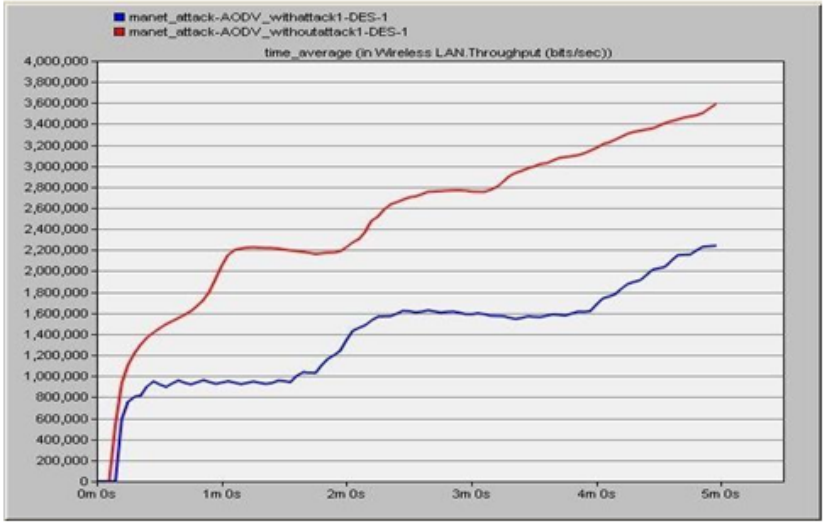

Figure8. Detection of physical jamming attack under AODV on the basis of throughput

Similarly, When the attack was found in the network, the delay of the network increased.

Figure9. Detection of physical jamming attack under AODV on the basis of delay

4.4 Analysis of jamming attack under AODV protocol when the proposed technique was applied:

When the proposed mechanism was applied to the network of the mobile nodes in which the attack was found, the throughput of the network first increased gradually and then reached to a promising level. On the other hand, the delay of the network decreased which can be seen in figures 10 and 11.

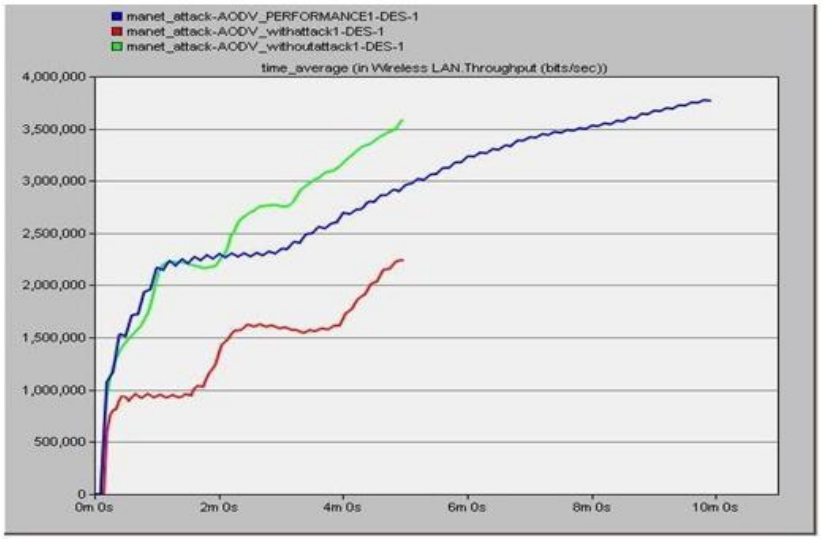

Figure10. Throughput of the network under AODV with the proposed approach

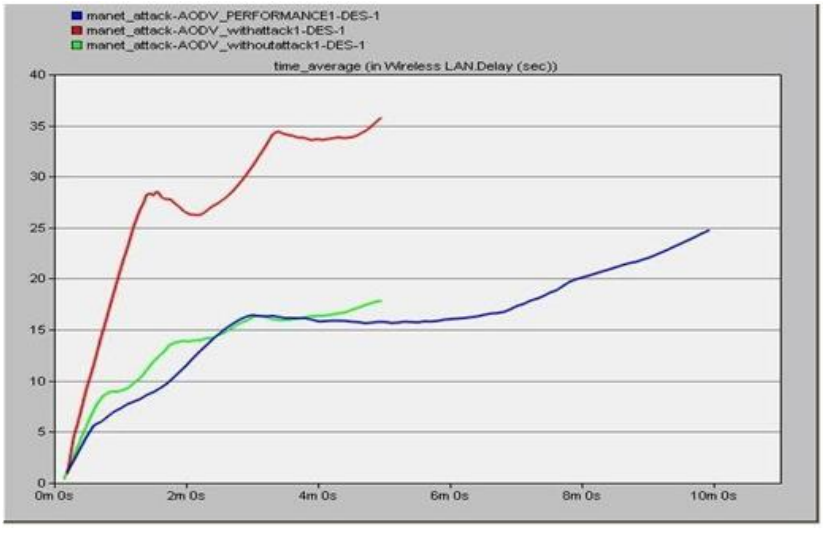

Figure11. Delay of the network with the proposed approach under AODV protocol

4.5 Comparison of the results obtained from the proposed technique under AODV and DSR protocol:

The AODV and DSR protocols are compared in this section on the basis of throughput and delay in order to detect the physical jamming attack. Following graphs show that AODV protocol gives better results than DSR protocol under the simple, attack and proposed scheme scenarios on the basis of throughput and delay. Figure12 shows that AODV protocol performs better than DSR protocol in terms of throughput when no attack was engaged in the network.

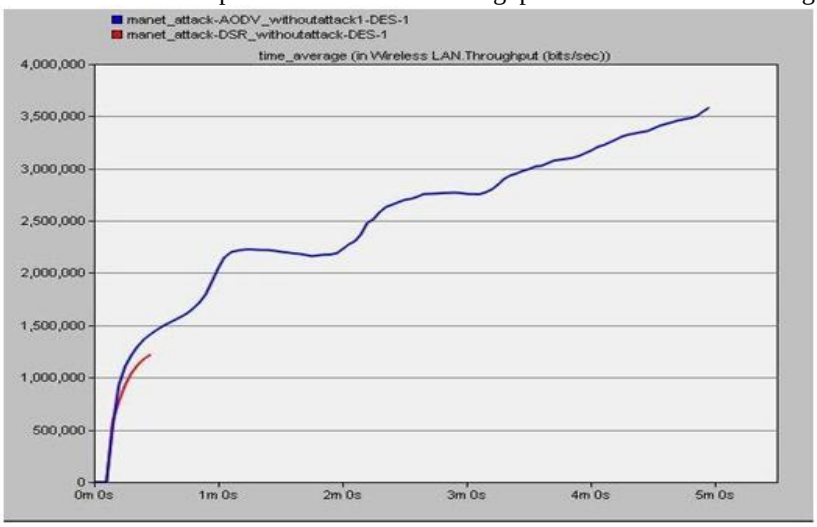

Figure12 Throughput of the network under AODV and DSR protocol

Figure13. shows that DSR protocol has lesser delay, when no attack was engaged in the network.

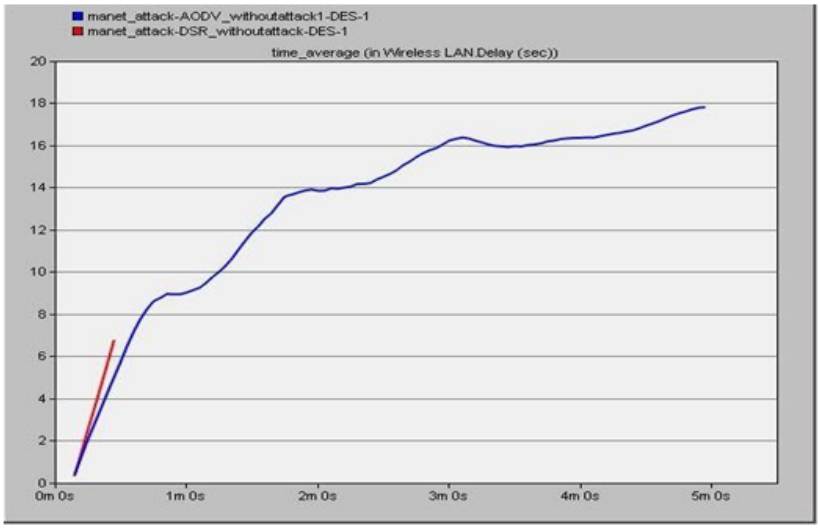

Figure13. Delay of the network under AODV and DSR protocol

However, when the attack was engaged into the network, AODV protocol came out to be the best.

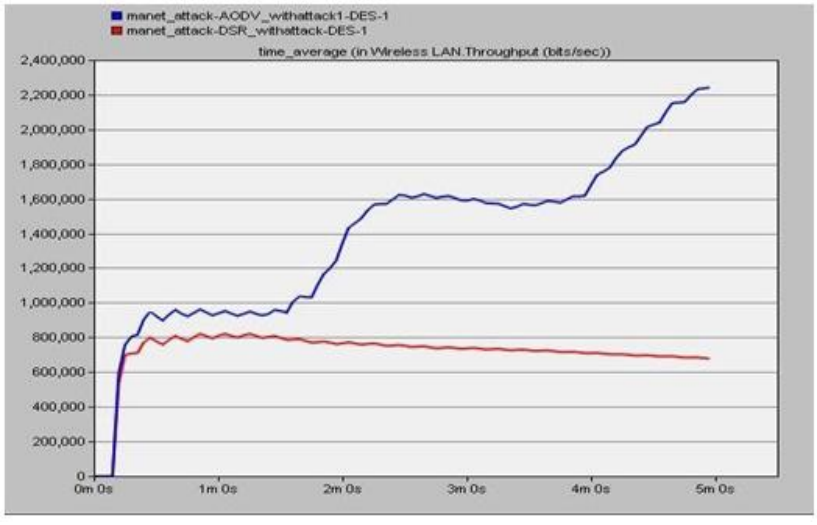

Figure14. Throughput of the network after attack under AODV and DSR protocol

Figure15. Delay of the network after attack under AODV and DSR protocol

Now, when the proposed strategy was employed in the attack network, AODV protocol yielded better throughput with lesser delay than DSR protocol. The figures16 and 17 depict the same .

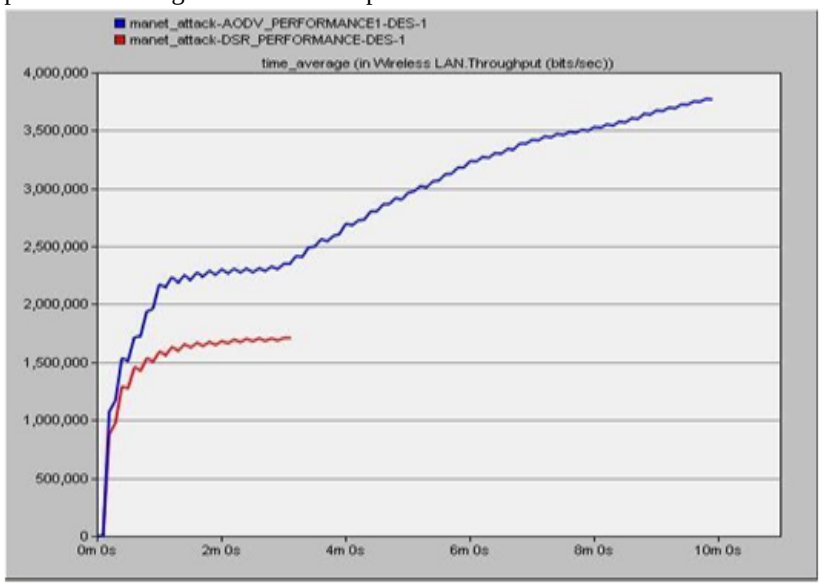

Figure16. Throughput of the proposed approach under AODV and DSR protocol

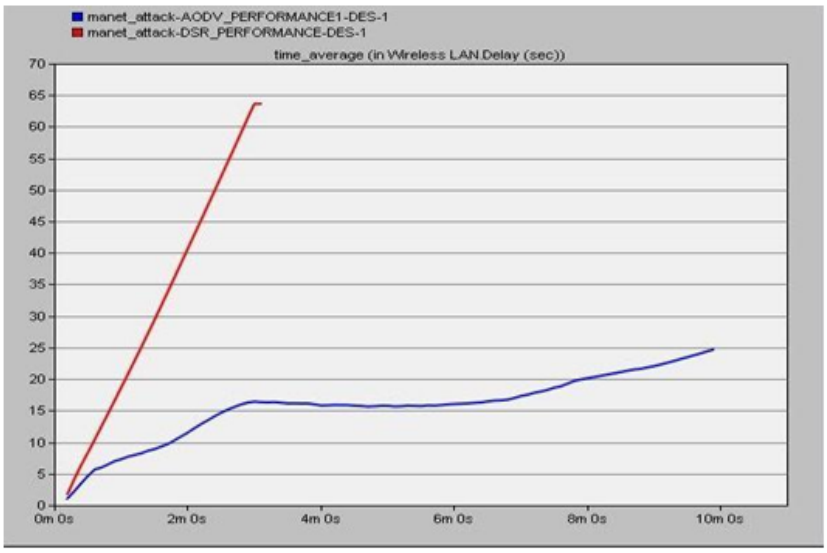

Figure17. Delay of the proposed approach under AODV and DSR protocol

V. CONCLUSION

A network-wide protection is required for the MANETs. So, in order to serve the purpose, jamming attack must be discovered. Various researchers tried to find the solution and did well in their efforts by providing us with several techniques. In order to improvise the throughput and decrease the delay, a Meliorated Detection mechanism is proposed which came out to be promising, both in terms of throughput and delay. In order to demonstrate this, the results of the proposed technique were analyzed and compared under AODV and DSR protocol in OPNET MODELER. AODV performed better. Future studies should consider the dynamic nature of the mobile networks in order to increase the throughput and decrease the delay under DSR protocol thereby providing network wide protection. Improved DSR parameters can be estimated in order to achieve the goal i.e. to decrease the network delay as much as possible.

REFERENCES

[1] W. Xu, W. Trappe, Y. Zhang, T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks", in MobiHoc'05: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, pp. 46–57, 2005.

[2] D. Chen, J. Deng, and P. K. Varshney, "Protecting wireless networks against a denial of service attack based on virtual jamming", in MOBICOM -Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking, ACM, 2003.

[3] D. Thuente, M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks", in Proceedings of the 25th IEEE Communications Society Military Communications Conference (MILCOM), October 2006.

[4] Chiang, J. T.; Hu, Y. C.; "Cross-layer jamming detection and mitigation in wireless broadcast networks", in Proc. 13th Annu. ACM MobiCom, Montréal, QC, Canada, pp. 346–349, 2007.

[5] R. L. Pickholtz, D. L. Schilling, L. B. Milstein, "Theory of spread spectrum communications—A tutorial", in IEEE Trans. Commun., vol. COM-30, no. 5, pt. 2, pp. 855– 884, May 1982.

[6] M. Strasser, S. Capkun, C. Pöpper, M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping", in Proc. IEEE Symp. Security Privacy, Berkley, CA, pp. 64–78, May 2008.

[7] W. Xu, W. Trappe, Y. Zhang, "Jamming Sensor Networks: Attacks and Defense Strategies", in IEEE Network, May/June 2006.

[8] T. X. Brown, J. E. James, A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks", in MobiHoc06, Florence, Italy.

[9] M. Li, I. Koutsopoulos, R. Pooverdan, "Optimal Jamming Attacks and Network Defenses Policies in Wireless Sensor Networks", in Proceedings of IEEE INFOCOM, 2007.

[10] A. Sampath, H. Dai, H. Zheng, B. Y. Zhao, "Multichannel Jamming Attacks using Cognitive Radios", in IEEE ICCCN, 2007

[11] K. Pelechrinis, I.Broustis, S.V. Krishnamurthy, C. Gkantsidis, "ARES: an Anti-jamming Reinforcement System for 802.11 Networks", in ACM CoNEXT, 2009.

[12] W. Xu, W. Trappe, Y. Zhang, "Anti-jamming Timing Channels for Wireless Networks", in ACM WiSec, 2008.

[13] I. Martinovic, P. Pichota, J. B. Schmitt, "Jamming for Good: A Fresh Approach to Authentic Communication in WSNs", in ACM WiSec, 2009

[14] A.; Mpitziopoulos, D. Gavalas, C. Konstantopoulos, G. Pantziou, "A Survey on Jamming Attacks and Countermeasures in WSNs", in IEEE Communications Surveys and Tutorials, Vol. 11, no. 4, 2009.

[15] Michelle X. Gong, Scott F. Midkiff, Shiwen Mao "A Cross-layer Approach to Channel Assignment in Wireless Ad Hoc Networks", in Journal of Mobile Networks and Applications, Vol. 12, No. 1, pg 43-56, Feb. 2007.

[16] Ali Hamieh, Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", in IEEE International Conference on Communications, pp.1-9, 2009.

[17] Kwangsung Ju, Kwangsue Chung, "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks", in International Journal of Security and Its Applications Vol. 6, No. 2, pp.149-154, April 2012.

[18] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, P. Havinga "Energy-efficient link-layer jamming attacks against WSN MAC protocols", in ACM Transactions on Sensor Networks, 5(1):1–38, 2009.

[19] Sisi Liu, Loukas Lazos, Marwan Krunz, "Thwarting Control-Channel Jamming Attacks from Inside Jammers", in IEEE Transactions on mobile computing, vol. 11, pp. 1545–1558, September 2012.

[20] Le Wang Wyglinski, M. Alexander "A combined approach for distinguishing different types of jamming attacks against wireless networks", in proc. In Communications, Computers and Signal Processing (PacRim), IEEE Pacific Rim Conference, pp. 809-814, 2011.

[21] Nor Surayati Mohamad Usop, Azizol Abdullah, Ahmad Faisal Amri Abidin, ''Performance Evaluation of AODV, DSDV & DSR Routing Protocol in GridEnvironment'', in IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.7, July 2009.

[22] Arif Sari, "Security Approaches in IEEE 802.11 MANET- Performance Evaluation of USM and RAS", in IJCNS International Journal of Communications, Network and System Sciences, 7, 365-372, 2014.

[23] Nadeem Sufyan, Nazar Abbass Saqib, Muhammad Zia " Detection of jamming attack in 802.11b wireless networks", in EURASIP Journal on Wireless Communications and Networking, 2013.
[24] Doru R, Vinoth P, " Mitigation of jamming attacks in wireless networks", in IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, 2013.
[25] Zhou Lu Wenye Wang, Cliff Wang " From Jammer to Gambler: Modelling and Detection of Jamming attacks against Time- Critical Traffic", in IEEE INFOCOM, 2011.
[27] Jerry T. Chiang, Yih-Chun Hu, " Dynamic Jamming Mitigation for Wireless Broadcast Networks", in IEEE IFOCOM, 2008.
[28] David J. Thuente, Benjamin Newlin, Mithun Acharya, " Jamming Vulnerabilites of IEEE 802.11e", in IEEE, 2007.

