Detection of Physical Jamming Attacks in MANETs

Aashish Mangla [1], Vandana[2]

M-Tech Student[1], Assit. Prof. [2] & Department of CSE
Delhi Institute of Technology, Management & Research
Faridabad, Haryana, India

***Abstract*—Because of the wireless type of the channel and particular features of MANETs, the radio interference attacks cannot be removed by conventional security procedures. These attacks result a important degradation on whole network packet transmission rates, throughput and delay on the MAC layer. A harmful node can continually transfer a radio signal in order to stop any kind of logical access to the medium and/or generalize with response. This process is known as jamming and the harmful nodes are called as jammers. The routing protocols of MANET could enhance system performance by enhancing data lost and throughput. To decrease the effect of the interruption, it is significant to detect its presence. Thus, in this paper, an improved detection mechanism has been suggested for detecting the physical jamming attacks in Ad Hoc on Demand Routing protocol thus decreasing the delay and enhancing the throughput. The results of the suggested mechanism are compared with the available mechanisms i.e. USM and RAS.**

Keywords: AODV, Delay, Defense Jamming attack.

I. Introduction

wireless networks have broadly commercial implementation due to their ease of use and setup and low cost. However, accessing the wireless network is very much easier as compare to accessing a wired networks, security becomes a important issue during the implementation of any wireless network. There are two categories of Mobile networks: Mobile Ad Hoc Networks (MANET) and Infrastructure networks. In Mobile Ad Hoc Network, the network may observe quick and unexpected configuration changes due to the presence of the mobile nodes. Each node in MANET has the responsibility to behave as a routing path and router in MANETs. Because of the wireless kind of the channel and particular features of MANETs, these are easily tapped by various attacks. A harmful node can continually transfer a radio signal in order to stop any kind of logical access to the medium and/or generalize with response. This process is known as jamming and the harmful nodes are known as jammers.

The jamming is classified as: Virtual and Physical Jamming attacks [10].

The physical jamming is found by uninterrupted transmissions and/or by assuring packet collisions at the receiver side. The jammers causing to these attacks can refuse complete access to the channel by controlling the wireless network completely.

Virtual Jamming Attacks can be found at the MAC layer by attacking on the DATA frames or CTS/RTS (Clear to Send/Rate to Send) frames. A benefit of MAC layer jamming is that the attacker node takes less power in directing these attacks in comparison of physical radio jamming. In virtual jamming attack harmful node propagate RTS packets without interruption on the transmission with unlimited period of time. During this whole process, the harmful node efficiently jam the transmission with a large amount of transmission on the wireless medium with low cost of power[2].

II. Literature Review

Wenyuan Xu et al. (2005) provides a complete description of the radio interference attacks and identify the serious issue of the presence of the jamming attack. Four different jamming attack models were suggested that can be employed by an antagonist to disable the procedure of a wireless network, and formulated their efficiency in terms of how every method influences the capability of a wireless node to send and obtain packets to and from the destination node. The author also talked about various measurements that forms the basis for discovering a jamming attack, and explained various scenarios where every measurement is not sufficient to reliably classify the existence of a jamming attack. The author realized that carrier sensing time and signal strength are unable to conclusively determine the existance of a jammer.

Ali Hamieh et al. (2009) explain that the military tactical and other security sensitive procedures are still the important applications of ad-hoc networks. One important challenge in planning of these networks is their susceptibility to Denial-of-Service (DoS) attacks. In this paper, the author takes a specific class of DoS attacks known as Jamming. A new way to determine of such attack by the formulation of error distribution was suggested.

ISSN: 2278 – 7798

Zhuo Lu Wenye Wang et al. (2011) objective at simulating and determining jamming attacks against time-critical traffic. The author presented a new metric, message invalidation ratio, to measure the time-critical applications performance. The author indicated through real-time experiments and gambling-based simulator that there exists a phase modulation process for a time-critical application under jamming at-tacks.

Sisi Liu et al. (2012) deal with the problem of preventing control channel DoS (Denial of Service) attacks evidenced in the form of jamming. The author takes a sophisticated antagonist who has knowledge of the cryptographic quantities and protocol specifies utilized to protect network operations. This kind of antagonist cannot be ceased by anti jamming processes that depends on spread spectrum. The author suggested a new security metrics to measure the capability of the antagonist to refuse access to the control channel, and presented a randomized distributed strategy that permits nodes to demonstrate and manage the control channel in the existence of the jammer. The suggested method is suitable for networks with fixed or dynamically distributed spectrum. Moreover, for uniquely determination of the set of compromised nodes, two algorithms were suggested, one for colluding nodes and one for independently behaving nodes [19].

III. System Model

3.1 Description of the First Scenario:
This scenario contains 100 mobile nodes randomly deployed in the simulation area of 1200 x 1200 m. Random waypoint mobility model is utilized for mobility of nodes with a constant speed of 20 m/s. By the help of this algorithm, random paths of the mobile nodes have been adjusted. The ad-hoc routing protocol is changed according to the needs of the simulation study for examining the results under a specific protocol such as AODV. Here, the start time is set to 10 seconds and the stop time is adjusted to the end of the simulation. The packet size and packet inter-arrival time and the packet size is set to 2000 (exponential) and 0.03 seconds (exponential).
The scenarios are modelled and examined by considering two parameters- Delay and Throughput.

1. Throughput- Throughput defines the total number of bits (in bits per sec) transferred from wireless LAN layers to the higher layers in all WLAN (Wireless LAN) nodes of the network.

2. Delay- Delay represents the end to end delay of all the packets obtained by the wireless LAN Macs of all the WLAN nodes in the network and transferred to the higher layers.

The simulation time is 300 seconds while the number of seeds utilized were 300 in order to give 1 hour simulation performance.

Table 1.Parameters for the first Scenario

Parameters Involved	Value used
No. of mobile nodes	100
Area of the network	1200*1200
Mobility speed of the mobile nodes	20 m/s
Ad-hoc Routing protocol	AODV
Start time	10 seconds
Stop time	End of Simulation
Packet Size	2000(exponential)
Simulation time	300 seconds
No. of Seeds	300
Simulation Kernel	Optimized

3.2 Description of the Attack Scenario:
Here, we have positioned two jammer nodes in the network to employ the physical jamming attack in the network. The jammer employed here is mobile pulse jammer. Here, the paths of the jammer nodes is adjust to VECTOR. The jammer base band frequency is considered as 2402 and the jammer bandwidth is adjust to 100000. The pulse width is considered as 2.0. The start time and the stop time is adjust to 10 seconds and end of the simulation respectively.

3.3 Description of the Third Scenario: for implementing the suggested method for the determining of the physical jamming attack, following detection method is suggested.

3.3.1 Proposed Technique
For enhancing the throughput of the whole network, the existence of the jammer node is very essential to be stated. Several techniques were preferred for determination, prevention and removing of the jamming attack. In order to improve the throughput and decrease the delay in comparison of the available techniques, an improved detection technique is suggested in this paper, for detecting the physical jamming attack.

1. In case, if packet size is beyond to a specific RTS threshold, then that packet would have to wait for a specific RTS/CTS

ISSN: 2278 – 7798

period in order to entirely forward that packet to its destination node. So, the buffer size is considered as 102400000.

2. Also, data rate of 54 mbps is taken which was 11 mbps previously in the simple and the attack scenario.

3. The value of the physical characteristics is set to Ex-tended Rate PHY.

4. Apart from performing the changes in the buffer size and data rate for the prevention of penalties caused by the withdraws of the available techniques and in order to enhance the throughput, enhanced AODV parameters are also acquired. Here, the active route timeout is taken as 30 seconds.

IV. Performance Results

4.1 Analysis of jamming attack under AODV protocol:

When the attack nodes were employed under AODV protocol into the network, then there is decrement in the network throughput thereby showing the existence of the physical jamming attack.

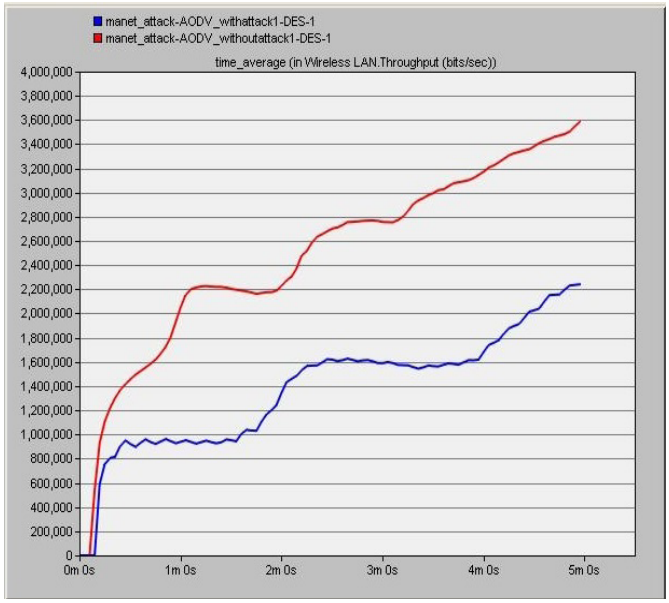

Fig 1. Detection of physical jamming attack under AODV on the basis of throughput

Similarly, due the presence of attack in the network, the delay of the network increased.

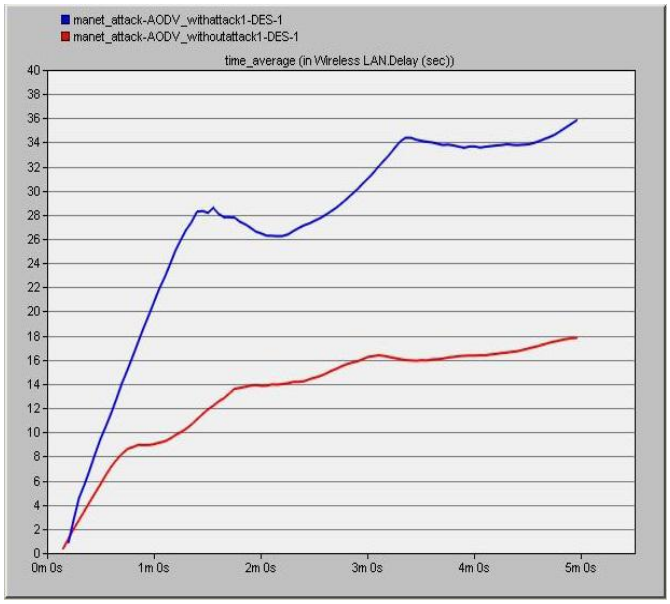

Fig 2. Detection of physical jamming attack under AODV on the basis of delay

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

When the suggested mechanism was employed to the network of the mobile nodes in which the attack was detected, first the throughput of the network increased slowly and then arrived to a predicting level. On the other side, the net-work delay decreased to a significant value.

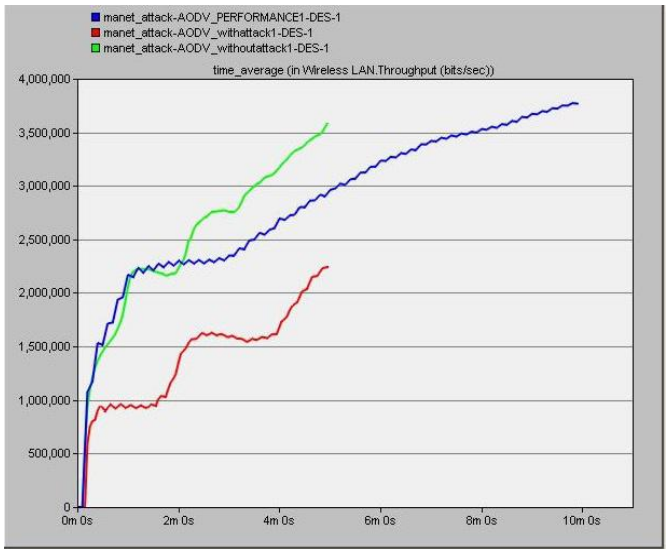

Fig 3.Throughput of the network under AODV with the Proposed Approach

ISSN: 2278 – 7798

Fig 4. Delay of the network with the proposed approach under AODV protocol

4.3 Comparison of the results obtained from the pro-posed technique to the existing techniques- USM and RAS under AODV protocol:

The available techniques were also simulated by using OPNET simulator. Following graphs indicate that USM performs better as compared to RAS in terms of the throughput but could not deal with the issue of increased delay. However the graphs plotted above, indicate that the suggested technique provides better results in comparison of RAS and USM technique in terms of throughput and delay.

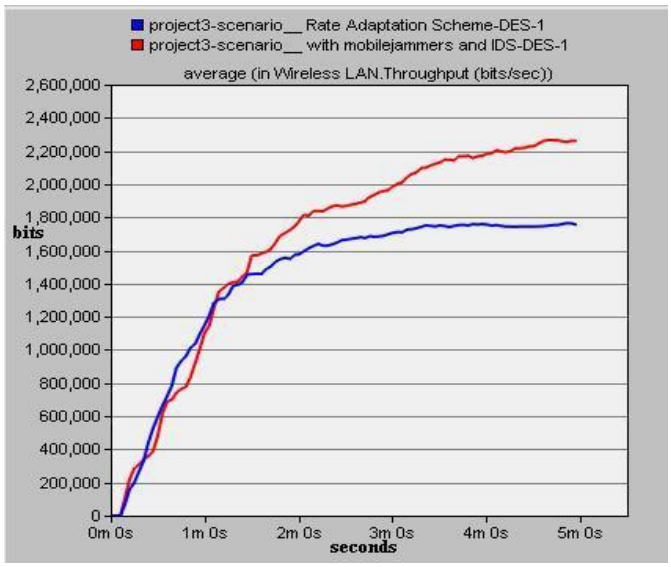

Fig 5. Throughput of USM and RAS under AODV protocol

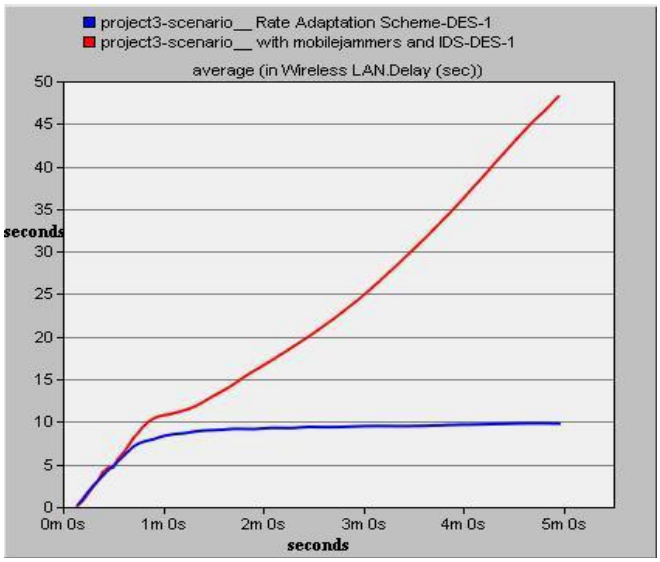

Fig 6. Delay of USM and RAS under AODV protocol

Table 2
Theoretical Comparison of the simulation results of the pro-posed technique with USM and RAS under AODV protocol

S.no	Parameters used	Proposed Scheme	USM	RAS
1	Throughput in bits/sec	highest	Less than proposed scheme and larger than RAS	least
2	Delay in seconds	Larger than RAS and less than USM	Less than proposed scheme but more than RAS	least

Table 3
Value based Comparison of the simulation results of the proposed technique with USM and RAS under AODV protocol

s.no	Parameter used	Proposed scheme	USM	RAS
1	Throughput in bits/sec	Near about 4,000,000	Near about 2,200,000	Near about 1,600,000
2	Delay in seconds	25	Near about 50 s	10

The Tables 2 and 3 helps in examining of the above discussion more clearly.

ISSN: 2278 – 7798

V. Conclusion

A network-wide security is needed for the MANETs. So, for serving the objective, jamming attack must be found. Many researchers tried to discover the solution and did well in their attempts by offering us with various techniques. In order to decrease the delay and enhance the throughput, an improved Detection mechanism is suggested which came out to be predicting, both in terms of delay and throughput in comparison of RAS and USM. In order to establish this, the results of the suggested technique were examined and compared under AODV by using OPNET simulator.

REFERENCES

[1] W. Xu, W. Trappe, Y. Zhang, T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks", in MobiHoc'05: Pro-ceedings 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 MO-BICOM -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 (MIL-COM), 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 spec-trum 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 Ap-proach 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 distin-guishing 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] Rama Krishna Challa, Saswat Chakrabarti, Debasish Datta "An Im-proved Analytical Model for IEEE 802.11 Distributed Coordination Func-tion under Finite Load", in International Journal of Communications, Network and System Sciences, Vol: 02 Issue: 03 , 237-247, 2009.

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

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

[24] 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.

ISSN: 2278 – 7798