Prevention of Jamming Attack in MANET

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 nature of the channel and particular features of MANETs, the radio interference attacks cannot be removed by traditional security techniques. An adversary can easily prevail over its medium access control protocol (MAC) and continuously transfer packages on the network medium. The authorized nodes keep propagating Request-to- Send (RTS) frames to the access point node for accessing the shared medium and begin data transfer. However, because of jamming attacks on the network, the access point node cannot allocate authorization access to shared channel. These attacks lead important reduction on entire network packet transmission rates, throughput and delay on the MAC layer since other nodes pull out from the communication. The suggested method employed for mitigating and preventing jamming attacks is implemented at the MAC layer that contains a combination of various coordination mechanisms. These are a combination of Point Controller Functions (PCF) that are utilized to coordinate whole network activities at the MAC layer and RTS/CTS (Clear-To-Send) strategies which is a handshaking process that reduces the collisions on the wireless network. The whole network performance and mechanism is modeled by employing OPNET simulator.**

Keywords: MANET, OPNET Simulation, PCF, RTS/CTS, Jamming Attack, Unified Security Mechanism

I. INTRODUCTION

The IEEE 802.11 attacks are examined in various studies by researchers. The most popular attack model of IEEE 802.11 is Jamming Attacks. Jamming is defined as a Denial of Service (DoS) attack that disrupts the communication among nodes. The aim of the adversary leading a jamming attack is to stop a legitimate receiver or sender from receiving or transmitting packets on the network. Adversaries or harmful nodes can establish jamming attacks at multiple layers of the protocol suite. The jamming attacks are modeled on MANETs that result in collisions in the mobile wireless network. The jamming is categorized into two classes as Physical and Virtual Jamming attacks. The physical jamming is established by continuous transmissions and/or by leading packet collisions at the receiver side. Virtual jamming happens at the MAC layer by attacks on data frames or control frames in IEEE 802.11 protocol [1]. Physical or Radio jamming in a wireless channel is a simple but interruptive form of DoS attack. These attacks are established by either a continuous transmission of radio signals or by sending random bits onto the wireless medium [2]. The jammers leading these attacks can refuse complete access to the channel by completely controlling the wireless medium. The nodes trying to interact have a remarkably large carrier sensing time waiting for the medium to become idle. This has an opposite propagating impact as the nodes enter into large exponential back-off periods. Virtual Jamming Attacks can be established at the MAC layer by attacks on the DATA frames or RTS/CTS (Rate to Send/Clear to Send) frames. An important benefit of MAC layer jamming is that the attacker node takes less power in directing these attacks in comparison of the physical radio jamming. Here, we concentrate on DoS attacks at the MAC layer resulting in collision of DATA frames or RTS/CTS control frames.

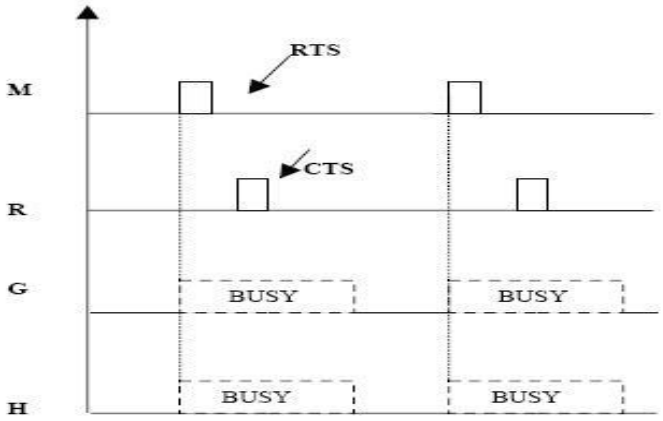

Figure 1. Jamming Attack

II. PROPOSED METHOD

The suggested method employed for mitigating and preventing jamming attacks is implemented at the MAC layer that contains combination of various coordination strategies.

ISSN: 2278 – 7798

The network throughput may reduce because of the Request to Send (RTS) collision difficulty, for that cause RTS/CTS fragmentation thresholds are also included into this technique. Wireless medium access control (MAC) protocols have to organize the transmissions of the nodes on the common transmission channel. The IEEE 802.11 working group suggested two different algorithms for contention resolution. These coordination functions of the MAC Layer are displayed in the Figure 2. The first one is Distributed Coordination Function (DCF) which is totally distributed and the second one is Point Coordination Function (PCF) that has a centralized access protocol.

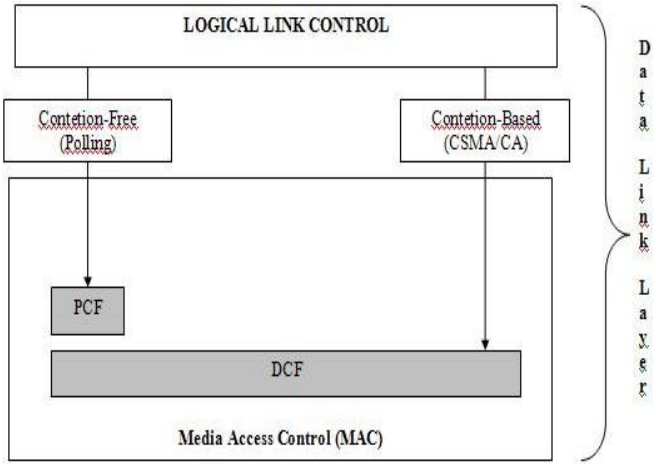

Figure 2. PCF and DCF Functionalities

In order to protect and prevent the network from hidden jammer node attacks and stop collisions on the network, the Request to Send/Clear to Send (RTS/CTS) strategy is also implemented. The RTS/CTS mechanism is a handshaking process that reduces the occurrence of collisions when hidden nodes are running on the network. The implementation of RTS/CTS mechanism will be displayed in the next section of the research through the simulation experiment. The working mechanism of RTS/CTS implementation is shown in Fig 3

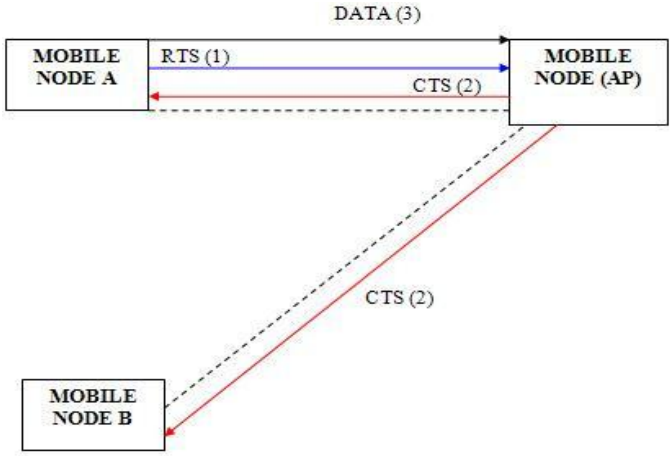

Figure 3. RTS/CTS working mechanism

III. SIMULATION MODEL AND EXPERIMENTAL DESIGN

The tool employed for the simulation study is OPNET 14.0 simulator. OPNET is a application and network based software employed for network management and analysis [9-10]. OPNET simulates communication devices, several protocols, architecture of various networks and techniques and offers simulation of their performances in the virtual environment. OPNET offers several development and research solutions which helps in the research of examine and enhancement of wireless technologies i.e. Wi-Fi, WIMAX, UMTS, examining and designing of MANET protocols, enhancing core network technology, offering power management solutions in wireless sensor networks. In our case we employed OPNET for simulating of network nodes, choosing its statistics and then running its simulation to obtain the result for analysis.

Table 1. Global Simulation Parameters for the Experiment

Parameters	Attributes
Protocol	**AODV**
Simulation Time	**300 (seconds)**
Simulation Area	**1000 x 1000 (meters)**
Pause Time	**100 Seconds**
Mobility Model	**Random Waypoint**
Mobility m/s	**10meters/seconds**
Performance Parameters	**Throughput, Delay, Load, Data Drop Rate**
Transmit Power(W)	**0.005**
RTS Threshold (bytes)	**1024 (bytes)**
Data Rate (Mbps)	**11Mbps**
Pkt. Reception power Threshold	**-95**
Buffer Size	**1024000**
Pkt. Size (bits)	**2000 (exponential)**
Pkt. Interarrival time (seconds)	**.03 (exponential)**
Trajectory	**VECTOR**
Start time (seconds)	**10**

ISSN: 2278 – 7798

End Time	**Infinity (End of Simulation time)**
No of Seeds	**300**

IV. PERFORMANCE METRICS

The performance metrics selected for the prevention and evaluation of jamming attacks on MANETs are network load, network throughput and packet end-to-end delay. Table 2 shows the chosen performance metrics for the simulation experiment.

Table 2. Simulation Performance Metrics

Performance Metrics
Network Throughput
WLAN Delay
Network Load
WLAN Data Dropped

The network throughput is the total performance of the network. It shows the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network. The WLAN Delay shows the end to end delay of all the packets obtained by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer. This delay involves medium access delay at the source MAC, reception of all the fragments individually, and transfers of the frames through AP, if access point capability is enabled. The network load shows the statistic that is formed for measuring the network load individually for every BSS. Thus, every dimension is a global statistic dealing with one WLAN BSS of the network. The WLAN Data Dropped rate is the overall size of the higher layer data packets (in bits/sec) lost by all the WLAN MACs in the network because of full higher layer data buffer or the size of the higher layer packet, which is greater than the highest permitted data size described in the IEEE 802.11 standard.

V. SIMULATION RESULTS AND DISCUSSION

After compilation of 3 scenarios with 50 mobile nodes and various parameters for every scenario, the simulation results are collected and examined in this section. The 3 scenarios are compiled within a Discrete Event Simulation (DES) environment, and gathered information is examined depending on the performance metrics.

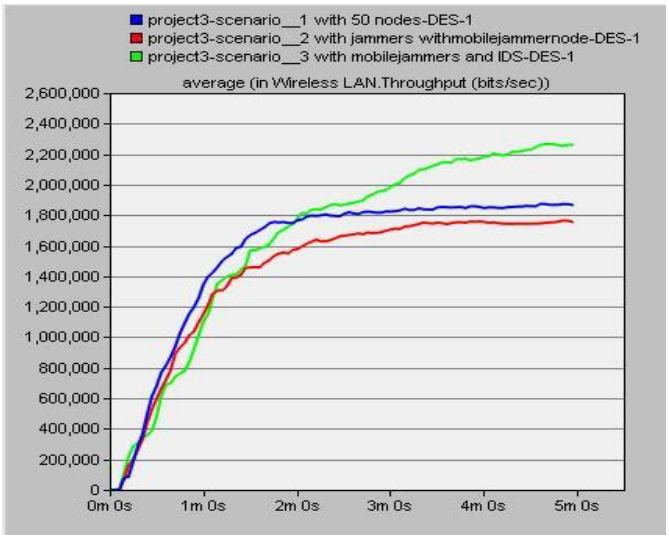

Figure 4. Average WLAN Throughput Statistics

As it is clearly indicated in the Figure above, the WLAN Throughput of the total network is examined with DES. Scenario 1 shows the scenario with no harmful event and normal network state, scenario 2 shows the network that is under the jamming attack and scenario 3 shows the mobile jammers and implementation of the suggested method.

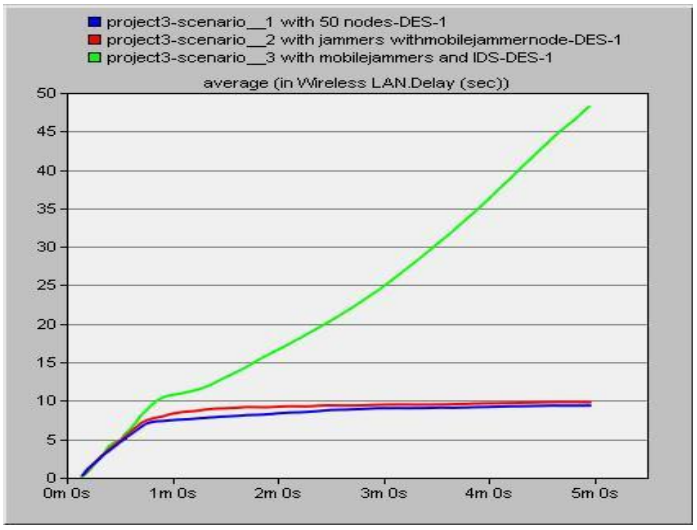

Figure 5 Average WLAN Delay Statistics

As it is depicted in Figure 5, there is a important increase realized on MANET delay for scenario 3 where the suggested mechanism is implemented.

ISSN: 2278 – 7798

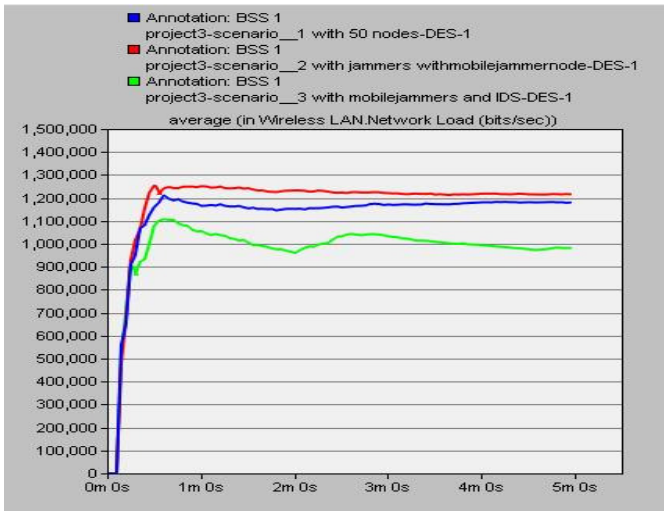

Figure 6. Average WLAN Network Load

As it can be viewed from the above figure, the WLAN Load level is enhanced when the jamming attack is established. On the other hand, the load is reduced when the mechanism is implemented on the particular nodes in the network.

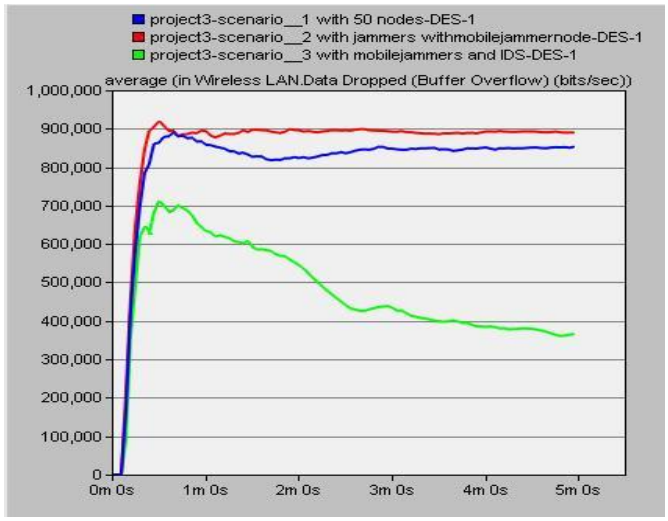

Figure 7. Average WLAN Data Dropped Rates

CONCLUSION

The objective of this simulation research study was to realize the effect of a combination of security techniques against jamming attacks. The united technique is implemented on the chosen nodes on the network and deployed in the particular area. The results found by the research clearly shows that, the implementation of these unified techniques have an important effect on the total network throughput positively. On the other hand, the implementation of these mechanisms does not only mitigate the jamming attack impacts, it also enhances the total performance above the normal state of the network. The united mechanism that consists a combination of RTS/CTS and PCF indicates enough performance in MANET. Since 2 mobile jammers utilized in this simulation experiment, the suggested security mechanism satisfactorily mitigated the impacts of the jamming attack on the network and enhanced the total performance of the network while enhancing data loss rate. The data lost rate reduced successfully. Since the jamming attack causes packet drop rate and low throughput effect on the network, the rate of delay appears acceptable on the network. Future studies can be conducted to modify the current model to reduce a total delay on the network.

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

ISSN: 2278 – 7798

[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