Detection and Prevention of Physical Jamming Attacks in Vehicular Environment

Mahendri[1], Neha Sawal[2]

M-Tech Student[1] Assit. Prof.[2] &Department of CSE & NGF College of Engineering &Technology
Palwal, Haryana, India

***Abstract*— Various studies in the literature have been covered by the researchers to solve security problems of vehicular Ad-Hoc Networks (VANET). Because of the wireless nature of the channel and particular features of VANETs, the radio interference attacks cannot be mitigated by traditional security methods. These attacks lead a important reduction on packet transmission rates, total network throughput and delay on the MAC layer since other nodes step back from the interaction. A harmful node can continuously transmit a radio signal in order to stop any kind of logical access to the medium and/or infer with reception. This procedure is known as jamming and the harmful nodes are called as jammers. VANET routing protocols could enhance system performance by improving throughput and data lost. To reduce the effect of the interruption, it is significant to identify its existence. So, in this paper, an improved detection mechanism has been suggested in order to determine the physical jamming at-tacks in Ad Hoc On Demand (AODV) Routing protocol thus improving the throughput and reduce the delay. The results of the suggested technique are compared with the available techniques USM and RAS.**

Keywords: AODV, Defense, Delay, Jamming attack.

I. INTRODUCTION

The developing demand of wireless communications and wireless devices tends to research on self-configuring and self curing networks without the help of any centralized framework or pre-established authority/infrastructure. This type of networks is called Ad hoc networks. Vehicular Ad hoc Networks (VANETs) is a part of Mobile Ad Hoc Networks (MANETs) that has came out because of latest development in wireless technology and sensor network. Vehicular Ad hoc Networks (VANETs) are ad-hoc network's real applications where real-time interaction between nearby roadside static infrastructure and vehicles is offered over wireless connections. It reduces both traffic congestion and vehicle crashes which are main problems around the whole world. The wireless interaction between two or more nodes in a VANET (Vehicular Ad hoc Networks) faces several unique issues. This is specifically appropriate for safety-critical applications i.e. lane change, pre-crash feeling, collision avoidance etc. Factors i.e. high vehicle speeds, low signal latencies, varying topology, traffic density, overall message size etc. are primary challenges that makes traditional wireless protocols and technologies unsuitable for VANETs (Vehicular Ad hoc Networks). Along with performance challenges, there are several security issues in VANET i.e. maintaining the validity of data packet, certifying sender of message, offering node secrecy with non-repudiation, existence, certificate cancellation etc. All these performance and security requirements coordinate to form VANET safety applications more challenging in comparison of other wireless applications.

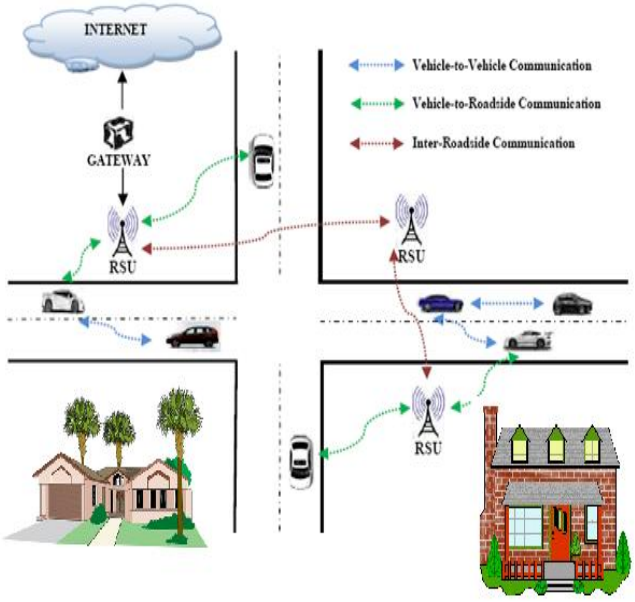

Fig.1. Vehicular Ad hoc Network

The routing protocols in VANET are categorized into three major categories:-

1. Proactive Routing Protocol-In proactive routing protocol, the mobile nodes transfer routing information and maintain the network topology information in routing table at periodic interval of time. These protocols are also called as table driven routing protocol.
2. Reactive Routing Protocol- Here the mobile nodes do not transfer routing information at regular interval of time. These protocols get a new path when it is needed. These protocols are also called as on demand routing protocol.
3. Hybrid Routing Protocol- It is the combination of both proactive and reactive routing protocols. A table driven mechanism is applied inside the routing zone of each node while an on demand mechanism is

ISSN: 2278 – 7798

applied for the nodes that are not inside the routing zone [10].

II. RELATED WORK

Wenyuan Xu et al. (2005) provide a detailed explanation of the radio interference attacks and identifying the vital issue of the existence of the jamming attack. Four different jamming attack frameworks were suggested that can be utilized by an antagonist to disable the operation of a wireless network, and measured 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 evaluations that supports as the basis for determining a jamming attack, and revealed different scenarios where every measurement is not sufficient to reliably classify the existence of a jamming attack.

Mario Strasser et al. (2008) addresses the problem of how can two devices that do not share any private information demonstrate a shared secret key over a wireless radio channel in the existence of a communication jammer. An inherent issue in solving this problem was that called anti-jamming techniques (e.g., frequency hopping or direct-sequence spread spectrum) which should support device communication at the time of the key establishment needed that the devices shared a secret spreading key (or code) before to the beginning of their communication

Sisi Liu et al. (2012) consider the problem of preventing control-channel DoS attacks demonstrated in the form of jamming. The author considered a sophisticated antagonist who has information of the protocol particulars and of the cryptographic quantities utilized to protect network operations. This kind of antagonist cannot be prevented by anti jamming mechanisms that rely spread spectrum. The author suggested a new security metrics to quantify 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 to networks with fixed or dynamically distributed spectrum.

III. System Model

3.1 Description of the First Scenario:

This scenario composed of 50 mobile nodes deployed arbitrarily in the region of 1000 x 1000 m. Nodes move in this region based on random waypoint mobility model with a constant speed of 10 m/s.

The scenarios are modeled and examined based on two parameters- Throughput and Delay.

1. 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.

2. 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 forwarded to the higher layers.

Table 1. Parameters for the first Scenario

Parameters Involved	**Value used**
No. of mobile nodes	50
Area of the network	1000*1000
Mobility speed of the mobile nodes	10 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 for engaging the physical jamming attack in the network. The jammer employed here is mobile pulse jammer

Table2 Jammer characteristics

Parameters involved	**Value used**
Type of Jammer	Pulse Jammer
Jammer bandwidth	100000
Jammer base band frequency	2402
Pulse width	2.0
Start time	10 seconds
Stop time	End of the simulation

3.3 Description of the Third Scenario:

For implementing the suggested technique for the determination of the physical jamming attack, following detection technique is suggested.

Proposed Technique

For enhancing the throughput of the overall network, the existence of the jammer node is very essential to be stated. Several techniques were adopted for the discovery, prevention

ISSN: 2278 – 7798

and mitigation of the jamming attack. For enhancing the throughput and reducing the delay in comparison of the available approaches, an improved detection mechanism is suggested in this paper, for the determination of the physical jamming attack.

1. In case, if packet size increased to a specific RTS threshold, that packet would have to wait for a specific RTS/CTS interval in order to completely route that packet to its destination node. So, the buffer size is considered as 102400000.
2. Also, high data rate of 54 mbps is considered which was formerly 11 mbps during the simple and the attack scenario.
3. The value of the physical characteristics is adjusted to Extended Rate PHY.
4. So, apart from performing the changes in the buffer size and data rate for the prevention of penalties lead by the disadvantages of the available techniques and for improving the throughput, enhanced AODV parameters are also followed. Here, the active route timeout is considered as 30 seconds.

IV. PERFORMANCE RESULTS

4.1 **Analysis of jamming attack under AODV protocol:**

When the attack nodes were employed into the network of the mobile nodes under AODV protocol, the throughput of the network reduced, thus describing the existence of the physical jamming attack.

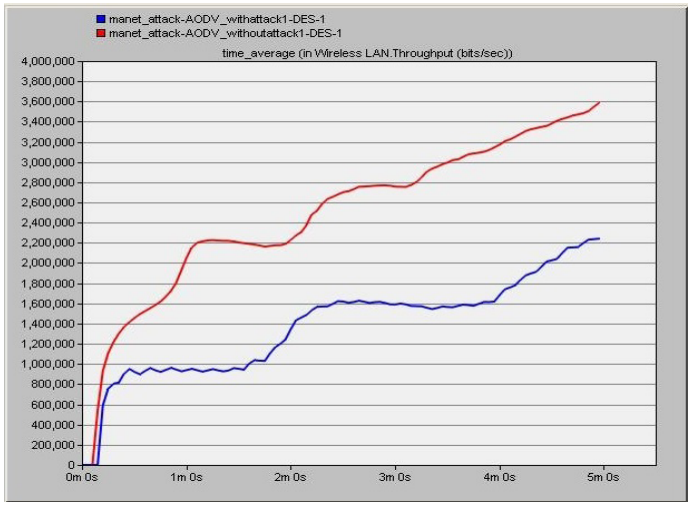

Fig 1. Detection of physical jamming attack under AODV on the basis of throughput

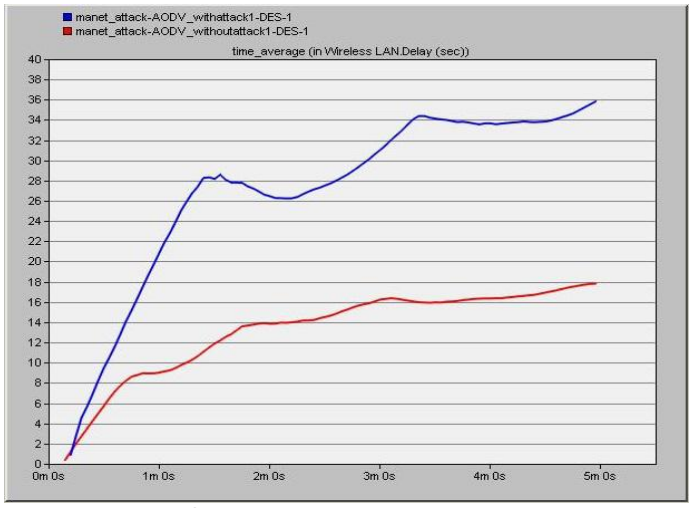

Fig 2. Detection of physical jamming attack under AODV on the basis of delay

4.2 Analysis of jamming attack under AODV protocol when the suggested technique was employed:

When the suggested technique was employed to the network of the mobile nodes in which the attack was detected, the throughput of the network first enhanced slowly and then arrived to a expecting level. On the other side, the delay of the net-work reduced to a important value in comparison of the attack scenario.

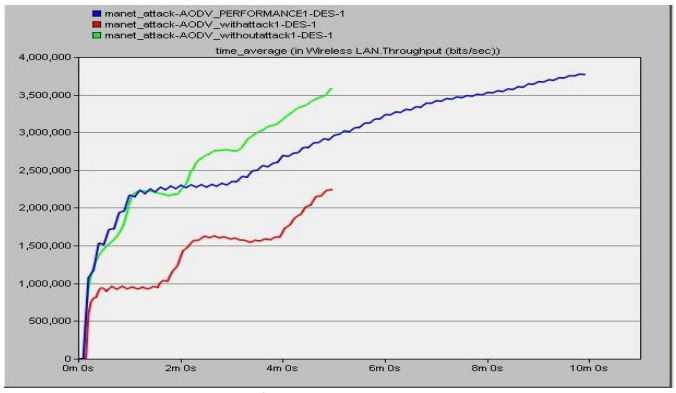

Fig 3. Throughput of the network under AODV with the proposed approach

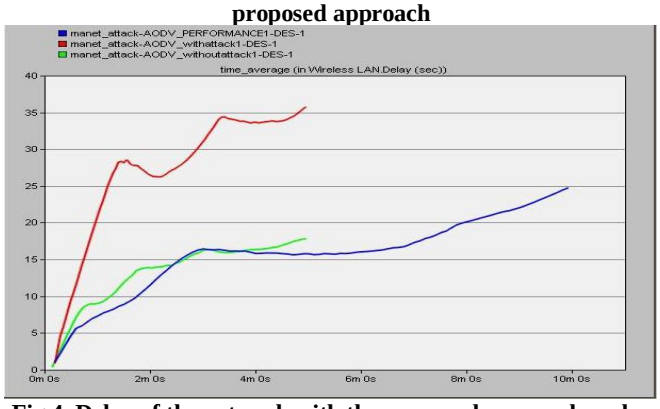

Fig 4. Delay of the network with the proposed approach under AODV protocol

ISSN: 2278 – 7798

4.3 Comparison of the results received from the pro-posed mechanism to the available techniques- USM and RAS under AODV protocol:

The available techniques were also simulated in OPNET Simulator. Following graphs display that USM was better than RAS in terms of the throughput but could not deal with the problem of enhanced delay. However the graphs drawn above, depict that the suggested mechanism provides better results as compared to RAS and USM technique in terms of throughput and delay.

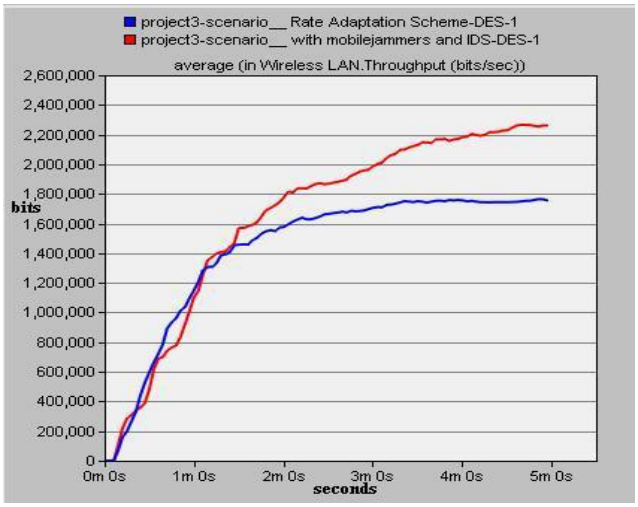

Fig 5. Throughput of USM and RAS under AODV protocol

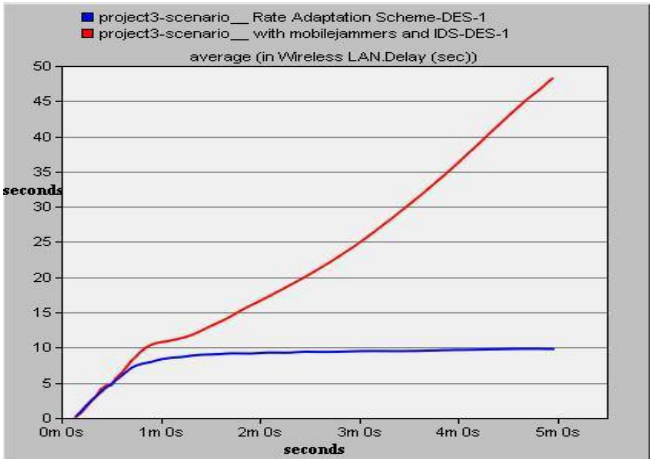

Fig 6. Delay of USM and RAS under AODV protocol

Table 3: Theoretical Comparison of the simulation results of the suggested mechanism with RAS and USM under AODV protocol

S.no	Parameters used	Proposed Scheme	USM	RAS
1	Throughput in bits/sec	highest	Less than propose-d 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 suggested mechanism with RAS and USM under AODV protocol

s.no	Parameters 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

CONCLUSION

A network-wide security is needed for the VANETs. So, for serving the aim, jamming attack must be detected. Several researchers attempt to discover the solution and did well in their attempts by offering us with various techniques. For improving the throughput and reducing the delay, an improved Detection mechanism is suggested which came out to be predicting, both in terms of delay and throughput, when compared to USM and RAS. For demonstrating this, the results of the suggested mechanism were examined and compared under AODV in 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: 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 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

ISSN: 2278 – 7798

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 sAttacks 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.

ISSN: 2278 – 7798