CGC International Journal of Contemporary Technology & Research
ISSN: 2582-0486 (online)

Securing Wireless LAN by Boosting Intrusion Detection Techniques

Rupinder Singh
Assistant Professor, Department of Computer Applications,
CGC,Landran

***Abstract*-The Wireless Fidelity (Wi-Fi) is a widely adopted technology due to its mobility and freedom in the presence of vulnerable security features. Several attempts have been made to secure Wi-Fi that ends up as the devices are vulnerable to various types of attacks and intrusions. Thus, the additional use of an external defense mechanism like Intrusion Detection System (IDS) is mandatory to secure WLAN. The Intrusion Detection Technique identifies the security threats by continuously monitoring the network activities. Many security threats affect the performance of network threats like Authentication attacks. Encryption cracking, Wormhole, Selective Jamming attack etc. Jamming attack is always an issue in wireless network. In jamming attacks the target node is adversely affected with proper internal knowledge of network secrets and routing protocols and these types of attacks launched at low intensity so that they are very difficult to detect and encounter. So to reduce the attack and algorithm is developed that helps in tracking the intrusion and then mitigating the attack. In NS2 simulation environment, results represents the network performance without Jamming attack and with Jamming attack and also if the Jamming is encountered how to save from that and by applying the proposed scheme the performance is very much like that no attack has even occurred. Main goal is to prevent the attack and check the various parameters after the attack is prevented.**

Keywords: Network Security, Wireless Sensor Network, Jamming attacks, Routing Protocol.

I. INTRODUCTION

Wireless LAN (that does not require cables to connect with different device) uses radio waves for the communication. An intruder attacks has been exceeded due to the wireless nature of LAN. Classification of wireless neighborhood area community attacks are proposed primarily ‘based at the vital parameters. In recent years, wireless communication technology has emerged very convenient in place of wired communication technology and has become more readily available for computer networks anywhere, whether it is for a home, an office, or any size of business.

Jamming attacks chokes the network, mostly the jamming is executed by using the knowledge of preserved information. The wireless medium provides faster accessibility, compatibility and connectivity between different users. Though it provides features but various types of attacks are invited because of its sharing medium. The adversaries with internal knowledge of network secrets take more effort on jamming the network or degrade the network performance. Anyone which has transceiver can easily inject spurious messages or create noise or interference or launch jamming attack in an ongoing transmission or block the transmission of legitimate users. In the simplest form, the jammer classifies first few bytes of transmitted packet and corrupts them by creating proximity of the targeted receivers or FM modulated noise or electromagnetic interference such as magnetic radiowaves.

`

II. DETECTION & PREVENTION OF JAMMING

The network implements a monitoring mechanism for detecting potential malicious activity by a jammer. The monitoring mechanism does a Pre Authentication Check for verifying the nodes authenticity.

Algorithm 1 Generating Key

1. Get the already shared key.
2. Compute the equation in the standard set of keys in the given simulation:

$$val = log10(val) * val$$

3. Produce the numeric key from the decimal key

$$val = val \times 10$$

4. Return the key value after rounding the key value to remove the decimal places

$$Key = round\ (val)$$

Now there are various nodes which are in network. They are sending frequent requests to other nodes and wants to access those nodes but before accessing those nodes or wants any communication with nodes all the nodes have to show their authentication which can be done with the algorithm shown above. Now from previous cases the

malicious nodes table can be generated well in advance from the previous traffic of the network. A node is said to be malicious if the node is showing the attributes of Jamming attack.

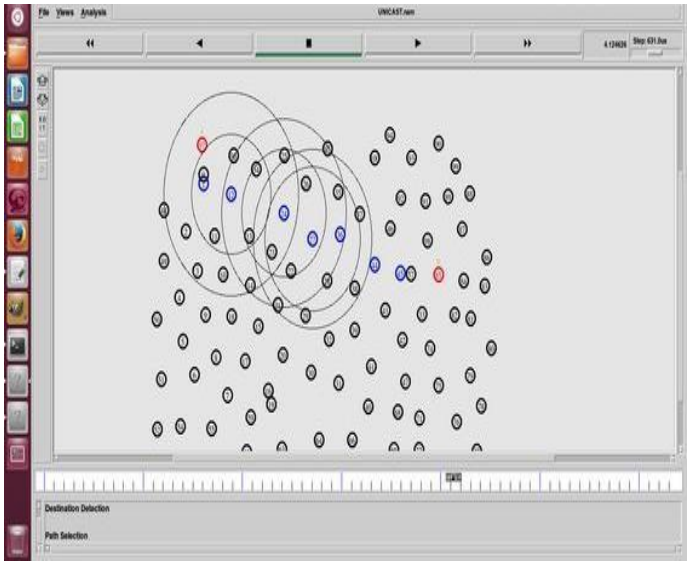
Algorithm 2:

1. When the route replies are received from different nodes.
2. All the replies must be checked with the malicious node table.
3. Now it the reply is similar to that of the malicious node then immediately the route should be aborted.
4. If the reply is different than the node is the authenticated node.

Simulation is defined as a scenario wherein precise set of situations are created artificially that allows you to study or experience something that would exist in truth. In specific, network simulation is a method wherein software models the behavior of a network both by way of calculating the interaction among the one of a kind network entity inclusive of data links, hosts, packets and so forth. In order to test the proposed techniques, the NS2 simulator is used to evaluate the performance with parameter shown in table

1	Simulator used	NS 2.35
2	No. of nodes	50
3	Area of flat grid	2000*1000
4	Transmission range	250m
5	Destination node	26(fixed)
6	Node deployment	Random
7	Simulation Time	25s
8	Initial energy	100j

1.1 Simulation scenario



III. Simulation and Results

Packet Delivery Rate: Packet delivery ratio factor evaluates the percentage of the successfully delivered packets among the given network or link in the given time (1 second in our case). The PDR shows the rising trend in the following graphs, which elaborates the rising network ability with each passing second, whereas the stability or straight line after 10^{th} second shows the performance of the fully converged network, which is communicating on the nearly constant speed to deliver the packets among the given networks $PDR = No.\ of\ packets\ received\ at\ the\ destination\ node / No.of\ packets\ generated\ at\ the\ source\ node * 100$.

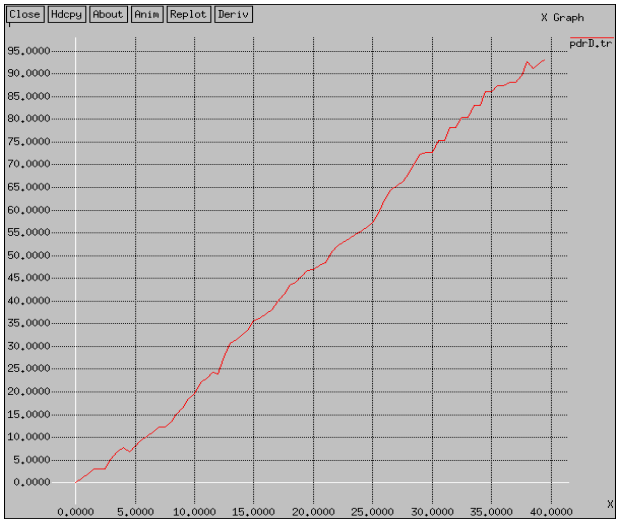


Fig 1. Shows the Packet delivery ratio (PDR) after the attack is prevented.

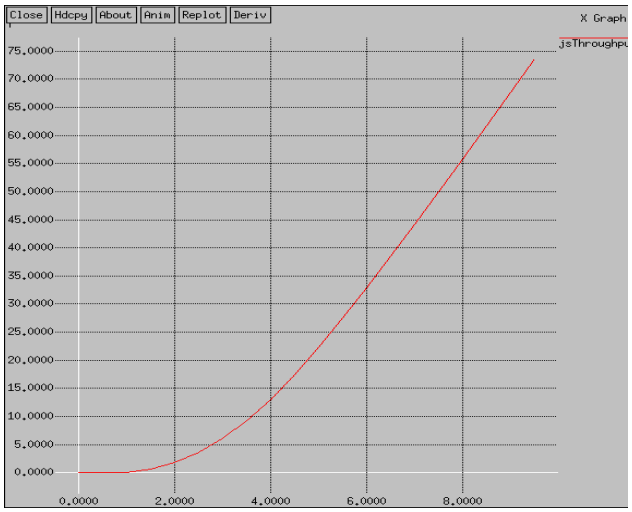


Fig. 2. shows the throughput after the attack is prevented

IV. Conclusion and Future Scope

The performance of the proposed technique is compared with that of Old techniques Transmission Range and at different time interval (5 to 25 sec.) for the detection of Jamming attacks in wireless LAN. The simulation results show that the proposed techniques are more effective than the old techniques which are used to mitigate the jamming attacks. The packet delivery ratio was improved considerably. The throughput is better what was seen in the old techniques. The proposed scheme also attains low false positive rate as compared to old scheme, which indicates the better detection efficiency of the proposed technique. The investigation shows that the proposed technique attains low false positive rate while increasing the packet delivery ratio. This work doesn't apply on MANET it can be extended to Wireless Sensor Networks and on MANET.

REFERENCES

[1] A wireless bounded breadth arrangement Association (2002). "Wireless Networking Standards and Organizations", WLAN Resource Center, April 17, 2002

[2] Wireless bounded breadth arrangement Medium Admission administration (1999) And Physical Band (PHYJ. Specification,

[3] A. Wood and J. Stankovic (2002). Denial of account in assay aspect network. IEEE pc,

[4] Taewoo Kwon, Emre Ertin, Anish Arora (2012) Reproducing constant wireless agreementachievement beyond environments, ad-lib Networks, ten (2012) 696"708, Elsevier

[5] Benot Latre, Bart Braem, Ingrid Moerman Chris Blondia, Piet Demeester (2011) A assay on wireless physique amplitude networks, Wireless Arrangement (2011) 17:1вЂ"18 , DOI 10.1007/s11276- 010-0252-4.

[6] Sung-Hwa Lim, Young-Bae blow, Cheolgi Kim and Nitin H. Vaidya (2011) appearance and accomplishing of multicasting for multi-channel multi- interface wireless cobweb networks, Wireless Arrangement (2011) 17:955вЂ"972.

[7] Petrioli, Chiara, et al. "ALBA-R: Load- balancing geographic routing around connectivity holes in wireless sensor networks." Parallel and Distributed Systems, IEEE Transactions on 25.3 (2014): 529-539.

[8] Y. Zhao, Q. Zhang, Y. Chen, and W. Zhu, "Hop ID Based Routing in Mobile Ad Hoc Networks," Proc. IEEE 13th Int'l Conf. Network Protocols (ICNP '05), pp. 179-190, Nov. 2005.

[9] S. Basagni, M. Nati, and C. Petrioli, "Localization Error-Resilient Geographic Routing for Wireless Sensor Networks," Proc. IEEE GLOBECOM, pp. 1-6, Nov./Dec. 2008.

[10] Xu, Jiu-qiang, et al. "Study on WSN topology division and lifetime." Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on. Vol. 1. IEEE, 2011

[11] C. Schleher, Electronic Warfare in the Information Age. Artech House,1999.

[12] D. Wood and J. A. Stankovic, "Denial of service in sensor networks,"IEEE Comput., vol. 35, no. 10, pp. 54-62, 2002.

[13] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in Proc. USENIX Security Symp., pp. 15-28, 2003.

[14] G. Noubir and G. Lin, "Low- power DoS attacks in data wireless LANs and countermeasures,"
SIGMOBILE Mob. Comput. Commun. Rev., vol. 7, no. 3, pp. 29-
30, 2003.

[15] J. M. McCune, E. Shi, A. Perrig, andM. K. Reiter, "Detection of denialof-message attacks on sensor network broadcasts," in Proc. IEEE Symp.Security Privacy, 2005.

[16] W. Xu et al., "The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. ACM Int'l. Symp. Mobile Ad Hoc Netw. Comput., 2005, pp. 46-57.

[17] W. Xu, T. Wood, W. Trappe, and
Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service," in Proc. ACM Workshop Wireless Security, pp. 80-89, 200

[18] Q.Huang, H.Kobayashi, and B.Liu. "Modeling of distributed denialof service attacks in wireless networks," in IEEE Pacific Rim Conf.Commun., Computers and Signal Process., vol. 1, pp. 113-127, 2003

[19] L.Sherriff, "Virus launches DDoS for mobile phone.