International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 09 | Sep 2023 www.irjet.net p-ISSN: 2395-0072

VARIOUS TYPES OF ATTACKS ON WIRELESS NETWORKS

Ms. Rajashri B.Patil[1], Dr. Nafees.M.Kazi[2]

M.Tech.(VLSI Design)Assistant Professor, E&TC Engg.Dept.
SSBT's College of Engineering And Technolgy, Bambhori, Jalgaon, M.S. (INDIA)

Abstract:-*Wireless communication safety and security necessitates taking all precautions to avoid unwanted access to information transferred via wireless networks.*

Our new networks wireless technology is improving all the time. As convenient as wireless connections are, they have one important disadvantage in terms of health. In compared to its wired equivalents, securing communications technology presents a greater challenge[5]. Wireless attacks are done in varied manners. In the actual world, many of these attacks are linked. Here are some of the different sorts of attacks that are prevalent amongst commonly deployed networks:

Keywords— Ad-hoc, MANET, Security measures, Wormhole, WSN

1. INTRODUCTION:

Wireless communication are great for convenience because they make it much easier to move around with our devices, while still remaining connected, Unfortunately, They also make it easy for attackers to target our networks.an attackers would need physical access ro tamper with it, but with wireless network, they can do it from across the street.

1.1. Sinkhole Attack:

Wireless systems are prone to a variety of attacks like a sinkhole attack. This is a typical way to the base station that a rogue node broadcasts in order to further mislead its neighbors. The rogue node has the potential to modify data, disrupt normal operations, or even confront a slew of extra network security challenges. It's a deliberate attack on transmission. As a sink node, the node seeps into the network and draws all data packets on it. This exploit puts all network traffic at risk[12]. Sinkhole attack will change the packet flow direction by enabling selective forwarding. It pulls his neighboring nodes, in particular, to a risky node. It is possible to create the environment required to attack Wormhole. This suppresses communications in a certain region by informing neighboring clusters that it is a sink node[8]. Sinkhole attack will change the packet flow direction while permitting selective forwarding. It pulls his neighboring nodes, in particular, to a risky node.

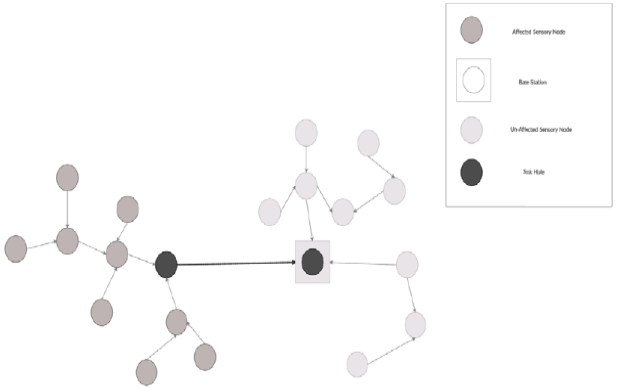


Fig 2 A Sinkhole Attack

It is possible to create the environment required to attack Wormhole. This suppresses communications in a certain region by informing neighboring clusters that it is a sink node [8,12].

1.2. Selective Forwarding Attack:

Predatory nodes refuse to assist packages in order to prevent particular packets from being exchanged further using this type of network attack. Packets may be dropped selectively or arbitrarily by the opponent.

The attacker tries to alter the Network in reaction to the packet error rate. Furthermore, there are two forms of selective forwarding:

1.2.1 Insider Attack:

Approvals of sensor nodes may be altered, or worse may end up attacking specific nodes and launch an attack on the whole network using any key. It's tough to pinpoint such an occurrence.

1.2.2 Outsider Attack:

The channel between genuine nodes is congested, and the route between both genuine nodes is stopped.

In a targeted transmission attack, malicious nodes It's a black hole that can't move any communications and just loses them to ensure they don't spread farther[7,8]. Yet, despite this failure, such a warrior is relocating the risks of

surrounding nodes and planning to seek a new path. A more subtle kind of an attack, the opponent moves packets in a methodical manner. Uninstalling or changing packages by a rival The Traffic endures, originating from a range of designated nodes, and suspicions of their wrongdoing are limited.

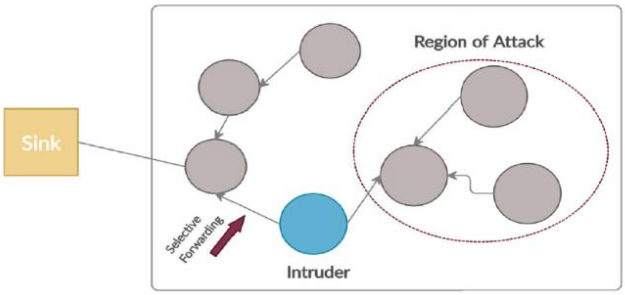


Fig 3 Selective Forwarding Attack

Because they use many types of attacks, it is very important. For example, an attacker may simply listen in on conversations, replicate node data, generating traffic purposefully. Sensor node information is disappointing. The wireless sensor network is strongly connected to their physical settings are being impacted by current protection issues.

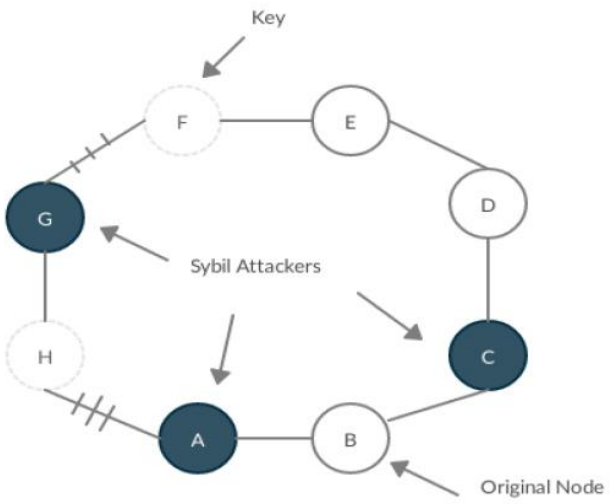


Fig 4: Sybil Attack

1.3 Wormhole Attack:

Wormhole is one of those attack in which hackers carefully position themselves within the network while listening to the network indefinitely and capturing wireless data. An attacker then gains access to part system and collects messages through a small bandwidth link. It may also replicate them over a tunnel in different areas. An attacker may deceive nodes that normally travel numerous hops from the basic station to believe they are in close vicinity in terms of hops[13,14]. This leads to a hole, if an opponent has a better path to the base station about the wormhole, leading to the traffic potentially getting attracted with the alternate routes being not as good. A wormhole attack makes use of multiple infected nodes and a private route known as a tube. When wormhole vulnerability is capitalised, the attacker funnels the packets that it receives at one point in the network, to another section of the network, and then pushes them again in the network. Because the tunnel has such a low values of latency in between nodes, that it can lead to it being picked up as an active path. This attack might start right away by tunneling every requisition to the principal node with DSR and AODV based systems. If neighboring nodes in the destination country get this Requisition packet, they need to retransmit while discarding other Requests on the path. As a result, finding routes other than the wormhole becomes highly difficult. Because it controls practically all routes identified after a wormhole, this aids the attacker in launching an attack on the infrastructure. Wormhole Attack is posing a severe danger to the WSNs. One of the most common attacks in WSNs is the wormhole attack, which involves an infected node packing packets from one network point to a remote point. Hackers in a wormhole attack may communicate quickly since they are connected directly to the other nodes in the WSN.

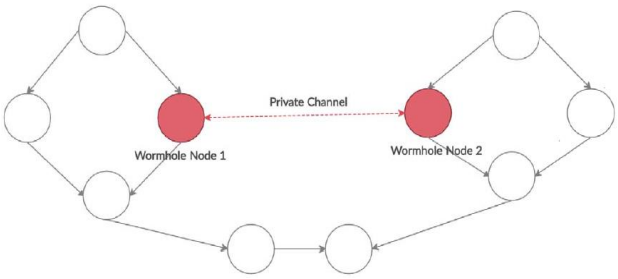


Fig 5 Wormhole Attack

2.0. Hello Flood Attack:

Many wireless sensor network algorithms allow nodes to transmit hello signals between neighboring nodes. When a node receives a message, it should assume that the transmission is inside the transmitter's radio range. In some cases, however, this idea may be inaccurate; Attacker employing ample of transmission power may convince adjoining network node to be his neighbor. A node hence persuaded to become a buddy by the invader, ends up passing False information with a high rate of transmission.[15]

Many of the neighboring nodes support broadcasting of Hello packets. The emitter is assumed to be within signal range by the node. The flood attack attempts to stop transmission

Hello messages that notify adjoining neighbor to be obtained from the nodes in this attack alert. If this is the case, this message is sent to a node, with the assumption that the transferring node is at the start, ready to make connections and join. Routing table, as a buddy. The base station, for example, communicates with all sensor nodes in a network by the path of the closest neighbor. To increase the strength of the network, send a message to all nodes. Message causes to be unsure about the message that will be sent to the neighbor's nodes. After that, both nodes take on board. If the attacker node is the starting point, the Hello message originating from the base station will be the shortest. The resource is readily monitored by network and base attackers, causing them to be cut off from the network entirely.

The Hello flood attack is a basic attack done at the network layer. These attacks are caused by a node that routes a hello packet, causing a multitude nodes making it the parental node, whether it is located in close vicinity or not. Due to the fact that both communications must be routed to this parental multiple hop, the latency is increased. Hello, packets are transmitted to a huge number of nodes throughout a big area of the network.

In the AODV protocol, there is a solution for flooding attacks where each and every node has its own blacklist, which is maintained each node. It is chosen and mentioned as to RREQ , it can transmit. Every node keeps count of RREQ requests sent by associates, and if the number of RREQ requests exceeds the previously determined threshold, the nearby nodes ID are blacklisted. RREQ from barred nodes is eventually dropped by network nodes. The only issue of the procedure is that it is time consuming. If the RREQ is not in place, the network will not be able to protect itself from flooding. The number is less than the threshold value. It has been noticed that such an attack has can affect the throughput to an extremity of 80%.

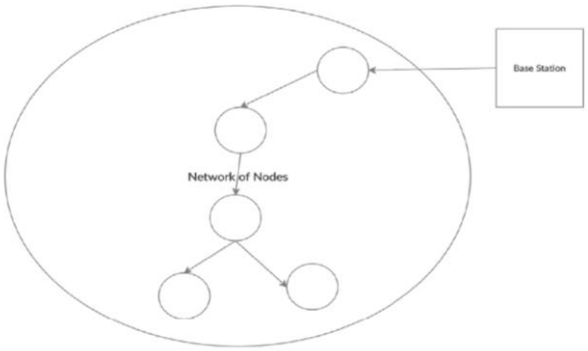


Fig 6 Victim network before attack

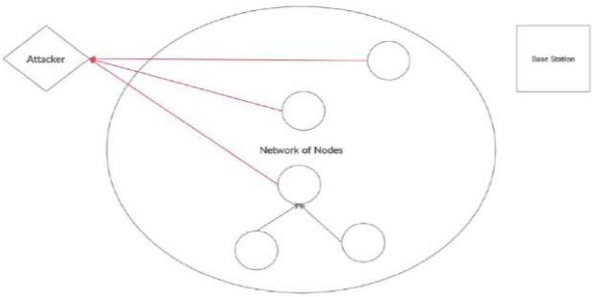
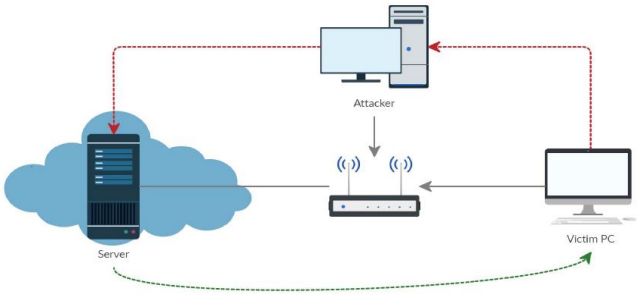


Fig 7 Victim Network after attack

2.1 Spoofed Attack:

Such attack is a result of a hostile party impersonating another user on network and then ending up targeting other network hosts. This leads to data lost or vulnerable, dissemination of malware, or giving up unauthorized access. The principal ways of such an attack are IP Spoofing, of addresses, ARP attacks, and server spoofing. TCP IP Suite protocols have many security loopholes causing both the packet's source and destination, become vulnerable to such attacks if transmitting and receiving hosts are comparable. Attacks like IP spoofing and ARP attacks can be used to launch attack on hosts in a network. Spoofing attacks employing TCP IP suite protocols can be shielded by employing firewalls having better packet checking or mechanisms verifying both parties of a message. Spoofing is a method of concealing a message or identifier connected with a reliable approved source. Spoofing dangers range from the well established phishing threats to caller ID spoofing, which is commonly used to deceive the network during email based spoofing. As well as a spoofing attack, other components of a network, such as IP address, DNS, or in some cases and an ARP service, are also attacked. Existing Solution to In order to prevent Link Spoofing Attacks, detection mechanism based on location information is utilized in combination with GPS and cryptography employing Time Stamp[16]. Each node is is secured with a time stamp and GPS based info. Each node broadcasts its positional Information making use of GPS to all the other nodes. As a result of which every node has an awareness of location information about the other nodes. Link Spoofing is done by making use of the distance amidst neighbor nodes, is checked to see whether a link can be established if there is a connection between the two nodes or not.[9]



2.2 Colluding Misrelay attack

In a colluding misrelay attack, a group of attackers cooperate in secret to change and discard routing packets in order to disrupt the usual flow of traffic. The purposes of a network is difficult to defend against this kind of attack. Detect. whenever node T sends any data, as shown in figure 9,It simply passes the data packets to Attacker 1.Packets to the attacker's second node without altering them But in case of similar packets reaching attacker , it sinks them without tinkering with these routing packets.[17]

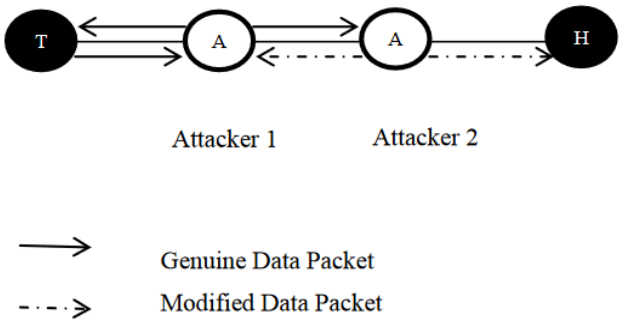


Fig 9 Colluding misrelay attack

Another form of network attack is a denial of service attack layer. The source node commences the process, as depicted in Figure 1.A request for route finding to deliver packets to the target, use RREQ a node. As indicated in the diagram, there is an attacker node that also passes RREQ to the target node; if the RREQ sent by attacker is the first to reach the target node's neighbors, and then the path for sending the packet from the attacker node to the target node is determined. Source will be routed through Attacker node. And what happens if the original RREQ transmitted by node Source reaches the node's neighbors. They will be discarded if they are a target node. As a result, the Source Node S will never be able to find the proper path. The attacker node is not included [11].

3.CONCLUSIONS

Because it is highly basic, easy to use, and more practical than other networks, the mobile ad hoc network has become extremely significant in human existence. Networks require configuration at all times, and the mobile Ad hoc network is the ideal strategy for sharing and exchanging information without the requirement for configuring an access point.

However, this strategy requires more research and efforts to provide security and limit the mobility of nodes that are labeled as "attacks

Acknowledgement

We are very much thankful to trustee Hon.Raosaheb Shekhawat, Management, Principal and HOD of E & TC Dr. M.P. Deshmukh for their moral support.

REFERENCES

[1] K. Lakshminarasimha and M. V. Subramanyam, "Diverse security intimidation and disputes in mobile adhoc networks," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 546-550, doi: 10.1109/I-SMAC.2017.8058239.

[2] S. N. Ghormare, S. Sorte and S. S. Dorle, "Detection and Prevention of Wormhole Attack in WiMAX Based Mobile Adhoc Network," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2018, pp. 1097-1101, doi: 10.1109/ICECA.2018.8474705..

[3] M. M. Singh and J. K. Mandal, "Gray Hole Attack Analysis in AODV Based Mobile Adhoc Network with Reliability Metric," 2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS), 2019, pp. 565-569, doi: 10.1109/CCOMS.2019.8821671.

[4] S. S. Kariyannavar, S. Thakur and A. Maheshwari, "Security in Mobile ADHOC Networks: Survey," 2021 6th International Conference on Inventive Computation Technologies (ICICT), 2021, pp. 135-143, doi: 10.1109/ICICT50816.2021.9358611..

[5] Boulaiche, M. Survey of Secure Routing Protocols for Wireless Ad Hoc Networks. Wireless Pers Commun 114, 483–517 (2020). https://doi.org/10.1007/s11277-020-07376-1.

[6] Abhilash K.J., Shivaprakasha K.S. (2020) Secure Routing Protocol for MANET: A Survey. In: Kalya S., Kulkarni M., Shivaprakasha K. (eds) Advances in Communication, Signal Processing, VLSI, and Embedded Systems. Lecture Notes in Electrical Engineering, vol 614. Springer, Singapore. https://doi.org/10.1007/978-981-15-0626-0_22

[7] G. Li, Z. Yan and Y. Fu, "A Study and Simulation Research of Blackhole Attack on Mobile AdHoc Network," 2018 IEEE Conference on Communications and Network Security (CNS), 2018, pp. 1-6, doi: 10.1109/CNS.2018.8433148..

[8] S. Pandey and V. Singh, "Blackhole Attack Detection Using Machine Learning Approach on MANET," 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020, pp. 797-802, doi: 10.1109/ICESC48915.2020.9155770.

[9] Talawar M.B., Ashoka D.V. (2020) Link Failure Detection in MANET: A Survey. In: Gunjan V., Zurada J., Raman B., Gangadharan G. (eds) Modern Approaches in Machine Learning and Cognitive Science: A Walkthrough. Studies in Computational Intelligence, vol 885. Springer, Cham. https://doi.org/10.1007/978-3-030-38445-6_13

[10] Khan, Burhan & Olanrewaju, Rashidah & Anwar, Farhat & Najeeb, Athaur & Yaacob, Mashkuri. (2018). A Survey on MANETs: Architecture, Evolution, Applications, Security Issues and Solutions. Indonesian Journal of Electrical Engineering and Computer Science. 12. 832-842. 10.11591/ijeecs.v12.i2.pp832-842.

[11] Islam N., Shaikh Z.A. (2013) Security Issues in Mobile Ad Hoc Network. In: Khan S., Khan Pathan AS. (eds) Wireless Networks and Security. Signals and Communication Technology. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-36169-2_2

[12] .Gagandeep, & Aashima,. (2012). Study on Sinkhole Attacks in Wireless Ad hoc Networks. International Journal on Computer Science and Engineering. 4. 1078-1084.

[13] .Ávila, K., Sanmartin, P., Jabba, D. et al. An analytical Survey of Attack Scenario Parameters on the Techniques of Attack Mitigation in WSN. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-09107-6

[14] Fu H, Liu Y, Dong Z, Wu Y. A Data Clustering Algorithm for Detecting Selective Forwarding Attack in Cluster-Based Wireless Sensor Networks. Sensors (Basel). 2019;20(1):23. Published 2019 Dec 19. doi:10.3390/s20010023

[15] Gupta A., Hussain M. (2017) Distributed Cooperative Algorithm to Mitigate Hello Flood Attack in Cognitive Radio Ad hoc Networks (CRAHNs). In: Satapathy S., Prasad V., Rani B., Udgata S., Raju K. (eds) Proceedings of the First International Conference on Computational Intelligence and Informatics. Advances in Intelligent Systems and Computing, vol 507. Springer, Singapore. https://doi.org/10.1007/978-981-10-2471-9_25

[16] He, L., Zhao, Y. Design of event-driven control strategy for spoofing attacks in wireless sensor networks. *SN Appl. Sci.* **2,** 1066 (2020). https://doi.org/10.1007/s42452-020-2854-5

[17] Kumar, Sunil and Kamlesh Dutta. "Security Issues in Mobile Ad Hoc Networks: A Survey." Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications, edited by Danda B. Rawat, et al., IGI Glo