2. Active Attack

As the attacker does a passive attack in order to get information about the wireless network, now attacker will do an active attack. Mostly, active attacks are IP spoofing & Denial of Service attack. Active attacks can be easily identified and resolved unlike of passive attacks.

1. IP Spoofing: In this attack, the unauthorized assessors are accessed by the attacker in wireless network.
2. Denial of Service Attack: in this type of attack, the attacker makes an attack on a particular target by flooding the packets to the server.

The attacker accesses the information of the AP of any active SSID. As shown in the fig 2 let's suppose a client communicating to sever over a TCP connection, then the attacker will be the man in the middle and splits the TCP connection into two separate connections. Now the first connection is from client to an attacker, and the second connection will be from the attacker to the server. So each and every request and response will be taking place between client and server via an attacker. So an attacker can steal information passing in the air between them.

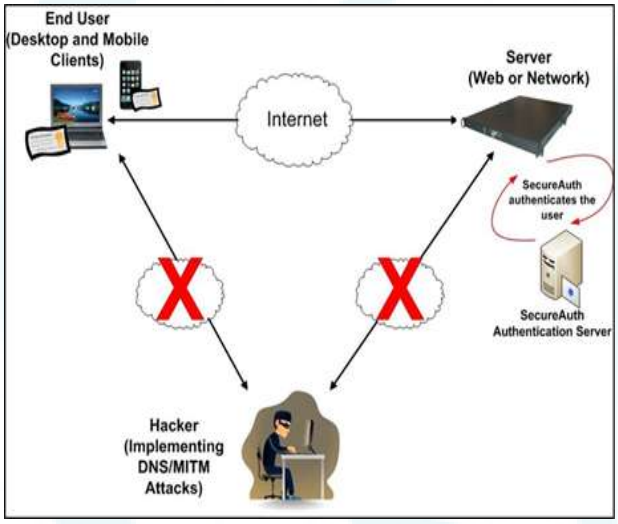

Figure 2: MITM attack scenario

3. Wireless Signal Jamming Attack

In this attack, wireless radio signals are used. An attacker may have a stronger antenna for a signal generator. First, the attacker identifies the signal patterns the target AP. Then he creates the same frequency pattern radio signals and starts transmitting in the air in order to create a signal flood in the wireless network. As a result, the target AP gets jammed; along with this the legitimate user node also gets jammed by signals. It disables the AP connection between a legitimate user of wireless network and the network itself. There can be mainly three reasons for jamming the wireless network, fun, spy, or attack.

This attack takes place when any fake or rough RF frequencies are making trouble with the legitimate wireless network operation. In some cases, such as a cordless telephone that uses the identical frequency to the wireless network, you might see some results in your wireless monitoring software or mechanism, but it is actually not a jamming of signal. It is not a very common attack, as it requires a ton of capable hardware.

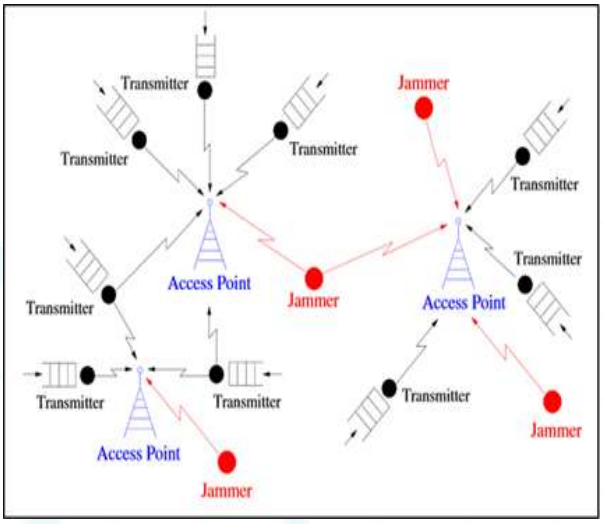

Figure 3: Access Points, Transmitters and Jammers

Above, figure 4 describes the architecture of a launched attack in which there are different access points, jammers and legitimate transmitters. The jammer's main function is making interference in the wireless communication.

2. Selective Signal Jamming

A solution to the selective jamming attack in the wireless network would be the encryption of packet to be sent. Here encryption is applied to the attributes except destination. The encryption is applied only to the attributes except destination hence during broadcasting there is no need for intermediate decryption. Each node decrypt the packet if it sent for that particular node from particular destination else it just forwards the received packet. This technique known as the Strong Hiding Commitment Scheme (SHCS) for packet hiding. This technique is based on symmetric cryptography. Therefore an attacker within the wireless network can't identify the source of incoming packet, because the packet is encrypted. Packet hiding methods make it difficult for attacker to identify its targeted node's messages [5] [6].

Jamming

How the node can identify that a particular node is a jammer? The answer is that a node which receives repeated acknowledgements for the same message or another situation is that the packet is held by a node in the network for a long time (not because of high network traffic) or if any node that violates the rules in a particular network region. Then the access point can identify that the particular node is a jammer.

By wormhole concept method, all other nodes within that network can understand information about the jammer. Next time when they send a message, they can select another path for transmitting message or transmit through the same path, but must apply the packet hiding technique. The packet can also be send through a shortest path between source and destination.

Any algorithm for finding the shortest path between a source and destination can be used. In wireless network, it is possible to find the path by analyzing the range of

nodes. Figure 4 shows a process flow, which describes the overall working of this concept when we implement it as practical.

NODE CREATION module creates the nodes in wireless network. When we create a node, it is assigned with the particular range, because for the calculation of shortest path. Nodes are mobile in nature. Among all nodes one node is selected as a jammer, then the source send packet after applying SHCS technique and transmit through shortest path between source and destination. The application of this concept arises when we require a secure communication such as emergency response operations, military.

3. Implementation

Each node is created using as separate thread, it is possible to assign each node its position, auto IP assignment, routing table updating. A jammer node is created, for applying selective jamming. A node can be repositioned to any location. A wormhole is generated automatically to migrate from one place to another using graphics API. An alarm is generated by the wormhole as packet to every node in the region. Some of the models need to considered are:

1. Network model

The network is a collection of nodes connected through wire or wireless links. Nodes can be communicating either directly or indirectly through multiple hops using both unicast or broadcast communication when needed. If there is no jammer, unencrypted communication can be performing else encrypted communications might perform. For encrypted broadcast communications, packet will send after applying packet hiding method.

2. Communication model

The source sent message to its destination either directly or indirectly. When the source gets the information about jammer, it hides the packet and sends again through the same path. A wormhole also generates and it alerts all access points in the network about the presence of jammer.

3. Adversary Model

The adversary can operate in full-duplex mode, thus being able to receive and transmit concurrently. This can be achieved with the help of multiple radios. In addition, the adversary is equipped with directional antennas that enable the reception of a signal from one node and jamming of the same signal at another. The adversary is assumed to be computationally bounded, although he can be significantly more powerful than the network devices. Solving well-known hard cryptographic problems is assumed to be time-consuming. The implementation details of the network functions at every layer of the protocol stack are assumed to be public.

4. Strong Hiding commitment Scheme (SHCS) Implementation.

The sender‘s’ has packet ‘P’ for a receiver ‘r’. The implementation of SHCS technique has following steps:

1. First apply a permutation on packet ‘P’. i.e., _1 (P).
2. Encrypt the permuted packet _1 (P) with static key ‘k’ except destination part. We obtain the commitment value, c= Ek (_1 (P)).
3. The sender broadcast this commitment value along with static key ‘k’.
4. At the receiver side, the reverse of above steps will take place.

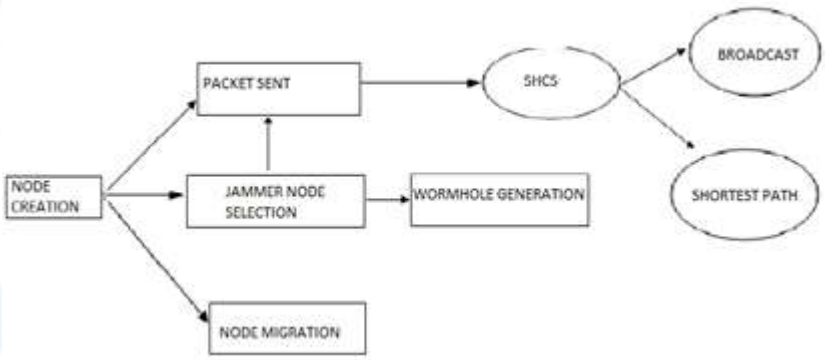

Figure 4: Process Flow

4. Performance Analysis

In packet-hiding technique on the network performance through simulations, the SCHS requires applications of permutation and one symmetric encryption at the source or sender side. At destination or receiver side, the inverse operations have to be performed. They can implement AES. These processing speeds are higher than the transmission speeds of most current wireless technologies. The wormhole-based anti-jamming technique using simulations, we can understand the frequency of number of success increases. The wormhole can effectively alert the presence of the jammer to other nodes. From this, we can understand the selective jamming attack can be effectively prevented by using packet hiding method and wormhole based anti-jamming technique. After including wormhole-based anti-jamming and transmission through shortest path, the performance of the packet hiding technique improved. It improves the performance and reliability of the wireless networks.

5. Conclusion

In this paper, a technique is proposed for sending message in wireless network even if an attacker is present along with the technique wormholes, which will alert all other nodes about the presence of a jammer. Here the packet sends through the shortest path between sender and receiver in presences of wormhole. Including wormholes and shortest path concept the performance of packet hiding method improved. This technique is very effective in emergency response operations, military, police networks etc. It improves the performance and reliability of wireless networks.

References

[1] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In *Proceedings of the second ACM conference on wireless network security*, pages 169–180, 2009.

[2] G. Noubir and G. Lin. Low-power DoS attacks in data wireless LANs and countermeasures. *ACM SIGMOBILE Mobile Computing and Communications Review*, 7(3):29–30, 2003.

[3] I. Damgard. Commitment schemes and zero knowledge protocols. *Lecture notes in computer science*, 1561:63–86, 1999.

[4] A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In *Proceedings of the Network and Distributed System Security Symposium*, pages 151–165, 1999.

[5] I. Damgard. Commitment schemes and zero knowledge protocols. *Lecture notes in computer science*, 1561:63–86, 1999.

[6] A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In *Proceedings of the Network and Distributed System Security Symposium*, pages 151–165, 1999.}

[7] Divya Ann Luke, Dr. Jayasudha. J .S Department of Computer Science and Engineering SCT College of Engineering, Trivandrum *Selective Jamming Attack Prevention Based On Packet Hiding Methods And Wormholes*.

[8] OPNET^{tm} modeler 14.5. http://www.opnet.com/solutions/network rd/ modeler.html.

[9] IEEE 802.11 standard. http://standards.ieee.org/getieee802/download/ 802.11-2007.pdf, 2007.

[10] A. Al Hanbali, E. Altman, and P. Nain. A survey of tcp over ad hoc networks. *IEEE Communications Surveys & Tutorials*, 7(3):22–36, 2005.

[11] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In *Proceedings of the IEEE ISIT*, 2007.

[12] D. Comer. *Internetworking with TCP/IP: principles, protocols, and architecture*. Prentice Hall, 2006.

[13] I. Damgard. Commitment schemes and zero-knowledge protocols. *Lecture notes in computer science*, 1561:63–86, 1999.

[14] A. Juels and J. Brainard. Client puzzles: A cryptographic countermea-sure against connection depletion attacks. In *Proceedings of the Network and Distributed System Security Symposium*, pages 151–165, 1999.

[15] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. *ACM Transactions on Sensor Networks*, 5(1):1–38, 2009.

[16] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In *Proceedings of the second ACM conference on wireless network security*, pages 169–180, 2009.

[17] R. C. Merkle. Secure communications over insecure channels. *Com-munincations of the ACM*, 21(4):294–299, 1978.

[18] G. Noubir and G. Lin. Low-power DoS attacks in data wireless LANs and countermeasures. *ACM SIGMOBILE Mobile Computing and Communications Review*, 7(3):29–30, 2003.

[19] C. Popper,¨ M. Strasser, and S. Capkun. Jamming-resistant broadcast communication without shared keys. In *Proceedings of the USENIX Security Symposium*, 2009.

[20] Website: Wireless Attacks Unleashed - InfoSec Institute.