International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 1, Jan-Feb-2022, ISSN (Online): 2395-566X

Review Paper on Attack on Under Water Mobile Ad-hoc Network

M. Tech. Scholar Uma Singh, Prof. Krishnakant Sharma
Department of Digital Communication,
Patel College of Science and Technology,Indore
umasingh137@gmail.com, Kksharma18685@gmail.com

Abstract-A Wireless networks, in compared to wired networks, are more susceptible to a variety of types of attack than wired networks. When a Wormhole tunnel is used to relay traffic from one site to another without using any cryptographic procedures that are negotiated over the network, it is referred to as the Wormhole Attack. Because of this, guarding against this attack is very challenging. In this paper, we look at the WSN concept as well as the Wormhole Attack. Following that, we'll speak about how wormhole attacks are categorised, as well as a number of the efforts now ongoing to detect and prevent them.

Keywords- Wireless Sensor Networks, Wormhole Attack.

I. INTRODUCTION

A wireless network is one that connects network nodes using wireless data links [1]. Infrastructure-based and Ad-hoc wireless networks are the two kinds of wireless networks. Each node in an infrastructure-based network has to establish and maintain intercommunication connections with other nodes through access points or base stations, but in an ad-hoc network, nodes may do so without the assistance of an existing infrastructure. With no central entity in a network, there is no infrastructure.

Ad hoc network security is problematic due to unpredictable network structure and poor connectivity between nodes. Wi-Fi networks are more vulnerable to eavesdropping and interference assaults. There are many small sensor nodes in MANET's wireless sensor network, which are constantly monitoring the surroundings. As a result of sensor nodes performing a variety of functions like as signal calculation, processing, and network self-configuration, the network's coverage and scalability may be expanded.

A WSN is made up of a large number of Sensor Nodes spread out across a large region. Each of these microscopic sensors has the ability to detect, analyse and transfer data over a radio frequency channel. "Figure 1" shows the four main components that make up each Sensor Node (SN): a sensor module; a processor module; a transceiver module; and a power module. A location locating system, a power generator, and a mobilise are all optional extras that may be included according on the application [16]. Both the sensors and the Analog to Digital Converters make up the Sensing unit (ADCs). After being converted to digital, the ADC sends the transformed analogue signals on to a processing unit where they are processed.

To make the SN work with the other SNs, it uses the processing unit, which has a tiny storage unit connected with it. To connect a node to the network, a transceiver device is used. A power rummage unit, such as solar cells, may assist the power unit. SN has a few components that are dependant on their application. There are many nodes in the network, each of which is capable of sensing and communicating with its peers and an external BS. If the BS is mobile, then it can connect to the Internet, where the reported data may be accessed, or it can be a fixed node that connects directly to WSN communications infrastructure.

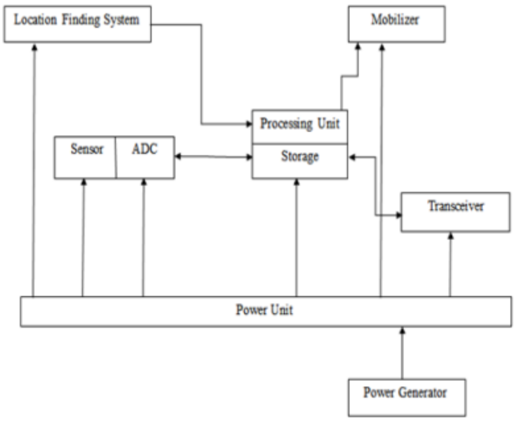


Fig 1.Components of Sensor Node.

Sensor nodes in WSNs are often located in outlying locations, making them ideal for WSNs to operate in. A single sensor node's dependability and accuracy are poor owing to the stringent resource limitations of these nodes. As a result, data collection and processing must be done in collaboration across several nodes [3]. Wireless Sensor Networks are vulnerable to security threats because of the nature of the transmission medium (broadcast nature).

The nodes of WSNs, on the other hand, are often located in hazardous or hostile environments, with no physical safeguards to keep them safe [17]. There are two sorts of attacks: active and passive. As part of an active attack, the attacker keeps tabs on the communication channel and listens in on it.

The following are examples of active attacks:

- **Sensor Network Routing Attacks:** A Review Corrupted Messages Malfunction of a Node Intimidation and Threats There is an issue with one of the nodes. DoS (Double-click) Attacks Attacks on the Node Replication Service Node that isn't there 9. Subversion Node
- **Passive attack** occurs when an unauthorised party keeps tabs on and listens in on the communication channel. Any intrusion on one's privacy is done passively [4].

II. WORMMHOLE ATTACK

If two or more malicious attackers conduct a Wormhole Attack, each of them receives data packets from a different network site via a wormhole tunnel and then sends them to a different place, creating the appearance that the two remote nodes are in close proximity. Allow me to explain by using a multi-hop network [18]. As demonstrated in, an ad hoc network may include nodes that are either mobile or static (Figure 2).

The circle denotes a network node or user, while the line symbolises the link between the two nodes shown in this diagram. Let's say node 2 wishes to send a message to node 9 through node 9. But before sending message, source node will pick a way to transmit message by utilising Predefined Routing Protocols which may be Proactive or Reactive in nature. Instead of using reactive routing protocol, which does not have any routing table, node 2 (the source node) will need to lookup routing information before sending any messages since it does not have a routing table because it employs proactive routing (i.e. proactive forwarding).

When using the Reactive Routing Protocol, the sender broadcasts an RREQ message to all of its nearby neighbours within a single hop of the destination. To be sure, every node that receives an RREQ message double-checks whether or not the message is meant for them before sending a reply message with route information back to the sender using the same route that the original request message used to reach the node in the first place [19].

Due to the limited bandwidth and power of nodes in an ad hoc network, routing systems often choose the route that is the shortest possible. Because of this, we may say that node 2 sends the message to nodes 2, 5, 6, 8, and 9. The intermediary nodes in the network serve as message routers, sending messages to their intended destinations. Assume the ad hoc network described above has been compromised by a wormhole. When node 2 and node 9 are attacked by two different attackers, they will be linked by a high-speed bus [20]. Although an attacker may not be a member of the network, the open nature of an ad hoc network means it may still overhear messages. When one of the attackers gets a message from a node in the attacker's vicinity, the other attacker in the network retransmits the message.

As a result, nodes 2 and 9—where the attackers are hiding—are led to assume that they are both directly linked. As a result, the attacker creates a fictitious connection in a network, say between nodes 2 and 9. Node 2 will transmit a message to node 9 through a wormhole tunnel as a result of this fictitious connection. As a result, the route is now 2- 9. Node 2-9 has replaced all previous routes in the network that went via nodes 2-5-6- 8-9.

Due to this, the vast majority of communications in the network are routed via the wormhole, placing the attacker well ahead of all other nodes [21]. Even if the attacker does not have cryptographic keys, he or she may use the bogus connection to store all communications that travel over it and utilise that data to evaluate content. In addition, an attacker has the potential to remove or change any node's message at any moment, which has an impact on security's availability and integrity.

Consequently, further assaults such as eavesdropping, congestion, packet loss spoofing and so on [5] are dodged by the Wormhole attack. It's one of the many DDoS assaults that don't need the attacker to have any prior understanding of cryptography. That's why a wormhole assault might go undetected for a long time. The launch of it can be done by a minimum of two nodes. Packets are tunnelled from the source to the destination node over wormhole links in two-ended wormholes, and the destination sends them back after they've received them.

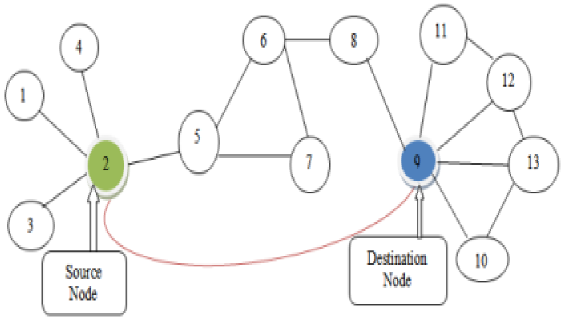


Fig 2. Wormhole Attack in Ad-hoc Network.

1. Wormhole Attack Classification:

Open, half-open, and closed wormhole attacks may be distinguished by whether or not the attackers can be seen in the routing and packet forwarding behaviour of wormhole nodes, as well as whether or not they want to conceal or reveal their identities. The source node is S, and the destination node is D in the following examples. M1 and M2 indicate malicious nodes.

1.1 Wormhole that's been opened: In this attack technique, the attacker adds a self-included header to the packet once the route is discovered. Malicious nodes in the route are known to the network nodes, yet they act as though they are neighbours with the legitimate nodes. According to (Figure 3), nodes S and D on the travelled route are visible, as well as the endpoints of wormholes M1 and M2, but nodes A and B on the destination path are concealed.

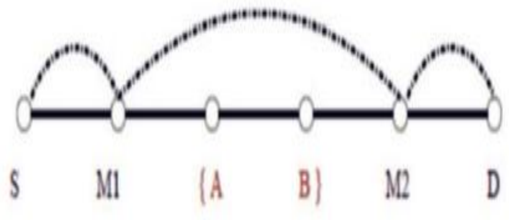


Fig 3. Open Wormhole Attack.

1.2 Wormhole with One Half Open: In this attack technique, the attackers don't do anything to the data in the packets they intercept. They just rebroadcast the packet after tunnelling it from one side of the wormhole to the other. In Figure 4, a malicious node M1 near the source (S) may be seen, but the second end (M2) is concealed, resulting in a route of S-M1-D for the packets delivered by S to D.

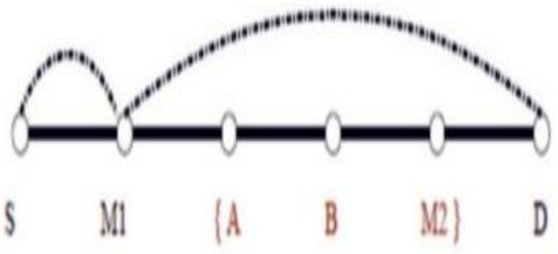


Fig 4. Half Open Wormhole Attack.

1.3 Wormhole that has been sealed off: All intermediary nodes (M1, A, B, and M2) on the route from S to D remain anonymous in this mode. Source and destination are always only a hop apart from one other in this game. As a result, people establish fictitious neighbours.

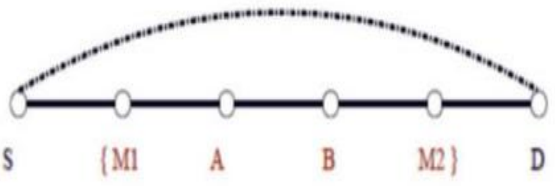


Fig 5. Closed Wormhole Attack

Based on the techniques used for launching attack, Wormhole Attack can be classified into five categories:

1.1.1 Packet Encapsulation: Wormhole Encapsulation is used in the attack to break up the routing information before sending it to the cooperating node. Due to the fact that the tunnel is formed through standard network nodes, no extra tools are required in this wormhole attack. At least two attackers are required. During traversal, the real hop count does not rise in this attack type [22]. The encapsulation-based wormhole attack (Figure 6) illustrates the vulnerability of routing systems that employ hop count as a route selection. Consider that in the presence of two malicious nodes M1 and M2, nodes S (source) and Sink (destination) attempt to find the shortest route between them. This happens because M1 receives the route request message from Node S, wraps it, and then passes it on to M2 through the path that exists between M1 and the second node, the destination node (E-F-G). Node M2 retransmits the packet in the same condition as before. No additional hops are required to transport RREQ between M1 andM2 due to its encapsulation (E-F-G). A second RREQ goes from S to sink along the route that includes nodes A-BC at the same time [23]. It seems as if the second path (S-M1-M2-Sink) is just three hops long, but in fact, it is really six hops long. Now, there are two possible ways from S to Sink (M1-E-F-G-M2-Sink). Since the second route looks to be the quickest, the sink opts towards it.

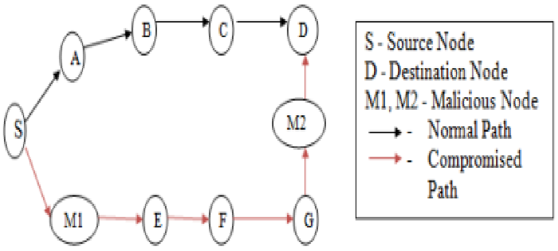


Fig 6. Wormhole Attack Using Packet Encapsulation.

1.1.2 High-Quality or Out-of-Band Channel Wormhole: An attacker employs a long-range wireless or cable connection in this scenario. Attackers use high-powered signals that are not accessible to the normal nodes in the network to broadcast route request messages, which then creates a tunnel from their point of origin to their point of destination via themselves [24]. For this assault to be successful, you'll need specific hardware. Here is an example of a top-notch channel-based assault (Figure 7). Malicious sensor nodes M1 and M2 are connected through an out-of-band channel. It is reasonable to suppose that an RREQ is sent from the source (S) to the sink (S), with the assumption that S's neighbours, A and M1, are receiving it. RREQ is tunnelled from Node M1 to M2, which broadcasts the packet to its neighbours, including the sink node, if it is present. RREQs are sent to sink node (S-M1-M2-Sink) and sink node chooses amongst them because the shorter and quicker path is preferred by sink node.

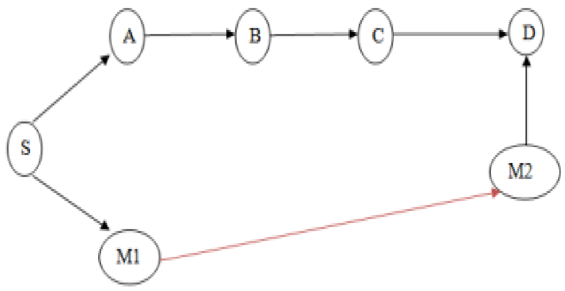


Fig 7. Wormhole Attack using tunnel between two nodes.

1.1.3 High-Power Transmission Capable Wormhole: To carry out this form of wormhole attack, the network must have at least one rogue node with strong transmission power, which can connect with other nodes across great distances. This request is broadcast loudly by every rogue node that gets an RREQ. There are several nodes that will rebroadcast the RREQ in order to reach their target. By using this technique, the malicious node enhances its chances of being included in the routes formed between the source and the destination even if no other malicious nodes are involved [7].

1.1.4 Packet Relay Wormhole: One or more malicious nodes may carry out this sort of attack. In this scenario, a rogue sensor node sends data packets to two distant sensor nodes, tricking them into believing they are neighbours. Fake neighbours may be produced in this manner. Replay-Based Assault is another name for this kind of attack. Figure 9(a) shows two nonneighboring sensor nodes A and B with a malicious neighbour node M1 (Figure 9(a)). Sensor nodes A and B may be tricked into thinking they are neighbours by using Node M1 to relay packets between them. (Figure 9(b)) shows that if many malicious sensor nodes work together, then sensor nodes that are several hops apart from each other may be attacked [7].

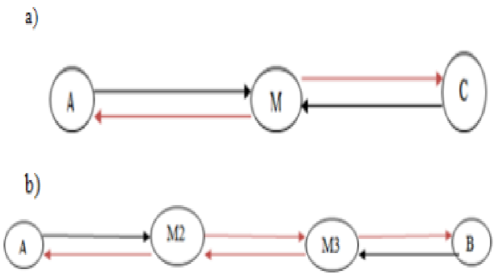
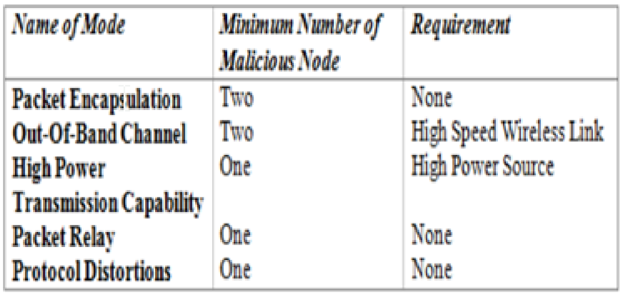


Fig 8. Replay Based Attack Using (a) one malicious node or (b) two malicious node.

1.1.5 Protocol Distortion Wormhole: A single rogue node uses a distorted routing protocol to try to attract network traffic. Since this attack has no significant impact on network routing, it may be safely dismissed as non-harmful. Also referred to as "rushing assault" in literary works [3]. By exploiting protocol distortion, routing systems that focus on "shortest latency" rather than "smallest hop count" run the danger of being compromised by wormhole attacks.

Table 1. Summary of Wormhole Attack Modes.



Name of Mode	*Minimum Number of Malicious Node*	*Requirement*
Packet Encapsulation	Two	None
Out-Of-Band Channel	Two	High Speed Wireless Link
High Power Transmission Capability	One	High Power Source
Packet Relay	One	None
Protocol Distortions	One	None

2. Detection of Wormhole Attack:

It's difficult to identify wormhole attacks because hostile nodes send out data packets that aren't harmful. Most wireless sensor network routing algorithms include lightweight cryptographic techniques to prevent unwanted nodes from injecting bogus data packets into the network, too [25]. Since the data packets are replayed in wormhole attacks, all cryptographic checks are bypassed. Most of the time, protocols used synchronised clocks, directional antennas, or positioning devices to accomplish their goals.

Mobile Ad-hoc Network wormhole attacks may be detected using a variety of methods.

2.1 Basedon Special Hardware Hu, Perrig and Johnson [9] proposed a mechanism, named packet leashes.

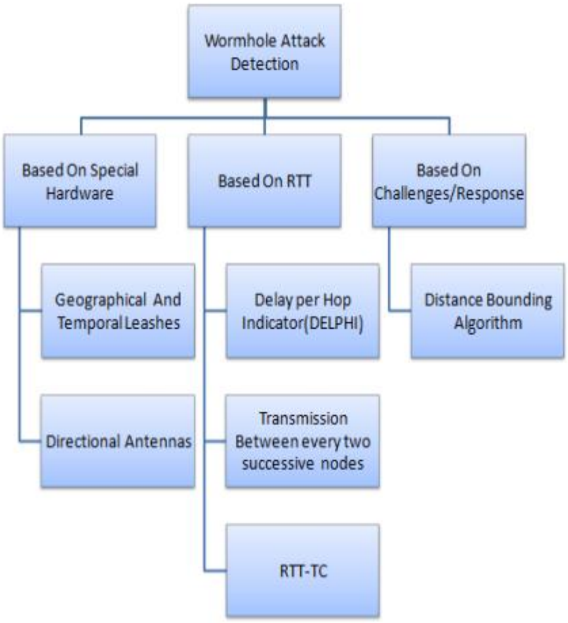

Wormhole Attack Detection
Based On Special Hardware
Based On RTT
Based On Challenges/Response
Geographical And Temporal Leashes
Delay per Hop Indicator(DELPHI)
Distance Bounding Algorithm
Directional Antennas
Transmission Between every two successive nodes
RTT-TC

Fig 9. Classification of Wormhole Attack Detection Mechanism.

It prevents packets from travelling outside the range of transmission. The book divides leashes into two categories: geographical and temporal (or time). To identify the neighbour relationship in Geographical Leashes, each node has a clock that is only weakly synced with the network's overall clock. Node attaches its current location and transmission time to a packet before transmitting it [26]. Nodes on the receiving end calculate distances and travel times based on packets that have been received by them. To determine whether or not a packet has travelled through a wormhole, the receiver must employ distance information. Geographic leash building necessitates the use of a Global Positioning System (GPS) since each node must be aware of its own position.

All nodes in a Temporal Leashes network must have their clocks perfectly synced. The receiver will then compare the received time to the packet's associated sending time. The arrangement is complicated and expensive since it requires specialised hardware to provide reliable time synchronisation between the nodes. This technique ignores congestion since processing and queuing delays are deemed insignificant by it [7]. It does not rely on GPS information, but instead uses a clock that is precisely synced across all nodes [5]. Directional antennas were proposed by Hu and Evans [9].

For this reason, it's possible to send packets in one way and receive them in the other direction even in ad hoc networks that lack wormhole links. As a result, a neighbourhood relationship can only be established when the directions line up in pairs. It necessitates the use of a directional antenna on each node [5] A wormhole detection system based on zone-based antennas has been suggested. Zones are numbered 1 to N clockwise around each sensor, with zone 1 pointing east at the start. This strategy is based on the transfer of directional information between nodes cooperating. First-time signal reception by a sensor node gives the inexact signal direction and allows the sensor to identify the foreign sensor node based on its zone [27]. After then, the sensor node works with the other nodes in the network to verify the validity of the unknown node [6]. Unlike other methods, this one doesn't need any kind of position or time synchronisation information from the nodes in the network. However, it does have certain drawbacks, such as antenna directional problems [7].

2.2 This approach can identify both hidden and disclosed wormhole assaults since it is based on RTT and King-Shan Lui's Delay per Hop Indicator (Delphi) [10]. A wormhole attack is detected in Delphi by measuring the latency between the sender node and the receiver. To identify wormhole attacks, the hop count and delay information of disarranged pathways are gathered and the delay per hop value is calculated. Node-to-node communications are referred as as hops. In a typical case, the packet's perception of delay in propagation should be consistent from hop to hop. In wormhole attacks, on the other hand, the latency is unacceptably great because of malicious nodes in the way. A path's latency per hop determines whether or not a wormhole assault would succeed. A wormhole may be found by comparing the delay per hop numbers of the different disarranged pathways. Wormhole attacks cannot be found using this technique. Because each node has the ability to vary the route length, wormhole nodes might do it in such a manner that they would be impossible to identify [7].

According to Tran et.al [11], wormhole assaults may be detected during the route building stage by measuring transmission time between every two sensor nodes along the constructed way. For example, the time it takes to go via a wormhole is far longer than the time it takes to travel between two genuine real neighbours who are within radio range of one another. Wormhole assaults disrupt the route-setting process before doing any damage. TTM doesn't need any additional gear. However, since only delays are taken into consideration, two verified neighbours with connection congestion are ignored, resulting in a significant false alert rate [7]. On the basis of topological comparison and round trip time measurement, Alam and Chan [12] created the RTT-TC method. By employing RTT measurements, this approach suspects a wormhole assault and then eliminates any real neighbours from the suspect list using topological comparison.

The Neighbor List in this approach is divided into two sections: TRST and SUS, which stand for Trusted and Suspected, respectively. If the RTT between two nodes is three times more than their current RTTavg, they may be connected via a wormhole tunnel. These two nodes' NodeIDs are added to their corresponding SUS lists if a wormhole tunnel is found [28]. When a source node discovers a non-empty SUS list, the wormhole detection mechanism is triggered. The SUS component of a node's Neighbor List contains all the nodes a node might possibly request packets from. The receivers then respond with their TRST list to the source, which is compared to the source's TRST list to see whether the connection has been compromised by the wormhole. Since there is no clock synchronisation required, this technique offers greater detection rates but higher message overhead [7].

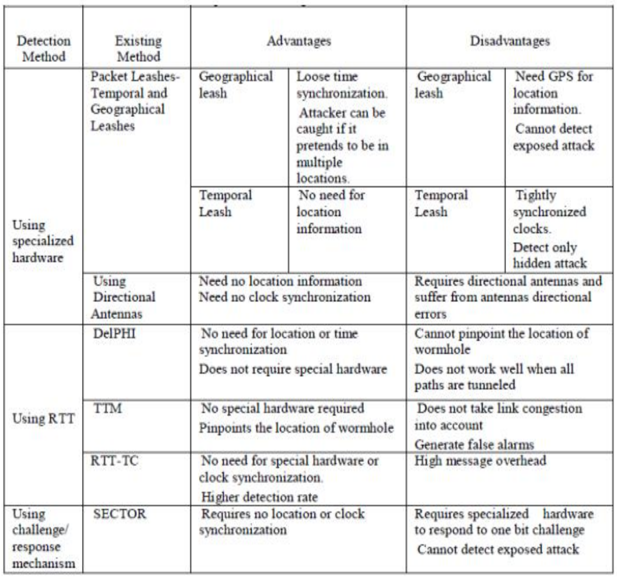
2.3 As a result of the problems encountered and the solutions adopted Using specialised hardware, Capkun et al. [14] developed the SECTOR protocol. The basic notion behind the protocol is that the speed at which data is sent between two sensors nodes may be used to determine how far apart they are. Using (mutual authentication with distance bounding) MADB protocol, the proposed approach does not need any clock synchronisation or position information [29]. The MADB protocol makes it possible for nodes to find out how far apart they are before they meet. Brands and Chaum [15] were the first to propose distance-bounding techniques. Using this approach, one side might set a feasible upper limit on the distance between them [30]. The first party may determine the distance to the other party's upper limit by measuring the time it takes to send out challenges and get answers. Brands and Chaum's distance-bounding methodology was updated by Capkun et al. The protocol makes it possible for both parties to know exactly how far the other party is away at the same time. It is also assumed that all parties have a symmetric key, which is why the nodes are created before the distance-binding protocol is executed.

III. CONCLUSION

We have described in full the wormhole attack in this work, including the many types. This attack's effects have been examined in detail, as well as the many strategies employed to prevent or lessen it. There have been several solutions proposed for assaults of this sort on the network.Each of these approaches has pros and cons.

Disadvantages come in the form of requirements (which might be either impracticable, expensive, or otherwise influence other elements of the ad hoc network like mobility or decentralisation) or their impact on overall performance of the network (by increasing load on network). Further research on the effects of this assault is essential if the threat posed by it is to be contained.

Table 2. Summary and Comparison of existing wormhole detection mechanism.



Detection Method	Existing Method	Advantages		Disadvantages	
Using specialized hardware	Packet Leashes-Temporal and Geographical Leashes	Geographical leash	Loose time synchronization. Attacker can be caught if it pretends to be in multiple locations.	Geographical leash	Need GPS for location information. Cannot detect exposed attack
		Temporal Leash	No need for location information	Temporal Leash	Tightly synchronized clocks. Detect only hidden attack
	Using Directional Antennas	Need no location information Need no clock synchronization		Requires directional antennas and suffer from antennas directional errors	
Using RTT	DelPHI	No need for location or time synchronization Does not require special hardware		Cannot pinpoint the location of wormhole Does not work well when all paths are tunneled	
	TTM	No special hardware required Pinpoints the location of wormhole		Does not take link congestion into account Generate false alarms	
	RTT-TC	No need for special hardware or clock synchronization. Higher detection rate		High message overhead	
Using challenge/ response mechanism	SECTOR	Requires no location or clock synchronization		Requires specialized hardware to respond to one bit challenge Cannot detect exposed attack	

REFERENCES

[1] http://en.wikipedia.org/wiki/Wireless_network.Wireless Network - Wikipedia, Retrieved March 4, 2015.

[2] Debnath Bhattacharyya, et al, “A Comparative Study of Wireless Sensor Networks and Their Routing Protocols”, In MDPI-2010, Basel, Switzerland, Nov. 2010.

[3] Shukla, M., Joshi, B.K. & Singh, U. Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. Wireless Pers Commun 121, 503–526 (2021).

[4] Dr.G.Padmavathi and Mrs. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks,” In Proceeding of the International Journal of Computer Science and Information Security (IJCSIS), Vol. 4, No. 1 & 2, 2009.

[5] Shaishav Shah and Aanchal Jain, “Techniques For Detection & Avoidance Of Wormhole Attack In Wireless Ad Hoc Networks”, In Proceeding of the International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 10, December-2012.

[6] Ali M, et al, “Mitigation of Wormhole Attack in Wireless Sensor Networks”, In Proceeding of the Atlantis Press 2012.

[7] Shukla, M., Joshi, B.K. & Singh, U. Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET. Wireless Pers Commun 121, 503–526 (2021).

[8] Maria Sebastian and Arun Raj Kumar P. “ A Novel Solution for Discriminating Wormhole Attacks in MANETs from Congested Traffic using RTT and Transitory Buffer”, In Proceeding of the I. J. Computer Network and Information Security, 2013.

[9] Yih-Chun Hu, Adrian Perrig, and David B. Johnson— “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks”, In Proceedings of the IEEE Conference on Computer Communications (Infocom), 2003, p. 1976-1986.

[10] L.Hu and D. Evans. “Using directional antennas to prevent wormhole attacks,” Proceedings of Network and Distributed System Security Symposium, pp. 131−41, Feb. 2004.

[11] Hon Sun Chiu and King-Shan Lui, “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”, International Symposium on Wireless Pervasive Computing (ISWPC), 2006.

[12] T Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Sungyoung Lee, and Heejo Lee,“ Transmission timebased mechanism to detect wormhole attack” ,In Proceedings of the IEEE Asia-Pacific Service Computing Conference, Dec. 11-14, 2007, p. 172-178.

[13] Mohammad Rafiqul Alam and King Sun Chan, “RTTTC: A Topological Comparison Based Method to Detect Wormhole Attacks in MANET”, 12th IEEE International Conference on Communication Technology, 2010, p. 991-994.

[14] S. Capkun, L. Buttyán, and J.P. Hubaux, “SECTOR: Secure tracking of node encounters in multi-hop wireless networks,” Proceedings of the 1st ACM workshop on Security of ad-hoc and sensor networks (SASN 03), pp.21−32, Oct. 2003.

[15] S. Brands and D. Chaum, "Distance-bounding protocols," In Theory and Application of Cryptographic Techniques, pp. 344−59, 1993

[16] N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/IC4.2015.7375649.

[17] U. Singh, M. Samvatsar, A. Sharma, and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570908.

[18] U. Singh, M. Shukla, A. K. Jain, M. Patsariya, R. Itare, and S. Yadav, Trust Based Model for Mobile Ad-Hoc Network in Internet of Things, vol. 98. 2020.

[19] M. Muwel, P. Mishra, M. Samvatsar, U. Singh, and R. Sharma, "Efficient ECGDH algorithm through protected multicast routing protocol in MANETs," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212743.

[20] U. Singh, V. Vankhede, S. Maheshwari, D. Kumar, and N. Solanki, Review of Software Defined Networking: Applications, Challenges and Advantages, vol. 98. 2020.

[21] U. Singh, M. Samvatsar, A. Sharma, and A. K. Jain, "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570908.

[22] V. K. Saurabh, R. Sharma, R. Itare, and U. Singh, "Cluster-based technique for detection and prevention of black-hole attack in MANETs," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212712.

[23] A. S. Chouhan, V. Sharma, U. Singh, and R. Sharma, "A modified AODV protocol to detect and prevent the wormhole usingh using hybrid technique," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212740.

[24] L. Baghel, P. Mishra, M. Samvatsar, and U. Singh, "Detection of black hole attack in mobile ad hoc network using adaptive approach," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212741.

[25] N. Arya, U. Singh, and S. Singh, "Detecting and avoiding of worm hole attack and collaborative blackhole attack on MANET using trusted AODV routing algorithm," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/IC4.2015.7375649.

[26] A. Sharma, D. Bhuriya, and U. Singh, "Secure data transmission on MANET by hybrid cryptography technique," in IEEE International Conference on Computer Communication and Control, IC4 2015, 2016, doi: 10.1109/IC4.2015.7375688.

[27] S. Singh, A. Mishra, and U. Singh, "Detecting and avoiding of collaborative black hole attack on MANET using trusted AODV routing algorithm," in 2016 Symposium on Colossal Data Analysis and Networking, CDAN 2016, 2016, doi: 10.1109/CDAN.2016.7570906.

[28] R. Verma, R. Sharma, and U. Singh, "New approach through detection and prevention of wormhole attack in MANET," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212719.

[29] D. Wagh, N. Pareek, and U. Singh, "Elimination of internal attacksfor PUMA in MANET," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212710.

[30] R. Parihar, A. Jain, and U. Singh, "Support vector machine through detecting packet dropping misbehaving nodes in MANET," in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212711.