International Journal of Scientific Research & Engineering Trends
Volume 8, Issue 5, Sep-Oct-2022, ISSN (Online): 2395-566X

Review of Wormhole Attack on Mobile Ad-hoc Network

M.Tech.Scholar Ms. Babita Kumari, Prof. Dr Rakesh Sharma
Department of Computer Science Engineering,
Sri Aurobindo Institute of Technology, Indore
Email- babita271996@gmail.com, rakesh.nsharma@sait.ac.in

Abstract- WSNs are unstable because to the wireless nature of communication since any attacker with the desire to steal the data may do so by inserting rogue nodes into the network. Attackers may carry out this by launching attacks such as wormhole, floods, grey hole, and others. The goal of routing protocols is typically to determine the shortest route between a source and a destination node. The hop count is used as a statistic to calculate the journey length. The wormhole attack, one of the several above-described attacks, is risky since it builds a tunnel by bypassing a few nodes in between them. The hop length is automatically decreased by the tunnel, resulting in a short route between the source and destination nodes. This article provides a concise overview of the methods or strategies for the identification and defence against wormhole attacks.

Keywords- WSN, Wormhole attack, Flooding attack, Hop count, MANET.

I. INTRODUCTION

Wireless Sensor Network is a promising platform for a variety of application areas such as environmental monitoring, battlefield surveillance, and homeland security domains and it is attracting many researchers to work on various problems related to this domain. The coverage, connectivity and energy related issues are very important in WSNs. However, WSNs appears that they are more prone to attacks than wired networks. In applications like military, without security, the use of Wireless Sensor Network in any application would result in disastrous consequences. The wireless nature of communication makes wireless sensor networks unreliable as any attacker with intent to steal the data can do so by deploying malicious nodes in the network. The routing protocols used to find a route from source to destination and then for transfer of data lack security measures. So it becomes easy for the attackers to attack the network, which can be done

by launching black hole attack, wormhole attack, flooding attack, Gray hole attack etc. Security allows Wireless Sensor Networks to use to maintain integrity of data and availability of all messages in the presence of resourceful adversaries. The main objective of confidentiality and authenticity is expected in sensor networks to safe guard the information travelling among the nodes of the network or between the sensor nodes and the sink node from disclosure.

Wormhole attack is a great threat to sensor networks since, this type of attack will not require compromising a wireless sensor in the network instead; it could be performed even at the starting phase during the sensors initializes to identify its neighbouring information. The Wormhole attacks are very difficult to stop since routing information given by a sensor node is very difficult to check. The wormhole attack is possible even when the attacker has not compromised with any hosts nodes and even if all communication provides confidentiality and are authenticated. This paper presents brief survey about the schemes or techniques related to the detection and prevention of the wormhole attacks in Section II.

II. VARIOUS ATTACKS ON WSN AND MANET

1. Black Hole:
The attacker node drops all the messages it receives from the genuine nodes.

2. Selective Forwarding:
In a selective forwarding attack, malicious nodes could prevent forwarding certain messages or even discard them; consequently, these messages would not propagate through the network.

3. Sinkhole Attacks:
In a sinkhole attack, the goal of the attacker is to attract all the traffic to a certain area or the network through a compromised node, by creating a sinkhole.

4. Sybil Attacks:
In a Sybil attack, a node presents multiple identities to the rest of the nodes. Sybil attacks are a threat to geographical routing protocols, since they require the exchange of coordinates for efficient packet routing. Ideally, a node only sends a set of coordinates, but under a Sybil attack, an adversary could pretend to be in many places at once or have multiple identities.

5. Hello Flood Attack:
An attacker uses high-powered transmitter to trick a large area of nodes into believing they are neighbours of that transmitting node. If the attacker intentionally broadcasts a false superior route to the base station, all of these nodes

will choose to transmit through the attacking node, despite many being out of radio range in reality. The intruder can broadcast a powerful advertisement to all the nodes in the network and hence, every node is likely to choose the adversary as the cluster-head. The adversary can then selectively forward information to the base-station or modify or dump it.

6. Denial of Service (DoS):
A Denial of Service attack in sensor networks and networks in generalise defined as any event that eliminates the network's capacity to perform its desired function. DoS attacks in wireless sensor networks may be carried out at different layers like the physical, link, routing and transport layers.

7. Wormhole attacks:
In wireless sensor, network when sender node sends a message to another receiver node in the network. Then the receiving node tries to send the message to its neighbouring nodes. The neighbour sensor nodes assume that the message was sent by the sender node (this is normally out of range), so they try to forward the message to the originating node, but this message never comes because it is too far away. Attacker can easily launch wormhole nodes in WSN without any information about the network. Wormhole attack is a great threat to sensor networks since, this type of attack will not require compromising a wireless sensor in the network instead; it could be performed even at the starting phase during the sensors initializes to identify its neighbouring information. In wormhole attack, attacker node captures the packet from one end and sends it to another end node by a tunnel using high transmission power. The Wormhole attacks are very difficult to stop since routing information given by a sensor node is very difficult to check. The wormhole attack is possible even when the attacker has not compromised with any hosts nodes and even if all communication provides confidentiality and are authenticated. There are various modes of attacks to initialize this attack and these are High Transmission Power, Packet Relay, Out of Band Channel and Packet Encapsulation.

III. LITERATURE SURVEY

Varshaet.al., Presented efficient method to detect a wormhole attack called modified wormhole detection AODV protocol (MAODV). Based on number of hops and delay of each node in different paths from source to destination wormhole attack is detected. It compares the delay per hop of every node in the normal path and a path that is under wormhole attack, finds that delay per hop of a path that is wormhole attack is larger in comparison of normal path. Advantages of this method are that it requires no special hardware and it do not require positioning system and clock synchronization. Shortcoming is that when all the paths are wormhole affected this method does not work well [1].

Harleenkaur, Neetu Gupta Proposed technique for protection AODV from wormhole attack in WSN. This paper proposed detection and isolation of the wormhole. [19] The methodology is to discover wormhole in the route suggest by AODV protocol by using data trackers in which wormhole detection is performed between all the possible combination of nodes and decision will be taken on the basis of each and every possible combination If wormhole is detected in any of possible combination then whole suggested path is consider to be as wormhole effect path elsewhere if all the combination is wormhole free then path is considering to be as worm hole free path [2].

Nishant Sharma Proposed a Location Based Approach to Prevent Wormhole Attack in Wireless Sensor Networks. The proposed scheme detects and further prevents wormhole attack in wireless sensor networks. The proposed scheme uses location information of nodes in network and uses Euclidean Distance Formula to further detect and prevent wormhole attack and make the communication between sensor nodes more secure and reliable [3].

S Subhaet.al. Proposed Message Authentication and Wormhole Detection Mechanism in Wireless Sensor Network. Proposed system to find the wormhole attack by using the RTT [20] between two successive nodes. Then worm hole attack is a malicious node tunnels message received in one part of the network over a low latency link and replay them in a different part. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole [4].

Rakhil R. Proposed a new idea for neighbour discovery process by introducing pre handshaking strategy. A pre handshaking strategy will analyze the activities of neighbouring node and help to reduce collision during data transmission and help to reach each packet to the correct receiver without dropping. The wormhole attack is one of the most severe attacks in WANET which can significantly disrupt the communications across the network. Moreover, it is a type of replay attack and launched by one or more malicious node. The challenges of this attack is hard to defend against and easy to implement. This paper presents a novel approach for neighbour discovery and mitigating the effect of wormhole attack. The proposed system does not require any special hardware or expensive mechanisms added to the wireless nodes [5].

ParmarAmishaet. al., Proposed the techniques dealing with wormhole attack in WSN are surveyed and a method

is proposed for detection and prevention of wormhole attack. AOMDV (Ad hoc On demand Multi path Distance Vector) [21] routing protocol is incorporated into these methods which is based on RTT (Round Trip Time) mechanism and other characteristics of wormhole attack. As compared to other solution shown in literature, proposed approach looks very promising. NS2 [22] simulator is used to perform all simulation [6].

Manish M Patel Proposed two Phase Wormhole Detection Approach for Dynamic Wireless Sensor Networks. They assume that a malicious entity can launch many kinds of wormhole attacks. It is able to launch high-speed low-latency tunnel. One malicious node records packet at one location and replays them to second malicious node at the location which is far away through out of band tunnel. The malicious node drops packets without forwarding them to the next node. In such situation, base station is not able to receive any information from the target area. The malicious entity can also modify the data packets [7].

Manish Patel and Dr. Akshai Aggarwal Proposed a wormhole [23] detection protocol that is based on neighbourhood and connectivity information. Performance analysis shows that the proposed approach can effectively detect wormhole attack with less storage cost. Proposed method can effectively detect wormhole attack in wireless sensor networks. Performance analysis shows that it has good storage cost and it is applicable to resource constrained wireless sensor networks [8].

Mosmi Tiwari et. al., Proposed Modified Hop Count Analysis Algorithm (MHCAA) for Preventing Wormhole Attack [24] in WSN. This paper considers this problem as severe issue an attempt to derive a mechanism to detect and prevent wormhole node in mobile ad-hoc networks. The objective of this paper is to study various ways to create wormhole attack and develop techniques to detect and prevent wormhole node using AODV routing protocol [9].

Madhu Sharma et al. The total examination sees that, security dangers catch the parcels as well as corrupt system execution. To beat powerlessness issues, work considers wormhole [24] attack as study target and will infer component to distinguish and keep versatile systems from security danger. A wormhole attack is extremely famous and applies on system layer by focusing on vulnerabilities of directing conventions. The entire works consider Ad-hoc On-Demand Routing convention and recognize a few vulnerabilities [10].

Parmar Amish et al. In this paper, the strategies managing wormhole attack in WSN are studied and a technique is proposed for identification and counteractive action of wormhole attack. AOMDV (Ad hoc on interest Multi path Distance Vector) steering convention is joined into this technique which depends on RTT (Round Trip Time) system and different attributes of wormhole attack. When contrasted with other arrangement appeared in writing, proposed approach looks extremely encouraging. NS2 test system is utilized to play out all recreation [11].

Miss. Supriya Khobragade et al. In wormhole attack, an aggressor hub keeps information parcels at one area in the Network and forward to another assailant hub [24] far away by burrowing, which again communicated them into the system locally. The proposed system is a productive location and counteractive action strategy called Wormhole Attack Prevention and Detection Using Authentication Based Delay per Hop Technique for Wireless Network. Recognition of wormhole attack is finished utilizing number of jumps and deferral of every hub in various ways accessible in system. The sender hub is able to recognize the two sorts of wormhole attacks. From quantitative perspective, significant system reproductions were directed to approve the proposed plan utilizing a NS2 arrange test system [12].

Pratima Sarkar et al. In this paper an endeavour has been made to quantify the execution of Ad-hoc On-Demand Distance Vector Routing (AODV) [26] convention. Numerous situations of wormhole attack are being actualized with shifting number of pernicious nodes in the system. A reproduction-based test has been done utilizing NS2 [27] test system for breaking down execution of the system based on three execution lattices Throughput, normal End-to-end Delay and Packet Delivery Function regarding expanding number of noxious nodes [13].

M. B. M. Kamel et al. , the creators proposed a safe and trust AODV (STAODV) to alleviate dark opening attacks in MANET. In STAODV, every hub has trust esteem and a vindictive hub table. Each approaching bundle has a security esteem, which is utilized to look at its wellbeing status. Limit esteem is predefined to decide the answer is sheltered or not. The STAODV inspects each RREP[28] parcel with the arrangement number and the jump check of a hub to goal, and furthermore looks at the wellbeing status of course answer. The recognition technique by utilizing arrangement number has been proposed in numerous papers. The STAODV will be fizzled when assailants collaborate to manufacture counterfeit grouping number in course answer message [14].

B.Cerda et al., The creators proposed the fake treatment parcel convention (PPP) to distinguish dark gap attacks and to recognize malevolent switches. In PPP, a confided in source hub sends a Phoney information bundle and additionally the fake treatment parcel. The distinction to them is that the fake treatment bundle is sent along a foreordained Hamiltonian way and navigates all switches. A noxious hub is distinguished on the grounds that it perceives the fake treatment bundle as a standard information parcel and drops the parcel. Re-enactment

results demonstrated that the PPP is equipped for finding pernicious nodes. Furthermore, the bigger system scale needs to utilize more fake treatment parcels to discover pernicious nodes. Last, the scientists did not contrast the PPP arrangement and existing plans in reproductions [15].

S. Sharma et al., The creators proposed the group and notoriety based agreeable noxious hub identification and expulsion (CRCMD&R) conspire. In CRCMD&R conspire, the bunch head hub ID of originator field records the group head's ID after it left the originator. In RREP bundle, it records the hub ID, the following hub of the hub sent RREP, prime item number, and the bunch head's ID of the hub sent RREP. Three extra tables are required in CRCMD&R plot, i.e., neighbour, authenticity esteem and notoriety level tables. In neighbor table, hub ID and group head's ID are recorded in each bunch head. In authenticity esteem table, it records hub ID, achievement tally, add up to tally and authenticity esteem.

The authenticity esteem acquired from the achievement check isolated by aggregate tally. In notoriety level table, the indiscriminate mode is connected to bunch heads to figure the notoriety. The notoriety esteem is determined as the hub sent RREP to the following hub of the hub sent RREP. The notoriety levels are grouped into four dimensions, i.e., pernicious, suspect, less reliable and dependable. Re-enactment results demonstrated that the CRCMD&R conspire beats standard AODV with higher aggregate throughput. Anyway, the utilized strategies are out-dated that were proposed by different specialists aside from the new thought of utilizing bunch system [16].

M. Rmayti et al. A Mobile A hoc Network (MANET) [29][30][31] is a lot of nodes that convey together agreeably utilizing the remote medium, and with no focal organization. Because of its innate open nature and the absence of framework, security is a confused issue contrasted with different systems. That is, these systems are defenceless against a wide scope of attacks at various system layers. At the system level, malevolent nodes can play out a few attacks running from aloof listening stealthily to dynamic meddling.

Wormhole is a case of extreme attack that has pulled in much consideration as of late. It includes the redirection of traffic between two end-nodes through a Wormhole burrow, and controls the directing calculation to give fantasy that nodes situated a long way from one another are neighbours. To deal with this issue, we propose a novel location model to enable a hub to check whether an assumed most limited way contains a Wormhole burrow or not. Our methodology depends on the way that the Wormhole burrow lessens essentially the length of the ways going through it [17].

Surinder Singh et al. The remote sensor organize has gathering of sensors which can detect the information and course this information to base station. As there is no physical association among sensor and base station the imperative information can be steered without wires. The communicate idea of remote sensor arrange makes it inclined to security risk to the significant information.

The assailant hub can identify the information by making their very own information accumulation and directing component. The quantity of attacks can be conceivable on the system layer. Out of these attacks' wormhole is one of the significant attacks which can change the steering strategy for the entire remote sensor organize. In this attack, the assailant hub can control the bundle transmission of entire system and course it to the passage of nodes. The significant disadvantage of this attack is to expand the parcel drop and exasperating the directing system. Various security methods are produced by the analyst to decrease the parcel drop proportion and secure the directing component of the system.

Out of every one of these procedures few identified with bundle drop proportion are talked about in this paper. The Light weight countermeasure for the wormhole attack (LITEWORP) based on Dynamic Source routing (DSR) convention security method, Delay per Hop Indication (Delphi) in view of AODV (Avoidance Routing Protocol) [32] Protocol security system and MOBIWORP dependent on DSR convention security procedure decrease the bundle misfortune rate 40%, 43% and 35% separately [18].

REFERENCES

[1] Umesh kumar chaurasia and Mrs.Varsha singh, "MAODV: Modified Wormhole Detection AODV Protocol", IEEE 2013.
[2] Harleen Kaur and Neetu Gupta, "Protecting AODV from Wormhole Attack in WSN" in International Journal of Engineering and Computer Science (IJECS), vol. 3, Page No. 8668-8672, October 2014.
[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). https://doi.org/10.1007/s11277-021-08647-1
[4] S Subha and UGowriSankar, "Message Authentication and Wormhole Detection Mechanism in Wireless Sensor Network" in IEEE Sponsored 9thInternational Conference on Intelligent Systems and Control (ISCO) 2015.
[5] Rakhil R and Rani Koshy, " An Efficient Algorithm for Neighbour Discovery and Wormhole Attack Detection in WANET" in International Conference on Control, Communication & Computing India (ICCC), November 2015.
[6] ParmarAmisha, V.B.Vaghelab, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol" in 7th

International Conference on Communication, Computing and Virtualization (ICCCV) 2016.

[7] ManishM Patel and AkshaiAggarwal, "Two Phase Wormhole Detection Approach for Dynamic Wireless Sensor Networks" in IEEE 2016.

[8] Manish Patel and Dr. AkshaiAggarwal, " Detection of hidden wormhole attack in wireless sensor networks using neighbourhood and connectivity information" in International Journal on Ad Hoc Networking Systems (IJANS) Vol. 6, No. 1, January 2016.

[9] Mosmi Tiwari, Deepak Sukheja, Amrita, " Modified Hop Count Analysis Algorithm (MHCAA) for Preventing Wormhole Attack in WSN" in Communications on Applied Electronics (CAE), vol.3, No.3 ,October 2016.

[10] Madhu Sharma, Ashish Jain, "Wormhole Attack in Mobile Ad-hoc Networks", IEEE, Symposium on Colossal Data Analysis and Networking (CDAN), 2016, pp. 1-4.

[11] Parmar Amish, V.B.Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol" , Science Direct , 7th International Conference on Communication, Computing and Virtualization 2016 , pp. 700-701.

[12] Miss. Supriya Khobragade, Prof. Puja Padiya, "Detection and Prevention of Wormhole Attack Based on Delay Per Hop Technique for Wireless Mobile Ad-hoc Network", International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016, pp. 133-1339.

[13] Pratima Sarkar, Chinmoy Kar, Biswaraj Sen,Kalpana Sharma , "Sensitivity Analysis on AODV with Wormhole Attack" , IEEE , 2nd International Conference on Next Generation Computing Technologies (NGCT-2016) Dehradun, India 14-16 October 2016 , pp. 803-807.

[14] M. B. M. Kamel, I. Alameri, and A. N. Onaizah, "STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET," in Proceedings of IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2017, pp. 1278-1282.

[15] B. Cerda, E. Martinez-Belmares, and S. Yuan, "Protection from black hole attacks in communication networks," in Proceedings of the International Conference on Security and Management, Las Vegas, NV, 2017, pp. 7-11.

[16] S. Sharma and S. Gambhir, "CRCMD&R: cluster and reputation based cooperative malicious node detection & removal scheme in MANETs," in Proceedings of 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 2017, pp. 336-340.

[17] M. Rmayti; Y. Begriche; R. Khatoun; L. Khoukhi; A. Mammeri University of Ottawa, Canada, "Graph-Based Wormhole Attack Detection in Mobile Ad hoc Networks" , IEEE, Fourth International Conference on Mobile and Secure Services (MobiSecServ) , March 2018 , pp. 1-6

[18] Surinder Singh and Hardeep Singh Sain , "Security Techniques for Wormhole Attack in Wireless Sensor Networks" , International Journal of Engineering & Technology, Issues 7 , 2018 , pp. 59-62

[19] 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.

[20] 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.

[21] 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.

[22] 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.

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

[24] 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.

[25] 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.

[26] 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/ICEC A.2017.8212741.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.