A Survey of Wormhole Attacks in Mobile Ad Hoc Networks

Sunil Kumar

Maharaja Agrasen University, Baddi (Distt. Solan), Himachal Pradesh

Abstract- **Wormhole attack is an insidious attack against the basic routing function of mobile ad hoc networks (MANETs) where an attacker captures the control and data traffics from one location in the network and tunnels (via out-of-band high powered wireless transmission or high speed wired link) them to another malicious node at a distant point located more than one-hop away, which broadcasts them locally. With the existence of wormhole attack, the network topology is demolished and normal routes are misguided. In this paper, the main focus is to study and analyse the different techniques and systems proposed by the researchers in the literature to countermeasure the effect of Wormhole attack for MANETs.**

Keywords— MANETs, wormhole attack, malicious nodes etc.

I. Introduction

A Mobile Ad hoc NETwork (MANET) is a wireless local area network model composed of a significant number of mobile nodes without a fixed infrastructure (i.e. base stations or access points). Due to the limited transmission capability of mobile nodes in the MANET, the intermediate nodes are used for forwarding the packets for other nodes in multi-hop fashion [1]. The flexibility and openness nature of mobile ad hoc networks make them attractive for wide applications in various fields, such as military communication, emergency search and rescue operations, disaster recovery, communication between moving vehicles (VANET), sensor networks, battlefields etc. [2]. However, distributed and cooperative nature of MANETs makes them highly vulnerable to the attacks [3,4]. In [5], Parsons and Ebinger thoroughly analyzed the impact of various security attacks (black hole attack, flooding attack, packet dropping attack, route disruption attack and wormhole attack) on the performance of MANETs. Their results showed that the degree of impact of attacks differs significantly according to attack type and parameters used.

The wormhole attack [6] is a dangerous attack in mobile ad hoc networks since it is relatively easy to launch, and difficult to detect. The main aim of wormhole attack is to demolished the network topology and misguide the normal routes in order to attract data packets to traverse specific nodes. In wormhole attack, the adversary connects two distant points in the network using a direct low-latency link (called wormhole link), and creates a fictive shortcut connection in the network. It involves two collaborating malicious nodes that forward the routing packets to each other. These nodes are called wormhole nodes. Once the wormhole link is established, the wormhole node eavesdrops on the packets at one end, tunnels them via wormhole link, and replays them to another end in the network. This makes an illusion that the two nodes are within communication range to each other as though they are more than one hop away actually. With the existence of wormhole and false information about a node's neighbours can demolish the network topology and severely affect the discovered route because most of the routing protocols use the number of hop-counts to determine the shortest path between the source and destination node. If the length of wormhole link is short, it will not be of more valuable to the adversary as it may be fail to attract much traffic, but if the length of wormhole link is long enough, it will attract a lot of traffic. During the route discovery process, the wormhole nodes can easily decrease the hop count by using either in-band or out-of-band channels. As a result, the route is established through the wormhole link between the sender and receiver because the route claimed through wormhole link would always be of shorter as compared to a route of real data communication as shown in figure 1. The wormhole attack leads to following dreadful situations in the network:

- Demolished the network topology and fracture the basic routing function of network.
- Destroy the coordination of routing protocol and halting the communication abilities of nodes.
- Bypass and attract a large amount of network traffic in order to lead the congestion in the network.
- Selectively drop the data packets.
- Manipulate the network traffic like modifying packets, changing the sequence of packets, etc.
- Traffic analysis in order to leak the confidential information.
- On the basis of collected network data, the attacker can execute more dangerous attacks further, such as man in the middle attacks, cipher breaking, protocol reverse engineering etc.
- By simply changing the state of the wormhole link on and off, the attacker can trigger a route oscillation within the network in order to lead a denial-of-service (DoS) attack.

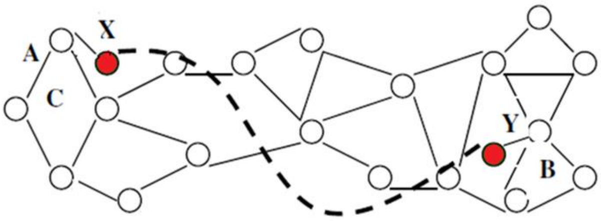


Figure 1: A Scenario of Wormhole Attack.

So, providing the secure communication over the mobile ad hoc networks against the wormhole attack is a major concern.

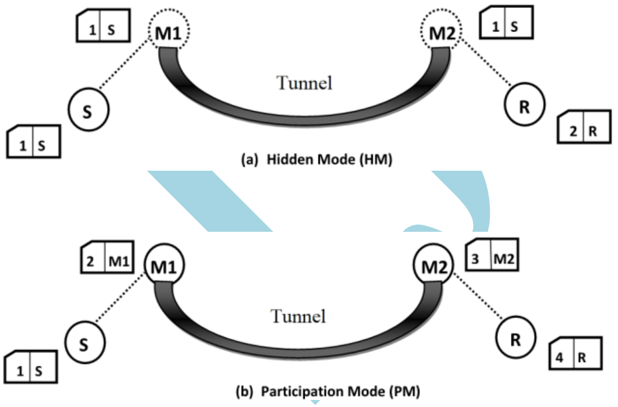
In this paper, a study of different techniques and systems proposed by the researchers in the literature to countermeasure the Wormhole attack for MANETs is presented. These techniques and systems are classified into following categories based on their operative procedure:

- Location, Distance and Time Based
- Hop-Count Analysis Based
- Graph and Geometric Based
- Neighborhood analysis Based
- Statistical Information Based
- Key Management Based

Rest of the paper is structured as follows. Section 2 briefly describes the background of wormhole attack. Section 3 summarizes the different techniques and systems proposed by the researchers in the literature to countermeasure the Wormhole attack for MANETs. Finally, the paper is concluded with future research directions.

II. Wormhole Attacks

Wormhole attacks can be basically launched in two modes: hidden mode (HM) and participation mode (PM) [7] as shown in figure 2. In the hidden mode, the malicious node at one end captures and forwards routing packets to other end without any modifications in the packets and wormhole nodes never appear in routing tables as legitimate nodes. In participation mode, the malicious nodes process routing packets as legitimate nodes and thus appear in an infected wormhole route as two adjacent nodes.



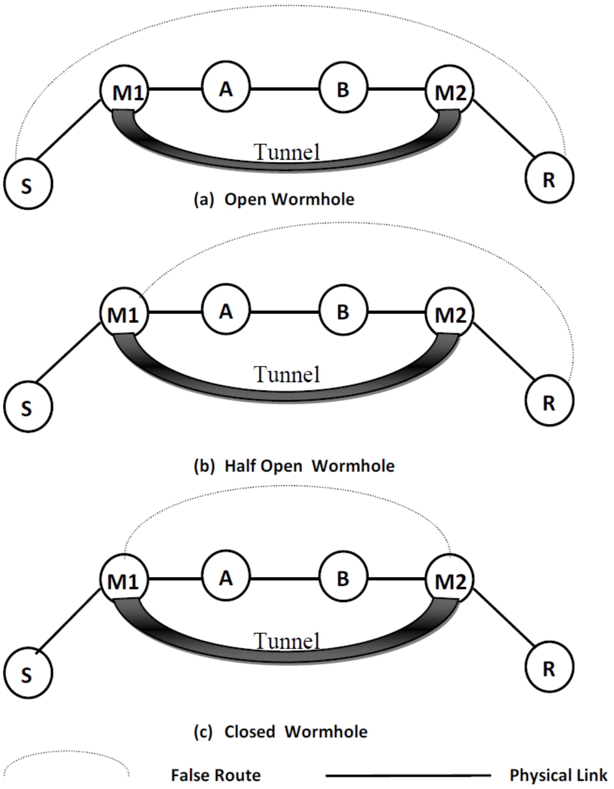
(a) Hidden Mode (HM)

(b) Participation Mode (PM)

Figure 2: Hidden Mode and Participation Mode Wormhole Attack.

In [7,8,9] , authors illustrated that a shortcut link between two HM or PM wormhole nodes can be established using any of the following modes:

1. Wormhole using encapsulation: The first malicious node M1 forwards a route request packet after encapsulating it towards to second malicious node M2 via good nodes.
2. Wormhole using out-of-band channel: The two colluding malicious nodes M1 and M2 communicate directly using different radio frequency band as compared to the frequency bands used by other good nodes. It requires an external high-bandwidth communication channel to establish a direct link between the wormhole nodes using either a long-range wireless directional antenna or a direct wired network cable.
3. Wormhole using high power transmission: The malicious node at one end transmits the packets at the maximum possible power towards second malicious node in order to increase the transmission range so that the packet reach at second malicious node faster than through normal mode.
4. Wormhole using Packet Relay Technique: In this technique, a malicious node relays the packets between two distant benign nodes (not-in-range) to give them the illusion that they are neighbors. The malicious node just plays the role of an invisible bridge between them.
5. Wormhole using Protocol Deviations: This is a special category of the rushing attack [10] where a malicious node exploits the protocol specification in order to disrupt the normal functioning of the network.



(a) Open Wormhole

(b) Half Open Wormhole

(c) Closed Wormhole

Figure 3: Classification of Wormhole Attacks.

III. Review Work

In the literature, researchers have proposed various detection strategies for the detection of wormhole attack in mobile ad hoc network. The proposed solutions against Wormhole attack are classified into following categories based on their operative procedure:

- Location, Distance and Time Based
- Hop-Count Analysis Based
- Graph and Geometric Based
- Neighborhood analysis Based
- Statistical Information Based
- Key Management Based

Location, Distance and Time Based

Azer et al. [11] have suggested wormhole attack preventive scheme based on a social science theory called diffusion of innovations. In this scheme, the routing protocol is customized in such a way that a route is selected on the basis of weights assigned (opinions to each other) to the nodes in the route.

In [6,12] Hu et. al. presented a wormhole attack detection scheme called packet leashes by restricting the transmission time of the packets. There are two types of packets leashes: Temporal packet leash where packet expiration time is appended with the packet and geographic packet leash where specific location and transmission time is appended with the packet. They also proposed an extension of the TESLA [13] broadcast authentication protocol named TIK protocol that enables the receiver to detect the wormhole attack. TIK requires accurate time synchronization between all communicating parties and implements a temporal leash. TIK combines hash tree authentication to confirm the time information in the control packet is not changed. The theory behind TIK is that the packet transmission time in case of wormhole attack can be significantly longer than the time synchronization error. WODEM [14] is a countermeasure against the wormhole attack for sensor networks. In WODEM, a few detector nodes equipped with location-aware devices and longer-lasting batteries detect wormholes, and normal sensor nodes are only required to forward control packets from the detector nodes.

In [15], Hu and Evans proposed a cooperative protocol whereby nodes are equipped with directional antennas devices and share directional information to prevent wormhole attack in the network. In [16], authors proposed an efficient method to detect and prevent the wormhole links in OLSR protocol with the assumption that wormhole attacks consists of relatively longer packet delay as compared to normal wireless propagation delay on a single hop. In [17], authors presented a protocol called Secure Tracking of Node Encounters in Multi-Hop Wireless Networks (SECTOR) that uses a set of rules for the secure verification of the time of encounters between nodes. By using the time of flight, it detects whether one hop neighbor is real neighbor or not. SECTOR uses Mutual Authentication with Distance-bounding (MAD) protocol with specialized hardware.

In [18], Wang and Wong proposed an end-to-end detection of wormhole attack (EDWA) that is based on the hop count estimation of shortest routing path between source and destination. If the hop count of the selected shortest path is much less than the approximated value than an alert of wormhole attack is raised at the source node. TrueLink [19] is a timing based MAC-layer countermeasure to the wormhole attack which verifies that a unique link exists to an apparent neighbor. The verification of a link between two nodes functions in two phases- rendezvous phase and authentication phase. In the rendezvous phase, the neighboring nodes exchange their nonces with respect to some tight timing constraints. In the authentication phase, both the nodes transmit a signed message, mutually authenticating themselves as the originator of their respective nonce.

SEEEP (Simple and Efficient End –to –End protocol) [20] and FEEPVR (First End-to-End Protocol to Secure Ad Hoc Networks with Variable Ranges) [21] are simple algorithms using GPS technology to defense against wormhole attack based on the measurement of length of route between source and destination in accordance to communication range. SLAW [22] is a secure localization scheme against the wormhole attacks in wireless sensor networks. The most important function of the SLAW is to construct a conflicting set for each locator on the basis of abnormalities during the message exchanges, which can be used to differentiate the dubious locators to achieve secure localization.

DelPHI (Delay Per Hop Indication) [23] is a wormhole detection scheme where average delay time per hop and length of each route are calculated in order to detect both kinds of wormhole attacks (hidden and exposed wormhole attacks). Khabbazian et al. [24, 25] formulate the effect of wormhole attack in building the shortest path in routing protocols with the help of analytical study and simulations. They observed that the attackers can disrupt around 32% of all communications across the network in the uniformly distributed network and around 40% to 50% of all communications in the grid topology network when the wormhole attack is strategically placed. In [24], they proposed a secure on-demand distance vector routing protocol which provides wormhole attack free route between the source and destination nodes. In [25], they also proposed a timing-based countermeasure to avoid wormhole attack in the networks. Proposed algorithm in [57] takes advantages of both watchdog and Delphi methods to detect wormhole attack.

In [26], the node ID and location based countermeasure against the wormhole attack has been presented. Every intermediate node attaches its ID and geographical position into routing packets, and source node calculates the distance between the one hop neighbor nodes of a route on the basis of information in route reply packet in order to detect the wormhole attack. A transmission time based mechanism (TTM) [27] has been proposed to detect wormhole attacks with the assumption that transmission time between two fake neighbors created by wormhole is considerably higher than that between two real neighbors.

Choi et al. [28] proposed a technique called Wormhole Attack Prevention (WAP) in which all nodes monitor the behavior of their neighbors through promiscuous mode. Each node maintains a neighbor node table that contains RREQ sequence number, neighbor node ID, sending and receiving time of RREQ packets and count. This approach also uses the concept of delay per hop value to prevent the wormhole attack. In this approach, the source node sets the Wormhole Prevention Timer (WPT) and waits until it overhears its neighbor's retransmission after sending out the RREQ packet. After sending the RREQ message, if the source does not receive the RREP message within the RREP waiting timer, it detects the existence of wormhole and inserts the route to its wormhole list. In [29], Nguyen and Lamont proposed an efficient and simple method to detect wormhole attacks, using a technique called reference broadcast synchronization (RBS). The RBS is used to synchronize node's clocks in MANET.

Alam, and Chan [30] proposed a hybrid approach of RTT measurements and topological comparison to detect wormhole attacks. The proposed approach relies on RTT measurements to identify suspected wormhole attacks and then apply topological comparison to exclude legitimate neighbors from the suspected list. Shi, Jin, Liu, and Song [31] proposed a time-based scheme in order to prevent the wormhole attacks in wireless ad hoc networks. The scheme consists of two phases: detection phase and location phase. In detection phase, the presence of wormhole attacks on the discovered route is detected. In location phase, the source nodes for wormhole attack are identified. Shin, and Halim [32] proposed a scheme to detect wormhole attack in the networks where entire functioning of the scheme is divided into three phases: routes redundancy, routes aggregation and calculating round-trip time (RTT) of all discovered routes. In routes redundancy, it is ensured that route request packet is really sent to the destination through multipath transmission. Routes aggregation is used to aggregate the similar routes in order to know every possible valid route between source and destination. Last phase is used to compute the average number of hops in accordance to the round-trip time of the discovered path and investigates the possibility of wormhole attackers.

Hop-Count Analysis Based

In [33] Jen, Laih, and KuoW implemented a new protocol called Multi-path Hop-count Analysis (MHA) using a hop-count analysis to prevent the wormhole attack in the networks. A Secure HOp-Count based LOCalization scheme (SHOLOC) [34] is proposed to authenticate beacon information and prevent from being arbitrary changed in hop-count. SHOLOC employs beacon nodes to detect wormhole attacks. This method represents the value of hop count by the number of hash operations on a nonce, and as a result malicious nodes cannot reduce the hop counts. In [35] the idea is suggested to find alternate shortest path between sender and receiver, and count the no. of hops to detect the wormhole attack. In [36], a secure ad hoc on-demand distance vector routing protocol called wormhole-avoidance routing protocol (WARP) is proposed. In WARP, each node maintains the data structure in the routing table for its direct neighbors (number of times a neighboring node involves itself in the different routing paths). Every node calculates the ratio of the number of real routes established through a neighboring node to the total number of route replies generated by the node. In [37, 38], authors also used the basic concept of Hop Count in order to detect and countermeasure the effect of wormhole attack.

Graph and Geometric Based

In [39], Lazos et al. presented a geography-based countermeasure to detect and prevent the wormhole attack. In this approach, a small fraction of the nodes have been assigned the responsibility of guards to access the location information and monitor the local traffic among the nodes in order to detect a wormhole attack. In [40], local connectivity information is used to detect wormhole attack in wireless multi-hop networks by exploiting the forbidden packing number in the Unit Disk Graph (UDG) embedding of network graphs. MDS-VOW [41] is a mechanism that reconstructs the layout of the sensors using multi-dimensional scaling. MDS-VOW detects the wormhole by visualizing the anomalies (fake connections through the wormhole and bend the reconstructed surface to pull the sensors that are far away to each other) introduced by the attack. In [42], authors suggested the use of attack graphs for intrusion detection and proposed two methods using the basic functioning of attack graphs. The first method helps in the prediction of a single or multiple step attack based on attack graph adjacency matrix. The second method is used for correlating intrusion events and building attack scenarios in accordance to attack graph distances.

Poovendran and Lazos [43] presented a graph theoretic framework for modeling wormhole links using the UDG communication graph model in Euclidean space. They also proposed a cryptographic mechanism to prevent wormhole attack in accordance to UDG communication graph model. Dong, Liu, and Liao [44] proposed two simple distributed detection techniques called basic and localized WormCircle to detect the wormhole attacks based on local connectivity information. In [45], authors presented a wormhole attack detection mechanism called Cell-based Open Tunnel Avoidance (COTA), which uses geographic information to detect the neighborhood anomalies. COTA achieves a constant space for every node on the path and computation overhead increases linearly to the number of detection packets.

Neighborhood Analysis Based

A protocol called LiteWorp is presented in [46] for detection and isolation of wormhole attack in static networks by setting all nodes in promiscuous mode. This protocol is based on neighborhood information and time information for detection and isolation of wormhole attack. In [46], Khalil et al. presented an approach for the detection of wormhole attack in static networks called LITEWORP, which relies on overhearing the one hop neighbor communication. Every node gathers full two-hop routing information from their direct neighbors. The information of two-hop neighborhood is used to detect wormhole attacks.

In [47], authors utilized the built-in routing table and neighbors' verification for the detection of exposed wormhole attack. In [48], authors proposed an effective method called Wormhole Attack Prevention (WAP) using neighboring node monitoring mechanism to detect and prevent the wormhole attack.In [49], each node keeps information of its neighbors and identifies replayed packet that are forwarded by two attackers in order to detect the wormhole attack. In [50], authors presented algorithm for detecting the existence of wormhole in the network where the relative frequency of a link is used to detect the wormhole attack.

WAPN [51], is a wormhole attack detection approach where neighboring-node-number helps in detecting the wormhole attack in the network as a wormhole attack usually increase the neighboring-node-number as a result of the wormhole link. In [52], authors proved that nodes attacked by the same wormhole are either 1-hop neighbors or 2-hop neighbors, and with a high probability, there are at least 3 nodes, which are non-1-hop neighbors, in the intersection of the two neighbor.

Statistical Information Based

In [53], Ning, Lijun and Xiangfang analyzed the effect of wormhole attack in multi-path routing protocol for MANETs. They also proposed a simple scheme called statistical analysis (called SAM) to detect wormhole attack and malicious nodes. The wormhole links are detected with the assumptions that wormhole link offers abnormally high frequency as compared to normal statistics. A probability mass function (PMF) is used to find the highest relative frequency.

In [54], Buttyán, Dóra, and Vajda proposed two statistical based detection techniques for wormhole attack. The first one is called Neighbor Number Test (NNT) which detects the wormhole attack with the assumption that wormhole attack will increases the one hop neighbors of the sensor nodes due to fake neighbors created by wormhole links. The second technique is called All Distances Test (ADT) which detects the wormhole attack with the assumption that wormhole attack will reduce the length of the shortest routes between all pairs of sensor nodes due to shortcut links formed by the wormhole attack.

Statistical Wormhole Apprehension using Neighbours (SWAN) [55], is a technique to detect the wormhole attack where localized statistical neighborhood information collected by mobile nodes is used to detect the attack.

Key Management Based

In [56], authors proposed the node-to-node authentication and compromise - tolerant security scheme using location-based keys. In [57], authors proposed a scheme where public and private keys are generated through one-way hash function. The neighborhood table is periodically updated by receiving the beacon packets from the neighbors in order to collect the information of real neighbours. The wormhole attack is detected at destination node in similar fashion. SECTOR [17] uses Mutual Authentication with Distance-bounding (MAD) protocol with specialized hardware.

.

IV. Conclusion

Security is very crucial for MANETs. Wormhole attack is very dangerous attack in mobile ad hoc networks as it is relatively easy to launch, and difficult to detect. It also disturbs entire routing process of the network. In this paper, a study of a number of detection and prevention techniques proposed by researchers in the literature on securing MANETs against wormhole attack has been presented. It has been observed that there is no proper wormhole detection technique that can detect all wormhole attacks completely, and still it is an active research area.

References

[1] Chlamtac, M. Conti and J. J. N. Liu, “Mobile ad hoc networking: imperatives and challenges,” Ad Hoc Networks, vol. 1 no. 1, pp. 13-64, Jul. 2003.

[2] J. Hoebeke, I. Moerman, B. Dhoedt and P. Demeester, “An overview of mobile ad hoc networks: applications and challenges,” Journal-Communications Network, vol. 3, no. 3, pp. 60-66, Jul. 2004.

[3] A. Mishra and K.M. Nadkarni, “Security in wireless ad-hoc networks,” in The Handbook of Wireless Ad-Hoc Networks, M. Ilyas, Ed. CRC Press, 2003, Ch. 30, pp. 499-549.

[4] S. Kumar and K. Dutta, “Securing Mobile Ad Hoc Networks: Challenges and Solutions”, International Journal of Handheld Computing Research (IJHCR), vol.7, no.1, pp.26-76, 2016.

[5] Parsons M.J and Ebinger P, " Performance evaluation of the impact of attacks on mobile ad hoc networks", In Proceedings of 28th IEEE International Symposium on Reliable Distributed Systems, pp. 40-48, Niagara Falls, New York, USA, September 27-30, 2009.

[6] Y.C. Hu, A. Perrig and D. B. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in Proceedings of Twenty-Second IEEE Annual Conference on Computer Communications (INFOCOM), vol. 3, San Francisco, CA, USA, 30 March-3 April 2003, pp. 1976–1986.

[7] G. Lee, D-K. Kim, and J. Seo, "An Approach To Mitigate Wormhole Attack In Wireless Ad Hoc Networks", IEEE International Conference On Information Security & Assurance, IEEE, pp. 220-225, 2008.

[8] Khalil Issa, Bagchi Saurabh, B. Shroff Ness, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", In Proc. of IEEE International Conference on Dependable Systems and Networks (DSN’05), pp. 612-621, 2005.

[9] M.A. Azer, S.M. El-Kassas A.W.F. Hassan, and M.S. El-Soudani, "Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a proposed Decentralized Scheme Marianne, " IEEE Third International conference on Availability, Reliability and Security, 2008.

[10] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," In Proceedings of the ACM Workshop on Wireless Security (WISE '03), pp. 30-40, 2003.

[11] M.A. Azer, S.M. El-Kassas, M.S. El-Soudani, "An innovative approach for the wormhole attack detection and prevention in wireless ad hoc networks", In Proceeding of IEEE International Conference on Networking, Sensing and Control (ICNSC), pp. 366-371, 10-12 April 2010.

[12] Y.-C. Hu, A. Perrig, D. B. Johnson, "Wormhole attacks in wireless networks", IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 370-380, Feb. 2006.

[13] A. Perrig, R. Canetti, J. D. Tygar, D. Song, "Efficient authentication and signing of multicast streams over lossy channels", In Proc. IEEE Symp. Security Privacy, pp. 56-73, May 2000.

[14] J.-H. Yun, I.-H. Kim, J.-H. Lim, and S.-W. Seo, “WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks,” Ubiquitous Convergence Technology Lecture Notes in Computer Science, pp. 200–209, 2007.

[15] Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," in Network and Distributed System Security Symposium (NDSS), San Diego.2004.

[16] Naït-Abdesselam, B. Bensaou, and T. Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks," in IEEE Communications Magazine. vol. 46, April 2008, pp. 127-133.

[17] Capkun, L. Buttyan, and J. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks," in ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN) Washington, USA October 2003, pp. 1-12.

[18] X. Wang and J. Wong, “An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks,” 31st IEEE Annual International Computer Software and Applications Conference - Vol. 1- (COMPSAC 2007), 2007, pp. 39-48.

[19] J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, “TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks,” Proceedings of the 2006 IEEE International Conference on Network Protocols, pp.75-84, 12-15 Nov. 2006.

[20] N. Gupta, S. Khurana, “SEEEP: Simple and Efficient End-to-End Protocol to Secure Ad hoc Networks Against Wormhole Attacks,” In Proceedings of the 4th International Conference on Wireless and Mobile Communications (ICWMC’08), Athens, Greece, 27 July–1 August 2008, pp. 13–18.

[21] S. Khurana and N. Gupta, "FEEPVR: First End-to-End Protocol to Secure Ad Hoc Networks with Variable Ranges against Wormhole Attacks," in Second International Conference on Emerging Security Information, Systems and Technologies, secureware, 2008, pp. 74-79.

[22] H. Chen, W. Lou, and Z. Wang, “On providing wormhole-attack-resistant localization using conflicting sets,” Wireless Communications and Mobile Computing, vol. 15, no. 15, pp. 1865–1881, 2014.

[23] H. S. Chiu and K.-S. Lui, “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks,” 2006 1st International Symposium on Wireless Pervasive Computing, Phuket, Thailand, 16–18 January 2006.

[24] M. Khabbazian, H. Mercier, and V. K. Bhargava, “NIS02-1: Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure,” In Proceedings of the Global Telecommunications Conference (GLOBECOM’06), San Francisco, CA, USA, 27 November–1 December 2006; pp. 1–6. ,

[25] M. Khabbazian, H. Mercier, and V. K. Bhargava, “Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks,” IEEE Transactions on Wireless Communications, vol. 8, no. 2, pp. 736–745, 2009.

[26] K. Lee, H. Jeon, and D. Kim, “Wormhole Detection Method based on Location in Wireless Ad-Hoc Networks,” New Technologies, Mobility and Security, Springer Netherlands, 2007, pp. 361-372.

[27] P. V. Tran, L. X. Hung, Y.-K. Lee, S. Lee, and H. Lee, “TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks,” In Proceedings of the 4th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 11–13 January 2007, pp. 593–598.

[28] S. Choi, D.-Y. Kim, D.-H. Lee, and J.-I. Jung, “WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks,” IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008), 2008, Taichung, Taiwan, 11–13 June 2008; pp. 343–348.

[29] D. Q. Nguyen and L. Lamont, “A Simple and Efficient Detection of Wormhole Attacks,” 2008 New Technologies, Mobility and Security (NTMS '08), pp.1-5, 5-7 Nov. 2008.

[30] M. R. Alam and K. S. Chan, “RTT-TC: A topological comparison based method to detect wormhole attacks in MANET,” 2010 IEEE 12th International Conference on Communication Technology (ICCT), pp.991-994, 11-14 November 2010.

[31] F. Shi, D. Jin, W. Liu, and J. Song, “Time-Based Detection and Location of Wormhole Attacks in Wireless Ad Hoc Networks,” 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp.1721-1726, Nov. 2011.

[32] S.-Y. Shin and E. H. Halim, “Wormhole attacks detection in MANETs using routes redundancy and time-based hop calculation,” 2012 International Conference on ICT Convergence (ICTC), pp.781-786, 15-17 Oct. 2012.

[33] S.-M. Jen, C.-S. Laih, and W.-C. Kuo, “A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET,” Sensors, vol. 9, no. 6, pp. 5022–5039, 2009.

[34] Y. Zeng, S. Zhang, S. Guo, and X. Li, “Secure Hop-Count Based Localization in Wireless Sensor Networks,” 2007 International Conference on Computational Intelligence and Security (CIS 2007), pp.907-911, 15-19 Dec. 2007

[35] T. Hayajneh, P. Krishnamurthy, and D. Tipper, “DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad Hoc Networks,” 2009 Third International Conference on Network and System Security, 2009.

[36] M.-Y. Su, “WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks,” Computers & Security, vol. 29, no. 2, pp. 208–224, 2010.

[37] S. Gupta, S. Kar, and S. Dharmaraja, “WHOP: Wormhole attack detection protocol using hound packet,” 2011 International Conference on Innovations in Information Technology, pp. 226-231, 25-27 April 2011.

[38] N. Agrawal and N. Mishra, “RTT Based Wormhole Detection Using NS-3,” 2014 International Conference

on Computational Intelligence and Communication Networks, (CICN), pp.861-866, 14-16 Nov. 2014.

[39] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. Chang, “Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach,” IEEE Wireless Communications and Networking Conference, Seattle, WA, USA, 2005; pp. 1193–1199.

[40] Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," in 26th IEEE International Conference on Computer Communications (INFOCOM 2007), IEEE, 2007, pp. 107-115.

[41] W. Wang and B. Bhargava, “Visualization of wormholes in sensor networks,” Proceedings of the 2004 ACM workshop on Wireless security - WiSe 04, 2004, pp.51-60.

[42] M. Azer, S. El-Kassas, M. M. S. El-Soudani, “Using Attack Graphs in Ad Hoc Networks - For Intrusion Prediction Correlation and Detection” In Proceedings of the International Conference on Security and Cryptography, 2006, pp.63-68

[43] R. Poovendran and L. Lazos, “A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks,” Wireless Networks, vol. 13, no. 1, pp. 27–59, Aug. 2006.

[44] D. Dong, M. Li, Y. Liu, and X. Liao, “Connectivity-Based Wormhole Detection in Ubiquitous Sensor Networks,” J. Inf. Sci. Eng., vol. 27, no. 1, pp. 65-78, 2011.

[45] W. Wang, B. Bhargava, Y. Lu, and X. Wu, “Defending against wormhole attacks in mobile ad hoc networks,” Wireless Communications and Mobile Computing, vol. 6, no. 4, pp. 483–503, 2006

[46] Khalil, S. Bagchi, and N. Shroff, “LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks,” 2005 International Conference on Dependable Systems and Networks (DSN05), pp. 612-621, 2005.

[47] Z. A. Khan and M. H. Islam, “Wormhole attack: A new detection technique,” 2012 International Conference on Emerging Technologies (ICET), pp.1-6, 8-9 Oct. 2012.

[48] S. Choi, D.-Y. Kim, D.-H. Lee, and J.-I. Jung, “WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks,” 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008), pp.343-348, 11-13 June 2008.

[49] G. Lee, J. Seo, and D.-K. Kim, “An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks,” in Proceedings of the 2008 International Conference on Information Security and Assurance (ISA 2008), 2008, pp. 220-225.

[50] S. Win, “Analysis of Detecting Wormhole Attack in Wireless Networks”, of Electronics and Communication Engineering, World Academy of Science, Engineering and Technology, Vol. 2, No. 12, pp. 422-428, 2008.

[51] F.-R. Kong, C.-W. Li, Q.-Q. Ding, G.-Z. Cui, and B.-Y. Cui, “WAPN: a distributed wormhole attack detection approach for wireless sensor networks,” Journal of Zhejiang University-SCIENCE A, Vol. 10, No. 2, pp. 279–289, 2009.

[52] Y. Wang, Z. Zhang, and J. Wu, “A Distributed Approach for Hidden Wormhole Detection with Neighborhood Information,” 2010 IEEE Fifth International Conference on Networking, Architecture, and Storage, pp.63-72, 15-17 July 2010.

[53] N. Song, L. Qian, and X. Li, “Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach,” 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05)”, Vol. 18, IEEE Computer Society, 2005.

[54] Buttyán, L. Dóra, and I. Vajda, "Statistical Wormhole Detection in Sensor Networks," in Security and Privacy in Ad-hoc and Sensor Networks: Springer, 2005, pp. 128-141.

[55] S. Song, H. Wu, and B.-Y. Choi, “Statistical wormhole detection for mobile sensor networks,” 2012 IEEE Fourth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 322-327, 2012.

[56] Y. Zhang, W. Liu, W. Lou, and Y. Fang, “Securing sensor networks with location-based keys,” IEEE Wireless Communications and Networking Conference, vol.4, no., pp. 1909- 1914, Vol. 4, 13-17 March 2005.

[57] R. Singh, J. Singh, and R. Singh, “WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks,” Mobile Information Systems, vol. 2016, pp. 1–13, 2016.