ISSN 2320-9984 03 >
9 772320 998015

Volume 1, Issue 3, October 2013 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Normalized Worm-Hole Local Intrusion Detection Algorithm (NWLIDA)

Aarfa Khan
M. Tech. Scholar
Department of Computer Science & Engineering
Lakshmi Narain College of Technology
Bhopal (M.P.) [INDIA]
Email : aarfakhan89@gmail.com

Prof. Shweta Shrivastava
Assistant Professor
Department of Computer Science & Engineering
Lakshmi Narain College of Technology
Bhopal (M.P.) [INDIA]
Email : shwetashri.26@gmail.com

Prof. Vineet Richariya
Head of the Department & Professor of
Department of Computer Science & Engineering
Lakshmi Narain College of Technology
Bhopal (M.P.) [INDIA]
Email : vineet_rich@yahoo.com

Abstract**—***A Mobile Ad-Hoc Network (MANET) is a arrangement of wireless mobile nodes which forms a temporary network for the communication without the access point, or centralized administration. Multiple routing protocols to establish the route from sender to receiver has been devised so far, since last few years ago, to find optimum path from a source to some destination.*

Wormhole attack is one of the serious routing attacks, which is launched by creation of tunnels and it leads to total disruption of routing paths on MANET. This paper presents, NWLID- a Normalized Worm hole Local Intrusion Detection which is the modified version of Local Intrusion Detection Routing Security over mobile Ad-Hoc Network which has a intermediate neighbor node discovery mechanism, packet drop calculator, individual node receiving packet estimator followed by isolation technique. NWLID algorithm effectiveness is evaluated by using ns2 network simulator.

Keywords:— *Ad-hoc Network; Black hole; Wormhole Node Detection; Tunnel; Preclusion Ration, Adjoining Node; Security;*

1. INTRODUCTION

A wireless network can be constructed by a group of mobile nodes, which are permitted to forward packets to each other. There is one assumption made routing protocols [1] by every node is to work in co-operative form and trustworthy. Among security attacks which are launched in network layer are very critical [2]. The Wormhole attack is one of the most severe security attacks [3] which can significantly degrades the communications across the network, it is a network layer attack launched by malicious nodes by creating a tunnel through which packets are received and replayed to other nodes disrupting the communication path and corrupting the routing processes.

Wormhole [4] tunnel is created by any two malicious nodes [5] initially, which collude together and gives an illusion that they are only one hop away from each other and causes the routing of packets to happen through them as having a neighbor node. Once wormhole pairs establish the path as a tunnel, they can temper packets, drop packets, reply or selectively forward them.

Evolution of impact of wormhole attack on AODV [6] depicts various network parameters like network throughput, average end to end delay, packet receiving ratio, packet drop rate are generally affected by the presence of wormhole nodes and their tunnels [7] in the network.

This paper presents various methods [8] to detect and prevent Wormhole attack. The rest of the paper is organization is, Section 2 discusses the Wormhole attack in Mobile ad-hoc network [2] and its classification & various modes in it. Section 3 shows the various techniques used for the detection and prevention of Wormhole attack. Section 4 presents the proposed technology and finally Section 5 presents our conclusions.

2. MANET

A Mobile Ad-hoc Network (MANET) is a collection of wireless mobile nodes that forming temporary network architecture for communication without any established infrastructure or centralized mechanism. In a MANET, the nodes are free to move anywhere in the network or out of the network and organize themselves into a network. MANET does not require any centralized controlling mechanism such as base stations; therefore, it is a striking networking option for connecting mobile devices quickly, dynamically and spontaneously.

2.1 Attacks in MANET

Attacks in MANET can be classified in terms of consequence and techniques as shown in Figure 1. as well as in Table 1. Based on consequence, attacks can be grouped into

Table. 1 Layered Models of MANET Attacks

MANET Security Layer	Attacks
Multi-layer attacks	DoS, Impersonation, Re-play, MIMA
Application layer	Repudiation, Data Corrup-tion
Transport Layer	Session Hijacking, SYN Flooding
Network Layer	Black hole Attack, Worm-hole Attack, Flooding At-tack, Byzantine Attack, Line Spoofing Attack
Data link layer	Traffic Monitoring and Analysis
Physical layer	Jamming, interception, Eavesdropping

Black Hole: All packets are accepted but forwarded by the specific node.

Routing Loops: Creates a loop in the communication path.

Network Partition: The network is partitioned into sub networks where nodes cannot communicate each other even though path exists among them.

Selfishness: A node will not serve as a intermediate for other nodes.

Sleep Deprivation: A node is pressured to use up its battery.

Denial of Service: A node is banned from sending or receiving packets Based on the techniques of attack, they can be appear into the network

Cache Poisoning: Information in routing tables is impersonated, removed or contains misleading information.

Fabricated Route Messages: Control packet, such as route requests packet and replies packet with attacker information are inserted into the network.

Rushing: In several routing protocols of MANET, only the messages that arrive earlier are accepted by the recipient. The malicious node can block legitimate messages that arrive later by distributing a false control message.

Wormhole: A tunnel is created between two nodes that can be used to transmit packets secretly.

Packet Dropping: A node tires to drops packets that are required to be routed.

Spoofing: Insert packet or control message with misleading or misrepresented source address.

Malicious Flooding: Forward large amount of packets data towards some targeted nodes

Figure1. Security attacks classification

3. WORM HOLE ATTACK

In physics, a wormhole is a hypothetical shortcut through space and time that connects two remote regions. The Wormhole attack is a kind of network layer is the most interest seeking attack in ad-hoc networks [2][3]. Wormhole attack is also called as tunneling attack because it makes tunnel between two attackers. In a wormhole attack, the attacker receives packets at one node in the communicating network, tunnels towards to another location and replays them there. This tunnel among two colluding attackers' nodes in the network is referred to as a Wormhole attack. It could be established by making link between two colluding attacker's nodes or through a single long-range wireless link. This attack is very hard to catch and easy to implement [3]. In this form of attack the attacker node may create a wormhole even for packets not addressed to it because of broadcasting nature of the radio channel. In the figure 2 below, the path from Sender S to Destination D via wormhole link (W1, W2) has the length of 5 when the usual path has the length of 11. Therefore, in most of the routing protocols, Sender (S) prefers sending data to Destination (D) along the path with wormhole link.

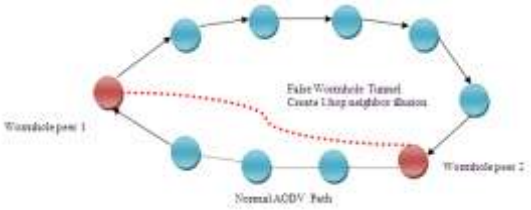

Figure 2. Wormhole link representation through Malicious Nodes

3.1 Wormhole Attack Modes

Wormhole attacks can be created using several modes, these modes are addressed below.

3.1.1 Wormhole using Encapsulation:

When an attacker node at one part of the network receives the route request packet, it tunnels towards it to a second colluding party at a distant location near the destination node. The second party then rebroadcasts the route request packet. The neighbors of the second colluding party hear the route request packet and drop any further legitimate requests that may arrive later on genuine multi-node paths.

3.1.2 Wormhole using Out-of-Band channel:

This mode of the wormhole attack is launched by having an out-of-band high-bandwidth channel between the attacker nodes. This Channel can be achieved, for example, by using a long-range directional wireless link or a direct wired link.

3.1.3 Wormhole using Packet Relay:

In this mode of the wormhole attack, a attacker node relays packets between two

distant nodes to convince them that they are neighbors to each other

3.1.4 Wormhole with High Power Transmission:

In this mode, when a single attacker node gets a route request packet, it broadcasts the request packet at a high power level, a capability which is not presented to other nodes in the network. Any node that receives the high-power broadcast rebroadcasts to the destination.

3.1.5 Wormhole using Protocol Deviations

An attacker node can lunch a wormhole by simply not complying with the protocol and broadcasting without backing off. The intension is to let the route request packet it forwards arrive first at the destination node and sit is therefore included in the path towards the destination.

3.2 Wormhole Attack Threats

We can consider wormhole attack as a two phase process launched by one or several attacker nodes.

3.2.1 In the first phase, the two attacker's end points of the tunnel may use it to pass routing traffic to attract routes through them.

3.2.2 In the next phase (second phase), wormhole attacker nodes could take advantage of the data in variety of ways. They can misuse the data flow by selectively dropping the packet or changed data packets, generating unnecessary Routing and controlling activities in the network by turning off the wormhole link periodically etc.

3.3 Wormhole Attack Types

The Wormhole attack can be classified into two types: Hidden attacks and Exposed attacks, depending on whether wormhole attacker nodes put their identity into packets headers when tunneling & replaying packets [2][3].

Hidden Attacks: In hidden attacks, wormhole attacker nodes do not update packets headers as they should so other nodes do not realize the existence of them, a packet P sent by node S is overheard by node W1, node W1 transmits that packet to node W2 (worm-hole 2) which in turn replays the packet into the communication network. Because W1 & W2 do not modify the packet header so D seems to get the packet directly from S. In this way it seems D & S are neighbors although they are out of radio range from each other. In this kind of attack, a path from S to D via wormhole attacker link will be:

$$S \rightarrow A1 \rightarrow B1 \rightarrow D$$

Exposed Attacks: In exposed attacks, wormhole nodes do not change the content of packets but they include their identities in the packet header as trustworthy nodes do. Therefore, other nodes are alert of wormhole node existence but they do not know wormhole nodes are attacker. In case of exposed attacks, the path from S to D via wormhole will be:

$$S \rightarrow A1 \rightarrow W1 \rightarrow W2 \rightarrow B1 \rightarrow D$$

4. DETECTION AND PREVENTION TECHNIQUES

Different techniques or protocols used for the detection and prevention of Wormhole attack in MANET are described below:

Packet Leashes: The concept of Geographical and Temporal packet leashes were introduced first for the detection and prevention of wormholes [4]. A leash is defined as any added information to the packet for the purpose of protecting against the wormhole. They require that all nodes in the simulation area have tightly synchronized clocks. Both geographical and temporal leashes require adding authentication data to each packet to protect the leash, which add processing and communication overhead in it.

Round Trip Time: A mechanism called Round Trip Time (RTT) was used to detect wormhole attack between two nodes in order to avoid use of any special dedicated hardware. Because the RTT between two fake (attacker) neighbors is

higher than that between two trustworthy neighbors so by comparing these RTTs between A and A's neighbors, node A can recognize which neighbors are bad one neighbors and which neighbors are good one neighbors. This scheme doesn't require any special hardware and easy to implement but it cannot applied to detect exposed attacks because no attacker neighbor is created in exposed attacks.

Directional Antennas*:* To ruin the wormhole, each node shares a secret key with every other node and maintains an updated list of its neighbors in its table. This scheme is applicable for secure dynamic neighbor detection. However, it only partially mitigates the wormhole problem.

LITEWORP: A lightweight countermeasure for the wormhole attack, called LITEWORP. The basic technique used is local monitoring whereby a node monitors traffic in and out of its near nodes and uses a data structure of first and second hop neighbors. The guard node can detect the wormhole if one of its neighbors is behaving maliciously or different from others. In case of sparse network, however, it is not always possible to find a guard node for a specific link.

***Time Based Mechanism*:** A transmission time based mechanism (TTM) was use to identify wormhole attacks during the communication. Wormhole is identified based on the data that is the transmission time between two bogus neighbors created by wormhole is considerably greater than that between two authentic neighbors which are within radio range area of each other. Outcome of TTM has good performance, little overhead and no special hardware required.

***Wormhole Attack Prevention*:** A technique called Wormhole Attack Prevention (WAP) was devised, which not only identify the fake route in the communication but also adopts some measures against action wormhole nodes from re-appearing during the route detection phase. All nodes examine its neighbor's performance when they send RREQ messages packet (Control Packet) to the destination by using a special list called Neighbor List. The WAP has the ability of identifying both the hidden and exposed attacks without any special hardware. A special timer is used to identify wormholes.

***Topological Comparison Based Method*:** A technique called RTT-TC, which is based on round trip time calculation and topological comparisons, was also introduced for the identification of wormhole attack in the network. The method is based on the following two observations of wormhole attacks: Two malicious neighbors with a wormhole tunnel in between has longer RTT, compared to the RTT with trustworthy neighbors and Two trustworthy neighbors usually share other trustworthy neighbors between them, and two fake neighbors do not share common trustworthy neighbors. The first rely is on RTT measurements to detect suspected wormhole attacks node and then use of topological comparison to separate out genuine neighbors from the suspected list.

***Using Wireless Protocol*:** A technique was devised and developed that prevents wormhole attackers on wireless networks. The design of this protocol is based on the mechanism asymmetric and symmetric key cryptography and a Global Positioning System (GPS). Nodes are separated here as GPS node and non-GPS node. Since non-GPS nodes require GPS nodes to identify relative location, asymmetric key cryptography plays a very important role to providing integrity and trust that only reports of location come from GPS nodes.

Packet Travel Time: An efficient technique was devised which was an improvement and modification over another algorithm which was depends on transmission time-based mechanism (TTM). Moreover, this algorithm emerges a new technique called Packet Travel Time (PTT). The proposed technique is to analyze all transmitted packets in the network. According to this method, nodes should have their network interfaces in the promiscuous

reception mode, and network links function bi-directionally.

5. LITERATURE REVIEW

5.1 "Wormhole Attack Detection Protocol using Hound Packet "author has proposed a technique that is protection against specific attack called Wormhole attack which enables an attacker to store packets at one location in the network, forwards them to another location, and re-inserted them into the network for the communication. The author has further suggested optimizing the hound packet to overcome from processing delay of the packet [3].

5.2 "Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation" author has proposes a method to detect and isolate wormhole attacks in mobile ad-hoc networks (MANETs). The key issue of this paper is to create multiple possible routes when sending Route Request (RREQ) from source to destination and to use those routes as reference of each other within the network, in order to find attacker nodes with malicious behavior within the network in the communication [4].

5.3 "A Robust Approach to Detect and Prevent Network Layer Attack in MANETS", a new semantic security technique is presented, which suits for the diverse MANET constraints and also is robust in nature. Outcome analysis shows the detection and prevention of the four attacks parallels i.e. packet dropping, message tampering, black hole attack and gray hole attack. In future work, they are considering measurement of more number of network parameters, to analyze the performance of such a network using the proposed approach [5].

5.4 "Wormhole Attack: A new detection technique", author proposed the use of the modified routing table to look into the suspicious links in the network, confirmation of wormhole existence, at the end isolating the confirmed wormhole nodes. The approach has been applied to DSDV routing protocol and the detection of self-sufficient wormhole nodes and attacks. In future work will involve the use of present approach for detection and prevention of wormhole attacks in other protocols as well [6].

5.5 "A Local Intrusion Detection Routing Security Over MANET Network", author proposes a Local Intrusion Detection (LID) security routing mechanism to protect against Black Hole Attack over Ad-hoc ODDV MANET routing protocol which works on network layer. By performing LID security routing mechanism, the security mechanism overhead would be decreased.

As a piece of future work, we will perform more enhanced intrusion detection mechanism that could perfectly detect group attack if applied on the MANET [7].

6. NORMALIZED WORM HOLE DETECTION ALGORITHM

Normalized Step1: (Source Node, Before Communication)
Broadcast RREQ packet
If RREP packet received
send data packets
Else
Reinitiates a new RREQ packet
End If
(Previous Node)
If RREP packet received from intermediate node
Buffer the RREP packet
Initiates a route to next node
send FRREQ packet to next node
If FRREP packet received
Extract FRREP packet information
If next node has a route to (destination & Intermediate nodes)
Discard FRREP packet
Unicast RREP to source node
Else
Discard both RREP and FRREP packets
Broadcast alarm message
End If
End If
End If
Normalized Step 2: (Intermediate Node, After Communication)
Send Data Packet to next node
Send FHellow Packet to Next to Next Node
If (Reply=AT)
Next node is Trustworthy
Else
Next Node is added to the Worm-hole List

Figure 3. Modified Normalized algorithm to detect Malicious Node.

Step 1: In order to mitigate the drawbacks in Local Intrusion Detection (LID) security routing mechanism [5]. We propose new mechanism called Normalized Worm hole Detection System (NWLIDS) security routing mechanism (Figure 4, Figure 5, and Figure 6) to allow the detection of the attacker to be locally;

In the Normalized Step First:

In this when the suspected intermediate node (node N5) unicast the RREP towards the source node (node N1) the previous node (node N4) to the intermediate node performs the process of detection and not the source node as shown in figure 4. First, the previous node buffers the RREP packet. Second, it uses a new route to the next node (node N6) and sends FRREQ packet to it. When the previous node receives the FRREP packet from the next hop node, it extracts the information from the FRREP packet and behaves according to following rules:

- If the next node (N6) has a route to intermediate node (N5) and destination node (N7), the previous hop node discard the FRREP, then unicast the RREP to the source node.
- If the next hop (N6) has no route to the destination node (N7) or the intermediate node (N5) or both of them (N5 and N7), the previous node (N4) discards the buffered RREP and the FRREP as well, at the same time broadcasts the alarm message to announce there is no secured enough route available to the destination node (N7).

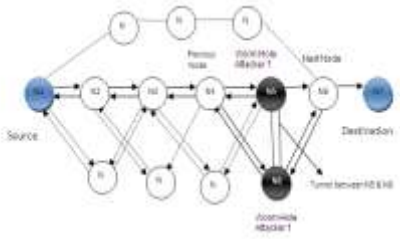

Figure 4. Before communication, LID process at Intermediate node

In the Normalized Step Second:

It may be the Case When the Node Receive the FRREQ message it's a Worm hole node instead of black hole node and replies a fake FRREP message; in that case black hole node comes in the network, to remove that node in the communication network, 2nd Normalized step to be perform for that in the communication FHellow packet format is devised, which is send by each intermediate node to consecutive neighbor of it next node, if replies by Preclusion Ratio(PR) if PR greater than 50% which means previous node its trustworthy and added to the list of trustworthy nodes otherwise it is Worm hole and it is added to the Worm hole list. As shown in the figure 5. Each node in the communication network sends FHellow Packet to next to its consecutive neighbor like N2 sends to N4 and N3 sends to N5.

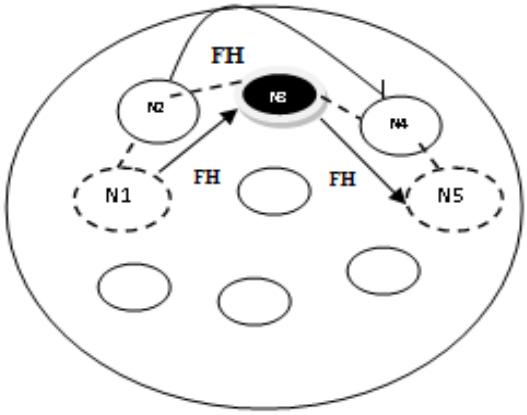

Figure 5. After communication, LID process at intermediate node

After Receiving the FHellow Packet at each node then each node checks Preculsion ratio and replies by PR as shown in figure 6. If it received the PR(above 50%) message means next node in the communication network is trustworthy and if it is received PR (below 50%) message means next node in the communication network is not trusthworthy or Worm hole node. As shown in the figure all nodes are receiving PR like N1, N2, N3, N4 and N5. Node N1 receives PR below than 50% hence Node N3 is not trustworthy.

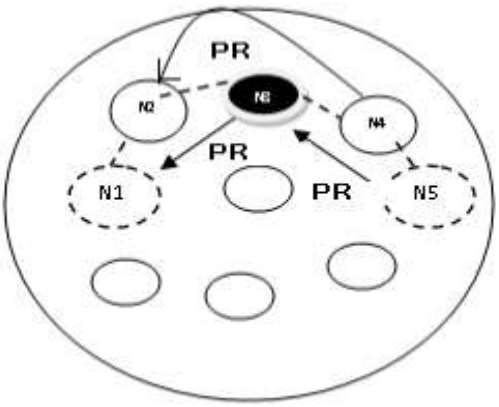

Figure 6. Preclusion Ratio calculation at intermediate node

7. CONCLUSION AND FUTURE RESEARCH DIRECTION

In this paper we have done surveys of all the paper publish in worm hole detection system and prose the terminology to remove the worm hole attack with greater effect by removing the drawback of Local Intrusion detection system.

In future we would like to implement this mechanism in ns2 and improve the process of wormhole detection methodology by removing overheads in the existing terminologies. Therefore, 7.1 Paragraph contains speculation on future research challenge.

No.	Method Name	Description	Encryption Used	Routing Protocol	Detection Quality	Service Efficiency	Attack Type
1.	NWLID Algo	Normalized Worm-hole local intrusion detection	No	AODV	Intermediate Neighbor discovery process confirm wormhole	Low False positive Rate	Hidden & Exposed Attacks
2.	PPN(2013)	Prime Product Number	Symmetric Encryption	AODV	Network throughput increases as cost of high overhead	No false detection	Malicious Node Detection
3.	WAD-HLA (2013)	Wormhole attack detection using hop latency and adjoining node analysis	Yes	AODV	RTT calculation per hop	Low False positive Rate	Hidden Attack
4.	MLDW(2013)	A Multilayered Detection mechanism for Wormhole attack	Encapsulation is used to launch the wormhole tunnel	AODV	Latency estimator, intermediate node discovery Used	Control Packet overhead	Wormhole Attack
5.	TARF(2012)	Trust aware routing Framework	No	AODV	Trust value calculation	Energy level of malicious node should be high	Hidden Attack
6.	WHOP(2011)	Wormhole detection protocol using Hound packet	Message Digest	AODV	Total hop count involve	Extra overhead	Wormhole Attack
7.	WORMEROS (2008)	A new framework for defending against wormhole attack	Encapsulation is used to launch the tunnel	AODV	RTT calculation, High Latency calculated	High False positive rate due to heavy traffic	Hidden Attack
8.	MOBIWORP (2008)	Detecting & Locating wormhole attack through statistical analysis	No	AODV	Neighbor discovery process confirm wormhole	Overhead, Tracing is required by central authority	Wormhole Attack
9.	LITE-WORP (2207)	Lightweight counter measure for wormhole in multi hop wireless network	Key Pairs are used	NO	Monitor Local Traffic	Only for stationary network	Wormhole Attack
10.	Delphi(2206)	Delay Per Hope Indicator	No	AODV	Work on every possible disjoint path	Complex	Hidden & Exposed Attacks
11.	SECTOR (2004)	Secure Tracking of node in multi hop	Yes	AODV	Require to calculate RTT	Directional Antenna & hardware require	Hidden Attack

7.1 To provide QoS up to a satisfactory level and removal of unwanted errors occurs in the wormhole detection still an open question. Finally it should be kept in mind that is the trade-off between network lifetime, security congestion and live ability. It is challenging issues to resolve all problems together. However the list is still open due to continuous emerging new technology.

REFERENCES :

[1] C.Sivaram Murthy and B.S Manoj, "Ad Hoc wireless Networks", Pearson Education, Second Edition India, 2001.

[2] Y. Zhang and W. Lee, "*Intrusion Detection in Wireless Ad Hoc Networks*," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (ACM MobiCom'00), Boston, MA, pp. 275-283, Aug. 2000. ISBN: 1-58113-197-6 doi: 10.1145/345910.345958

[3] S. Gupta, S. Kar and S. Dhamaraja, "*Wormhole Attack Detection Protocol using Hound Packet*", International Conference on Innovation in Information Technology, IEEE, Jan 2011, pp. 226-231.

[4] S.Y. Shin and E.H. Halim, "Wormhole *Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation*", ICTC 2012, IEEE, July 2012, pp. 781-786.

[5] G.S. Mamatha and S.C. Sharma, "*A Robust Approach to Detect and Prevent Network Layer Attack in MANETS*", International Journal of Computer Science and Security, Vol. No.3, pp 276 -285.

[6] Z.A. Khan and M.H. Islam, "*Wormhole Attack: A new detection technique*", IEEE, July 2012, pp. 1-6

[7] M. Abdelhaq, S. Serhan, R. Alsaqour and R. Hassan, " *A Local Intrusion Detection Routing Security Over MANET Network*", International Conference on Electrical Engineering and Informatics, Indonesia, 17 July 2011, pp. 1-6

[8] H. Weerasinghe and H. Fu, "*Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation*" IEEE, Jan 2007, pp. 274-283.

[9] I. Woungang, S.K. Dhurandher, R.D. Peddi and M.S. Obaidat, "*Detecting Black-hole Attacks on DSR-based Mobile Ad-hoc Networks*", IEEE Jan 2012, pp.1-5

[10] Pirzada, A.A., Datta A.*," Trustworthy Routing with the AODV Protocol*, IEEE, pp. 19-24 (2004)

[11] Prathapani, A. Santhanam, L. Agarwal D.P." *Intelligent Honey Pot Agent for Black Hole Attack Detection in Wireless Mesh Networks"*. IEEE, pp. 753-758 (2009)

[12] Sangi, A.R., Lui J., Sue L.: "A Performance Analysis of AODV Routing Protocol under Combined Byzantine Attacks in MANETs". IEEE, pp. 7-12 (2009)

[13] Bala, A., Bansal, M., Singh, J., *and "Performance Analysis of MANET under Black Hole Attack*": IEEE First International Conference on Networks & Communications. pp. 141—145 (2009)

[14] Shukla, P.K., Bhadauria, S.S, Silakari, S.:"*ARA-MAC: A Qualifying Approach to improving Attack Resiliency and Adaptability in Medium Access Control Protocol for WLAN*" 802.11.: International Journal of Computer Applications (0975 – 8887) Volume 49 – No. 19, pp. 01—10 (2012).

[15] Y. Hu, A. Perrig, and D. Johnson,

"*Packet leashes: a defense against wormhole attacks in Wireless Ad Hoc Networks*", In Proceedings of the IEEE Conference on Computer Communications (Infocom), 2003

[16] L. Hu and D. Evans, "*SECTOR Using directional antennas to prevent wormhole attacks*", in Proceedings of the IEEE Symposium on Network and Distributed System Security (NDSS), 2004.

[17] Lijun Qian, Ning Song, and Xiangfang Li,"*MOBIWORP Detecting and locating wormhole attacks in Wireless Ad Hoc Networks through statistical analysis of multi-path*", IEEE Wireless Communications and Networking Conference - WCNC 2005.

[18] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, "*LITEWORP: A Lightweight countermeasure for the Wormhole Attack in Multihop Wireless Networks*", International Conference on Dependable Systems and Networks (DSN 2005): 612-621.

[19] Hon Sun Chiu King-Shan Lui, "*DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks*", International Symposium on Wireless Pervasive Computing ISWPC 2006.

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

[21] Tran, P.V., Hung, L.X., Lee, Y.K., Lee, S., Lee, H.: TTM: "*An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks*", IEEE Consumer Communications and Networking Conference, 2007.

[22] T. Van Phuong, N. T. Canh, Y. K. Lee, S. Lee, and H. Lee, "*Transmission time-based mechanism to detect wormhole attacks*," in Proceedings of IEEE Asia-Pacific Services Computing Conference (APSCC '07), pp. 172–178, December 2007.

[23] F. Nait-Abdesselam, B. Bensaou, and T. Taleb, "*Detecting and avoiding wormhole attacks in wireless ad hoc networks*," IEEE Communications Magazine, vol. 46, no. 4, pp. 127–133, 2008.

[24] Q. N. Dang and L. Lamont, "*A simple and efficient detection of wormhole attacks*," in Proceedings of the New Technologies, Mobility and Security Conference and Workshops (NTMS '08), pp. 1–5, November 2008.

[25] H. Vu, A. Kulkarni, K. Sarac, N. Mittal, "*WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks*". In Proceedings of International Conference on Wireless Algorithms Systems and Applications, LNCS 5258, pp. 491-502, 2008.

[26] S. Choi, D. Kim, D. Lee, J. Jung, "*WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks*". In International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 343-348, 2008.

[27] Guoxing Zhan, Weisong Shi, Julia Deng,"*Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs*", IEEE Transactions on dependable and secure computing pp 1545- 5971(2012).

[28] Vandana C.P, A. Francis Saviour Devaraj, "*Evaluataion of impact of wormhole attack on AODV*", International Journal of Advanced Networking and Applications, ISSN 0975-0290 Volume: 04 Issue: 04 pp. 1652-1656, 2013.

[29] Vandana C.P, A. Francis Saviour Devaraj, "*WAD-HLA: Wormhole Attack Detection using Hop Latency and Adjoining node analysis in MANET*", International Journal of Advanced Networking and Applications, ISSN 0975-0290 Volume: 04 Issue: 04, 2013.

[30] Nidhi Nigam and Vishal Sharma, "A *Novel Approach for Wormhole Detection in MANET* "International Journal of Computer Applications (0975 – 8887) Volume 63– No.7, February 2013.