PERFORMANCE EVALUATION OF WORM HOLE ATTACK ON AD HOC ON DEMAND MULTIPATH DISTANCE VECTOR ROUTING

[1]RAMYA DORAI, [2] RAJARAM. M

[1]Adhiyamaan College of Engineering, Department of Computer Science Engineering, Hosur, Tamilnadu, India

[2]Vice-chancellor, Anna University, Chennai, Tamilnadu, India

E-mail: [1]ramyadorai.aom@gmail.com

ABSTRACT

Mobile Adhoc Network (MANET) is a self-configuring network of mobile nodes connected by wireless links. Security is a dominant concern in MANET due to its intrinsic vulnerabilities. MANETs are receptive to attacks due to its open medium, dynamically changing network topology, cooperative algorithms, lack of central monitoring and management point, and lack of a line of defense. Nodes depend on each other for packet transmission from source node to destination node through routing. The efficiency of a network degrades due to the presence of malicious nodes. This study evaluates the impact of wormhole attack on MANET. Adhoc On-demand Multipath Distance Vector (AOMDV) routing is considered for evaluation.

Keywords: *Multimodal Biometrics, Fingerprint, Finger Vein, Radial Basis Function (RBF) Classifier, BAT, Gravitational Search*

1. INTRODUCTION

A MANET forms a temporary/short-lived network without fixed infrastructure where nodes move freely and randomly and configure themselves. In MANETs, a node is both router and host with network topology changing swiftly [1]. MANETs face many operating constraints like limited battery charge per node, limited transmission range and limited bandwidth. Generally MANET routes are often multi-hop by nature [2].

MANET nodes perform the routing functions in addition to being hosts. Wireless transmission range limitations require multiple hops routing. So nodes, depend on each other for packet transmission from source node to destination node through routing. Networks nature places two basic requirements on routing protocols. First, it must be distributed and second, as topology changes frequently, it must compute multiple, loop-free routes while ensuring minimum communication overheads. MANET routing protocols fall into three general categories based on route discovery time: Proactive, Reactive and Hybrid routing protocols [3].

Network security is arguably an important global issue. MANETs are prone to attacks due to their inherent nature of node mobility and lack of a central governing infrastructure. The methods used in wired networks for security are not directly applicable to ad hoc networks [4]. MANET attacks are classified into passive attacks and active attacks, according to attack means. A passive attack does not disrupt normal network operation; attacker snoops data exchanged in network without touching it but confidentiality is violated. Passive attack detection is difficult as network operation is not affected. Passive attacks are listed as eavesdropping, traffic analysis and traffic monitoring [5].

An active attack alters or destroy data being exchanged in a network thus disrupting normal network functioning. Active attacks are either internal or external. External attacks are from nodes not of the network. Internal attacks are from compromised nodes within the network. As the attacker is part of the network, internal attacks are more severe and harder to detect than external attacks. Active attacks, whether by external adversary or internal compromised node involves actions like impersonation, fabrication, modification and replication [6]. Active attacks include black hole, wormhole, gray hole, resource consumption, information disclosure, routing attacks and also include jamming, modification, impersonating, Denial of Service (DoS) and message replay.

Multipath routing is transmitting data using more than one path from sender to receiver reducing risk of adversaries monitoring traffic in all paths from the sender. This assumes that an adversary cannot monitor all paths simultaneously due to practical infeasibility. Multipath routing attracted attention including a research on use of multipath routing for secure data delivery [7].

A wormhole is an attack against a MANET routing protocol where two or more nodes create an illusion that two remote network regions are directly linked through nodes that seem neighbors, but are actually distant from each other [8]. This shortcut is created by connecting apparent neighbors through a secret communication channel/tunnel, generated by an attacker introducing transceivers linked to each other with a high quality but low-latency link. Thus, the attacker takes transmitted packets from one region and reinserts them into another.

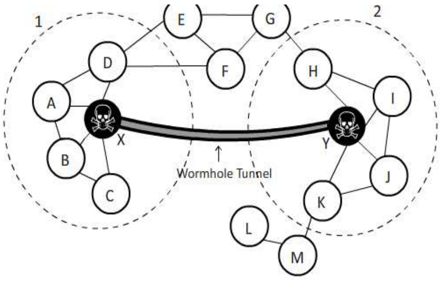

Figure 1 Wormhole Attack (Between X And Y There Is A Wormhole Attack Which Forms A Tunnel)

There are many negative repercussions for Ad-Hoc networks in a successful Wormhole attack. Consequences can be, according to:

- **Eavesdrop on communication**: Process intercepting packets flow in network.
- **Spoofing attack**: Injecting bogus packets / impersonating another sender.
- **Record packets**: Using eavesdropping on communication generates copies of intercepted packets flow in the network.
- **Replay the packets**: Passively re-inserting packets elsewhere in the network. Actively follows same process but alters intercepted packets.
- **Unauthorized Access**: Malicious node enters a node group or subgroup, masquerading as if from the network.
- **Disrupt routing**: In route discovery, the attack interrupts normal flow of protocols searching for a valid path. A consequence of this can be a Sinkhole attack where a trusted node, modifying routing packets and masquerading as a trusted one, attracts other nodes ensuring that all traffic passes through it, to launch centralized attacks.
- **Denial-of-Service (DoS)**: After having supplanted a reliable node with valid routes for packet forwarding, malicious nodes discard messages received and do not send them to destination node. This attack is also called a Black Hole Attack [9].
- **Selectively discarding data packets**: It is a Black Hole Attack but does not drop all intercepted packages. This is known as Gray Hole Attack.
- **Clandestine traffic analysis** [10]: At a given time t Wormhole tunnel obtains traffic statistics from network to use them against it.
- **Creating routing loops**: To waste network energy.

In this study, the effects of the wormhole attack on the performance of the network are investigated. Investigations are carried out for varying maliciousness to study the impact on network performance such as throughput, number of hops and route discovery time. Ad hoc On-demand Multipath Distance Vector (AOMDV) routing is used for evaluation.

2. RELATED WORK

Wormhole attacks on MANET were analyzed with different routing protocols including OLSR and AODV by Sadeghi and Yahya [11] with the aim to find out which was more vulnerable. OPNET simulation was used and results revealed that AODV was more vulnerable compared to OLSR. Hence, MANET applications using proactive routing protocols were more trusted compared to reactive protocols.

Wormhole attacks in MANET were reviewed by Maulik and Chaki [12]. MANET's use of wireless medium for communication made them vulnerable to many security attacks. A comprehensive review on recent state of the art research results upon wormhole attacks and applicable mitigation measures was performed. All works reviewed here were published in last five years, of which 80% were published in last three years. Simulation results in NS2 quantified comparative performances of the proposed solutions.

An evaluation comparison of AODV and DSR routing protocols in MANET was performed by Ahuja, et al., [13]. Wormhole was one of the many attacks on MANETs. AODV and DSR routing protocols performance was evaluated under wormhole attack and it was compared to their performance without such an attack. Performance parameters included Throughput, average end to end delay and Packet Delivery Patio (PDR). Qualnet Simulator 5.0 was used for simulation.

An efficient wormhole attack detection method named Modified wormhole detection AODV protocol (MAODV) was proposed by Chaurasia and Singh [14]. Wormhole attack detection was performed by using hops in various paths from source to destination and delay of a node in varied paths from source to destination. The destination detected both types of wormhole attacks. Simulations justified the performance of MAODV protocol.

An Advanced Encryption Standard (AES) based routing algorithm (AODV-Wormhole Attack Detection Reaction - called AODV-WADR-AES) to secure AODV based MANETs against wormhole attacks was investigated by Woungang, et al., [15]. This included substituting the AES part by Triple Data Encryption Standard (TDES), yielding AODV-WADR-TDES routing algorithm, to study the algorithm's performance where mobile devices incompatible with AES were part of eMANET nodes. Simulation showed that AODV-WADR-AES scheme outperformed AODV-WADR-TDES scheme regarding end-to-end delay, PDR and number of packets traversing the wormhole link.

A survey on wormhole attack in MANET was undertaken by Nagrath and Gupta [16]. Adhoc networks are very open by nature. Anyone with proper hardware and network topology knowledge and protocols can connect to a network thereby permitting potential attackers to infiltrate a network to attack its participants to either steal or alter information. The Wormhole attack doesn't need to exploit any network node as it can interfere with route establishment. MANET's total routing system can even be brought down through a wormhole attack. This study discusses modes of wormholes, how they disrupt routing in AODV, DSR, OLSR and also explains solutions and countermeasures on wormholes.

Wen-Cheng, et al., [17] undertook research on AODV routing protocol whose running process includes two procedures like route finding and route maintenance. AODV protocol uses the hop-by-hop routing method to transmit packets. Wormhole attack was a special attack aimed at adhoc networks. Based on AODV protocol analysis and attack conditions of wormhole attack, the method and algorithm aimed at wormhole attack were researched and a method to improve AODV protocol was suggested.

A new detection mechanism for wormhole attack called RTT-TC, based on Round Trip Time (RTT) measurements and Topological Comparisons (TC) was presented by Alam and Chan [18]. In a wormhole attack, the collaborators are spurious entities who silently record packets at a location and tunnel them to another in the network. This type of attack is possible even when the network uses authentication. The new scheme was evaluated with MANET running an AODV routing protocol. Simulation showed the new method achieving high detection rate and alarm accuracy.

Xiu-feng, et al., [19] analyzed wormhole attack topology and then combined cryptography and trust mechanism to design a new Multipath Trust-based Secure Routing protocol (MTSR). MTSR based on AODV and SAODV was distributed and resists almost all available routing attacks like discarding, flooding, spoofing, Sybil, jamming, rushing and specially wormhole attack. Its trust value computation uses the principle of slowly increasing and decreasing sharply and requires no additional equipment, strict assumptions, node location or precise time information.

3. METHODOLOGY

3.1 Wormhole Attacks

Wormholes are classified based on resources used for attacks:

1. According to attack mode, Wormhole is classified as:

- Wormhole using encapsulation
- Wormhole Out-of-Band Channel
- Wormhole with High Power Transmission
- Wormhole using Packet Relay
- Wormhole using Protocol Deviations

2. Depending on whether attackers are visible in paths [20] Wormholes are classified as:

- **Open Wormhole Attack:** The attackers are themselves in a RREQ packet header following route discovery procedure. Other nodes know that malicious nodes lie on the path but think that such nodes are direct neighbors.
- **Half open Wormhole Attack:** One side of a wormhole does not modify a packet and only the other modifies the packet after route discovery procedure.
- **Closed Wormhole Attack:** The attackers do not modify packet content, even when the latter is a route discovery packet. Instead they simply tunnel the packet from one side of the

wormhole to the other and rebroadcast the packet.

3. Depending on resources used for an attack Wormhole is classified as:

- **Out-of-band wormholes:** The colluder nodes establish a direct link between a wormhole tunnel's two end-points in a network. This link is created using an external wired link. This is also called Hidden Wormhole Attack [21], using hardware introduced by attacker and without compromising network hosts.
- **In-band wormholes:** An in-band wormhole needs no additional hardware infrastructure. It consumes existing communication medium capacity to route tunneled traffic. Thus, the network's own nodes are involved in the attack [22]. This attack is of 2 types: self-contained in-band wormhole and extended in-band wormhole.
    - **Self-contained in-band Wormhole:** a subtype of "Inband wormhole" it uses network resources and involves other nodes in the network. Intruders create a false link between attacker nodes themselves.
    - **Extended in-band Wormhole:** Also known as Exposed Wormhole Attack and Byzantine Wormhole Attack [23], it is another "In-band Wormhole" subtype which creates a wormhole that extends beyond attackers by forming tunnel endpoints. A false link is advertised between two nodes which are not attacker nodes.

3.2 AOMDV multipath protocol

The AOMDV routing protocol is a multipath extension of the AODV protocol which aims to find loop-free and link-disjoint multipaths during route discovery. AOMDV uses advertised hop-count to guarantee loop free feature. Advertised hop-count is the maximum hop-count of multiple paths to destination node d available at intermediate node i. It ensures that alternate paths at each node are disjoint, and so achieves path disjoint-ness without source routing [24]. AOMDV route tables have a list of paths for each destination to support multipath routing. All paths to a destination have same destination sequence number. AOMDV route maintenance is similar to that in AODV. A RERR for a destination is generated when last path to that destination fails.

The basis of the AOMDV protocol is in guaranteeing that multiple routes revealed are loop-free and disjoint, and in discovering paths through a flood-based route discovery. AOMDV path revise rules exploited locally at every node and have a major role in preserving loop-freedom and disjoint-ness characteristics. The AOMDV [25] protocol locates multiple paths involving two stages which are: i) A route update rule establishes and maintains multiple loop-free paths at every node, and ii) A distributed protocol locates link-disjoint paths. AOMDV protocol locates node-disjoint or link-disjoint and it is dependent more on routing information previously available in the fundamental AODV protocol, thus preventing overhead acquired to determine multiple paths. Specifically, it does not use any specific control packet. Additional RREPs and RERRs for multipath discovery and protection together with extra fields in routing control packets (i.e., RREQs, RREPs, and RERRs) are the only extra overhead in AOMDV compared to AODV [26].

AOMDV suppresses duplicate Route Requests (RREQs) at intermediate nodes in two different variations, resulting in either node as seen in figure 2 (a) or a link as in Figure 2(b) disjoint. AOMDV can be configured to either to discover the link or node disjoints paths. Disjoint alternate paths are a better choice than overlapping alternate paths, as probability of interrelated and concurrent failure is reduced [27]. This helps in an adversarial environment where malicious activity can lead to additional link failure. Finding a disjoint path is straightforward in source routing, but hop-by-hop routing i.e. AOMDV is more efficient regarding creating less overhead number of paths in any source and destination and is directly proportional to number of nodes in the network. AOMDV works efficiently in dense and heavy networks.

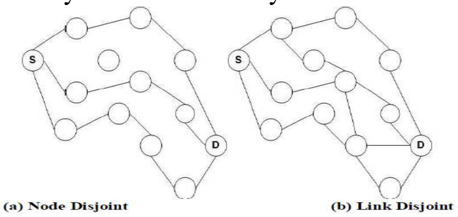

Figure 2 AOMDV Multipath (A). Node Disjoint And (B). Link Disjoint

4. EXPERIMENTAL RESULTS

AOMDV routing protocol is used for evaluating the network performance under wormhole attack. The simulations are carried out with 15% and 30% of the nodes being malicious. The figure 3 to 6 shows throughput, route discovery time, average number of hops and average cache replies used respectively with 15%, 30 % of malicious nodes and without malicious. The table 1 to 4 shows the same as figure 3 to 6.

Table 1 Throughput In Bits/Second

SIMULATION TIME IN SECOND	THROUGHPUT IN BITS/SECOND		
	WITH 15% OF NODES BEING MALICIOUS	WITH 30% OF NODES BEING MALICIOUS	WITHOUT MALICIOUS NODES
0	145024	92858.66667	192630.2222
90	705952	387385.7778	962219.5556
180	749464	406205.3333	1025188.444
270	684924.4444	350461.3333	1086577.778
360	698288.8889	351782.2222	969894.2222
450	727837.3333	375069.3333	965991.1111
540	790920.8889	396460.4444	1031745.778
630	744360	366158.2222	1103592
720	732068.4444	338061.3333	1095487.111
810	696901.3333	354487.1111	1051896.889
900	#N/A	#N/A	#N/A

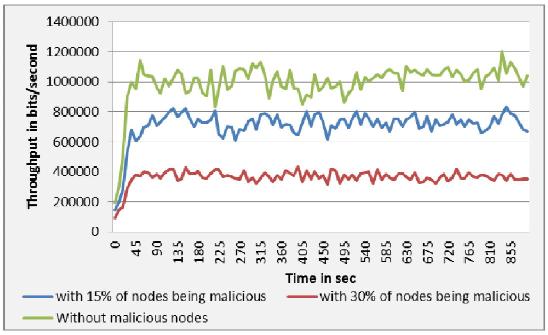

Figure 3 Throughput In Bits/Second

From figure 3 it is observed that the throughput is decreased due to the wormhole attack for AOMDV, with 15 % and 30 % of nodes being malicious. Throughput is high only for the nodes without malicious nodes.

Table 2 Average Number Of Hops

Simulation time in second	Average number of hops		
	with 15% of nodes being malicious	with 30% of nodes being malicious	Without malicious nodes
0	2.111856823	1.940944882	2.00955414
90	3.75	3	2.379310345
180	2.5	2.666666667	1
270	3	2.583333333	2
360	2.666666667	2.5	2.285714286
450	3	3	1.4375
540	3	3	1.4375
630	2.5	3	1.666666667
720	4.5	3	1.25
810	2.571428571	3	1.782608696
900	2.571428571	2.625	1.875

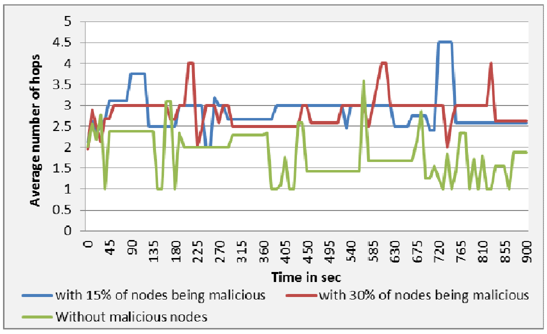

Figure 4 Average Number Of Hops

From figure 4 it is observed that the average number of hops is increased due to the wormhole attack for AOMDV with 15 % and 30 % of nodes being malicious. Average number of hops is low only for the nodes without malicious nodes.

Table 3 Route Discovery Time in second

Simulation time in second	Route Discovery Time in second		
	with 15% of nodes being malicious	with 30% of nodes being malicious	Without malicious nodes
0	0.37739186	0.275366156	0.304826769
90	0.078941221	0.07911354	0.060347817
180	0.069385309	0.060399064	0.056045869
270	0.064641246	0.054707401	0.052434672
360	0.061549018	0.050996281	0.051283371
450	0.057587858	0.053711556	0.049028792
540	0.05554929	0.055594557	0.045647299
630	0.05301865	0.054276174	0.046341383
720	0.051644931	0.054220428	0.045054744
810	0.050095859	0.052290957	0.045398673
900	0.051050493	0.055115432	0.04637335

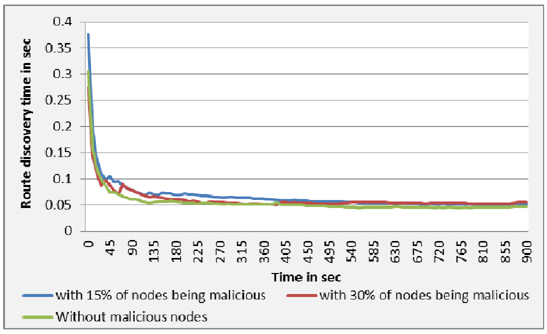

Figure 5 Route Discovery Time In Sec

From figure 5 it is observed that the time taken for route discovery is high due to the wormhole attack for AOMDV with 15 % and 30 % of nodes being malicious. The time taken for route discovery is less only for the nodes without malicious nodes.

Table 4 Average Cached Replies used

Simulation time in second	Average Cached Replies used		
	with 15% of nodes being malicious	with 30% of nodes being malicious	Without malicious nodes
0	74	40	125
90	35.18182	32.63636	67.09091
180	41.7619	39.33333	73.33333
270	40.16129	38.51613	70.90323
360	39.4878	39.70732	71.02439
450	39.72549	41.92157	69.09804
540	38.52459	41.63934	68.63934
630	39.05634	41.78873	68.77465
720	39.97531	40.7037	68.97531
810	40.54945	40.93407	68.21978
900	#N/A	#N/A	#N/A

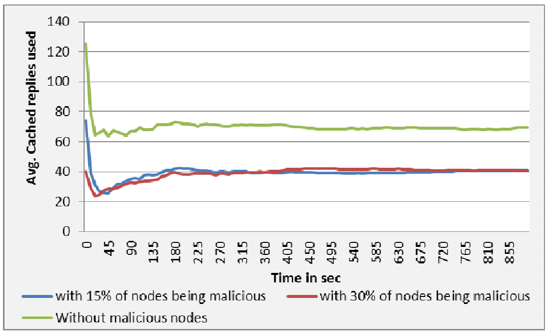

Figure 6 Average Cached Replies Used

From figure 6 it is observed that the average cached replies is low due to the wormhole attack for AOMDV with 15 % and 30 % of nodes being malicious. The average cached replies is high only for the nodes without malicious nodes.

5. CONCLUSION

Network security is arguably an important global issue. A wormhole is an attack against a MANET routing protocol where two or more nodes create an illusion that two remote network regions are directly linked through nodes that seem neighbors, but are actually distant from each other. AOMDV routing protocol evaluated impact of wormhole attack on MANETs. Simulations were carried out with 15% and 30% of nodes being malicious. The resulting graph showed throughput, route discovery time, average hops number and average cache replies used respectively with 15%, 30 % of malicious nodes and without malicious nodes.

6. REFRENCES

[1] Taneja and Kush "A Survey of Routing Protocols in Mobile Ad Hoc Networks", 2010.

[2] Tantubay "A Review of Power Conservation in Wireless Mobile Adhoc Network (MANET)", 2011.

[3] Agrawal, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", 2011.

[4] Sanyal "A NOVEL MULTIPATH APPROACH TO SECURITY IN MOBILE AD HOC NETWORKS (MANETs)".

[5] Mamatha and Sharma "Network Layer Attacks and Defense Mechanisms in MANETS- A Survey", 2010.

[6] Jawandhiya "A Survey of Mobile Ad Hoc Network Attacks", 2010.

[7] W.Lou, and Y.Fang, "A multipath routing approach for secure data delivery", *MILCOM 2001*, 2, 1467, 2001.

[8] Kruus, Peter; Sterne, Dan; Gopaul, Richard; Heyman, Michael; Rivera, Brian; Budulas, Peter; Luu, Brian; Johnson, Tommy; Ivanic, Natalie; Lawler, Geoff; , "In-Band Wormholes and Countermeasures in OLSR Networks," Securecomm and Workshops, 2006 , vol., no., pp.1-11, Aug. 28 2006-Sept. 1 2006.

[9] Hoang Lan Nguyen; Uyen Trang Nguyen; , "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks," Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on , vol., no., pp. 149, 23-29 April 2006.

[10] Mahajan, V.; Natu, M.; Sethi, A.; , "Analysis of wormhole intrusion attacks in MANETS," Military Communications Conference, 2008. MILCOM 2008. IEEE , vol., no., pp.1-7, 16-19 Nov. 2008.

[11] Sadeghi, M., & Yahya, S. (2012, July). Analysis of Wormhole attack on MANETs using different MANET routing protocols. In *Ubiquitous and Future Networks (ICUFN), 2012 Fourth International Conference on* (pp. 301-305). IEEE.

[12] Maulik, R., & Chaki, N. (2010, October). A comprehensive review on wormhole attacks in MANET. In *Computer Information Systems and Industrial Management Applications (CISIM), 2010 International Conference on* (pp. 233-238). IEEE.

[13] Ahuja, R., Ahuja, A. B., & Ahuja, P. (2013, December). Performance evaluation and comparison of AODV and DSR routing protocols in MANETs under wormhole attack. In *Image Information Processing (ICIIP), 2013 IEEE Second International Conference on* (pp. 699-702). IEEE.

[14] Chaurasia, U. K., & Singh, V. (2013, August). MAODV: Modified wormhole detection AODV protocol. In *Contemporary Computing (IC3), 2013 Sixth International Conference on* (pp. 239-243). IEEE.

[15] Woungang, I., Dhurandher, S. K., Koo, V., & Traore, I. (2012, December). Comparison of two security protocols for preventing packet dropping and message tampering attacks on AODV-based mobile ad Hoc networks. In*Globecom Workshops (GC Wkshps), 2012 IEEE* (pp. 1037-1041). IEEE.

[16] Nagrath, P., & Gupta, B. (2011, April). Wormhole attacks in wireless adhoc networks and their counter measurements: A survey. In *Electronics Computer Technology (ICECT), 2011 3rd International Conference on* (Vol. 6, pp. 245-250). IEEE.

[17] Wen-Cheng, J., Jing, P., & Jian-Ling, Z. (2010, September). Research and Improvement of AODV Protocol in Ad Hoc Network. In *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on* (pp. 1-3). IEEE.

[18] Rafiqul Alam, M., & Chan, K. S. (2010, November). RTT-TC: A topological comparison based method to detect wormhole attacks in MANET. In*Communication Technology (ICCT), 2010 12th IEEE International Conference on* (pp. 991-994). IEEE.

[19] Xiu-feng, Q., Jian-wei, L., & Sangi, A. R. (2010, November). MTSR: wormhole attack resistant secure routing for ad hoc network. In *Information Computing and Telecommunications (YC-ICT), 2010 IEEE Youth Conference on* (pp. 419-422). IEEE.

[20] M. Azer, S. El-Kassas, and M.M.S. El-Soudani, "A Full Image of the Wormhole Attacks - Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks", presented at CoRR, 2009.

[21] Xia Wang; Wong, J.; , "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks," Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International , vol.1, no., pp.39-48, 24-27 July 2007.

[22] R. Gopaul, P. Kruus, D. Sterne, and B. Rivera, "Gravitational analysis of the in-band wormhole phenomenon", Proc. 25th Army Science Conference, Orlando, FL, Nov. 2007.

[23] Eriksson, J.; Krishnamurthy, S.V.; Faloutsos, M.; , "TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks," Network Protocols, 2006. ICNP '06. Proceedings of the 2006 14th IEEE International Conference on , vol., no., pp.75-84, 12-15 Nov. 2006.

[24] Tekaya, “Multipath Routing with Load Balancing and QoS in Ad hoc Network”, 2010.

[25] V.C.Patil, Rajashree, V.Biradar, R.R. Mudholkar, S.R.Sawant, “On-Demand Multipath Routing Protocols for Mobile Ad Hoc Networks Issues and Comparison”, International Journal of Wireless Communication and Simulation, 2010,Vol. 2(1), pp. 21-38.

[26] Jain “Trust Based Routing Mechanism Against Black Hole Attack Using AOMDV-IDS System In MANET Format”, 2012.

[27] Giri, “Analysis of DHT Based Multi-Path Routing Protocol with Other Routing Protocols in MANETS”, 2012.