International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 5 (2016) pp 3282-3288
 https://dx.doi.org/10.37622/IJAER/11.5.2016.3282-3288

# Evaluation Performance of Worm-Hole Attack Using Proposed AODV In MANET

**Satheesh N**
*Research Scholar, Department of CSE, Karpagam University, Coimbatore, Tamil Nadu, India.*

**Prasadh K**
*Principal, Mookambika Technical Campus, Ernakulam, Kerala, India.*

**Abstract**
A Mobile Ad hoc Network (MANET) is a collection of self-configuring nodes which uses the wireless link between communicating devices (mobile devices) to form an arbitrary topology without infrastructure. Dynamic topological changes caused by high node mobility make routing and securing communication challenging. Thus, the MANET is vulnerable to attacks due to their dynamic, lack of both distributed infrastructure and centralized authority. This study proposes an improved Ad Hoc On-Demand Distance Vector (AODV) where two packets are introduced, Hello_src and Src_reply, to mitigate the wormhole attack. Wormhole attack impact is analyzed with the proposed AODV Routing protocol. Parameters like end to end delay, throughput, and cache replies number evaluated performance.

**Keywords:** Mobile Ad Hoc Network (MANET), Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol, Wormhole attack, end to end delay, throughput, cache replies, Hello_src, Src_reply.

## Introduction

Ad hoc network technology development and use of mobile and hand-held devices ensure that MANETs plays a big role in information technology. MANET supports mobile nodes, wireless links for connectivity, without pre-existing communication infrastructure [1]. MANET nodes communicate with each other's wireless transmission ranges. Thus, in a multi-hop concept various intermediate hosts transfer packets sent by the source node before it reaches destination node. Communication success between two nodes is dependent on other nodes' cooperation. A MANET is self-configuring and is formed automatically by mobile nodes without fixed infrastructure or centralized management [2].

MANETs is vulnerable to attacks due to their dynamic, distributed infrastructure less nature and also due to its lack of centralized authority. Limited power backup and individual nodes computational capability hinder complex security algorithms and key exchange mechanisms implementation. Node mobility ensures dynamic network topology forcing frequent networking reconfigurations which creates additional chances for attacks. Generally MANET attacks are categorized into active or passive attacks [3].

Passive attacks do not disrupt normal network operations; the attacker snoops on data exchanged in a network without touching it. Nonetheless, confidentiality is violated. Passive attacks are hard to detect as the network operation is not touched. A solution is to use powerful encryption mechanism to encrypt data for transmission, making it tough for an attacker to get useful information from data overheard. Passive attacks are listed as traffic analysis, eavesdropping and traffic monitoring [4].

An active attack alters or destroys data being exchanged in the network disrupting normal network functioning. Active attacks are classified as internal or external attacks. External attacks are by nodes, not of the network. Internal attacks are by compromised nodes which form part of the network. As the attacker is part of the network, internal attacks are severe and harder to detect than external attacks. Active attacks by an external advisory or by internal compromised node involve actions like modification, impersonation, fabrication and replication [5]. Active attacks include black hole, wormhole, gray hole, resource consumption, information disclosure, routing attacks and also includes impersonating, jamming, modification, Denial of Service (DoS), and message replay.

Wormhole attack affects even single nodes. Usually two or more attackers connect through a link called wormhole link. Such attacks captures packets at one end and replay them at the other using private high speed network. Wormhole attacks are easy to put on, but they damage network greatly. Figure 1 shows a wormhole attack and a link between node x and y.

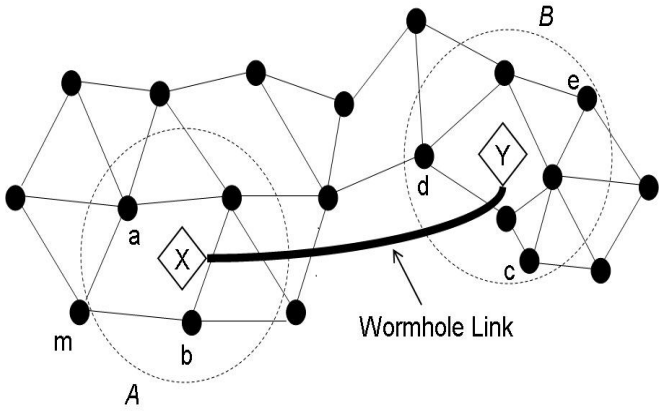


**Figure 1:** Wormhole Attack

Wormhole attacks are replay attacks that are specifically challenging in MANETs. Even if routing information is confidential, by encryption or authentication, wormhole attack can be effective and damaging. An attacker tunnels a request packet RREQ to the destination node without increased hop-count value from the source node preventing other routes from discovery. Wormhole attack can be merged with message dropping attacks to prevent destination nodes from receipt of packets [6].

An improved AODV is proposed in this study where two packets-Hello_src and Src_reply-are introduced, and impact of wormhole attack on MANET is evaluated. This study is structured as follows: Section II reviews related works available in the literature. Section III details AODV routing and performance metrics to evaluate wormhole attack impact on MANET and the Haval hash function. Section IV provides experimental results and section V concludes the paper.

## Related Work

Security issues are of paramount interest in wireless networks than in wired networks. The wormhole attack is a disturbing attack in wireless networks, where two or more malicious nodes create a bigger virtual network tunnel, used to transport packets between tunnel end points. Such tunnels emulate shorter network links where the adversary records transmitted packets at one network location, tunnels them to another and then retransmits them into the network. Anita, et al., [7] analyzed performance of a On Demand Multicast Routing Protocol (ODMRP) under influence of wormhole nodes under varied scenarios and to design a Worm Hole Secure ODMRP (WHS-ODMRP) by applying a certificate based authentication mechanism in route discovery. The new protocol reduced packet loss due to malicious nodes considerably and enhanced performance.

A trust based Ad hoc On Demand Routing protocol for MANET was presented by Gupta and Pandey [8]. The suggested algorithm works on the honest value concept calculated on concept of hop and trust to protect network from malicious nodes. The proposed protocol's performance was analyzed using throughput, drop packets number, packet delivery ratio and received packets number with variation of node numbers, speed and simulation time. Results proved that the proposed method performed better and enhanced network security.

A well-organized method to detect and elude wormhole attacks in OLSR protocol was proposed by Naït-Abdesselam [9] which attempted to pinpoint links that were part of a wormhole tunnel. Then with the application of a proper wormhole detection mechanism to suspicious links by exchanging encrypted probing packets between two supposed neighbors was undertaken. This has many advantages, including its non-reliance on time synchronization or location information and high detection rate under varied scenarios.

An eigen vector and degree centrality to evaluate individual trust value was proposed by Kumar and Parthipan[10]. They designed and built NS2 over Dynamic Source Routing (DSR) prototype, during a Worm Hole Attack in a highly mobile and hostile environment.

Message authentication effectively prevents bogus messages and MANET worm-hole attacks. But, it can be a double-edge sword threatening mobile user privacy, e.g., location privacy, if authenticity proofs used in message authentication were abused. Such abuse was prevented by Liang, et al., [11], who suggested a new message authentication scheme, which ensures users identity privacy and non-transferability. They introduced information based on a theoretical model to gauge privacy levels that the proposed scheme attained. Simulation results proved the proposed scheme could greatly reduce violation of MANET mobile users' privacy.

Gateway nodes provide connectivity to nodes in MANET. Vulnerability of gateway where adversaries could forcibly introduce routes with wormholes to exploit routing race conditions was identified by Das, et al., [12], and termed pseudo routes. The pseudo route attack was a generalized wormhole attack where wormhole start and end points are any two nodes on the route with even multiple wormholes being present on same route. End-to-end approach with localization information detects and prevents pseudo route attacks. Simulation revealed that the impact was more when the gateway was at network corner.

AODV protocol security was influenced by malicious node attack where such nodes inject a fake route reply claiming to have shortest and freshest route to destination. But, when data packets arrive, malicious nodes discard them. To prevent malicious node attack, PPN (Prime Product Number) scheme was presented to detect and remove malicious node by Gambhir and Sharma [13].

Active Peer-to-Peer (P2P) worms attack neighbour peers based on a hit-list and pose a threat to both P2P network and Internet. Luo, et al., [14] presented a mathematical model of an active P2P worm propagation where simulate active P2P worms spread after analyzing the mathematical model. Results shows factors which affect active P2P worms propagation like state of P2P network, scan rate of P2P worms and security knowledge peers have. They also study the last phase of active P2P worms spread and discover that very limited P2P network space guaranteed active P2P worm self-propagation when timely repair of security holes by peers was impossible for many reasons.

A novel algorithm to detect worm-hole attacks in wireless multi-hop networks using connectivity information to search for forbidden substructures in connectivity graph was proposed by Maheshwari, et al., [15]. The new approach totally localized the algorithm being independent of wireless communication models. But, knowledge of model and node distribution estimated a parameter in the algorithm. Simulation results for three different communication models and two different node distributions show the algorithm detecting wormhole attacks with 100% detection and 0% false alarm probabilities when network was connected to high probability. At very low densities, network disconnection chances were high as also the detection probability.

An agent based log analyzing system integrating P2P network concepts and mobile agents to realize detection and protection from damage caused by worms in early stages was proposed by Katoh, et al., [16]. Experimental results revealed the proposed system collected useful information from a wide

network area, and ensured flexible and on-demand network traffic logs analysis to detect hostile network attacks.

## Aodv Reactive Routing Message Formats

AODV is a reactive routing protocol using RouteRequest (RREQ), RouteReply (RREP) and RouteError (RERR) as control signals. Message Formats for AODV's RREQ, RREP and RERR is as follows:

***Message Formats in AODV***

| Type | J | R | G | D | U | Reserved | Hop Count |
|---|---|---|---|---|---|---|---|
| RREQ ID | | | | | | | |
| Destination IP Address | | | | | | | |
| Destination Sequence Number | | | | | | | |
| Originator IP Address | | | | | | | |
| Originator Sequence Number | | | | | | | |

**Figure 2:** Route Request message (RREQ)

The Route Request message format is illustrated in figure 2 and contains the following fields:

| | |
|---|---|
| Type | 1 |
| J | Join flag; reserved for multicast. |
| R | Repair flag; reserved for multicast. |
| G | Gratuitous RREP flag; indicates whether gratuitous RREP should be unicast to specified node in Destination IP Address field. |
| D | Destination only flag; indicates that destination may respond to RREQ. |
| U | Unknown sequence number; indicates destination sequence number is unknown. |
| Reserved | Sent as 0; ignored on reception. |
| Hop Count | Number of hops from Originator IP Address to node handling request. |
| RREQ ID | A sequence number uniquely identifying specific RREQ in conjunction with originating node's IP address. |
| Destination IP Address | The IP address of destination for which route desired. |
| Destination Sequenc | The last sequence number received from originator for any route to the destination. |
| Originator IP Address | IP address of node which originated Route Request. |
| Originator | The current sequence number for use in route entry points towards route request originator. |

| Type | R | A | Reserved | Prefix Size | Hop Count |
|---|---|---|---|---|---|
| Destination IP Address | | | | | |
| Destination Sequence Number | | | | | |
| Originator IP Address | | | | | |
| Life Time | | | | | |

**Figure 3:** Route Reply message (RREP)

The Route Reply message format is illustrated in figure 3, and includes the following fields [17]:

| | |
|---|---|
| Type | 2 |
| R | Repair flag; used for multicast. |
| A | Acknowledgment required; |
| Reserved | Sent as 0; ignored on reception. |
| Prefix Size | If non-zero, 5-bit Prefix Size specifies that indicated next hop may be used for nodes with similar routing prefix (defined by Prefix Size) as requested destination. |
| Hop Count | Number of hops from Originator IP Address to Destination IP Address. For multicast route requests this indicates hops number to multicast tree member sending RREP. IP address of destination's route is supplied. Destination sequence number associated with the route. |
| Originator IP Address | IP address of node which originated RREQ for which the route is supplied. |

Lifetime The time in milliseconds and nodes receiving RREP consider route valid.

| Type | N | Reserved | Destination Count |
|---|---|---|---|
| Unreachable Destination IP Address | | | |
| Unreachable Destination Sequence Number | | | |
| Additional Unreachable Destination IP Address (If needed) | | | |
| Additional Unreachable Destination Sequence Number (If needed) | | | |

**Figure 3:** Route Error message (RERR)

The Route Reply message format is illustrated above, and has the following fields [18]:

| | |
|---|---|
| N | flag |
| Reserved | 0 (RERR is ignored) Number of out-of-reach destinations. |
| Unreachable Destination IP Address | Destination's IP address is not reachable due link problem Destination sequence number whose IP address is not reachable due to link breakage. |

***AODV-Route Discovery***

Figure 4 explains route discovery in AODV routing protocol.

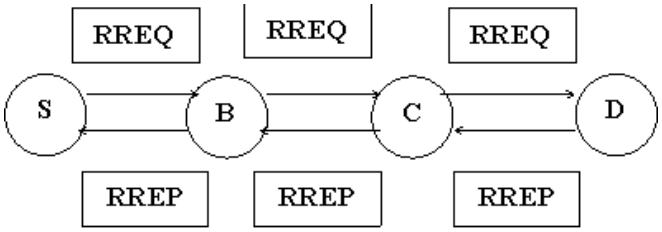


**Figure 4:** AODV Routing Discovery

Source node S broadcasts RREQ throughout network. When a RREP message is received, a node creates or update route to destination D. The hop count is incremented by one and updated RREP is then forwarded to originator of the corresponding RREQ. Source node S receives a RREP if there are destination paths. Buffered data packets are sent to destination D on newly discovered path. If a link failure occurs, then node generates a RERR message having addresses and corresponding destination sequence number of active destinations that are unreachable due to link failure. The RERR message is forwarded to all neighbors who are precursors of unreachable destinations on the node. A node on receipt of a RERR invalidates corresponding entries in routing table, removing destinations without the transmitter of RERR as next hop from unreachable destinations list. If there are destination originators in the cropped list, then updated RERR is forwarded to them [19].

Usually, AODV routing protocols do not reset a new shortest routing path during expiry, as it has to maintain it till nodes are disconnected. Hence, improved AODV routing protocol is proposed to reset a new shortest routing path during packet forwarding. Improved AODV routing protocol maintains expiry time created first. So, in routing table expiry time is not updated. It is updated in a cycle.

***Proposed message packets for AODV***

In wormhole attacks, a hostile node monitors channel, records packets overheard in its vicinity, and tunnels them to remote located colluding node, who replays them in its floor. When tunnelling targets routing control packets like HELLO messages and RREQ, nodes close to attackers cannot discover legitimate routes originating and ending in vicinity of the two attackers respectively: In typical wormhole attack scenario, such legitimate routes span more hops than one or two hops declared by wormhole attackers. This severely disrupts network operation.

An efficient method to detect and prevent wormhole attacks in AODV is proposed in this research by introducing Hello_src and Src_reply. The new solution tries to pinpoint links that could belong to wormhole tunnels, and applies to suspicious links an appropriate wormhole detection mechanism through an exchange of hash keyed probing packets between source and destination.

Every node regularly broadcasts a HELLO message to discover its one-hop neighbors. On receipt of a HELLO message, a node regards the HELLO message originator as neighbor. On the other hand, in a wormhole attack, this message is replayed from afar (more than one hop away). While this does not compromise nodes, it gives wrong information to underlying routing protocol and ultimately causes its failure in locating adequate routes. Two nodes are regarded as neighbors only if they are in transmission range of each other. In the proposed approach, network links with high probability to be involved in a wormhole attack are first detected. A commonly accepted and invoked wormhole attacks representative feature consists of relatively longer packet latency compared to normal wireless propagation latency on single hop. This is because, in a wormhole attack, many multi-hop routes are channelled to wormhole. The load on a single route increases leading to larger queuing delays in wormhole. However, this is not a sufficient condition for existence of a wormhole, as packet transmission is affected by congestion and intra-nodal processing. So delay, alone, can lead to false wormhole identification. Instead, this approach treats links experiencing long delays as suspicious links. Hence, wormhole verification should be undertaken only on such suspicious links.

The Hello_src packet which is an extension of existing Hello packet of AODV is introduced. This study assumes that clock time of nodes is synchronized as soon as a node is accepted in network. During neighbor discovery, synchronized time is attached to reserved bit in unix time format when Hello message is broadcast. All neighbor nodes in receiving range of receiving Hello message respond by appending Hello message with current received time in unix format and reply.

Once reply is received, approximate distance between two nodes is computed as follows.

$$t_i = \frac{2d}{l}$$

*where*

$t_i$ = time taken for $\text{Hello}_{src}$ to reach destination and back

$l$ = speed of light

d=distance between the two nodes

A worm hole is suspected when d is greater than maximum transmission capacity of sender node. An alternate route is discovered ignoring suspicious neighbourhood node. But, if an alternate route is not located, the proposed AODV routing protocol implements a secure-reply packet confirming the packet reaching destination.

A new packet secure-reply, Src_reply, is introduced. Message Digest (MD) also called hashing or digital fingerprint can be added to reply message to verify message integrity. The algorithm called HAVAL uses principles behind design of MD family. Also, HAVAL uses Boolean functions and these have properties which are as follows:

1. They are 0-1 balanced,
2. They are highly non-linear,
3. They cannot be transformed into another by applying linear transformation to input coordinates and
4. They are not mutually correlated via linear functions or via biased output.

The hash function HAVAL is a simple iteration of a compression function and is described as follows:

$$\mathrm{H}_0 = IV,\ \ \mathrm{H}_j = \text{compress}\left(\mathrm{H}_{j-1}, \mathrm{M}_j\right)\ \ (1 \le j \le t),\ \ \text{hash}\left(\mathrm{M}\right) = \mathrm{H}_t$$

Here M denotes message divided into t blocks $M_j$ of 1024 bits each. IV is an initial value of 256 bits, and $H_j$ represent

International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 5 (2016) pp 3282-3288
© Research India Publications. https://dx.doi.org/10.37622/IJAER/11.5.2016.3282-3288

chaining variables with 256 bits length. Each compression function application transforms chaining variable to a new value under control of current message block $M_j$, and final value for the chaining variable serves as a 256-bit hash value of message M. Two messages collide regarding a one-way hashing algorithm if they are compressed to same digest. For HAVAL hashing, there are two different possibilities for a message pair to collide like: numbers of passes which process messages are the same or they can differ [20].

Source decodes message and sends Src_reply packet with data packets for every prime number value sent by destination with current unix time. Destination replies to source with a secure ack-reply packet, hash value and receipt time of Src_reply packet. Assuming an maximum latency of 20% of sum of times taken for a node to reach its neighbor computed through Hello_src source can assume there is no wormhole attack if Secure ack-reply reaches it within 1.2 times of total Hello_src time computed from source to destination. This is additional security to mitigate wormhole attacks.

## V. Experimental Results

The experiments are conducted with 25 nodes distributed over two square kilometers. AODV routing protocol is used. Three experiments are conducted the first without malicious nodes and the second with 20% of the nodes being malicious. The third experiment is with proposed AODV (Hello_src and Src_reply AODV). Figure 5 to 7 shows the performance comparisons of three experiments. Table 1 to 3 shows the result value of above mentioned comparisons.

**Table 1:** Throughput in bits/sec

| Simulation time in second | Throughput in bits/sec | | |
|---|---|---|---|
| | AODV | AODV with worm hole attack | proposed AODV |
| 90 | 1822203 | 274132 | 1773914 |
| 180 | 1666133 | 400081 | 1591491 |
| 270 | 1683251 | 721772 | 1600771 |
| 360 | 1760596 | 774880 | 1701088 |
| 450 | 1442900 | 818632 | 1335115 |
| 540 | 1601023 | 600280 | 1486710 |
| 630 | 1626348 | 793182 | 1556903 |
| 720 | 1671467 | 782567 | 1622994 |
| 810 | 1754683 | 698013 | 1634136 |

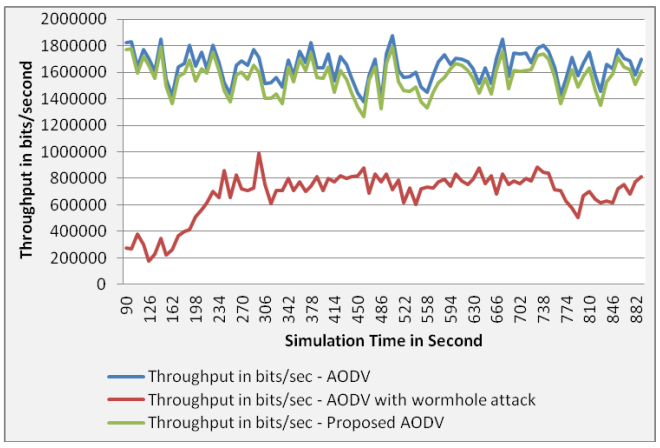


**Figure 5:** Throughput in bits/second

From the figure 5, it is observed that throughput is reduced by 58.63% in the presence of 20% of malicious nodes in MANET. The proposed AODV routing drastically improves the throughput in malicious environment achieving a throughput which is 5.05% less than the throughput achieved by AODV in a non-malicious environment.

**Table 2:** Cached Replies sent

| Simulation time in second | Cached replies sent | | |
|---|---|---|---|
| | AODV | AODV with worm hole attack | proposed AODV |
| 90 | 48 | 16 | 18 |
| 180 | 55 | 25 | 27 |
| 270 | 45 | 19 | 20 |
| 360 | 52 | 18 | 19 |
| 450 | 46 | 19 | 20 |
| 540 | 39 | 11 | 12 |
| 630 | 51 | 27 | 28 |
| 720 | 64 | 56 | 59 |
| 810 | 47 | 41 | 43 |

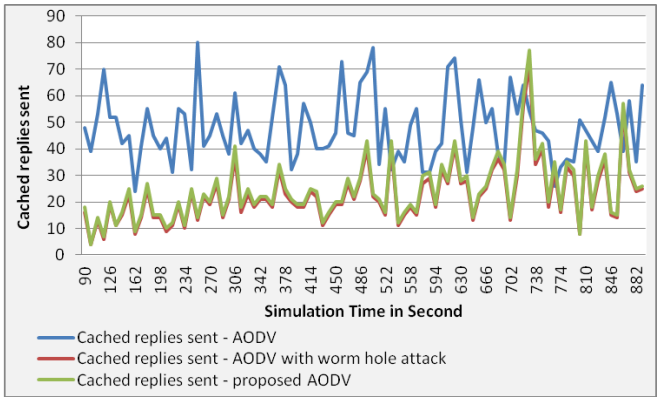


**Figure 6:** Number of cache replies

Figure 6 shows the number of cache replies sent in route discovery process. From the figure, it is observed that number of cache replies is three times more in the presence of 20% of malicious nodes.

**Table 3:** End to End Delay

| Simulation time in second | End to End Delay | | |
|---|---|---|---|
| | AODV | AODV with worm hole attack | proposed AODV |
| 90 | 0.007232 | 0.00806381 | 0.00785 |
| 180 | 0.005291 | 0.0094155 | 0.008994 |
| 270 | 0.006585 | 0.00915062 | 0.008702 |
| 360 | 0.007233 | 0.00877301 | 0.008476 |
| 450 | 0.008095 | 0.00809977 | 0.007495 |
| 540 | 0.008002 | 0.008214 | 0.007628 |
| 630 | 0.008245 | 0.00868752 | 0.008317 |
| 720 | 0.008243 | 0.00883724 | 0.008581 |
| 810 | 0.007987 | 0.01064928 | 0.009918 |

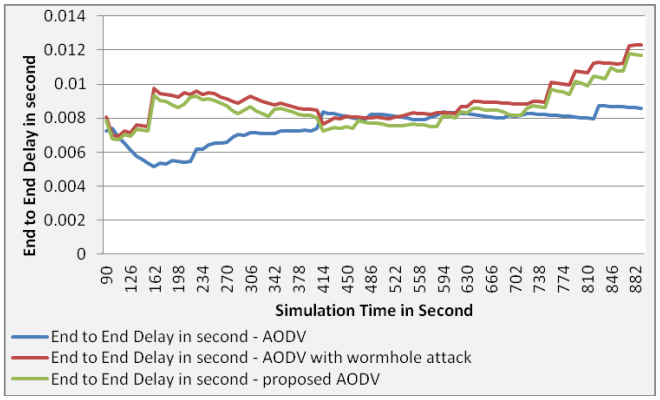


**Figure 7:** End to end delay

Figure 7 shows the comparison of end to end delay measured in seconds for normal and wormhole attacked MANET. It is seen that end to end delay is more variable in the presence of malicious nodes that create wormhole attack. The proposed AODV decreases the end to end delay by 5.1% in the malicious environment when compared to the AODV.

## Conclusion and Future Work

In this paper, performance variances in MANETs were evaluated in the presence of malicious nodes. An improved AODV with packets Hello_src and Src_reply to mitigate the wormhole attack was proposed. During neighbor discovery, synchronized time is attached to reserved bit in unix time format when Hello_src packet is broadcasted. All neighbor nodes in receiving range of receiving Hello message respond by appending Hello message with current received time in unix format and reply. A worm hole is suspected based on the delay and alternate route is discovered ignoring suspicious neighbourhood node. The proposed AODV routing protocol implements a secure-reply packet, Src_reply, confirming the packet reaching destination in case if alternate route is not available. Three experiments were conducted, first without malicious nodes, the second with 20% malicious nodes and the third is with the proposed AODV. Experiments show that throughput, end to end delay and cache sent performance decreases when it has 20 % of malicious nodes. The proposed AODV achieves improved throughput and decreased end to end delay in the malicious environment.

## References

[1] Murthy, C. S. R., & Manoj, B. S. (2008). Routing protocols for ad hoc wireless networks. Ad Hoc Wireless Networks: Architectures and Protocols, 299-364.

[2] Kaushik, S., & Kaushik, M. (2012). Analysis of MANET Security, Architecture and Assessment. International Journal of Electronics and Computer Science Engineering (IJECSE, ISSN: 2277-1956), 1(02), 787-793.

[3] Agrawal, S., Jain, S., & Sharma, S. (2011). A survey of routing attacks and security measures in mobile ad-hoc networks. arXiv preprint arXiv:1105.5623.

[4] Mamatha, G. S., & Sharma, D. S. (2010). Network Layer Attacks and Defense Mechanisms in MANETS-A Survey. International Journal of Computer Applications, 9(9).

[5] Jawandhiya, P. M., Ghonge, M. M., Ali, M. S., & Deshpande, J. S. (2010). A survey of mobile ad hoc network attacks. International Journal of Engineering Science and Technology, 2(9), 4063-4071.

[6] Jhaveri, R. H., Patel, A. D., Parmar, J. D., & Shah, B. I. (2010). MANET routing protocols and wormhole attack against AODV. International Journal of Computer Science and Network Security, 10(4), 12-18.

[7] Anita, E. M., Bai, V. T., Raj, E. K., & Prabhu, B. (2011, February). Defending against worm hole attacks in multicast routing protocols for mobile ad hoc networks. In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on (pp. 1-5). IEEE.

[8] Gupta, N. K., & Pandey, K. (2013, August). Trust based Ad-hoc on Demand Routing protocol for MANET. In Contemporary Computing (IC3), 2013 Sixth International Conference on (pp. 225-231). IEEE.

[9] Naït-Abdesselam, F. (2008). Detecting and avoiding wormhole attacks in wireless ad hoc networks. Communications Magazine, IEEE, 46(4), 127-133.

[10] Kumar, S., & Parthipan, V. (2011, April). SOPE: Self-organized protocol for evaluating trust in MANET using Eigen Trust Algorithm. In Electronics Computer Technology (ICECT), 2011 3rd International Conference on (Vol. 2, pp. 155-159). IEEE.

[11] Liang, X., Lu, R., Lin, X., & Shen, X. (2010, December). Message authentication with non-transferability for location privacy in mobile ad hoc networks. In Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE (pp. 1-5). IEEE.

[12] Das, G., Fazio, M., Villari, M., & Puliafito, A. (2006, April). Vulnerabilities of Internet Access Mechanisms from Mobile Ad Hoc Networks. In Advanced Information Networking and Applications, 2006. AINA 2006. 20th International Conference on (Vol. 1, pp. 851-858). IEEE.

[13] Gambhir, S., & Sharma, S. (2013, February). PPN: Prime product number based malicious node detection scheme for MANETs. In Advance Computing Conference (IACC), 2013 IEEE 3rd International (pp. 335-340). IEEE.

[14] Luo, W., Liu, J., Liu, J., & Fan, C. (2009, December). An Exact Model for Active P2P Worms Propagation. In Frontier of Computer Science and Technology, 2009. FCST'09. Fourth International Conference on (pp. 553-558). IEEE.

[15] Maheshwari, R., Gao, J., & Das, S. R. (2007, May). Detecting wormhole attacks in wireless networks using connectivity information. In INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE (pp. 107-115). IEEE.

[16] Katoh, T., Kuzuno, H., Kawahara, T., Watanabe, A., Nakai, Y., Bista, B. B., & Takata, T. (2006, November). AWide Area Log Analyzing System Based on Mobile Agents. In Computational Intelligence for Modelling, Control and Automation, 2006 and International Conference on Intelligent Agents, Web Technologies and Internet Commerce, International Conference on (pp. 26-26). IEEE.

[17] Singh, A., Tiwari, H., Vajpayee, A., & Prakash, S. (2010). A survey of energy efficient routing protocols for mobile ad-hoc networks. IJCSE) International Journal on Computer Science and Engineering, 2(09), 3111-3119.

[18] Lanjewar, A., & Gupta, N. (2013). Optimizing Cost, Delay, Packet Loss and Network Load in AODV Routing Protocol. arXiv preprint arXiv:1304.6486.

[19] Kim, Y. D., Moon, I. Y., & Cho, S. J. (2009). A comparison of improved AODV routing protocol based on IEEE 802.11 and IEEE 802.15. 4. Journal of Engineering Science and Technology, 4(2), 132-141.

[20] Zheng, Y., Pieprzyk, J., & Seberry, J. (1993, January). HAVAL—A one-way hashing algorithm with variable length of output. In Advances in Cryptology—AUSCRYPT'92 (pp. 81-104). Springer Berlin Heidelberg.