TRUST BASED AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL AGAINST WORMHOLE ATTACK

[1] N SATHEESH, [2] Dr. K. PRASADH

[1]Research Scholar, Department of CSE, Karpagam University, Coimbatore, India

[2] Mookambika Technical Campus, Muvattupuzha, Kerala, India

E-mail: [1]nsatheesh1983@gmail.com , [2]ksprasaadh@gmail.com

ABSTRACT

Mobile Ad hoc Networks (MANET) consists of mobile devices that communicate with each other without any predefined infrastructure/centralized administration. In network nodes can join or leave a network freely, MANETs are vulnerable to unauthorized data manipulation as it does not verify user identity before ensuring data access. Thus it is challenging to design security mechanisms that protect MANETs from routing attacks in the presence of malicious nodes. This study proposes a trust based Adhoc On-demand Distance Vector (AODV) protocol. Experiments were conducted in two scenarios and the results proved that the new method outperformed traditional AODV.

Keywords: *Mobile Adhoc Network (MANET), Adhoc On-demand Distance Vector (AODV), Routing, Trust, Wormhole attack*

1. INTRODUCTION

MANETs are wireless mobile node systems that dynamically self-organize in arbitrary/ temporary network topologies. A wireless mobile hosts group dynamically establishes a network on the fly, without any communication infrastructure. However, this network architecture and topology are liable to attack internally and externally [1]. Hence, the ultimate goal for MANET security is providing services like authentication, confidentiality, anonymity, integrity, and availability.

A weakness in security systems is vulnerability. A system can be vulnerable to unauthorized data manipulation as it does not verify user identity before ensuring data access. MANETs are more vulnerable than wired networks. Their vulnerabilities include the following [2]:-

- Lack of centralized management
- Resource availability
- Scalability
- Cooperativeness
- Dynamic topology
- Limited power supply
- Bandwidth constraint
- Adversary inside the Network
- No predefined Boundary

Malicious node(s) attack MANETs using different ways like sending fake messages many times, fake routing information and advertising fake links to interrupt routing operations [3]. Attacks are categorized based on attack behavior i.e. Passive or Active attacks. A passive attack does not alter transmitted data within a network, but it includes unauthorized “listening” to network traffic or accumulating data from it. Passive attackers do not disrupt routing protocol operations but try to discover information from routed traffic.

Active attacks are very severe and prevent message flow between nodes. Such attacks are either internal or external. Active external attacks are by outside sources not belonging to the network. Internal attacks are from malicious nodes that form part of the network and are more severe and tougher to detect than external attacks [4]. Such attacks generate unauthorized network access which helps attackers to make changes like packet modification, DoS and congestion.

A wormhole attack is a severe attack where two attackers are placed strategically in a network. The attackers listen to network and record wireless data. The attacker creates a tunnel to record ongoing communication and traffic at one network position, channeling them to another network position. The attack creates a direct link between each other in a network and receives packets at one end and transmits it to the other end of the network. When attackers are in this position, it is known as out of band wormhole [5].

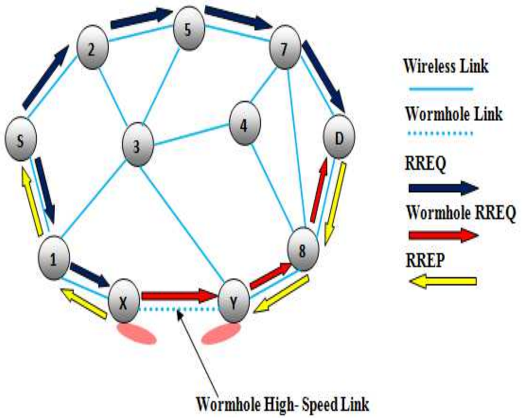

Figure 1: Wormhole attack

This attack compromises network security. For example, when a wormhole attack comes against AODV routing protocol, then all packets are transmitted through this tunnel and no route is discovered. If the tunnel is created honestly, it does not harm the network and provides efficient network connections [6]. A potential solution to avoid wormhole attack is integrating prevention methods into intrusion detection systems. But isolating the attackers is hard with a software-based approach as packets forwarded by a wormhole are similar to packet sent by legitimate nodes.

AODV is a reactive routing protocol that creates a destination path when needed. Routes are not built till certain nodes send route discovery messages as an intention to communicate/ transmit data to each other. Routing information is stored in source nodes, destination nodes and intermediate nodes on active routes handling data transmission [7]. An attacker tunnels a request packet directly to the destination node without increasing hop-count value preventing other routes from being discovered.

It disrupts communication badly as AODV is unable to locate routes longer than one or two hops. It is easy for attacker to ensure that the tunneled packet arrives with better metric than normal multi-hop route for tunneled distances lengthier than single hop transmission range. Malicious nodes retransmit eavesdropped messages again in an exclusive channel available to the attacker [8]. A wormhole attack can merge with message dropping attack to prevent destination nodes from receiving packets.

This study proposes an improved AODV. This study is organized as follows: Section 2 reviews related works in literature. Section 3 explains methods and materials used in the study. Section 4 discusses results and Section 5 concludes the paper.

2. RELATED WORK

A risk-aware response mechanism to cope with identified routing attacks was suggested by Zhao et al., [9] based on Dempster-Shafer mathematical theory of evidence. Additionally, experiments proved the effectiveness of the new approach through consideration of many performance metrics.

Severe attacks against MANETs like blackhole attack, sinkhole attack, RREQ flood, selfish node behavior, hello flood and selective forwarding attack were investigated in detail by Ehsan and Khan [10]. A detailed NS-2 implementation to launch such attacks successfully using AODV routing protocol was presented and a comprehensive/comparative analysis of attacks was undertaken. Packet efficiency, routing overhead and throughput were performance metrics. Simulation showed that attacks like RREQ flood and hello flood drastically increased protocol routing overhead. Route modification attacks like sinkhole and blackhole are deadly, severely affecting packet efficiency and reducing throughput to unacceptable levels.

Improving secure Enhanced-On Demand Multicast Routing Protocol (EODMRP) to safeguard against flooding and blackhole attacks was presented by Sreenath et al., [11]. Solutions were implemented and tested using GloMoSim (2.03). Performance analysis revealed improvement in packet delivery ratio in blackhole attack with a marginal increase in average end-to-end delay and normal routing overhead. The new mechanism for flooding attack worked even when malicious nodes identity was unknown. It also did not use any additional network bandwidth. It is simple and maintained/improved network throughput when there were no malicious nodes, but network faced excess traffic congestion.

Yu et al., [12] proposed a routing algorithm with routing metric linking both requirements on a node's performance and trustworthiness. Both of the proposed algorithms could be integrated into routing protocols for MANETs, such as AODV and DSR. As an example such an integrated protocol called Secure Routing Against Collusion (SRAC) was presented where a node makes a routing decision, on its trust and performance of its neighboring nodes. The simulation results have validated the advantages of the proposed attack detection over some known protocols.

Lu et al., [13] implemented Bad Adhoc On-demand Distance Vector (BAODV) for AODV suffering black hole attack which simulated black hole attack in MANET by one node acting as malicious in the network. Based on BAODV, a secure and efficient MANET routing protocol SAODV protocol, was suggested which addresses AODV security weaknesses and could withstand black hole attacks. Experimental analysis revealed that SAODV routing protocol was more secure than basic AODV.

Two routing protocols in large-scale network - DOA and AODV routing protocols – were analyzed by Jasmine Jeni et al., [14] who injected them with black hole attacks and evaluated quality parameters like packet delivery ratio and an average end to end delay. Network simulation was by NS2 and protocols performances were compared for efficiency.

An approach to combat black hole attack using negotiation with neighbors who claim to have a destination route was proposed by Medadian et al., [15]. Simulation showed that the new protocol provided improved security and performance regarding packet delivery than traditional AODV during black holes with reduced additional delay and overhead.

Effects of Wormhole attack on MANETs were studied by Sadeghi and Yahya [16] using a proactive routing protocol (OLSR) and a reactive routing protocol (AODV). OPNET simulation showed network load, throughput and traffic received and end-to-end delay with Wormhole and without Wormhole on OLSR and AODV in MANET. Results showed AODV being more vulnerable to the wormhole attack compared to OLSR. So, MANET application that used proactive routing protocol is more trusted compared to that which is reactive.

Two malicious attacks i.e. gray, black hole and two types of selfish behaviors i.e. type-1, type-2 were considered by Alkatheiri and Liu [17]. These attacks were simulated with AODV. Simulation showed enormous decrease in packet delivery ratio and extensive packet dropping by malicious/misbehaving nodes. The study could be a valuable asset for researchers working to ensure secure routing protocols to mitigate malicious or misbehaving attacks.

A reputation based scheme to resist flooding attack impact in MANETs proposed by Choudhury et al., [18] observed the behavior of a network node periodically, limiting its route request sending rate.

A method to detect and isolate wormhole attacks in MANETs was proposed by Shin and Halim [19]. Routes redundancy starts where source sends RREQ using all ways to a destination. Routes connecting sources and destinations are listed with the number of hops from each route. Suspicious network nodes were isolated and not considered for transmission. Simulation showed its ability to prevent increasing packets dropping, based on wormhole isolation in the new scheme compared to normal AODV protocol and using earlier time-based calculation.

A new approach that modified existing AODV routing protocol proposed by Chavda and Nimavat [20] found a safe route between sending and receiving nodes. Simulations showed that the new approach was more efficient than normal AODV, having high packet delivery ratio and throughput.

A mechanism to ensure Secure Route Discovery for AODV protocol (SRD-AODV) to prevent black hole attacks proposed by Tan and Kim [21] required source and destination nodes to verify sequence numbers in Route Request and Route Reply messages, based on defined thresholds prior to establishing the connection with a destination node to send data. Simulation NS2 showed improved packet delivery ratio for three different environments compared to standard AODV protocol.

AODV routing protocol performance degradation was discussed by Sangi et al., [22] mainly when byzantine attacks are initiated in combination.

A solution to detect and avoid black hole attacks (single and cooperative) was suggested by Biswas et al., [23] which ensured secure packet transmission with efficient resource utilization of mobile hosts simultaneously. According to a new solution, trust evaluation in every network node was based on parameters like node stability defined by its mobility and pause time and remaining battery power. Node trust is the basis for selection of most reliable transmission route. Simulation showed that the new solution ensured good performance regarding throughput, secure routing and efficient resource use.

3. METHODOLOGY

3.1 Ad hoc On-demand Distance Vector (AODV)

AODV routing protocol is reactive; so routes are determined only when needed. Hello messages detect and monitor links to neighbors. When Hello messages are used, every active node broadcasts a Hello message periodically that all neighbors receive [24]. As nodes periodically send Hello messages, a link break is perceived when a node fails to receive many Hello messages. As data flows from the source to destination, nodes on a route update timers associated with routes to source and destination, maintaining routes in the routing table. When a route is not used for some time, a node is unsure if a route is still valid; consequently, it removes the route from its routing table.

Route discovery is initiated when a source needs a destination route and does not have it in its routing table. To initiate route discovery, a source floods a network with a RREQ packet specifying destination where the route is requested. On receipt of a RREQ packet, a node checks to see whether it is a destination or route to a destination. If either is true, the node generates an RREP packet and sends it back to the source along reverse path. Every node on the reverse path sets up a forward pointer to node it received RREP from. This ensures a forward path from source to destination. If a node is not a destination and does not have a destination route, it rebroadcasts RREQ packet [25]. Duplicate RREQ packets are thrown out at intermediate nodes. When source node receives first RREP, it begins sending data to a destination.

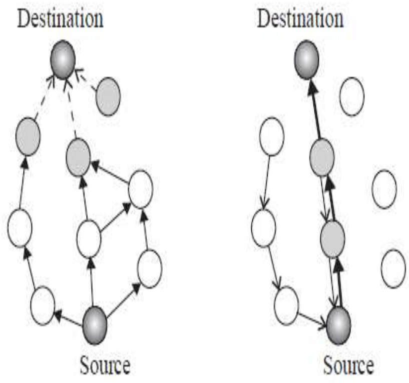

Figure 2: RREQ Broadcast RREP Propagation and Subsequent Route

To transmit data packets, route request RREQ (Route REQuest message) is broadcast to the entire network. Three cases are possible on receipt of a RREQ message by a node. In the first, if node that received the message provides a route to requested destination in its routing table, it responds with a RREP (Route REPly message). In the second case, if it has no destination information, it retransmits the message to neighbors that had not received it. If all neighbors have received same message and/or node has lost connection, it sends an error message RERR (Rout ERRor message). On receipt of a reply message, a source node sends data packets on the shortest path [26].

3.1.1 Proposed Message Packets for AODV

In wormhole attacks, a hostile node monitors channel, records packets overheard and tunnels them to a remotely located colluding node, which replays them on its floor. When tunnelling targets routing control packets like HELLO messages and RREQ, nodes close to attackers cannot distinguish between legitimate routes originating and ending in the vicinity of the two attackers respectively: In typical wormhole attacks legitimate routes span more than the one/two hops declared by wormhole attackers disrupting network operations.

An efficient method to detect and prevent AODV wormhole attacks is proposed in this research by introducing Hello_src and Src_reply. Hello_src packet is an extension of AODV Hello packets. The study assumes that nodes clock time is synchronized when a node is accepted in a network. Synchronized time is attached to the reserved bit in unix time format during neighbor discovery when a Hello message is broadcast. Neighbor nodes in a Hello message receiving range respond by appending Hello message with current received time in unix format and reply.

When a reply is received, an approximate distance between two nodes is computed:

$$t_i = \frac{2d}{l} \qquad (1)$$

where
t_i = time taken for $\text{Hello}_{\text{src}}$ to reach destination and back
l = speed of light
d = distance between the nodes

A wormhole is suspected when d is greater than sender node's maximum transmission capacity. Ignoring suspicious neighborhood node, an alternate route is discovered. But, if this is not possible, the proposed AODV routing protocol implements a secure-reply packet confirming packet reaching destination.

Src_reply, a new packet secure-reply is introduced. Message Digest (MD) also called hashing or digital fingerprint is added to reply message to verify message integrity. The HAVAL algorithm uses principles behind MD family design. HAVAL also uses Boolean functions and their properties are:

1. They are 0-1 balanced,

2. They are highly non-linear,

3. They cannot be transformed into another through application of a linear transformation to input coordinates and

4. They are not mutually correlated through linear functions or through biased output.

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

Here M denotes a message divided into blocks Mj of 1024 bits each. IV is an initial value of 256 bits, and Hj represent chaining variables with 256 bits length. Every compression function application transforms chaining variable to a new value under current message block Mj, control and final value for chaining variable serves as a 256-bit hash value of message M. Two messages collide regarding a one-way hashing algorithm when they are compressed to a same digest. For HAVAL hashing, there are two different possibilities for a message pair to collide: numbers of passes that process messages are the same or they differ [27].

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

3.1.2 Trust Evaluation

Trust defined in the model is a node's confidence on another node. Trust value means level of a node's trustworthiness, which is computed based on various trust evaluation factors. Sensor nodes in this scheme, do not compute all other nodes' trust values in the network, but compute only neighbor nodes' trust values accumulatively.

Trust Evaluation Factor**.** Each sensor node has *k* trust evaluation matrices that stores trust evaluation factors for *k* neighbor nodes. Trust evaluation matrix has many trust evaluation factors as follows:

Link quality: Link quality is a promising parameter, as it defines an ability of a link and devices to support traffic density for the connection period. Link state between two neighbors is affected by parameters like distance, battery power and mobility.

Distance: This contains distance information between two nodes. *xi* means x coordinate and *yi* means y coordinate of node *i*.

$$D_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (2)$$

where $0 \leq i,j \leq k$ and $i \neq j$

Sensing communication: This includes communication ratio information and represents a node's level of selfishness and normality.

- Si: sensing communication value of node i, where 1 ≤ i ≤ k
- ssi: sensing success count of node i
- sfi: sensing failure count of node i

Sensing result: This represents sensing result information for detected events and has sensing data and sensing time for events.

- Ri=<sri, sti>: sensing result value of node i, where 1 ≤ i ≤ k
- sri: sensing data of node i
- sti: sensing time of node i

Mobility: Mobility is an important MANET routing protocols evaluation parameter. A more rigorous mobility definition expresses network topological change given by the formula:

$$mob = \sum_{i=1}^{n} \frac{M_i}{n}$$

$$M_x = \sum_{t=0}^{T-\Delta t} \frac{\left|A_x(t) - A_x(t+\Delta t)\right|}{T}$$

$$A_x(t) = \sum_{i=1}^{n} \frac{dist(n_x, n_y)}{n-1}$$

(3, 4, 5)

Where,

$dist(n_x, n_i)$: distance between nodes x and y.

N: nodes number

$A_x(t)$: average distance between node x and all other nodes, at time t.

M_x: average relative mobility of node x regarding other nodes during simulation time.

T: Simulation time.

At: Time period used in computation.

Trust value: This factor represents a node's total trustworthiness evaluated on other trust evaluation factors.
Ti: trust value of node i, where 1 ≤ i ≤ k

4. EXPERIMENTAL RESULTS

The proposed methods were evaluated using 100 nodes in the area of 9 sq km. Transmission range of node is 250 m. The node pause was varied from 10 sec to 60sec. AODV Header modification is used to accommodate trust values. The experiments were conducted for two scenarios:

- 5 % of malicious nodes in the network
- 10 % of malicious nodes in the network

The results for the experiments with 5% of malicious nodes are as follows:

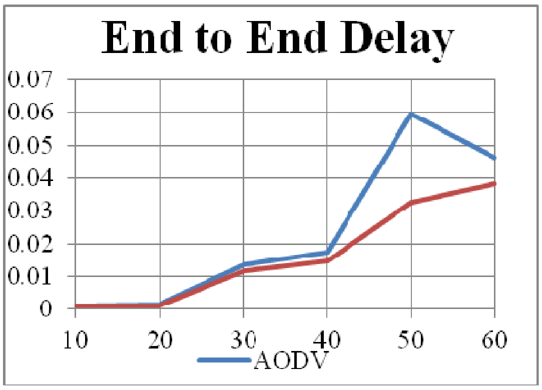

Figure 3: End to end delay in presence of 5% of malicious nodes

The proposed trust based AODV reduced end to end delay by 58.53% when compared with AODV for node pause time of 50 seconds. The proposed trust based AODV reduced end to end delay by 13.38% when compared with AODV for node pause time of 30 seconds. On average the proposed trust based AODV reduced of End to End delay by 33% when compared with AODV with 5% of malicious nodes in the network.

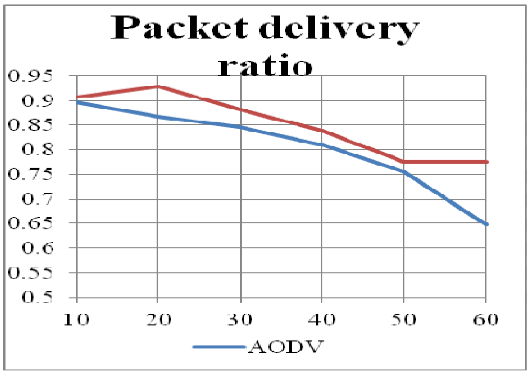

Figure 4: Packet delivery ratio in presence of 5% of malicious nodes

The proposed trust based AODV increased packet delivery ratio by 17.81% when compared with AODV in node pause time of 60 seconds. The proposed trust based AODV increased packet delivery ratio by 1.34% as least value when compared with AODV in node pause time of 10 seconds. Averagely trust based AODV increased by 5.70% of packet delivery ratio when compared with AODV with 5% of malicious nodes in network.

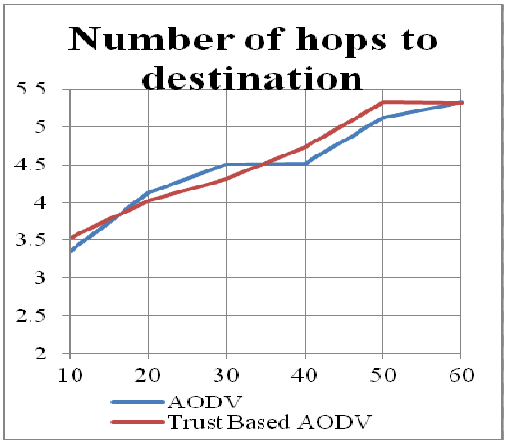

Figure 5: Number of hops to destination in presence of 5% of malicious nodes

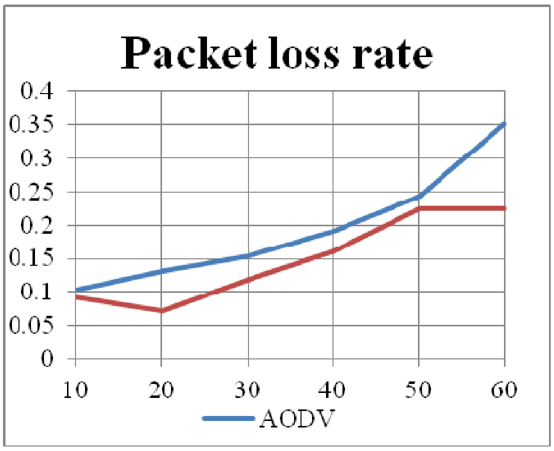

Figure 6: Number of hops to destination in presence of 5% of malicious nodes

The proposed trust based AODV reduced packet loss rate by 44.12% when compared with AODV for node pause time of 60 seconds. The proposed trust based AODV reduced packet loss rate by 8.07% when compared with AODV for node pause time of 50 seconds. The proposed trust based AODV on an average reduced packet loss rate by 27.4259% of when compared with AODV for 5% of malicious nodes in network.

The results for the experiments with 10% of malicious nodes are given below:

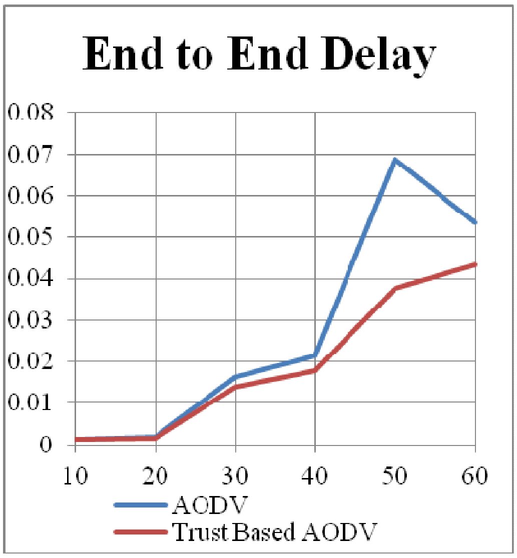

Figure 7: End to End delay in presence of 10% of malicious nodes

The proposed trust based AODV reduced End to End delay by 58.65% compared with AODV for node pause time of 50 seconds. The proposed trust based AODV reduced End to End delay by 11.38% when compared with AODV in node pause time of 10 seconds. The trust based AODV reduced End to End delay by 34.48% when compared with AODV for 10% of malicious nodes in the network.

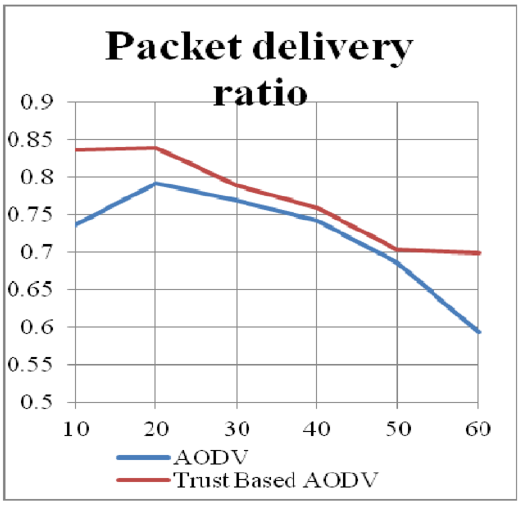

Figure 8: End to End delay in presence of 10% of malicious nodes

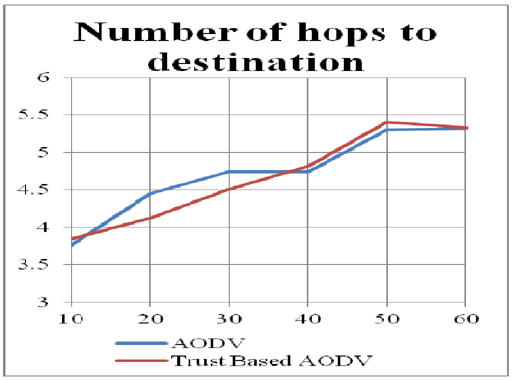

Figure 9: Number of hops to destination in presence of 10% of malicious nodes

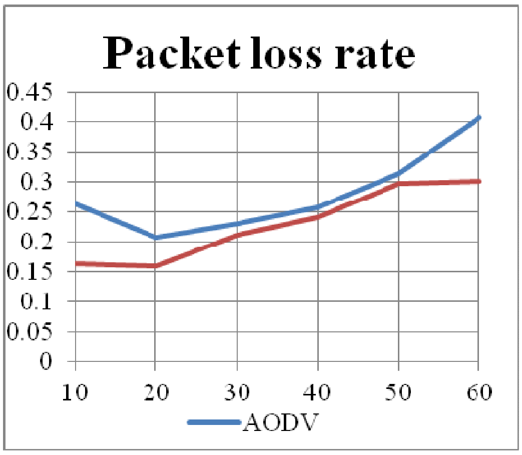

Figure 10: Packet loss rate in presence of 10% of malicious nodes

The proposed trust based AODV reduced packet loss rate by 47.06% when compared with AODV for node pause time of 10 seconds. The proposed trust based AODV reduced packet loss rate by 5.64% as least value when compared with AODV for node pause time of 50 seconds. The proposed trust based AODV on an average reduced packet loss rate by 19.97% when compared with AODV for 10% of malicious nodes in the network.

5. CONCLUSION

Wormhole is an attack on MANET routing protocols where colluding nodes create an illusion that two remote MANET regions are directly connected through nodes that appear to be neighbors but are actually far from each other. A trust based AODV is proposed and trust evaluation calculated. Experiments revealed that trust based AODV improved packet delivery ratio and reduced end to end delay and packet loss rate greatly in malicious nodes presence. The new method outperformed AODV protocol. Trust based AODV increased packet delivery ratio by 6.83% when compared to AODV when 10% of malicious nodes was present in the network.

REFERENCES:

[1]. Weng, J. Security Issues in Mobile Ad Hoc Networks-A Survey.

[2]. Goyal, P., Parmar, V., & Rishi, R. (2011). manet: Vulnerabilities, challenges, attacks, application. JCEM International Journal of Computational Engineering & Management, 11(2011), 32-37.

[3]. Ngadi, M., Khokhar, R. H., & Mandala, S. (2008). A review current routing attacks in mobile ad-hoc networks. International Journal of Computer Science and Security, 2(3), 18-29.

[4]. Aarti, D. S. (2013). Tyagi,"Study Of Manet: Characteristics, Challenges, Application And Security Attacks". International Journal of Advanced Research in Computer Science and Software Engineering, 3(5), 252-257.

[5]. Ullah, I., & Rehman, S. U. (2010). Analysis of Black Hole attack on MANETs Using different MANET routing protocols. School of Computing Blekinge Institute of Technology, Sweden.

[6]. Achint Gupta, D., Vj, P., & Upadhyay, S. (2012). Analysis of Wormhole Attack in AODV MANET Using OPNET Simulator. International Journal, 1(2).

[7]. Bhosle, A. A., Thosar, T. P., & Mehatre, S. (2012). Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET. International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol, 2.

[8]. Zhao, Z., Hu, H., Ahn, G. J., & Wu, R. (2012). Risk-aware mitigation for manet routing attacks. Dependable and Secure Computing, IEEE Transactions on, 9(2), 250-260.

[9]. Ehsan, H., & Khan, F. A. (2012, June). Malicious AODV: implementation and analysis of routing attacks in MANETs. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (pp. 1181-1187). IEEE.

[10]. Sreenath, N., Amuthan, A., & Selvigirija, P. (2012, January). Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETS. In IEEE International Conference on Computer Communication and Informatics (ICCCI 2012), Coimbatore, India.

[11]. Yu, M., Zhou, M., & Su, W. (2009). A secure routing protocol against byzantine attacks for MANETs in adversarial environments. Vehicular Technology, IEEE Transactions on, 58(1), 449-460.

[12]. Lu, S., Li, L., Lam, K. Y., & Jia, L. (2009, December). SAODV: a MANET routing protocol that can withstand black hole attack. In Computational Intelligence and Security, 2009. CIS'09. International Conference on (Vol. 2, pp. 421-425). IEEE.

[13]. Jasmine Jeni, P. R., Vimala Juliet, A., Parthasarathy, R., & Messiah Bose, A. (2013,

March). Performance analysis of DOA and AODV routing protocols with black hole attack in MANET. In Smart Structures and Systems (ICSSS), 2013 IEEE International Conference on (pp. 178-182). IEEE.

[14].Medadian, M., Yektaie, M.H., Rahmani, A-M., (2009). "Combat with Black hole attack in ODV routing protocol in MANET," First Asian Himalayas International Conference, (pp 1-5).

[15]. 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.

[16]. Alkatheiri, S., & Liu, J. (2011). AODV outing protocol under several routing attacks in MANETs. In 2011 IEEE 13th International Conference on Communication Technology (pp. 614-618).

[17]. Choudhury, P., Nandi, S., Pal, A., & Debnath, N. C. (2012, July). Mitigating route request flooding attack in MANET using node reputation. In Industrial Informatics (INDIN), 2012 10th IEEE International Conference on (pp. 1010-1015). IEEE.

[18]. Shin, S. Y., & Halim, E. H. (2012, October). Wormhole attacks detection in MANETs using outes redundancy and time-based hop calculation. ICT Convergence (ICTC), 2012 International Conference on (pp. 781-786). IEEE.

[19]. Chavda, K.S.; Nimavat, AV., (2013). "Removal of black hole attack in AODV routing protocol of MANET," Computing, Communications and Networking Technologies (ICCCNT), 2013 ourth International Conference on, (pp.1-5)

[20]. Tan, S., & Kim, K. (2013). "Secure Route Discovery for Preventing Black Hole Attacks on AODV-ased MANETs," High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference (pp.1159-1164)

[21]. Sangi, A. R., Liu, J., & Zou, L. (2009, December). A performance analysis of aodv routing protocol under combined byzantine attacks in manets. InComputational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on (pp. 1-5). IEEE.

[22]. Biswas, S., Nag, T., & Neogy, S. (2014, February). Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET. In Applications and Innovations in Mobile Computing (AIMoC), 2014(pp. 157-164). IEEE.

[23]. Chakeres, I. D., & Belding-Royer, E. M. (2004, March). AODV routing protocol implementation design. In Distributed Computing Systems Workshops, 4. Proceedings. 24th International Conference on (pp. 698-703). IEEE.

[24]. Mueller, S., Tsang, R. P., & Ghosal, D. (2004). Multipath routing in mobile ad hoc networks: Issues and challenges. In Performance tools and applications to networked systems (pp. 209-234). Springer Berlin Heidelberg.

[25]. 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.

[26]. Hur, J., Lee, Y., Hong, S. M., & Yoon, H. (2006). Trust management for resilient wireless sensor networks. In Information Security and Cryptology-ICISC 2005(pp. 56-68). Springer Berlin Heidelberg.

[27]. Kadri, B., Moussaoui, D., & Feham, M. (2011). Link quality based ant routing algorithm for MANETs (LQARA). In Proceeding of the 12 th Post Graduate Network Symposium (pp. 218-223).

[28]. Djenouri, D., Derhab, A., & Badache, N. (2006). Ad Hoc Networks Routing Protocols and Mobility. Int. Arab J. Inf. Technol., 3(2), 126-133.