Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 8
August 2023

An Advanced Trust-Based Routing Protocol for Mobile Ad-Hoc Network under Worm-Hole Attack Using Mobility Model

Versha Matre and Dr. Pradnya Ashish Vikhar
Department of Computer Science & Engineering
Dr. A.P.J. Abdul Kalam University, Indore (M.P.) - 452010, India

Abstract:-Mobile ad hoc Network (MANET) is one of the comprehended technologies in network and communication. MANET offers revelatory features that support to enhance operations. In this work for MANET's secure routing and enhanced routing protocol is presented. The offered routing method is a trust-based routing protocol that evaluates the characteristics of middle nodes in the network. During the estimation of nodes, a weighted trust valuation for all medium routers is computed to produce a secure route establishment. To calculate weighted trust the network parameters of nodes are employed i.e. packet drop proportion, RRT and energy consumption rate. Furthermore, a trust threshold is employed for categorizing the malicious and legal nodes in a network route. Thus trust threshold is applied to produce opinions for the selecting of a secure and effective path. Ultimately, a relative study between conventional AODV and offered trust- based AODV is achieved. The developmental effects establish the offered routing is effective and secure as analogized to conventional AODV routing protocol.

Keywords: -Mobile Adhoc Network (MANET), Security, Trust Computation, Routing Protocol improvements, Implementation.

1. Introduction

Mobile ad hoc network (MANET) is one of the popularized networks and communication technology. The MANET is a set of wireless nodes that are allowed to transfer with each different by employing Wi- Fi. The nodes are restricted to transmit in a special range, therefore the middle nodes are employed to produce a route and transfer communications (1). The MANET self-organizing network therefore nodes are independent from the network. Therefore, any moment a substitutive node can adjoin or leave the network. Also, the network isn't affecting any centralized authority or controller therefore the routing and different opinions are produced by the nodes itself (2).

The properties of MANET allow other usages to hold advantage of other manufactured and military assignments (3). In this work, an army employment is offered to secure network communication. Where we accepted, the network contains two malicious nodes that are interconnected with a high- speed LAN. Also both the attackers are testing to prorogate the message of the network. Corresponding variety of status is understood as a wormhole attack.

The wormhole attack is substantially set exploiting two or further inside attackers. These attackers are tunneling the data from one situation of the network to another (4). Due to this traffic in the network is crystallized. As traffic is created utmost of the network data is broke down to deliver(5). Thus the wormhole is a serious attack form in the network. In this work, a particular research of the wormhole attack is offered and a trust- based result is proposed. This part provides an overview of the suggested composition and the following section provides the particulars of the wormhole attack.

2. Wormhole Attack In Manet

This part provides particulars about the wormhole attack and the working of AODV routing. These particulars support to judge the offered result.

A. Wormhole attack

The wormhole attack is one of the routing grounded attacks in MANET. During this when a malicious node receives the transmitted packets at one location it tunnels it to another position in the network (6). In distribution to serve this activity in network two or further attackers produce a high-speediness channel. This malicious channel is known as a wormhole link. This wormhole link is a wired link between two attackers (7). An

illustration of a wormhole attack is presented in figure 1. In this illustration, a MANET is established with two nodes source(S) and destination(D). There are some middle nodes similarly accessible which are tagged as A, B, andC. Except these middle nodes two another nodes are similarly extant in this figure X and Y(8).

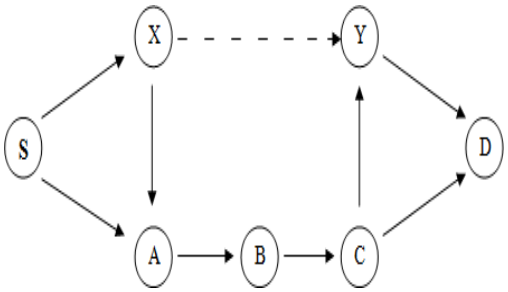

Figure 1: wormhole attack

X and Y are accepted as the malicious nodes, which are interconnected to each different exploiting a dotted line. This dotted link between both is a high- speediness bus that carries packets from source X to the Y position applying the tunnel. Due to these cautions, utmost of the traffic is transferring on through created wormhole links (9). When a suggestive quantity of traffic is tested to transferring through the malicious link the form of traffic is created and utmost of the packets are dropped (10).

B. AODV routing

AODV routing protocol is similarly comprehended as ad- hoc on- demand vector routing. The AODV contains three aspects of route detection and operation. The initial phase is understood as route detection, the root node broadcasts an RREQ (route request) message, and the neighbor nodes who admit the RREQ message correspond the IP address of destination (11). If IP address corresponded with receiving node also node keeps the RREQ message elsere-broadcast the message to their neighbors. As the RREQ packet admitted by the destination, the destination node circulate the RREP (route reply) message for root node (12). The identical procedure is applied to deliver the RREP message to the root node. As the root node admitted the RREP message the route is demonstrated. Source node usages the identical route to transmit with the destination node. The phase is comprehended as route maintenance, if any routing node leaves their position also path becomes abundant. Therefore the intermediate node tested to retrieve the path exploiting required nodes. If the path isn't retrieved also the third aspect is reprocessed andre-route detection is initiated(13). This part provides an overview of the two key conceptions of the MANET. The following section includes the proposed work in detail.

3. Proposed Work

This part provides an understanding of the proposed work and the result for enhancing the security of the AODV routing protocol.

A. System overview

MANET is expensive in other real- world operations. The mobility of nodes makes it additionally expensive. Therefore, the network can exist applied for other military and disaster management assignments. Thus, where immediate deployment and its riddance needed the MANET infrastructure is applied. In other operations, i.e. confidential assignments, disaster, and consolation operation these networks are important productive. In this composition, a script is assumed where a cluster of unprepared workforces is located. Then each cluster element of the team is viewed as a node. Every node transmitting with each disparate but there are two hidden attackers extant who are interconnected with a wired LAN to interrupt the message (14).

Corresponding to the characteristics of the hidden attacker nodes, it's a form of a wormhole attack. Thusan implicit result is needed that can distinguish the attacker nodes and get around or bypass these malicious nodes. Thus the suggested composition is allowed to propose a trust- based routing protocol. That protocolpre-examines the network nodes and simply communicates with the assigned nodes. This part provides an overview of the suggested composition. The following section provides the suggested routing protocol's working.

B. Methodology

The advanced methodology of self-assured routing is turning upon the variation of the AODV routing protocol. In this environment, the extension of AODV is offered by the objectification of trust representative's computation. The extension of the protocol involves the estimation of each node which is affected in operational message. Thus, network characteristics are applied for associating

the node trust valuations.

Parameters:

The succeeding parameters are scaled for trust calculation

1. Round trip time: - due to traffic formed by the wormhole attackers, the packet delivery speediness is affected. Therefore we compute the round trip time (RTT) for the nodes. To compute RRT the succeeding formula is applied

$$RTT = \frac{T_R - T_S}{2H_c}$$

Where, TR is the time of receiving the packet, Ts is the time of transferring packet, and Hc is the hop count.

2. Packet drop rate: - Due to the wormhole attack network suffers from traffic. Therefore the malicious node has a suggestive quantity of packet drop. Therefore packet drop rate is involved as the trust representative. To compute the packet drop rate of a node the succeeding formula is applied

$$PDR = \frac{total\ drop\ packets}{total\ packets\ sent}$$

3. Rate of energy consumption: - The transmitting and admitting of data and control packets take a situated quantity of energy. Therefore if any node in network consumes additional energy as analogized to different nodes, therefore it means it behaves abnormally. Thus, it's a necessary representative for trust computation. To calculate the energy consumption quality of the node, we accepted a node has a situated energy position $E1$ at sampling time $T1$, and during the following sampling time $T2$ the energy status becomes $E2$. therefore the quality of energy consumption can subsist calculated employing the succeeding formula

$$\delta = \frac{E_1 - E_2}{T_2 - T_1}$$

$$\delta = \frac{\Delta E}{\Delta T}$$

4. Trust Computation: - To take trust during the message we establish with a standard functioning network. That network contains a faction of nodes without any malicious node. We choose three pairs of nodes irregularly. Each pair contains a root node and a destination node. Now each root node initiates message and employing this message described three representatives are computed. Allow the pair($S1$, $D1$) calculate $RTT1$, $PDR1$ and $\delta 1$. Also, all pairs of node computing the contributed three parameters. After that, a threshold valuation is calculated as.

$$RRT_{threshold} = \frac{RRT_1 + RRT_2 + RRT_3}{3}$$

$$PDR_{threshold} = \frac{PDR_1 + PDR_2 + PDR_3}{3}$$

And

$$O_{threshold} = \frac{\delta_1 + \delta_2 + \delta_3}{3}$$

Presently we've three other thresholds for finding the malicious node. And to produce regulation-grounded category the computational rate increases. To conserve the computational resources we associate all parameters into a trust valuation. To calculate combined trust valuation we apply this formula

$$Trust = RRT_{threshold} * w1 + PDR_{Threshold} * w2 + \delta_{threshold} * w3$$

The trust valuation is applied to evaluate each node in the network. If a node's trust valuation high than or equal to threshold trust valuation also protocol get around node. Employing this ground rule the network becomes self-assured and provides the maintenance in the interpretation of the network.

A.**Proposed algorithm**

Table1: Proposed Algorithm

This part introduces the operation of offered trust-based routing. Table 1 contains the necessitated steps.

Input:NetworknodesN

Process:

1. Source node initiateroutediscovery
2. Waitfor replymessagefromalldestination
3. Foreach path inroutingtable
   a. ComputenodeRTT
   b. ComputenodePDR
   c. ComputeNodeδ
   d. CalculateNodetrust
   If$Node_{trust} < trust_{threshold}$
      i. Nodeislegitimate
      ii. Gotonextnode
   Else
   f. i. Nodeismalicious
      ii. ii.Gotonext path
   g. Endif
4. Endfor

Corresponding to the presented procedure, we've a network with N number of nodes. The root initiates the route detection procedure by message of RREQ and RREP communications. The protocol waits for all the practicable responses from the destination. Thus, we've multiple path explains how trust valuations are employed to estimate the routes. If any untrusted node establish in the route also the algorithm avoids that node and tries to explore another way options between root and destination. By employing the routing table entryway each route is estimated against the computed trust valuations. Also among the entire attainable options most assured path is chose as the direct routing way. The below- presented algorithm

4. SIMULATION

The succeeding architecture of the network is implied to simulate the advanced routing protocol. Table 2 contains the parameters and applicable valuations.

Table 2: simulation setup

S.No.	Simulationproperties	Values
1	Antennamodel	OmniAntenna
2	Radio-PropagationModel	TwoRayGround
3	ChannelType	Wireless Channel
4	RoutingProtocol	AODV
5	NoofMobileNodes	20, 40, 60, 80, 100
6	Simulationarea	1000X1000

5. Results Analysis

This part provides an analysis of network interpretation for both types of developmental scripts. During experimentations, other interpretation parameters are scaled and described.

A. End to end delay

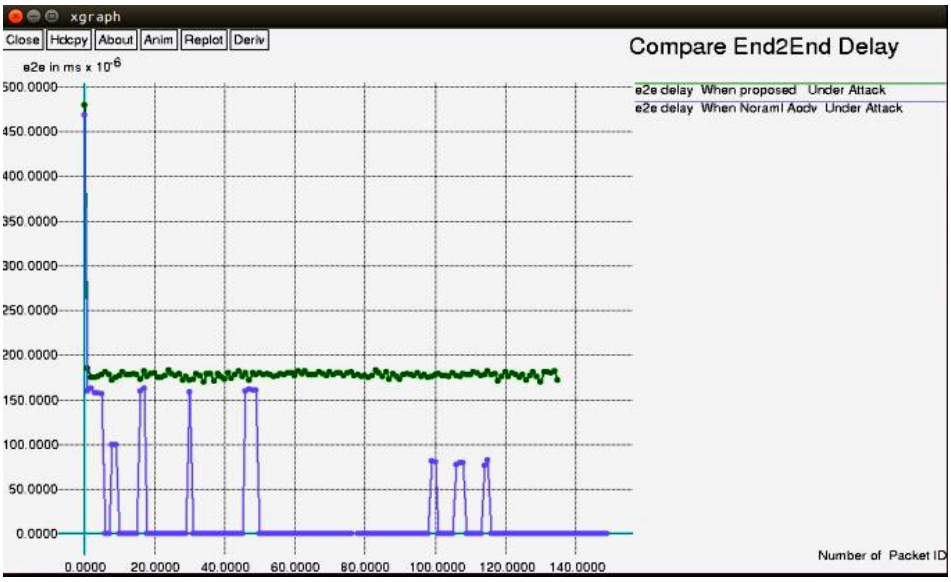

Figure 3: End to End Delay

The end to end delay is traced as the quantity of time needed to deliver a packet from root to destination. To compute end to end delay the succeeding formula is applied

$E2Edelay = Receivingtime - sendingtime$

End to end delay of the network for both routing methodologies. Figure 3 demonstrates interpretation of both routing scheme under attack order. The blue line shows the e2e delay of conventional AODV and the green line shows the interpretation of the trust- based protocol. Corresponding to observe effects conventional AODV routing incapable to deliver packets to the destination. Therefore end to end delay of the network tends to 0. On the distinct hand, the proposed methodology is suitable to get around the aftereffect of wormhole attack.

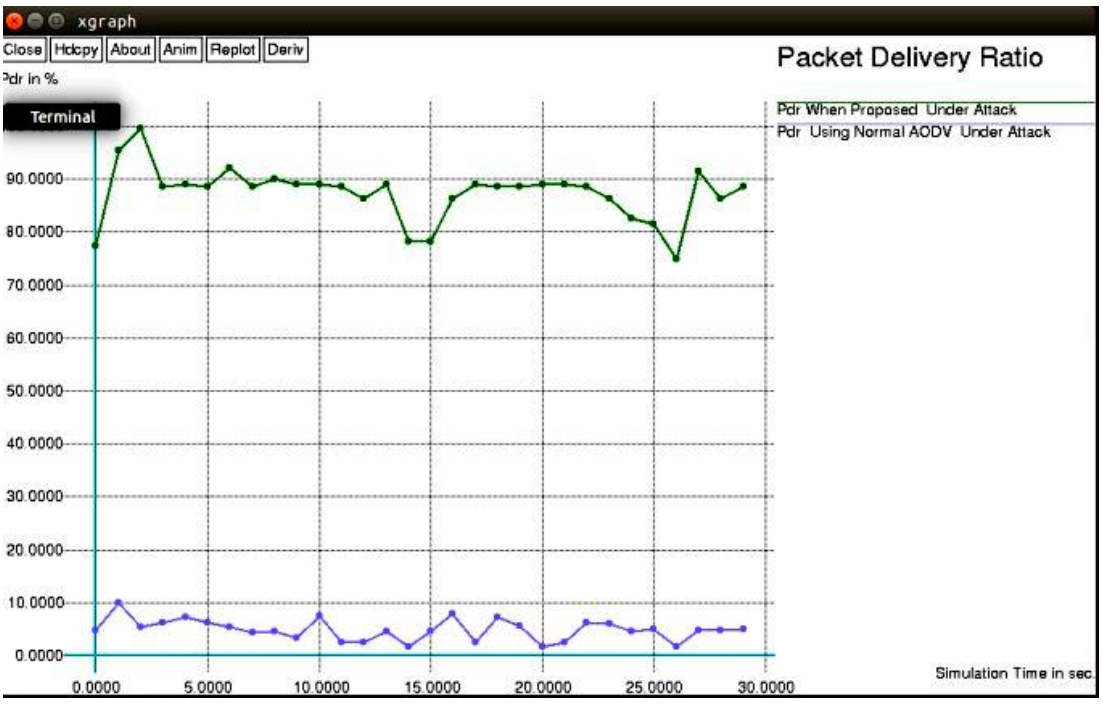

Figure 4: Packet Delivery Ratio

B. Packet delivery ratio

The composition of packets successfully delivered to the target node and rate of a total composition of packets is comprehended as packet delivery rate. The packet delivery ratio (PDR) is computed employing the succeeding formula

$$packetdeliveryratio = \frac{totaldeliveredpackets}{totalsentpackets}$$

The packet delivery rate of both approaches is described in figure 4. In this illustration, the green line shows the suggested approach interpretation and the blue line is employed for conventional AODV interpretation demonstration. As the contributed line graph the suggested approach shows the improved degree of packet delivery rate as analogized to the conventional methodology of routing because the conventional methodology isn't suitable to transmit the data to the target node during the attack contingencies.

C. Network Throughput

It's a measure of network effectiveness. The throughput of the network can exist defined as the quality of successfully message delivery with reference to time. It's typically measured in terms of bits per second or data packets per second.

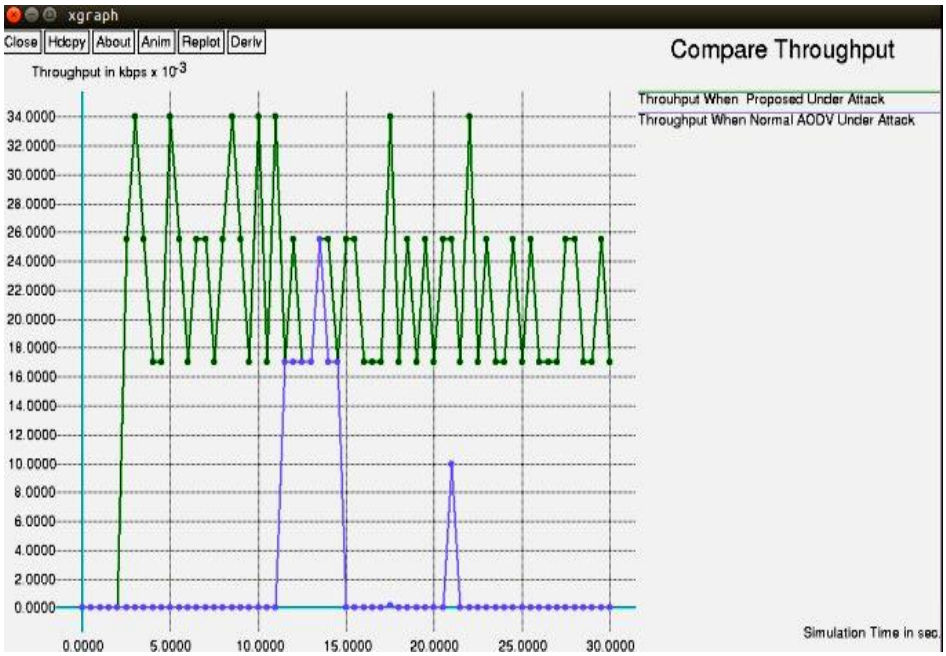

Figure 5: Throughput

Figure 5 shows the approximate throughput of both the protocols. The developmental observances are described in figure 5. The offered methodology shows advanced throughput as analogized to the conventional AODV. Because conventional AODV isn't suitable to deliver packets due to attack and offered methodology get around the malicious nodes in routes.

D. Energy consumption

The network requires a quantity of energy to accomplish network circumstances. Truly during transferring and admitting any packets. Thus an effective network interpretation is similarly described by the energy consumption of network nodes. Figure 6 demonstrates the energy consumption of the network for both the protocols. Then the green line shows the energy consumption of the conventional AODV and the red line shows the interpretation of the suggested secure routing protocol.

Corresponding to the secured energy consumption of the networks, the proposed methodology preserves the energy as analogized to the conventional method. Therefore the offered methodology is energy effective and extensively secure for helping the wormhole attacks in MANET.

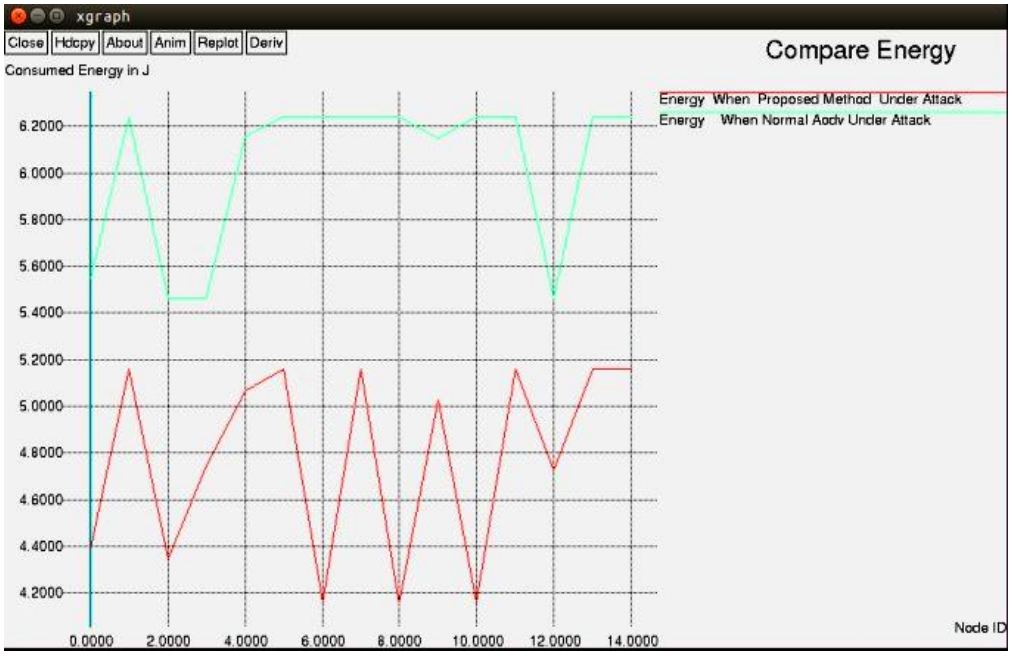

Figure 6: Energy consumption

E. Packet drop Ratio

The quality of unsuccessfully delivered data can exist termed as a packet drop rate. Therefore it's the rate of undelivered packets and the comprehensive packets transferred. That can exist computed employing the succeeding formula

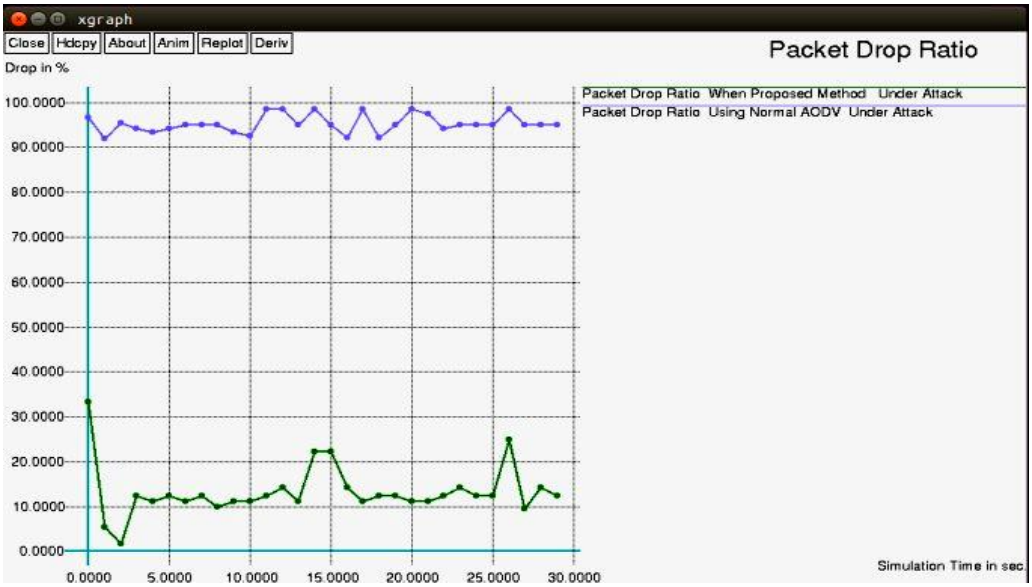

Figure 7: Packet drop ratio

Formula:

$$PDR = \frac{totalundeliveredpackets}{totalpacketssent}$$

The relative packet drop rate of the advanced secure AODV routing protocol and conventional AODV routing protocol is contributed in figure 7. In this illustration, the green line shows the quantity of packet drop employing the proposed methodology and the blue line shows conventional AODV interpretation. Corresponding to the secured interpretation, the offered methodology has the lower packet drop rate as analogized to

the conventional methodology. Therefore the suggested methodology is effective, energy conserving and efficient for protecting the network and can exist employed to secure the message in other real- world usages.

6. Conclusion & Future Work

This part provides a summary of the focused research work executed for shielding MANET against the wormhole attack. Therefore grounded on developmental observances and strategy points of lookout the consequence and future extension of the composition are offered.

A.Conclusion

The mobile ad hoc network is an efficient technology for communication networks. The nodes are self-dependent, mobile, self- organizing, and decentralized. Thus that network is applied in varied employments. But the network isn't significant self-assured for the distinctive types of routing based attacks. In this environment, the advanced composition is devoted to researching other routing based attacks. Also, the base is produced to study the wormhole attack. The wormhole attack is continually stationed employing two or further attackers. These attackers tunnel the data from one situation of the network to another position of a network applying high- speediness links. Due to this, the network creates traffic and utmost of the data dropped.

Table 3: Performance Summary

S.No.	Parameters	Proposed AODV	Traditional AODV
1	Packet delivery ratio	High	Low
2	Endtoenddelay	High	Low
3	Throughput	High	Low
4	Packetdropratio	Low	High
5	Energyconsumption	Low	High

In ordering to correct the discussed wormhole challenge in the mobile ad hoc network, a trust-based result is offered for system and execution. The offered trust- based methodology initial computes the threshold trust valuations grounded on the ideational network conditions. After scaling the threshold trust each way is estimated against the calculated threshold and if the node trust is lower than the calculated threshold we label that node as legal else that node is labeled as the malicious node.

The execution of the offered methodology is executed applying NS2 (network simulator 2). Furthermore for measuring the performance of the network the X graph tool is applied. The calculated performance of both the network methods is established using table 3.

Corresponding to the secured results as presented in table 2 the offered routing protocol is secure, energy effective and offers responsible data delivery under the wormhole attack. Therefore the advanced methodology is passable for non-identical fields of operations and usefulness.

B. Future work

The main goal of the advanced work is to enhance the security of the routing protocol for the wormhole attack is attained successfully. The given away composition is effectual and can exist offered for the succeeding research fields

1. The offered trust- based routing method presently prevents the wormhole attack in the closer future it's tested to affect the different attacks to rectify the security effects.
2. The advanced composition involves the

calculation of restricted network parameters, in the future, additional network characteristics are researched for enhancing the security of MANET.

References

[1] M. Arioua, Y. E. Assari, I. Ez-zazi, A. E. Oualkadi, "Multi-hop cluster based routing approach forwireless sensor networks", Procedia Computer Science 83 (2016) 584 – 591, 2016 Published by ElsevierB.V

[2] S. Chettibi, S. Chikhi, "Dynamic fuzzy logic and reinforcement learning for adaptive energy efficientroutinginmobilead-hocnetworks",Applied SoftComputing 38(2016) 321–328,2015ElsevierB.V

[3] M. Shila, W. Shen, Y. Cheng, X. Tian, and X. Shen, "AMCloud: Toward a Secure Autonomic MobileAd Hoc Cloud Computing System", IEEE Wireless Communications • April 2017, 1536-1284/17/$25.00 ©2017IEEE

[4] Anal Patel, Nimisha Patel, Rajan Patel, "Defending Against Wormhole Attack in MANET", 2015 FifthInternationalConferenceonCommunicationSystemsandNetworkTechnologies,978-1-4799-1797-6/15

[5] Tuna, D. G. Kogias, V. C. Gungor, C. Gezer, E. Taşkın, E. Ayday, "A survey on information securitythreats and solutions for Machine to Machine (M2M) communications", J. Parallel Distrib. Comput. 109(2017)142–154, 2017ElsevierInc.

[6] P. Amish, V. B. Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Networkusing AOMDV protocol", Procedia Computer Science 79 (2016) 700 – 707, 2016 The Authors. PublishedbyElsevierB.V

[7] N. Nissar, N. Naja, A. Jamali, "Lightweight authentication-based scheme for AODV in ad-hoc networks",2017 International Conference onWireless Technologies, Embedded and Intelligent Systems (WITS),10.1109/WITS.2017.7934616

[8] S. Chiu, K. S. Lui, "DelPHI: wormhole detection mechanism for ad hoc wireless networks", 2006 1stInternational Symposium on Wireless Pervasive Computing, IEEE2006,DOI:10.1109/ISWPC.2006.1613586

[9] Hlavacek, J. M. Chang, "A layered approach to cognitive radio network security: A survey", ComputerNetworks xxx(2014)xxx–xxx, 2014ElsevierB.V. Allrightsreserved.

[10] M. Bouabdellah, N. Kaabouch, F. E. Bouanani, H. B. Azza, "Network layer attacks and countermeasuresin cognitive radio networks: A survey", Journal of Information Security and Applications 38 (2018) 40–49,2017ElsevierLtd

[11] P. Patel, R. Bansode, b. Nemade, "Performance Evaluation of MANET Network Parameters using AODVProtocol for HEAACK Enhancement", Procedia Computer Science 79 (2016) 932 – 939, 2016 TheAuthors.PublishedbyElsevierB.V

[12] A. Nayyar, "Flying Adhoc Network (FANETs): Simulation Based Performance Comparison of RoutingProtocols:AODV,DSDV,DSR,OLSR,AOMDVandHWMP",978-1-5386-3060-0/18/$31.00©2018IEEE

[13] Dhaka, A. Nandal and R. S. Dhaka, "Gray and Black Hole Attack Identification using Control Packets in MANETs", Procedia Computer Science 54 (2015) 83 – 91, 2015 The Authors. Published by Elsevier B.V.

[14] Mamata Rath, Binod Kumar Pattanayak, "Methodical survey on real time applications inMANETS:Focussingonkeyissues",978-1-4799-5958-7114/$31.00102014IEEE.