OLSR Protocol Denial of Service Attack Solution Using Fictitious Nodes and Key Management

R.Bhuvaneswari[#1],Prof.R.Ramachandran[*2]
[#1]Research Scholar,Faculty of Computer Science and Engineering,SathyabamaUniversity,Chennai.
bhuvana_ron@yahoo.com
[*2]Professor and Head,Department of Electronics and Communication Engineering,
Dhanalakshmi College of Engineering, Tambaram,Chennai.
chandra557@yahoo.co.in

***Abstract*—Mobile ad hoc Network (MANET) is more commonly outlined as a network containing workforce of self-sustaining nodes interconnected with the aid of wireless connections. Considering that the entire mobile nodes in MANET can transfer freely, every node can behave as a router to forward packets from source to destination. So routing security needs to be relevant in MANET which results in performance degradation. The Denial of service (DoS) attack has more force in MANET that intents several forms of severalattacks in the ad hoc network. In order to beat the DoS attack we advocate a new methodology that is best suitablefor Optimized link State Routing (OLSR) protocol.**

The new mitigation system is to shield the OLSR protocol from node isolation attack. Securing information under such circumstances becomes an important consideration. In Elliptic Curve Cryptography (ECC), large size keys are required and secret sharing among neighbors should be initiated repeatedly because of the mobility of nodes. Therefore, an efficient key management scheme which overcomes the above drawbacks is still a prime requirement in MANETs.

Keyword - OLSR, Network Layer Attacks, Security, Denial of Service, MANET, Fictitious.

I. INTRODUCTION

A Mobile ad-hoc network (MANET) is a self-sustaining network system of routers and hosts related through Wi-Fi links. They are able to be setup in any place without any want for external infrastructure like wires or base stations. The routers are free to maneuver randomly and arrange themselves. The network can also be hooked up in anyplace without any geographical restrictions.

Mobile ad-hoc network is compatible for areas where fixed infrastructure is just not viable. Due to the fact that these networks have no constant infrastructure or centralized administration, they're often referred to as no fixed topology community. MANETs more commonly suffer from security attacks since of its features like open medium, altering its topology dynamically, lack of important monitoring and administration, and no clear security mechanism. The nodes keep in touch with every other on the foundation of mutual trust. This attribute makes it easier for the attacker to go throughout the network and get access to the continuing conversation.

Routing protocols in MANET will also be labeled into two classes: reactive protocol and proactive protocol. In proactive routing protocols, all nodes have to maintain a steady view of the community topology. When a network is dynamic, respective updates must be propagated in the course of the network to inform the alternate. In reactive routing protocols for mobile ad-hoc networks, which are also called “on-demand” routing protocols, routing paths are looked for, when wanted. These days, the most promising protocol in the field of MANET tends to be the Optimized link State Routing (OLSR) protocol.,due to the fact that the total outcome shows that the OLSR protocol presents connectivity and routing with a good performance. It has valuable aspects such as no route discovery lengthen and ease of integration into existing systems, which makes it good-fitted to time vital and emergency rescue functions. OLSR is liable to various forms of assaults.

Even though many study works had been applied for routing attacks in MANET, most of it targeted in most cases on re-active routing protocols. Optimized link state routing (OLSR) protocol which is a proactive routing protocol presents promising efficiency in phrases of bandwidth and visitors overhead but it surely does no longer include any protection measures.

II. BACKGROUND STUDY

The Optimized link State Routing protocol (OLSR) is a proactive link state routing protocol. In OLSR routing protocol, there are two forms of manipulate packets used: Hello packets and Topology control packets (TC). Hello packets are used to construct the regional of a node and to realize the nodes which are within the environment of the node. And this is also used tocompute the multi-hop relays of a node. The OLSR protocol makes use of the periodic broadcast of hello packets to set up the connection.

The Hello messages are received by way of all one-hop neighbors; however the Hello messages usually are not forwarded to different nodes by way of the acquired node. This hello message broadcasting will happen for each constant interval; this is often called Hello interval. This allows for the nodes to realize its two-hop neighbors considering the fact that the node can passively take part in the transmission of its one-hop neighbor. The reputation of these links with the other nodes in its local will also be asymmetric, symmetric or Multi Point Relay (MPR).

The principal talents of using OLSR is it does now not require that the link reliable for the manipulate messages. The messages might be dispatched periodically and the delivery does no longer have to be sequential.

The OLSR is easy to combine with present operating systems and it most effectively interacts with the host routing table. This is more suitable for the appliance, which wants fast transmission of the information packets with low extend.

The main process of OLSR is as follows.

- ✓ Neighbor sensing
- ✓ MPR (Multi Point Relay) selection
- ✓ MPR information declaration
- ✓ Route table calculation.

The foremost concern of OLSR is it desires more time to rediscover a damaged link. And it additionally wants extra processing vigor at the time of alternate route discovery. With the protection constraint, in OLSR the entire TC messages are wanted to be secured. And the host and gateways are statically configured with a view to promote the routes to the legitimate addresses.

The important thing to proposetheOLSR is the use of multipoint relay (MPR) to provide efficient flooding mechanism through reducing the quantity of transmissions required. MPR announce this understanding periodically of their manipulate messages [1]. Handiest nodes selected as MPR nodes are in charge for advertising as well as forwarding MPR selector record marketed by means of other MPRs. The protocol is first-rate compatible for big and dense network as the process of MPRs works well on this context. Thereby a node announces to the community, that it has reachability to the nodes which have chosen it as an MPR. The protocol makes use of the MPRs to facilitate efficient flooding of manipulate messages within the community.

A node selects MPRs from among its one hop neighbors with symmetric bidirectional links. Hence, deciding on the route through MPRs routinely avoids the problems associated with data packet switch over uni-directional links. In OLSR protocol two varieties of routing message are used, specifically, hello message and TC message.

A Hello message is the message that is used for neighbor sensing and MPR determination. In OLSR, each and every node generates Hello message periodically (each good day INTERVAL). A node’s hello message includes its own deal with and records its 1-hop neighbors. A TC message is the message that's used for route calculation. MPR nodes advertise TC message periodically, in order to avoid flooding. A TC message includes the record of the sender’s MPR selector. The protocol functioning of OLSR is as follows.

A. Neighborhood Discovery

Neighborhood Discovery is the system, whereby each router discovers the routers which can be in direct verbal exchange variety of itself (1-hop neighbors), and detects with which of those it will probably set up bi-directional communication.

B. MPR Flooding

MPR Flooding is the procedure whereby every router is competent to and effectively behaves community-huge pronounces.

C. Link State Advertisement

Link State advertisement is the procedure whereby routers are settling on which link state knowledge to advertise by means of the community.

III. ATTACKS AGAINST OLSR

We now talk about more than a few protection dangers in OLSR. The intention shouldn't be to stress flaws in OLSR, because it does not comprise safety measures in its design, like a couple of other routing protocols. Even as these vulnerabilities are exact to OLSR, they can be obvious as situations of what different hyperlink state routing protocols, comparable to OSPF, are subject to.

Additionally that an attacker performing identification spoofing or message replay wishes to alter the Message Sequence number discipline of the spoofed or replayed message.

A. Blackhole Attack

Black hole attack is a kind of DOS attack which is launched by malicious intruder existing in the ad hoc network. An attacker sends fake routing expertise to the neighbor node that it is having the shortest course between source and destination. So, the other nodes send knowledge by means of the malicious nodes and the attacker will seize all of the data. An attacker drops the information packets or modifies the information packets coming from the source node and sends it to the vacation spot. Handiest with the support of hello & TC message the know-how is exchanged between the nodes in OLSR protocol [3].

The node performing as a black hole sends a fake hello to the nodes and shows that it is having more than one neighbor node for retransmitting the information. In these hello messages an attacker node claims to have links to more neighbors than it virtually has. So the source node selects that node as a Multipoint Relay (MPR) node. When black hole node is selected as a MPR node then all of the information which is distributed via the neighbor nodes of the MPR will go via them and the complete data packet shall be captured.

The more neighbors the attacking node claims to have, the bigger the competencies effect of the assault. As a result of the false message of the attacker, in its local falsified TC messages with too few entries or no TC messages as a result of an empty MPR selector set are propagated. Accordingly, the attacker is equipped to seize the routes. These time nodes have been taken over and act as black hole node. This leads to a few changes in the network.

B. Wormhole Attack

A wormhole attack is quite often carried out with the aid of two or extra malicious nodes in conspiracy. Two malicious nodes at exclusive places send received routing messages to one another by way of a secrete channel. In this method, although the 2 malicious nodes are located far from every different, they show up to be within one-hop communiqué variety. Accordingly, the route passing via the malicious nodes is probably to be shorter than any other normal one. Wormhole nodes can effortlessly take hold of the route from the supply node to the vacation spot node, after which sniff, drop, or selective-drop knowledge packets handed by means of.

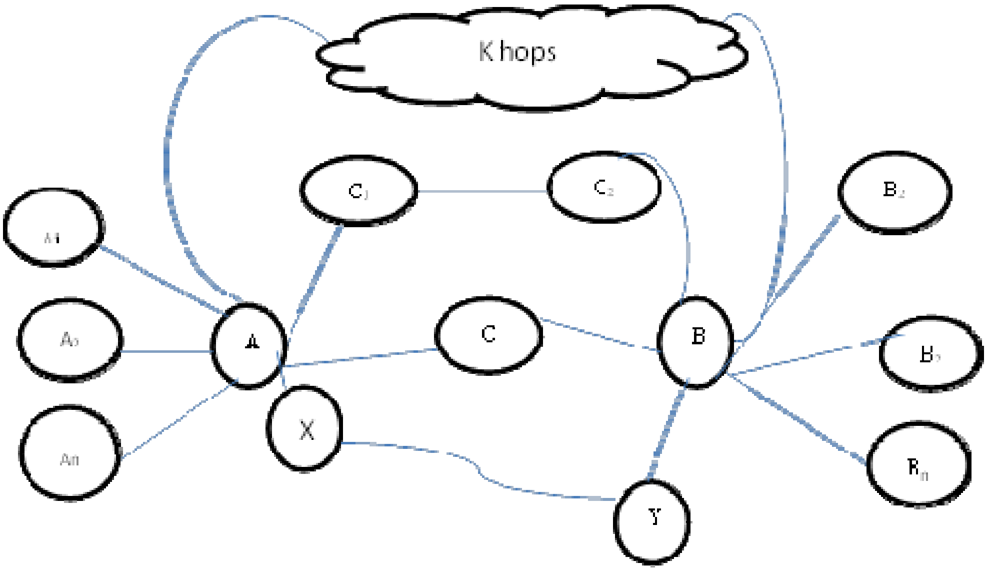

Fig.1. Wormhole Attack Model

Considering a wormhole attack can closely affect topology construction, it could be lethal to many adhoc routing protocols, above all proactive routing protocols similar to OLSR, which periodically exchange manage packets for neighbor discovery and topology development. Figure 3.1 depicts an ad hoc network together with a wormhole tunnel.

When node A broadcasts its good day message, node X (an attacker) copies this hi there message and tunnels it to node Y (the colluding attacker) by way of the built wormhole. Y receives A's hello message and replays it in its flooding. When node B receives the replayed hello message, B deems node A to be its one-hop neighbor. Following an identical method, node A may be delivered to assume node B to be its one-hop neighbor. After a distinctive time, a symmetric hyperlink will also be situated between A and B consistent with the OLSR mechanism. As soon as this spoofed symmetric hyperlink is headquartered, A and B are probably to decide on each and every others as multipoint relays (MPRs), which then leads to an alternate of some topology manage (TC) messages and knowledge packets via the wormhole tunnel.

C. Greyhole Attack

Grey hole is a node that may change from behaving thoroughly to behaving like a black hole that it is actually an attacker and it'll act as a usual node at other intervals. Every node continues a routing table that neighborsthe next hop node understanding which is a route packet to vacation spot node [9]. If a supply node is in ought to route a packet to the vacation spot node it uses a detailed route and it'll be checked in the routing table whether it is available or no longer. If a node initiates a route discovery procedure by using broadcasting Route Request (RREQ) message to its neighbor, by way of receiving the route request message the intermediate nodes will replace their routing tables for reverse route to the source [10]. A route reply message is distributed back to the supply node when the RREQ question reaches either to the destination node or to every other node which has a current path to vacation spot.

The grey gap attack performs its motion in two different phases:

Phase 1: With the rationale of interrupting packets on fake route, a malicious node performs the OLSRprotocol to give value as best itself having a valid route to destination [4].

Phase 2: The grey gap attack is elaborate to search out. On this the nodes drop the intermittent packets with a particular likelihood. When the packets are usually not dropped, the grey hole attacker behaves like ordinary node then it switches to its malicious behaviour [4].

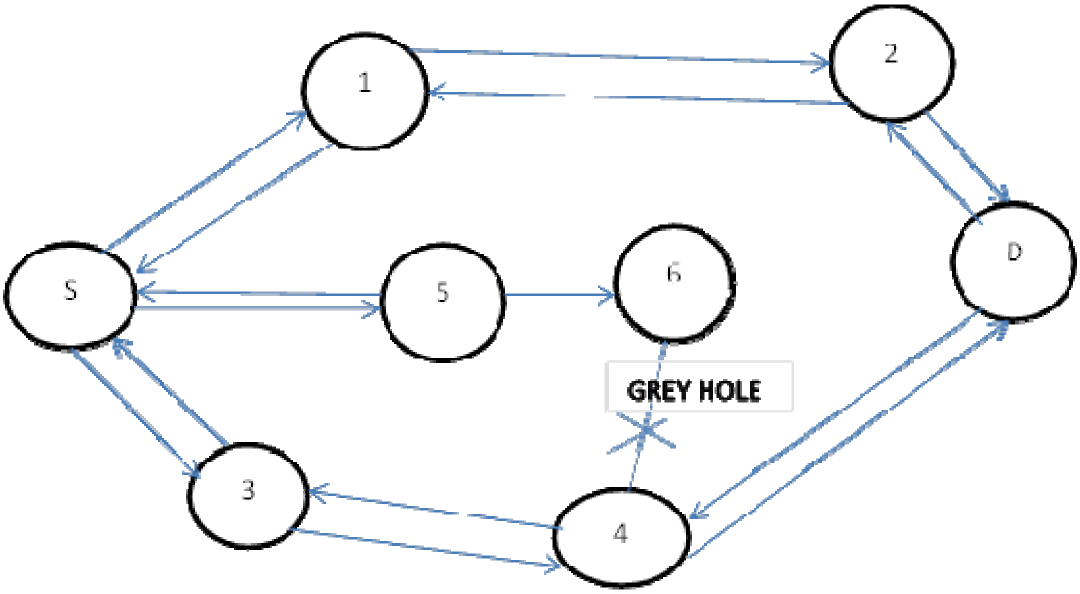

Fig. 2.Grey hole Attack Model

IV. PROPOSED SYSTEM METHODOLOGY

The primary requirement of the proposed procedure is that each and every node will handiest use expertise to be had to it, without relying on any centralized or neighborhood relied on authority. Our procedure does now not actively verify the Hello message; as an alternative it checks its integrity with the aid of searching for contradictions between the Hello message and the identified topology. We permit for lone MPR nominations, provided that no contradictions are observed.

A. Find Multipoint Relaying

Each node finds Multipoint Relaying by way of OLSR technique. In this procedure MPRs are chosen by means of a node as a subset of its 1-hop neighbors, such that the MPR set permits insurance plan for all of its 2-hop neighbors. By minimal MPR selection, a node is ready to keep up a correspondence to all 2-hop neighbors with minimal duplication. As a consequence, both topology control messages and data packets are most effectively forwarded by using this minimal MPR set, permitting for fewer replica messages at the same time keeping the network with huge protection.

1 Hop neighbors and 2 Hop neighbors are calculated based on the all on hand paths previously calculated. The number of destination a distinctive node can attain is recognized and paths to reach every destination with the aid of 2 Hops are calculated.

Minimal MPR set is discovered by means of settling on the one hop nodes which is able to reach all of its two hop nodes quite simply. From the minimal set a MPR is chosen by the way of voting mechanism and which MPR gets extra help might be elected as the only MPR for the unique node. MPR is chosen for each node and the 2 Hop paths to reach each area is discovered and the tables are up-to-date. To notice that, MPR slash the quantity of reproduction retransmission messages even as forwarding a broadcast packet.

Even within the face of contradictions, an MPR can be nominated for all 2-hop neighbors for whom it is the sole access point. It can't, nonetheless, be nominated as sole MPR for two-hop neighbors that may be reached by means of other paths.

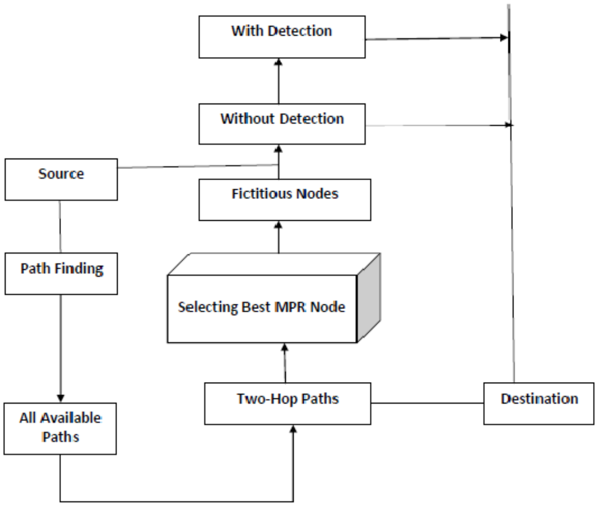

Fig. 3. Proposed System Architecture

We justify this assumption considering that bogus TC messages don't forestall a legit (attacked) sufferer from transmitting a valid TC that contradicts the fictitious one. In essence, by means of publishing a fraudulent TC, the attacker discloses that he's attacking; allowing others to take preventive measures. A fake howdy message is a way more crippling assault, because it eliminates a sufferer from the community without its skills. As a consequence, DOS and network disruption due to fraudulent TC messages is outside the scope of this paper. In order to avert nodes within the community from disseminating false information about their connectivity to the others, we installed a mechanism requiring every node to examine whether or not an assault can also be made by way of it. If one of these lie is viable, the node adds a fictitious node to the network, preventing anyone from claiming false connectivity to this false node. That's,the accountability for correctness of the connectivity know-how is delegated to the nodes themselves, as they have to inhibit others from utilizing them falsely. The issue mechanism for adding or eliminating fictitious nodes is given through:

- ✓ Each node has to add a fictitious node.
- ✓ A fictitious node does not belong to the adjacent nodes.
- ✓ New node advertises fictitious node by default, and only then calculates rule 1.
- ✓ Removing the fictitious node is done when is false.
- ✓ Examination must be performed periodically.

B. Detecting the Attack & System Recovery

In this module, we put in force the detection of isolation assault by way of an acknowledgement scheme. The target node can preserve track of the information packets and listens for acknowledgement from the communicating nodes. If the information is dropped or now not forwarded to the other nodes the acknowledgement is lost and the target node will look ahead to some TTL time. After that the goal node will intimate different nodes concerning the false MPR. Now the MPR is valuated for the attacking procedure and if observed guilty the MPR node is dropped from network and an additional MPR from minimal MPR set is employed for data forwarding. Now the network recovery will be done and all of the nodes will update their files through casting off the attacker node. All the OLSR paths may also be up to date leaving the attacking MPR.

To evaluate trust, a notion of believe measure is used in this paper. One of the most nodes in the MANET could show up or disappear relying on their pace and course of movement. The node within the given network area creates new hyperlink if it comes in that network area, whereas hyperlink could break if the node moves out of the field.

When nodes move and alter the topology in MANETs, the new companions will evaluate their trust stages. Even current nodes in the community will always calculate the trust while taking part in routing. By evaluating believe levels of nodes situated on different parameters, security can be inherently built into the routing protocol.

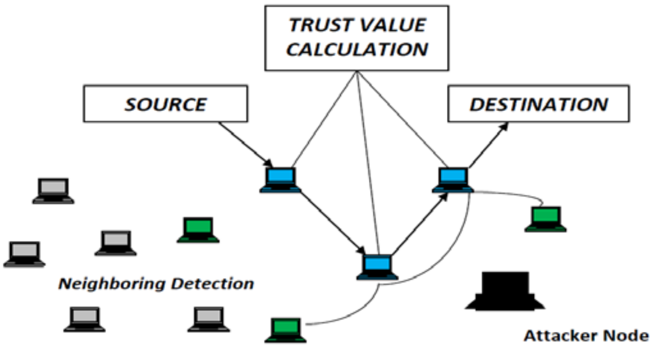

Fig. 4.Structure of the Proposed System

The believe phases of nodes examine the routing habits headquartered on set of trust attributes of the nodes and then such direction with maximum common trust measure is selected for routing. The nodes moving in same path (with identical speeds) are likely to keep the verbal exchange for long time. Such cellular nodes in routing route constitute so much steady and useful course for routing. Trust degree is evaluated utilizing three behavioral and one identity parameters, particularly Residual energy, Distance between Nodes, pace of nodes and affiliated group as per the philosophy described below.

V. KEY MANAGEMET INTEGRATED IN OLSR PROTOCOL

For creating faster, smaller and more secure network ECC is used in MANETS. ECC algorithm is being used for encryption and decryption. Communication is secured as the data cannot be viewed while passing through the network.The algorithm thus provides strong privacy protection, complete unlink ability and content unobservability for ad hoc networks. ECC is strongly resistant to attacks due to compromise between nodes.

ECC stands for Elliptic Curve Cryptography. It contains certain advantages. ECC is applied in case of devices that have several constraints in terms of bandwidth, battery power, processing computation efficiency, network connections, memory. This allows implementing cryptography in platforms that are constrained, such as wireless devices, sensor networks, smart cards, RFID’s and thin-clients. For example, the current key size recommendation for legacy public schemes is 2048 bits. A vastly smaller 224-bit ECC key offers the same level of security as 3072 bit legacy key which enables ECC more applicable for smaller devices [3].

Taking into consideration the above issues, our work focuses on the advantages of implementing ECC in wireless networks. ECC over prime fields is implemented for obtaining better performance characteristics in securing SSL(Secure Socket Layer).Using smaller key sizes ECC offers security equivalent to RSA and DSA.

The benefits of ECC are advantageous in applications where bandwidth, computation efficiency, processing efficiency, Power availability or storage is constrained.

An Elliptic Curve [I3] over F_q, is defined in terms of the solutions to an equation in F_q. The form of the equation defining an Elliptic Curve over F_q, differs depending on whether the field Fis a prime finite field or a characteristic binary finite field specified by the subscript q in F. An Elliptic Curve E over the field F is a smooth curve in the long Weierstrass form and is given by the equation (1.1)

$$Y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \qquad (1.1)$$

Where the coefficients a_i εF are real numbers and the variables **x** and y take on values in the **real** numbers.

Let E(F) denote the set of points **(x, y)** εF' that satisfy this equation, along with a 'point at infinity" denoted **0** 1141.

ECC makes use of Elliptic Curves in which variables and coefficients are based on the elements of a finite field. Two families of Elliptic Curves are used in cryptographic applications. The prime curve over F_q, makes use of a simplified cubic equation. In which the variables and coefficients take on values is the set of integers from 0 through p - 1 and in which calculations are performed over modulo p. The other is the binary curve defined over $F_2{}^m$, where variables and coefficients all take on values in Galois Field GF (2^m) and calculations are performed over GF (2^m).

A key exchange between users A and B can be accomplished as follows,

Step 1: A selects an integer nAless than n. This is A's private key. A then generates a public key P_A= nA*G; the public key is a point Eqn (a, b).

Step 2: B similarly selects a private key nBand computes a public key P_B.

It obtains the secret key K=nA*P_B. B generates the secret key K=nB*$P_{A.}$

Similarly the encryption and decryption can be obtained by the following

An encryption / decryption system requires a point G and an elliptic group Eqn (a, b) as parameters. Each user A selects a private key nAand generates public key P_A=nA*G. To send encrypted message, A chooses random positive integer k to produce the cipher text $C_m$consisting of the pair of points

$$\boldsymbol{Cm = kG, Pm + KPb} \qquad \textbf{(1.2)}$$

To decrypt the cipher text, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point.

$$\boldsymbol{Pm + KPb - nB(KG) = Pm + K(nBG) - nB(KG) = Pm} \qquad \textbf{(1.3)}$$

A has masked the message P_m by adding kP_B to it. No one except A knows the value of k, so even though P_B is a public key, nobody can remove the mask kP_B. For an attacker to recover the message, the attacker would have to compute k given G and kG, which is assumed hard in elliptic curve cryptography.

A. Implementation of ECC in MANET using OLSR

The Implementation involve simulations of MANET by forming a network with 'n' number of mobile nodes comprising sender nodes as 'S', receiver nodes as 'R' and other participating mobile nodes called shareholders(SH). First of all the user is asked to enter a message in binary form then the user is asked to enter the number of shares in which he wants to distribute the message after that the threshold value is entered by the user which is the minimum number of users required to retrieve the original message. The polynomial equation generated by finite field curve of x, y coordinates is used for generating the cipher texts based on the shares.

Now at the transmitter end the encrypted shares are generated which are in x, y coordinates and are transmitted to the receiver.

At the receiver's end the user is asked to enter the number of shares needed to recover the message followed by the index number of the shares by which the receiver can decipher the cipher texts using private key.

VI. CONCLUSION

In this paper, the MANET performance evaluation has been discussed for node isolation assaults. Proposed trust worth process have been simulated and five efficiency measures Packet supply Ratio (PDR), Time and protection, believe degree and community Throughput are evaluated . It is discovered that in all the simulations, the fashioned OLSR protocol results in a gradual increase in the PDR, believe level and community Throughput.

When we use proposed approach it is found that the community Throughput turns into constant. That is in view that the proposed system selects highest common trust degree route and routes the packets. Accordingly, we arrive with the conclusion that the proposed system, presents so much more desirable routing safety in comparison with fashioned OLSR, for various percentages of detecting malicious nodes.

Now we have considered simply the highest of 20 MANET nodes. When network dimension rises i.e., more than 20 MANET nodes, scalability hassle will occur. If a network subject is improved, the trail links could get altered and calculation of believe worth for gigantic community of nodes may just outcome in develop in time and this may also be taken as future work.

REFERENCES

[1] Mohanapriya, Marimuthu and IlangoKrishnamurthi,"Enhanced OLSR for Defense against DOS Attack in Ad Hoc Networks," Journal Of Communications And Networks, Vol. 15, No. 1, pp. 31-37,February 2013.

[2] D. Malik, K. Mahajan, and M. Rizvi, "Security for node isolation attack on olsr by modifying mpr selection process," in First International Conference on Networks Soft Computing (ICNSC), Aug 2014, pp. 102–106.

[3] Ms. Bhavna Sharma, &MrsVandanaMadaan, "Enhancing security of MANETs by implementing Elliptical Curve based Threshold Cryptography," in International Journal of Engineering and Computer Science, 2015. Volume 4 Issue 7, July 2015, pp. 13346–13350.

[4] K. Anandhi, B. Selvarani, A. NizreenaBanu& R. RohinBatcha, "A Comparative Study on Elliptic Curve Cryptography for MANET," International Journal of Research Engineering, Science and Technologies, vol. 1, no. 7, April 2016.

[5] M.CharlesArockiaraj, Dr.P.Mayilvahanan, "Overhead Minimization In Manet Using Improved Elliptical Security Algorithm,"International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-2, Issue-1,January 2016.

[6] A.Naveena, Dr.K.Ramalinga Reddy. "A Review: Elliptical Curve Cryptography in Wireless Ad-hoc Networks,"International Research Journal of Engineering and Technology, Vol.3, No.6. June 2016.

[7] Ankur Thakur and Anuj Gupta, "BlackHole Problem with OLSR Protocol in MANETs," International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 4. pp, 1-4, Sept 2014.

[8] Edna Elizabeth N.,Subasree S., S.Radha,"Enhanced security key management scheme for MANETs," WSEAS Transactions on communications, Volume 13 , 2014.

[9] Nadeem and M. Howarth, "Protection of manets from a range of attacks using an intrusion detection and prevention system," Telecommunication Systems, vol. 52, no. 4, pp. 2047–2058, 2013.

[10] Nadeem and M. P. Howarth, "An intrusion detection & adaptive response mechanism for manets," Ad Hoc Networks, vol. 13, Part B, no. 0, pp. 368 – 380, 2014.

[11] SharadAwatade, &PankajChandre, " Detection and Prevention of Attacks on MANETs Using Advanced EAACK and Hybrid Key Cryptography,"Proceedings of 44th IRF International Conference, 29th November 2015.

[12] Dega Ravi Kumar Yadav , K. Nikitha Reddy , N. Vamshi Krishna, " Authenticated Mutual Communication between two Nodes in MANETs," International Journal of Computer Science and Information Technologies, Vol. 4 (2) , 2013, 331- 333.

[13] M.CharlesArockiaraj, Dr.P.Mayilvahanan, "Overhead Minimization In Manet Using Improved Elliptical Security Algorithm,"International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-2, Issue-1,January 2016.

[14] A.Naveena, Dr.K.Ramalinga Reddy. "A Review: Elliptical Curve Cryptography in Wireless Ad-hoc Networks,"International Research Journal of Engineering and Technology, Vol.3, No.6. June 2016.

[15] LeventErtaul, NituChavan," Security of Ad Hoc Networks and Threshold Cryptography,"Distributed Computing Systems Workshops,Proceedings of 24th International Conference on IEEE, 2014.

[16] D. Dhillon, J. Zhu, J. Richards, and T. Randhawa, "Comparison of RSA-Threshold Cryptography and ECC-Threshold Cryptography for Small Mobile Adhoc Networks," Int. J. Advanced Networking and Applications, Volume: 03, Issue: 04, Pages:1245-1252,2012.

[17] R. Cavalcanti and M. A.Spohn, "On improving temporal and spatial mobility metrics for wireless ad hoc networks," Information Sciences, vol. 188, pp. 182-197, 2012.

[18] Jean-Marc Robert, HadiOtrok, AbdelkarimChriqi, "RBC-OLSR: Reputation-based clustering OLSR protocol for wireless ad hoc networks,"Computer Communications, vol. 35, pp. 487-499, 2012.

[19] R. K. Singh, R. Joshi, M. Singhal, "Article: Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET),"International Journal of Computer Applications, vol. 68, pp. 25-29, April 2013.

[20] Koul, A., & Sharma, M. (2015),"Cumulative Techniques for Overcoming Security Threats in Manets,"International Journal of Computer Network and Information Security,7(5), 61-73.

AUTHOR PROFILE

Ms Bhuvaneswari received her B.E degree from Avinashilingam University in the year 2004.She completed her M.Tech degree in Information Technology from Anna University in the year 2009.She is currentlypursuing her PhD in Sathyabama University under the Faculty of Computer Science and Engineering. She is working as Assistant Professor in the Department of Computer Science and Engineering, Saveetha Engineering college, Chennai. She also has published few papers in international journals and conferences. Her research interests are wireless adhoc networks, security issues of wireless networks and routing protocols in adhoc networks.

Prof Ramachandran is a graduate in Telecommunication Engineering, Post graduate in Communication Systems (Anna University, Chennai) and obtained PhD (Anna University, Chennai) in "Optical Neural Networks". He has served initially for 20 years in telecommunication field in a Government of India organization. After this he joined as a faculty in the department of Electronics and Communication Engineering, Sri Venkateswara College of Engineering, Sriperumbudur and served for 25 years. Now, at present he is Professor and Head of the department of Electronics and Communication Engineering, Dhanalakshmi College of Engineering, West Tambaram,Chennai-601301.