Secure and Efficient Location-Aided Routing Against DDOS Attack in Manet

H.J Shanthi1, E.A Mary Anita

Abstract*— A wireless LAN is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. There are many routing protocols used in wireless networks for transmission of message, among which, Location-Aided Routing (LAR) protocol is used to find the location of destination. This may be possible using Global Positioning System (GPS) in mobile. We concentrate on other malicious attacks that would have caused tremendous loss by impairing the functionalities of the computer networks. Denial of Service (DoS) and Distributed DoS (DDoS) attacks are two of the most harmful threats to the MANET functionality. From this point of view, LAR provides a solution against DoS and DDoS attacks. LAR does not have any security mechanism, so we propose a SE_LAR technique which includes traffic analysis methods and extended OEDA method. It is helpful to analyze the traffic, to detect an overwhelming traffic, legitimate nodes, congestion on network, and snooping attacks. Mobile Ad Hoc Network (MANET) is even more vulnerable to such attacks. So, in this paper, we propose Secure Location-Aided Routing (SE_LAR). Its results are compared with existing secure routing protocols like ISE_DREAM, SE_DREAM protocols. Using the existing SE_DREAM routing protocol malicious nodes are detected by traffic analysis process which is to monitor flooding impact on MANET. The OEDA method discriminates the attacker nodes from reputable nodes by evaluating the addresses in the response signal. But, it cannot be used for dense network, and cannot detect indirect Sybil attack. So, we introduce extended OEDA method with two schemes such as by refering cache memory of neighbor node scheme, and passive Sybil node identity detection, which is incorporated with SE_LAR routing protocol. OEDA method is currently incorporated with the SE_DREAM protocol, generally better known as ISE_DREAM, to produce the route to destination substantially more robust against DDOS attack. Finally we decide using the performance parameters to find out the best alternative among the three different routing protocols. Calculation of the performance of the computation compares SE_DREAM, ISE-DREAM and SE-LAR standards, the overall performance measurements by the NS2 simulator and using the parameters. To determine the effect of network size on the total performance of these protocols, we have three different phenomena.

Index Terms: Mobile Ad-Hoc Network (MANET), Denial of Service attack (DoS), Distance effect routing algorithm for mobility, Distributed Denial of Service attack (DDoS), SE-Location Aided Routing (LAR).

Manuscript published on 30 September 2019
***** Correspondence Author

H.J Shanthi1*, **,** Assistant Professor, AMET Deemed to be University, Chennai, Tamilnadu, India.

E.A Mary Anita, Professor, S.A.Engineering College, Chennai, Tamilnadu, India.

I. INTRODUCTION

The advances in the Mobile Ad-hoc Network have the ability to operate independently. In the present scenario, the mobile node is being used by everyone to contact and to form networks. The MANETs are used in many places such as military battle field, tactical network and disaster recovery [1]. MANETs have a significant attribute, which means that it does not need an infrastructure network with low cost for constructing the networks[21]. Normally, mobile node is used in two different ways which act as a mobile node or router [2]. Out of these acting as a router is very important. In order to create functionality of a mobile network that has a lot of misbehavior node connections Sybil node and legitimate node, it introduces DDOS on MANETs [3]. Finding the folder attacker is very difficult, because the nodes in this network are dynamically mobile, reducing the trustworthiness of the path provided for further communication in MANETs. Geographical Routing Protocols (GRP) provides the best solution when such a position exists. The two main characteristics of GRP are less memory overhead, communication overhead and minimum angle of the forwarding node information [4].

As a result of the dynamic nature of mobile nodes, it is an important task in MANET, to make changes in the nodes location by providing reliable path among mobile nodes. The Geographic routing protocols provide reliable paths in MANETs as an SE_LAR with less memory overhead based node cache memory by prohibiting predecessors with a minimum coverage area from source node view. We certainly have preferred Location-Aided Routing protocol for Mobility to give the protection against attacking nodes in the precautionary path [5]. The recommended security plan is used on the geographic routing protocol LAR which provides a secure path through reduced memory overhead, communication overhead and minimal energy intake. To start with traffic analysis approach, of every node is initiated by the source node with SE_LAR routing protocol which gives solution on flooding attack. We have proposed new protocol called Secure and Location-Aided Routing (SE_LAR).

The overall appearance of the black hole / gray-hole attack on the MANETs network is in losing the high performance of the network by destroying data packets and perhaps being forwarded directly to the destination node [6]. Sybil attacker may likewise influence adhoc networks negatively. The node which decline to share its resource with other nodes is a selfish node. The main idea of selfish node is to drop the data packets and preserve the resource for its own use[20][22].

Identification of reliable and trustworthy bad behavior of nodes can help to correct the malicious ones by helping security increase its demand or confidence, reduce the reputation of others or trust its virtual identities. The proposed method will provide SE_LAR routing protocol robust against flood attack, grayhole attack, blackhole attack. The traffic analysis method will give the way to solutions against flooding attack and along with exiting approaches like OEDA [7] , it name called extended OEDA. It will make the SE_LAR rugged against Black hole/Gray-hole attack and Sybil attack. These safety and security techniques are simply used in the forwarding area[23]. This means that there is less information available to use the security system, which provides more efficiency with the expression of some malicious nodes on the network. Extended OEDA method works like bait node, which can detect Sybil nodes in two different schemes. Scheme 1 by referring cache memory of neighbor nodes schemes, which works together with a source node and neighbor nodes and collects hop count from neighbor nodes and also a neighbor of neighbor nodes. The second scheme is passive Sybil node identity detection scheme, which works together with a source node and neighbor nodes and it collects hop count and affinity value from neighbor nodes and also a neighbor of neighbor nodes

II. RELATED WORK

Malgi et al [9], have proposed the idea of Anonymous Position based Security aware Routing Protocol (APSAR), how the protocol behaves, and anonymity protection between source to destination nodes. Information sharing nodes which are not in its coverage, the gap between them is divided into several segments and zones and feeds security. Rao et al[10], have made the suggestion on Secure Geographical Routing used with the Adaptive Position Update Technique (APUT). How it works, source node creates a group signature, because secure data transition is required. [11] The author proposed the secure location aided routing protocols, it provided security to channels. But it did not focus on the attacker. It comprises Diffie-hellman algorithm and shared security key is used to a protected path by communicating members. [12] The author proposed the secure LAR routing protocol with a neural network technique. It introduced a security framework. It focused area on energy consumption of nodes when overhead occurred on MANET, its framework provided a solution. [13] The author proposed the Trust enhanced cluster based multipath routing. It forms a cluster as a cluster head, supercluster head for computing trust value based on frame/packet loss rating, forwarding node energy, routing overhead. [14] The author proposed the secure location aided routing protocol. It comprises cryptographic feature works on two different environments such as geographic, non-geographic area. [15] The author proposed the universal framework for analyzing and detecting a various attacker in MANET. And they had incorporated with reverse search algorithm which provided the detecting rules. [16] The author proposed a defense against mechanism Sybil attacks. The forwarding node table has RSS values. It comprises previous message exchange detail which helpful for detecting Sybil node in MANETs.

Carter et al[17] , have proposed the idea of Secure Position Aided Ad-Hoc Routing (SPAAR), the way it works, the present position of node information on routing table. Routing table keeps track of the information of one-hop, that is the distance. The source node knows its truthiness' before making the forwarding packets. Pathak et al[18], have proposed were made on Geographic routing protocol and Greedy perimeter stateless routing Protocol (GPSRP) with Adaptive Position Update(APU) techniques that work together. The way it operates is using RC4 algorithm to encrypt source node information. Ranjini et al [19] have suggested the proposal to set up a highly skilled security routing on the dynamic network, by examining the searing security between source and destination node sand then forwarding data packets. Malgi et al[20], have proposed the Security Certificate Location Aided Routing Protocol With Dynamic Adaptation Of Request Zone (SC_LARDAR), and it focuses attention on Blackhole attack, to provide certificate based security scheme on flooding RREQ packets.

III. PROPOSED METHODS ON SECURE LAR

The DDOS attack is a more vulnerable attack in MANETs, which might include flat attack, black hole attack, gray hole attack, etc., Each node must cooperate with other nodes to form a communication link among mobile nodes. The malicious nodes present in the network, pose serious consequences that are created in reliable communication among the nodes in MANET. In order to create some reliable communication, malicious node necessarily requires the routing information. So, malicious nodes monitor network activity, if legitimate node can send data packet via network, it detects what is the possibility of forwarding nodes on request zone to destination node, where it creates flooding attack. Therefore, this paper has provided a better geographical routing protocol SE_LAR to offer the protection against DDOS attack. SE_LAR discovers the secure path by using location information of node statistics like referring cache memory of a neighbor node scheme, and passive Sybil node identity detection at every node in the communication area. To detect expected zone for the destination, a source node require the instantaneous neighbor node and it knows the destination node location, and then transmits the relay route request packet towards the request zone. In SE_LAR, every node maintains the location information of neighbor nodes in cache memory location in the network. It updates the information in route request packets forward which to the next neighbor of forwarding node in request zone. Extended OEDA invokes the first scheme when source node forwards packet in dense network and second level scheme works on sparse networks. The originality is present in the use of node performance parameter ratio on packet received, packet loss and delay of the node which could be used for the next hop selection in the mobile ad hoc network.[24]. Figure 3 (a) and (b) shows the request and response packet format of a SE_LAR routing protocol.

Type	Reserved	Hop Count
Broadcast ID		
Destination ID		
Destination sequence number		
Request zone		
Source location information		
Source sequence number		
Source ID		
Destination location information		

(a)

Type	Reserved	Hop Count
Destination ID		
Destination sequence number		
Source ID		
Source sequence number		

(b)

Figure 3: (a) LAR Route request packet format, (b) LAR Route response packet format

The request packet includes location information of destination node and hop count and we have embedded Traffic analyses method with LAR protocol to provide the solution against flooding attack in MANET which is called Secure Location-Aided Routing (SE_LAR) In addition to this, we propose extended OEDA approach to vanquish the Black hole /Gray hole and Sybil attacker inside the request zone. Hence we have named our proposed scheme as Improved SE_DREAM (ISE_DREAM). Our proposed secure routing scheme consists of 4 phases. They are,

- Zone discovery
- Traffic analysis
- OEDA approach
- Routing Data Packets

Zone discovery

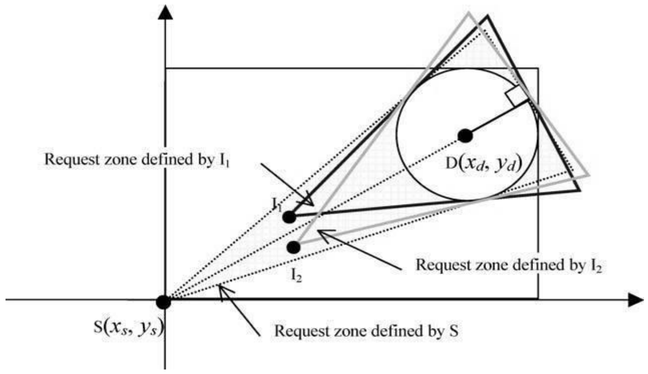
Request zone defined by I₁
I₁
D(x_d, y_d)
I₂
Request zone defined by I₂
S(x_s, y_s)
Request zone defined by S

Figure 4: Forwarding node determines which one is shorter distance with low time consumption

LAR location information is updated in all packets which creates low overhead on network which is used for the future path discovery. The location information of every node knows the neighbor node which is used for flooding the route request path to D for a request zone [3]. There are methods used to detect intermediate nodes between S and D in LAR protocols. In process 1, the source node creates a LAR box called request zone in which source node occupies a location in border of box and request zone consists of forwarding nodes and destination node as an expected zone.

The SEcure Location-Aided Routing (SE_LAR) routing protocol does not know location of all nodes in existing environment. Here every node automatically knows current location and neighbor node location using GPS(Xlp, Ylp). Many authors have not focused on the expected zone location. But our SE_LAR routing protocol provides that detail with additionally three types of forwarding area likes triangular, rectangular, circular area. If S and D both are in same coverage area of S. Location D is known by GPS(Xd, Yd) at time to by using equation 1.

$$V[(t1 - t0) + \Delta t) \qquad (1)$$

Where t0 is time of request creation at source, t1 is time of knowing detail about the destination node to source node, Δt is used for computing time interval, and V is node speed in coverage. The expected zone D, whose location is identified by axis information (XD, YD), and it is shown in the circle shapes in Figure 4. t1 is defined as the most recent reachable time to destination node location information, t0 is defined as the time taken by source node to trigger route request packet on network, (Vavg) denotes average velocity of D which is given in equation 2.

$$R = Vavg \times (t1 - t0) \qquad (2)$$

Where R is radius of circle which is centered at (XD, YD). SE_LAR box is divided into two zones like request zone and expected zone. Request zone contains source node S in corner of box at (XS, YS). Expected zone contains destination node D in center of circle at (XD,YD). The source node S determines the forwarding nodes present in expected zone; it forwards the route request packets onwards. In process 2, we give the LAR's second step, which means that if the nodes are present in the request zone closer to D's direction rather than the neighbor's nodes have sent the packet, it will determine if the distance is far off in the forwarding area. In the LAR domain and the LAR step, growth or reduction of the dimensions of the forwarding area through an error factor is decided.

IV. TRAFFIC ANALYSIS

SE_LAR routing protocol has two mechanisms for detecting malicious nodes in MANETs like traffic analysis and extended ODEA methods which consist of two schemes. Different ways of traffic analysis methods are used in MANETs. We consider the main way of traffic analysis. Because, we are using SE_LAR routing protocol, forwarding packet in the forwarded area in which no one legitimate node is found. If it is not a node in the forwarded area, the SE_LAR routing mechanism changes to rectangle shape from the shape of the triangle. So all the nodes in this forwarded area receive packet and detect destination node from triangle area. If No forwarding node is found such as void area or more number of Sybil node presented greater than legitimate node which is computed in $\Theta = 0.6 X |Fn(Xsource)|$ where Fn is a forwarding node and Xsource is a source node, then rectangle area shape changes to circular shape. If Participating node is involved using SE_LAR routing, there is source node S, Destination node D, forwarding nodes or neighbor node. The distance between S and Dis identified using the scheme1 or scheme2 which gathers every node information likeneighbor node details up to destination node value (Xd, Yd) and the center point of source node value(Xs, Ys). With this information destination node computes number of hop count with affinity value needed to receive data packets between S and D node, after this destination node generates reply signal which had part of the information as hop count, affinity value fields.Then source node computers computing values based on reply message which is had between S and forwarded node.

Algorithm working principle for forwarding node in SE_LAR

Step 1: Forwarding node is found between the S and D with coverage area shape as triangle, or rectangle, or circular shape.

Step 2: Forwarding node receives packet from source node.

Step 3: When the forwarding node receives packet, it evaluates stored information about forwarded packet within cache memory.

Step 4: Forwarding node contains information about the destination, it will generate route response signal sent to source node otherwise forward route error message.

Step 5: source node obtains additional information from route response or route error that information is about the traffic flow of forwarding node, data collision information, time taken to reach the destination node within threshold level of cache memory.

Algorithm working principle for source node in SE_LAR

Xsource is a source node, Xi is a collection of neighbor nodes of Xsource, Xj is a collection of neighbor nodes of Xi, Xmalicious is a malicious node which introducs Sybil nodes in direct communication or indirect communication in MANETs network. So extends OEDA method introduces two schemes which works based in network where scenarios like dense or sparse network. Scheme 1 works on dense network more numbers of nodes are involved.

Step 1: Source node identifies performance of forwarding node activity when source node receives route reply packet in which source node computes the total time of memory overhead and communication overhead.

Step 2: Source node works based on the following condition, when the SE_LAR routing protocol initiates area change discovery.

Step 3: based on error message, the source node verifies no more node exits in forwarding area which is detected based on extended OEDA method.

Step 4: If network type is dense then the source node triggers scheme 1 on forwarding area for detecting Sybil nodes.

Step 5: If network type is sparse, then the source node triggers scheme2 on forwarding area for detecting Sybil nodes.

Step 6: When source node obtains error message due to void area or more number of Sybil nodes existing more than legitimate nodes then source node changes its view in extended format , they show either which in Figure 5 and Figure 6 or which in Figure 8 and Figure 7.

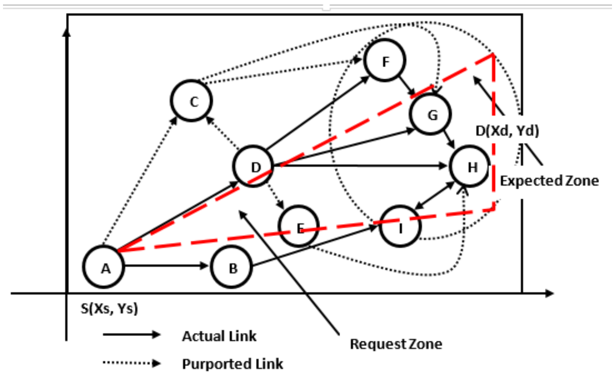

Figure 5: source node SE_LAR constructs triangle shaped area for sending packet to destination node without high traffic and DDoS.

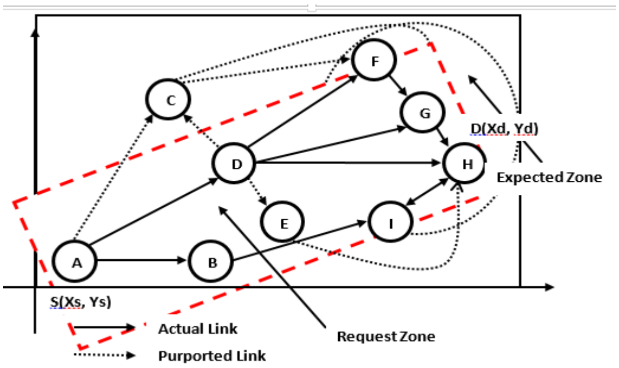

Figure 6: when source node was obtaining massage of forwarding nodes that have been void area or more Sybil nodes on transmission paths. So source node SE_LAR changes their view from triangular shape to rectangular shape.

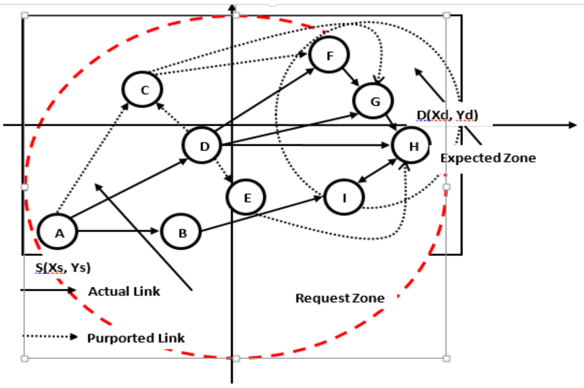

Figure 7: when source node was obtaining massage of forwarding nodes that have been void area or more Sybil node on transmission paths. So source node SE_LAR changes their view from rectangular shape to circular shape.

Route request or route reply message is used for communication to destination node D, communication path isestablished between node S and node D in MANETs. MANET obtains new topology structures with communicated area shape. It is occasionally monitored due to the following main reason. In the case of a node to detecting its next hop with the link is unreachable of destination node, while it is important for source node to re-send request packet to the destination nodes, when source node packet did not reach to destination node within time otherwise it received error response packet. Whenerror or reply error packets are received, the main source node of the broken link for the new way the request starts. Route request packet is received at each node as it is moving into forwarding area, and thus can reach the destination. A node obtains packet in second time, packet re-broadcast will not be sent. [6] In this papers' author (s) have proposed the process of discovery in the mathematical structure, two-way request to the link above and the way in response to upward. Source and destination node are available within source node coverage which evaluates by equation (3) and route response is given by equation (4).

$$R_{RQ} = S_{h=1} + \sum_{h=2}^{H=h+1} N_n + D_{H=h+1} \quad (3)$$

$$R_{RQ} = (S_{h=1} + \sum_{h=2}^{H=h+1} N_n + D_{H=h+1})C_i \quad (4)$$

Where R_{RR} and R_{RQ} is hop count of route request and route response messages, C_i is an additional coverage area of forwarding nodes with its index value.Route request packet to the destination node is detected, a route request packet is provided by destination node. In the same order, the response packet comes back to the source node. This concept is further clarified; if source node or forwarding node sends / forwards request signal towards to destination node in two different paths, destination node also had reply message in two different paths which is given in equation (5).

$$R_{RP} = H + \frac{H}{2} + (Nn - h - 2)p \quad (5)$$

Both route request and route response packet encounter problems on existing network, if any one of network node path is affected by control overhead and route discovery overhead in forwarding area, its memory value fields are affected. It will be helpful for node to take decision and analyze traffic. Equation (6) and equation (7) are given the discovery of route in MANETs.

$$R_{Discovery} = R_{RR} + R_{RQ} \quad (6)$$

$$R_{Discovery} = (S_{h=1} + \sum_{h=2}^{H=h+1} N_n + D_{H=h+1})C_i + H + \frac{H}{2} + (Nn - h - 2)p \quad (7)$$

SE_LAR routing protocols with its route maintenance overhead

Data transmit path is created, and then path tracking phase has been maintained between source and destination node for further communication. The SE_LAR have a logical mechanism, if any one of transmission path is broken then it finds and repairs them. It works for a specific period only. So SE_LAR performs overall link monitoring for the specific period which is computed by equation (8).

$$FN_{Nn} = 2\left(\frac{T}{t}\right) l \quad (8)$$

Where FN_{Nn}forwarding node with its neighbor nodes, T is is route life time, l is periodic interval time of route request packets.

$$FN_{Nn} = \sum_{i=}^{N} 2\left(\frac{T}{t}\right) l \quad (9)$$

Sum of the overhead on SE_LAR routing protocol

SE_LAR manipulates the link overhead on network whose field contains the sum of routing overhead value and the routing path discovery. Routing overhead is computed when nodes are exchanging message during data transmissions which is shown in equation (10) and (11).

$$R_{overhead} = R_{descovery} + FN_{Nn} \quad (10)$$

$$R_{overhead} = (S_{h=1} + \sum_{h=2}^{H=h+1} N_n + D_{H=h+1})C_i + H + \frac{H}{2} + (Nn - h - 2)p + \sum_{i=}^{N} 2\left(\frac{T}{t}\right) l \quad (11)$$

SE_LAR routing protocol is monitoring the hop count field value of route replay in between source and destination node, when either forwarding or destination node had high mobility, therefore link may be meted out any one of these: break down, hop count increase.

Extended OEDA approach

Extended obliging entice discovery approach (EOEDA) method is incorporated with SE_LAR routing protocol which is used for detecting attacks like Black hole / Gray hole, Sybil attack in MANETs. Sybil node creates the problem on route discovery, It suggests wrong path information to reach destination node, it acts as trust worthy node, but it works to give wrong information when discovery path is sought. Malicious node automatically gives the shortest path to reach destination to route request source node SE_LAR routing protocol gets route response message and extracts IP address of response node. Extended OEDA method consists of two schemes such as by referring cache memory of neighbor nodes and passive Sybil node identity detection. Figure 8 shows the execution steps of an extended OEDA method on SE_LAR routing protocol.

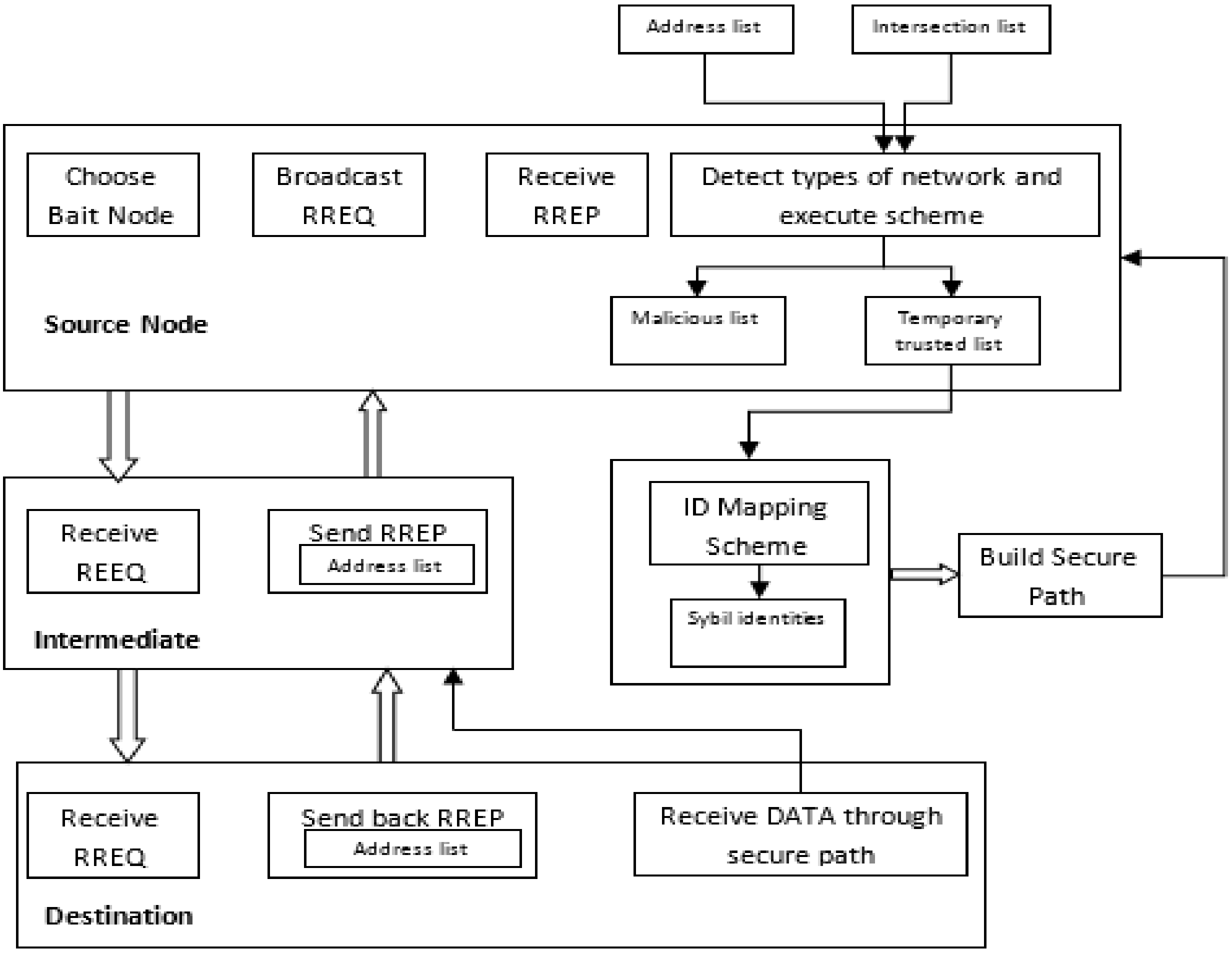

Figure 8: EOEDA method execution steps

Scheme: By referring cache memory of neighbor nodes

Bait node verifies the neighboring nodes data for detecting malicious node or Sybil nodes in MANETs. Based on the Bait node verifying the response message, if any malicious node had introduced some set of Sybil nodes detail which are not neighbor nodes of bait node but are neighbor nodes of malicious nodes. Bait node verifies if any void area occurred toward destination node. Bait node finds out what are the nodes acting as a stationary or dynamic node in MANETs. Scheme 1 has two different phases' for detecting Sybil node by bait node like identification phase, detecting Sybil node phase. Assume a process with source node called Xsource or bait node which works if any Sybil node is present in its working environment. All one hop neighbor nodes or forwarding nodes are called Fn(Xsource), where Fn(Xsource)={X1, X2,…Xn} and |Fn(Xsource)| = N, here Xi; Ci =1,2,3,….N denotes the forwarding nodes as neighbor list of nodes of Xsource, which consists of legitimate node(Ln), Malicious node(Mn) and Sybile node(Sn) such that Sn >> Ln.

Phase 1: Node identification phase

It is a primary phase of extended OEDA methods, Xsource finds neighbor nodse through one hop. Xsource broadcasts its message to its immediate forwarding neighbor nodes Xi. After Xsource receives reply message, then its neighbor sends broadcast message. Xsource does not verify second level of message which is verified by their request from forwarding nodes. If Xsource suspects any one of neighbor node as malicious node, then Xsource does not reply to that node. Malicious node only introduces a Sybil node. Xsource records the IP address of all nodes with base on request and reply message in first level hop, second level hop and third level hop. Figure 9 and 10 show direct communication from source to destination node.

Phase 2: Detecting Sybil Node phase (DSN)

Xsource finds one hop forwarding neighbor Xi by using method DSN(Xsource, Xi). IN this phase, each forwarding neighbor node knowS total number of neighbor node occurrences to each node. Where in Xsource node detects their count.

Retrieval Number C6870098319/2019©BEIESP
DOI: 10.35940/ijrte.C6870.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

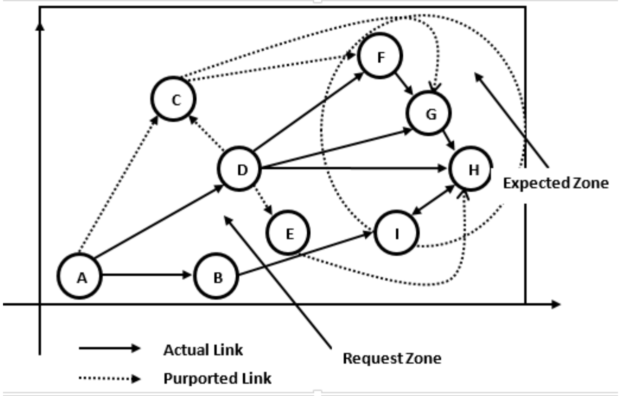

Figure 9: direct communication from source to destination node

ID	A	B	C	D	E	F	G	H	I
A	-	1	1	1	0	0	0	0	0
B	0	-	0	0	0	0	0	0	1
C	0	0	-	0	0	1	1	0	0
D	0	0	1	-	1	1	1	0	1
E	0	0	0	0	-	0	0	1	0
F	0	0	0	0	0	-	1	0	0
G	0	0	0	0	0	0	-	1	1
H	0	0	0	0	0	0	0	-	1
I	0	0	0	0	0	0	0	1	-

Table 2: Xsource detects common neighbors between Xsource and forwarding neighbors Xi

Xsource is a node A, Xi is a node B, C, D, E, F, G, H, I	
Xsource ∩ Xi	**Forwarding neighbor node**
A ∩ B	I
A ∩ C	F,G
A ∩ D	C,E,F,G,I
A ∩ E	H
A ∩ F	G
A ∩ G	H.I
A ∩ H	I
A ∩ I	H

Table 3: Xsource detects count of neighboring nodes for every node

The above table 2 and table 3 scenarios describe Xsource as a verifier of the forwarding neighbor nodes with respective IP address from B to I. Node D is a malicious node which has two Sybil nodes introduced with the identification names as C and E. Xsource node detects malicious node and Sybil node through Sybil node detecting algorithms. Table 2 represents the adjacency matrix of Xsource and its neighbor node. The malicious node D introduces Sybil nodes C and E in Figure 1. The second level hop message and third level of hop message are observed by Xsource node. If first level hop message of neighbor nodes did reply to second and third level hop message of neighbors near it and the remaining neighbor group. When void area or more number of Sybil nodes occur in forwarding direction, Xsource extends the focus view which is shown in Figure 5, 6 and 7.

Scheme 2: passive Sybil node identity detection

This scheme is triggered when mobile node works in sparse type network with set of mobile nodes in mobility, in which Xsource node may meet multiple Sybil nodes belonging with malicious nodes in mobility of either Xsource or malicious node. Therefore, we propose passive sybil node identity detection phase which works in following steps.

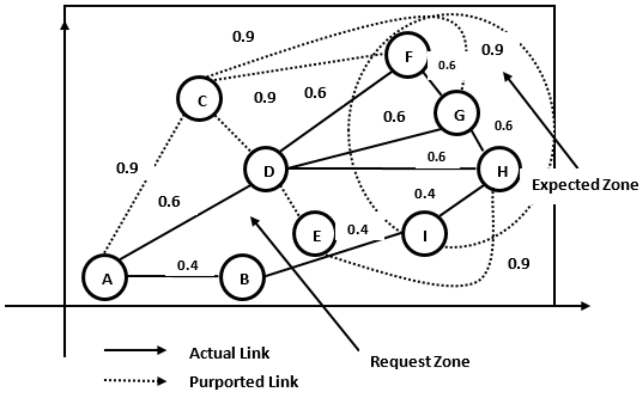

Figure 10: Undirected communication from source to destination node with its affinity value.

This scheme 2 does not require any special type of hardware, antenna, and there is no need of synchronization clock. The working principle of passive Sybil node identity detection: Xsource node requires at least one trusted node for observing other nodes in networks and it acts as an observer node in MANETs, which receives message from other nodes. The malicious node introduces Sybil node in network and creates Sybil attack. The observer node is observing neighbor node signal during observation period, which may differ from the signal used to transmit data, discover forwarding neighbor node and route reply. The observation node is used to allocate separate memory location for the nodes visited and how many times they occur and associated details are stored. The observation node analyzes their memory like any Sybil node id presented group of Sybil node IP, how many times they were repeated, which node introduced in them working environment.

Detecting mechanism

Observer node detects communication signal of two nodes Ti,j during observation period, the observer node does not detect communication signal of two nodes Li,j then we compute affinity value between the two setoff nodes Ai,j=[(Ti,j +Li,j) (Ti,j – 2Li,j)] / µ . Where µ is the total number of times both nodes computation, occur in observer nodes.

Routing data packets:

In the traffic analysis and extended OEDA approach, the source node sends packet over request zone, in which source node detects, to find whether any malicious node is present with Sybil node in forwarding direction. Therefore source node triggers extended OEDA method which has two schemes like by referring cache memory of neighbor node scheme and passive Sybil node identity detecting malicious node and Sybil node in different type of network. If more number of Sybil nodes are present in forwarding zone towards which source node compares them with legitimate nodes and invokes extended view for forwarding packets.

V. RESULTS AND DISCUSSION

Table 4: Simulation parameters

Parameters types	Parameter values
Numbers of nodes	10, 20, 30, …50
Antenna type	Omni antenna
Mobility model	Random way point
Transmission range	250m
Traffic model	CBR
MAC protocol	802.11
Mobility speed	10,20,30,40, m / msec
Path loss model	Two ray ground
Simulation area	1500 X 1000 m
Simulation time	60 m sec

We took three routing protocols like ISE_DREAM, SE_DREAM and SE_LAR routing protocols incorporated with mobile nodes in MANETs. We took for testing of experiments different numbers of nodes with different intervals. We used an area of 1500 X 1000 sq.m for our simulation. All nodes are utilizing the UDP/CBR traffic model for transmitting data from source to destination nodes. The time interval between each packet is 0.05 m sec. the remaining parameters are detailed in Table 4. Ns2 simulation software is used for the wired network or wireless network mobile network with data communication and its issues have been analyzed. It works as discrete time event driven model, in which it has two types of languages C++, and OTCL (Object Oriented Tools Command Language). NS2 has two platforms for simulation: one for animated model running in a front end and other platform used its recorded operations. The performance parameter tested includes packet delivery ratio, end-to-end delay, packet loss ratio, communication overhead, routing overhead and throughput. PDR (%) = $\frac{\sum(Pr)}{\sum Pi}$x 100 , Where PDR denotes Packet Deliver Ratio, Pr denotes the number of received, Pi refers the number of packets sent by Xsource node.

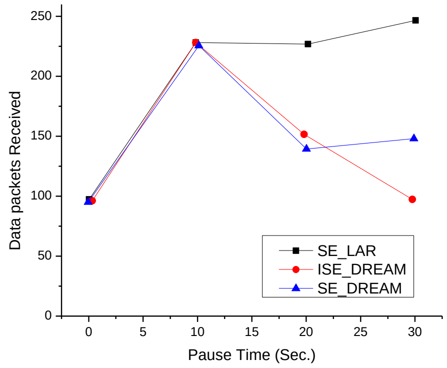

Figure 10: packet delivery ratio vs. pause time.

Packet delivery ratio is compared on SE_LAR, ISE_DREAM and SE_DREAM routing protocols which it computes the sent packets from a source node and received packets of destination node which computes by using awk script from NS2 simulation trace file. It computes the packet delivery ratio from the results of ISE_DREAM, it as show SE_LAR routing protocols in Figure 10. The performance PDR compared the SE_LAR routing protocol uses in MANET shows that deliver ratio is high for extended OEDA methods.E2E delay (ms) = $\frac{\sum(At-St)}{\sum Pi}$, Where E2E delay is denoted end-to-end delay, At and St are denoted the arrive time of packet and sent time of packet, Pi denotes the number of packets sent by Xsource node.

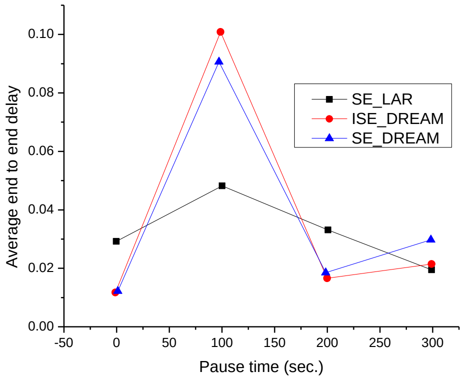

Figure 11: end-to-end delay vs. pause time

Figure 11 shown, the average end-to-end delay of ISE_DREA and SE_LAR. ISE_DREAM gives average end-to-end delay higher rather than SE_LAR routing protocol. ISE_DREAM gives the highest delay because every bait node only takes responsibility for rout selection for communication a source and a destination node, detecting the malicious node with Sybil node in MANETs. Bait node provides secure path details to the source node to the destination node. But SE_LAR routing protocol has extended OEDA methods in which it comprises two schemes for different scenarios.

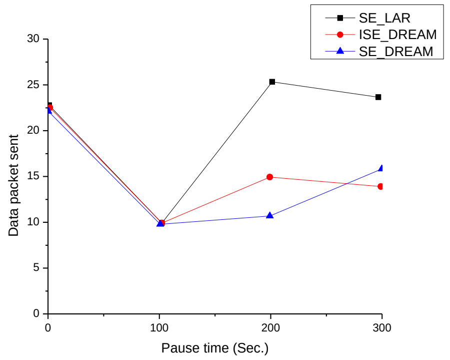

Figure 12: packet loss ratio vs. Pause time

Figure 12 shown packet loss ratio is evaluated by working condition of the network, if packet loss ratio is low then the network is working as a good condition otherwise the working network have been affected by any of them like congestion occurs, network overhead, higher handoff, the higher number of malicious nodes introduces Sybil node. SE_LAR routing protocol compared with existing ISE_DREAM in which we obtain a result is SE_LAR of packet loss ratio is lower than ISE_DREAM routing protocols.RO (%) = $\frac{NRP}{NRP+ NRPS}$x 100 , Where RO stands to routing overhead, is denoted the number of routing packets and is referred to a number of routing packet send. Figure 13 and 14 showed the normalized routing overhead and throughput.

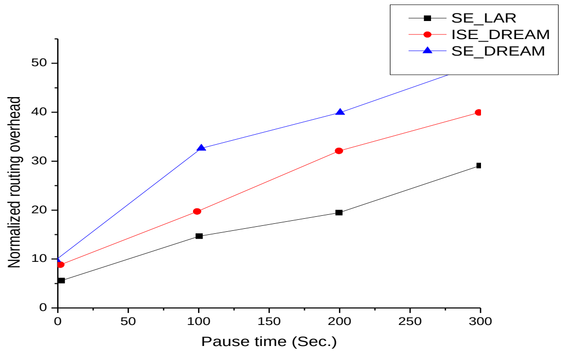

Figure 13: Normalized routing overhead vs. pause time

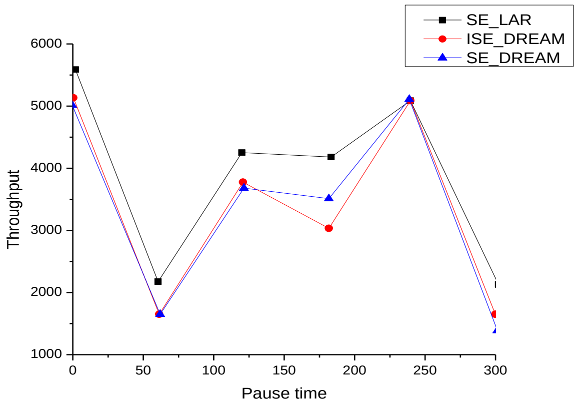

Figure 14: throughput on ISE_DREAM vs SE_LAR.

We compute throughput based on several packets transmitted by a source node and several packets delivered to a destination node within simulation time it measures which in bits per second. T=NDP *PS / ST, where T denotes the throughput, NDP and PS is several a delivered data packet and packet size, and ST is simulation time. The performance comparison of the output of the three difference routing protocols using SE_LAR, ISE_DREAM, and SE_DREAM. In figure 14 shows the results, SE_LAR, and SE_DREAM performance is much lower than ISE_DREAM. SE_LAR is finding an optimal way from source to destination nodes. SE_LAR finds new routes have reduced the control overhead traffic. So, it increased latency in finding a new route.

VI. CONCLUSION

This paper proposes a new secure routing protocol SE_LAR which is compared with ISE_DREAM, and SE_DREAM routing protocols. DREAM and LAR routing protocol did not provide secure communication. So if any packet is transmitted using in both protocols, they meet issues such as DDoS, denial information, acknowledgment loss, congestion. Therefore, we added security mechanism in LAR which is named as a SE_LAR which is robust against DDOS attack. The traffic analysis methods detected flooding attacks in request zone, extended OEDA method detected malicious and Sybil node by using two different schemes in different types of network. SE_LAR provides to subsequent the data packet forwarded to trusted node which is recommend by neighbor node list. SE_LAR routing protocol provides high security rather than ISE_DREAM communication with mobile nodes speed is low. In our future work will implemented in high speed mobility environment with dense network.

VII. REFERENCES

1 Loo, Jonathan, J. L. Mauri, and J. H. Ortiz. "Mobile Ad Hoc Networks." Mobile Ad Hoc Networks: Current Status and Future Trends (2012).

2 Mauve, Martin, Jorg Widmer, and Hannes Hartenstein. "A survey on position-based routing in mobile ad hoc networks." IEEE network 15.6 (2001): 30-39.

3 Kumar Karn, Chaitanya, and Chandra Prakash Gupta. "A survey on VANETs security attacks and sybil attack detection." International Journal of Sensors Wireless Communications and Control 6.1 (2016): 45-62.

4 Oubbati, Omar Sami, et al. "A survey on position-based routing protocols for Flying Ad hoc Networks (FANETs)." Vehicular Communications 10 (2017): 29-56.

5 Sarkar, Subir Kumar, Tiptur Gangaraju Basavaraju, and C. Puttamadappa. Ad hoc mobile wireless networks: principles, protocols, and applications. CRC Press, 2016.

6 Vishnu, K., and Amos J. Paul. "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks." International Journal of Computer Applications 1.22 (2010): 38-42.

7 Shanthi, H. J., and EA Mary Anita. "Secure and efficient distance effect routing algorithm for mobility (SE_DREAM) in MANETs." Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC–16'). Springer, Cham, 2016.

8 Ko, Young-Bae, and Nitin H. Vaidya. "Location-Aided Routing (LAR) in mobile ad hoc networks." Wireless networks 6.4 (2000): 307-321.

9 Malgi, Priyanka, and Ulka Padwalkar. "E-APSAR: Enhanced Anonymous Position Based Security Aware Routing Protocol For Manets." (2014).

10 Chen, Quanjun, Salil S. Kanhere, and Mahbub Hassan. "Adaptive position update for geographic routing in mobile ad hoc networks." IEEE Transactions on Mobile Computing 12.3 (2013): 489-501.

11 Yuan, Bai, et al. "Location-aided and secure routing protocol for heterogeneous multi-hop wireless networks." The Journal of China Universities of Posts and Telecommunications 23.1 (2016): 49-54.

12 Pragathi, YVS Sai, and S. P. Setty. "Performance Analysis and Validation of Fuzzy based Secure LAR Routing Protocol in MANETs using NN Tool." (2017).

13 Devi, Vallala Sowmya, and Nagaratna P. Hegde. "Multipath Security Aware Routing Protocol for MANET Based on Trust Enhanced Cluster Mechanism for Lossless Multimedia Data Transfer." Wireless Personal Communications 100.3 (2018): 923-940.

Retrieval Number C6870098319/2019©BEIESP
DOI: 10.35940/ijrte.C6870.098319
Journal Website: www.ijrte.org

14 Muthupriya, V., S. Revathi, and BS Abdur Rahman. "Secure Location Aided Routing (SLAR) for mobile ad hoc networks." 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). IEEE, 2017.
15 Zhang, Xin, et al. "Universal Analysis and Detection Framework for Location Aided Routing." 2016 21st International Conference on Engineering of Complex Computer Systems (ICECCS). IEEE, 2016.
16 Kumari, S. Vadhana, and B. Paramasivan. "Defense against Sybil attacks and authentication for anonymous location-based routing in MANET." Wireless Networks 23.3 (2017): 715-726.
17 Carter, Stephen, and Alec Yasinsac. "Secure position aided ad hoc routing." (2003).
18 Pathak, Vivek, Danfeng Yao, and Liviu Iftode. "Securing location aware services over VANET using geographical secure path routing." 2008 IEEE International Conference on Vehicular Electronics and Safety. IEEE, 2008.
19 Ranjini, S. Sharon, and G. Shine Let. "Security-efficient routing for highly dynamic MANETS." Int. J. Eng. Adv. Technol.(IJEAT) 2.4 (2013). Shih, Tzay-Farn, and Hsu-Chun Yen. "Location-aware routing protocol with dynamic adaptation of request zone for mobile ad hoc networks." Wireless Networks 14.3 (2008): 321-333.
20 Vennila, G., and D. Arivazhagan. "Hash based Technique to Identify the Selfish Node in Mobile Ad-hoc Network." Indian Journal of Science and Technology 8.14 (2015): 1.
21 GaneshKumar K, Arivazhagan D. New cryptography algorithm with for effective data communication. Indian Journal of Science and Technology. 2016; 9(48): 108970
22 Vennila G, Arivazhagan D & Manickasankari N. Prevention of Co-operative Black Hole attack in Manet on DSR protocol using Cryptographic Algorithm. International Journal of Engineering and Technology (IJET). 2014; 6(5): 2401.
23 Kumar, Ganesh, and A. Arivazhagan. "Modeling Portable Manager Aiding In the MANET Communication." Indonesian Journal of Electrical Engineering and Computer Science 9.3 (2018): 572-576.

VIII. AUTHOR PROFILE

Ms. Shanthi H.J, working as Assistant Professor in Academy of Maritime Education and Training (AMET) Deemed to be University. She has vast experience in teaching information technology subjects. She has published various research articles in SCOPUS/UGC/Referred international/ national journals. Received best teacher award from various institions.