Journal of Theoretical and Applied Information Technology
10th October 2013. Vol. 56 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT LOCATION AND DETECTION (ELD) BASED MOBILE AD-HOC IMPLEMENTATION WITH EMBEDDED SYSTEMS

[1] RAJARAM.M, [2] Dr.V.SUMATHY

[1] Assistant Professor Department of Electronics and Communication Engineering
Park college of Engineering and Technology, Coimbatore, India
[2] Associate Professor, Department of Electronics and Communication Engineering
Government College of Technology Coimbatore, India
E-mail: [1] happyramm900@gmail.com , [2]sumi_gct2006@yahoo.com

ABSTRACT

A Mobile Ad-hoc Network (MANET) is a temporary wireless network composed of mobile nodes, in which an infrastructure is absent. If two mobile nodes are within each other's transmission range, they can communicate with each other directly; otherwise, the nodes in between have to forward the packets for them. Several routing protocols have already been proposed for ad hoc networks. This paper suggests an approach to utilize location information obtained by using $DLRDP_F$ (Dynamic located Routing and Detection Protocol Far), if the destination is Remote and $DLRP_L$ (Dynamic located Routing and detection Protocol Local), if the destination is local. in this routing scheme affected various attacks. In MANETs, it is difficult to identify malicious attacks as the topology of the network dynamically changes. In this Progress we proposed new efficient dynamic detection scheme for attacks also . Using location information to help routing is often proposed as a means to achieve scalability benefits like Packet delivery ratio, Average delay ,packet loss and Qos in large mobile ad-hoc networks. and detect the attacks . We use the network simulator 2 (ns-2) system to conduct the MANET simulations and consider scenarios for location and detection. and on the Tiny based Real time operating systems.

Keywords: *Adhoc networks, Location, Detection attacks, Scalability benefits, Tiny 2.OS*

1. INTRODUCTION

Mobile Ad Hoc Networking comprehensively covers all areas of the technology, including protocols and models, with an emphasis on the most current research and development in the rapidly growing area of ad hoc networks. Each node in an ad hoc network is in charge of routing information between its neighbors,[1] thus contributing to and maintaining connectivity of the network. Since ad hoc networks have proven benefits, they are the subject of much current research. Existing routing protocols use the existing information about links in the network to location[12]. There are Three main routing strategies classified as topological based; proactive protocols [**2**] that maintain routing information for each node in the network and stores this information in routing tables, such as Destination-Sequenced Distance Vector (DSDV) , Wireless Routing Protocol (WRP) , and Optimized Link State Routing Protocol (OLSR) [6]. The second type is reactive routing protocols which maintain route on demand, such as Ad hoc On-Demand Distance Vector (AODV) [**6**], Dynamic Source Routing (DSR) [**4**], Temporally Ordered Routing Algorithm (TORA) [4], and Associatively - Based Routing (ABR) [27]. The Third type is hybrid routing protocols are combination of proactive and reactive example is ZRP.Position based routing protocols exploit positional information to direct flooding towards the destination in order . to reduce network overhead and power consumption, Location Aided Routing Protocol (LAR), GRID[1] and Greedy Perimeter Stateless Routing (GPSR) [6] are all examples of position based routing protocols. This may result in worst scaling properties in larger mobile ad hoc networks

Effected for malicious attacks and other cases . It may causes un authenticated address, Daniel of Services (DOS) and Honey pots In this issue detection techniques as well as preventive measures are in urgent need to protect ad hoc network. The mobile ad hoc networks have several

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

salient characteristics,[3] such as Dynamic topologies, Bandwidth constrained, variable capacity links, Energy-constrained operation, Limited physical security [**1**]. Due to these features, mobile ad hoc networks are particularly location is effected for vulnerable to denial of service attacks[4] launched through compromised node

Existising Location based detection issues: Location information is used to reduce the search space for a desired route [13] It is difficult to Location based detection attacks because malicious nodes impersonate legitimate nodes [**4]** The node is unprotected from outside signal(16) *The signature-based IDS* uses pre-known attack scenarios and compare them with incoming packets traffic. (**17)** cause a loop in routing path(44**)** Destination address does not equal destination location with effected by attacksThe idea of locations of its one-hop neighbors is sufficient for a node to determine its local view of the planar graph it should effected for attacks.

In reactive ad hoc networks, techniques such as dynamically limiting the scope of route requests and attempting local repairs to broken routes are often depends upon the attacks[14] in these problems we recovery by using location based detection scheme dynamic efficient location based anomaly detection its defined as technique that quantitatively defines the baseline profile of a normal system activity, where any deviation from the baseline is treated as a possible system anomaly. It is rather easy to detect an attack, the traffic signature of which is identifiable [5] by using misuse based located detection(4).

In this manner location based detection Scheme each mobile node maintains consistent routing information of all the nodes in the network with periodic updates. Whenever a node wants to forward a packet, the route to the respective destination is selected from the available table information and if effected for attacks it shows as periodic intervals to identify the location based route is under by attacks In this paper, we propose a dynamic location based anomaly detection scheme based on a Efficient learning method. The location based MANET hosts are mobile on their own so that the MANET environment is dynamically changing.[13] Our Efficient method is based on a computational stastical theory that shows location based scalable benefits, and two types of attacks in [4] and [18] as a case study that concerns one of the most popular MANET routing protocols, i.e., the ad hoc on-demand distance vector (AODV) [16] The simulation results of the network simulator 2 (ns-2) [17] and implement with Real time operating systems. Location based packets in the whole network will consume a lot of resource of network. To reduce congestion in a network, the protocol adopts some methods. A node can not originate more than ROUTE REQUEST messages per second. After broadcasting a ROUTE REQUEST, a node waits for a ROUTE REPLY. Finally implemented with embedded based operating systems .

2. RELATED WORK

There are a numerous protocols addressing the issue of routing in MANETs, routing becomes a challenge as the nodes are mobile, thus resulting in loss of packets, delay and inefficient communication. Also the problem of insecure wireless links poses a threat to communication in MANETs.In these papers, their research only relate to location and detection Rather than focus on the effect of location based routing and detection attack[4] and [44] in mobile ad hoc networks we have to proposed new schemes of route type $DLRDP_F$ (Dynamic located and Detection Routing Far), if the destination is Remote and $DLRP_L$ (Dynamic located and Detection Routing Local), destination is local[47]. In this issue we related Geographic routing protocol forwards data packets using location information of wireless devices [13] **.** and improve the Scalability analysis for efficient progress. Avoiding loop problems due to mobility and The dynamic training method allow the training data to be updated at regular time of intervals and maintain cooperative localize routing.[4][9] Compared with other neighbor-based routing protocols such as Ad-Hoc On-Demand Distance Vector Routing (AODV) [16], the geographic routing can reduce the communication overhead during route search procedure . in this scheme we have proposed to launch a location in far distance[7] could be effected for detection based attacks and local routing also.

A. Dynamic Secure Schemes for Routing Procedures

Ad hoc routing protocols have been proposed as a technique to enhance the security in MANETs ie(AODV) is to proposed mild implementation of location and detection based routing in care of DLRDPF and DLRPL. The survey conducted by **Abbas Jamalipour and Youngbae Kong** [4] overviewed the various secure routing protocols and pointed out their drawbacks and advantages . They also proposed a location based routing protocol LAR [1][6][44], which prevents the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

compromised nodes from tampering with the uncompromised routes, and the secure efficient ad hoc on demand distance vector (AODV) [20],[11], which is a secure routing protocol, Procedures for update the location Route should be in the Format access of D_F is location information and setup is XD and YD Are connecvity link of nodes and link access of group nodes specify Z(D) is nearest node of Destination t0,t1 are time slots finally Efr is dynamic location far routing. C is defined as dynamic route identification with detection and €f is error occurred in route

Step1 : D_F (X_D,$_{YD}$)…….1

Equation 1 is applicable even with a more efficient route model (e.g., including multi-path and geographical effects), as long as the distance related informations can be isolated empirically.

Step2: **X_D = (i+j+k+….n) nodes……2**

Step3: Y_D= Z(D) nearest node of Destination….3

Step4: to, t1 ……4

Step5: Efr= [DX_D,+D_{YD}]……5

Step6: C=(J avg*(time)+€f….6

Step7: DX_D, +D_{YD})+€f…….7

Total time needed TT= C + Processing time + Network Delay +€f

In a MANET that consists of N nodes, the route discovery using the above principle.

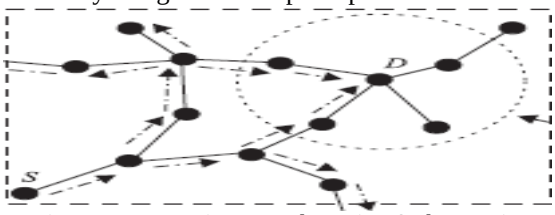


Figure 1 : Dynamic Located Routing And Detection Protocol Far

In dynamic location based routing[46] source part of concern as well as known as the destination and source part send the Packet Request (RREP) to nearest node part of destination .In this approach The Dynamic location Router to route messages while avoiding the dependency [4]of the router on all possible destinations while maintaining its efficiency. Additionally we found attacks also the destination of the route is determined based **on** location[28].

In addition, when the sink moves out of a destination area, it will rebuild a new destination area and broadcast its location information among the entire network. These are the main informations of computing $DLRDP_F$ (Dynamic located and Detection Routing Far), if the destination is Remote and $DLRP_L$ (Dynamic located and Detection Routing Local), destination is local Methods.

I) **Obtain Status of Dynamic located route of Destination**

A node may learn and cache multiple routes to any destination. This support for multiple routes allows the reaction to routing changes to be much more rapid, since a node with multiple routes to a destination can try another cached route if the one it has been using should fail. This caching of [14] multiple routes also avoids the overhead of needing to perform a new Route Discovery each time a route in use breaks.

II) **Send Packet Using DLRDRFL Method**

The source sends the packet to an immediate neighbor node that best improves the distance to D if any attacks have available its shift to malicious detection scheme.

III) **Path Discovery and Evaluation**

The source needs to discover the route to the destination before transmitting any packets the route consists of multiple links and the route is broken if any of the link fails. Thus the route lifetime becomes the minimum lifetime of all links in this route. Every link is formed by two adjacent mobile nodes, which have limited battery energy and can roam freely, and it is broken if any of the two nodes is not alive due to exhaustion of energy or if these two nodes move out of each other's transmission range.

IV) Each node searches for all nearest path of Location Route: • Analysis of the Euclid distance (r) between the node and all other nodes within the network • Compare r with the maximum radio transmission range)[25] of the node.

B)Dynamic located and Detection Routing Local

Procedures for update the location Route should be in the Format access of D_F is location information and X_L and Y_L Are connecvity link of nodes and link access of group nodes specify of iL+jL+kL+….n is nearest node of Destination along with shortest path local access t0,t1 are time slots finally Efr is dynamic location far routing. C is defined as dynamic route identification[3],[4],[6] with detection and €f is error occurred in route.

Step1: D_L (X_L,$_{YL}$)…….8

Equation 1 is applicable even with a more efficient route model (e.g., including multi-path and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

geographical effects), as long as the distance related informations can be isolated empirically

Step2: X_L = (i+j+k+….n) nodes……9
Step3: Y_L =Link Access……. 10
Step4: to,t1…… ……. 11
Step5: Efr= X_L(iL+jL+kL+….n)…….12
Step6:C=Efr+ D_F ($X_{D,YD}$)…… 13

Total time needed TT= Efr + Processing time + Network delay

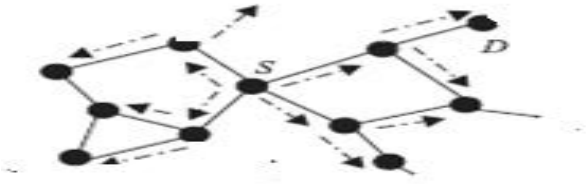


Figure2: (Dynamic Located Routing And Detection Protocol Local),

A)Forward scheme is applicable to establish of this routing

A node announces its presence, position, and velocity to its near local nodes (other nodes within radio range) by broadcasting periodic HELLO packets. Each node maintains a local node' identities and geographic positions. The header of a packet destined for a particular node contains the destination's identity as well as its geographic position. When node needs to forward a packet toward location *P*, the node consults its neighbor table and chooses the neighbor closest to *P*. It then forwards the packet to that neighbor, which itself applies the same forwarding algorithm. The packet stops when it reaches the destination. [13]. In this Scheme of routing could be performed as Source send the packets to node by node which is the nearest path of destination achieved as shortest path algorithm example if node A wants to send packet to E node means it could be performed which is shortest path near to E node and updated to that route automatically and performed.

B) Analysis of Route termination

Similar to Route Drop (R), Route Drop (S), or Route Drop (D), the packet is dropped due to expiration of the time-to-live field (TTL)[20]

C) **Very Normalized Geographical Routing (VNGR)**

- *Selecting location servers:* At any given point of time, for each destination node, the nodes that are located along the north-south direction in the geographic area form the *update quorum* (location servers). [26]
- Each node selected as a location server in the north or south direction broadcasts the update to its one hop neighbors in addition to Multicasting it to the next location server in the update direction
- **Performing queries***:* When a source node initiates a location request for a destination node
- Addition to its own location, each node also includes a list of its neighbors and their locations in the beacon.
-

3. DYNAMIC LOCATION BASED ROUTING AND DETECTION

Several attacks are available we are using Location based routing the possibilities of location based attacks increasesAttacks on location can be further classified as Distance Fraud, Mafia fraud, Terrorist Fraud and Distance Hijacking Attack [18],[34]. Then detection of the presence of a malicious insider node will help a great deal to reduce the possibility of loss of important data. Many techniques have been suggested to detect the presence of malicious nodes in the past; in our work to find attacks in location based routing scheme.

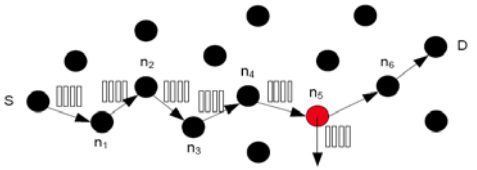


Fig 3: Routing With Detection Of Attacks

Source sending the packets from n1 node to n6 node and it have satisfies the principle of DLRDPF and DLRPL. But node n5 is attacked by malicious attacks Due to the fact that the MANET environment dynamically keeps evolving, envisioning a robust anomaly detection method becomes imperative to thwart the malicious attacks against it. .In this matter propose a new Multiple anomaly-detection scheme(MADS) [48] based on a Efficient dynamic learning process that allows the training data to be updated at particular time intervals and detect the attacks. Our efficient dynamic learning process involves calculating the projection distances based approach.

I. Network Maintance -Based Attack Detection

The various attacks based techniques adopted by network monitoring. Which it is used to detect attacks in network A large server can be set up on a backbone network, to monitor all traffic; or smaller systems can be set up to monitor traffic for a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

particular server, switch, gateway, or router. Attacks on network computer system could be devastating and affect networks and corporate establishments. Detecting network scans[29] is extremely important because such an activity is usually a precursor of the propagation of a worm, and therefore the precursor of possible location based attacks Tseng *et al*[48]. introduced a method that places a network monitor inside the network. In this method, the constantly monitors the packet flow in the network within a certain range to detect any attacks. Enclosed with detectors AODV state transition analyses helped for network Maintance and Monitoring.

II. Efficient Anomaly detection

An extended finite state automaton (EFSA) is similar to a finite-state machine except that transitions and states can carry set of parameters. we distinguish two types of transitions-**an Huang and Wenke Lee[4]** input and output transitions. Input transitions include packet-receiving events and output transitions in this matter additionally found location based attacks detection. In specification-based detection[5], the attacks were detected as deviant packets from the conditions defined by EFSA

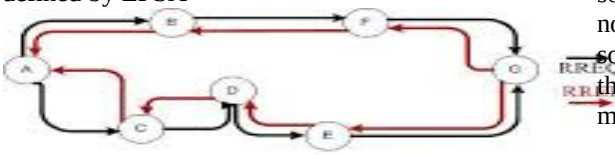


Figure 4 Route-Discovery Process On AODV With Proper Route

AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the adhoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. Sun *et al.* [36] proposed an anomaly detection method in which mobility is considered. This method computes the recent link change rate (*LCR*recent) and can select the training data, the link change rates of which have the smallest Euclidean distance to *LCR*recent. [52]However, the change of network states can be caused not only by mobility. To solve this problem we would find the time intervals of the concern system. The main themes of the progress is

I)Find the correct routes from source to destination

II)Attacks were detected in correct located path by NMEFSA Method.

III) Period Intervals correctly identified

E)ATTACKS ON DLRPL,DLRPF AND AODV PROTOCOLS

I)AODV PREFACE

The AODV routing protocol is a reactive routing protocol; therefore, routes are determined only when needed. Figure 5 shows the message exchanges of the AODV[52],[48] protocol. Hello messages may be used to detect and monitor links to neighbors.[26] If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors

receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the estination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop- byhop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the estimation and can begin sending data. If multiple RREPs

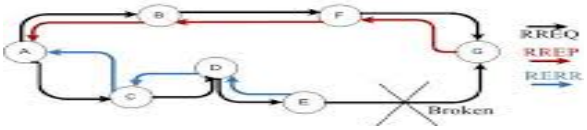


Figure 5 Transferring RERR Messages On AODV.

received by the source, the route with the shortest hop count is chosen If data is _owing and a link break is detected, a Route Error (RERR) is sent to the source of the data in a hop-byhop fashion. As the RERR propagates towards the source, each intermediate node invalidates routes to any unreachable destinations. When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery if necessary[15].

II) DLPF AND DLPL PROTOCOL PREFACE

In these protocol are location based routing protocols and dynamic anomaly detection related with local and far

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig 6 DLRPL effected by attacker

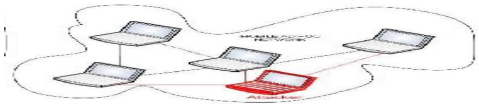


Fig 7 DLRPF Effected by attacker

Mobile Ad hoc Networks is an on demand routing protocol which decreases the search area given by LAR[2]. In LAR the search area is the smallest rectangle containing both sender as well as receiver. DLRPF and DLRPL reducing the routing overheads. Figure 6 and 7 have send the packets from source to destination is under DLRPF and DLRPL scheme [50]and it have detects a disconnection of route, it generates route error (RERR) messages and puts the invalidated address of node *D* into its list and then sends RERR to node *A*. malicious attack have in progress And consideration with geographical routing mechanism. [33],[32] Node which is closest to this line of sight will be chosen as the next intermediate node. As the transmitting node check the distance of every neighboring node from base line and find the closest neighbor for further transmission[12][8]. if malicious attacks have identified in this region using to detection based principles. There are Four phase in this protocols

I)**Route discovery**: All these information is collected by source node before sending the RREQ packet to nearest nodes If destination address is not equal to the neighbor node[24] address then it check the value of TTL, if TTL is less than or equal to zero the node discard the RREQ of the Route Discovery .

II)**Route Reply**: In route reply phase if destination receives the RREQ packet then it check the packet header destination address.

III) **Route maintenance**: In Ad-hoc network there is high mobility of nodes, links between nodes are likely to break. Thus, we need to maintain the routing path.

IV) **Route extension**: In Ad-hoc network there are multiple level route break are available so we need this constraint to performing as packets would no loss.

Procedures for become dynamic status level of this protocol are

1. Combination two protocols DLRPF and DLRPF Come under the attack detection it should have better efficient.
2. Protocols cooperate the path finding and projection angles based attack avoid techniques.

F)Classification of Attacks

We can classify the attacks against DLRPL,DLRPF and AODV[9][52][51]

1) **Route Disruption***:* A malicious node either destroys an existing route or prevents a new route from getting established and performed.

2) **Route Invasion***:* A malicious node adds itself into route between source and destination nodes.

3) **Node Isolation***:* A given node is prevented from communicating with any other nodes. It differs from route disruption in the route disruption is targeting at a route with two given nodes, while node isolation is targeting at all possible routes to or from a given node.

4) **Resource Consumption***:* The communication bandwidth in the network or storage space at individual nodes is consumed.

5) **Location Attacks**: The attack node violates the above rules to exhaust the network resource. Firstly, the attacker selects many IP addresses which are not in the networks if he knows the scope of IP address in the networks. Because no node can answer ROUTE REPLY packets for these ROUTE REQUEST, the reverse route in the route table of node will be conserved for longer. The attacker can select random IP addresses if he cannot know scope of IP address. Secondly, the attacker successively originates mass ROUTE REQUEST messages for these void IP addresses. The attacker tries to send excessive ROUTE REQUEST[47] without considering ROUTE REQUEST_RATELIMIT in per second. The attacker will resend the ROUTE REQUEST packets without waiting for the ROUTE REPLY or round-trip time, if he uses out these IP addresses. The TTL of ROUTE REQUEST is set up to a maximum without using expanding ring search method. In the Location Attacks, the whole network will be full of ROUTE REQUEST packets which the attacker sends A short explanation of the preceding three attacks is given here.

i)Modification of RREP AND ROUTE REQUEST: It have an source node receives multiple RREP messages, it selects the node that has the largest Set dest Dst_ Seq value and accordingly constructs a route. destination IP address and source IP address is spoofed to a randomly selected node is called MRREP 1.

ii)Each node decides whether to forward an RREQ message.

iii) Malicious Stack group attacking : It have an network will become congested with a huge amount of RREQ traffic. And destination IP address and source IP address is spoofed.

Journal of Theoretical and Applied Information Technology
10th October 2013. Vol. 56 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. EFFICIENT LOCATED DYNAMIC ANOMALY DETECTION

The appropriate feature selection for Efficient anomalies detection in routing process is the first and the most important action that must be performed and then delineate the module of the detection scheme [4] based on the enhance projection distance calculation and improve the scability benefits**.** We introduce ELDAD(Efficient located dynamic anomaly detection) method

I) Introduction and meaning of Features

Every node it have an specified of time slots to stack or record of packets in this efficient anomaly detection we introduced time slot $\Delta\tau f$ *and* $\Delta\tau l$ *in the content value of* $\Delta\tau$

$\Delta\tau$ f and $\Delta\tau$l in the combination value of $\Delta\tau$…….. 14

Network state expressed as x= [x1, x2, . . . , xp]$^{T...}$…… 15

P-dimensional vector

xp=(xl+xf) ……. 16

where each feature

xl=(1……..l)……. 17

xf=(1…….f)…….. 18

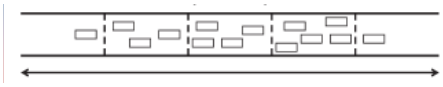
is measured

We calculate the Mean vector from Equation (16) using training data set D of NM time slots

$$x^P = 1/MN \sum_{i=1}^{NM} xiyj \quad \text{…… 19}$$

Packets arrival in the observed network in time slot aspects

Network ($\Delta\tau$ **f +** $\Delta\tau$**l)**



(Δ**T Learn)** time interval

Figure 8: Feature definition

In this figure8 $\Delta\tau$ f + $\Delta\tau$l are far and near packet arrival in the observed network in time slots aspects .

II) **Route finding features**: It have a high adoption based 1.number of received and Forward RREQ messages 2) Number of outbound RREQ and RREP messages;3) Number of received RREP messages (two types).

III)**Route Abnormality Features**

The route abnormality features comprise the following: 1.Number of received RERR messages; 2) number of outbound RERR messages; 3) number of dropped RREQ messages; 4) number of dropped RREP messages.

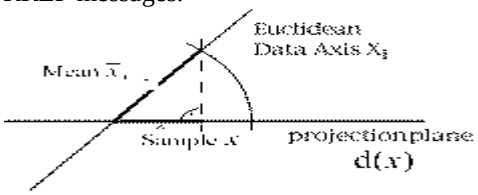


Figure 9 : Distance Of Sample X To The First Principal Element Φi. D(X) Is The Projection Distance

Fig9 states that The same destination IP address and Dst_ Seq are recorded only once for each time slot. The number of dropped RREP messages will increase, and this acts as a sign of abnormality in the network. We applied Normalized Projection angle its used to For the traffic that flow across each node, the network state in time slot i is expressed by three-dimension vector xi = (xi1, xi2, xi3). Here, the groups of normal states are considered to be gathered close in feature space Source part of this concern sending packets to destination .

a) **Detection Module by Normalized Projection Distance for Efficient located dynamic anomaly detection**

The normal and attack states as two different categories can be considered. In this section, we describe the detection module by using the projection distance from figure 9. Let us consider a training data set $\boldsymbol{N} = \{\boldsymbol{x}\}$ collected by each node i $(i = 1, \ldots, N)$, where N is the number of all nodes participating in MANET, and M is attacks the current time interval consists of D_i .

We calculate the Mean vector from Equation (16) using training data set D of NM time slots

$$\overline{x}^P = 1/MN \sum_{i=1}^{NM} xi\ yj \quad \text{……} \quad \textbf{20}$$

When the distance is larger than the threshold (which means it is out of range as normal traffic and effected for route)

$$d(xp; Di) > MI \text{: attack …21}$$

$$d(xp; Di) \leq MI \text{: normal. ……22}$$

Here, when M_i is the maximum value of projection distance for node i in the training data sets $\boldsymbol{D}_i$, the suffix I of M_I is extracted from all the nodes.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

***b)*Proposal of Efficient Dynamic Anomaly Detection**

In this new a learning method that can follow these changes is indispensable. We explain the idea of location schemes with efficient dynamic anomaly detection.

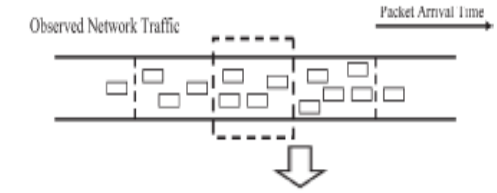
1)Network Traffic and packet arrival time should be analyzed.

2.Location based schemes D_F $(X_{F,YF})$ & D_L $(X_{L,YL})$ compare with aodv.

3. Let T_0 be the current time interval, and let T_1 be the first time interval. By using the data collected in T_1, initially, the

first principal element is calculated for above schemes. If state to is normal then the corresponding data set will be used as the efficient training data set.

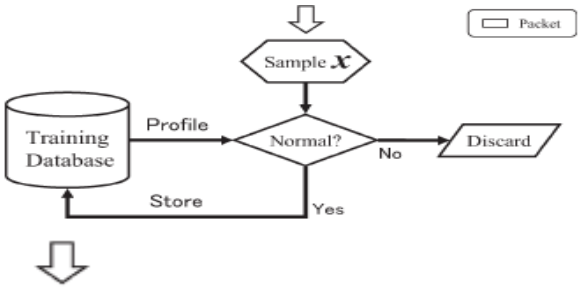
4. Otherwise, it will be treated as the data including attack, of location schemes and it will consequently be discarded with local and far route. The following diagram is mentioned above the statements related



Location Dlrpf and Dlrpf Compare with Aodv

I) D_F $(X_{F,YF})$

II) D_L $(X_{L,YL})$



Scalability benefits implementation with Tiny OS

Figure 10: Flow Chart Of The Proposed Method For Learning And Evaluation

5. PERFORMANCE EVALUATION

The performance of the location based detection discussed in this paper is evaluated through simulation by NS 2[53] In the evaluation, the aforementioned location based detections are presented for comparison together with the original AODV. We have implemented Location attack in a network simulator and conducted a series of experiments to evaluate its effectiveness. The wireless networks simulation software, from Network Simulator ns-2 is used finally implement with tiny based OS. In this paper we comparison the following parameters i)Packet delivery ratio ii)Avarge packet Delay iii) iii) Packet loss iv) QOS[31]

I)Simulation Setup

The experiments were carried out by using ns-2 (version 2.34)

We assume that the simulation network being used is in a place where various events in a MANET .and following table is Simulation setup for our proposed work.

Table 1: Simulation setup1

S.NO	ITEMS	DESCRIPITION
1	Simulator	NS-2
2	Simulation time	10 000 s,
3	Simulation area	1000 m × 1000 m
4	Number of MNs	50
5	Transmission range	250m
6	Randomly executed	2500 to 5000 s.
7	Bit rate	512 B.
8	Pause time	10, 50, 100, 200, and 500 s,
9	Model	Random way point (RWP)
10	MAC Protocol	IEEE 802.11 DCF
11	Routing Protocols	AODV, LAR

IA. Packet Delivery Ratio

Packet delivery ratio is defined as the ratio of data packets received by the destinations to those generated by the sources. This performance metric gives us an idea of how well the protocol is performing in terms of packet delivery at different speeds using different traffic models.[16]

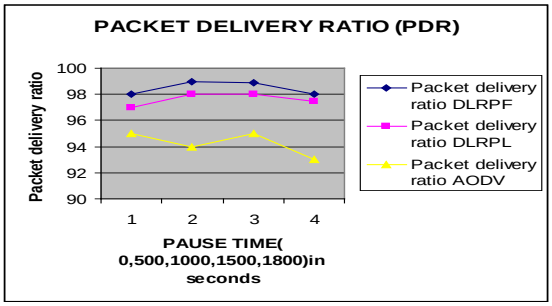


Figure 11: Packet Delivery Ratio

In this figure 11 our simulation results are shown that location based detection (DLRPF and DLRPL) packet delivery ratio is higher than AODV

Journal of Theoretical and Applied Information Technology
10th October 2013. Vol. 56 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Packet Delivery Ratio

S.NO	DLRPF	DLRPL	AODV
PDR(%)	98	97.5	95

The table 2 comparison proves that DLRPF and DLRPL based detection improves **2.75 %** higher than AODV. We observe the impact of pause time on packet delivery ratio. The results show that the packet delivery ratio is maximum when the pause time is equal to the simulation time (i.e. when the nodes in the network are static). The DLRPF and DLRPL shows the best performance with 97.5% packet delivery at 1800s pause time.

IB.Avarge Packet delay

The average end-to-end delay of data packets is the interval between the data packet generation time[43] and the time when the last bit arrives at the destination[16][30].

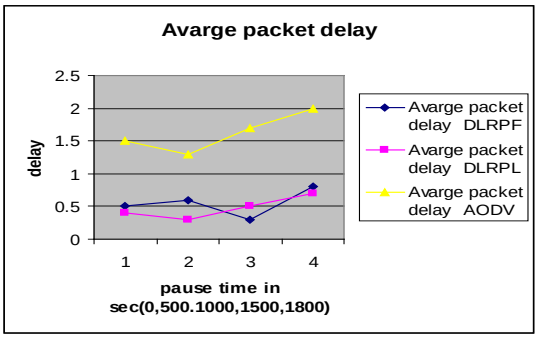


Figure 12: Avarge Packet Delay

As shown in Figure: 12**,** this simulation experiment showed us that AODV is are having higher delays than others**,**

Table 3: Avarge Packet Delay

S.NO	DLRPF	DLRPL	AODV
Avarge packetd elay	0.55	0.475	1.175

This analysis exclusively deals with the network speed and communication effectiveness. Higher the delay, lower is the speed and possibility of packet drop and so needs the fault tolerance approach of selecting these protocols.

IC. Packet loss

Packet loss is measured at all mobile hosts. Every host monitors the networking layer and the MAC layer for all kinds of packet losses. The network configuration for the experiments is a 1000m x l000m square field with 30 hosts

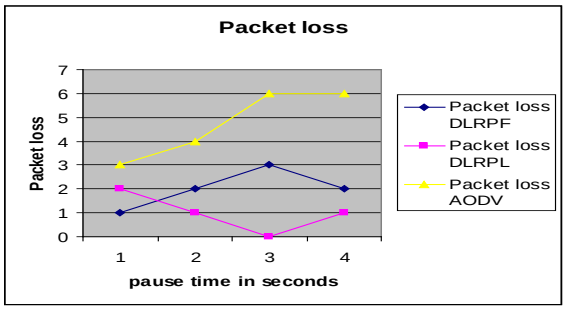


Figure 13: Packet Loss

In this figure 13 our simulation results are shown that location based detection (DLRPF and DLRPL) packet loss is very adopted in AODV and low in DLRDF and DLRPL scheme.

Table 4: Packet Loss

S.NO	DLRPF	DLRPL	AODV
Packet loss	2	1	4.7

The table 2 comparison proves that DLRPF and DLRPL based detection improves **3.2 %** higher than AODV. We observe the impact of pause time on packet loss . Each data point in the result figures represents which are randomly generated with the same parameters.

ID. QOS(Quality Of services)

QoS is a set of service requirements to be met by the network while transporting a flow. A flow is a packet stream from a source to a destination (unicast or multicast) with an associated (QoS)[31].

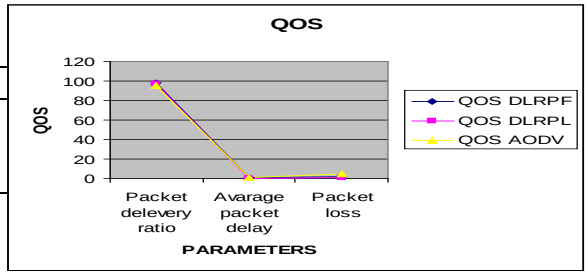


Figure 14: Quality Of Services

6. EXPERIMENTAL RESULTS

In figure 15 a shows the creation of clusters with 50 mobile nodes as it is shown in the NAM console which is a built-in program in NS-2-allinone package[53] after the end of the simulation process. In this figure 15 A deals with experimental results shown that location based detection and how malicious attacks and efficient anomaly detection is efficiently detected and packets are discarded and dropped of RRER messages in this manner our results shown that efficient based location and detection

Journal of Theoretical and Applied Information Technology
10th October 2013. Vol. 56 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

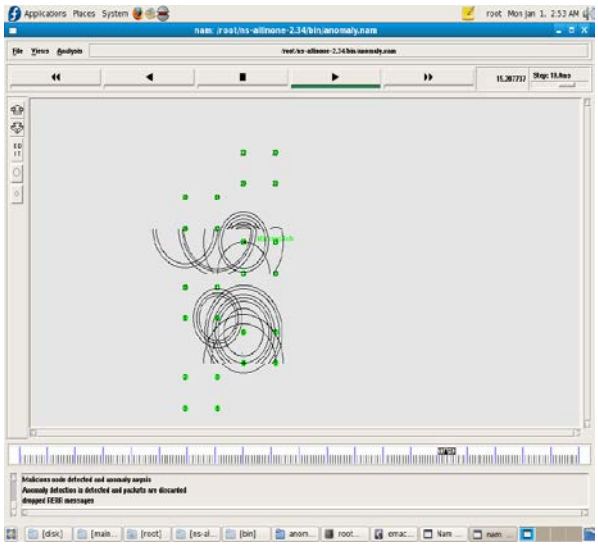


Figure15(A) Location And Detection Based Manets

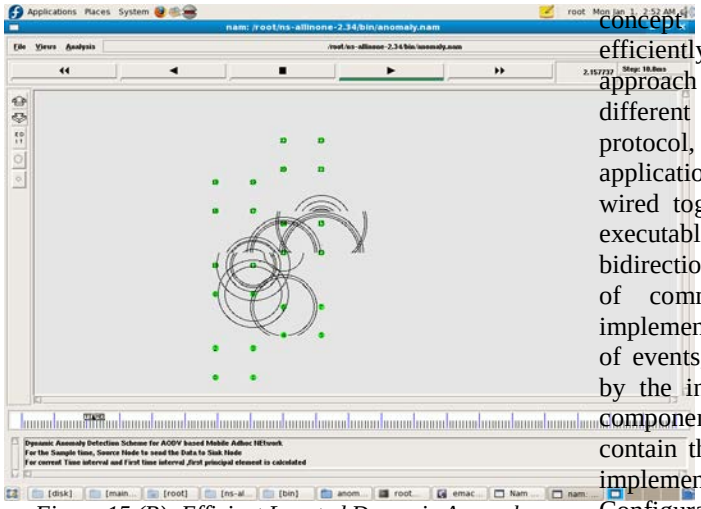


Figure 15 (B): Efficient Located Dynamic Anomaly Detection

In figure 15b states that Efficient Located dynamic Anomaly Detection for the sample access source node send packets to sink node and for current time interval and location based first element is calculated.

7. IMPLEMENTATION WITH TINY BASED OPERATING SYSTEMS

TinyOS [17]is an embedded operating system written in the nesC programming language as a set of cooperating tasks and processes. It is intended to be incorporated into smartdust. TinyOS started as a collaboration between the University of California, Berkeley in co-operation with Intel Research and Crossbow Technology,[21],[22],[23] and has since grown to be an international consortium, the TinyOS Alliance. In this scenario we updated our scalability results like packet delivery ratio, Avarge delay, packet loss an in tiny based operating systems. TinyOS is a set of NesC components that can be understood as a program-library for own applications, which have to be implemented as NesC components as well. The components of TinyOS[45] offer various functions ranging from abstraction-layers to the un- derlying hardware over a scheduler to automatic routing mechanisms. TinyOS and custom components can be used by "wiring" them to own applications, thus allowing the NesC compiler [49]to effectively determine the necessary dependencies. Most of NesC's components are optional to use, some are mandatory (such as the "MainC" component, which initializes all custom software).[39] TinyOS is defacto OS for motes, used in almost all the popular motes(micaz, Intel, etc) available in market. i)**Concept**s: TinyOS uses a unique concept of components and interfaces, for efficiently modularizing the programming. This approach gives a lot of edibility to switch between different components such as different network protocol, keeping the main code intact. TinyOS applications con sist of one or more components wired together to form one complete application executable. Components uses and provide bidirectional interfaces. An interface specify a set of commands, which are functions to be implemented by the interface's provider, and a set of events, which are functions to be implemented by the interface's user. There are two types of components: modules and configurations. Modules contain the actual program code that provides the implementation of one or more interfaces. Configurations are used to connect or wire the interfaces used in modules to the interfaces provided by other modules.[42] Every application is described by a top-level configuration that wires together the components inside. TinyOS have two running threads performing all the required operations. One thread is used to execute tasks and other is used to execute hardware events handlers[24]. Tasks are functions that perform main computation, and are scheduled by OS.

Figure 16 Tiny OS Node

In this tiny os we are used implement our scalability results with high efficient oriented .we

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

can define scalability in Tiny Opearting systems is more detailed and efficient statement.

i)Scalability: The simulator must be able to handle large networks of thousands of nodes in a wide range of configurations.[21] The largest TinyOS network that has ever been deployed was approximately 850 nodes; but our approach we taken as only 50 to 100 nodes of the simulator

```
interface StdControl { // booting management
  command result init();
  command result start();
  command result stop();
}
interface ADC and Timer { // data collection
  command result getData() &result_t0&t1 get data ();
  command result getContinuousData() &result_t0&t1;
  getContinuousData();
  event result_t dataReady(uint16_t data);
}
interface packet delivery { // networking
  command result send(uint16_t addr, uint8_t len, TOS_MsgPtr msg);
  event result_t 2packet delivery sendDone(TOS_MsgPtr msg, result_t2
success);
}
interface average delay { // networking
  command result_t3 send(uint16_t addr, uint8_t len, TOS_MsgPtr
msg);
  event result_t3 average delay Done(TOS_MsgPtr msg, result_t
success);
}
interface scheduler and task { // networking
  command result_t4 send(uint16_t addr, uint8_t len, TOS_MsgPtr
msg);
  event result_t4 interface scheduler and task Done(TOS_MsgPtr msg,
result_t success);
}
Send and receive packets interface Send and  ReceiveMsg { //
networking
  event TOS_MsgPtr  sender & receive(TOS_MsgPtr mn );
}
```

ii) **Tiny OS interfaces with scalability benefits and Task**

TOSSIM [36]. Bit-level discrete event simulator and emulator of TinyOS[35], i.e. for each transmitted or received bit a event is generated instead of one per packet. This is possible because of the reduced data rate (around 40 kbps) of the wireless interface. TOSSIM simulates the execution of nesC code on a TinyOS/MICA, allowing emulation of actual hardware by mapping hardware interruptions to discrete events. A simulated radio model is also provided. Emulated hardware components are compiled together with real TinyOS components using the nesC compiler. Thus, an executable with real TinyOS applications over a simulated physical layer is obtained. Additionally, there are also several communication services that provide a way to feed data from external sources. The result is a high fidelity simulator and emulator of a network of TinyOS/Motes.

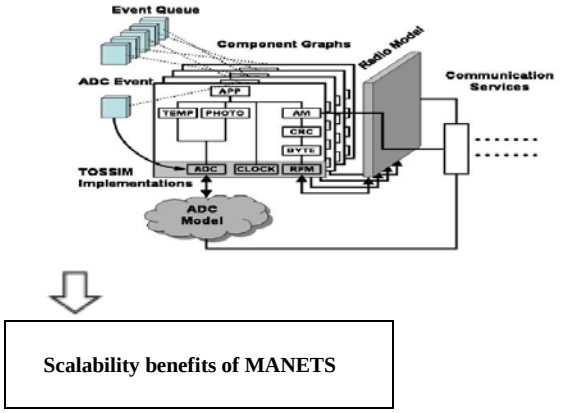


Figure 17: TOSSIM Architecture: Frames, Events, Models, Components, And Services

TOSSIM is designed considering four requirements, which are essential for efficient TinyOS simulation environment. First, scalability: The simulator must be able to handle large scale sensor networks. Secondly, completeness: The simulator must cover as many system interactions as possible. Third, fidelity: The simulator must capture the network behavior accurately. Fourth, bridging: The simulator must bridge the test implementation and the real implementation. A TinyOS program is composed of components, which are independent computational entities. Components have three computational concepts: commands, events, and tasks.

iii)TOSSIM with Scalability approaches of manet

In our proposed approach we enhance the scalability benefits like packet delivery ratio, average delay and packet loss involved in tiny based Operating systems [36],[37]and some enhanced features are base supporting[40][41] for proposed work .i) Injecting packets into the network dynamically ii) Packets can be scheduled to arrive at any time iii) Evaluating the results of TOSSIM 2.xwith mobility extension for mobile wireless nodes iv) TOSSIM can simulate large-scale networks up to thousands of nodes v) TOSSIM[19] allows developers to test and verify the code that will run on hardware motes.

a)Procedures

1. Predefined topology file is loaded to the nodes
2. Noise traces are assigned to the nodes.
3. Nodes are booted at particular times
4. Packets are injected.
5. Topology definition can be in different formats and can be stored in text files.

iv) **Basic Instrumentation of Tiny 2.0**

We use Tiny 2.0 OS [38] in this study as the experimental platform. It is widely available and

Journal of Theoretical and Applied Information Technology
10th October 2013. Vol. 56 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

has been used in wire- less network research. Each Mica mote has a 4MHz Atmel processor(128K EEPROM and 4KB RAM), 512KB flash memory, and an ASK (amplitude shift keying) low power 433 MHz radio [39]. To simplify experimental control and data collection, we used or wrote several pieces of instrumentation and experimentation software. The first such software module is a simple traffic generator. Driven by a clock which has an
accuracy of one millisecond, the traffic generator repeatedly sends out packets tagged with a sequence number. The exact periodicity depends on the experiment[41],[43]. A second module allows us to upload experimental parameters (such as packet delivery ratio, Avarge delay and Packet loss experiment duration)[16][45] wirelessly to all motes within the radio range.

8. PERFORMANCE RESULTS

In this section, we compare the performance (Packet delivery ratio, Average delay, and packet loss) of our Protocols (DLRPF + DLRPL AND AODV) with respect to TinyOS 2.0.

a) **Packet Delivery ratio**: In this proposed approach packet delivery ratio is improved and Every node knows how many packets it has received. These numbers can be sent to UART or be piggybacked in the wireless packets[43]. Then, with these numbers known, the packet delivery ratio is

Number of packets received / number of packets sent

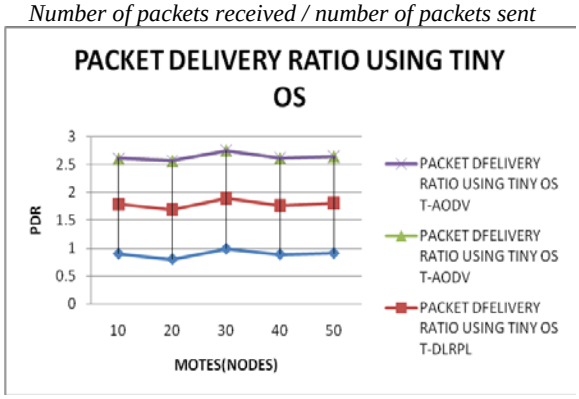


Figure: Packet Delivery Ratio Using Tiny 2.0 OS

b)Average Delay: In this proposed approach average delay are monitored and its reduced Its defined for a successfully as the time time interval from time of the packet is at the head of line of the queue ready to be transmitted until acknowledgement for this packet is received[30].

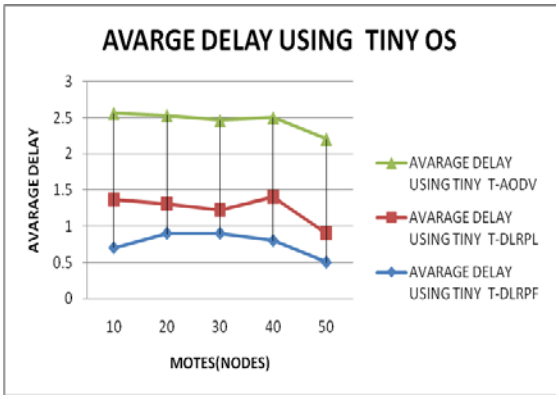


Figure : Avarge delay using Tiny 2.0 os

c)**Packet loss**: To understand the causes of packet loss, we take a close look into the work flow on a node that forwards a packet and transmission timeout is common and accounts for a large portion of packet drops in this proposed one packet loss is reduced to compare other one

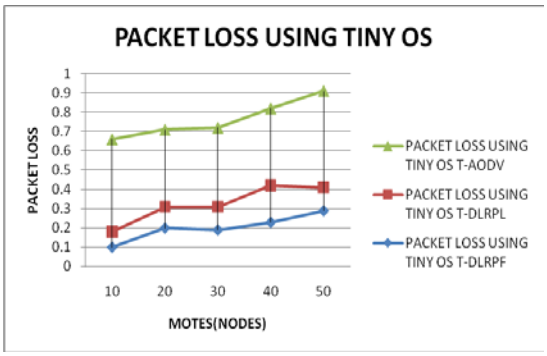


Figure: Packet Loss Using 2.0 Tiny OS

d)Results: We carried out experiments on two platforms each time increasing the rate of packets sent, and measuring the effective packet delivery ratio and Avarge packet delay and packet loss. For better comparison, we ran the same experiments on the TinyOS version 2.0

Table5: Comparison Of Results

Approach	Packet delivery ratio	Average packet delay	Packet loss
DLRPF	0.90	0.76	0.22
DLRPL	0.89	0.476	0.124
AODV	0.84	1.214	0.438

e) Experiments: Its used in network development fields like i)large scale networks ii) small scale networks **[50]**

9: CONCLUSION

In this paper we introduced new concept of location based detection schemes like (DLRPF and DLRPL

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

) and compared with AODV. Here, we find out the performance on the basis of packet delivery ratio, Average packet delay and packet loss and its simulated by NS2. Then we enhance these results through Tiny based operating systems versions 2. It is also envisaged to implement the scalability benefits of manets and functionalities to support Networking and embedded based communication.

REFERENCES

[1] Young-Bae Ko and Nitin H. Vaidya , Location-Aided Routing (LAR) in mobile ad hoc networks: Wireless Networks 2002.

[2] Khalid Kaabneh, Azmi Halasa , An Effective Location-Based Power Conservation Scheme for Mobile Ad Hoc Networks: American Journal of Applied Sciences 6 (9): 1708-1713, 2009

[3] Tracy Camp, Jeff Boleng, Performance Comparison of Two Location Based Routing Protocols for Ad Hoc Networks : Department of Math. and Computer SciencesColorado School of MinesGolden, CO 80401.

[4] Hidehisa Nakayama, Yoshiaki Nemoto, A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks : IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 5, JUNE 2009.

[5] Haitao Liu Rajiv Gupta, Temporal Analysis of Routing Activity for Anomaly Detection in Ad hoc Networks: Department of Computer Science The University of Arizona Tucson, Arizona 85721.2006

[6] Ljubica Blazevic, Member, IEEE, A Location-Based Routing Method for Mobile Ad Hoc Networks: IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 3, NO. 4, OCTOBER-DECEMBER 2004.

[7] Nilesh P. Bobade, Nitiket N. Mhala, Performance Evaluation of Ad Hoc On Demand Distance Vector in MANETs with varying Network Size using NS-2 Simulation : (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 08, 2010.

[8] S. Mangai and A.Tamilarasi, An Improved Location aided Cluster Based Routing Protocol with Intrusion Detection System in Mobile Ad Hoc networks : Journal of Computer Science 7 (4): 505-511, 2011.

[9] Amit Kumar Saha ,Khoa Anh To , Physical Implementation and Evaluation of Ad Hoc Network Routing Protocols using Unmodified Simulation Models: *SIGCOMM ASIA WORKSHOP*, April 12.14, 2005, Beijing, China.

[10] Haiying Shen, and Lianyu Zhao , ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs: IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, JUNE 2013.

[11] Lidong Zhou , Zygmunt J. Haas, Securing Ad Hoc Networks: epartment of Computer Science , Cornell University Ithaca, IEEE network, special issue on network security, November/December, 1999 [12] RAM RAMANATHAN AND JASON REDI, A BRIEF OVERVIEW OF AD Hoc NETWORKS: CHALLENGES AND DIRECTIONS: IEEE Communications Magazine 50th Anniversary Commemorative Issue/May 2002.

[13] Saumitra M. Das, Himabindu Pucha and Y. Charlie Hu,: Performance Comparison of Scalable Location Services for Geographic Ad Hoc Routing: IEEE INFOCOM 2005.

[14] Yi-an Huang and Wenke Lee,Attack Analysis and Detection for Ad Hoc Routing Protocols, : College of Computing Georgia Institute of Technology 801 Atlantic Dr. Atlanta, GA, USA 30332.

[15] M.L Sharma, Noor Fatima Rizvi , Performance Evaluation of MANET Routing Protocols under CBR and FTP traffic classes: Int. J. Comp. Tech. Appl., Vol 2 (3), 392-400.

[16] Pankaj Rohal1, Ruchika Dahiya, Study and Analysis of Throughput, Delay and Packet Delivery Ratio in MANET for Topology Based Routing Protocols (AODV, DSR and DSDV): INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY , Vol. 1, Issue II, Mar. 2013.

[17] Paolo Pagano, Prashant Batra, and Giuseppe Lipari, A Framework for Modeling Operating System Mechanisms in the Simulation of Network Protocols for Real-Time Distributed Systems :IEEE 2007

[18] Arun Kumar. R, Abhishek M, A Review on Intrusion Detection Systems in MANET: International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013.

[19] Leonardo B. Oliveira , Michael Scott, TinyPBC: Pairings for Authenticated Identity-Based Non-Interactive Key Distribution in Sensor Networks: Supported by CAPES (BrazilianMinistry of Education)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

grant 4630/06-8 and FAPESP grant 2005/00557-9

[20] Guojun Wang, Tian Wang, Weijia Jia, Local Update-Based Routing Protocol in Wireless Sensor Networks with Mobile Sinks: IEEE Communications Society subject matter experts for publication in the ICC 2007 proceedings

[21] Philip Levis, Nelson Lee, TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications: *SenSys'03*, November 5–7, 2003, Los Angeles, California, USA.

[22] Benedikt Driessen, Efficient Embedded Implementations of Security Solutions for ad-hoc Networks: Ruhr-University BochumSeptember, 2007.

[23] Leonardo B. Oliveira, Diego Aranha, TinyTate:Identity-Based Encryption for Sensor Networks: Supported by The State of S˜ao Paulo Research Foundation under grant 2005.

[24] XUANLONG NGUYEN, MICHAEL I. JORDAN, A Kernel-Based Learning Approach to Ad Hoc Sensor Network Localization. ACM Transactions on Sensor Networks, Vol. 1, No. 1, August 2005.

[25] Simardeep Kaur, Anuj K. Gupta, Position Based Routing in Mobile Ad-HocNetworks: An Overview: IJCST Vol. 3, Iss ue 4, Oct - Dec 2012.

[26] Mehran Abolhasan, Tadeusz A. LPAR: an adaptive routing strategy for MANETs:Jornal of telecommunication and technology 2003.

[27] V.N.Sastry and P.Supraja , Location-Based Associativity Routing for MANET: 2005 IEEE.

[28] Mr. Yahia Jazyah and Dr. Martin Hope: A New Routing Protocol for MANET: 2009 PGNet

[29] Shilpa Jaiswal, Sumeet Agrawal, A Novel Paradigm: Detection & Prevention of Wormhole Attack in Mobile Ad Hoc Networks: International Journal of Engineering Trends and Technology-Volume3Issue5- 2012.

[30]A.Boomarani Malany , V.R.Sarma Dhulipala, Throughput and Delay Comparison of MANET Routing Protocols: Int. J. Open Problems Compt. Math., Vol. 2, No. 3, September 2009.

[31] Masoumeh Karimi, Quality of Service (QoS) Provisioning in Mobile Ad-Hoc Networks (MANETs): Technological University of American (TUA)USA.

[32] Ramakrishna M ,DBR: Distance Based Routing Protocol for VANETs: International Journal of Information and Electronics Engineering, Vol. 2, No. 2, March 2012.

[33] Sonam Jain, Sandeep Sahu, Topology vs Position based Routing Protocols in Mobile Ad hoc Networks: A Survey: International Journal of Engineering Research & Technology (IJERT): Vol. 1 Issue 3, May – 2012.

[34] Indu Kashyap & R.K. Rathy, An Efficient Location based Reactive Multi-path Routing Protocol for MANET: International Journal of Computer ApplicationsFebruary 2012.

[35] Kayhan Erciyes, Orhan Dagdeviren**,** Modeling and Simulation of Mobile Ad hoc Networks: Modeling and Simulation of Mobile Ad hoc Networks

[36] Werner Backes and Jared Cordasco, MoteAODV – An AODV Implementation for TinyOS 2.0: IFIP International Federation for Information Processing 2010

[37] Paolo Pagano, Mangesh Chitnis, ERIKA and OpenZB: an implementation for realtime wireless networking: *SAC'09* March 812,
2009, Honolulu, Hawaii, U.S.A.

[38] Tonio Gsell , TinyOS Instrumentation: Fall Term 2007.

[39] www.tinyos.com

[40] www.tossim.com

[41] Philip Levis†, Sam Madden, The Emergence of Networking Abstractions and Techniques in TinyOS. r

[42] Philip Levis†‡, Nelson Lee†, Matt Welsh], and David Culler, TOSSIM: Accurate and Scalable Simulation of Entire TinyOS Applications.

[43] Jerry Zhao, Ramesh Govindan , Understanding Packet Delivery Performance In Dense Wireless Networks.

[44] Gagandeep, Aashima, Pawan Kumar, Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review: International Journal of Engineering and Advanced Technology (IJEAT) June 2012.

[45] Prof. Dr. Roger Wattenhofer, Philipp Sommer, Johannes Schneider, Ad Hoc And Sensor Networks TinyOS Lab Exercise, December 18, 2009.

[46] Hadi Noureddine, Hamed. Al-Raweshidy, Qiang. Ni , FORTEL: Forecasting Routing Technique using Location information for Mobile Ad hoc Networks:IEEE Symposiums 2010.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[47] Chen Junyan, Liu Cheng, Xiong Huagang, Chen Youzi , An Efficient Location-Aided Link State Routing Protocol for MANETs: ©2010 IEEE.

[48] Dr.R.Satyaprasad, A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks: *(IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 2, No.3, March 2011*

[49]www. tiny.org

[50] Amjad Osmani , Abolfazl T.Haghighat , Shirin Khezri , Performance improvement of two scalable location services in MANET: 2010 International Conference on Computational Intelligence and Communication Networks. [51] V. Zangeneh, S. Mohammadi, New Multipath Node-Disjoint Routing Based on AODV Protocol: World Academy of Science, Engineering and Technology 52 2011.

[52] YU-DOO KIM1,*, IL-YOUNG MOON1, SUNG-JOON CHO, A COMPARISON OF IMPROVED AODV ROUTING PROTOCOL BASED ON IEEE 802.11 AND IEEE 802.15.4: Journal of Engineering Science and Technology Vol. 4, No. 2 (2009)

[53]www.ns2.com

[54]www.tossim.org