PROTECTED RELIABLE ROUTING FOR MANET USING BEES ALGORITHM

Dr. S. Ramesh
Associate Professor
Department of Information Technology
Sethu Institute of Technology, Virudhunagar, INDIA
E-mail: itz_ramesh87@yahoo.com

Abstract-To maintain the information that is required to properly route the traffic is a key issue in MANET. Among the available routing techniques trust based routing techniques seem to be better. In trust based routing technique, security threats that occur during routing as well as network initialization is a left out problem. In this proposed scheme Protected Reliable Routing (PRR) ensures security in all expected parameters. Node formation is done by two way secured encrypted techniques which double checks for false node by ECDSA in case of multicast communication and HMAC embedded with MD5 in case of unicast communication and then allocates IP for new node. In routing to avoid delay,Bees algorithm is being used to choose the optimized path from source to sink based on the higher objective value and then source node gathers recommendation from neighbour node, analyse them by calculating confidence value and response value. The result thus obtained is again handpicked based on high communication rate to have a better knowledge about destination. Efficiency of PRR is shown by comparing it with existing techniques in terms of overhead, packet delivery ratio, packet loss and throughput. Analysis graph highlights that PRR is highly optimized with better results.

Keywords: MANET, Trust based routing, bees algorithm, security attacks

1. INTRODUCTION

Mobile Adhoc Network is an infrastructure less networks that is connected wirelessly. Nodes in this type of network act themselves as a router as a result of which there is no need of central administrator [1]. Topology of MANET is sensitive to time and they have minimum communication range that leads to multihop communication. To continuously maintain the information to properly route the traffic is always an open challenge in MANET. Air pollution monitoring, military purposes VANET, SPANs, industry sector, Bluetooth are few applications of MANET. Because of its widespread applications security in MANET has become mandatory. Though there are many successful routing techniques available in networking they are not fit enough to satisfy MANET's behavior. Existing techniques like AODV with reputation, TSDRP, S-DSR, HAODV, grade trust technique provides routing in MANET but security is not focused on the better way. Researches continuously try to solve this issue in MANET; as a result trust based routing techniques are found to be a solution for routing in MANET.

Trust is a general opinion of a node about its neighbor node. Trust managing should be done with keen case thus they satisfy all predefined properties they have follows. Firstly trust is dynamic (i.e.) it depend on the temporary and local data which are subject to change any time due to mobile nature of nodes in MANET. Secondly they are subjective; not all nodes have same trust values for a particular node which purely depend on the individual performance of the evaluated node with evaluating node. Thirdly trust is not necessarily transitive if node A trusts node B and node B trusts node C it doesn't mean that A trusts C. Fourth trust is asymmetric (i.e.) trust is not essentially reciprocal. Finally trust is context dependent; the trust value depends on the content of routing. As MANET is a dynamic network, trust based routing techniques enquire about the destination node before dropping data into destination. Routing process is proceeded or dropped based on enquiry result.

Recommendation based trust model with an effective defence scheme is a technique that provides secure routing in MANET with a help of cluster manager algorithm used for filtering the recommendations as trustworthy and untrustworthy to avoid wrong recommendations but it failed to deal with the possibility of attacks during network formation.

In this paper the proposed scheme is PRR, where during network formation the dual check parameters in the gate of the network is done by ECDSA scheme in case of multi cast and HMAC embedded with the MD5 in case of unicast. Further during data transfer initially the optimized path is chosen by Bees algorithm and then the path is analyzed by neighbor recommendations. These recommendations are filtered by calculating confidence value and response value for each received recommendations followed by communication path preference and finally the data is delivered to the destination.

The paper is organized as follows. Section II covers the related work, Section III describes the proposed technique in detail. Simulation results and its performance evaluation are depicted in section IV.

2.RELATED WORK

Mobile Adhoc network is a trending network with widespread applications. Routing data packets from one node to another is an onerous task to accomplish. This section provides a summary of schemes that are compatible with Mobile Adhoc Networks.

A.Addressing techniques

Filter based addressing protocol (FAP) works on the basis of distributed address data base stored in the filter which helps to avoid address overhead[2]. ID based dynamic algorithm allocates new IP from every host based on the trusted third party so that it would be possible to stay away from security threats that may occur during dynamic configuration[3]. ID based secured distributed dynamic IP configuration is an address allocating scheme where the node is able to assign address to its sub nodes without broadcasting the information to the entire network without the help of the trusted third party[4]. Secure and distributed robust address configuration is an addressing scheme where the nodes are checked dually before joining into the network[5]. The encryption techniques used for dual check at the gate of the network could be modified to get better efficiency.All these techniques discussed so for are dependent on DAD mechanism which may cause broadcast storm problem.

B.Bee routing techniques

Bees' algorithm, a bio inspired optimization algorithm is described along with its various versions and it was proved to be efficient[6]. Bee colony routing has been used to implement routing in ICMANET which is a disconnected mobile Adhoc network. This scheme ensures reliable data transfer based on the objective value[7]. BeeAdhocconf is an address allocation scheme for MANET using bees logic, which is proved to be efficient even for large scale MANET at low complexity, overhead and latency[8]. A routing scheme by combining bee routing protocol with LoDis to transfer data in the MANET has been described to get optimal result in data delivery[9]. AES is used here to ensure efficiency of routing to avoid attacks in the network.

C.Trust based routing techniques in MANET

Grade trust technique removes the extreme routing calculation and diminishes communication overhead [10]. They divide the network entity into three sets namely trusted friends, friends and possible friends. So that it could reduce efficient route selection and packet delivery. HAODV is a trust based routing protocol where honest values based on hop will be incremented and decremented with respect to phases and the honest value based on the trust is used for path trust calculation[11]. Modifying the route

reply packet's structure is a kind of routing protocol which includes the battery power of the node and the trust value[12]. Since the protocol keeps limited number of nodes in the path it is inefficient in case of large MANET. Trust based security model is a technique which gains the trustworthiness of the other nodes and helps them to ensure the security decisions[13]. Trust information table contains trustee value, referential value and combined trust value. Light weight trust based routing protocol is a intrusion detection system for evaluating trust value with low resource[14]. This could be amalgamated with any kind of AODV protocol.

Fuzzy trusted dynamic source routing is a reactive routing protocol based on DSR. A trust model based on the fuzzy recommendation similarity (RFSTrust) has been proposed for MANET environment in order to secure the network from selfish nodes [15]. This is to improve the performance of MANETs routing schemes and to assist node behaviour detection. The protocol works on the basis of fuzzy dynamic programming theory which inputs a filter trust routing algorithm. Recommendation based trust model with an effective defence scheme is a trust node where routing is done on the basis of recommendations from neighbour which is filtered as trustworthy and untrustworthy by cluster manager algorithm[16]. It filters them by confidence value deviation value and closeness centrality value.

Since MANET is dynamic in topology node initialization must be focused more to illustrate secure data routing in the network. Formation of network with one or more gateways and maintaining secure data transfer across the network is a mandatory one.

3. PROPOSED MODEL

The proposed technique solves the issue with attacks expected during node initialization as well as routing process. The protocol prevents the network from attacks during network formation, bee routing protocol is being used to pick optimized path from source and destination which provides fast and secure data delivery during routing process.

Protected Reliable Routing is a proposed technique comprises of two components namely node initialization component and routing component. Node initialization component explains the steps for a new node to join the MANET and routing component defines the procedure to route the data in MANET using PRR scheme.

A.Node initialization Component

If a new node N_n has to join a MANET within its radio range, it initially sends requests to all the nodes nearby On receiving the request from a new node, the host node ((i.e,) the node which is already a member of MANET) checks whether the request is from authenticated node or a malicious node. (Multicast authentication). This process is done by validating the node ID and the signature sent by new node. Once the request is validated the host node sends a reply to the new node.

On the other hand, the new node receives one or more reply messages, whose authentication is also checked by new node (Unicast authentication)[24]. This cross check is a process of validating IP address, host ID and the message tag sent by the host node. Once new node verifies the response messages, it selects one IP based on first come first served and rejects the rest of the IP offered to them. New node sends accept message to the host node of the chosen IP which is again authenticated as said before. On receiving accept message from new node the host node sends acknowledgment on account of which the new node is joined to the network. The node joins the network with the IP address provided earlier by the host.(Algorithm 1)

Multicast authentication

Here the data to be sent with the node ID of the new node is generated using MD5. With the help of the private key and the hash value, the generated signature is identified using ECDSA algorithm[25]. The node ID appended with signature is been sent to the hosts nearby.

In authentication part, the host receives request from the new node, and it generates hash function separately for the node ID and then the signature is decrypted using the sender's public key and the verification algorithm. The request is valid only if the hash values' matches (the one that is generated by host node from new node ID and the decrypted hash value).

Unicast authentication

Unicast authentication is done by embedding HMAC along with MD5. The data to be authenticated (i.e,) the new IP address, host ID are initially processed by MD5 to produce a 128 bit hash value. The hash value thus obtained is then processed to the HMAC code to get a message tag. The response message is a combination of this message tag new IP address to be assigned to the new node and the host's ID.

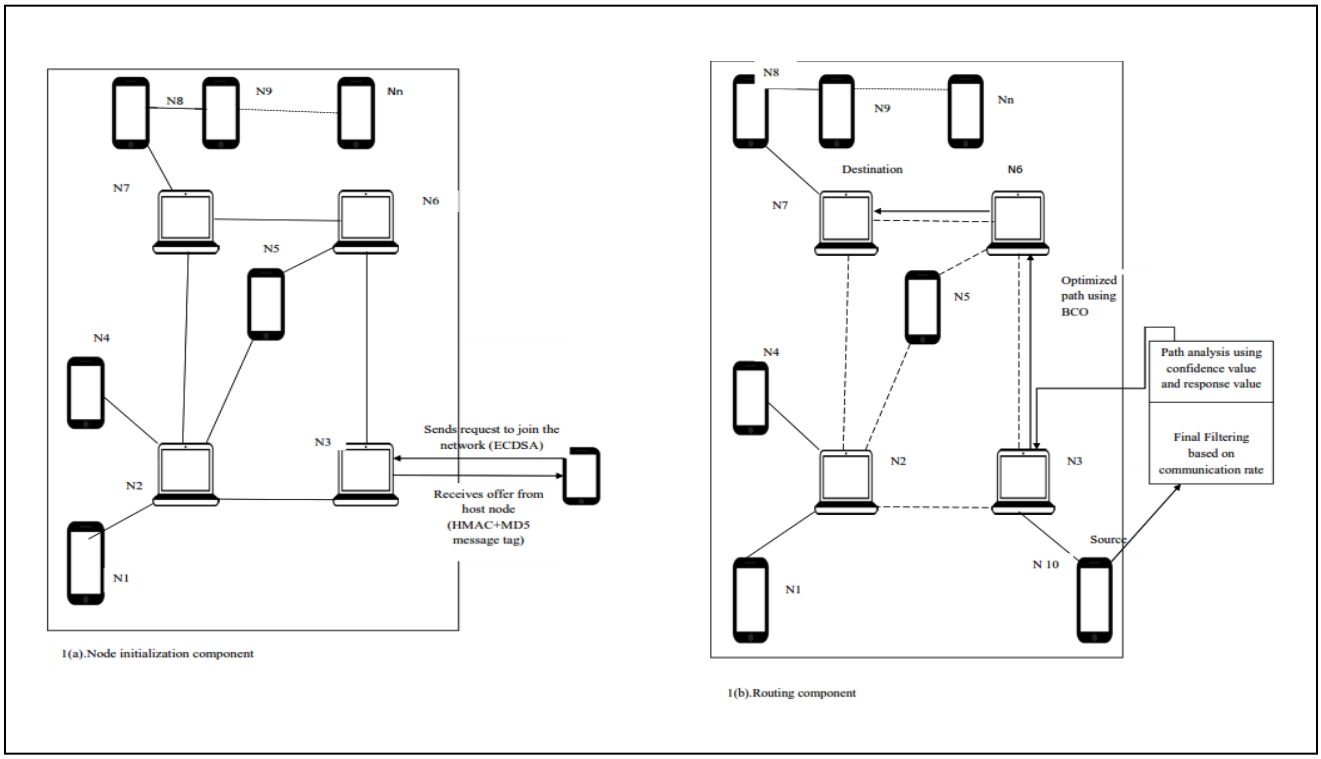

Figure.1.Components of protected reliable routing

Figure 1 portrays the components of the protected reliable routing scheme. The node initialization component shows how the new node joins into the mobile Adhoc network along with its security parameters. N1 to Nn (where n>1) are the nodes initially present in the network, when a new node requests to join the network the necessary security parameters are checked at the gateway and then it is added into the network.

The routing component of the protected reliable routing shows how the data is transferred between a source node and the destination node in MANET. N10 and N7 are the source and destination nodes respectively. Optimal path between N10 and N7 is identified using bee's algorithm. It identifies the optimal path with the help of the objective value. Once the optimal path is found the path is analyzed with certain calculation based on the opinion of the neighbor nodes and the data is transferred.

B.Routing Component

After finding source and destination nodes, the bee routing is used to find the optimal path from source and destination. Initially the objective values of the nodes are set to be zero. Objective value increases by one on each successful data delivery. In forward phase, the data is transferred to destination node via relay nodes if any. In backward phase, once the data is delivered successfully the path details are shared to estimate the path's efficiency based on the objective value. The path with high objective value is finalized as the optimal path.

Algorithm.1.Node Initialization
Set freshness=0
Send request to nodes within its radio range
Req(Node ID+Signature)
Verify ID with signature
For(each verified ID : requests)
Send response(New ID + Proxy ID+Message tag)
End for
From list of responses select ip [by FCFS]
For(rejected IP: responses)
Send(ignore IP+proxy ID + Signature)
End for
For(Accepted ip:responses)
Send (Accept IP+ proxy ID+Message tag)

End for
Do
Join node into network
While(Ack==true)
End while

The highest priority path is chosen for data transformation [18]. Before data delivery the source needs to know about the destination so its sends opinion request to neighbor nodes of the destination node. Then responses from its neighbors are collected. Responses just collected are analyzed by certain calculations.(Algorithm.2.)

Path Analysis

For each opinion received the confidence value and the response value is been calculated[19,20]. *Confidence value* is the trust bon between the source and neighbour node. It is calculated by

$$Z_{conf}=1-\sqrt{12}\sigma_{ik}$$

Where σ_{ik} is variance between i and k.

Response Value is the time taken by neighbour node to reply for the opinion request.

$$Z_{res} = \text{Response received time} - \text{request sent time}$$

After calculating the confidence value and response value the data cluster is formed [21]. The Euclidian distance between those data cluster is calculated. Shortest distance vectors are then merged together and then the values are compared to the predefined confidence value and the response value [22]. Opinions that satisfy the majority rule are selected for the trust calculation. After path analysis, the results

are then checked by communication rate [23,24]. *Communication rate* is defined as the total number of successful data delivered via particular node. Communication rate of the particular node is maintained in that node itself, based on which the opinion is finally taken for indirect trust value calculation.

4.RESULTS AND DISCUSSION

The performance of the PRR is tested in the simulated network using NS2[25]. The network is analyzed in terms of throughput, packet loss, packet delivery ratio, overhead and latency. In addition to this, the simulated network is flooded with location dependent attack to check the performance of the PRR in the presence of malicious nodes.

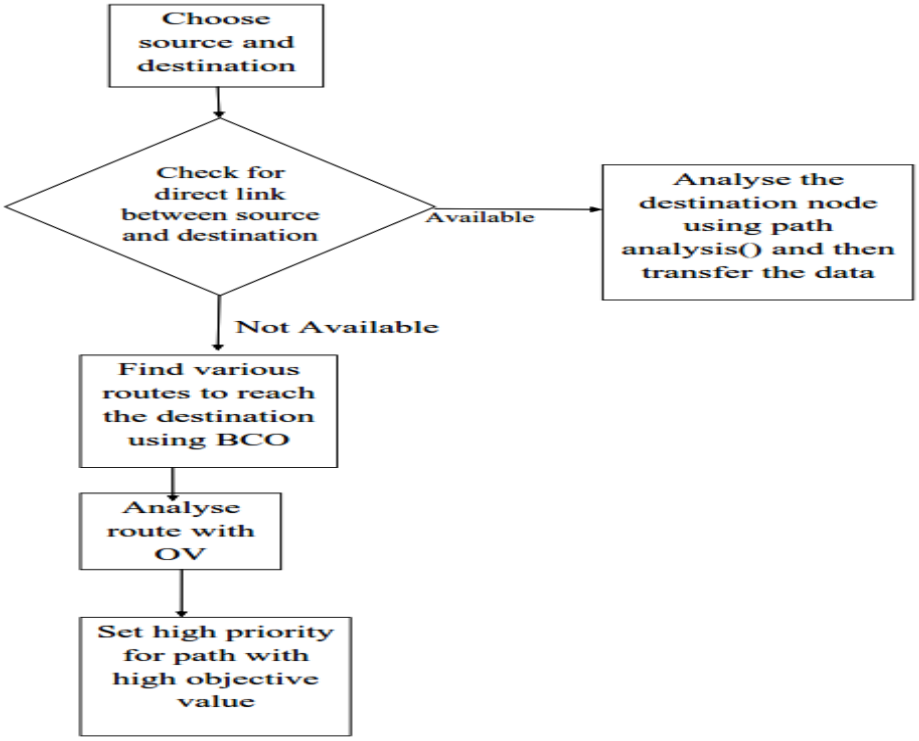

Figure.2.Flow chart of bee routing

Parameter	Value
Nodes	200
Area	1800x1800
Speed	15m/s
Radio range	300m
Movement	Random way point Model
Routing protocol	Bee
Source destination pair	45
Transfer capacity	4kbps
Application	CBR
Trust threshold	0.4

Fading timer	10s
d_{min}^{conf}	0.5
d_{max}^{conf}	0.9
Maximum time to Respond	30s

Table.1.Network configuration parameters

Algorithm.2.Protected Reliable Routing

Pick source and destination
BCO()
{
Find no.of possible paths to reach destination(Fwd phase)
Exchange information by waggle dance
Calculate OV for each possible path
Set highest priority for path with high OV
}
For(High priority path: list of possible paths)
Confirm as route
Path analysis()
End for
Path analysis()
{
Send recommendation request to neighbour
Receive recommendations
Choose trustworthy()
{
For all recommendations calculate Z_{conf} *and* Z_{res}
Create data vector
Merge data vector by Euclidian distance
Trustworthy = ($Z_{conf} \leq Conf^{threshold}$ *and* $Z_{res} \leq$ *max.time to respond)*
}
For(trustworthy:recommendations)
Analyse path preference
Path which has more no.of communication rate is given first preference
Ignore rest
End for
}

A. Simulation Parameters

The scenario setup to be made for the simulated environment in NS2 is given in Table.1. Mobile Adhoc network with 200 mobile nodes is simulated in an area of 1800x1800 square meters with the random way point model. Nodes are randomly selected and injected to cause location dependent attack. This is done

to check the proposed scheme's results in the presence of malicious node. In network there are 45 source destination pairs present and each transfer 4 packets of 75s of constant bit rate (CBR). Location dependent attack is at its peak rate of 80% to test the proposed scheme's performance even at the presence of malicious node. It is tested to check the data is safe to what extent.

B. Performance Evaluation

The figure 3 shows the performance of the PRR in the network throughput in case of dishonest recommendations. The network's performance without PRR seemed to drop on increasing false nodes gradually from 0% to 80% while the presence of PRR helps to hold the network performance up to 80% even at high malicious node rate. The throughput of PRR is 85 % right from zero malicious node rates and it maintains the same scenario at high malicious node rate (i.e,) 88 % at its peak.

.

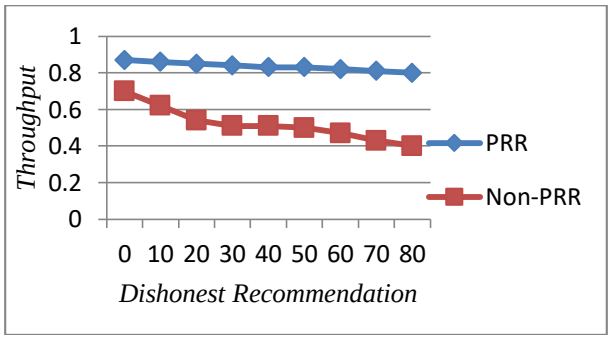

Figure.3.Network Throughput

Packet loss is the amount of data packet loss in the way to destination. Figure.4. shows the packet loss impact with and without PRR. Without PRR the packet loss gradually increases from 0 to 80%. The proposed PRR protocol eradicates the packet loss in the presence of PRR as shown in the graph.

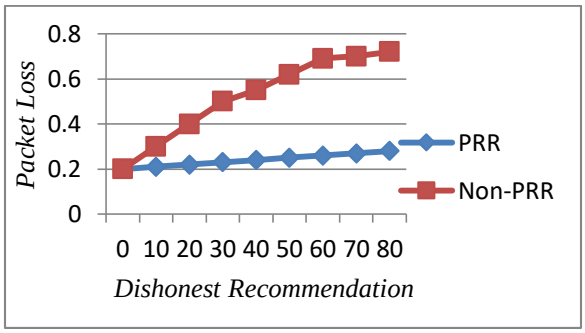

Figure.4.Packet Loss

Overhead is the excess computational time required to complete a task. Figure 5 shows the performance of PRR in terms of overhead. In the presence of 100 nodes in the network. PRR tends to show very less overhead while comparing to values without PRR. Proposed PRR seems to be better in network performance than in its absence.

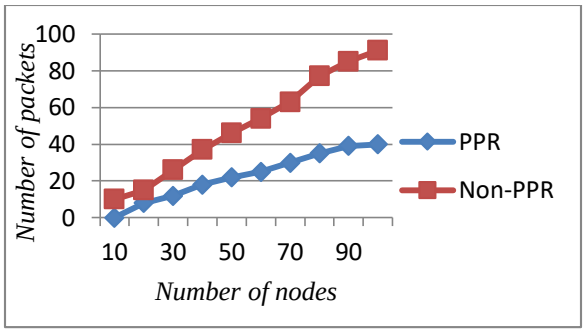

Figure.5.Overhead

Delivery ratio is defined as the amount of data packets that have been successfully delivered to the destination without delay. Figure.6. shows the simulated network where the packet delivery ratio is better. In the PRR mechanism, it delivers 80 packets successfully out of 90 sent packets while in non-PRR it delivers only half of the sent packets.

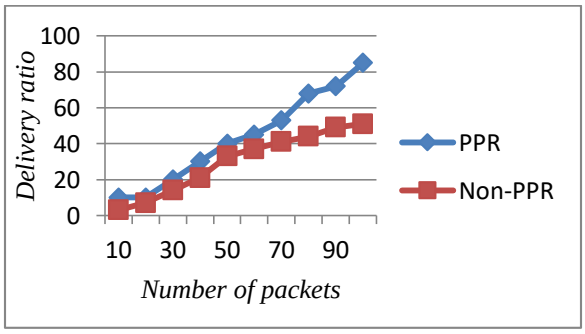

Figure.6.Delivery ratio

Latency is the amount of time required to travel from a node to another node in the network. The performance of the network in terms of latency with PRR and without PRR is shown in the figure.7. In the presence of 100 nodes in the network PRR tend to show very less addressing latency than the latency without the proposed scheme.

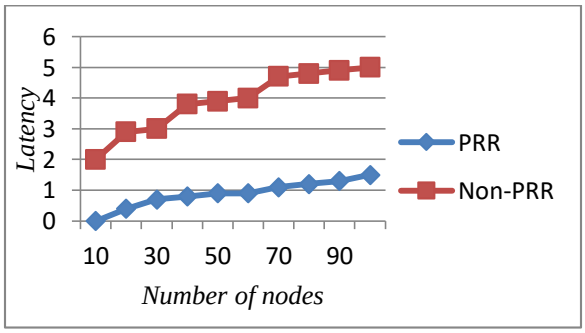

Figure.7.Delivery Latency

The network injected with malicious nodes based on the location dependent attack may cause many issues in the network. The graph shows the trust value of nodes in the presence of attack in to cases; with the proposed scheme routing protocol and without the proposed scheme routing protocol. Figure.8 (a) and 8(b) shows that PRR maintains the trust value of good node as well as distrust of bad node in the same level in the presence of location dependent attacked nodes. Without the proposed scheme the network fails to produce at least half of the expected efficiency.

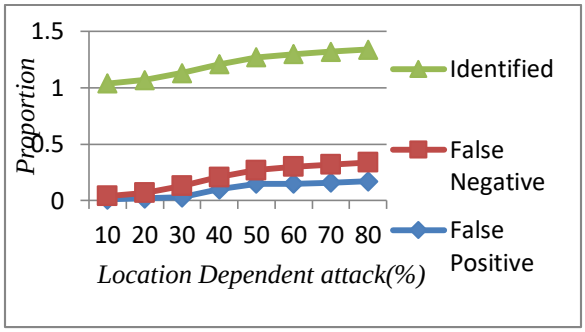

Figure.8.a) Location dependent attack with PRR

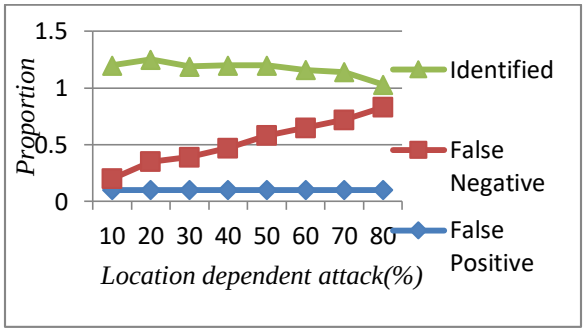

Figure.8.b) Location dependent attack without PRR

From the analysis it is clear that in the simulated network the proposed scheme PRR performs better and it shows efficient routing.

5.CONCLUSION

In this paper we have illustrated the protected reliable routing by appending privacy during node initialization and bee routing algorithm with confidence value and response value during data routing. The neoteric PRR provides favorable overhead, delivery ratio, throughput and packet loss. PRR in this paper provides expected level of security at node initialization as well as during the routing process. Security at node initialization is done with dual check of ECDSA and MD5 along with HMAC in case of unicast as well as multicast authentication respectively. Once the network is formed, the nodes are ready for routing and optimized path is found using bee routing protocol which reduces time delay. After the path selection, the selected path is analyzed with confidence value and response value based on the opinions generated by neighbor nodes. Confidence value and the response value of the opinions are calculated and compared with threshold; the results thus obtained are checked with communication rate to get the trustworthy opinion. The results obtained with network throughput, packet loss, overhead, latency,

and delivery ratio are compared as shown in the graph which shows that proposed PRR is efficient for routing in MANET. It tends to lay with safe efficiency even at the presence of malicious nodes flooded by location dependent attack.

ABBREVIATIONS

PRR:Protected Reliable Routing; MANET: Mobile Adhoc Network;CBR: Constant bit rate; TSDRP:Trust based secure demand routing protocol; RRP: Route reply packet;

ACKNOWLEDGEMENTS

The author would like to thank the reviewers for their thorough review and helpful suggestions

FUNDING

Not Applicable

AVAILABILITY OF DATA MATERIALS

Not Applicable

AUTHOR'S CONTRIBUTIONS

Dr.S.Ramesh individually contributes to the main idea,designed and implemented the algorithms and drafted the manuscript. Designed ,carried out the simulation and analyzed the result by himself

COMPETING INTERSTS

The author declares that they have no competing interests.

REFERENCES

[1].H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks,'' Communications Magazine, IEEE, 40, (10), pp. 70-75, (2002).

[2]. N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, "An efficient and robust addressing protocol for node autoconfiguration in ad hoc networks," Networking, IEEE/ACM Transactions on, vol. PP, no. 99, p. 1, (2013).

[3]. P. Wang, D. S. Reeves, and P. Ning, "Secure address auto-configuration for mobile ad hoc networks," in Proceedings of 2nd Annual International Conference MobiQuitous, pp. 519–522, (2005).

[4]. U. Ghosh and R. Datta, "A secure dynamic ip configuration scheme for mobile ad hoc networks," Elseiver Ad Hoc Networks, vol. 9, no. 7, pp. 1327 – 1342, (2011).

[5]. U. Ghosh and R. Datta, "A secure addressing scheme for large scale managed MANETs",IEEE transactions on network and service management,(2015).

[6].Baris yuce and Michael.S.packianather, "Honey bees inspired optimization method : The bees algorithm" Insects ISSN 2075-4450,(2013).

[7]. Ramesh, S & Ganesh Kumar, P, 'BCR routing for intermittently connected mobile ad hoc networks', International Journal of Engineering and Technology, ISSN: 0975-4024, vol. 6, no. 1, pp. 66 -74(2014).

[8].Filomena de Santis,"An efficient bee inspired auto configuration algorithm for mobile Adhoc networks", International journal of computer applications,(2012).

[9]. Ramesh, S & Indira, R, 'B-LoDiS Routing for Intermittently Connected MANET with Agent AES Approach', Internetworking Indonesia Journal, ISSN: 1942-9703 Vol.7, No.1 B, pp. 13-23(2015).

[10] David Airehrour, Jairo Gutierrez,Sayan Kumar Ray "GradeTrust: A Secure Trust Based Routing Protocol For MANETs" International Telecommunication Networks and Applications Conference (ITNAC) (2015).

[11] Naveen Kumar Gupta, Kavita Pandey "Trust Based Ad-hoc On Demand Routing Protocol for MANET" 978-1-4799-0192-0/13/$31.00 ©IEEE (2013).

[12]. Heena, Neeraj kumar "Battery Power and Trust Based Routing Strategy for MANET" IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) (2014).

[13] KefayatUllah ,Rajib Das,Prodipto Das, Ananya Roy "Trusted and Secured Routing in MANET: An Improved Approach" International Symposiwn on Advanced Computing and Communication (ISACC) (2015).

[14]. N. Marchang R. Datta "Light weight trust based routing protocols for mobile Adhoc networks" IET Inf. Secur., 2012, Vol. 6, Iss. 2, pp. 77–83 (2012)

[15]. H. Xia,Z. Jia, L. Ju,Y. Zhu "Trust management model for mobile Adhoc netork based on analytic hierarchy process and fuzzy theory" ET Wirel. Sens. Syst., 2011, Vol. 1, Iss. 4, pp. 248–266 2011

[16]. Antesar M. Shabut, Keshav P. Dahal, Sanat K. Bista, Irfan U. Awan "Recommendation based trust model with an effective defence scheme" IEEE transactions on mobile computing, (2015).

[17]. Sesha bargavi, Seetha viswanadharaju "A trust based secure routing schemes for MANETs" 6th International Conference - Cloud System and Big Data Engineering (Confluence) (2016).

[18]. M.K. Denko, T. Sun, and I. Woungang, ''Trust management in ubiquitous computing: A Bayesian approach,''Computer Communications, 34, (3), pp. 398-406, (2011).

[19]. Ramesh, S & Ganesh Kumar, P, 'A secure 3-way routing protocols for intermittently connected mobile ad hoc networks', The Scientific World Journal, Hindawi Publications,(2014).

[20]. P. Chatterjee, I. Sengupta, and S. K. Ghosh, "A distributed trust model for securing mobile ad hoc networks," in Proceedings of the 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, (Washington, DC, USA), pp. 818–825, (2010).

[21]. A. Cavalli and J. Orset, "Secure hosts auto-configuration in mobile ad hoc networks," Ad Hoc Networks, vol. 3, no. 5, pp. 656–667, (2005).

[22]. K. Weniger, "Pacman: passive autoconfiguration for mobile ad hoc networks," Selected Areas in Communications, IEEE Journal on, vol. 23, pp. 507–519, (2005).

[23]. X. Wang and H. Qian, "Dynamic and hierarchical ipv6 address configuration for a mobile ad hoc network," International Journal of Communication Systems, (2013).

[24]. Ramesh, S , Praveen, R, Indira, R& Ganesh Kumar, P, 'A survey on routing methodologies for ICMANET', Proceedings of the fourth IEEE International Conference on Advanced Computing, Anna University, Chennai, pp. 1-6(2012).

[25]. T. Issariyakul and E. Hossain, ''Introduction to network simulatorNS2,'' Springer, (2011).