IJCTA, 9(40), 2016, pp. 203-212
© International Science Press

Trust and Neighbor Coverage Based Probabilistic Rebroadcast routing for MANET

S. Baskaran* J. Arputha Vijaya Selvi and V.R. Sarma Dhulipala*****

Abstract : A mobile ad-hoc network is formed by using the various nodes with wireless link and random topology. Infrastructure like central station, router, and switch are not used in network structure. Providing Security for routing and data packets is one of the difficulties in MANET routing. The proposed TNCPR protocol works in two phases. In the first phase source node challenge the neighbor nodes and list the trusted, non-trusted nodes separately. The data about the trusted nodes and non-trusted node lists are shared with the other nodes periodically. Further the nodes in the trusted list are appraised depends on complete for the source node and other nodes. This enables the malicious nodes isolated. In the second phase when a node agrees to transfer data it broadcasts a route request message only through the nodes in the trusted list and it integrates the benefits of coverage knowledge of neighbor and the probabilistic mechanism. In this paper, it is proposed that the trust and neighbor coverage based probabilistic rebroadcast protocol to decrease the overhead in MANET. By simulation results it's shown that the proposed architecture decreases the routing overhead when the packets routed through trusted nodes.

Keywords : Mobile ad hoc networks, neighbor coverage and Trust, Routing Overhead, Probabilistic rebroadcast.

1. INTRODUCTION

In present computerized world, rapidly and fast emerging technologies are required for businesses and industries. The basic provision of the Computer Networking (CN) is most essential in the present world. The CN has countless categorizations system among these categorizations wireless networks get a significant role. The main benefit is taken by Mobile Ad hoc Networks (MANETs) is mobility and scalability.

MANETs are very elastic, there is no infrastructure or administration is required. These nodes perform both as a router and also the host. Therefore, mobile ad-hoc networks are fit for short-lived communication links.

The major challenge in MANETs is design of secured and efficient routing protocol to improve the quality of service, reduce the routing overhead, security, scalability. Due to change of mobile node positions in MANETs path failures happens because of frequent link breakages, hence once again route to be discovered, this rises the routing protocols overhead and rises end to end delay and decrease the packet delivery ratio.

Sanjay K. Dhurandher et al. [1] suggested the FACES algorithm provides a highly secure routing among nodes. The mobile nodes are rated in the scale between zero and ten. And also having challenges for verifying the nodes. The protocol is implemented in four stages; initially there will be no criteria exists, first stage verifies the nodes by making challenges. Second stage it calculates the trust levels for all nodes in the network. Third Stage it shares the trusted node list with other nodes. The first three

* Research Scholar, Vels University, Tamil Nadu, India

** HOD (ECE) & Dean (R & D) Kings College of Engineering, Punalkulam, Thanjavur, Tamil Nadu, India

*** AP/Physics, BIT Campus, Anna University Campus, Trichy, TN, India.

stages will be performed periodically. In the Fourth stage data transmission occurs through the trusted nodes based on the ratings calculated. Congestion occurs in the highly rated path due to more packets transmission. Zhang et. Al [2] suggested neighborhood coverage based probabilistic rebroadcast protocol to decrease the routing overhead, the neighbor coverage knowledge comprises added connectivity factor and coverage ratio. Also rebroadcast delay is implemented to get the neighbor coverage information. The initial idea for the protocol is derived from the above. Initially nodes in the network will be kept either in trusted list or non-trusted list. When the node deiced to transmit data through trusted nodes, neighbor coverage knowledge and the probabilistic mechanism are used to optimize the rebroadcast traffic during data transmission.

2. RELATED WORK

Marti et al. [8] implemented Pathrater ans Watchdog and mechanism in Dynamic Source Routing (DSR) protocol that optimizes the packet forwarding method. The selfish nodes are identified by Watchdog and the Pathrater helps routing protocol to escape selfish nodes during data transmission. Nodes are rated based upon the feedback received from the Watchdog. The route is selected through the highest rated nodes. It is difficult to identify the misbehaving nodes during the following occasions like Partial dropping, false misbehavior, Limited transmission power Ambiguous collisions, and Receiver collisions.

A probabilistic broadcasting system is proposed by Kim [3] based on coverage area and neighbor confirmation. Probabilistic approaches with the area-based approach are implemented in the protocol. The rebroadcast probability is adjusted by a node dynamically. The coverage is assessed by the distance from the sender.

Aminu [4] proposed a rebroadcast probability function to decide the suitable rebroadcast probability for a specified node; it keeps the data about the packet counter value with key simulation parameters. Rebroadcast and end-to-end delay is improved compare to the schemes.

A trust based multipath routing is suggested by Prayag Narula et al. [5]. The direct trust and the recommendation from the peers are added and assigned to the node. A node with less trust is given less number of self-encrypted message; hence malicious node has less opportunity to break through the encryption strategy. Non-trusted routes are avoided; to prevent the brute force attack because they may decrypt messages if adequate amounts of the message are available to them.

Dahill et al. [6] proposed Authenticated Routing for Ad-hoc Networks (ARAN) applies asymmetric public-key cryptographic mechanisms to avoid all expected attacks. ARAN requires a trusted certificate server in the network.

Y.Hu. et al. [7] proposed SEAD (Secure Efficient Ad hoc Distance vector), based on Destination Sequenced Distance Vector (DSDV) protocol. It uses one way hash function which guards against Denial of Service attack. It fails identify the update malicious node when the same metric is used. A finite size hash chain is used in SEAD nodes, when all their elements have been used then it must be generated again.

3. NEIGHBOR COVERAGE AND TRUST BASED PROBABILISTIC REBROADCAST ROUTING FOR MANET

The TNCPR is implemented in two stages:

Stage 1:

1. Challenge the neighbor nodes
2. Rate the trusted nodes
3. Share trusted nodes

Stage 2:

4. Calculate the rebroadcast delay
5. Calculate rebroadcast probability using connectivity factor and additional coverage ratio
6. Route through trusted nodes

1. Challenge the neighbor nodes

Challenge the neighbor enables a node to create the trusted node list and non-trusted node list, this happens when there is no criterion existing initially. To prove the honesty and integrity the neighbor nodes are tested using the challenge mechanism. Assume that node X challenge the neighbor node Y

Step 1: All the neighbor nodes are kept in the unauthenticated list initially by the node X

Step 2: Node X picks the neighbor Y and shares the trusted nodes list

Step 3: Now Y sends the trusted list or unauthenticated list if it is initial stage

Step 4: After getting the list node X selects the node Z which is reachable via Y and other neighbor.

Step 5: A starts encrypts it with the public key of Z and routs through both routes after including node X's public key.

Step 6: Node Y forwards the challenge packet to node Z. Node Z decrypts the packet and replies the difficulties using the public key of X, which is obtained through the challenge packet.

Step 7: Node X receives the challenge reply from network routes and compares it. Incase both are similar then and there node X adds node Y in its trusted list.

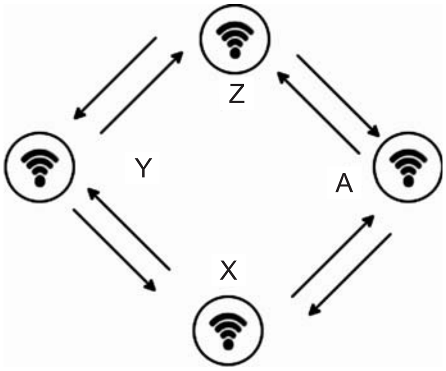

Figure 1

In the following occasions node Y is kept in the non-trusted list by the node X.

1. When node Y does not response to the challenge
2. When the result from the node Z through node Y and other node differs
3. When the other route is malicious and Y reply is correct
4. When node Y does not have any common neighbor with node X
5. When the node Y has only node X in its communication range

Description of Challenge

Each node is start with a large pair of prime number which are very secret to that node. Therefore X is done with (a, b) and Z with (c, d). Whenever, the X challenges node Y, X forward a huge random prime number which is denoted as "n" to Z over the two different kinds of routes. Consider the node Z calculate c^d mod n and forwards the response over two different kinds of routers. After that X relates two results to find at a conclusion on the challenged node Y. Here it is very challenging to find the c and d from the given mode functions due to the n, c, and d are huge prime numbers. This is very efficient process and also is very challenging for doing any kinds of malpractices node to authenticate. To share the kinds of trusted nodes in this proposed TNCPR algorithm, first challenge is required to show its behavior is correct.

2. Rate the trusted nodes

Trusted nodes are rated between zero to ten value. Initially nodes which are accomplished the challenge effectively are kept the trusted nodes list. Sharing the trusted node list is done the share trusted node stage. For example X is the trusted node for Y and Z is the trusted node for Y hence X will include Z in in its trusted list. Each node the trusted list is rated in three different classes Net Rating (NR), Trust Rating (TR) and Data Rating (DR).

A. *Data Rating*

The Data rating of a node in the trusted node list is calculated based on data transmission completed for the source node. Based on the number of packets transmission decides a nodes DR with five data ratings is defined as follows.

$$\mathrm{DR}(i) = \mathrm{DR}(i-1) + \mathrm{D}(i-2) + \mathrm{DR}(i-3) + \mathrm{D}(i-4) + \mathrm{D}(i-5) \qquad (1)$$

The DR for a specific session is considered as

$$\mathrm{DR} = 10*(1 - e^{-\lambda x}) \qquad (2)$$

Where x is defined as the number of transmitted data packets and λ is defined as the factor which is used to define the number of data packets which is associate to the rating.

B. *Trust Rating*

During the trusted list sharing stage a node receives the trusted nodes list from its neighbors and incorporates the rating with its trusted node. If node X and node Y have a mutual trusted node Z, then and there node X acquires the rating of the node Z from node Y, as shown below ().

Situation 1:

Net Rating (NR) of Y in list X = 10 of NR of Z in list of
Y = 6
Hence, Obtained Rating (OR) = 6

Situation 2:

NR of Y in list X = 7 of NR of Z in list of
Y = 6
Hence, Obtained Rating (OR) = 0.7*
6 = 4.2

The Weighted average of the net ratings gotten through the sharing stage of trusted node is defined as follows

$$\text{Obtained Rating} = \frac{\text{Obtained Rating} = (\text{Net Rating of B in the list of A*Net Rating of C in the list B})}{10} \qquad (3)$$

C. *Net Rating*

TR represents the attitude of the node towards integrity of another node; DR signifies a personal opinion of a node resulting on the foundation of earlier data transmissions. Mutually the ratings are significant to recognize the malicious nodes. The NR would be weighted mean of the two ratings is defined as follows

$$\mathrm{NR} = \frac{(\mathrm{W1*DR} + \mathrm{W2*FR})}{10} \qquad (4)$$

Where W1 and W2 defined as the weights allocated to DR and TR correspondingly. The values W1 and W2 are network in need of and can be learnt with experience.

4. SHARE TRUSTED NODES

Sharing the trusted nodes is the periodic procedure, the control packet FREQ is used to complete the task. After receiving the FREQ control packet, a node based on the nodes with the non-trusted list, unauthenticated list and trusted list. During the process the following rules must be followed.

1. Any node in the network can make the request for share trusted nodes
2. After sharing the trusted node which is initiated for those nodes which are not in the trusted list.

5. CALCULATE THE REBROADCAST DELAY

When a node s sends an RREQ packet to the node x_i, using the neighbor list in the RREQ packet node x_i determines the how many of its neighbor nodes are covered by the source nodes. if the node x_i has more neighbors uncovered by node s than node x_i rebroadcast the RREQ packet to the uncovered neighbors. Equation [5] describes calculation of UnCovered Neighbor set U(x_i).

$$\mathrm{U}(x_i) = \mathrm{N}(x_i) - [\mathrm{N}(x_i) \cap \mathrm{N}(s)] - \{s\} \tag{5}$$

Where N(x_i) is the neighbor set of node x_i, and N(s) is neighbor set of s. Where node x_i receives the RREQ packet from node s. Initial UCN set is obtained based on (5). Node x_i can receive duplicate RREQ packets from its neighbors because of broadcast characteristics of network. Hence node x_i could adjust the U(x_i) with the neighbor knowledge.

A rebroadcast delay is implemented to exploit the neighbor knowledge and avoid the channel collisions. After receiving the RREQ a node calculates the rebroadcast delay depends on the neighbor list in the RREQ packet. The calculation of rebroadcast delay Td(x_i).

$$\mathrm{T}d(x_i) = \text{Max delay X T}p(x_i) \tag{6}$$

Max delay is the constant delay and the Tp(x_i) is the delay ratio of x_i. The delay time decide the node transmission order. Nodes with less common neighbors are permitted to broadcast initially which makes other nodes with lowest delay to further adjust its UCN. The broadcast delay used to determine the neighbor knowledge very quickly.

6. CALCULATE REBROADCAST PROBABILITY USING CONNECTIVITY FACTOR AND ADDITIONAL COVERAGE RATIO

The rebroadcast probability system calculates the information about the local node density, connectivity metric and Uncovered Neighbors (UCN).

The rebroadcast probability is divided in to two different kinds of parts:

(*a*) In addition Coverage Ratio, which is the ratio is defined as the number of nodes that should be enclosed by a single broadcast to the entire number of neighbors;

Assume the node x_j has lowest delay than node x_i, hence node x_j may listen to node x_i RREQ packets, using the neighbor list received through RREQ packet from x_i, the node x_j further adjust its UCN

$$\mathrm{U}(x_i) = \mathrm{U}(x_i) - [\mathrm{N}(x_i) \cap \mathrm{N}(x_j)] \tag{7}$$

After adjusting the UCN the RREQ packet from x_i is discarded. Rebroadcast probability is gotten by merging the surplus coverage ratio and connectivity factor. The added coverage ratio is defined as follows

$$\mathrm{ACR} = \frac{|\mathrm{U}x_i|}{|\mathrm{N}x_i|} \tag{8}$$

The ratio indicates that number of nodes furthermore protected by this rebroadcast against to the total number of nodes in the network. As Ra is bigger, more nodes need to receive and process the RREQ packet and thus, the rebroadcast probability should be set higher.

(*b*) Connectivity Factor(CF), which reflects the association of the number of neighbors and network connectivity of a given node.

Connectivity factor is calculated using a heuristic formula

$$\mathrm{CF} = 5.1744 \log n\, \mathrm{N}(x_i) \tag{9}$$

Xue and Kumar [9] derived that if network connectivity probability methods 1 when each node connects to more than 5.1774 log n of its nearest neighbors. Hence 5.1744 can be used as the network's connectivity metric.

Here the rebroadcast probability is obtained as follows

$$\mathrm{Pre}(x_i) = \mathrm{ACR} * \mathrm{CF} \tag{10}$$

If the probability is Pre(x_i) is greater than 1 set the probability 1.

7. ROUTE THROUGH TRUSTED NODES

Source node initiates a Route Request message with number of data packets to be sent. And it evaluates the route available through the trusted nodes. The best possible route is selected for data transmission, after sending packets source node wait for the acknowledgement. Destination sends the acknowledgement via multiple routes to the source. Here the public key mechanism used to encrypt the packets. Sequential challenge method is used to identity the misbehaving node during the data transmission. If any node found dropping the packets is dropped from the trusted nodes list and kept in non-trusted node list also it reduces the rating of the node.

Route Evaluation: When the source node gets the different route reply messages it examines the route on the fundamental of the subsequent standards

In case more than then routes values is similar after that, it computes the mean choose the route with the extreme mean value

It computes reduces net rating value of the node in each and every route. It selects the route having the minimum value of maximum net rating of a node in the route.

In case the mean get the similar value, then compute the quality of the router is consider as follows

The node computes the Net Rating of the means value it divides this values of means with the route's quality factor.

Where, the quality factor of the route is the divergence from the mean. lesser the divergence is greater the quality of the route. The Quality Factor can be calculated in following ways

1. Standard Deviation;
2. Mean Absolute Deviation (MAD)

Where, the MDA is a known as well-defined scale measure. These scales are utilized to replace the conventional assessments of the scale for example the sample standard deviation and sample variance. Rousseeuw and Croux [12] author initiate the alternatives to MAD, pointing out two problems of it.

Where $$Qn = \text{first quartile of } (|x_i - x_j|) : i < j)$$

Here x_i and x_j are the values of net rating of particular route arranged in ascending order.

These can be calculated O(n log n) time and O(n) space. The Qn is the quality factor use it to divide the mean to get the path's quality. The data is then routed through this path.

8. SIMULATION ANALYSIS

The simulation analysis is using NS-2 Simulator.

To assess the performance of proposed TNCPR, it has related with the existing FACES protocol using NS-2 simulator.

The performances of routing protocols are evaluated using the following performance metrics:

1. Number of Malicious Nodes Insulated from the Network.
2. Number of Packets Routed over Malicious Nodes.
3. Packet Overhead.
4. Number of Data Packets dropped by Malicious Nodes.

5. Energy Consumed in the Network
6. Packet delivery ratio

Table 1

Simulation parameter	*Value*
Simulator	NS-2 (v. 2.34)
Topology size	800 m X 800 m
Number of Nodes	30, 40, 50, 70
Mobility	Random way point
Transmission range	250 m
Bandwidth	2 Mbps
Interface queue length	50
Traffic type	CBR
Number of CBR connections	10,12,14.. 20
Packet Size	512 bytes
Packet Rate	4 packets / sec
Pause Time	0s
Min Speed	1m/s
Max Speed	5m/s

Protocols Compared

FACES: Friend based Ad hoc routing utilizing Challenges to Establish Security and TNCPR.

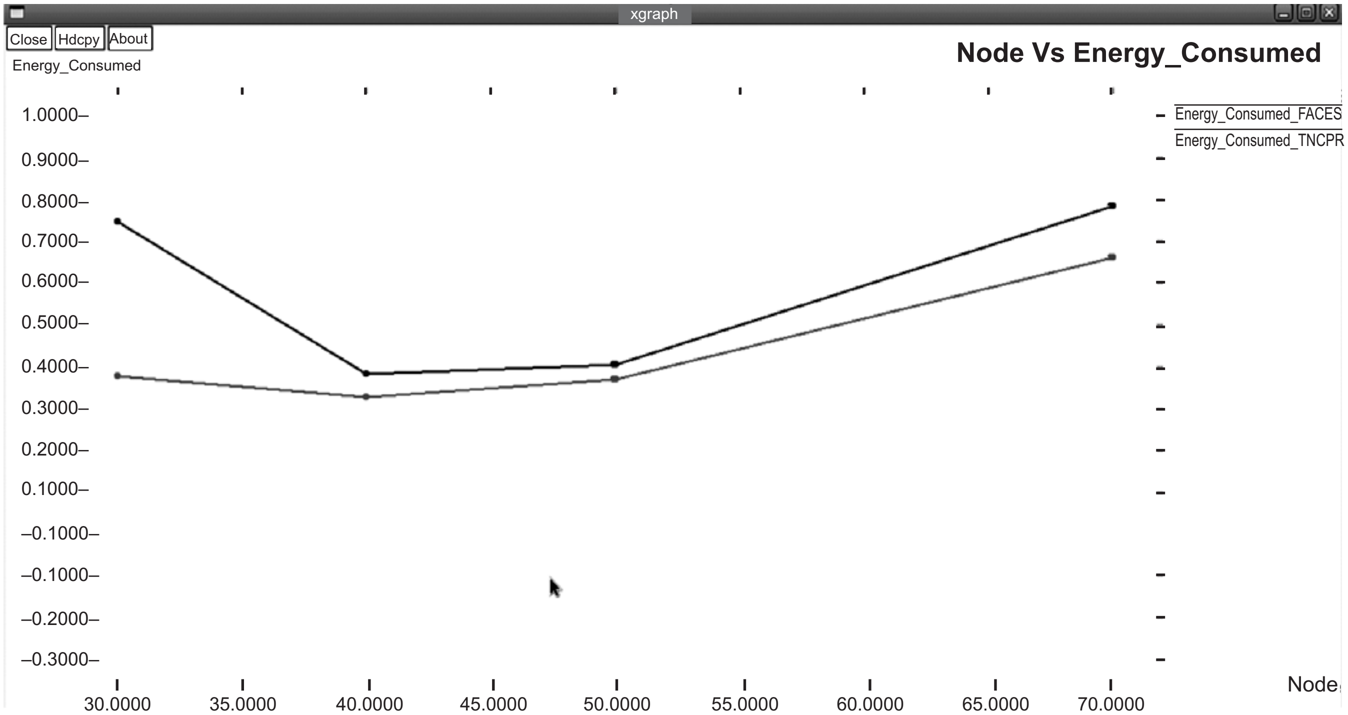

Figure 2: No. of nodes Vs Energy consumed

The TNCPR protocol initially isolates the malicious nodes using the challenge mechanism. After isolating the malicious nodes route is established only through the trusted nodes which is shared with all other nodes.

Percentage of energy consumption of the network indicates energy utilization. In mobile adhoc network energy is the major problem. Here TNCPR consumes less energy compare to FACES algorithm because the TNCPR using the delay and rebroadcast probability which reduces the control overheads. Energy consumption increased when there is number of packets increased.

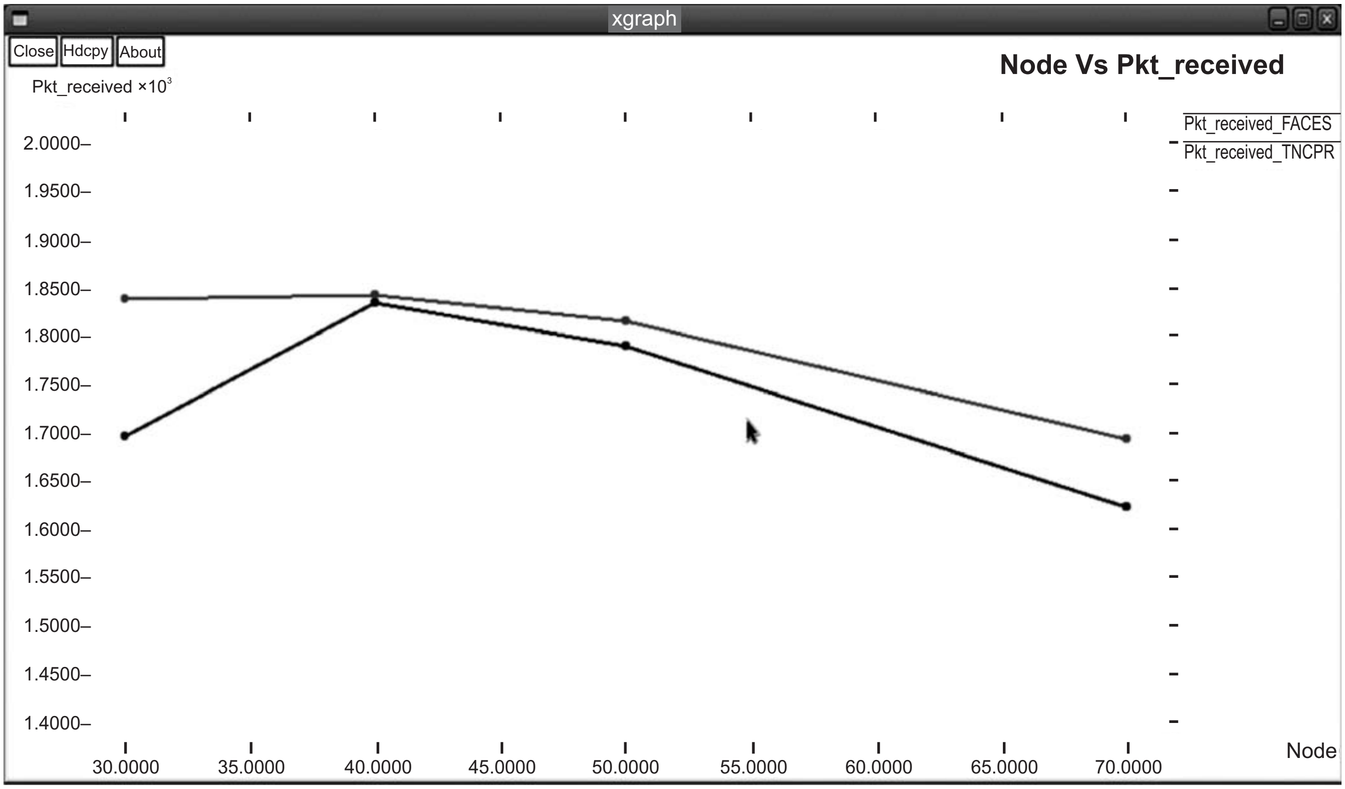

Figure 3: No. of nodes Vs Packet received

No. of packets received is improved in TNCPR protocol compare to the FACES protocol.

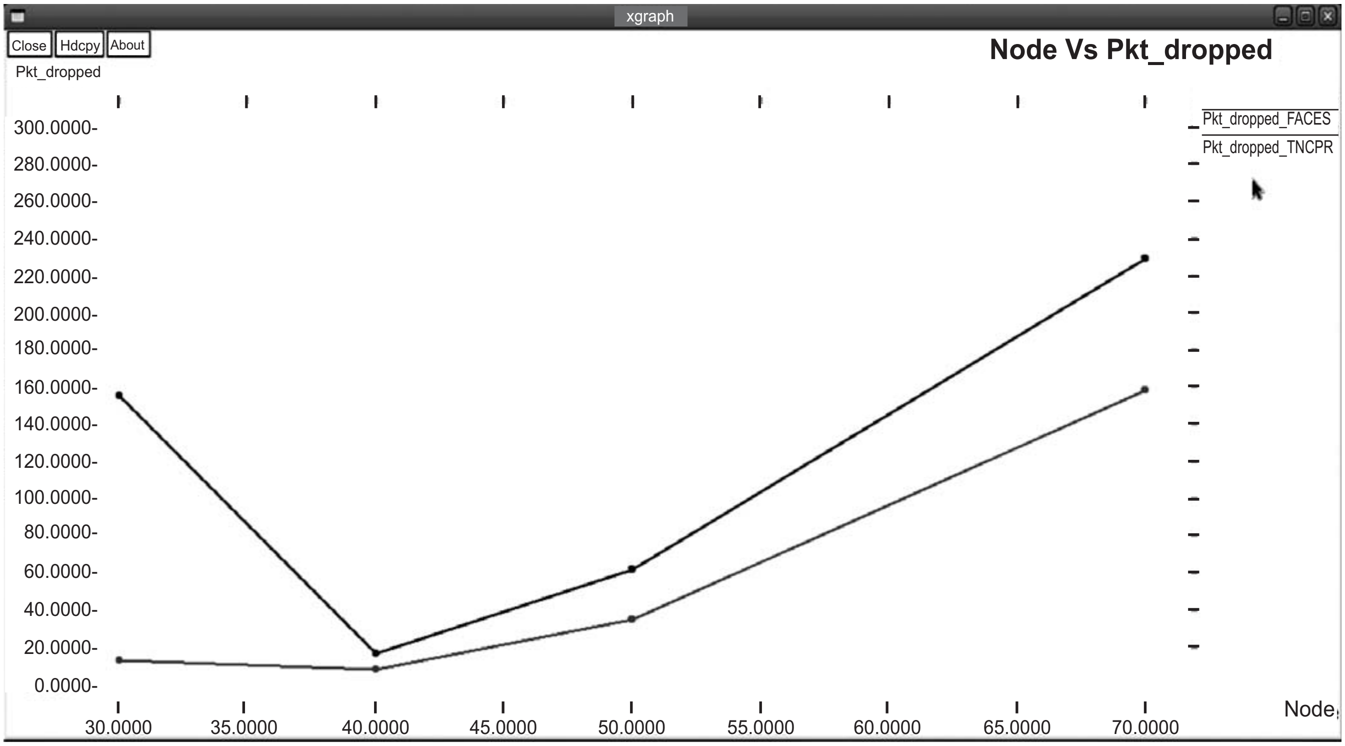

Figure 3: No. of nodes Vs Packet dropped

In the Fig 4, we can see that the packet drop very less in TNCPR, as it competently rejects routes with malicious nodes. When the number of nodes increased with mobility, it is found that the number of packet drop increases

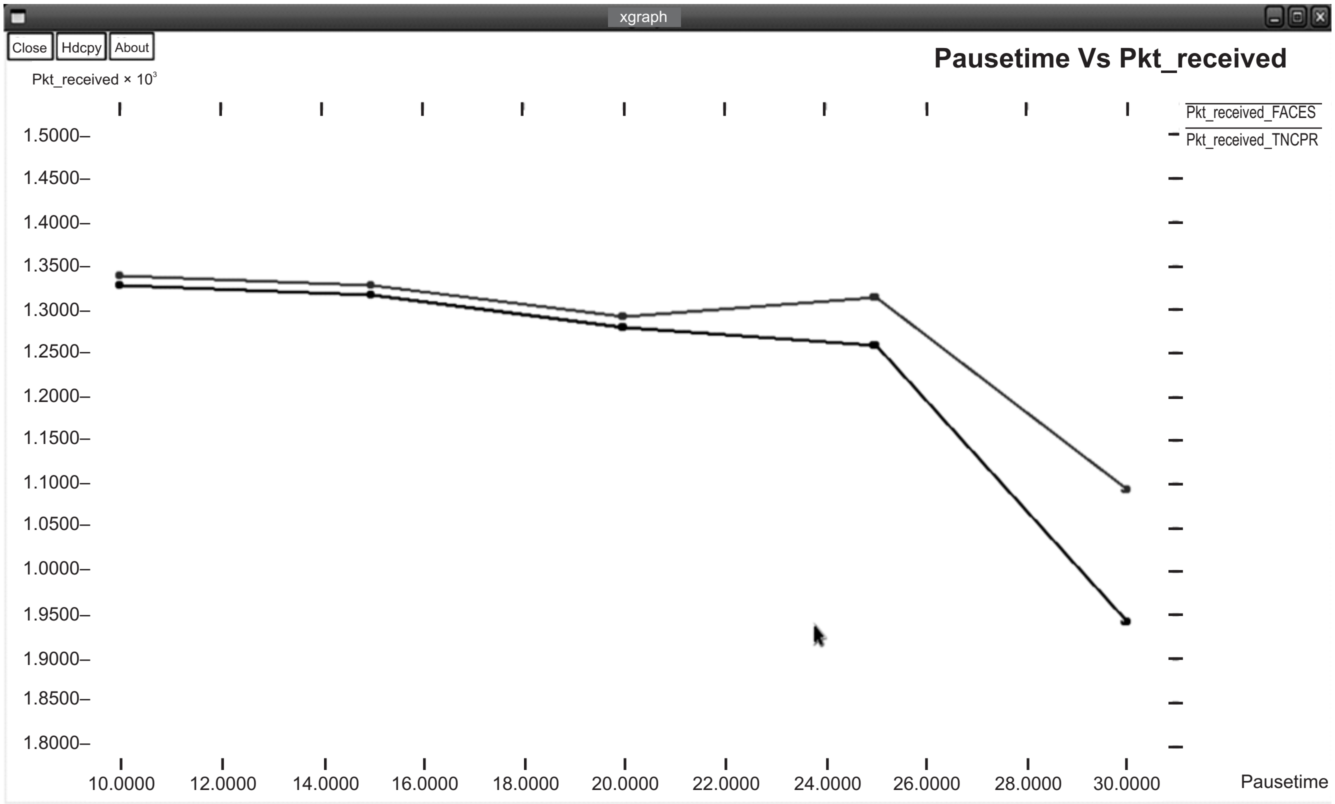

Figure 4: No.of Nodes Vs Control Overheads

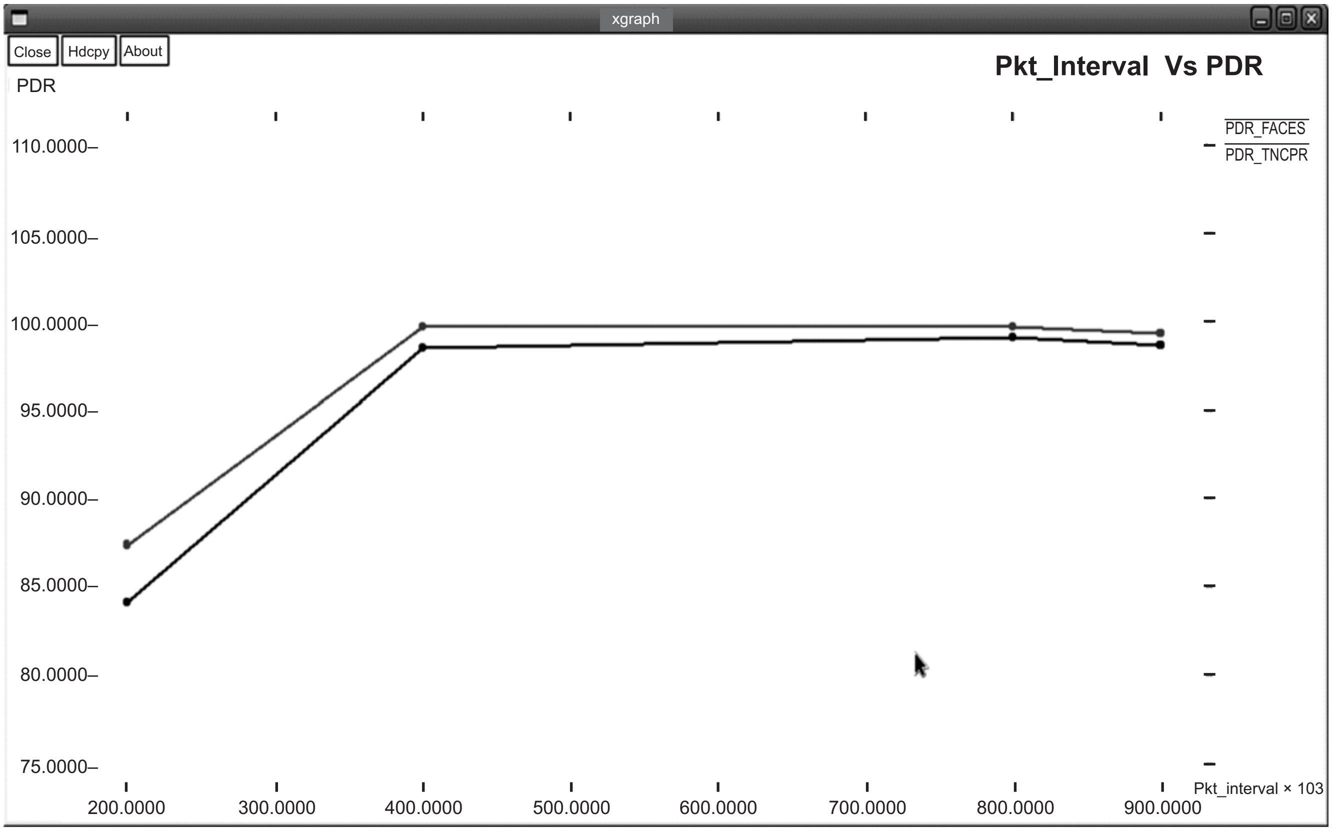

Figure 5: Packet interval Vs PDR

Control Overhead: Total no of control overhead ratio to total no of received packet, here it is examined that average no of routing packets need to deliver a single data packet. This metrics provides an idea about the obtain bandwidth used by the deliver data traffic overhead

Packet Delivery Ratio: Is used to computer the no of received packets by the destination separated by no of packets send by the source node. This metrics provides an idea of how the protocol performing the packet delivery process at the time of simulation process. It gives that the malicious node are limited after security launching.

9. CONCULSION

After an extensive simulation and logical analysis of the proposed TNCPR algorithm using different kinds of setup get the conclusion which is provides the robust process in term of security for mobile ad hoc networks and additionally it gives the better results when compared with other trust based protocols. In future, in this work plan to implement ARAN and ARIADNE is as secure routing protocols and which is are compared with the TNCPR protocol which process is used to established secure routing protocols for MANETs.

10. REFERENCES

1. Sanjay K. Dhurandher, Mohammad S. Obaidat, Fellow, IEEE, Karan Verma, Pushkar Gupta, and Pravina Dhurandher "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems" IEEE SYSTEMS JOURNAL, VOL. 5, NO. 2, JUNE 2011.
2. Xin Ming Zhang, Member, IEEE, En Bo Wang, Jing Jing Xia, and Dan Keun Sung, Senior Member, IEEE "A Neighbor Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad Hoc Networks"
3. J. Kim, Q. Zhang, and D.P. Agrawal, Probabilistic Broadcasting Based on Coverage Area and Neighbor Confirmation in Mobile Ad Hoc Networks," Proc. IEEE GlobeCom, 2004.
4. Aminu Mohammed, Ould-Khaoua, M., and Mackenzie, L. (2009) An improved rebroadcast probability function for an efficient counter-based broadcast scheme in MANETs. In: 25th Annual UK Performance Engineering Workshop (UKPEW'09), Jul 2009,
5. P. Narula, S. K. Dhurandher, S. Misra, and I. Woungang, "Security in mobile ad-hoc networks using soft encryption and trust based multipath routing," Sci. Direct Comput. Commun., vol. 31, pp. 760–769, 2008.
6. K. Sanzgiri, B. N. Levine, C. Shields, B. Dahill, and E. M. Belding- Royer, "A secure routing protocol for ad hoc networks," in Proc. 10th IEEE Int. Conf. Network Protocols (ICNP), Paris, France, Nov. 12–15, 2002, pp. 78–89.
7. Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks Journal, 1, 2003, pp.175-192.
8. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. MobiCom 2000, Boston, MA, Aug. 2000, pp. 255–265.
9. F. Xue and P.R. Kumar, "The Number of Neighbors Needed for Connectivity of Wireless Networks," Wireless Networks, vol. 10, no. 2, pp. 169-181, 2004
10. D. P. Agrawal and Q.-A. Zeng, Introduction to Wireless and Mobile Systems. Pacific Grove, CA: Brooks/Cole, Thomson, 2002
11. M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in WiSe'02: Proc. of 1st ACM Workshop on Wireless Security, Atlanta, GA, Sep. 28, 2002, pp. 1–10.
12. P. J. Rousseeuw and C. Croux, "Alternatives to the median absolute deviation," J. Amer. Statist. Assoc., vol. 88, no. 424, pp. 1273–1283, Dec. 1993
13. A. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems. Boca Raton, FL: CRC, 2005, pp. 32:1–32:20.
14. C.Sivaram murthy, B.S.Manoj, "Ad hoc wireless networks: Architectures, and protocols", Pearson Education, 2004.