Implementation and analysis of enhancement in opportunistic network using NS2

Sandeepak Bhandari
Aleksandras Stulginskis University, Kaunas, Lithuania
e-mail: sandeepak525@gmail.com

***Abstract*—Opportunistic network is a new class of wireless network. This network is based on store-carry-forward mechanism. An architecture and functionality are different from another wireless network such as wireless sensor network or mobile ad hoc network. Unlike mobile ad hoc network opportunistic network do not need end to end path between source and destination nodes for providing communication between them. In this paper, methodology for enhancement in opportunistic network is proposed and implement by using network simulation. Multi-hop relay technique and Virtual-ID used together to enhance the performance of opportunistic network and at last performance of opportunistic network is analyzed by using three different cases in opportunistic network.**

Keywords—Opportunistic network; Bundle layer; Store-carry-forward manner and relay technique

I. INTRODUCTION

A new network is invented or a class of delay tolerance network in which some device which is carried by the users in their daily life and can pass message when they get opportunity, hence network is called opportunistic network [1]. It is framed by the hubs having ability to bolster this system, the hubs are associated wirelessly. The hubs are versatile or stable so no settled foundation is available in this system and this system can work even in disconnected environment [2]. Each hub has a limited range in which they can convey or can forward the message. A hub can forward a message just when some other hub comes in his range. The hubs need to store the message until another hub is not come in his range [3]. All hubs need to work in the store-convey forward way in this system.

In this network, group of intermediate nodes help to send a message from source to destination. Hubs have no predefined topology of the system, two hubs may be or never associated, no fix route between two nodes is use to send message [4]. Network topology may change due to activation and deactivation of the node. If destination node is not in the range of source node, then it passes the message to the nearest node in its range and so on node by node closer to the destination. This system is anything but difficult to execute in any circumstance or any environment like war and catastrophe inclined territories where correspondence is for brief time furthermore, needs rapidly. In such environment, we have less time to actualize the system topology or to make a foundation [5]. At such an area or time this system is extremely helpful to encourage the client to convey.

II. BASIC TERMS USED IN OPPORTUNISTIC NETWORK

A. Nodes

Nodes are the basic component of a network which has the property of receiving and forwarding the message. Nodes are may be fixed or moving depends upon the network. Like a computer with blue tooth, radar, a laptop, a mobile phone etc. when a source node want to send a message to a destination it checks its entire closest node and pass the message to the node which is in its range and closest to the destination [6]. After that next closest node receiving the message and then repeat the above procedure until message not delivered to the correct location.

B. Information Sprinkler

An information sprinkler is a dedicated and a stable node which is fixed in a dedicated location in a cluster of opportunistic network or a stable node is present in every cluster of the opportunistic network [3] Information sprinkler works same as other nodes in opportunistic network it can also forward the message like other intermediate nodes. It uses data sharing protocol

C. Find Opportunity

In this system hubs, can just forward the message when they inspire chance to send it. Opportunity is characterized as the halfway hubs comes in the scope of the hub needs to send the message at exactly that point they can forward the message. A hub needs a neighbor hub which is nearest to it and lies in his range. Presently the message is conveying by the neighbor hub and a similar idea is currently use by the neighbor hub to forward the message thus on till the message is not compasses to the goal hub. At times, the source hub itself likewise motivated chance to forward the

message to the goal, if goal or source hubs change their area and inside the scope of each other.

D. Message Exchange

When two nodes discovered each other successfully then only they can share the message or data [11]. A node can exchange data to its closest node within the direct range. Then nodes pass the data to its closest node and then the next neighbor node store the message and wait for the opportunity to forward the message to next node.

E. Relay Technique/Toplogy

When the source and destination are interconnected by means of some nodes. In such a network the source and destination cannot communicate to each other directly because the distance between the source and destination is greater than the transmission range of both of them [12], hence the need of intermediate node(s) to relay.

III. PROPOSED METHODOLOGY

In opportunistic network, no fixed infrastructure is available and no end to end path is setup between source and destination node to provide communication between them. So, there is no mechanism to find the selfish node [10] which is not interested to forward the message from source node or may edit the original message from source to destination node [7,8]. In opportunistic network message is passes through multiple intermediate node between source and destination node. So, three distinct mechanisms are used to provide a secure communication between source and destination node regardless number of intermediate nodes to be used to delivered a message from source to destination node and vice-versa, three different mechanisms are authentication, using of virtual-ID and relay technique.

A. Authentication

Every node in the opportunistic key has a unique –ID and password which is stored at the stable node in table form. To start the communication, each node needs to get Virtual –ID from the stable node of its cluster. In this simulation set up [13], there are two clusters and each cluster has one stable node. To get the Virtual-ID from the stable node, node needs to provide its unique-ID and password.

B. Using of Virtual-ID

After authentication, and the node is the valid then stable node issue a Virtual-ID of source node and destination node along with secure session key and send it to the source and destination node. The secure session key is used to encrypt the message at the source end and decrypt at the destination node [9]. The Virtual –ID and secure session key is valid for a single session of communication between source and destination node [14]. Whenever a new communication is beginning between two nodes, a new virtual-ID and a secure session key is need to communicate

C. Relay technique

At last relay technique is used to provide communication between source and destination node if both nodes are not within the range of each other. The default range of mobile node to receive and forward the message is 250 meters (in NS 2) but this value can be used by setting value of the receiving threshold (RXThresh_).

IV. SIMULATION SETUP

Network Simulator 2 [16,17] is used to configure the opportunistic network with 13 nodes, the network is divided into two clusters using position based clustering technique [15], having three mobile nodes and two stable nodes and all configuration regarding opportunistic network that is implemented in this research paper are shown on below table 1. The range of mobile nodes to receive and forward the message is 250 meters and stable nodes are directly connected with each other.

In simulation setup, three different simulations are implemented with different numbers of mobile nodes are used to provide the communication between source and destination node and analyze the performance of opportunistic network in different parameters such as throughput, packet loss, delay and privacy. In this section, main idea of enhancement of opportunistic network is shown through figures of simulation.

TABLE I. SIMULATION PARAMETERS

Parameters	**Value**
Terrain Area	800m x 800m
Simulation Time	6 seconds
MAC Type	802.11
Application Traffic	CBR
Routing Protocol	AODV
Data Payload	1000Bytes/Packet
Number of Nodes	13
Number of Sources	1

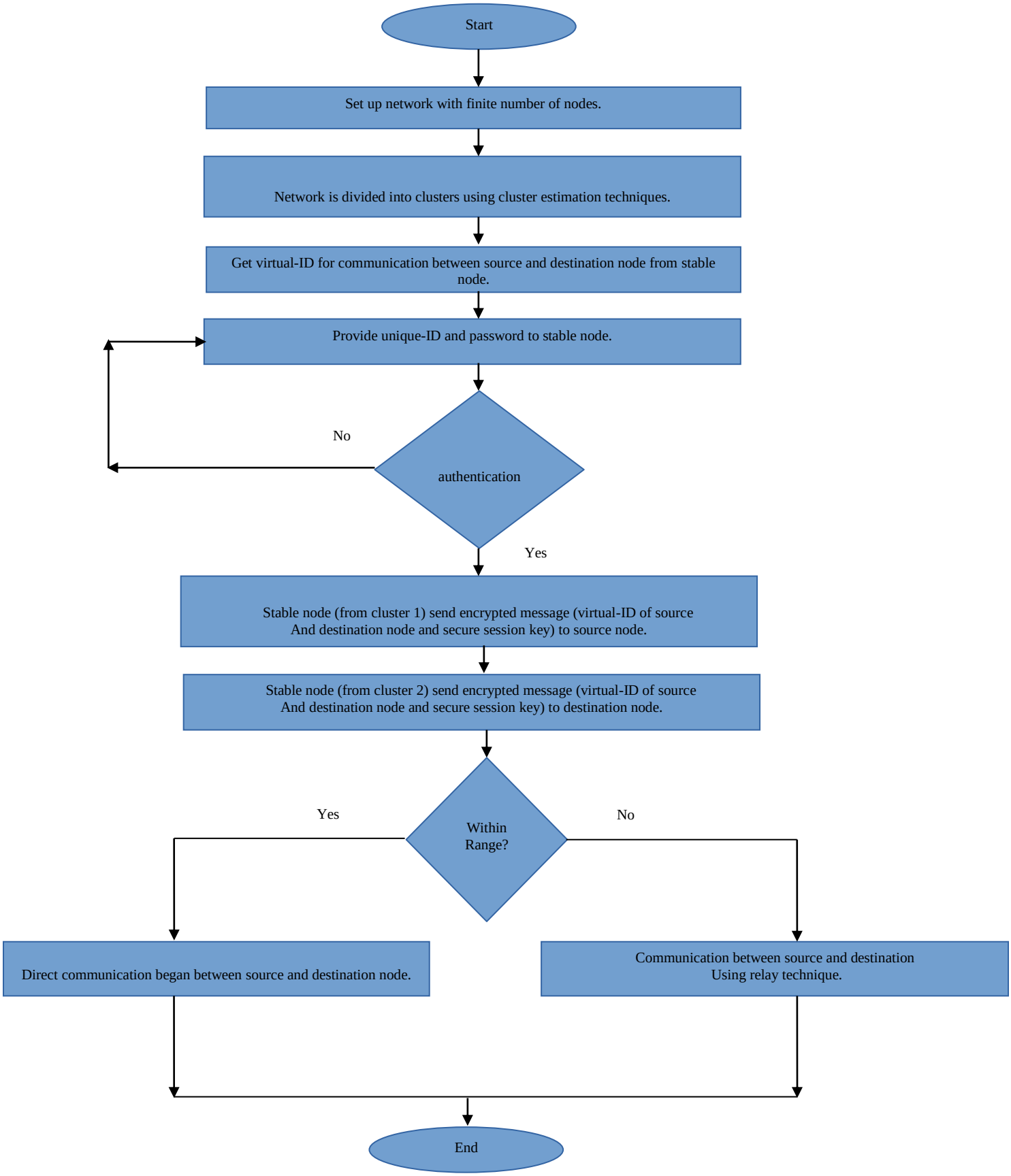

Fig.1. Proposed Methodology.

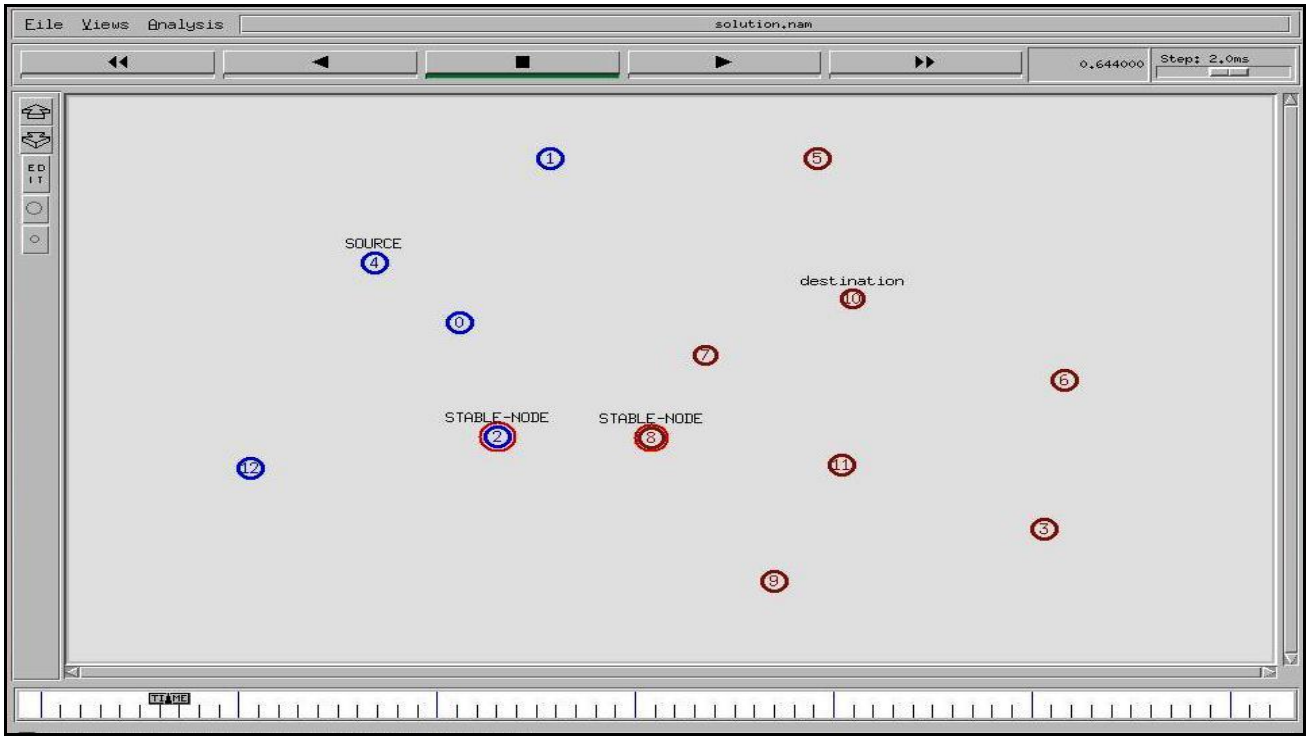

Fig.2. Simulation setup

Above figure demonstrates the simulation setup with 13 hubs along with 2 stable hubs. The opportunistic network is divided into two clusters using position based clustering technique. One cluster with blue color having 5 nodes and node 2 is stable node of this cluster and another cluster having 8 nodes and node 8 is stable node. Node 4 and node 10 are the source and destination node in the opportunistic network.

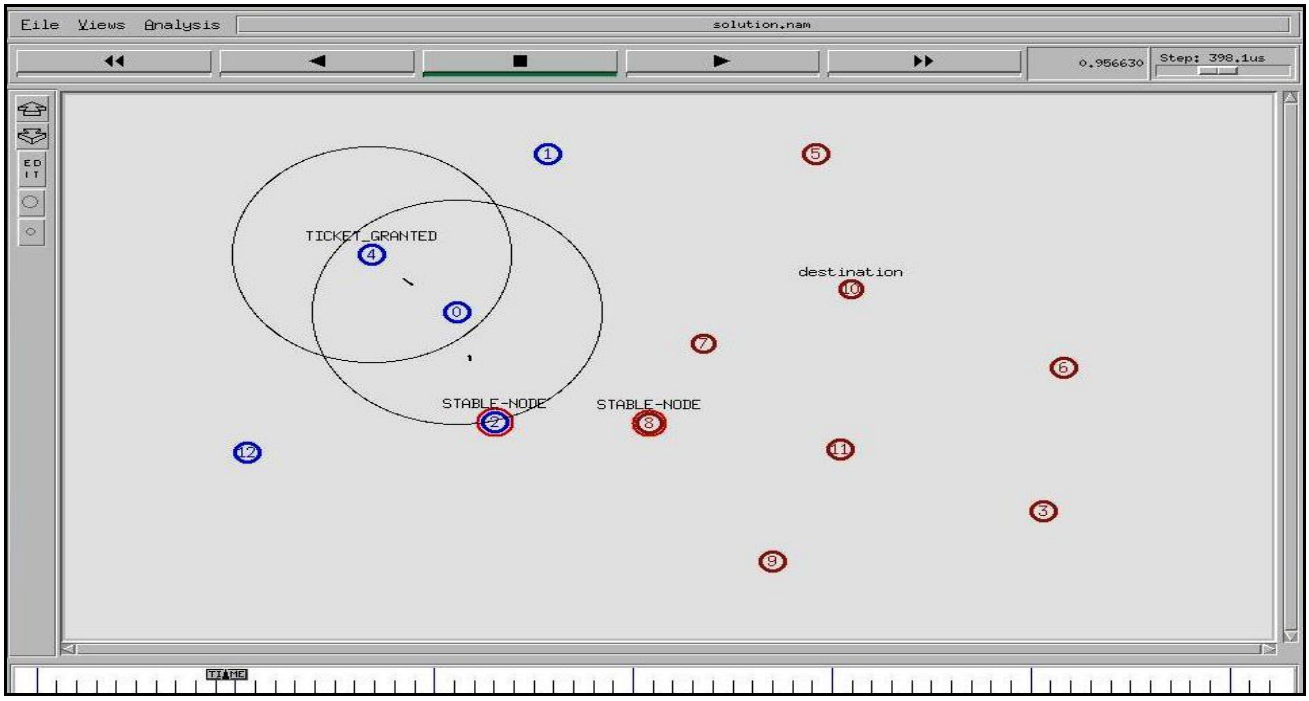

Fig.3. Stable node issued Virtual ID to source node.

In Figure 3, stable node issue virtual ID to the source node and destination node i.e. node 4 and node 10 respectively along with secure session key which is used at source and destination end for encryption and decryption respectively. Before getting virtual ID from the stable node, source node must provide its unique ID and password for authentication.

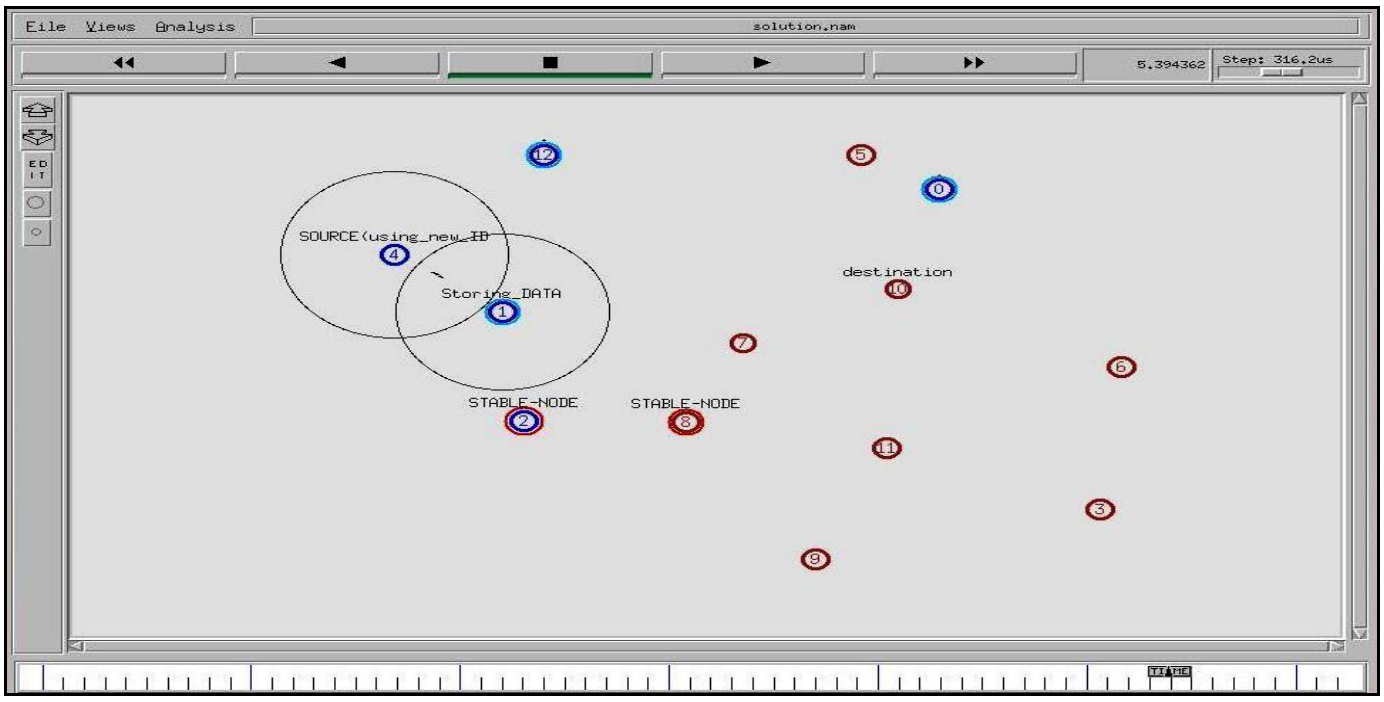

Fig.4. Communication between source and intermediate node using Virtual ID.

In Figure 4, source node start communication with destination node by sending message to the intermediate node by using virtual ID and this message is encrypted with secure session key so intermediate do not understand the message and it simply forward the message to the next node in which its range and this process repeat until the message received by the destination node.

.

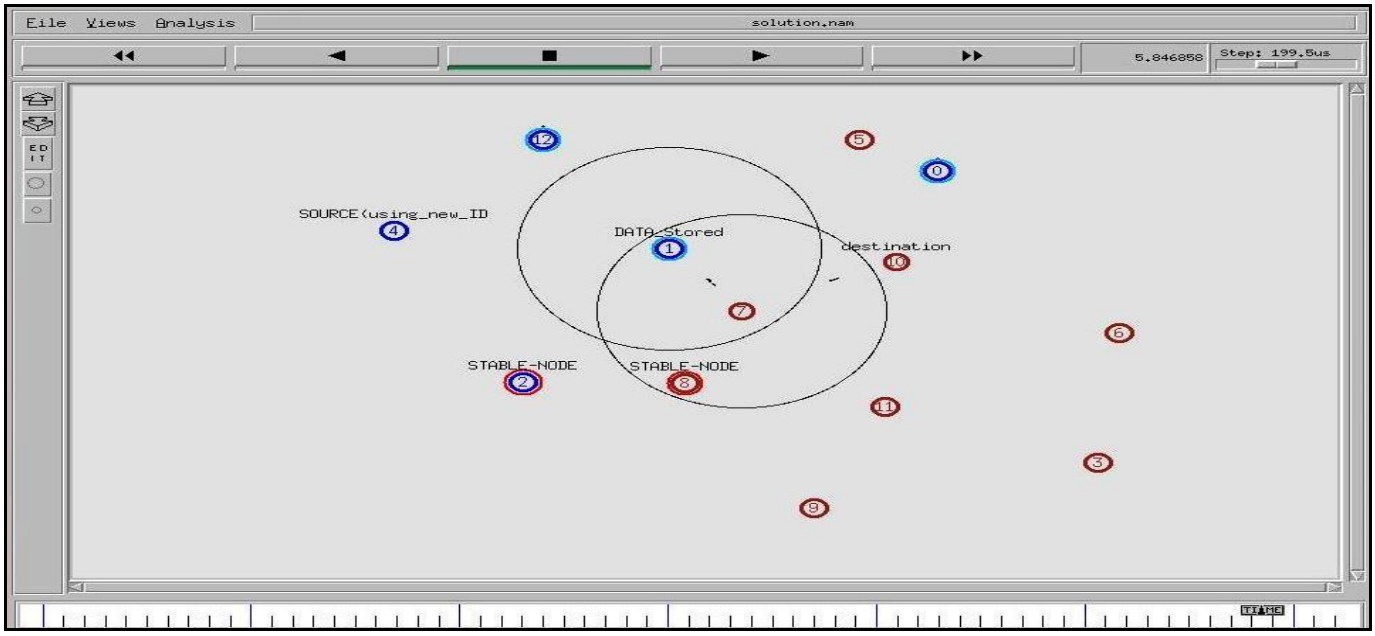

Fig.5. Communication between intermediate node and destination node using Virtual ID.

In Figure 5, the message is received by destination node 10. The message passes through the node 1 and node 7 to provide communication between source node and destination node. In this research paper three different simulations are set up and implemented. In each simulation, different numbers of mobile nodes are used to analyze the performance the performance of opportunistic network in different parameters.

V. SIMULATION RESULTS

In this section, the output of the implementation of enhanced opportunistic network using proposed methodology is shown in the form of graphs. The X axis of graph represent the time of simulation in seconds whereas Y axis of graph represent the number of packets.

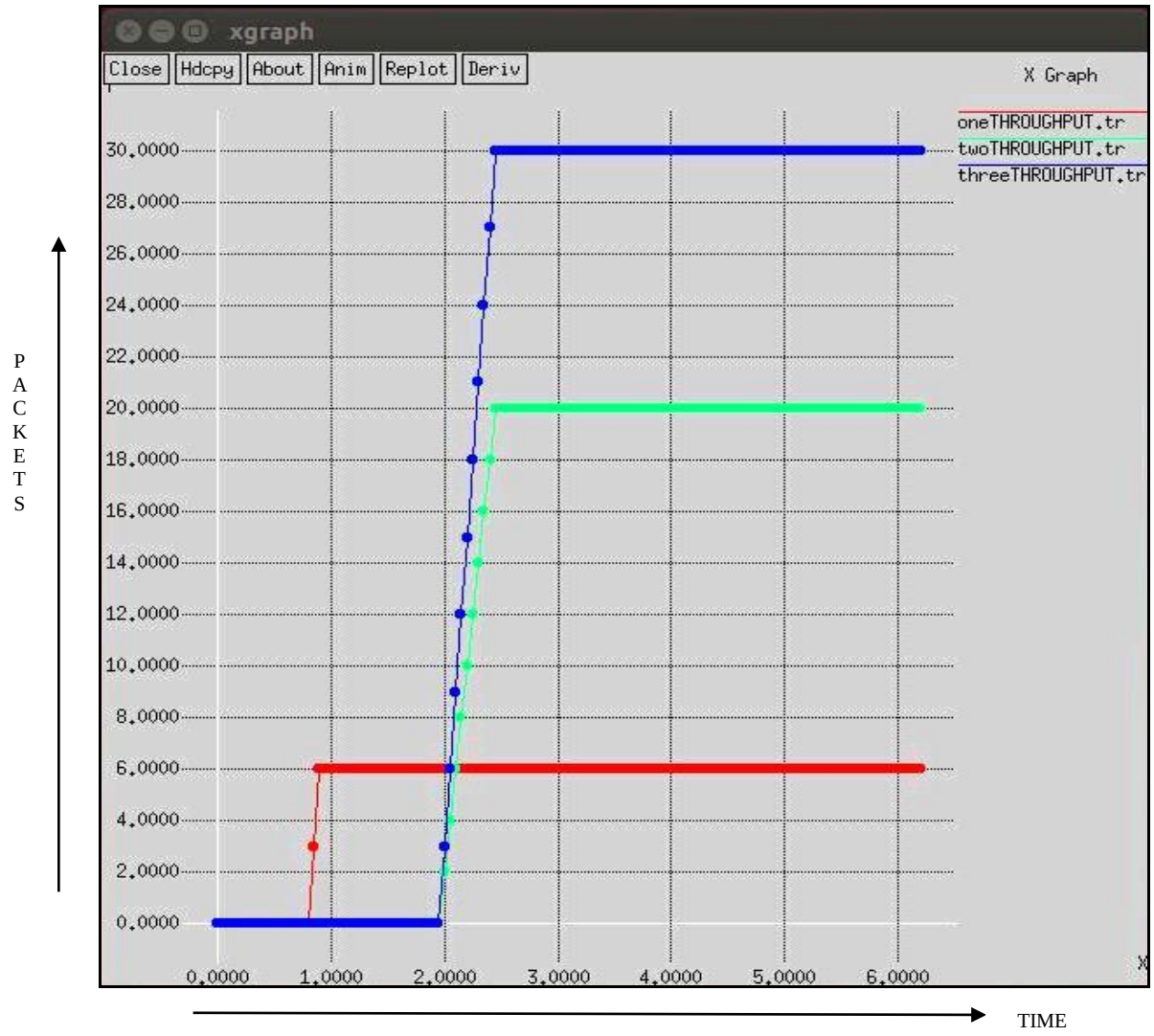

Fig.6. Throughput graph

In above graph (Fig. 6) shows the throughput of enhanced opportunistic network i.e. maximum number of packets successfully received at the destination end in per second [18, 19]. In this research paper the performance of opportunistic network is analyzed through three different cases by taking different number of mobile nodes. In above graph, there are three different outputs for each simulation red, green and blue lines shows the output of first (one mobile node), second (two mobile nodes) and third simulation (three mobile nodes) respectively. In each output the throughput of network is continuously increasing.

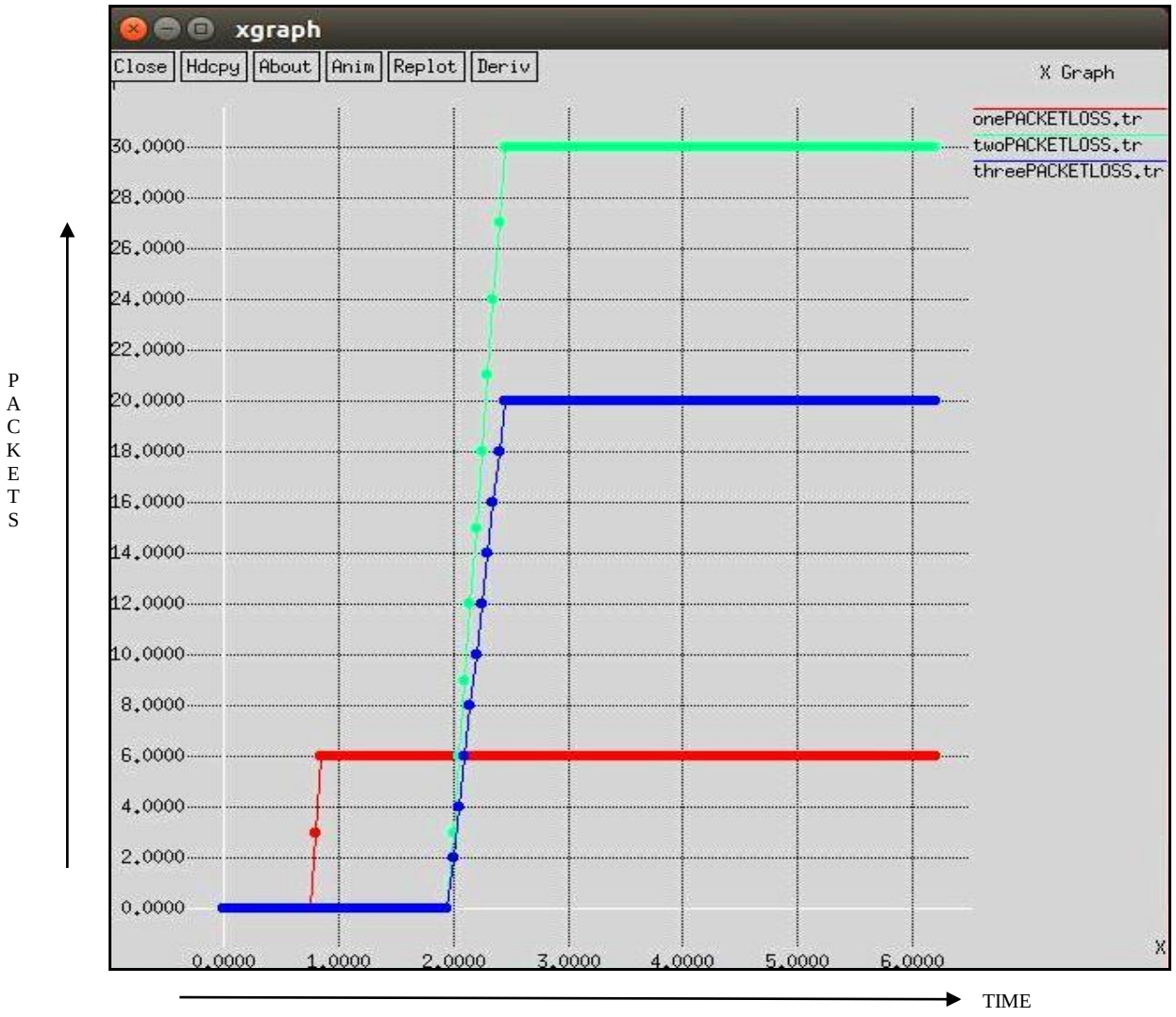

Fig.7. packet loss graph

In above graph (Fig.7) shows the packet loss of enhanced opportunistic network i.e. number of packets are received at the destination end with respect to number of packets are send from the source end [19]. From above graph the packer loss of opportunistic network is decreasing i.e. in first, second and third cases there is 6, 30 and 20 number of packets are loss respectively. In below graph (Fig. 8) shows the delays of enhanced opportunistic network i.e. numbers of packets are delay at the destination end [20]. As there is no fixed infrastructure in opportunistic network i.e. opportunistic network is collection of mobile and stable nodes. So, message is delivered only when there is opportunity in network i.e. when two nodes are within the range of each other, so delay may be high in some cases.

In this research paper, three different techniques namely authentication, virtual-id and relay techniques are used together to improve the performance of opportunistic network. In below table, table II shows the simulation results which depicts that the proposed methodology improving the performance of opportunistic network by increasing throughput and decreasing the packet loss and delay. The proposed methodology is better than traditional methodology [9] in which only relay technique is used to provide communication source and destination node by comparing the results of both methodology, for instance the delay in traditional methodology for single mobile node is 5 packets per second [9] and in proposed methodology the delay for single mobile node is 2 packets per second which shows that proposed methodology is better than traditional methodology. In proposed methodology three different simulations are set up with different number of mobile nodes namely case I, case II and Case III to analyze the performance of opportunistic network while in traditional methodology no such cases are implemented and analyzed.

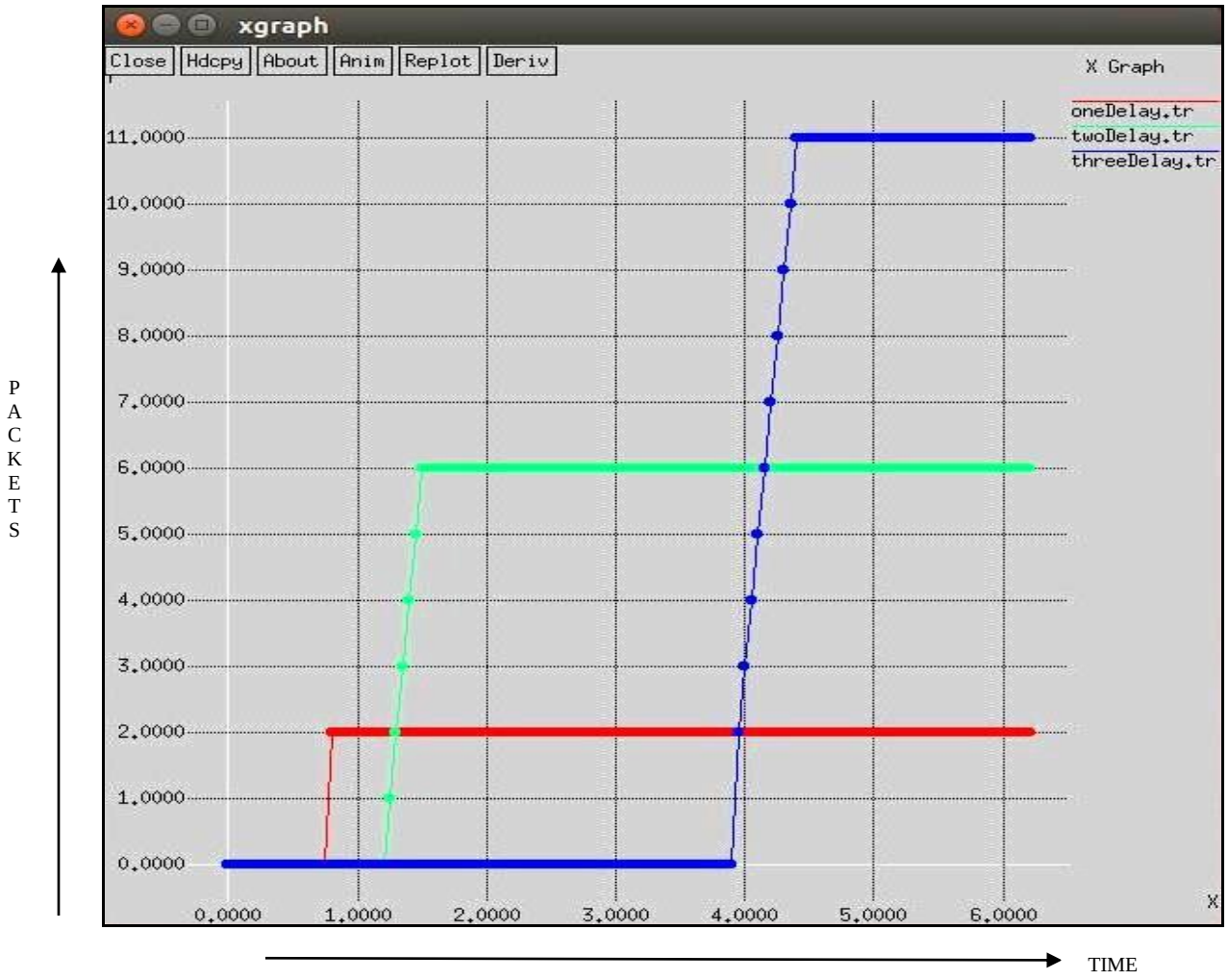

Fig.8. Delay graph

TABLE II. SIMULATION RESULTS

Parameters	**Case I**	**Case II**	**Case III**
Throughput	6	20	30
Packet loss	6	30	20
Delay	2	6	11

VI. CONCLUSIONS

In this research paper, the performance of opportunistic network is enhanced by using proposed methodology, in which three different mechanisms are used such as authentication, virtual ID and relay technique. First network is divided into two clusters using position based clustering. When a node wants to communicate, first it must get virtual ID from its stable node by providing its unique ID and password to the stable node for the valid authentication of node. After authentication, node will get virtual ID from stable node and start its communication with other node by using virtual ID instead of its actual ID, which enhance the privacy of node and provide a secure communication. When source and destination nodes are within the range of each other then they can directly communicate with each other otherwise they communicate by using relay technique. From Simulation results, it shows that proposed methodology is useful in improving the performance of opportunistic network in terms of delay, packet loss and throughput parameters. Along with the performance of opportunistic network, it also enhanced the privacy of user or node.

REFERENCES

[1] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, J. Scott, "Impact of Human Mobility on the Design of Opportunistic Forwarding Algorithms", IEEE Infocom.IEEE Computer Society, 2006.

[2] P. Jan, L. Doboš, A. Čižmar, "Opportunistic Networks and Security," Journal of Electrical and Electronics Engineering, vol. 5(1), pp. 163-166, 2012.

[3] L. Lilien, Z. H. Kamal, V. Bhuse, A. Gupta,"The Concept of Opportunistic Network and their Research Challenges in Privacy and Security," "Mobile and Wireless Network Security and Privacy", Book Chapter, pp. 85-117, 2006.

[4] L. Pelusi, A. Passarella, M. Conti, "Opportunistic Networking: data forwarding in disconnected mobile ad hoc networks", IEEE Communications Magazine, vol. 44(11), 2006.

[5] D. Nain, N. Petigara, H. Balakrishnan, "Integrated Routing and Storage for Messaging Applications in Mobile Ad Hoc Networks", in Proceedings of WiOpt, Autiplis, France, March, 2003.

[6] S. Jain, K. Fall, R. Patra, "Routing in a delay tolerant network," Proceedings of the ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, pp. 145–158, 2004.

[7] A. Shikfa, M. Onen, R. Molva, "Privacy and Confidentiality in context based and epidemic forwarding." Elsevier, pp. 1493-1504, 2010.

[9] S. Bhandari, S. Arora, "Issues of multi-hop relaying in Opportunistic Network," International Journal of Research, vol. 2(10), 2015.

[10] W. Dong, V. Dave, L. Qiu, Y. Zhang, "Secure friend discovery in mobile social networks", Proc. IEEE Infocom, pp. 1647-1655, 2011.

[11] A. Yao, "Protocols for secure computations," Proc. IEEE FOCS, pp. 160-164, 1982.

[8] A. Shikfa, M. Onen, R. Molva, "Local key management in Opportunistic network." International Journal Networks and distributed Systems, vol. 9(1), pp. 97-116, 2012.

[12] B. Poonguzharselvi1, V. Vetriselvi, "Trust Framework for Data Forwarding in opportunistic network Using Mobile Traces," International Journal of Wireless Network, vol.4(6), pp. 115-126, 2012.

[13] K. Fall, "A delay-tolerant network architecture for challenged internets," Paper presented in the proceeding of the ACM Conference on Applications, Technologies, Architecture and Protocols for computer Communications, pp. 27-34, 2013.

[14] S. Bhandari, S. Arora, "Privacy Enhancement of Node in Opportunistic Network by Using Virtual-Id," International Journal on Soft Computing (IJSC), vol.6(4), November 2015.

[15] L. Dora, T. Holczer, "Hide-and-Lie: Enhancing Application-level Privacy in Opportunistic Networks," Proceedings of the Second International Workshop on Mobile Opportunistic Networking (MobiOpp). In ACM, pp.135-142, 2010.

[16] NS-2, The ns Manual (formally known as NS Documentation) available at http: //www. isi.edu/nsnam/ ns/doc.

[17] S. A.Mohammed, S. B. Sadkhan, "Design Of Wireless Network Based On NS2," Journal of Global Research in Computer Science, vol. 3(12), pp. 1-8, 2012.

[18] G. Costantino, F. Martinelli, P. Santi, "Privacy-preserving interest casting in opportunistic networks," IEEE wireless communications and networking conference: mobile and wireless networks, 2012.

[19] Zhang, Y. Zhang, J. Sun, G. Yan, "Fine-grained private matching for proximity-based mobile social networking," Proc. IEEE Infocom, pp. 1969–1977, 2012.

[20] Y. Zheng, X. Xie, W. Ma, "GeoLife: A Collaborative Social Networking Service among User, location and trajectory," IEEE Data Engineering Bulletin, vol. 33(2), pp. 32-40, 2010.