Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.78 – 86

RESEARCH ARTICLE

TO DETECT AND ISOLATE SELECTIVE PACKET DROP ATTACK IN OPPORTUNISTIC TYPES OF NETWORK

Mandeep Kaur[1] (M. Tech Student at Doaba Institute of Engineering and Technology)

Parminder Singh[2] (Assistant Professor at Doaba Institute of Engineering and Technology)

[1]CSE & PTU, India

[2]ECE & PTU, India

[1] saroamandeep1@gmail.com; [2] parminder.db@gmail.com

Abstract: ***Nodes in MANETs are mobile, so they can change their location according to their requirements. Hence no fixed infrastructure is present in this network. It has one Sub category also known as opportunistic network networks. All nodes work on store and carry Scheme in it. Opportunistic network has some security and privacy issues. Malicious node can easily trigger attacks on this network. In this paper, our main aim is to ensure privacy. In this work, a network architecture is proposed in which a node want to send a message to a destination and it doesn't want to explore its identity as well as destination identity then it first communicate with stable node(trusted node) and get a virtual id for a period a time. Stable node act as special node, which contains information of every node of the cluster and authenticate the nodes who wishes to communicate and provide virtual id to that nodes. And also a session key is provided for encryption of message to the source and decryption key to the destination for maintaining the confidentiality of the message. This approach provides privacy to the user and reduces the packet loss by a selfish node. The graphs represent the change in packet loss and throughput of opportunistic network.***

Keywords: MANET, Selective Packet Attack and store-carry scheme.

I. Introduction

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of wireless mobile devices. Nodes are connected wirelessly and also responsible for data forwarding (no data transfer or routing device is present i.e. router, switch). Opportunistic Network is sub category of MANET. Opportunistic network is typically wireless. Nodes are typically hand held devices carried by people. No infrastructure is required. Nodes communicate directly with each other. Nodes have no predefine topology of the network, two nodes might be or never connected, no fix route between two nodes is used to send message. 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 network is very easy to implement in any situation or any environment like war and disaster prone areas where communication is for

short time and needs very quickly. In such environment we have less time to implement the network topology or to make an infrastructure. At such a location or time this network is very useful to facilitate the user to communicate.

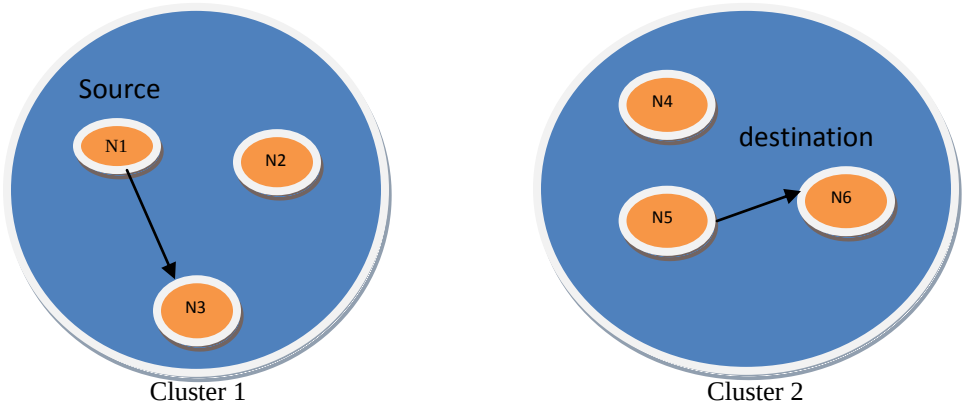

Fig 1.1 Opportunistic networks

In Opportunistic network, network is divided into clusters. Each node can communicate with each other and node in other cluster through intermediate nodes (nearby nodes). In above diagram there is node N1 which is source node and node N6 which is destination node. Node N1 will forward message to nearby intermediate node N3. Now node N3 will move and forward message to the nearest node N5 in other cluster. Node N5 will forward the message to destination node.

II. Review of Literature

Jia Jianbin (2013) introduced about Hop count is an important parameter for routing strategies in wireless network. Particularly in the opportunistic networks, due to the intermittent connectivity between mobile nodes, it imposes great impact on the delivery performance in terms of delivery ratio and average latency. They established a framework to analyze opportunistic multi-hop relaying benefit based on the concept of Good Relay Ratio (GRR), and discussed the factors that impact max-benefit hop count in three typical multi-hop forms. Finally, they make a set of realistic trace-driven simulation to verify the analytical results. It is expected that the framework and result implications are meaningful to the routing strategy design in opportunistic networking.[1] **G. Costantino, Fabio Martinelli, Paolo Santi (2012)** found that Message forwarding is a fundamental brick to spread information among users in opportunistic networks. In this report, they consider the recently proposed interest-casting networking primitive for opportunistic networks, in this a packet generated by a sender should be delivered to all users in the network – potentially unknown to the sender same interest in that. However, the implementation which is used now is of interest-casting assume from users to make forward decision they have to exchange their interest profile, which is very sensitive information of user and not forward to strangers, that's why they mention a technique and proposes an easy way of message sharing between users interested in same subject or topic. However, it is implicitly based on a fully trusted network, even if a malicious node can be completely trusted.[2] **Iain parris and Tristan Henderson (2011)** assimilate the knowledge about the new communication paradigm in which whenever user comes into contact with each other, their device which is able to communicate wirelessly to send or receive message. They find that users in opportunistic network may have privacy concern like confidentiality of the transmitted message, or disclosure of their privacy information.[4] **M.Erdogan (2010)** proposes a new routing approach for opportunistic network called p% partial flooding algorithm. As flooding it is possible to find a best path to reach the destination with minimum number of hop count and end to end delay, but this algorithm have a big disadvantage because it uses the network resources in excessive manner as all nodes are try to forward a single packet of message.[6] With the proposed algorithm they focus to decrease the traffic over the network by randomly select a neighbor node.**L. Dora and T. Holczer (2010)** find in their research that delay tolerance network and mobile ad hoc network are same or we say that DTN is MANET. In both network message is send by same principal store carry and forward and raises

new aspects of the privacy problem. Such as an attacker can build a fake user identity and trace the nodes. In their study they present an attacker model and some proposed attackers are implemented and then analyze both attack and there efficiency and propose a new method or defence mechanism called hide n lie strategy. They show that without any defence mechanism, the nodes are traceable that is a risk to the privacy of nodes but with the technique they purpose, the success of finding a node in network is equal to find a node by an attacker. Sometimes their Strategy increases the message delivery ratio. **I. Parris (2010)** presents two new schemes for enhancing privacy in social network routing in opportunistic network. They demonstrate that boom filter can prevent eavesdropping of social network by making very small effect on the network performance. Also they find that there is a possibility to carry on the sender's social network by removing 60% of the node from social network, a delivery ratio is still maintaining up to 90% of unaltered social network routing. They evaluate these schemes in real world and both are adopted by the network.[8]

III. Selective packet drop attack in opportunistic network

In this method the network is initialized with the finite number of nodes, the network is divided into two clusters. Every node has a range in which they can communicate with other nodes. All nodes are mobile and can change their location except stable node. But for the implementation only one node is made mobile and others are made fixed (they are mobile in reality). The ID of each node is exposed. If any node in one cluster wants to send data to the node in another cluster then it will have to send request to the stable node. Stable node will forward data to mobile node in its range. Now the mobile node will move towards other cluster, if it found the node nearby it (in its range) which can forward data to the destination, then it will forward data to that node which will further forward data to the destination node. As the network ID of every node is exposed, the mobile node which knows the ID of every other node can become malicious for some nodes whose data it don't want to forward. It will become malicious for that node and will not forward its data and will start dropping the data packets. Due to which the sender node can lost its important data which is dropped by the malicious node. This is called selective packet drop attack.

IV. Problem Formulation

The aim of the implementing privacy in the opportunistic network is to attract more users to use this network. As privacy is the main concern and in this network there is not a fixed infrastructure is present and the message is forward through many intermediate nodes, there may be a selfish node which is not interesting to forward the message to a particular destination, or the user doesn't want to show his identity when want to communicate or send message to a particular destination, then it is risk to the privacy of user or the packet dropped by the selfish node. Also the content of message is also access by the intermediate nodes, so there is a problem that how to encrypt the message and share a key between source and destination without showing it to intermediate nodes.

Algorithm

1) The network is initialized with the finite number of nodes.
   Take 13 nodes in this implementation. Every node has a range in which they can communicate with other nodes. All nodes are mobile and can change their location except stable node. In this implementation we show only one node which can move. Other nodes are fixed (only for implementation they are mobile in real time)
2) The whole network is divided into clusters
   Network of 13 nodes are divided into 2 clusters. Every cluster has a stable node which is directly connected with the stable node of other cluster.
3) In each cluster one fixed node is defined
   In every cluster there is a fixed node called stable node or sprinkler node. Features of this node is same as the other node it also transfer a message only when other nodes comes in his communication range.
4) In fixed node database is maintained and ID of each node and password is stored Stable node also maintained a table in his database, in which password is stored with the respective ID of a node.
   Stable node uses this table to authenticate the node. Table also contains many more columns like session key column, virtual id of source, Virtual Id of destination and etc.
5) The node which wants to communicate to the other node will first communicate with the fixed node to get the virtual ID

When a node wants to send message, it first sends a request message to the stable node to get a virtual ID. This message is forward by the intermediate nodes to the stable node.

6) The source node send its credentials (USER_NAME & PASSWORD) which authenticate the valid node of group and also with which node it want to communicate) to the fixed node

In the request message source node send its USER_NAME & PASSWORD which is use by the stable node to authenticate the valid user of the cluster. The source node also sends the destination node ID to whom it want to send the message. This message is encrypted by the public key of stable node which is shown to all nodes.

7) When fixed node verifies the credentials ,fixed node communicate with the stable node of the cluster in which destination is present and will send the virtual ID's of the source and destination , to the source node + the secure session key.

Once the source node authenticates the user then stable node communicate with the stable node of destination cluster and exchange information and update their table. Now stable node of source cluster will sends a new virtual ID to the source , new ID of destination and a session key with which the source node encrypt the message. This message is now encrypt by the public key of the source node. And stable node also sends a new virtual ID to the destination, virtual id of source node and session decryption key. This message is encrypted by the public key of destination node.

8) Source node now send message with new ID and encrypt the message with session key.

Flow Chart:

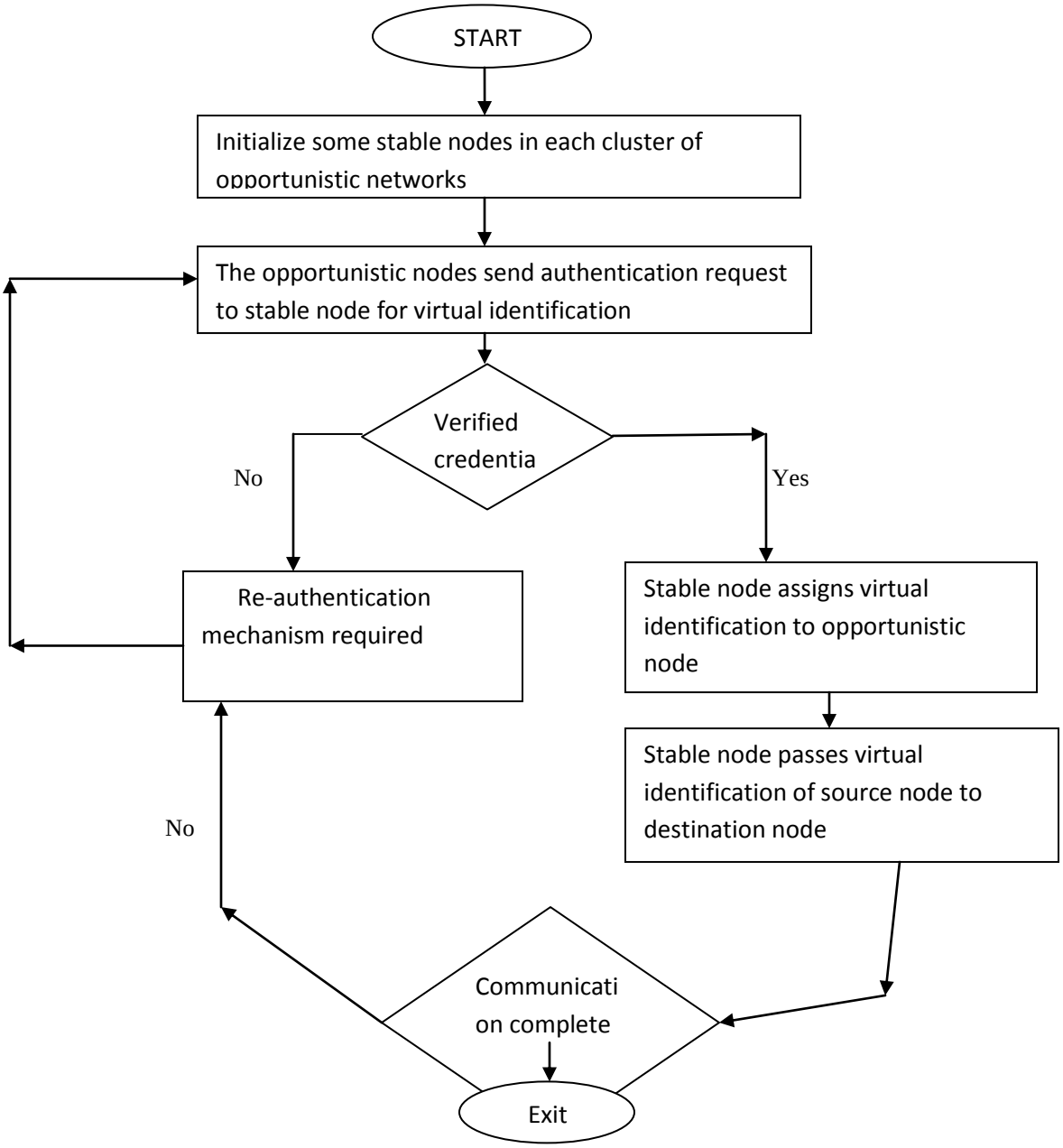

Figure 1.2 Flow Chart for the Algorithm

V. Experimental Results

The proposed network and the privacy based methodology are implemented in NS 2.35. NS (network simulator) environment is one such facility which lends a high performance language for technical computing. It uses the standard of network and show like actual outputs.

Comparison of both techniques in term of packet loss

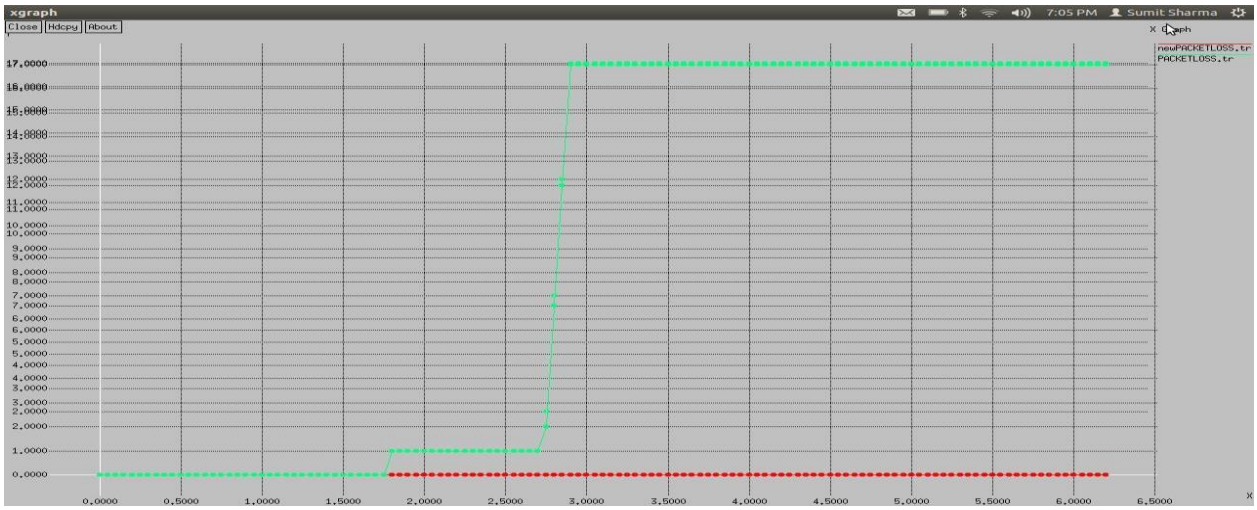

Figure 1.3 Comparison graph of old and new Packet loss

- Graph is plotted between the number of packet (y-axis) and the time (x-axis).
- Green line shows the packet loss by the previous method.
- Red line shows the packet loss by proposed algorithm.

Comparison of both methods in the form of throughput

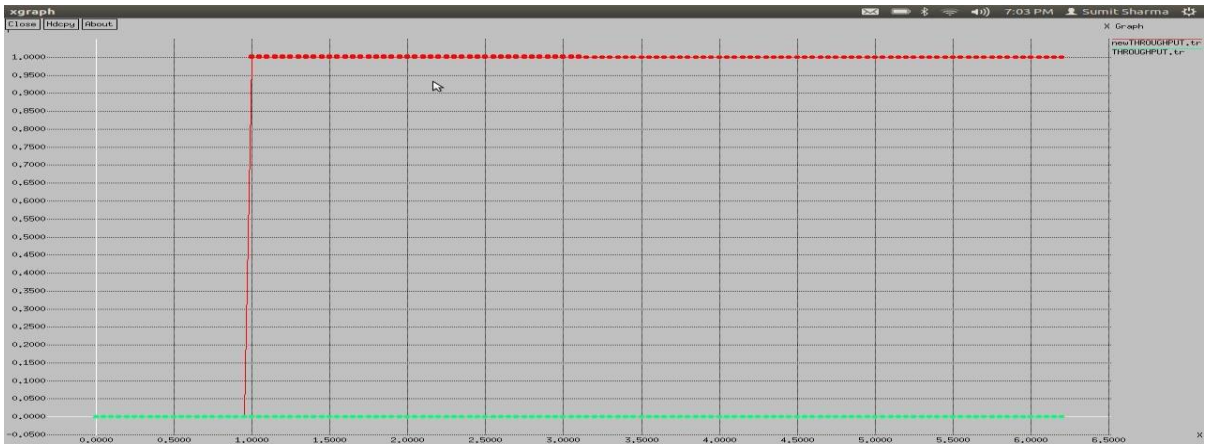

Figure 1.4 Comparison graph of old and new Throughput graph

- Red line shows throughput by net algorithm
- Green line show throughput by previous algorithm
- Throughput is lies between 0 and 1 along y-axis
- Time along x-axis

Comparison of both methods in the form of Energy loss

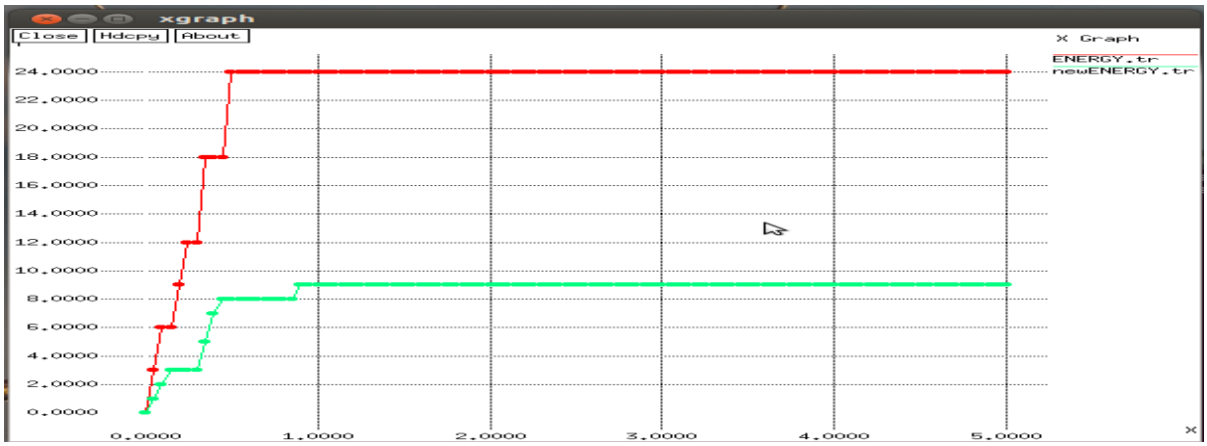

Figure 1.5 Comparison graph of old and new Energy loss graph

- Red line shows energy loss by previous algorithm
- Green line show energy loss by net algorithm
- Energy loss lies between 0 and 1 along y-axis
- Time along x-axis

Comparison of both methods in the form of Response time

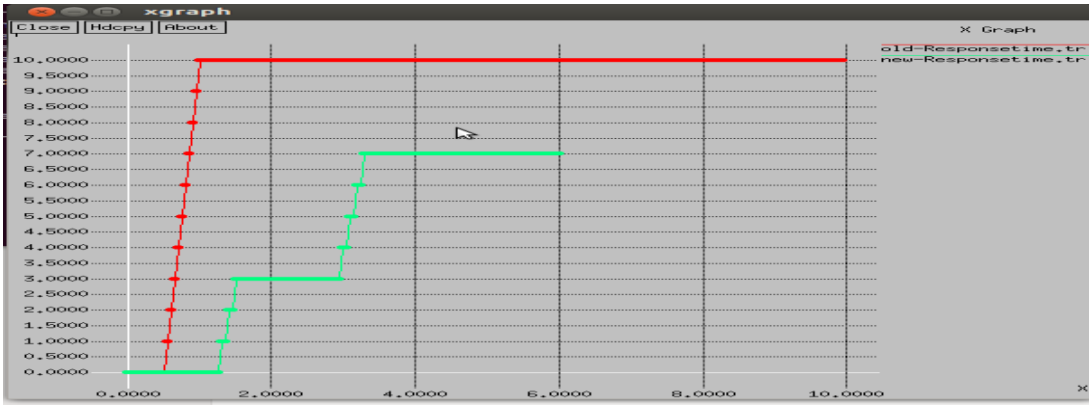

Figure 4.21 Comparison graph of old and new Response time graph

- Red line shows response time by previous algorithm
- Green line show response time by net algorithm
- Response time lies between 0 and 1 along y-axis
- Time along x-axis

Comparison of both methods in the form of Message exchange

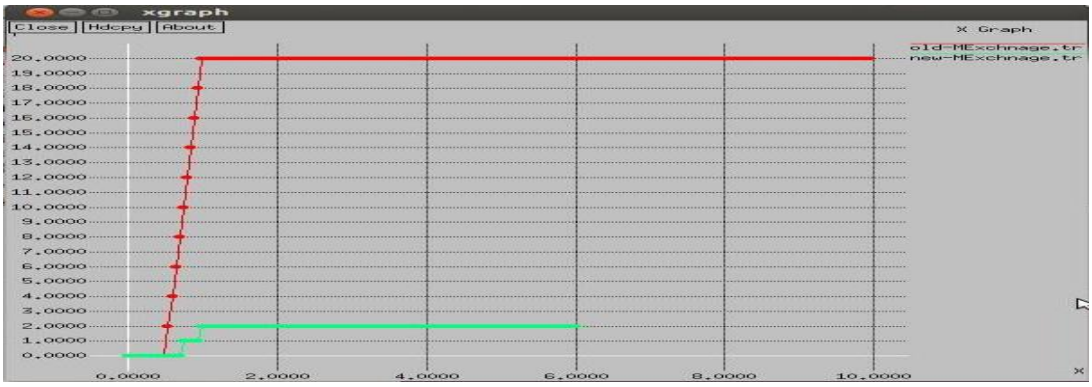

Figure 4.22 Comparison graph of old and new Message Exchange graph

- Red line shows message exchange by previous algorithm
- Green line show message exchange by net algorithm
- Message exchange lies between 0 and 1 along y-axis
- Time along x-axis

Conclusion

In this research we find that opportunistic network is very useful if privacy is maintained. In this work, a network architecture is proposed in which a node want to send a message to a destination and he doesn't want to explore its identity as well as destination identity then it first communicate with stable node(trusted node) and get a virtual id for a period of a time. Stable node act as special node, which contains information of every node of the cluster and authenticate the nodes who wishes to communicate and provide virtual id to that nodes. And also a session key is provided for encryption of message to the source and decryption key to the destination for maintaining the confidentiality of the message. This approach provides privacy to the user and reduces the packet loss by a selfish node. And the graphs represent the change in packet loss and throughput of opportunistic network.

References

[1] Jia Jianbin, Chen Yingwen, Xu Ming, Xia Geming, and Xiao Xiaoqiang, "Towards the Benefit of Multi-Hop Relaying in Opportunistic Networking", IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing 2013

[2] G. Costantino, Gianpiero, Fabio Martinelli, and Paolo Santi. "Privacy-preserving interest-casting in opportunistic networks." Wireless Communications and Networking Conference (WCNC), 2012 IEEE. IEEE, 2012.

[3] Xie, Xingguang, et al. "Social relationship enhanced predicable routing in opportunistic network." Mobile Ad-hoc and Sensor Networks (MSN), 2011 Seventh International Conference on. IEEE, 2011.

[4] I. Parris, Iain, and Tristan Henderson. "The impact of location privacy on opportunistic networks." World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a. IEEE, 2011.

[5] Verma, Anshul, and Dr Srivastava. "Integrated routing protocol for opportunistic networks." arXiv preprint arXiv:1204.1658 (2012).

[6] Erdogan, Mustafa, et al. "Routing with (p-percent) partial flooding for opportunistic networks." Future Network and Mobile Summit, 2010. IEEE, 2010.

[7] 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, February 2010 pages 135-142.

[8] Parris, Iain, Greg Bigwood, and Tristan Henderson. "Privacy-enhanced social network routing in opportunistic networks." Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on. IEEE, 2010.

[9] I.Parris.," Privacy enhanced opportunistic networks.**"** Proceedings of the Second International Workshop on Mobile Opportunistic Networking (MobiOpp), pages 213–214, Pisa, Italy, February 2010. ACM Press. Extended abstract. DOI: 10.1145/1755743.1755794

[10] A.Chaintreau, A. Mtibaa, L. Massoulie, and C. Diot. ―Diameter of opportunistic mobile networks‖. In Proceedings of ACM Sigcomm CoNext, December 2007. also available as Thomson technical report CR-PRL-2007-07-0001.

[11] Boldrini, Chiara, Marco Conti, and Andrea Passarella. "Impact of social mobility on routing protocols for opportunistic networks." World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a. IEEE, 2007.

[12] W. Li and A. Joshi,‖ Security Issues in Mobile Ad Hoc Networks- A Survey‖ Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County.

[13] L. Pelusi, A. Passarella, and M. Conti, ―Opportunistic Networking: data forwarding in disconnected mobile ad hoc networks,‖ IEEE Communications Magazine, vol. 44, no. 11, Nov. 2006.

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

[15] PAPAJ Jan, DOBOS Eubomir, CUMAR,‖ Opportunistic Networks and Security" Journal of Electrical and Electronics Engineering- Volume 5, Number 1, May 2012

Authors' Profile

Author 1: (Mandeep Kaur) Presently Ms. Mandeep kaur is working as a Lecturer in SBSSMK College Nurpur Bedi , Ropar.

Author 2: (Parminder Singh) Presently Mr. Parminder Singh is working as an Asst.Prof in ECE. Dept, Doaba Institute of Engineering & Technology, Kharar.

