Design of trust model based on ideas of Localization in opportunistic networks

Mr. Ravinder Singh

Abstract— Opportunistic networks are used in the remote, disaster prone areas where there is no network between the users and to create a network without any relation between nodes. In this paper we are creating a trust scenario for Opportunistic networks that is based on the methods of localization.
We are proposing a model to overcome issues regarding opportunistic network nodes mobility, storage and security. The model is a layered approach that needs input of one and output to other and a trusted node is implemented that can overcome the opportunistic network problem and provides optimal performance of the system.

Index Terms— Black Node, Mobilityof nodes, Manet, Opportunistic Networks, Store-Carry-Forward, Trust Model, Trusted Node

1 INTRODUCTION

During the few years researches on ad hoc networks has focused on a large number of applications. Originally working for military applications, and aimed at improving communication and disaster prone areas multi-hop ad hoc networks have largely been proposed in many scenarios.

In this paper we will study on Opportunistic Networks and focus on the security and trust model for opportunistic network that are based on localization based methods of Opportunistic network.

TRUST – According to this paper, trust is a level of approach in which the problems regarding the opportunistic network will be eliminated and the communication between nodes is in trusted manner.

Opportunistic network are a subclass of Delay-Tolerant Network where communication opportunities (contacts) are intermittent, so end-to-end path between the source and the destination may never be stationary or fixed. The link performances in opportunistic networks are typically variable or extreme. Long propagation and varying queuing of delays might be introduced and many protocols are designed to assume. One can exploit mobility of nodes and local forwarding in order to data transfer. Data that can be stored and carried by taking advantageous steps of node mobility and then forward during opportunistic contacts. In its entire chunks of message are transferred from a storage place to other storage place in another node along with a path that is expected to access the destination. Oppnets networks are different from many typical networks, in which the working nodes are all deployed together, it self-reconfigures itself, and then works to detect all “foreign” devices or systems that are using all kinds of communication media i.e. Bluetooth, wired Internet, Wi-Fi, RFID and satellite etc. At this stage Oppnets starts working differently from typical and traditional networks.

Oppnets is a collection of communication devices or nodes that can communicate without any fixed infrastructure and pre-determined organization for the available links.

1. Oppnets, also known for any **path routing**, they are characterized as one of the necessary evolution of traditional MANET with wireless networks properties.
2. Oppnets consists of human carried mobile (nodes) that communicate with each other having no physical infrastructure.
3. Each node have limited storage and limited power to work upon.
4. Oppnets are more general than MANETs, because it works over the dissemination communication rather than conversational communication.
5. Oppnets are created by individual nodes. All stations can be easily disconnected for some time intervals, and that opportunistically exploits any contact with other station to forward messages.

The messages and all communication is done "store-carry-forward" model

In order to provide the effective communication between nodes, there is a necessary step to consider different aspects. The concept of mobility in Oppnets is to provide effective communication between unconnected groups of stations.

In this research discussing the security issues related to Black nodes and will shortly bring the mobility ideas in Oppnets with main interest of maintaining an optimal approach on routing and forwarding mechanism and want to work on trust model to evaluate neighbours forwarding behaviour, security and storage performance and to apply this model to opportunistic routing in order to provide the secured transmission of data.

2 LITERATURE REVIEW

A. Opportunistic Networks and Security

The opportunistic networks (Oppnets) are the most challenging evolution of Mobile Ad - Hoc Networks (MANET). Oppnets provides a feature to communicate between two devices in offline modes also by opportunistically selection any nearby device to move messages closer to the final nodes. So taking this point in knowledge security enhancement is necessary. [16]The securing the network is very important part of research. In this article basic security issues are introduced, described and there formally explains basic security mechanisms and algorithms.

B. Survey of Opportunistic Networks

This article defines opportunistic network as one type of challenged networks where network connections are independent and where performance of links are highly variable and extreme. In this type of network, there does not exist any complete path from source node to destination node for maximum period of the time. In addition, it path is highly unstable and can change or break quickly [3]. So, in order to communication possibly in an opportunistic network, the intermediate nodes may take supervision of data during the blackout, bottlenecks and forward it when the connectivity reconfigures. In this paper, they discuss some research challenges in an opportunistic network.

C. Opportunistic Networks: The Concept and Research Challenges in Privacy and Security

In this research paper they introduced a new technology, which they call opportunistic networks or Oppnets. An oppnet grows from its base the, real couple of nodes employed together at the time of the initial oppnet deployment. The base concept formulates into a larger network by enhancing invitations to join the oppnet to foreign devices, node clusters and typical networks that it is able to contact. A new node that becomes a fully-verified member, or helper, is allowed to invite outer nodes[13].

D. Routing techniques for Opportunistic Networks and Security Issues

Opportunistic networking has considerable interest from the research scenario in few years. In opportunistic networks, mobile nodes are able to communicate with one another even if a route connecting each of them never exists. An oppnet grows from its base to the original set of nodes employed together at the time of the initial stage. The formulation base grows into a larger network by extending invitations to join the oppnet to foreign stations, nodes, or networks that it is able to join. The design methodology of reliable routing techniques for opportunistic networks is usually a big challenge. In this paper, they survey the various routing algorithms for the opportunistic networks as well as they discuss the security aspect for the opportunistic networks [10].

3 PROBLEM FORMULATIONS

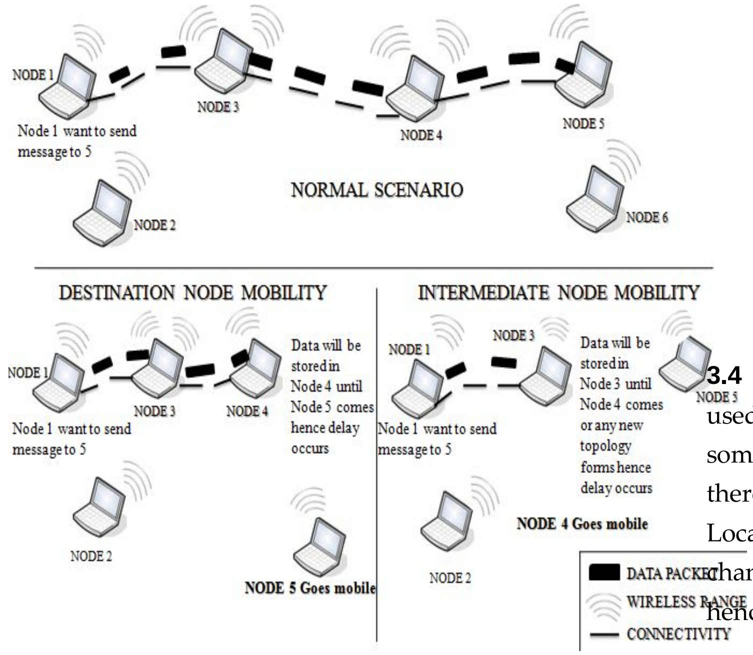
Opportunistic network have many problems when working over it but the main problems on which this paper is emphasized are the following:

3.1 Mobility – As the nodes in opportunistic network are not Stationary and are mobile with in a fixed range of network. But as the nodes are mobile by nature so can move at any point of time out of network or change the topology [16].

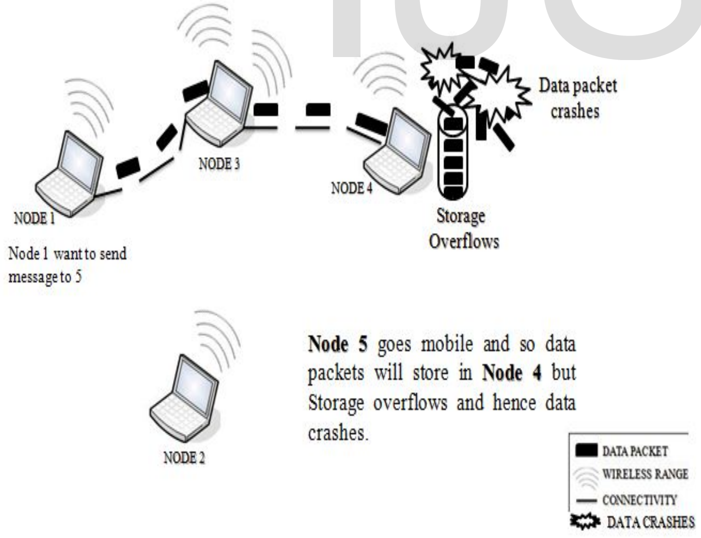
It also increase the time of receiving the message to destination, hence increases delay.

A. DESTINATION NODE MOBILITY – Taking in consideration of issue in which the destination node moves from the network and message in not delivered to it until it comes to the range of other node.

B. INTERMEDIATE NODE MOBILITY – Taking in consideration of issue in which the intermediate node goes mobile and hence due to which message is not reached to destination, delay occurs until intermediate nodes comes back to the network.


NODE 1
NODE 3
NODE 4
NODE 5
Node 1 want to send message to 5
NORMAL SCENARIO
NODE 2
NODE 6
DESTINATION NODE MOBILITY
INTERMEDIATE NODE MOBILITY
NODE 1
NODE 3
NODE 4
Data will be stored in Node 4 until Node 5 comes hence delay occurs
Node 1 want to send message to 5
NODE 2
NODE 5 Goes mobile
NODE 1
NODE 3
Data will be stored in Node 3 until Node 4 comes or any new topology forms hence delay occurs
NODE 5
Node 1 want to send message to 5
NODE 2
NODE 4 Goes mobile
DATA PACKET
WIRELESS RANGE
CONNECTIVITY

3.2 Storage – As when any node goes mobile from the network the message is kept to the node before it and the message will be transferred to node later when node comes back. During such time there occurs issue of storage on nodes. It is very difficult to predict that how much storage space each node needs to overcome the problem of memory overflow[3].


Data packet crashes
NODE 3
NODE 4
NODE 1
Node 1 want to send message to 5
Storage Overflows
Node 5 goes mobile and so data packets will store in Node 4 but Storage overflows and hence data crashes.
NODE 2
DATA PACKET
WIRELESS RANGE
CONNECTIVITY
DATA CRASHES

3.3 Security – As the nodes are intermittent so there is a issue that how can we trust on the nodes to work on the mechanism of forward message from intermediate nodes until it reaches destination[16].

A. BLACK NODE – As nodes are mobile that message is forwarded in the manner of Store-Carry-Forward manner which shows a problem that if any Malicious node out of network hack any of intermediate node and gains the identity of intermediate node then no one can find out that it was the BLACK NODE and hence intruding the messages forwarded from it .

B. MESSAGE PRIVACY – Message that is transferring between nodes is not secured and can be intruded or hacked by any node within the network.

3.4 Network struck – As the opportunistic network is mainly used in War- prone area, So there occurs a chance that due to some reasons whole network goes down or struck badly so there is a need to overcome such a big problem.

Localization based methods – This paper will emphasis on the changing locations of nodes in opportunistic networks and hence purposes a mechanism to overcome such problem.

4 RESEARCH METHODOLOGY

Based on the problems, in this paper a methodology is defined by which above problem eradicates.

Considering a network scenario of nodes that are in a network of each other, each node having a limited storage and energy .

But there is a node named TRUSTED node is a node in the network which will be in a range of all nodes and this node have more storage space and energy(battery life) than that of other nodes and all issues will be overcome by TRUSTED NODE.

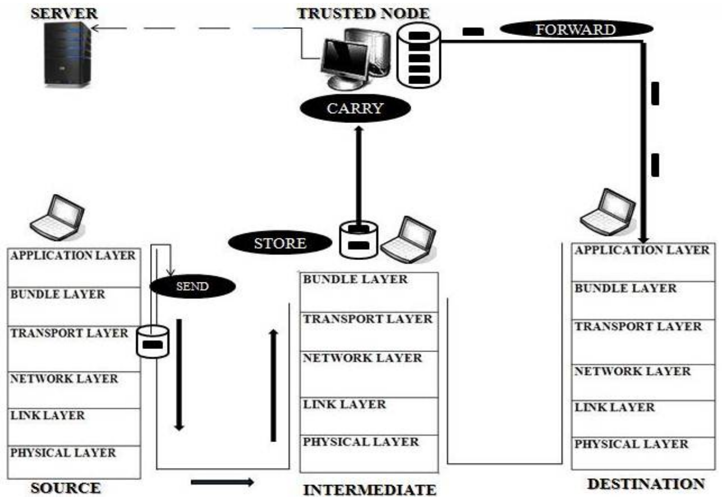
4.1 For Mobility Issue –

A. DESTINATION NODE MOBILITY

When nodes are interconnected with each other Data will be transferred in the manner of Store-Carry-Forward. When a scenario occurs that destination node is not in the range of the other nodes. At that point of time the message from last node from network (the node that was near to connect the destination) will transfer the message to trust node and the last node will delete it from it buffer. Hence when the destination node will come back the message will be transferred to it from the trusted node directly. By this node may be anywhere due to mobility and can come at any time will able to receive the message.

B. INTERMEDIATE NODE MOBILITY

When data is being transferred from source to destination then it has to be forwarded from many intermediate nodes. Taking in consideration of a scenario in which intermediate node is down or intermediate node move out of range from connected nodes and hence breaking the topology , in such a condition message forwarded to last node will check that next hop is not there to forward message and it does not find any other node to transfer message . so it will transfer the message to trusted node and then trusted node will send the message to destination directly.



4.2 For Storage Issue –

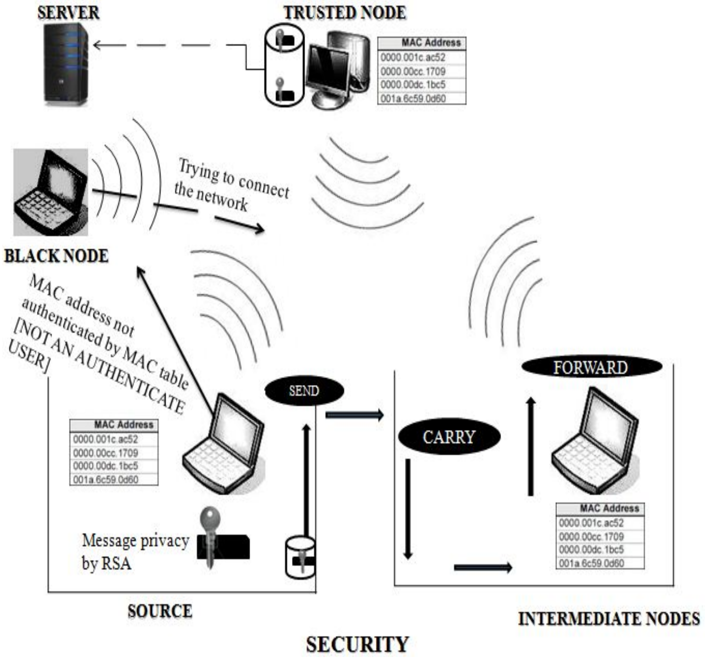
As when destination node is not in network or intermediate node is not in network , in such a conditions the last node which received the message have a chance of memory overflows but after using a trusted node .All the message will be transferred to trusted node and hence stortage problem at nodes decreases and storage issue only remains on Trusted node , but as it have a large storage area , there is very less chance of such issue but if occurs then the message that are residing in memoryof Trusted storage from a long time will be transferred to a server and when node come back the message will be back to trusted node and then client. Hence trusted node eradicates this problem also

.

4.3 For Security Issue

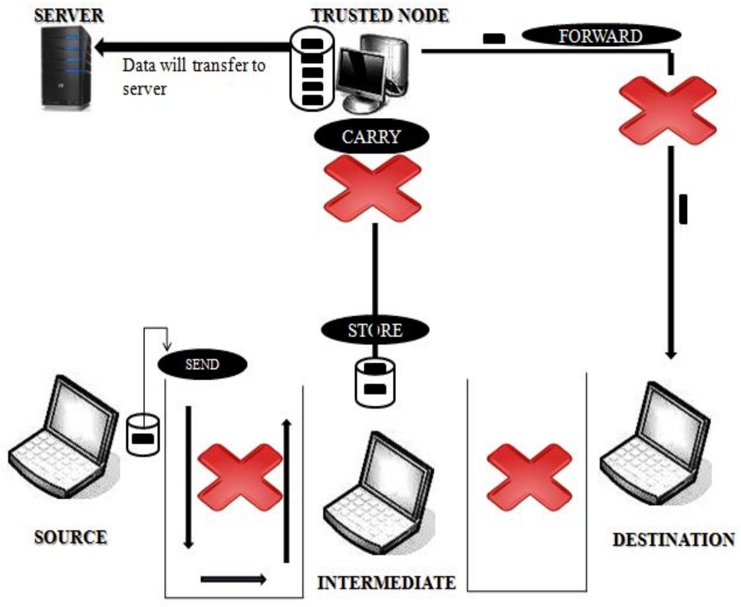
In case of security issue we have to use some traditional methods to secure the network.

A. BLACK NODE – In the situation of Black node (Node that works in the network by taking identity of other node of network) a method is defined in which those nodes that are connected in a network for permanent use . such nodes will have the table of the MAC address of all other nodes in network that are authenticated to that network . so whenever any new node comes in picture of network before it connection to any node its MAC address will be verified in the list of MAC table on all nodes . If it is authenticated then access the network resource otherwise will be considered a black node and hence will never be apart of network.



B. MESSAGE SECURITY – The message that is being Transferred between nodes will be secured by a cryptographic RSA algorithm.

4.4 Network Struck – In case of the situation occurs in which whole networks goes down and strucked due to any cause then all the messages that was moving in network will be transferred to Trusted node and it will send the messages to the server. Messages will reside over server until network reworks again after then will be transferred back to trusted node and rest the work of trusted node to send the messages to correct destination.



NETWORK STRUCK ISSUE

.

5 CONCLUSION AND FUTURE WORK

In this paper I have concluded that opportunistic network is very efficient way of communicating between different mobile nodes in the war prone area and natural calamity area but have some problems in it, so if a trust model over such problems is created in which such problems are eradicating then this network will sooner become a futuristic network. In our future work, we will implement new proposed technique and other mobility issues and compare results with the previous techniques.

6 6 ACKNOWLEDGEMENT

7 I am very thankful to department of information technology (IT) of Lovely Professional University (LPU) Punjab India for providing the required facilities needed for the successful completion of this paper. I am also very thankful to those who have helped me directly or indirectly for accomplishment of this work.

8 REFRENCES

[1] AnshulVerma, (March 2011) "Integrated Routing Protocol for Opportunistic Networks" International Journal of Advanced Computer Science and Applications,Vol. 2, No.3, Chaintreau, A. Mtibaa, L. Massoulié, and C. Diot, (December 2007) "Diameter of opportunistic mobile networks", Thomson technical report CR-PRL-2007-07-0001.

[2] Andreas Georgakopoulos, Kostas Tsagkaris, Vera Stavroulaki (2011), "Specification and assessment of a fitness function for the creation of opportunistic networks" Future Network & Mobile Summit 2011 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds) IIMC International Information Management Corporation.

[3] Chung-Ming Huang, Kun-chan Lan and Chang (November 2008) "A Survey of Opportunistic Networks", Zhou Tsai Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan, Taiwan, R.O.C.

[4] Boldrini ,A. Passarella, and M. Conti, (2007) "Users Mobility Models for opportunistic Networks: the Role of Physical Locations" IEEE wireless rural and emergency communication – WRECOM07.

[5] Chen Zhou1, Dai Wei2, Zhang Sanfeng1, Ji Yi1 (2012) "An Interest Based Opportunistic Network Mobility Model and Routing Method", (2012) IEEE

[6] Chen xi, Tian youliang (2012), "Security in opportunistic networks" International Conference on Industrial Control and Electronics Engineering.

[7] Er Upinder Kaur, Er. Harleen kaur Lecturer, (July 2005) "Routing techniques for opportunistic Networks and Security Issues" Computer Science, Baba Farid College, Bathinda, Punjab, India. Lecturer, Computer Science, Baba Farid Engg. College, Bathinda, Punjab, India.

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

[9] Hua Zhu, Kejie Lu (2007) **"**RESILIENT OPPORTUNISTIC FORWARDING: ISSUES AND CHALLENGES**",** IEEE

[10] Hoang Anh Nguyen, Silvia Giordano (2009) "Routing in opportunistic network"International Journal of Ambient Computing and Intelligence.

[11] Parris and T. Henderson, (June 2011) "The impact of location privacy on opportunistic networks", Proceedings of the Fifth IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications (AOC), Lucca, Italy, IEEE Computer Society Press.

[12] Jingyi Hu, Pingyi Fan, Ke Xiong (2011), "Cooperation-based Opportunistic Network Coding in Wireless Butterfly Networks" IEEE Globecom.

[13] Leszek Lilien, Zille Huma Kamal, Vijay Bhuse, and Ajay Gupta (March 2006),"Opportunistic Networks: The Concept and Research Challenges in Privacy and Security"

[14] Leszek Lilien, Zille H. Kamal, Ajay Gupta, Vijay Bhuse, (November 2006), "Opportunistic Networks" IEEE WiSe (Wireless Sensornet) Lab, Department of Computer Science Western Michigan University, Kalamazoo, MI 49008-5466

[15] L. Pelusi, A. Passarella, and M. Conti, (November 2006) "Opportunistic Networking: data forwarding in disconnected mobile ad hoc networks," IEEE Communications Magazine,vol. 44, no. 11.

[16] PAPAJ Jan, DOBOS Eubomir,(May 2012) "Opportunistic Networks and Security" CÚMÁR Anton Technical University of Kosice, Slovakia, Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics

[17] P. Gupta and P. R. Kumar, (March 2000) "The Capacity of Wireless Networks," IEEE Trans. Info. Theory, vol. 46, pp. 388–404.

[18] Suvadip Batabyal, Parama Bhaumik (2012)"Improving Network Performance with Affinity based Mobility Model in Opportunistic Network",IEEE 2012

[19] Suhas Diggavi (August 2006) “Opportunistic network communications” School of Computer and Communication Sciences Laboratory for Information and Communication Systems (LICOS) Ecole Polytechnique Fédérale de Lausanne (EPFL) Lausanne, Switzerland

[20] Yao-Nan Lien, Yi-Shiuan Lin(March 2012), “Placement of Control Network for Mobile Agents over Opportunistic Networks” The 8th International Workshop on Mobile Peer-to-Peer Computing 2012, Lugano.

[21] Yaozhou Ma and Abbas Jamalipour (2006), “Opportunistic Virtual Backbone Construction in Intermittently Connected Mobile Ad Hoc Networks” IEEE ICC 2011.