International Journal of Scientific & Engineering Research, Volume [illegible]
ISSN 2229-5518

STUDY OF OPPORTUNISTIC NETWORK: ITS APPLICATION, MESSAGE TRANSFERRING TECHNIQUES, SECURITY AND PRIVACY ISSUE

Ms. Pragati Ambekar **Dr. M.A. Rizvi**

Abstract- Mobile ad-hoc network are also infrastructureless networks but they have limited range of wireless transmission. The limited radio band results in reduced limited data rates compared to the wireless network. Hence optimal usage of bandwidth is necessary by keeping low overhead. As application environments of MANETs increase their traditional communication paradigms needs adequacy. Opportunistic network is one of the most developing areas of network which provides communication even in disconnected mode. Nodes are mobile and can change their location, message or packet is forwarded through many intermediate nodes so identity of users shown to all. Specifically today's ad hoc network are evolving towards opportunistic network where the proactive and reactive approaches for routing management are integrated or definitely substituted with techniques that exploit communication opportunities, whenever they arise, to forward messages on a hop-by-hop basis, but such kind of message transferring technique may lead to problems in the network. There can be several issues that may result in degrading the performance of opportunistic network. This paper provides a review of opportunistic network, message transferring techniques, security and privacy issues in opportunistic network.

Index Terms— MANETs (mobile adhoc network), infrastructureless networks, Opportunistic network, wireless network

1 INTRODUCTION

Mobile ad-hoc networks are the ones in which nodes are mobile. So according to the requirements these nodes can change their location. These nodes can enter, leave and switch on/off their connectivity whenever they want to do so. So no fixed infrastructure is followed in this type of network. Nodes are connected wirelessly and are also responsible for data forwarding. Tracking the topology of the network to forward the message packets can also be done by these nodes. The mobility activation and deactivation may also result in the changes of topology, so all nodes share routing information and also keep track of these routes. Opportunistic network, usually called as "*oppnets*" is a category of delay tolerant network. Opportunistic network is a wireless ad-hoc network. It is an extension of mobile ad-hoc network. In this network connections are not stable and connections occur at irregular intervals. Connections occur according to reachability of the intermediate node to the destination node. It is supported by nodes which has the capability to work in this kind of network. These nodes are wirelessly connected to each other. This network is also used in disconnected environment. As network topology is not fixed in opportunistic network therefore store and forward technique is used for transmission of data and thus route establishment takes place dynamically. These intermediate nodes first of all search for a suitable node in their communication range which can successfully carry the message closer to the destination. When a node comes in the communication range then this message is forwarded to this node. Now this node will find another suitable node in its range and this process gets repeated until the successful delivery of message is done to the desired destination. In this process each and every node gets an opportunity to select a suitable node in their range, so these networks are known as opportunistic network [2]. The motive of opportunistic network is to deliver message and enable communication between islands of connectivity i.e. nodes or network partitions that are disconnected. Every node can communicate and forward message only in its finite range. In this network, store-carry-forward manner is used for delivery of messages from one end to another. So, intermediate nodes help to send the message. No fixed topology changes with activation and deactivation of nodes. If source node and destination node are not in range then source node passes message to nearest node in its range and this process takes place until the message reaches to the desired destination node.

The network provide following functionalities [4]:

- **Node discovery:** Here a network node is able to discover other network node in direct communication range.
- **One hop message exchange:** A node is able to send and receive arbitrary data to or from any other node in direct communication range.

- *Pragati Ambekar is currently pursuing masters degree program in Computer technology Application in Rajiv Gandhi prodyogiki vishwavidyalaya, Bhopal, India,. E-mail: ambekar.pragati@gmail.com*
- ***Dr. M.A. Rizvi** is currently working as Associate and Head professor in NITTTR ,Bhopal ,India,E-mail: marizvi@nitttrbpl.ac.in*

2 MESSAGE TRANSFERRING STRATEGIES

There are two dissemination strategies to deliver messages in opportunistic network [3]. They are:

1. **Single copy case:** In this case only one message is

fowarded throughout the network, but it is not resilient to node failures, malicious node behavior or dropping of messages dull to full buffer.

2. **Multi copy case:** In this case several copies are forwarded over the network thus making network more resilient and message delivery yield a shorter delay than single copy case since several paths are used in parallel. But this creates overhead, i.e. additional transmission of messages. For this purpose node will communicate more often and will lead to quicker battery drainage and it will also buffer more messages.
The multi copy scheme can be broadly classified into:
Limited: Here a message is replicated for a fixed no. of times and forwarded to different nodes in the network.
Unlimited: Here there is no limitation of no. of replications of a given message that occurs in the network.

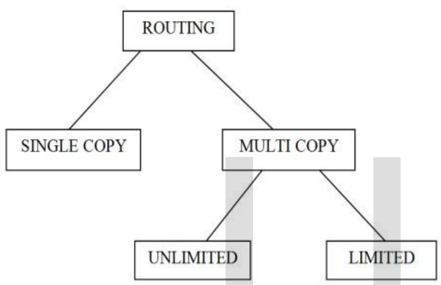

Fig.1

Depending on the application and the shared information, privacy preserving mechanism may also be an important issue.

3 ISSUES

1. **COOPERATION ENFORCEMENT**
In opportunistic networks there is no infrastructure and in particular no designated routers [7]. All nodes are expected to participate in the forwarding process so as to increase communication opportunities and the throughput along. This raises the issue of selfishness; nodes are inclined to forward only those packets that interest them while ignoring others. In case of small devices where there is scarcity of resources this issue becomes more critical and even fosters selfish behavior. Nodes therefore need good incentives in order to cooperate with each other for the greater good.

2. **SECURE ROUTING**
Routing is also one of the issue, when global infrastructure is not present , then addresses are network specific and have no meaning outside, hence naming becomes an obstacle. Thus conversational communication between a source and a destination is replaced by content dissemination where destinations are implicitly defined by their interest or their context rather than an explicit address [7].

4 SECURITY AND PRIVACY CHALLENGES

Devices which are carried by people and vehicle constitute an opportunistic network. The device use short range radio to communicate. Since node contacts are sparse. Therefore, node store message in their buffers, carrying them and forwarding them upon node encounters. This kind of communication leads to a set of challenging issues. Like other networks, this network also faces networking issues and challenges [2]. Some of them are as follows:

- **HETEROGENITY:** This network consists of hete ogeneous devices such as cell phones, sensors, cameras etc. These devices may depend on different technologies which gives rise to interoperability issue.
- **HIGH MOBILITY OR INTERMITTENT CONNECTIVITY:** As the nodes are mobile here so end-to-end connectivity is not established and there is also previous knowledge about network information. Therefore traditional ad- hoc routing protocols cannot be used here.
- **CONTACT:** Contact with another node might take place at unpredicted time due to high mobility of nodes.
- **STORAGE CONSTRAINT:** The intermediate nodes should have enough of storage space for storing of messages till it makes opportunistic contact with another node. As insufficient space may lead to dropping of packets and hence useful information may be lost.
- **DELAY TOLERANCE:** Store and forward technique is used for delivery of messages from one end to another. The intermediate nodes between source and destination stores the message till it gets the opportunity to connect itself to another node in its range and the process is followed till it reaches the destination
- **SECURE ROUTING:** There is a need of listing the trusted devices. These can be owned by institutions such as police stations, government offices, hospitals, universities etc. The route must be chosen in such a way that passes through maximum trusted devices. But this is very challenging. For this purpose secret keys and digital signatures can be used
- **NODE PRIVACY AND OPPNET PRIVACY:** Authentication and authorization, intrusion prevention and intrusion detection guarantees the privacy of a node. To prevent malicious node from joining the network privacy of oppnets also needs to be maintained
- **DATA PRIVACY:** Data privacy is provided in a way called encryption. So, public key cryptography can be

used. Here, controller encrypts data with public key and device decrypts it with their private keys. Public key is broadcast in a secure manner; otherwise a malicious device can distribute its own public key.

- **DATA INTEGRITY:** Data integrity is ensured by the use of digital signatures. But devices which have limited battery power may find it expensive.
- **IDENTIFY ATTACKS:** The attacks can be:

  Man in the middle attack: In this if a person sends request for help to the controller then a malicious node may not forward the request further but it will ensure the person that the help is on the way. To solve this problem the person can send redundant messages to the controller with the help of multiple neighbors.

  Packet dropping: Dropping of packets may take place by malicious nodes. To solve this attack, redundant messages can be sent through various different neighbors to the controller.

  DOS (Denial of Service): Malicious node can generate fake request due to which network becomes unavailable for real emergencies. To solve for this attack limit over total number of request can be placed. The weak devices (have low battery) can also be attacked. To solve this, weak devices have to be identified and their work load should be minimized.

  ID spoofing: Malicious node may generate re quest with many IDs. These attacks can be solved by checking neighboring nodes for ID spoofing
- **INTRUSION DETECTION:** Malicious node may enter and leave the node. Hence a secure detection mechanism is required that can detect them and spread (securely) their info throughout the network and that too in their presence. An embedded detector has mechanism for detecting attacks by malicious node.

5 Application

A. **Active Collaboration [4]:** It exploits the physical proximity of users not only it allows the exchange of digital information with users nearby, it also allows for use of device as link to the user him or herself, via non intrusive user notification ,such as for instance, a subtle device vibration, users are made aware of each other. This may lead to face to face collaboration, for instance a conversation or pursuing a common goal in real world. Its advantage is user's knowledge does not need to be stored on the device as a whole.

B. **Passive Collaboration [4]:** It allows passing of any kind of information from and to others users with communication range. This happens without any user interaction. It leads to autonomous information dissemination. It is a form of digital word-of-mouth communication for instance, similar to the way rumors spread by word-of-mouth. Since user device act without user control and interface, an incentive scheme might be crucial for application acceptance due to the fact that users share private resources (memory, battery, CPU). Otherwise, a user might be interested in taking part in an application at all.

Conclusion

This paper describes the concept of opportunistic networks, strategies of forwarding messages from one end to another and security/privacy issues related to these network opponents consist a newly identified category of computer networks. Oppnets will facilitate many applications [8]. As an example, they can help building an integrate network called for in various critical or emergency situation. Oppnnets can be used to enable connectivity in an area where any existing communication or information infrastructure has been fractured or partially destroyed. Oppnets will integrate various systems that were not designed to work together. The integration will enhance the flow of information that, for example, can assist in rescue and recovery efforts for devastated areas, or can provide more data or phenomena that are just developing, such as Answering to the identified privacy and security challenges in oppnets will contribute to advancing knowledge and understanding not only for the opportunistic network ,but will simultaneously advance the state of the art of computer privacy and security and security in ad-hoc and in general purpose computer networks.

References

[1] Routing Protocols in Infrastructure-less Opportunistic Networks International Journal of Advanced Research in Computer Science and Software Engineering Research Paper :(www.ijarcsse.com)

[2] Navneet Kaur and Gauri Mathur: Opportunistic Networks: A Review (IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 18, Issue 2, Ver. III (Mar-Apr.2016), PP 20-26.)

[3] FREDRIKBJUREFORS (Opportunistic Networking Congestion, Transfer Ordering and Resilence.)https://uu.divaportal.org/smash/get/diva2:713179/FULLTEXT01.pdf

[4] Manas kumar yogi1, vijayakranthi chinthala2: A Study of Opportunistic Networks for Efficient Ubiquitous Computing (International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.)

[5] (A Study of Opportunistic Networks for Efficient Ubiquitous Computing.)International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014 Copyright to IJARCCE www.ijarcce.com 5187

[6] Opportunistic mobile social network https://en.wikipedia.org/wiki/opportunistic_mobile social_ network:.

[7] Abdullatif Shikfa: Security Issues in Opportunistic Networks (Eurecom 2229, route des Crêtes - BP 19306560 Sophia-Antipolis, France) Ritu Manjot Kaur Sidhu M.Tech Scholar Associate Professor CGC, CGC, Mohali, India Mohali, India

[8] Leszek Lilien,1,2 Zille Huma Kamal,1Vijay Bhuse, 1 and AjayGupta1 (Opportunistic Networks: The concept and research challenges in privacy and security.