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
www.iosrjournals.org

Opportunistic Networks: A Review

Navneet Kaur, And Gauri Mathur,
[1]*M.Tech Scholar, Lovely Professional University, Punjab, India*
[2]*Assistant Professor, Lovely Professional University, Punjab, India*

Abstract: *Opportunistic network is a wireless ad hoc network. It is a type of delay tolerant network and an extension of mobile ad hoc networks. This network has a special characteristic which is intermittent connectivity. From intermittent we mean that connections are not stable and connections occur at irregular intervals. Connection may or may not occur which depends on the suitability of selecting a node which can carry the message closer to the destination or to the destination itself. End to end connections for transmission of data are unavailable here and they use store and forward technique for transmission of data. As end to end connections are not present so routes are established dynamically without having any knowledge about the network topology. Here, intermediate nodes are used for the delivery of message to its intended destination. These intermediate nodes store the messages with them until they find any other suitable node in their communication range which can successfully take the message closer to the destination. Once, a node is found within the range, the message is forwarded to that node. Now this selected node will find another suitable node in its range and the process is repeated until there is successful delivery to the destination. As every node has an opportunity to select a suitable node in their range, so these networks are known as opportunistic networks. This paper provides a quick review of mobile opportunistic networks including their routing protocols, challenges, and applications.*

Keywords: *Opportunistic network; Routing protocols; Security; Privacy; Applications*

I. Introduction

Opportunistic is a category of delay tolerant network. It is formed by the nodes which have the capability to support this kind network. The nodes in this are connected wirelessly. The nodes can be mobile or stable, so fixed infrastructure is not present her. This network can also be used in disconnected environment. Every node has a finite range in which they can communicate or can forward the message. A node can forward a message only when any other node comes in its range. The nodes have to store the message until another node comes in its range. In this network all the nodes work in the store-carry-forward manner. In this network, the intermediate nodes help to send the message from source to destination. Nodes have no fixed topology of the network. It is not necessary that fixed route between source and destination is available. Activation and deactivation of the node can change the topology of the network. If a source node cannot find the destination node in its range, then it passes the message to the nearest node in its range and this process goes on so that the message comes closer to the destination.

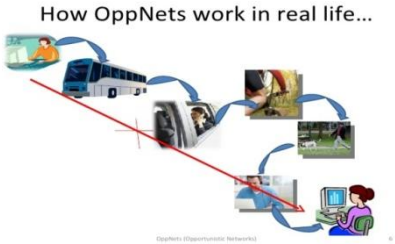

Fig 1: An Example Of OPPNET

The above figure (Fig 1) is one of the best examples to explain about opportunistic networks. This example describes that how OPPNET actually work in real life. In the example, the lady on the computer shown at the top left corner of the figure wants to send a message to a lady who is sitting on another computer (shown at the lower right corner of the figure). This process will go through a number of steps which are explained as follows:

- The lady working on the computer sends the message to a bus which is passing by from that area.
- The bus, which is passing through the traffic on the road, uses its Bluetooth to forward the message to the mobile of a person sitting in the car which is also passing through the bus stop at the same time.
- The person gets out of the car to enter into a restaurant. The person's mobile phone forwards the message to a cyclist who is passing nearby.

- The cyclist reaches a park and forwards the message to the person walking in the park who is having a mobile phone.
- The person passes by an office where an employee is working on his laptop. The message is forwarded to the laptop.
- The message is then finally sent to the intended receiver.

Searching for opportunity

In opportunistic networks, the nodes can only forward the message when they get an opportunity to send it. Opportunity means that a node is able to forward the message only when the intermediate nodes come in its range of communication. The node which wants to send the message needs a neighbor node which is closest to it and lies in its range. Now the message is carried by the neighbor node and the same process is now used by the neighbor node to forward the message. This process goes on till the data reaches the intended destination node. There can be one or many intermediate nodes in the midway of the source and the destination. The links between nodes are temporary. Activation and deactivation of nodes changes can change the topology of the network.

Message exchange

When two nodes find each other in their communication range, then only they can have a communication with each other. A node can forward the message to a node which is closest to it or is within its direct range. The node sends the data to its closest node and then the next neighbor node stores the message and waits for the opportunity to forward the message to next node. If a node is deactivated due to some reason and carries the data, then whenever it is activated it can carry on with the communication process as opportunistic network is a part delay tolerance network so time to send a message is not a big deal in this network. The main concern is that message reaches its intended destination. The following figures show how communication takes place. The figures involve the use of different network clusters to depict communication

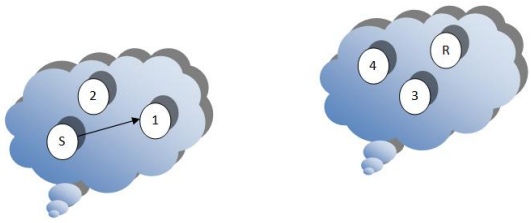

Fig 2: Message forwarding to an intermediate node by source

In Fig 2, Node S (source node), wants to send the message to the node R (destination node), node S forwards the message to only that node which is in its range. Node 1 and Node 2 are in the communication range of source node, so the source node passes the message to a node in its communication range. Node S forwards the message to Node 1.

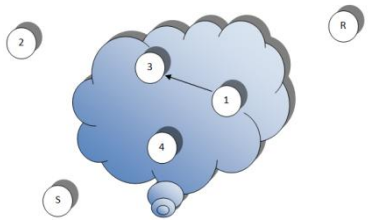

Fig 3: Message forwarding between intermediate nodes

In Fig 3, Node 1 leaves the range of source node, and stores the message with it until another node comes in its range. Here, Node 4 and Node 3 appear in the range of communication of Node 1. And Node 1 passes the message to the Node 3.

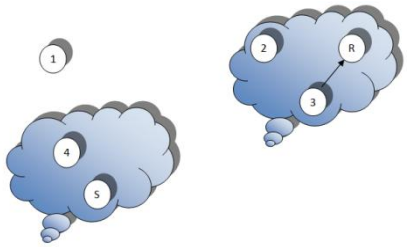

Fig 4: Message forwarding between intermediate node and destination

In Fig 4, Node 3 is now in the range of communication of Node R (may be Node 3 moves or Node R is moves to be in range) and forward the message to destination Node R. If Node R does not appear within the range of Node 3 then Node 3 stores the message and when it gets opportunity, forwards it to another node.

Literature Survey

A glimpse of the related work is shown in Table 1.

Table 1

Author(s)	Year	Title	Description
Huang, Lan, and Tsai	2008	A Survey of Opportunistic Networks	Provides a quick overview of opportunistic networks, and its issues and overview of the solutions to various issues in an opportunistic network
Lilien, Kamal, Bhuse, and Gupta	2006	Opportunistic networks: The Concept and Research Challenges in Privacy and Security	Investigates about the basics of oppnet operations, privacy and security challenges in oppnet
Lindgren, Doria, and Schelen	2003	Probabilistic Routing in Intermittently Connected Networks	A protocol is proposed which uses history of node encounters and transitivity to enhance performance over previously existing protocols
Pelusi, Passarella, and Conti	2006	Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad hoc Networks	Taxonomy of routing approaches and case studies have been discussed
Ritu, and Sidhu	2014	Routing Protocols in Infrastructure-less Opportunistic Networks	A survey in routing protocols based on opportunistic networks is presented
Vahdat, and Becker	2000	Epidemic Routing for Partially-Connected Ad Hoc Networks	A protocol is proposed that uses pair-wise exchanges of messages among the nodes
Juang, Oki, Wang, and Martonosi	2002	Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet	Discusses about the application (Zebranet) that includes nodes carried by animals under study across large wild area
Small and Haas	2003	The Shared Wireless Infostation Model - A New Ad Hoc Networking Paradigm (or Where there is a Whale, there is	Extends infostation concept by combining it with ad hoc networking and an improvement in SWIM

		a Way)	
Pentland, Fletcher, and Hasson	2004	DakNet: Rethinking Connectivity in Developing Nations	Discusses about the low cost communication for remote villages
Doria, Uden, and Pandey	2002	Providing connectivity to the saami nomadic community	Describes the Saami Network Connectivity (SNC) project that seeks to establish Internet communication for the Saami population of Reindeer Herders, who live in remote areas
Leguay, Friedman, and Conan	2005	Dtn routing in a mobility pattern space	A generic routing scheme is proposed using the formalism of a high-dimensional Euclidean space constructed upon mobility patterns.
Musolesi, Hailes, and Mascolo	2005	Adaptive routing for intermittently connected mobile ad hoc networks	A flexible framework is proposed for the evaluation of context information using probabilistic, statistical, autonomic and predictive techniques

Routing Protocols For Oppnet

Traditional MANET routing cannot be used for such networks. OPPNET routing protocols (as in Figure 5) can be classified as :

1. *Forwarding-based approach* - This approach is based on the type of knowledge node uses to select the best path for transmission to the destination node. It can further be classifies into :

- Direct transmission - Here, the source node generates a message and it holds it until the message reaches its destination. It consists of less overheads and long delays.
- Location-based - Here, to pass the message, nodes choose those nodes which are closest to the destination. MobySpace [11] is an example of this. It uses nodes' mobility patters for routing. The measure of closeness represents the probability that the nodes will come into contact with each other.
- Knowledge-based - Here selection of the nodes depends on the knowledge of the source, network or the intermediate nodes. Context Aware Routing (CAR) [12] is an example of this. It is a general framework for the evaluation and prediction of context information, aimed at achieving efficient and timely delivery of messages

2. *Flooding-based approach* - Here, every node broadcasts the message to all its neighbouring nodes.

- Epidemic routing - Epidemic routing scheme [6] is the solution to send a message when the context information is not present. It uses pair-wise exchange of messages between the nodes. The disadvantage is that congestion occurs due to flooding.
- Estimate/prediction routing - Here, nodes estimate the probability of each link to destination and then use the information to select the nodes for forwarding purposes. PROPHET [3] is an example of this type of routing which means Probabilistic Routing Protocol using History of Encounter and Transitivity. If a user visits a node many times, there is a possibility that it will visit that node again. Delivery predictability metric is maintained at every node.

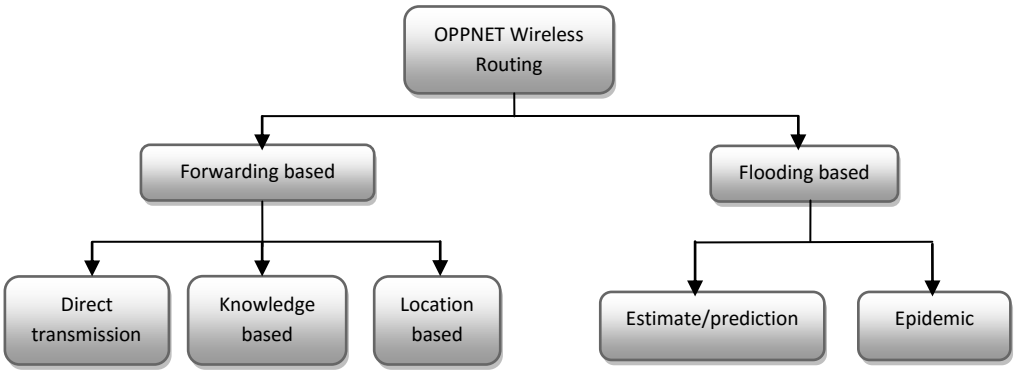

Fig 5: Classification of OPPNET routing protocols

Security and Privacy Challenges in OPPNET

Like other networks, this network is also not devoid of networking issues and challenges. Key issues and challenges in opportunistic networks may include:

- Heterogeneity - OPPNET is a heterogeneous network consisting of various kinds of 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) - Due to very high mobility of the nodes, end-to-end connection cannot be established and there is a lack of the previous knowledge about network information. Therefore, traditional ad-hoc routing protocols cannot be used in case of opportunistic networks.
- Contact - Due to high node mobility, there is possibility that a node might make contact with another node at an unpredicted time.
- Storage constraint - The intermediate nodes need to have enough storage space for storing the messages until they make an opportunistic contact with another node. If there is not enough storage space, then packets may be dropped and hence useful information may be lost.
- Delay tolerance - Messages are delivered using store and forward technique. The intermediate nodes between the source and the destination store the messages received by other nodes and on arriving an opportunity of connecting with another node, it will forward the message to that node, and the process goes on until the message is received by its intended destination.

Also many privacy and security challenges [2] arise out of opportunistic networking:

- Secure routing - A list of trusted devices need to be maintained. They can be owned by institutes such as police stations, government offices, hospitals, universities, etc. The route must be chosen 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 - Privacy of a node can be guaranteed by authentication and authorization, intrusion prevention and intrusion detection. Privacy of OPPENT also needs to be maintained as malicious nodes can join the network.
- Data privacy - Encryption is a way of providing data privacy. Public key cryptography can be used this case. Here, the controller can encrypt data with public key and devices can decrypt it with their private keys. A secure mechanism is needed for the broadcast of the public key, otherwise a malicious device can also distribute its own public key.
- Data integrity - Digital signatures can be used to ensure data integrity. But they can be expensive for those devices which have limited battery power.
- Identify attacks - The attacks can be :

A. 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.
B. Packet dropping - The malicious node can drop the packets. To solve for this attack, redundant messages can be sent through different neighbors to the controller.
C. DoS(Denial of Service) - The malicious nodes can generate fake requests due to which they make the network unavailable for real emergencies. To solve for this attack, limit can be placed over the total number of requests that the devices can send. The weak devices (which may have low battery power) can also be

attacked. To solve for this attack, weak devices need to be identified and their workload need to be minimized.

D. ID spoofing - A malicious node can generate requests with many Ids. To solve for this attack, the nodes need to keep a check on their neighbors for ID spoofing.

- Intrusion detection - Malicious devices or nodes enter and leave the network. Hence a secure detection mechanism is required that can detect them and can securely spread their information throughout the network and that too in their presence. An embedded detector can be used that has the mechanisms for detecting the attacks by the malicious nodes.

Applications

There are various applications that can benefit from opportunistic computing. Applications of OPPNET include:

- *Opportunistic computing* - It uses shared resources, services and applications so as to perform distributed tasks.
- *Recommender systems* - It is used to track user activities and mobility patterns and using this information to give recommendations on various items.
- *Mobile data offloading* - Due to an increase in the number of smart phones, 3G and 4G networks are overloaded. So, mobile data offloading in opportunistic networks is used to reduce the load on 3G and 4G networks.
- *OPPNET for Wildlife monitoring and OPPNET for rural areas* - Refer to the next section.
- *Crisis Management* - Traditional communication networks cannot be used where there are unexpected disruptive events. Hence, opportunistic networking can be used to interconnect the parts of the telecommunication network and then can be used for specific networks.
- *Pervasive healthcare* - Opportunistic networking can be used to create a system intelligent devices that can keep a track of patients surroundings. This may include Body Area Networks (BAN). Opportunistic networking can be used for monitoring physical and physiological parameters.

Case studies (realistic projects)

Various real life applications have been implemented in OPPNET. These are :

- *Wildlife monitoring* - Its main purpose is to track the wild species to have a knowledge about their behaviour and to study their interactions with each other. These systems have special sensors to sense the behaviour of the animals. Zebranet [8] is a project based upon this. In this project, zebras is the category of the animals that needs to be tracked. Another project is Shared Wireless Infostation Model (SWIM) [9]. Here whales are the wild species to be tracked and studied.
- *Rural area network* - This is for providing internet facilities to the rural areas. DakNet Project [10] is an example of this. Here hubs are built up in the villages. DakNet can also support email, audio/video messaging and e-commerce. Another project is Saami Network Connectivity (SNC) [11] to provide network facilities to the Saami population.

II. Conclusion

Opportunistic network is vast area in the field of ad hoc networking. They are used when a fixed path between the source and the destination is absent. They are characterized by their intermittent connectivity. This is a type of mobile ad hoc network. In this kind of network end-to-end connection is absent means complete path between two nodes desiring to communicate is unavailable. The routes are constructed dynamically. OPPNET uses store and forward technique for transmission of data. The intermediate nodes perform the role of routers. They store the messages until they find any other suitable node in their communication range. In this way, the nodes carry the message closer to the destination. The process goes on until the message reaches its intended destination. Opportunistic network has various applications but has a number of security and privacy issues. This paper provides a quick review of various concepts and challenges in opportunistic networks.

References

[1]. C. Hunag, K. Lan, and C. Tsai, A Survey of Opportunistic Networks, IEEE, *Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference*, Okinawa, 25-28 March 2008, pp. 1672- 1677.

[2]. L. Lilien, Z. H. Kamal, and A. Gupta, Opportunistic Networks:The concept and research challenges in Privacy and Security, *WSPWN*, 2006.

[3]. A. Lindgren, A. Doria, and O. Schelen, Probabilistic Routing in Intermittently Connected Networks, *ACM SIGMOBILE Mobile Computing and Communications Review*, 2003, pp. 19-20.

[4]. L. Peluci, A. Passarella, and M. Conti, Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad hoc Networks, *Communications Magazine*, IEEE (Volume:44, Issue:11), November 2006, pp. 134-141,

[5]. Ritu, and M. Sidhu, Routing Protocols in Infrastructure-less Opportunistic Networks, *IJARCSSE* (Volume:4, Issue:6), June 2014.

[6]. A. Vahdat, and D. Becker, Epidemic Routing for Partially-Connected Ad Hoc Networks, Department of Computer Science Duke University NC 27708, 2000.

[7]. P. Juang, H. Oki, Y. Wang, and M. Martonosi, Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet, *Proceedings of the 10th international conference on Architectural support for programming languages and operating systems*, vol. 37, 2002, pp 96-107.
[8]. T. Small and Z. J. Haas, The Shared Wireless Infostation Model - A New Ad Hoc Networking Paradigm (or Where there is a Whale, there is a Way), *Proceedings of the Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing* (MobiHoc 2003), Annapolis, MD, USA, June 1-3, 2003.
[9]. A. Pentland, R. Fletcher, and A. Hasson, DakNet: Rethinking Connectivity in Developing Nations, *IEEE Computer*, vol. 37, January 2004, pp. 78-83.
[10]. A. Doria, M. Uden, and D. P. Pandey, Providing connectivity to the saami nomadic community, *Proceedings of the 2nd International Conference on Open Collaborative Design for Sustainable Innovation* (dyd 02),Bangalore, India, December, 2002.
[11]. J. Leguay, T. Friedman, and V. Conan, Dtn routing in a mobility pattern space, *Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, 2005, pp. 276–283.
[12]. M. Musolesi, S. Hailes, and C. Mascolo, Adaptive routing for intermittently connected mobile ad hoc networks, *IEEE WoWMoM*, 2005, pp. 183–189.