Routing techniques for Opportunistic Networks and Security Issues

Er Upinder Kaur[1], Er. Harleen kaur [2]
[1] Lecturer, Computer Science, Baba Farid College, Bathinda, Punjab, India.
[2] Lecturer, Computer Science, Baba Farid Engg. College, Bathinda, Punjab, India.
raj_chawla94@yahoo.com[1], harleengrover@gmail.com[2]

Abstract
Opportunistic networking has received considerable interest from the research community in recent years. In opportunistic networks, mobile nodes are enabled to communicate with each other even if a route connecting them never exists. An oppnet grows from its seed—the original set of nodes employed together at the time of the initial oppnet deployment. The seed grows into a larger network by extending invitations to join the oppnet to foreign devices, node clusters, or networks that it is able to contact. The design of efficient routing techniques for opportunistic networks is usually a big challenge. In this paper, we survey the various routing techniques for the opportunistic networks as well as disscuss the security aspect for the opportunistic networks
Keywords: Computer networks, opportunistic networks, privacy, security, routing techniques.

1. Introduction:

1.1. Opportunistic network:

An opportunistic network is a wirelessly connected node. Nodes may be either fixed or mobile. Communication range is not fixed. In which device make link to the user. Different nodes make collaboration to exchange data from source to destination[1][2]. In which when node find opportunity they use it. The device exchange data to or from spontaneous manner whenever they come in close. Network topology makes change during the active and deactivates nodes. . In which there is no direct connection between source node to destination node ,network node only discover its nearest neighbor node and by use this it forward message. Message is delivered hop by hop closer to the destination. Network follow to function

(1) Find opportunity:

Network is able to find opportunity in direct communication range. . A node needs to find neighbor node in its vicinity in order to start collaboration. Neighbor nodes act as spontaneous manner whenever they come in close. The nodes link temporary.

(2) Message exchange:

When two nodes successfully discovered each other both nodes share data in user awareness. A node can exchange data to its neighbor nodes within the direct range. Nodes pass data to it's successfully discover neighbor nodes. Data is distributed to all the nodes through the information sprinkler.

(3) Information sprinkler:

An information sprinkler is a dedicated node which is not mobile. It is

fixed in dedicated location in opportunistic network. Information sprinkler

works as other opportunistic network nodes. It uses data sharing protocol.

It collect information from opportunistic nodes that in its range. One

information sprinkler is connected to other information sprinkler through

wired or wire fewer networks which have other nodes in its range. Data collect form one information sprinkler is distributed to other information sprinkler with in short period of time.

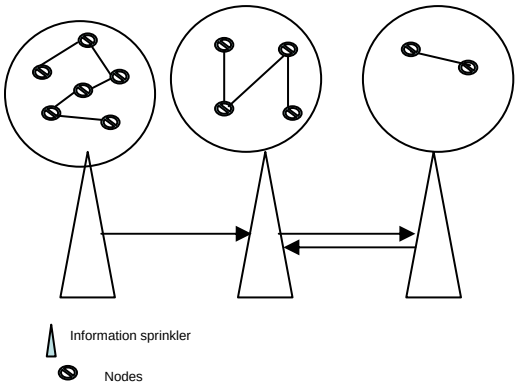

Fig: 1 Opportunistic Network

(4) Nodes:

Nodes are any network component which has the property of receiving and forwarding the message. Nodes may be mobile or fixed in dedicated location. Like a computer with blue tooth, a radar, a laptop, a wi –fi network, a mobile phone etc. when one source node have message and it want to sent to the particular destination node then source node find its all possible bound neighbor nodes and distribute the message that particular node that is closer to it with the destination node address. So hop node receiving the message and then repeat the above procedure until message not delivered to the correct location.

2. Routing Approaches in Opportunistic Networking

Routing is the most compelling challenge in opportunistic networking. The design of efficient routing strategies for opportunistic networks is generally a complicated task due to the absence of knowledge about the topological evolution of the network. Routing performance improves when more knowledge about the expected topology of the network can be exploited [8]. Unfortunately, this kind of knowledge is not easily available, and a trade-off must be met between performance and knowledge requirement. Depending on the particular routing approach followed, opportunistic networks may be classified at a very top level into two categories: infrastructure-less and infrastructure-based networks [6].

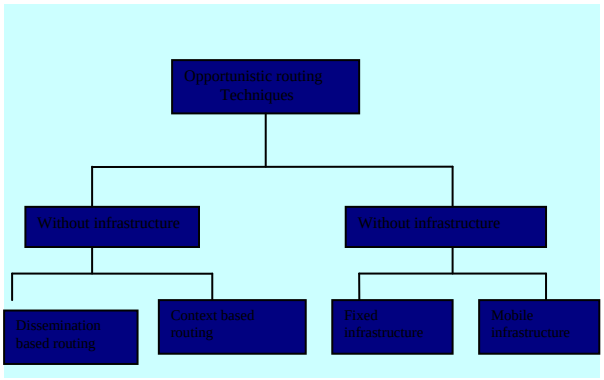

Fig: 2 Routing Techniques for Opportunistic Networks

2.1. Infrastructure-less Opportunistic Networks

In infrastructure-less opportunistic networks two basic routing approaches are used: dissemination-based and context-based routing. Dissemination-based algorithms are essentially forms of controlled flooding, and differentiate themselves for the policy used to limit flooding. Context-based approaches usually do not adopt flooding schemes, but use knowledge of the context that nodes are operating in to identify the best next hop at each forwarding step.

2.1.1 Dissemination-based Routing

Routing techniques based on data dissemination perform delivery of a message to destination by simply diffusing it all over the network. The heuristic behind this policy is that, since there is no knowledge of a possible path towards the destination nor of an appropriate next-hop node, should a message be sent everywhere. It will eventually reach the destination by passing node by node. Dissemination-based techniques are very resource hungry. Moreover, due to the considerably high number of transmissions involved, dissemination-based techniques suffer from high contention and may potentially lead to network congestion. To increase the network capacity the spreading radius of a message is typically limited by imposing a maximum number of relaying hops to each message or even by limiting the total number of message copies present in the network at the same time. When no relaying is further allowed, a node can only send

directly to destination when/in case met. The first protocol exploiting dissemination techniques is the Epidemic Routing protocol [7]. In Epidemic Routing messages diffuse in the network similarly to diseases or viruses, i.e., by means of pair-wise contacts between individuals/nodes. A node is infected by a message when it either generates that message or alternatively receives it from another node for forwarding. The infected node stores the message in a local buffer. A node is susceptible to infection when it has not yet received the message2 but can potentially receive it in case it comes into contact with an infected node. The infected node becomes recovered once having delivered the message to the destination node and, as a result, it also becomes immune to the same disease and does not provide relaying to the same message any more. The dissemination process is somehow bounded because each message when generated is assigned a hop count limit giving the maximum number of hops that that message is allowed to traverse till the destination. When the hop count limit is one, the message can only be sent directly to the destination node. Further we discuss epidemic routing are represented by PROPHET and the MV routing [4] protocols. In both protocols, messages are exchanged during pair-wise contacts as in epidemic routing. However, a more sophisticated method to select the messages to forward to an encountered node is introduced. Basically, the choice depends on the probability of the encountered nodes to deliver the messages successfully to their eventual destinations. The delivery probability relies on observations on the meetings between nodes, and both on the meetings between nodes and the visits of nodes to geographical locations occurred in 2 the message itself represents the infection/virus. the recent past (in MV Routing).
Network-coding-based routing [5] also falls in the category of dissemination-based algorithms, but takes an original approach to limit message flooding. Messages are combined together (encoded) at nodes before being forwarded. Then, the codes produced are sent out instead of the original messages. Codes are spread in different directions like in other dissemination-based routing protocols. The number of codes generated is higher than the number or original messages combined together. This is to allow much more robustness against both packet and path loss. Encoding is performed at both source and intermediate nodes. Network-coding-based routing can be generalized by recursively using erasure-coding techniques at intermediate nodes [7]. It outperforms flooding, as it is able to deliver the same information with a fewer number of messages injected into the network.

2.1.2 Context-based Routing

Most of the dissemination-based techniques limit messages' flooding by exploiting knowledge about direct contact with destination nodes. Context-based routing exploits more information about the context nodes are operating in to identify suitable next hops towards the eventual destinations. The usefulness of a host as next hop for a message is hereafter referred to as utility of that host. Usually, such routing techniques are able to reduce significantly the message duplication and resource consumption (e.g., bandwidth, memory, energy) of dissemination-based techniques. Since they also reduce network congestion, it has been shown that they are able to reduce delays and message loss as well. The main cost paid for these advantages is the fact that context information must be kept at nodes and circulated among nodes. However, recent results show that resource consumption is far lower even when these additional costs are considered [3][4]. In the Context-Aware Routing (CAR) protocol each node in the network is in charge of producing its own delivery probabilities towards each known destination host. Delivery probabilities are exchanged periodically so that, eventually, each node can compute the best carrier for each destination node. The best carriers are computed based on the nodes' context. Among the context attributes needed to elect the best carrier there are, for example, the residual battery level, the rate of change of connectivity, the probability of being within reach of the destination, the degree of mobility. When the best carrier receives a message for forwarding, it stores it in a local buffer and eventually forwards it to the destination node when met, or alternatively to another node with a higher delivery probability. Actually, CAR provides a framework for computing next hops in opportunistic networks based on the multi-attribute utility theory applied to generic context attributes. Simulation results show that CAR is more scalable than epidemic routing as the protocol overhead is approximately constant regardless of the node buffer size.

In MobySpace Routing [3] the nodes' mobility pattern represents the context information used for routing. The protocol builds up a high dimensional Euclidean space, named MobySpace, where each axis represents a possible contact between a couple of nodes and the distance along an axis measures the probability of that contact to occur. Two nodes that have similar sets of contacts and that experience those contacts with similar frequencies are close in the MobySpace. The best forwarding node for a message is the node that is as close as possible to the destination in this space. This in fact improves the probability that the message will eventually reach the destination. Obviously, in this virtual contact space just described, the knowledge of all the axes of the space also requires the knowledge of all the nodes that are circulating in the space3. Both CAR and MobySpace Routing require full knowledge of possible destinations to enable forwarding.

The History-Based Opportunistic Routing Protocol (HiBOP) [4] provides a framework for managing and exploiting context information that does not require all nodes to know each other. In HiBOP nodes exchange context information about the users when getting in touch. Each node remembers context information seen in the past (such information is enforced based on how often it is "seen" on encountered nodes). A node carrying a given message asks the encountered nodes to compute their delivery probability towards the destination(s). The delivery probability is computed based on the match between context information about the destination stored in the message itself, and context information stored by the encountered node itself. Messages are forwarded along a gradient defined by increasing

match between the destination information and the context information of the carrying node. Hence, the algorithm dynamically selects as next hops those nodes that share more and more context information with the destination(s). HiBOP exploits social relationships among users to 3[8] also proposes an optimization that does not require the knowledge of all contacts between nodes. Identify good carriers for messages.

2.2. Infrastructure-based Opportunistic Networks:

Infrastructure-based opportunistic networks are characterized by the presence of special nodes that are used for collecting messages from source nodes and delivering them to their destinations. Such special nodes are generally more powerful than regular nodes as they have high energy budget and large storage capacity. They may either act as a gateway toward a less challenged network, or they can simply increase the connectivity between (regular) nodes in the network. We can distinguish opportunistic networks with fixed infrastructure and with mobile infrastructure depending on the mobility of special nodes. When using a fixed infrastructure special nodes are stationary and are located at specific geographical points. On the other hand, in opportunistic networks with mobile infrastructure special nodes move around in the network area following either pre-defined or completely random paths.

2.2.1 Routing based on Fixed Infrastructure

A fixed infrastructure consists of special fixed nodes, i.e., base stations, which are sparsely deployed all over the network and act as message collectors. Base stations offer high capacity and robust data exchanges to the mobile nodes nearby. Moreover, they have high storage capacity to collect data from many nodes passing by. A source node wishing to deliver a message keeps it until it comes within reach of a base station, then forwards the message to the base station.

Base stations are generally gateways towards less challenged networks. Thus, the goal of an opportunistic routing algorithm is to deliver messages to the gateways, which are supposed to be able to find the eventual destination more easily. Two variations of the protocol are possible. The first one works exactly as described above, and only node-to-base-station communications are allowed. As a result, messages experience fairly high delays. The classical example of this approach is the Infostation model. A second version of the protocol allows both node-to-base-station and node-tonode communications. This means that a node wishing to send a message to a destination node delivers the message to the base station directly if within communication range, otherwise it delivers the message opportunistically to a near node that will

eventually forward it to the base station when encountered (routing schemes presented earlier can be used in this phase). Such a protocol has actually been proposed in the Shared Wireless Infostation Model (SWIM) [4]. As it results from the above examples, historically, fixed base stations play a passive role in the opportunistic forwarding strategy because they simply act as information sinks. However, many benefits can be envisioned by running an opportunistic routing algorithm also at base stations. Base stations, for example, can simply collect the messages sent by the visiting nodes and then wait for the destination nodes to be within reach to forward the stored messages to them. Base stations of a mobile infrastructure typically play such an active role. Despite allowing energy saving at the mobile nodes, a routing approach relying on a fixed infrastructure is highly expensive due to the costs of the infrastructure. Moreover, it suffers from scalability issues since the addition of new nodes implies the expansion of the infrastructure. Using a mobile infrastructure instead of a fixed infrastructure is a valuable opportunity to realize a cheap and flexible infrastructure. A mobile infrastructure is composed of mobile nodes that move around in the network place following either pre-determined or arbitrary routes and gather messages from the nodes they approach. These special nodes may be referred to as carriers, supports, forwarders, MULEs, or even ferries. They can be the only entities responsible for the delivery of messages, when only node-to-carrier communications are allowed, or they can simply help increase connectivity in sparse networks and guarantee reachability of isolated nodes. In the latter case, delivery of messages is accomplished by both carriers and ordinary nodes and communications are allowed both node-to-node and node-to-carrier [9].

3. Security issues for opponents

One of the sources of privacy and security threats is the fact that authentication cannot, in general, be performed when devices join the network. It is not possible to guarantee that malicious devices will not join. Moreover we might not be able to classify or rate devices as malicious until they join the oppnet, and we detect their notorious behavior. Delivering secret keys securely to all non-malicious devices (and only to non malicious devices) is very difficult in such an ad hoc environment. Hence, relying alone on cryptography-based authentication mechanisms (e.g., Kerberos) will not help in all situations. So, MITM, packet dropping, ID spoofing (masquerading), DoS and other attacks are even bigger threats in opportunistic networks.

Malicious devices or malicious networks will be able to join an oppnet because of the lack of an initial authentication mechanism. Therefore, there is a need to detect and isolate malicious nodes, clusters, or networks. Securely distributing information about malicious entities in the presence of malicious entities is a challenge. If shared securely, this second-hand reputation information can be used by all oppnet nodes to protect themselves from attackers. Even if that information could be distributed securely, voiding those entities while maintaining connectivity is another challenge. For a review of intrusion detection in wireless ad hoc networks we refer reader to [8]. However, we need to emphasize that the highly heterogeneous nature of oppnets makes real-time intrusion detection and response in them even more challenging than in other types of networks. The intrusion detection approach most relevant for oppnets comes from the AAFID project, in which autonomous agents perform intrusion detection using embedded detectors. An embedded detector is an internal software sensor that has added logic for detecting conditions that indicate a specific type of attack or intrusion. Embedded detectors are more resistant to tampering or disabling, because they are a part of the program they monitor. Since they are not executing continuously, they impose a very low CPU overhead. They perform direct monitoring because they have access to the internal data of the programs they monitor. Such data does not have to travel through an external path (a log file, for example) between its generation and its use. This
reduces the chances that data will be modified before an intrusion detection component gets it.

4. Conclusion and future work:

At the top level of our taxonomy, we have divided routing techniques for opportunistic networks between algorithms that do exploit some form of

infrastructure, and algorithms that do not. In this, the data MULEs and message ferrying architectures are the most promising approaches. They are susceptible to various improvements but have the potential to be utilised as bases for more general and global architectures. For example, in the data MULEs approach, lower-level nodes exploit the higher level and more capable mobile devices (the MULEs), which, in turn, exploit a further infrastructure level, i.e., the Access Points. However, routing algorithms exploited at each layer are pretty trivial or do not exist at all. In such a network, each level of the infrastructure is an opportunistic network in which nodes may exploit routing algorithms to communicate among themselves, and may rely on the upper levels of the infrastructure to reach nodes that are too far away. For example, a low level can consist of devices such as PDAs, or smart phones. An opportunistic routing algorithm can make those devices able to communicate with each other. To reach nodes too far away for such routing to be effective, a higher level consisting, for example, of a "city-bus network" might be used. In this scenario, buses will act similarly to MULEs. However, multi-hopping will be used also at this level of the network via a (possibly different) opportunistic routing algorithm. This will enable connection among different clouds of the lower-tier devices just by relying on the city-bus network. Clearly, the city-bus network might exploit further infrastructure levels such as a mesh network formed by Access Points, or even access the Internet through standard Wi-Fi Access Points. In opportunistic networks better routing technique is a challenge when we consider it with the security also, so our next step is to introduce the mobile agents in the routing with infrastructure to increase security in these networks once the security concept is designed and developed, such a network might actually represent a fundamental building block for the Next-Generation Internet.

References:

[1]. Pelusi, L., Passarella, A. and Conti, M. (2006) 'Opportunistic networking: data forwarding in disconnected mobile ad hoc networks', IEEE Communications Magazine, Vol. 44, pp.134–141

[2]. L. Lilien, A. Gupta, and Z. Yang, "Opportunistic Networks and Their Emergency Applications and Standard Implementation Framework," submitted for publication

[3]. J. Leguay, T. Friedman, and V. Conan, "Evaluating Mobility Pattern Space Routing for DTNs", in Proceedings of the IEEE Infocom 2006, Barcelona, Spain, April 2006.

[4]. C. Boldrini, M. Conti, I. Iacopini, and A. Passarella, "HiBOp: a History Based Routing Protocol for Opportunistic Networks", Proc. IEEE WoWMoM 2007, Helsinki, Finland, June 2007.

[5]. Y. Gu, D. Bozdag, E. Ekici, F. Ozguner, and C. Lee, "Partitioning Based Mobile Element Scheduling in Wireless Sensor Networks", Proc. IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON 2005), pp. 386- 395, S. Clara, USA, Sept.2005.

[6]. J. Widmer and J.-Y. Le Boudec, "Network Coding for Efficient Communication in Extreme Networks", Proc. of ACM SIGCOMM 2005

Workshop on delay tolerant networks, Philadelphia, PA, USA, August 22–26, 2005.
[7]. A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks", Tech. Rep. CS-2000-06, Department of Computer Science, Duke University, Durham, NC, 2000.
[8]. J. Sushant, K. Fall, and R. Patra, "Routing in a delay tolerant network," in Proceedings of SIGCOMM'04, August, 2004.
[9] V. Karpijoki, "Security in Ad hoc Networks", Proceedings of the Helsinki University of Technology, Seminars on Network Security, Helsinki, Finland, 2000.