AN INTRODUCTION TO WIRELESS MOBILE SOCIAL NETWORKING IN OPPORTUNISTIC COMMUNICATION

Navdeep Kaur

Department of Electronics Technology, Guru Nanak Dev University
Amritsar, Punjab, India
navdeep.mahal88@gmail.com

ABSTRACT

Next generation networks will certainly face requesting access from different parts of the network. The heterogeneity of communication and application software's changing situations in the environment, from the users, the operators, the business requirements as well as the technologies. Users will be more and more mobile, protocols, etc. will increase and render the network more complex to manage. Opportunistic communication has emerged as a new communication paradigm to cope with these problems. Opportunistic networksexploits the variation of channel conditions, provides an additional degree of freedom in the time domain and increase network performance.The limited spectrum and the inefficiency in the spectrum usage require such a new communication to exploit the existing wireless spectrum opportunistically by allocation of spectrum based on best opportunity among all possibilities.

KEYWORDS

Opportunistic communication, Wireless communication, Social Networks, Mobile technology.

1.INTRODUCTION

Continuous developments of mobile technologies and use of devices such as smart phones in everyday life increase need to be continuously connected to others through WiFi and to the Internet, anywhere and at any time. In mobile environments user connectivity is mainly affected by wireless communications constraints and mobility of user. These boundary conditions do not allow us to design communication environments based on unique and fixed connected networks or assume a stable path between each pair of source and destination. [7] Any mobile node can exchange information opportunistically during their periods of contactwith any other node, fixed or mobile. Network protocols are designed to be extremely resilient to events such as long partitions, node disconnections, etc, which are very features of this type of self-organizing, self-adaptable mobile social networks. This is achieved by temporarily storing messages at intermediate nodes, waiting for future opportunities to forward messages towards their destination. The mobility of users plays an important role in opportunistic networks as mobility can increase the capacity of wireless networks through opportunistic communications. [1]A new paradigm and a new technology of opportunistic networks or oppnets to enable integration of the

DOI : 10.5121/ijdps.2013.4306

diverse wireless communication, computation, mobile social applications, mobile advertising, media sharing and location-based services,sensing, storage and other devices and resources that surrounds us more and more. As communication and computing systems are becoming more and more pervasive, the related privacy and security challenges also become complex to manage.The advantages of opportunistic communications include potentially high capacity, low cost, localized communications, fully decentralized operation and independence of any infrastructure. These benefits are directly related to the varying capabilities of the available networking technologies. Cellular data today is often slowing, expensive (especially when roaming) and not even always available (rural areas, underground transportation, popular mass events, disaster situations to name a few examples). Bluetooth or WiFi can both offer always available, essentially free, local connectivity. In addition, WiFi offers higher bandwidths compared to the available cellular networks. Consequently, there is a huge opportunity and unused network capacity available in opportunistic encounters that are exploit efficiently.

2. OPPORTUNISTIC MOBILE SOCIAL NETWORKS

Personal mobile devices have become ubiquitous and an inseparable part of daily lives. These devices have evolved rapidly from simple phones and SMS capable devices to smart phones that we use to connect, interact and share information with our social circles. The smart phones are used for traditional two-way messaging such as voice, SMS, multimedia messages, instant messaging or email. Moreover, the recent advances in the mobile application development frameworks and application stores have encouraged third party developers to create a huge number of mobile applications that allow users to interact and share information in many wayssuch as Bluetooth and WiFi leading to complicated communication by the multiple wireless interfaces. Some examples are networked games, location based services and online social networking (tweeting, status and location updates, reviews, recommendations, photo sharing and so forth). [1]

The popularity of smart phones and applications would not have been possible without the availability of Internet connectivity. Typical smart phones come equipped with multiple radio interfaces including cellular radio (2G, 3G or emerging 4G technologies), 802.11 (WiFi), Bluetooth and Infrared. In addition to the global Internet connectivity, some of the available interfaces (notably Bluetooth and WiFi) can be used for local device discovery and direct device-to-device data communications. Today, this functionality remains mostly unused or is very limited to applications such as synchronization of data with a PC or manual file transfers. All of the smart phone applications follow instead the traditional Internet application development paradigm and depend on some type of infrastructure based communication service. The local context, mobility or opportunistic contacts between mobile devices are practically never taken into account. The social networking applications have proven their popularity in the current Internet and many compelling opportunistic networking applications are naturally about social networking (introduction services, friend finders, recommendations, content sharing, gaming). Human mobility, on which the opportunistic networks rely for forwarding, is directly related to social behavior of people.Opportunistic mobile social networks that we define as decentralized opportunistic communication networks formed among human carried mobile devices that take advantage of mobility and social networks to create new opportunities for exchanging information and mobile ad hoc social networking. [13]

3.OPPORTUNISTIC CONCEPT

Opportunistic mobile networks consist of human carried mobile devices such as smart phones that communicate with each other in a ”store-carry-forward” fashion, reduce the corresponding communication overheadwithout any infrastructure. Opportunistic mobile networks present distinct challenges compared to classical fixed networks, such as the Internet, that assumes the availability of a contemporaneous, reasonably low propagation delay, low packet loss rate path between the two end points that communicate. In opportunistic networks, disconnections and highly variable delays caused by mobility of mobile devices moving into wireless rangeare the norm. Another major challenge in opportunistic communication arises from the small form factor of mobile devices that introduces resource limitations compared to static computing systems. Moreover, implementation and deployment of actual opportunistic mobile networks, systems and applications is challenging, very often expensive and time-consuming as mobility itself is a significant problem in mobile networking. Opportunisticmobile networks can be seen as a generalization of DTNs (Delay Tolerant Networks). Specifically, in opportunistic mobile networks such as in DTNs, mobile social applicationsand location-based services not a prior knowledge is assumed about the possible points of disconnections, nor the existence of separate Internet like sub networks is assumed. Opportunistic mobile networks are formed by individual nodes, that are possibly is connected for long time intervals, and that opportunistically exploit any contact with other nodes to forward messagesusing routing protocols, suchas DSR (Dynamic Source Routing). The routing approach between conventional DTNs and opportunistic mobile networks is therefore quite different. As in DTNs,continuous end-to-end connectivity may never be available as it is concerned with interconnecting highly heterogeneous networks, the possible points of disconnections (and, sometime, the duration of disconnections) are known, routing can be performed along the same lines used for conventional Internet protocols, considering the duration of the disconnections as an additional cost of the links.

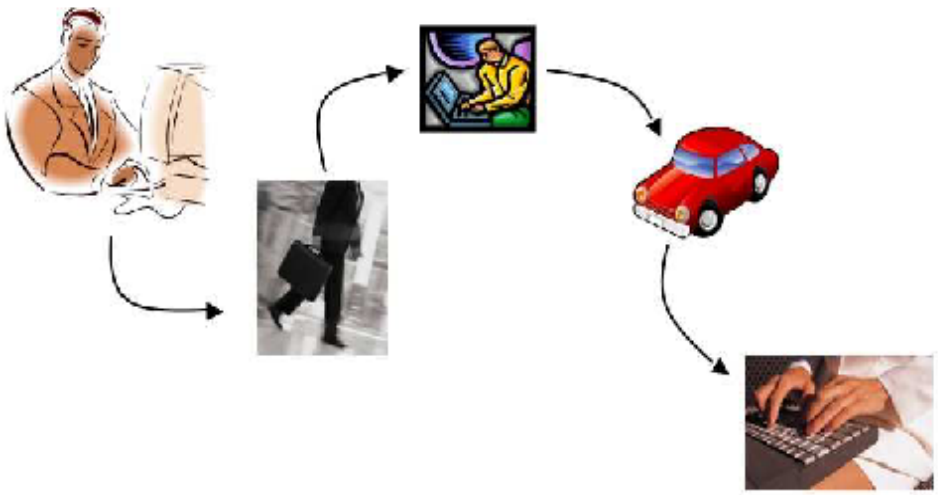

Figure1. The opportunistic mobile networking concept [1]

Since opportunistic mobile networks do not assume the same knowledge about the network evolution, routes are computed dynamically while the messages are being forwarded from the source towards the destination, which is essential to handle frequent routing changes and to reduce the corresponding communication overhead. Each intermediate node evaluates the suitability of encountered nodes to be a good next hop towards the destinationduring their periods of contact. Opportunistic mobile networks share the idea of delay and disruption tolerance of DTN but are designed with the assumption of more unpredictable mobility. [14] Thus, they can be considered as a generalization of DTNs. [5] Device discovery is essentially the first step of opportunistic communication.For example, as shown in Figure 1, the user at the desktop opportunistically exchanges information, via a WiFi ad hoc link or through Bluetooth, a message for a friend to a user passing nearby, "hoping" that this user will carry the information closer to the destination. This user passes close to a train station, using Dynamic Source Routing(DSR) and forwards the message to a traveler going to the same city where the destination user works. At the train station of the destination city a car driver is going in the same neighborhood of the destination's working placefacilitate message forwarding. The driver meets the destination desktop useron his way, and the message is finally delivered from source. [1]For efficient opportunistic communications use of Bluetooth and WiFi is there. Commonly useBluetooth for a very practical reason of battery lifetime, however, for contact discovery and power on the higher power radio (e.g. WiFi) only on demand when more capacity or faster transmission is required.

4.GOAL FOR OPPORTUNISTIC MOBILENETWORKS

The goal for opportunistic mobile networks is to use opportunistic algorithms for maximizing the throughput that can be provided by opportunistic algorithms. The global knowledge of network including context information would enable optimal routing. The opportunistic mobile networks goals can be realized by alleviating first of all thecommunication problems including bottlenecks and gapsin spectrum utilization that are often theroot causes of resource shortages. [10] The another goal of opportunistic mobile networks is analysis of human mobilitylike time user spend at specific locations, node mobility information, history of node behavior as dynamic routing of information is used in opportunistic communication.Opportunistic mobile network's performance improves when more knowledge about the expected topology of the network can be exploited.

5.FORWARDING IN OPPORTUNISTIC NETWORKS

Opportunistic Networks architecture deploys simple forwarding schemes.

5.1.Oblivious Algorithms

The performance of forwarding algorithms in opportunistic networks is often evaluated against two oblivious corner cases: direct delivery (a message is delivered only when the source meets the destination) and epidemic forwarding (a message is flooded to all encountered nodes). Direct delivery represents the worst case in terms of delay and success rate but does not consume any network resources. Epidemic forwarding finds always the delay-optimal path if it exists but it wastes a lot of communication and storage resources in the network.

5.2.Contact History Based Algorithms

Many forwarding algorithms use the contact history to make the forwarding decision. Each node maintains a forwarding metric for every other node in the network.Upon an opportunistic encounter the nodes exchange their forwarding tables (or summaries of stored data including the destinations) and determine if the encountered node is a better forwarder (i.e. has a better value of the metric) for some of the stored data messages. Only selected data messages are replicated reducing the overhead and increasing the probability of rapid, successful delivery.

5.3.Social Network Inspired Algorithms

This algorithm suitable for opportunistic networks as they rely on human mobility, and hence are characterized by human social interaction.In SimBet node centrality in the social network and the similarity with the destination are used to select the good next hops. Similarly, Bubble Rap forwards data first to the global hubs of the network in order to reach the destination community, and then among the members of the community to the locally central nodes until the destination is reached. A recently proposed forwarding algorithm called People-Rank takes a similar approach and applies ideas of Page Rank web page ranking algorithm to opportunistic social networks. PeopleRank gives higher weight to nodes that are socially connected to other important nodes of the network. [2]

5.4. Multicasting

All the routing algorithms are aimed to route messages from a source to a single destination. The natural extension is multicasting, distribution of messages to a group of nodes. Similarly to unicast routing, multicasting in DTNs and opportunistic networks introduces novel challenges compared to multicasting in traditional connected networks [15].

6.ROUTING IN OPPORTUNISTIC COMMUNICATION NETWORKS

The design of efficient routing and forwarding strategies for opportunistic communication is generally inherent complex 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. A key piece of knowledge to design efficient routing protocols is amount of contextinformationin which the users communicate. Context information, such as the users working address and institution, the probability of meeting with other users or visiting particular places, can be exploited to identify suitable routing protocols to learn the network state, autonomically adapt forwarders based on context information about the destination and thus optimize their operations.

6.1.Context-Oblivious Routing

Basically, routing techniques in this type of routing exploit some form of flooding. In this policy when there is knowledge neither of a possible path towards the destination nor of an appropriate next-hop node, a message should be disseminated as widely as possible leads to high overload and networks congestion. To limit high overload, possible techniques is to control flooding by limiting the number of copies and by limiting the number of hops.Protocols in this class might be

the only solution when no context information is available. They generate a high overhead (as we also highlight inthe performance evaluation section), may suffer high contention and potentially lead tonetwork congestion. To limit this overhead, the common technique is to control flooding by either limiting the number of copies allowed to exist in the network, or by limiting the maximum number of hops a message can travel.

6.2. Partially Context-Aware Routing

Partially context-aware protocols exploit some piece of context information to optimize forwarding e.g. Encounter information and mobility information. Examples of this type of routing include Probabilistic Routing Protocol using History of Encounters and Transitivity (PROPHET),Spray & Focus and Bubble Rap.

6.3. Fully Context-Aware Routing

Fully context-aware protocols exploits any context information like node mobility information, history of node behavior or networks connectivity to optimize routing,and provide general mechanisms to handle and use context information and can be customized for the specific environment. These routing protocols can be used with any set of context information, thus allowing the system to be customized to the particular environment it has to operate in.Two protocols only fall in this category, i.e. context-aware routing (Musolesi, Hailes, and Mascolo, 2005) and HiBOp (History-based Opportunistic Routing protocol).

6.4.Mobility-Based Routing Protocols

Routing protocols that lie in the mobility-based category exploit more context information to make forwarding decisions, such as the mobility information of nodes. Node mobility impacts the effectiveness of routing in opportunistic mobile networks proved that it increases the performance of ad hoc networks, especially in the routing of messages when efficient routing techniques are deployed. When network mobility departs from the well-known random waypoint mobility model, the overhead carried by epidemic and/or taking into account the knowledge of node mobility can further reduce flooding based routing schemes. [6]

7. ADVANTAGES OF OPPORTUNISTIC COMMUNICATION

1. Potentially high capacity.
2. Low cost.
3. Localized communications.
4. Fully decentralized operation.
5. Independenceof any infrastructure.
6. Varying capabilitiesof the available networking technologies. [3]

8. PRIVACY AND SECURITY CHALLENGES FOR OPPORTUNISTIC NETWORKS

8.1 Increasing Trust And Secure Routing

A list of "more trusted" devices can be maintained. For example, we can trust more the devices owned by certain institutions, such as devices at police stations, government offices, hospitals, public libraries, universities or reputable companies. Once a list of trusted devices is made (which is a challenge), these devices will be used for more critical tasks than unknown devices or distrusted devices (such a 'black list' could be maintained as well). Secure routing can use both lists. Selecting a route that passes through only trusted devices (or as many trusted devices as possible) is challenging.

8.2. Helper Privacy and Oppnet Privacy

Oppnet can be feasible only if privacy of helpers can be guaranteed. Privacy of a helper can be guaranteed by its access controls (authentication and authorization) and by its intrusion prevention (using security primitives, relying on trust, secure routing etc.). Intrusion detection should be used as the second line of privacy security of information for helpers when prevention fails or cannot be used due to its inefficiency. Elimination or isolation of bad entities from oppnet via intrusion detection is very important for benevolent nodes. The problem of guaranteeing access control and performing real time intrusion detection for oppnets are more difficult than for the Internet, wireless or ad hoc networks because of the highly heterogeneous nature of participating devices and the spontaneous manner in which oppnets are formed. Privacy of oppnet is also important. Malicious entities can join the oppnet with the sheer purpose of violating privacy of oppnet members. A fear of having one's privacy violated can prevent candidate helpers invited by an oppnet from joining, or can cause reluctance (a passive or an active resistance) of the candidate helpers ordered by an oppnet to join.

8.3. Protecting Data Privacy

Messages in oppnet might be sent from one device to another device (peer to peer), or there can be intra-cluster communication among devices in some specific area. A local cluster head (a trusted device doing an extra job) can use public key cryptography while communicating with its neighbors. A cluster head can announce its public key. With in a communication network, each source node can encrypt data with the help of public key and, upon receiving encrypted data; the destination cluster head can decrypt them with its private key.

8.4. Ensuring Data Integrity

Data integrity is a part of data security, also a part of any secure communication. Digital signatures can be used to guarantee integrity of data. But they are too expensive computationally for weak devices (like cell phones, PDAs etc.) running on a limited battery power. Hence, alternatives should be devised to guarantee integrity of data packets. Also, packet sizes may vary when it travels through an oppnet. Suppose that a packet is sent from a cell phone to the base station through a PC connected to the Internet. In this case, the packet size when it travels from the cell phone to the PC will be different from the packet size when it travels from the PC to the base station. If packet fragmentation and aggregation cannot be performed securely, the end-to-end security mechanisms could fail.

8.5. Identifying Most Dangerous Attacks And Sketching Solutions

Some of the most important attacks, their effects and initial solutions to prevent those attacks:

8.5.1.MITM

Suppose a malicious device is on the path connecting a person in the house that needs help and the central controller. In this case, if the person sends request destined to the controller, the malicious device instead of forwarding it might inform the person that help is on the way. It could also tamper with messages broadcast by the controller.

Solution: A person in need can send redundant messages to the controller through multiple neighbors. This will increase the chances that least one of the multiple message copies will reach the controller, even if there are attackers on some paths. So, redundancy of routes can be exploited to avoid the attackers.

8.5.2. Packet Dropping

The malicious device might drop some or all the packets between the person in need and the controller. In the worst case, it might forward packets containing insignificant information and drop packets containing critical information.

Solution: The above-proposed idea of sending redundant messages using multiple neighbors may work if no adversary is situated on at least one path. Again, redundancy of routes can be exploited to avoid the attackers.

8.5.3.DoS Attacks By Malicious Devices

Malicious devices can generate false requests for help. They will keep the rescue team busy and unavailable for real emergencies.

Solution: Upper limit can be placed on the number of requests any device can generate. Thus, it will limit the number of times any device can send a false help request. In addition, the rescue team can attempt contacting the requester to confirm an emergency request.

8.5.3.1.DoS attacks on weak links

DoS attacks may target a “weak” device, such as a cell phone that is critical to oppnet operation (e.g., if it is the only device that connects two parts of a city). The battery of the cell phone is a very precious resource and should be used sparingly till an alternative connection is found. Some attacks may target only critical weak devices. Such surgical attacks are capable of defeating the goal of oppnets, which is to maintain connectivity in crisis.

Solution: Identification of weak devices, their strengthening (e.g., providing backups for them), or minimizing their workload is a major task for maintaining connectivity in oppnets. [9]

8.5.3.2. ID Spoofing

Mapping some node properties (like location) into node ID by a controller can be dangerous.A malicious device capable of masquerading can generate requests with multiple IDs, resulting in many false alarms for the rescue team. Services that need authentication can be misused if their IDs can be spoofed.A device capable of spoofing ID of a trusted node or a node with critical functions can pose many kinds ofattacks.

Solution: Although it is difficult to guarantee that malicious nodes will not join the oppnet, nodes can watch their neighbors for possible attempts of ID spoofing. The SAVE protocol can provide routerswith information needed for sourceaddress validation. This protocol needs to be modified to suit theheterogeneous nature of oppnets. [12]

8.5.4.Intrusion detection

The intrusion detection approach performs 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. An embedded detector performs direct monitoring because it have access to the internal data of the programs it monitor and analyzes intruders. Such data does not have to travel through an external path between its generation and its use. This reduces the chances that data will be modified before an intrusion detection component gets it. [11]

9.ENERGY-EFFICIENT OPPORTUNISTIC TOPOLOGY CONTROL IN WIRELESS NETWORKS

Topology control has been proposed as a promising technique to achieve energy and power efficiency in wireless mobile social networks. Existing fixed topology control algorithms used in wireless communication assume that wireless links are static, either connected or disconnected. Taking advantage of the time and frequency varying characteristics of wireless communication links, the energy-efficient opportunistic topology control problem, which exploits opportunistic communication to maximize energy-efficiency as well as to satisfy given network performance requirementby dynamic routing of context information. Opportunistic communication exploits the time-varying characteristic of wireless communication links to improve network performance of wireless mobile social network. Since every coordinator always turns on its radio, opportunistically leverage time diversity of channel conditions among multiple coordinators rather than relying on single coordinator. As shown in Figure 4, when node F transmits a packet of data to its neighboring coordinator C, there is a small probability that coordinator A or B can overhear the packet even link qualities of link FA and FB are bad. Since link AO has higher quality than link CO, the packet has a higher probability to reach O if node A successfully receives and forwards the packet. Furthermore, if link FA and FB can congregate to provide the same probability for a packet from node F to reach sink O as the topology in Figure 4, which save more energy by switching node C to a non-coordinator without sacrificing the end-to-end network performance from node F to sink O. [4] An adaptive device discovery protocol for reducing

energy and power consumption in different communication environments such as Bluetooth or WiFi of smartphone-based opportunistic communications are also used.

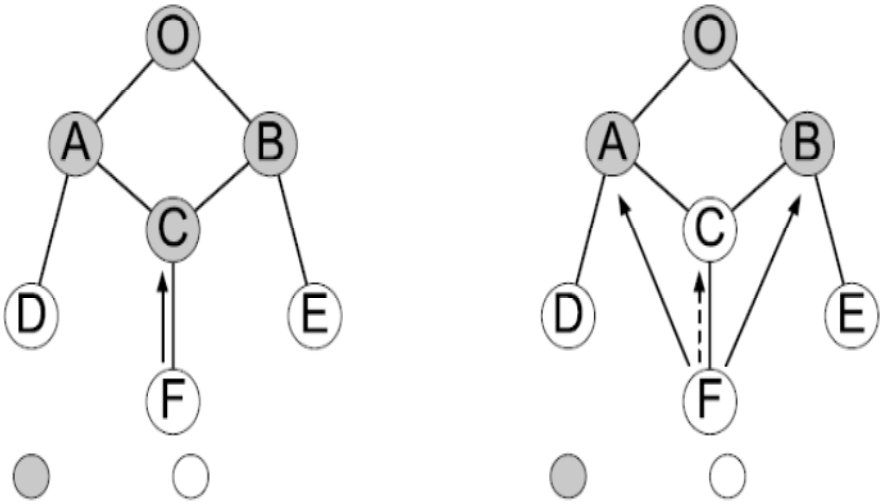

Figure4.Energy-efficient opportunistic topology control [4]

10. APPLICATIONS OF OPPORTUNISTIC COMMUNICATION

10.1.Wildlife Monitoring

Opportunistic networks applied to interdisciplinary projects focusing on wildlife monitoring. Usually, small monitoring devices are attached to animals, and an opportunistic network is formed to gather information and carry it to a few base stations based on the best opportunity possibly connected to the Internet. Contacts among animals are exploited to aggregate data, store and carry them closer and closer to the base stations. This is a reliable, cost-effective and non-intrusive solution of wildlife monitoring.

10.2.Internet Connectivity to Rural Areas

The use of opportunistic communication to bring Internet connectivity to rural areas. In developing countries and rural areas deploying the infrastructure required to enable conventional Internet connectivity is typically not cost-effective as fixed routing in conventional Internet connections. However, Internet connectivity is seen as one of the main booster to bridge the digital divide. Opportunistic networks represent an easy-to-deploy and extremely cheap solution forInternet connectivity to rural areas. Typically, rural villages are equipped with a few collection points that temporarily store messages, which are addressed to the Internet for wireless mobile social networking communication. Simple devices mounted on food court, bus, bicycles joggers

or motorbikes thatperiodically pass by the village collect these messages and bring them in regionswhere conventional Internet connectivity is available (e.g., a nearby city), where they can be delivered through the Internet to the destination.

10.3. Moving Vehicles

Opportunistic communication is to allow access to the Internet from moving vehiclessuch as for smart phones, the most popular mobile devices [8]. Such vehicles could gain access to the Internet from roadside wireless access points. Symmetrically, content created by the user of a mobile device could be placed into the infrastructure. By avoiding onerous charges for data transfer imposed by cellular providers, this mode of transfer makes it possible for device users to access rich multimedia content at low cost. This communication is opportunistic because vehicles lose connectivity as they move past the access point.

11. OPPORTUNISTIC COMMUNICATION IN MIMO WIRELESS LINK

In wireless communication systems multiple antennas at transmitter side and receiver side increase the transmission capacity (or bit rates) and improving the spectrum efficiency. Orthogonal Frequency Division Multiplexing can be applied in a multiuser applications leading to a highly flexible, efficient communications system.OFDM is a multicarrier multiplexing technique that divides an OFDM signal which is a sum of several sinusoids channel with a higher relative data rate into several orthogonal sub-channels with a lower data rate and has become one of the standard choices for high-speed data and multiuser transmission. [16]

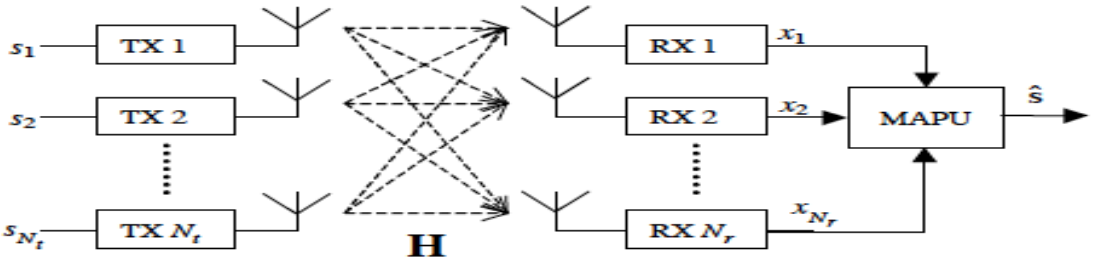

Figure 5. The physical model of a multi-antenna link

A communication system comprising **Nt**transmit (TX) and **Nr** receive (RX) antennas will be considered with MAPU = Multi Antenna Processing Unit. Fast and efficient algorithms are used to determine the optimal selection of antennas opportunistically at transmitter and receiving side. Opportunistic communication forming MIMO links gives advantage of multiuser diversity.

12. CONCLUSIONS

The continuous growth in wireless mobile networks connectivity, together with the increasing number of networked computational pocket devices equipped with wireless communication capabilities (e.g. WiFi, Bluetooth) populating among the global population, call for a deep rethinking of traditional communication systems and service architectures. It gives a strong

background for developing in opportunistic networks in which any mobile node can communicate opportunistically with any other node, fixed or mobile. Opportunistic mobile social networks are a novel communication paradigm that exploits opportunistic encounters between human carried devices and social networks for mobile social networking as opportunistic communication is implemented to obtain a more efficientutilization of the limited available radio spectrum gives overall high throughput.Wireless mobile social networking in opportunistic communication provides energy and power efficiency as well as privacy and network security by using different routingprotocols and topologies even it targets environments where mobile or fixed nodes wish to communicate are highly dynamic and of unpredictable topology.

REFERENCES

[1] ChiaraBoldrini, Marco Conti, Andrea Passarella, (2008) "Social-based Autonomic Routing in Opportunistic Networks", Springer 2008, pp 1-37.

[2] JianweiNiu, Xing Zhou, (Sept 2009) "A Data Transmission Scheme for Community-based Opportunistic Networks", 5th International conference on Wireless communications, Networks and Mobile Computing (Wi COM) IEEE, pp 1-5.

[3] MichelaPapandrea, Salvatore Vanini, Silvia, (June 2009)"A Lightweight Localization Architecture and Application for Opportunistic Networks"World Of Wireless, Mobile, and Multimedia Networks &Workshops (WoWMoM) IEEE, pp 1-3.

[4] Jian Ma, Chen Qian, Qian Zhang, (2008)"Opportunistic Transmission based QoS Topology Control in Wireless Sensor Networks",IEEE, pp 1-6.

[5] Schurgot, Mary R., (July 2012) "Beyond traditional DTN routing: social networks for opportunistic communication", Communications Magazine IEEE, Volume: 50, Issue: 7 , pp155 – 162.

[6] Hoang Anh Nguyen, Silvia Giordano, (2008) "Routing in Opportunistic Networks", Signals and communication, Springer.

[7] G. A.Medina-Acosta and Jos´e A. Delgado-Pen´ın, (2009) "Opportunistic Communication (Cognitive Radio) over Primary Discarded Subchannels by Applying a Double Power Distribution", Hindawi Publishing Corporation International Journal of Digital Multimedia Broadcasting, Volume 2010, pp 1-10.

[8] J.OttandD.Kutscher , (2005) "A Disconnection-Tolerant Transport for Drive-thru Internet Environments", In Proceedings of IEEE INFOCOM2.

[9] Leszek Lilien,1,2ZilleHuma Kamal,1 Vijay Bhuse,1 and Ajay Gupta, (2006) " Opportunistic Networks :The Concept and Research Challenges in Privacy and Security".

[10] L. Pelusi, A. Passarella, and M. Conti, (Nov. 2006) "Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad Hoc Networks," IEEE Communications, Vol. 44(11), pp. 134-141.

[11] D. Zamboni, (August 2001) "Using Internal Sensors for Computer Intrusion Detection", CERIAS Technical Report 2001-42, CERIAS, Purdue University, West Lafayette, IN.

[12] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang, (2001) "SAVE: Source Address Validity Enforcement Protocol," UCLA Technical Report 01-0004, Los Angeles, CA.

[13] N. Eagle and A. Pentland. (2005) "Social serendipity: Mobilizing social software", IEEE Pervasive Computing.

[14] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K. Fall, and H. Weiss, (April 2007) "Delay-Tolerant Networking Architecture", RFC 4838 (Informational).

[15] W. Zhao, M. Ammar, and E. Zegura, (2005) " Multicasting in delay tolerant networks: semantic models and routing algorithms", WDTN'05: Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-tolerant networking.

[16] A. van Zelst, R. van Nee and G.A. Awater, (2000) "Space Division Multiplexing (SDM) for OFDM systems"Bell Labs, Lucent Technologies.