International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 4, December - February, 2018 | Pages 26-31

WIRELESS MOBILE SOCIAL NETWORKING IN OPPORTUNISTIC COMMUNICATION

R. Ganeshan
Assistant Professor, Dept of CSE, St. Joseph College of Engineering Sriperumbudur, India
Dr. Paul Rodrigues
Professor, Dept of CSE, Indra Gandhi College of Engineering and Technology Chengalpattu, India

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. 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 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. 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.

2. RELATED WORK

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.

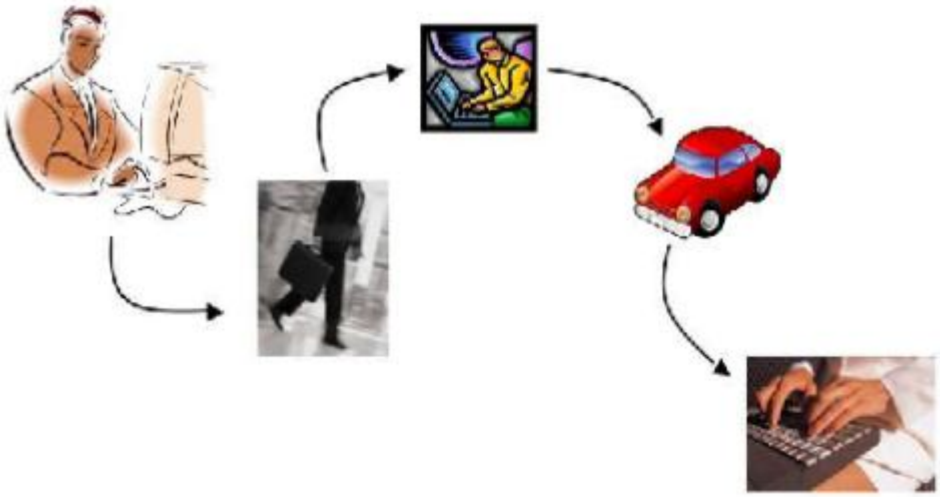

Fig.1.Networking Concept

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. 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 range are the norm.

3. PROPOSED SYSTEM

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. Opportunistic mobile networks can be seen as a generalization of DTNs (Delay Tolerant Networks). Specifically, in opportunistic mobile networks such as in DTNs, mobile social applications and 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 messages using routing protocols, such as 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. 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 context information in 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. 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.

4. ANALYSIS

Until recently, cellular networks were driven primarily by the need to provide voice telephony (Kumar & Manjunath 2008). However, with the growth of demand for mobile internet access, there arose a need to provide packetized data access on these networks as well. While mobile networks were developed with the primary objective of providing wireless access for voice services for mobile users, the growth of the internet as the de facto network for information dissemination has made internet access an integral requirement in most countries. While mobile phones have gained overwhelming prominence in the past decades, mobile phone networks were introduced as far back as the early 1980s and this technology was able to provide access to the wired phone network to mobile user, The mobility of wireless networks is another attribute that endears them to users.

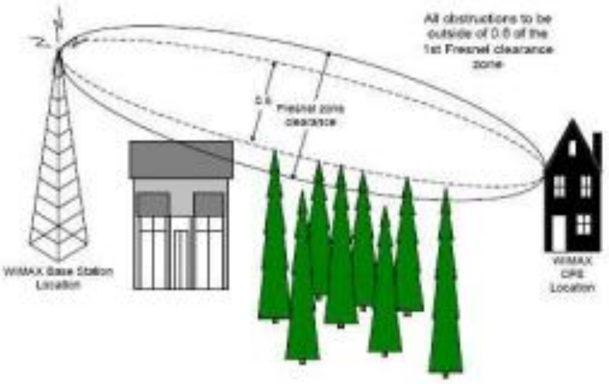
All obstructions to be outside of 0.6 of the 1st Fresnel clearance zone
0.6
Fresnel zone clearance
WiMAX Base Station Location
WiMAX CPE Location

Fig.3.Transmission

Wireless networks are built with the consideration that most users who want to access data will be mobile and wired connections may therefore prove to be a major inconvenience. With wireless networks, a person will remain connected as long as they are in within the range of an Access Point. Even so, mobility is not always a requirement for WLANs especially in indoor business settings where the users may be restricted to one physical location all day. Fifteen years ago, wireless networks were mostly limited to large institutes and government facilities which could afford the prohibitive cost of wireless infrastructure as well as laptops. However, the cost of wireless networks has reduced significantly which has aided in the growth of wireless LANS. It is more economical today to invest in a wireless network infrastructure than it is to set up a wired network which means that more individuals and organizations are opting for wireless networks.

CONCLUSION

This paper set out to discus wireless networks which are increasingly becoming preferred over wired networks by many users. The paper began by offering an overview of networking and then proceeded to define wireless networking and discuss the various technologies that are used. From the discussions provided in this paper, it is clear that wireless network solutions are increasing in popularity as they become more affordable and are adopted by more people. This paper has elaborated how wireless networks provide freedom from place restriction, scalability and flexibility. The most popular technologies are; Bluetooth, Wi-Fi, WiMAX and Cellular networks. The paper has confirmed that the mobility of wireless networks is their most desirable characteristic. It has been noted that in spite of their merits, there are a few significant issues with wireless networks which are primarily: quality assurance and security issues. Wireless links are noisier and less reliable than wired links due to the interference that occurs as the signals are transmitted. Engaging in site surveys before setting up a wireless network can help to mitigate this issue. Using strong encryption standards and can resolve the security issues inherent with wireless networks.

REFERENCES

1. Chenoweth, T Robert, M & Sharon, T 2010, "Wireless Insecurity: Examining User Security Behavior on Public Networks", Communications of the ACM, 53(2): 134-138.
2. Ganesh, R & Pahlavan, K 2000, Wireless Network Deployments, Springer, Boston.
3. Jordan, R & Abdallah, C 2002, "Wireless communications and networking: an overview", IEEE Antenna's and Propagation Magazine, 44 (1): 185-193.
4. Kumar, A & Manjunath, K 2008, Wireless Networking, Morgan Kaufmann, Boston.
5. Kumar, A 2010, "Evolution of Mobile Wireless Communication Networks: 1G to 4G", International Journal of Electronics & Communication Technology, 1(1): 68-72.
6. Malone S, 2004, Case Study: A Path towards a Secure, Multi-role Wireless LAN in a Higher Education Environment, SANS Institute, Massachusetts.
7. Mamaukaris, K V and Economides, AA 2003, Wireless technology in educational systems. International PEG Conference, St. Petersburg.