Mobile Ad Hoc Networks

Jiankun Hu
RMIT University, Australia

INTRODUCTION

The history of computer networks can be traced back to the early 1960s, when voice-grade telephone networks dominated the communication networks. With the increasing importance of computers, as well as the ever-increasing expense of centralized mainframe computers that were growing in size, there was a need to decentralize computer systems. This trend also highlighted the need to connect computers together, by means of computer networks, so that their capacity could be shared among geographically distributed users. Unlike the circuit switching telephone networks, where voice is transmitted at a constant rate between sender and receiver, the traffic in computer networks tends to be bursty. To meet the requirements of data communications, people began to invent more efficient and robust networks, i.e., packet switching networks. The first published work on packet-switching techniques was that of Leonard Kleinrock (Kleinrock, 1961, 1964). The first packet-switching computer network called ARPANET was developed in 1969 and then became the ancestor of today's public Internet (Kurose & Ross, 2001).

Over the last 30 years, the Internet has existed as a network with a fixed infrastructure that consists primarily of local area networks (LANs) interconnected via gateways or routers. However, such technology does not consider the requirements of mobile users, where locations of machines or even network topology may frequently change. With the increasing utilization of mobile devices such as laptops, PDAs, etc., as well as the development of wireless LAN technology, the next challenge was to be able to roam, i.e., be connected anywhere, anytime, within a connected environment. Mobile Internet protocol (IP) was designed to support such mobility through location management, tunneling, and security mechanisms (Macker & Corson, 1998). However, such solutions still relied on a fixed infrastructure. However, there are many important applications that cannot rely on the existing infrastructure. Typical examples include rapidly deployable battlefield networks, disaster relief management, wearable computing, virtual conferencing, home networking, sensor networks, personal area networks, etc.

Mobile ad hoc networking provides a useful technology to address this problem. Mobile ad hoc networking research was initiated nearly 20 years ago by the U.S. Government, including the Defence Advanced Research Projects Agency (DARPA), the U.S. Army, and the Office of Naval Research (ONR) (Macker & Corson, 1998). Ad hoc networks are autonomous networks operating either in isolation or as "stub networks" connecting to a fixed network. They do not rely on any existing infrastructure. There is no centralized authorization entity, such as central server, firewall, or router. Each node serves as router and forwards packets for other nodes in the network. The nodes may be located anywhere, such as in airplanes, ships, vehicles, or even on people. The nodes are normally equipped with wireless transmitters and receivers using antennas. The topology of the network continuously changes, which is in contrast with the static topology of existing Internet. There have already been several popular ad hoc networks including IEEE 802.11, Bluetooth, HomeRF, etc. (Othman & Xue, 2002). IEEE 802.11 wireless LANs are the fundamental components for most mobile technologies. Its position is very similar to that of the wired Ethernet. In 1997, the IEEE 802.11 standard was formed and involves the medium access control (MAC) and physical (PHY) layers for a wireless network connectivity. Subsequently, a family of IEEE 802.11 standards have been created ranging from 802.11a to IEEE 802.11 i. The difference among these standards is mainly in operational band and data rates (Wave Report, 2004). 802.11a, b, and g are the most popular WLANs. 802.11a operates in the 5 GHz band with data rate up to 54 Mbps. 802.11b operates in the 2.4 GHz band with data rates up to 11 Mbps. 802.11g is developing a higher-speed PHY extension to the 802.11b standard, while keeping backward compatibility with the 802.11b standard. The target data rate is at least 20 Mbps (WAVE Report, 2004).

Apart from the evolution of 802.11 that is based on networking technologies focusing on the MAC and PHY layers, another technology, Bluetooth, is becoming the most popular networking technology. Bluetooth tries to connect all kinds of devices, such as printers, computers, mobile telephones, digital cameras, PDAs, etc., without cables (Haartsen, Allen, Inouye, Joeressen, & Allen, 1998). Ad hoc network technology is the key to realizing our dream of communication anywhere, anytime, and will have a great impact on our future.

CRITICAL ISSUES OF AD HOC NETWORKING TECHNOLOGIES

Ad hoc networks have many benefits, such as self-reconfiguration and adaptability to highly variable mobile characteristics, such as power and transmission conditions, traffic distribution variations, and load balancing. However, such benefits come with some new challenges, largely due to the unpredictability of network topology resulting from the mobility of nodes. Although ad hoc networking technology has been developed over 20 years and has shown great promise, there still exist many open problems. The following sections will discuss several critical issues.

Security

An ad hoc network is a collection of mobile nodes without the requirement for a centralized control systems or fixed infrastructure. Security has become a primary concern in ad hoc networks because of the inherent poor quality of wireless mobile networks and the lack of centralized control mechanism. The wireless channel is accessible to malicious attackers. Without centralized control systems, there is no suitable place where traffic monitoring or access control mechanisms can be deployed. Consequently, there is no boundary between inside network and outside world. In fact, many existing ad hoc routing protocols such as Ad Hoc On Demand Distance Vector, the Dynamic Source Routing, and wireless MAC 802.11 protocols assume a trusted and cooperative environment. This provides a significant opportunity for an attacker to become a router and disrupt network operations by intentionally disobeying the protocol specifications (Yang, Luo, Ye, Lu, & Zhang, 2004). Furthermore, portable devices are vulnerable to compromise or physical capture, which may provide access for attackers to sneak into the network through these subverted nodes (Yang, Luo, Ye, Lu, & Zhang, 2004; Othman & Xue, 2002).

Routing

As the topology of an ad hoc network is, by definition, constantly changing, it is very difficult to route packets between any pair of nodes. Multicast routing is also difficult, because the multicast tree is no longer static due to the random movement of nodes within the network (Hong, Xu, & Gerla, 2002).

Quality of Service (QoS)

The random nature of communication within ad hoc networks makes it very difficult to guarantee the quality of service (QoS) offered to a device. Also, for portable mobile terminals, limitations on power consumption pose a constraint on the storage and processing capacity of the device, which further reduces the capacity to maintain a high QoS in an ad hoc network (Lee & Lee, 2002; Raju, Hernandez, & Zou, 2000; Sivakumar, Sinha, & Bharghavan, 1999).

CONCLUSION

Ad hoc network technology is the key to the realization of the dream of ICT anywhere, anytime, and is likely to have a great impact on our near future. This article has introduced the technology and discussed some of the implications and challenges it poses to the community. Several critical issues have been discussed. Among them, security is the most important, as using the wireless ad hoc networking environment makes networks vulnerable to unsolicited attacks. Cryptographic mechanism is still the basis for secure membership management, secure routing, prevention of eavesdropping, etc.; but it cannot help other issues commonly available in traditional networks, such as denial of service (Buttyan & Hubaux, 2003; Manikopoulos & Ling, 2003). For QoS in ad hoc networks, QoS-based routing seems to offer a promise to meet end-to-end QoS requirements (Aggelou & Tafazolli, 2001). However, such an approach cannot deal with hand-off very well. Although the current development of mobile ICT has not yet completely solved all the critical issues, it is still feasible to deploy current mobile technology to some simple application scenarios that have low security requirements, such as routine conferences and regional community development applications, etc. However, current technology development for mobile ICT has great application for many regional community needs, and this sector will benefit a great deal from exploration of its potential.

REFERENCES

Aggelou, G. N., & Tafazolli, R. (2001). QoS support in the 4th generation mobile multimedia ad hoc networks. *Proceedings of the Second International Conference on 3G Mobile Communication Technologies* (pp. 412-416).

Buttyan, L., & Hubaux, J. P. (2003). Report on a working session on security in wireless ad hoc networks. *ACM SIGMOBILE Mobile Computing and Communications Review, 7*(1), 74-94.

Haartsen, J., Allen, W., Inouye, J., Joeressen, O., & Allen, W. (1998). Bluetooth: Vision, goals, and archi-