How Hyperlan, IEEE 802.11 and Bluetooth are Responsible in Growth and Commercial Deployment of MANET

Krishan kumar
Ph D (CSE) Research Scholar, Singhania University
Pacheri bari (jhunjhunu) Rajasthan, India

Abstract - A Mobile Ad Hoc Network is a collection of mobile wireless nodes. It has no authority and is dynamic in nature. Energy conservation issue is essential for each node and leads to potential selfish behavior. Nodes can tend to limit their support to other nodes as this costs energy and has no revenue. Thus, despite the fact that technology and networking are here to stay, practical problems certainly arise from being highly uncoordinated. And the nodes move, which introduces uncertainty and complexity into the forwarding process. The need of mechanisms for stimulate.

I. INTRODUCTION AND OBJECTIVE OF RESEARCH WORK

Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ‘‘ad-hoc’’ network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure, e.g., disaster recovery environments. Ad hoc networking concept is not a new one, having been around in various forms for over 20 years. Traditionally, tactical networks have been the only communication networking application that followed the ad hoc paradigm. Recently, the introduction of new technologies such as the Bluetooth, IEEE 802.11 and Hyperlan are helping enable eventual commercial MANET deployments outside the military domain. These recent evolution have been generating a renewed and growing interest in the research and development of MANET. This paper attempts to provide a comprehensive overview of this dynamic field. It first explains the important role that mobile ad hoc networks play in the evolution of future wireless technologies. Then, it reviews the latest research activities in these areas, including a summary of MANET_s characteristics, capabilities, applications, and design constraints. The paper concludes by presenting a set of challenges and problems requiring further research in the future.

A major goal toward the 4G Wireless evolutionis the providing of pervasive computing environments that can seamlessly and ubiquitously support users in accomplishing their tasks, in accessing information or communicating with other users at anytime, anywhere, and from any device [1]. In this environment, computers get pushed further into background; computing power and network connectivity are embedded in virtually every device to bring computation to users, no matter where they are, or under what circumstances they work. These devices personalize themselves in our presence to find the information or software we need.

The new trend is to help users in the tasks of everyday life by exploiting technologies and infrastructures hidden in the environment, without requiring any major change in the users_ behavior. This new philosophy is the basis of the Ambient Intelligence concept [1]. The objective of ambient intelligence is the integration of digital devices and networks into the everyday environment, rendering accessible, through easy and ‘‘natural’’ interactions, a multitude of services and applications. Ambient intelligence places the user at the center of the information society. This view heavily relies on 4G wireless and mobile communications. 4G is all about an integrated, global network, based on an open systems approach. Integrating different types of wireless networks with wire-line backbone network seamlessly, and convergence of voice, multimedia and data traffic over a single IP-based core network are the main foci of 4G. With the availability of ultra-high bandwidth of up to 100 Mbps, multimedia services can be supported efficiently; ubiquitous computing is enabled with enhanced system mobility and portability support, and location-based services are all expected. Fig. 1 illustrates the networks and components within 4G network architecture.

II. Review of Literature

In 1997, the IEEE adopted the first wireless local area network standard, named IEEE 802.11, with data rates up to 2 Mbps [2]. Since then, several task groups (designated by the letters from _a_, _b_, _c_, etc.) have been created to extend the IEEE 802.11 standard. Task groups_ 802.11b and 802.11a have completed their work by providing two relevant extensions to the original standard [3], which are often referred to with the friendly name of Wireless Fidelity (Wi-Fi). The 802.11b task group produced a standard for WLAN operations in 2.4 GHz band, with data rates up to 11 Mbps and backward compatibility. This standard, published in 1999, has become an ‘‘overnight success’’, with several IEEE 802.11b products available on the market currently. The 802.11a task group created a standard for WLAN operation in the 5 GHz band, with data rates up to 54 Mbps. Among the other task groups, it is worth mentioning the task group 802.11e (attempting to enhance the MAC with QoS features to support voice and video over 802.11 networks), and the task group 802.11g (that is working to develop a higher speed extension to the 802.11b).

The IEEE 802.11 standard defines two operational modes for WLANs: infrastructure-based and infrastructure-less or ad hoc. Network interface cards can be set to work in either of these modes but not in both simultaneously. Infrastructure mode resembles cellular infrastructure-based networks. It is the mode commonly used to construct the so-called Wi-Fi hotspots, i.e., to provide wireless access to the Internet. In the ad hoc mode, any station that is within the transmission range of any other, after a synchronization phase, can start communicating. No AP is required, but if one of the stations operating in the ad hoc mode has a connection also to a wired network, stations forming the ad hoc network gain wireless access to the Internet.

The IEEE 802.11 standard specifies a MAC layer and a Physical Layer for WLANs. The PHY
layer uses either direct sequence spread spectrum (ISM band, 2.4–2.4835 GHz), frequency-hopping spread spectrum, or infrared (IR) pulse position modulation (300–428,000 GHz) to transmit data between nodes. Infrared is more secure to eavesdropping, because IR transmissions require absolute line-of-sight links, contrary to radio frequency transmissions, which can penetrate walls and be intercepted by third parties unknowingly. However, infrared transmissions are more receptive to interference, e.g., sunlight [4].

III. Methodology

The MAC layer offers two different types of service: a contention-free service provided by the Distributed Coordination Function (DCF), and a contention-free service implemented by the Point Coordination Function (PCF). The PCF is implemented on top of DCF and is based on a polling scheme. It uses a Point Coordinator that cyclically polls stations, giving them the opportunity to transmit. Since the PCF cannot be adopted in the ad hoc mode, hereafter it will not be considered. The DCF provides the basic access method of the 802.11 MAC protocol and is based on a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme. According to this scheme, when a node receives a packet to be transmitted, it first listens to the channel to ensure no other node is transmitting. If the channel is clear, it then transmits the packet. Otherwise, it chooses a random ‘‘back-off value’’ which determines the amount of time the node must wait until it is allowed to transmit its packet. During periods in =which the channel is clear, the node decrements its backoff counter. When the backoff counter reaches zero, the node transmits the packet. Since the probability that two nodes will choose the same backoff factor is small, the probability of packet collisions, under normal circumstances, is low. In WLAN, there is usually just one antenna for both sending and receiving, and hence the stations are not able to listen while sending. For this reason, in the CSMA/CA scheme there is no collision detection capability. Acknowledgment packets (ACK) are sent, from the receiver to the sender, to confirm that packets have been correctly received.

As no collision detection mechanism is present, colliding stations always complete their transmissions, severely reducing channel utilization, as well as throughput, thus presenting new challenges to conventional CSMA/CD-based MAC protocols. Several works have shown that an appropriate tuning of the IEEE 802.11 backoff algorithm can significantly increase the protocol capacity [5]. The basic idea is that the random backoff duration, before attempting to transmit the packet, should be dynamically tuned by choosing the contention window size as a function of the network congestion. By following this approach, the authors in define and evaluate an extension to the IEEE 802.11 protocol to optimize protocol capacity and energy consumption, showing also that the optimal capacity state, and the optimal energy consumption state almost coincide. In wireless ad hoc networks that rely on a carrier- sensing random access protocol, such as the IEEE 802.11, the wireless medium characteristics generate complex phenomena such as the hidden station and the exposed-station problems. 4 The hidden-station problem occurs when two (or more) stations, say A and C, cannot detect each other_s transmissions (due to being outside of each other transmission range) but their transmission ranges are not disjoint. As shown in Fig. 4, a collision may occur, for example, when the station A and station C start transmitting towards the same receiver, station B in the figure. A virtual carrier-sensing mechanism based on the RTS/CTS mechanism has been included in the 802.11 standard to alleviate the hidden-terminal problem that may occur by using the physical carrier sensing only. Virtual carrier sensing is achieved by using two control frames, Request To Send (RTS) and Clear To Send (CTS), before the data transmission is actually taken place. Specifically, before transmitting a data frame, the source station sends a short control frame, named RTS, to the receiving station announcing the upcoming frame transmission. Upon receiving the RTS frame, the destination station replies by a CTS frame to indicate that it is ready to receive the data frame. Both the RTS and CTS frames contain the total duration of the transmission, i.e., the overall time interval needed to transmit the data frame and the related ACK. This information can be read by any station within the transmission range of either the source or the destination station. Hence, stations become aware of transmissions from hidden station, and the length of time the channel will be used for these transmissions. The exposed-terminal problem results from situations where a permissible transmission from a mobile station (sender) to another station has to be delayed due to the irrelevant transmission activity between two other mobile stations within sender_s transmission range. Fig. 5 depicts a typical scenario where the ‘‘exposed station’’ problem may occur. Let us assume that station A and station C can hear transmissions from B, but station A cannot hear transmissions from C. Let us also assume that station B is transmitting to station A, and station C has a frame to be transmitted to D. According to the CSMA scheme, C senses the medium and finds it busy because of B_s transmission, and therefore refrains from transmitting to D, although this transmission would not cause a collision at A. The ‘‘exposed station’’ problem may thus result in loss of throughput. It is worth pointing out that the hidden-station and the exposed-station problems are correlated with the Transmission Range (TX_range). TX_range is the range (with respect to the transmitting station) within which a transmitted packet can be successfully received. The transmissionrange is mainly determined by the transmission power and the radio propagation properties. By increasing the Transmission Range, hidden-station problem occurs less frequently, while the exposed station problem becomes more important as the TX_range identifies the area affected by a single transmission. In addition to the Transmission Range, also the Physical Carrier Sensing Range and the Interference Range must be considered to correctly understand the behavior of wireless (ad hoc) networks:

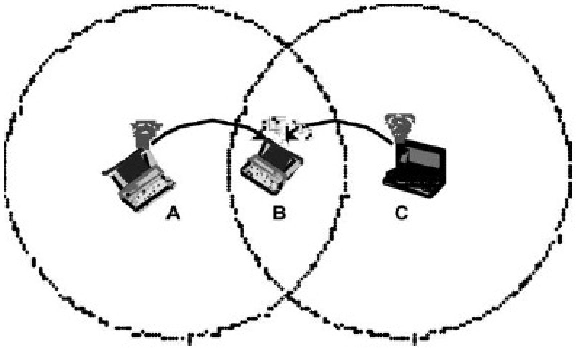

Fig. 4. Hidden-station problem.

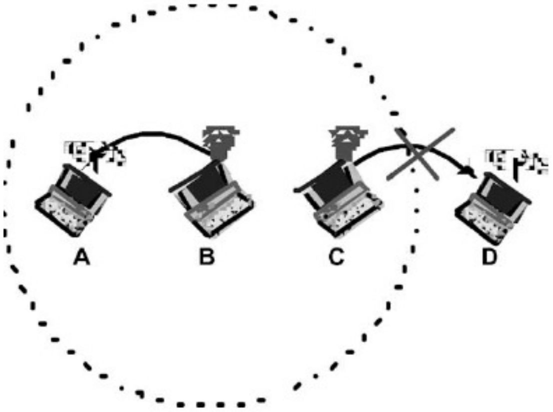

Fig. 5. Exposed-station problem.

- The Physical Carrier Sensing Range (PCS_range) is the range (with respect to the transmitting station) within which the other stations detect a busy channel. It mainly depends on the sensitivity of the receiver (the receive threshold) and the radio propagation properties.

- The Interference Range (IF_range) is the range within which a station in receive mode will be interfered with by a transmitter, and thus suffer a loss. More precisely, a transmitting station A can interfere with a receiving station B if A is within the B interference range. The interference range is usually larger than the transmission range, and is a function of the path loss model. Altogether, the TX_range, PCS_range, and IF_range define the relationships existing among 802.11 stations, when they transmit or receive.

IV. Findings about Network security and cooperation

Wireless mobile ad hoc nature of MANET brings new security challenge to the network design. Mobile wireless networks are generally more vulnerable to information and physical security threats than fixed wired networks. Vulnerability of channels and nodes, absence of infrastructure and dynamically changing topology, make ad hoc networks security a difficult task. Broadcast wireless channels allow message eavesdropping and injection (vulnerability of channels). Nodes do not reside in physically protected places, and hence can easily fall under the attackers_ control (node vulnerability). The absence of infrastructure makes the classical security solutions based on certification authorities and on-line servers inapplicable. Finally, the security of routing protocols in the MANET dynamic environment is an additional challenge.

The self-organizing environment introduces new security issues that are not addressed by the basic security services provided for infrastructure based networks. Security mechanisms that solely enforce the correctness or integrity of network operations would thus not be sufficient in MANET. A basic requirement for keeping the network operational is to enforce ad hoc nodes_ contribution to network operations, despite the conflicting tendency (motivated by the energy scarcity) of each node towards selfishness [6].

V. Conclusion

In coming years, mobile computing will keep flourishing, and an eventual seamless integration of MANET with other wireless networks, and the fixed Internet infrastructure, appears inevitable. Ad hoc networking is at the center of the evolution towards the 4th generation wireless technology. Its intrinsic flexibility, ease of maintenance, lack of required infrastructure, auto-configuration, self administration capabilities, and significant costs advantages make it a prime candidate for becoming the stalwart technology for personal pervasive communication. The opportunity and importance of ad hoc networks is being increasingly recognized by both the research and industry community, as evidenced by the flood of research activities, as well as the almost exponential growth in the Wireless LANs and Bluetooth sectors.

From the economic standpoint, the main question to be addressed in the MANET model is the identification of business scenarios that can move MANET_s success beyond the academy and research labs. Currently, apart from specialized areas (battlefield, disaster recovery, etc.), the main business opportunity appears to be in tools (see, e.g., Mesh Networks 5 and SPAN works 6), which let PDAs and/or laptops, set up ‘‘self-organizing networks’’. However, no clear understanding of a MANET ‘‘killer application(s)’’ has yet emerged. Legacy, content-orientated services and applications enhanced by the self-organizing paradigm could become such an application, as similar to SMS, it would allow to exploit the mobility provided by cellular systems. Users_ benefits gained with the use of the ad hoc technology could make the difference compared to legacy applications (shared whiteboard, chat, file-sharing). Part of bringing the MANET technology to the users is the development of large testbeds with direct users_ involvement, as in [190].

References

[1] E.L. Madruga, J.J. Garcia-Luna-Aceves, Scalable multicasting: the core assisted mesh protocol, ACM/Kluwer Mobile Networks and Applications Journal 6 (2001) 151–165.: 3.

[2] IEEE standard for Wireless LAN- Medium Access Control and Physical Layer Specification, P802.11, November 1997.

[3] Web site of the IEEE 802.11 WLAN: http://grouper.ieee.org/grups/802/11/main.html.

[4] Wireless World Research Forum (WWRF): http://www.ist-wsi.org.

[5] J. Weinmiller, M. Schl€ager, A. Festag, A. Wolisz, Performance study of access control in wireless LANs-IEEE 802.11 DFWMAC and ETSI RES 10 HIPERLAN,ACM/Baltzer Mobile Networks and Applications 2 (1997) 55–67.

[6] P. Michiardi, R. Molva, Simulation-based analysis of security exposures in mobile ad hoc networks, in: roceedings of European Wireless Conference, 2002.

[7] European Commission, FET-IST Programme, MobileMAN project (IST-2001-38113). Available from <http:// cnd.iit.cnr.it/mobileMAN/>..