An increasing number of households own more than one computer and use WLANs to network and access the Internet through a single DSL or cable modem connection. In parallel to these private WLANs owned and used by companies and individuals, public WLANs are emerging, providing wireless Internet access in public places such as airports, hotels, cafes, libraries, malls, convention centers, and hospitals. Today, there are tens of thousands of public hotspots (www.publicinternetproject.org) in the U.S. alone.

Several entrepreneurial organizations have embarked on various approaches to cluster these private and public WLANs to create pervasive wireless broadband networks (WBNs) that can be citywide or even nationwide [10]. Among them, many not-for-profit initiatives have evolved into community-oriented wireless commons, in which participants share their hotspots with others. As wireless access needs increase with the rapid proliferation of mobile handheld computing devices, wireless commons are expected to play an indispensable role for communications and commerce in coming years. Thus it becomes important to understand: How do these wireless commons create common good? How can the participants who consume the freely available

By Jan Damsgaard, Mihir A. Parikh, and Bharat Rao
resources cause an eventual demise of the commons? What countermeasures will allow the commons to continue to flourish?

We conducted an extensive research study spanning over two years to understand this intriguing but important phenomenon. Here, we present the lessons learned, which can be useful to various constituents, including individual users, commons organizers, community leaders, technology providers, mobile operators, regulators, and researchers.

The building of communications infrastructure and services, especially in the “last mile,” has traditionally been undertaken by for-profit companies, which collect fees for access to their proprietary infrastructure. In the wireless arena, T-Mobile, Wayport, Telstra, and British Telecom are some of the companies that have established their own WBNs through this traditional approach. This planned growth approach is similar to the provision of telephone services, cellular services, electricity, water, and television cable. For it to succeed, huge up-front infrastructural investment, stable technologies, and regulation are required.

In the wireless arena, several community-oriented wireless commons are emerging in parallel to provide wireless access to community members and create alternate WBNs. Wireless commons are based on the notion that each commons participant allows other participants to access the Internet through his or her WLAN hotspot. Thus, all participants can access the Internet even when they are operating in other participants’ hotspots. In a wireless commons, therefore, the user is both a provider and consumer of wireless service. This is similar in some ways to open source projects in the software sector, and it is the opposite of the traditional model in which a user is only a passive consumer and the provider is a separate company. This emergent, organic growth approach depends on the commitment and contributions of participants willing to share their WLANs with others. If only a few participants are willing to share, the resultant wireless commons will be highly fragmented, but if the idea catches on there is a potential for a comprehensive and robust infrastructure.

Wireless commons can be one of two types: closed or open. Closed commons are made up of a specified group of user members, like consumer cooperatives. Usually, founding members come together to develop the initial charter of a commons with a specific purpose, policies, and regulations. New members, who agree with the purpose and rules, are invited into the commons and are required to register their devices. These groups are characterized by shared understanding, common history, written rules, and accepted norms for resource utilization and sanctions for violators. User participation is authenticated and monitored through MAC address filtering, masking ESSID, and/or adding a special login layer.

Open commons are formed by communities and enthusiasts with the objective of providing bandwidth resources free of charge to the general public. Once an open commons is set up, more enthusiasts can add their WLANs to it and the open commons grows. In some cases, open commons are initiated, operated, and/or funded by local business associations, charitable foundations, large corporations, and government organizations. NYCwireless, WAGZ in Athens (Georgia, U.S.), SWAG in Sydney (Australia), and Wireless Leiden (Netherlands) are examples of such open commons [6]. Founding members of open commons have specific shared goals or interests that provide the reason for developing a common resource. These groups are characterized by intense interactions, strong emotional ties, shared activities, intra-community support, and social conventions, language, or protocols [11]. The overall objective is to share the available resources in such a way that optimizes the good for the group. Open commons are not directly controlled by any pre-specified rules, but they are often self-governed by general societal norms for
fair usage and the users’ adherence to them in practice.

The Tragedy of the Commons
As noted earlier, a wireless commons is a group in which individuals take actions toward creating and using a common resource by opening their private WLANs to others. However, some individual actions may have unintended effects on the group, especially when the interests of the group and individual are in conflict. Actions that are justified from the perspective of an individual may be unjustified from the perspective of the group or society to which the individual belongs. Consequently, the actions with positive effects at the individual level can exert negative effects at the group level. This tension between individual and group interests has often been characterized using “the tragedy of the commons” metaphor [5].

Hardin [5] describes the tragedy as a situation in which too many actors have privileges to consume a common resource leading to its overuse and eventual collapse. Many have studied the behavior of commons and the implications of Hardin’s suggestions in various fields [8]. The tragedy of the commons has been described as a social trap because behavior that gratifies an individual in the short-term has high long-term collective costs [3, 9]. When an individual gets locked into a self-gratifying behavior that is destructive for the common resource, other individuals in the group may copy the behavior for selfish reasons. In the long term, these individuals become victims of their collective actions. This self-inflicting mechanism is labeled as downward causation, in which the parts are constrained by the whole [1, 2]. If each individual realizes she is a part of a perishable whole, she might moderate her actions so her consumption of the common resource will not lead to its destruction, but instead to a sustainable common resource.

In a wireless commons, Internet access bandwidth—a common and finite resource—is shared by a group of users. Action of one commons user, however appropriate from that individual’s perspective, can have negative repercussions for the group. For the tragedy to occur, it is assumed that each commons user, as a rational being, will seek to maximize private gain as a wireless commons participant. Using Hardin’s [5] framework, a user would try to maximize his utility by considering the marginal utility of adding an additional wireless device to a wireless commons to use the available bandwidth. As a consequence, each rational person keeps adding wireless devices to the commons, resulting in insufficient bandwidth for all devices in the commons—and leading to the downfall of the commons. One member may decide not to add more devices to preserve the commons, but she has no means to prevent others from adding more devices. Thus, a race to consume the commons begins until the commons is entirely gone.

Here, we analyze causes of such tragedies and discuss what can be done to prevent them or reduce their effects, allowing the commons to stay healthy and grow to provide better services.

Causes and Countermeasures
There are numerous ways in which members can harm the wireless commons (see the accompanying figure). Using a pasture and cattle metaphor, we describe various causes of the tragedy and discuss ways to deal with them. While the pasture and cattle metaphor is not an exact parallel to wireless commons, it provides a comparable, familiar example to understand the perils in the common good provided by wireless commons.

Overgrazing. This is the most common form of destroying the commons. Using the pasture metaphor, overgrazing occurs when cow owners add more cows than the pasture can sustain. Such overgrazing can result in the starvation of all cows. In the WBN context, overgrazing involves adding more wireless devices than the available bandwidth can bear. As a result, the available bandwidth is below the practical use for any device. In open commons, not much can be done to reduce this, because one member cannot prevent others from adding more devices than their fair share. However, when overgrazing becomes a critical problem, commons organizers can add a maximum limit on connect time for all devices and have a predefined time lapse before a specific device can reconnect. This can reduce the load on the network but not overgrazing, as the overgrazing member can still have an unfair share of whatever time/bandwidth is available. In closed commons, one way to deal with this is to limit devices in a hotspot to a specific number per registered user depending on backhaul bandwidth availability. Another way is to limit network access to a specified amount of time. Both can be implemented through a software-based solution, which can serve users on a first-come-first-served basis.

Stealing. As those who milk cows that belong to another are stealing, in the WBN context, those who usurp the devices of others and use them for private needs are stealing. Examples include gaining access to and taking over the bandwidth of someone else’s wireless device or using processing power or storage capacity of other users without their permission or knowledge. Stealing becomes more important in
When an individual gets locked into a self-gratifying behavior that is destructive for the common resource, other individuals in the group may copy the behavior for selfish reasons. These individuals become victims of their collective actions.

commons where there are many permanent, stationary devices and fewer nomadic devices. The former are more likely to be penetrated by unscrupulous users. When a commons primarily has nomadic devices, this peril is less relevant. In open commons, users must safeguard their devices through various security protocols to avoid thievery by other users. In closed commons, each attached device should be automatically monitored for bandwidth usage. If a device continuously uses more bandwidth than normal, the availability should be reduced, or the user should be removed from the commons. Similar to this scenario is the creation of an “evil twin,” in which a hacker creates an identical access point masquerading as a real one in a closed commons, using tools like Airsnort, and captures private information of commons users [7].

Poaching. As poachers ensure the availability of grass for their cows by destroying cows belonging to others, in the WBN context, poachers block the operation of others’ devices so the remaining devices have more bandwidth. Unlike with stealing, where a device is partly hijacked and used by another user, in poaching a device is disabled by a poacher. In open commons, protecting devices from such miscreants is the only way to deal with poaching. In closed commons, community monitoring and periodical analysis of user complaints by the overseeing body of the commons can identify offenders. If they continue to poach, after an initial warning, they can be removed from the commons.

Tainting. Using the pasture metaphor, tainting involves infecting cows belonging to others through negligence. A cow owner may allow a cow with a contagious disease to enter the pasture out of carelessness or ignorance. In the WBN context, tainting involves adding a device with computer viruses or worms, or attaching an access point that does not fully comply with the wireless standard and may cause disruptive signals that affect other devices. The user who brings a tainted device may not even know that the device is tainted. In open commons, the best ways to deal with tainting is to regularly vaccinate devices and avoid the use of the hotspots with non-standard, non-certified equipment. In closed commons, infected devices should be quarantined. When a new hotspot is added, its usability and compliance to the standard should be fully checked before making it a part of the commons.

Contamination. When a pasture is polluted, the amount of grass available for grazing is reduced, and the commons cannot sustain as many cows. Someone who does not have enough cows to make use of her fair share of the pasture could feel inclined to contaminate the commons out of jealousy; preventing others from having what she cannot have. In the WLAN context, contamination means shutting down or password protecting a hotspot when one does not require the use of the commons. Another mode of contamination can be maliciously consuming the bandwidth for trivial purposes such that others cannot use it. Even bringing an 802.11b compliant device in an entirely 802.11g hotspot can contaminate the hotspot because it may cause the speed of the entire network to regress to the older and slower 802.11b standard. Contamination differs from tainting in that tainting affects a specific unprotected device(s), whereas contamination affects all devices in a hotspot. In open commons, not much can be done to stop contamination, as it is not practical to regulate the behavior of the users. In closed commons, such members or the hotspots can be removed from the commons.

CONCLUSION

Wireless commons provide a unique and organic way to build a wireless broadband infrastructure. This approach, however, is prone to be negatively affected by various individual actions, which may seem completely rational from the perspectives of individuals but can be detrimental on the group
level. In most cases of the wireless commons, some technological solutions are available to reduce misuse of the available resources, but the commons primarily depend on the cooperative behavior of the users [4]. Increasing the number of hotspots or the bandwidth may not resolve the tragedy, as each member of a commons may still be compelled to add devices to the commons leading to its demise. Here, we outline some steps that may help slow down the tragedy. Given it is mostly a social problem, technical solutions may only help postpone the inevitable. If the rate of technological innovations outpaces the rate at which bandwidth is used, as in the past, the wireless commons that continuously upgrade technologies and take additional preventive steps would survive. Recently, 802.16x (Wi-Max) wireless standards have emerged. They provide a bigger footprint and higher bandwidth, but they may not protect wireless commons from the issues we discussed in this article.

**Infrastructure-related steps**
- Install MAC address filtering,
- Deploy network administration software for continual link-quality monitoring,
- Register only a limited number of devices per user in closed commons,
- Permit only standard and certified network equipment in commons,
- Assist users in installing firewalls and virus protection software on their computing devices.

**Operations-related steps**
- Periodically monitor user logs, statistics, and performance reports,
- Set maximum log-in time limits for connecting devices when a hotspot gets saturated frequently,
- Encourage users to monitor intrusions and update safeguards on their computing devices,
- Automatically quarantine tainted devices,
- Set up mechanisms for logging, monitoring, and resolving user complaints. Also, check for patterns in the complaints that match a specific peril,
- Develop guidelines to warn first-time offenders and reprimand regular offenders.

Although wireless commons are similar to other types of commons (including physical commons such as the cattle and pasture scenario used earlier), they have unique characteristics, such as:

1. Wireless commons are not a natural resource but are created by people.
2. The size of a WBN commons is not fixed like its physical counterparts; its size varies depending on the number and quality of hotspots associated at a given point of time.
3. The utilization of a wireless commons fluctuates rapidly and constantly; many people move through certain physical areas (such as train stations) at certain times of the day, resulting in no or poor service in some parts of the WBN and underutilization in other parts. This also creates a disincentive for people close to public meeting places to open their WLAN.
4. The resources made available by a wireless commons are perishable; that is, if they are not used at the time of availability, they vanish.

These critical differences may also affect the ways and the speed at which the wireless commons would be affected by the tragedy.

**References**


**Jan Damsgaard** (damsgaard@cbs.dk) is a professor in the Department of Informatics, Copenhagen Business School, Denmark. **Mihir A. Parikh** (mihir.parikh@bus.ucf.edu) is an assistant professor in the Department of Management Information Systems, University of Central Florida, Orlando. **Bharat Rao** (brao@poly.edu) is an associate professor in the Department of Management at Polytechnic University, New York.