distributed to the access point and the device to encrypt the bidirectional traffic – keys are not shared between clients on the same access point. This brings enterprise-grade security to public hotspots.

Public hotspots differ from enterprise or home access points in that the various users on a Passpoint hotspot have no reason to trust one another. Therefore Passpoint requires that when the network type is 'public', whether free or chargeable, individual users are firewalled from each other – it is possible to address one hotspot-connected device from another, but the traffic has to pass through a firewall function either integral to or upstream of the access point before being delivered to the recipient.

Passpoint also requires a proxy-ARP implementation on the access point to prevent ARP spoofing attacks from one client to another. Similarly, multicast or broadcast (it's the same function in Wi-Fi, frames are received by all clients of the AP) requires a Group Key to be shared across all devices and can be disabled on Passpoint hotspots: this represents another need for the proxy ARP function above. And Passpoint prohibits P2P operation, DLS and TDLS methods of peer-to-peer communication within the hotspot.

There are recommendations in Passpoint that a mobile device should provide an indication to the user that link-layer security is in use and that the device is connected to a hotspot using Passpoint. As users become aware of the improved security available on Passpoint hotspots they should become familiar with these indicators (similar in concept to the security-lock displayed on browsers) and notice when they are absent. It's not yet clear whether the industry will develop universal logos for these indications.

Note that even though Passpoint guarantees good over-the-air security when correctly implemented, it is likely that traffic will be decrypted on the access point and forwarded onto the backhaul connection and the Internet en-clair. Users should be aware that if they want privacy over the wired portion of the connection, they will need to implement end-to-end security such as a VPN function. This is no different from a home access point or many small businesses, but it should be borne in mind when considering hotspot use.

BROADER APPLICATIONS FOR PASSPOINT

Passpoint includes so many parameters and options that we will surely find many new and unexpected applications for it in the coming months and years. But the basic public hotspot application will be the most immediate.

Over the coming months and years we will see an explosion in the number of public Wi-Fi hotspots. Some of the impetus will come from cellular service providers eager to offload traffic, particularly high-bandwidth video users in high-density locations such as city centers, airports and stations, sports stadiums and shopping centers. Now that hotspot operators and service providers can rely on known behavior in the client, and mobile device providers can pre-configure handsets, tablets and PCs based on predictable network behavior, the amount of traffic that is automatically passed to Wi-Fi networks will snowball.

Many countries and cities will see a significant increase in service provider-owned hotspots. But Passpoint offers advantages to independent hotspot operators too. Now it is very easy for a single hotspot to accept authenticated traffic from all cellular service providers' subscribers, and if commercial roaming agreements can be put in place this will allow landlords of public areas like shopping centers and airports to use one set of WLAN infrastructure to provide Wi-Fi offload service for every Wi-Fi enabled device that enters their area. Further, these devices will be pre-configured to connect to Wi-Fi without any user intervention.

Stadium operators in particular will benefit from Passpoint, as spectators' mobile devices will automatically seek out the stadium WLAN and authenticate to their home service providers. This will remove the current obstacles to access for delivery of video and images to accompany the game: the spectator will only need to bring up a browser or other client, as Passpoint will take care of the connection mechanisms.

Beyond public access we see an opportunity for dual-use public-private networks, where a single access point can offer private access, perhaps for a small business or retail establishment, while simultaneously advertising Passpoint-based public service. This would be an ideal vehicle for a managed-service solution, where the service provider ships the customer pre-configured access points and manages them remotely, gaining the hotspot footprint while adding revenue from the dedicated private customer.

And Passpoint will tip the scales on a question universities and hospitals, in particular, face with increasing urgency, how to provide cellular service in areas that are too hard to reach or too high in density for the cellular macro network to cover well. Since Wi-Fi interfaces are becoming universal on cellular devices, a single WLAN can potentially support all cellular users, in contrast to solutions such as Distributed Antenna Systems (DAS) which are set up per-carrier, and pico/femtocells that are still immature for large deployments.