Attacks on Wireless LANs

Sayed Wiqar Ali Shah

www.sysbh.com

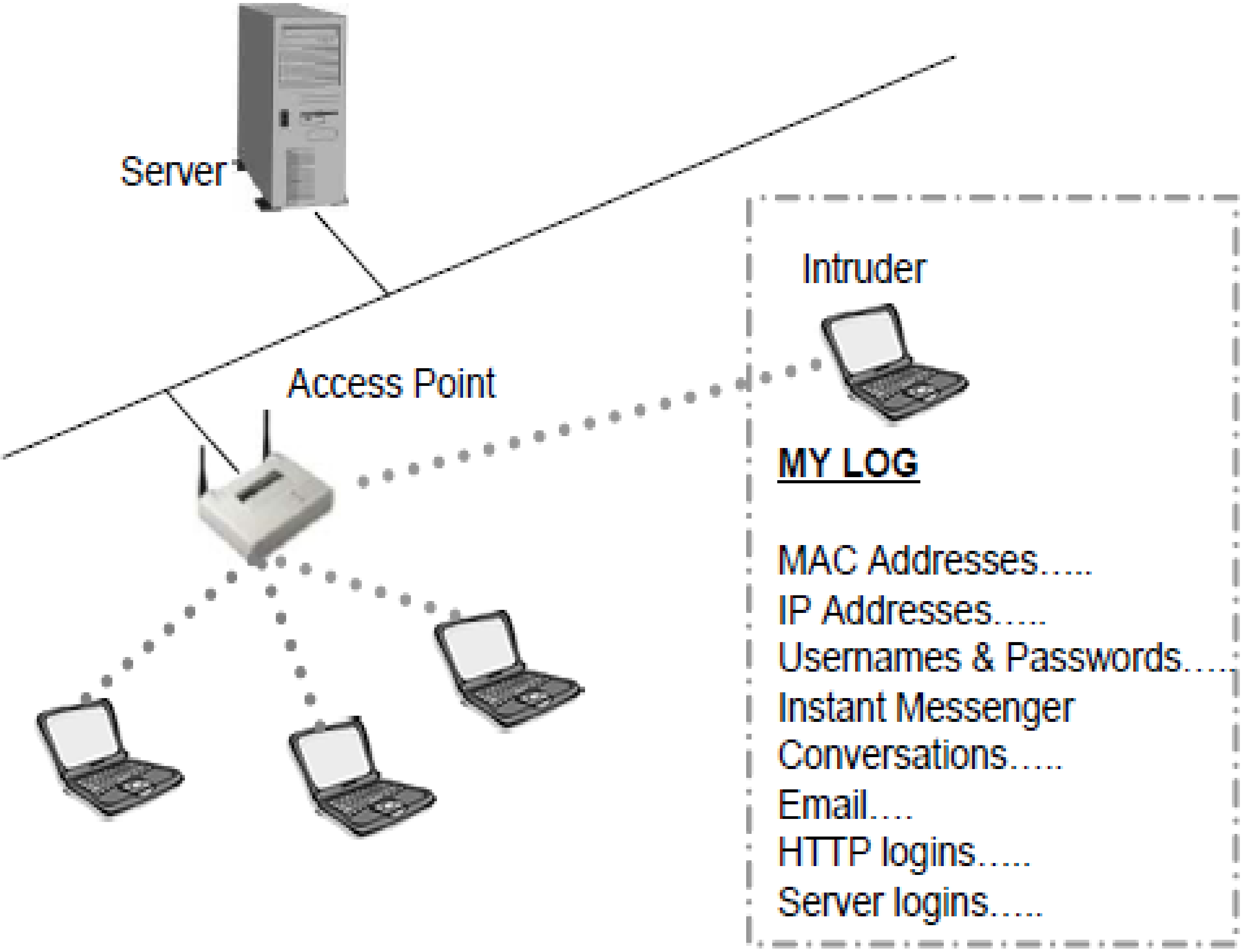
- A malicious hacker can seek to disable or attempt to gain access to a wireless LAN in several ways. Some of these methods are:

1. Passive attacks (eavesdropping)
2. Active attacks (connecting, probing, and configuring the network)
3. Jamming attacks
4. Man-in-the-middle attacks

Passive Attacks

- Eavesdropping is perhaps the most simple, yet still effective type of wireless LAN attack. Passive attacks like eavesdropping leave no trace of the hacker's presence on or near the network since the hacker does not have to actually connect to an access point to listen to packets traversing the wireless segment. Wireless LAN sniffers or custom applications are typically used to gather information about the wireless network from a distance with a directional antenna, as illustrated in Figure. This method of access allows the hacker to keep his distance from the facility, leave no trace of his presence, and listen to and gather valuable information.

Passive Attack Example



MY LOG

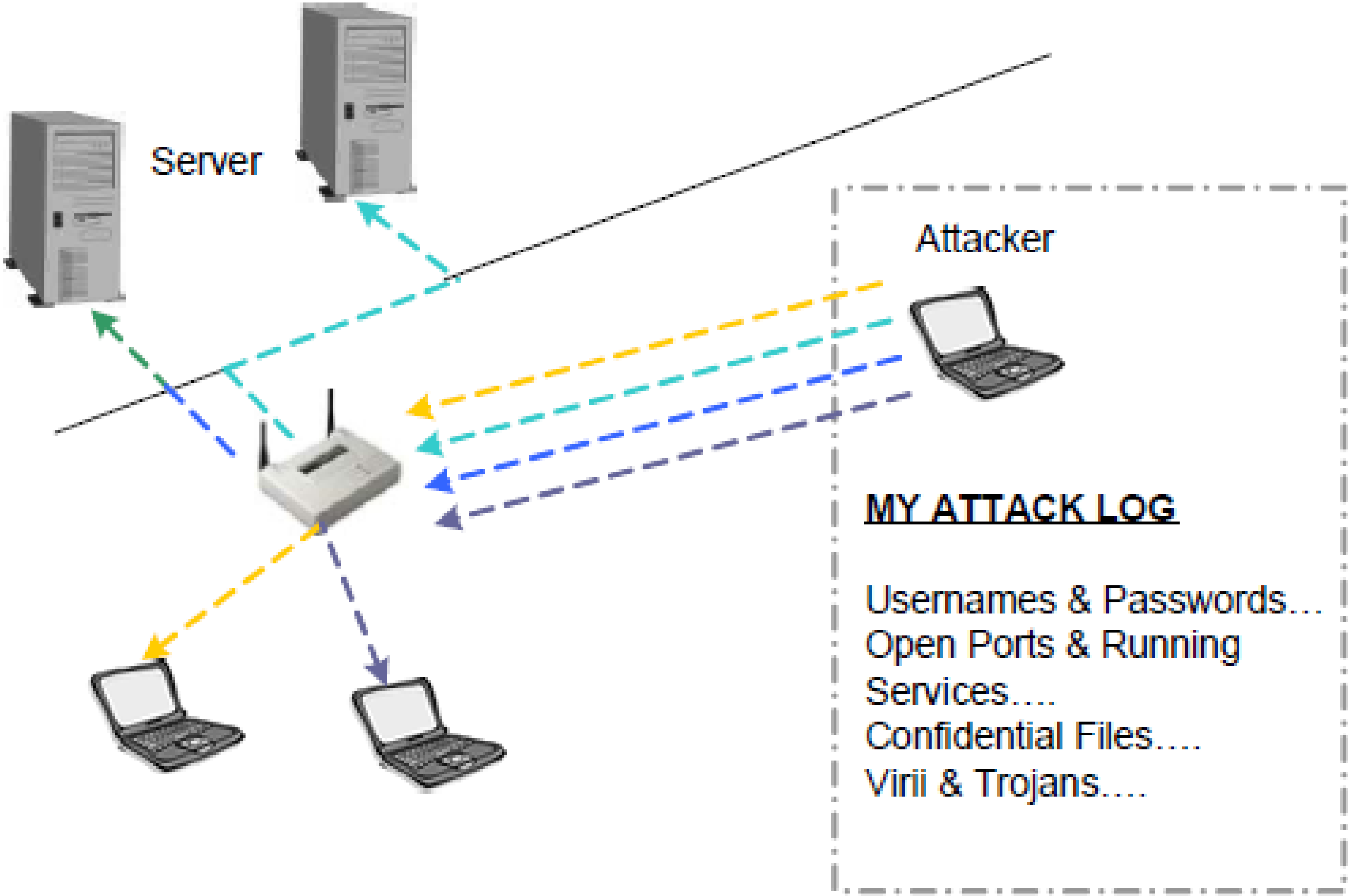
MAC Addresses…..
IP Addresses…..
Usernames & Passwords…..
Instant Messenger Conversations…..
Email….
HTTP logins…..
Server logins…..

- There are applications capable of gathering passwords from HTTP sites, email, instant messengers, FTP sessions, and telnet sessions that are sent in clear text. There are other applications that can snatch password hashes traversing the wireless segment between client and server for login purposes. Any information going across the wireless segment in this manner leaves the network and individual users vulnerable to attack.
- Consider the impact if a hacker gained access to a user's domain login information and caused havoc on the network. The hacker would be to blame, but network usage logs would point directly at the user. This breach could cost a person their job.

Active Attacks

- Hackers can stage active attacks in order to perform some type of function on the network. An active attack might be used to gain access to a server to obtain valuable data, use the organization's Internet access for malicious purposes, or even change the network infrastructure configuration. By connecting to a wireless network through an access point, a user can begin to penetrate deeper into the network or perhaps make changes to the wireless network itself. For example, if a hacker made it past a MAC filter, then the hacker could navigate to the access points and remove all MAC filters, making it easier to gain access next time. The administrator might not even notice this change for some time. Figure 10.7 illustrates an active attack on a wireless LAN.

Active Attack Example



MY ATTACK LOG

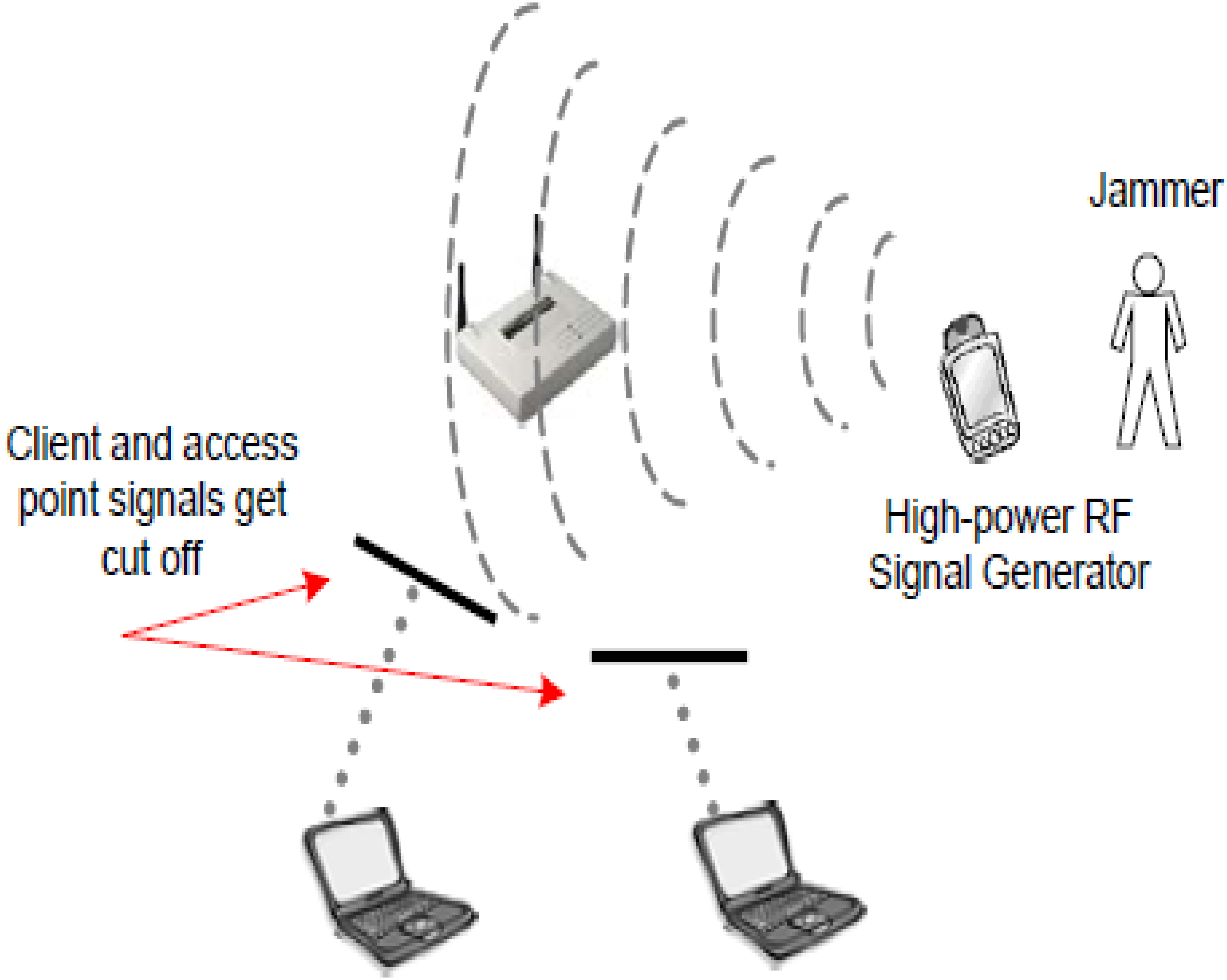
Usernames & Passwords…
Open Ports & Running Services….
Confidential Files….
Virii & Trojans….

- Some examples of active attacks might be a drive-by spammer or a business competitor wanting access to your files. A spammer could queue emails in his laptop, then connect to your home or business network through the wireless LAN. After obtaining an IP address from your DHCP server, the hacker can send tens of thousands of emails using your Internet connection and your ISP's email server without your knowledge. This kind of attack could cause your ISP to cut your connection for email abuse when it's not even your fault. A business competitor might want to get your customer list with contact information or maybe your payroll information in order to better compete with you or to steal your customers. These types of attacks happen regularly without the knowledge of the wireless LAN administrator

Jamming

- Whereas a hacker would use passive and active attacks to gain valuable information from or to gain access to your network, jamming is a technique that would be used to simply shut down your wireless network. Similar to an overwhelming denial of service (DoS) attack aimed at web servers, so a wireless LAN can be shut down by an overwhelming RF signal. That overwhelming RF signal can be intentional or unintentional, and the signal may be removable or non-removable. When a hacker stages an intentional jamming attack, the hacker could use wireless LAN equipment, but more likely, the hacker would use a high-power RF signal generator or sweep generator. Figure illustrates an example of jamming a wireless LAN.

Jamming Attack Example



Jammer

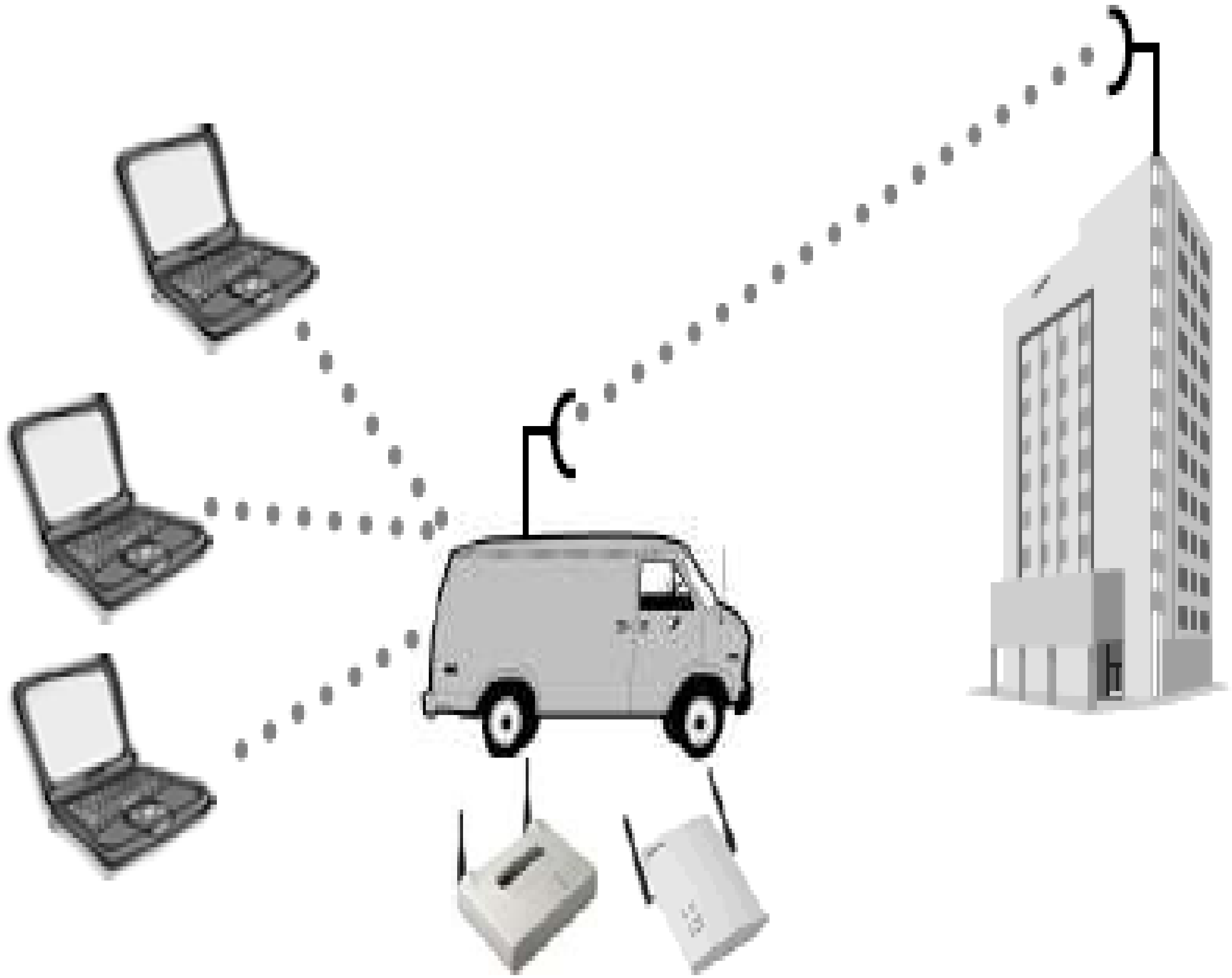
High-power RF Signal Generator

Client and access point signals get cut off

Man-in-the-middle Attacks

- A man-in-the-middle attack is a situation in which a malicious individual uses an access point to effectively hijack mobile nodes by sending a stronger signal than the legitimate access point is sending to those nodes. The mobile nodes then associate to this rogue access point, sending their data, possibly sensitive data, into the wrong hands. Figure illustrates a man-in-the-middle attack, hijacking wireless LAN clients. In order to get clients to reassociate with the rogue access point, the rogue access point's power must be much higher than that of the other access points in the area *and something* has to actively cause the users to roam to the rogue access point. Losing connectivity with a legitimate access point happens seamlessly as a part of the roaming process so some clients will connect to the rogue accidentally.

Man-in-the-middle attack



An access point and sometimes a
workgroup bridge are used to hijack users

- The person perpetrating this man-in-the-middle attack would first have to know the SSID that the wireless clients are using, and, as we've discussed earlier, this piece of information is easily obtained. The perpetrator would have to know the network's WEP keys if WEP is being used on the network. One particular problem with the man-in-the-middle attack is that the attack is undetectable by users. That being the case, the amount of information that a perpetrator can gather in this situation is limited only by the amount of time that the perpetrator can stay in place before getting caught. Physical security of the premises is the best remedy for the man-in-the-middle attack.

- Thank you.