IPSA SCIENTIA POTESTAS EST

est.2009

HORIZON
CAMPUS

FACULTY OF INFORMATION TECHNOLOGY

BIT (Hons.) in Networking and Mobile Computing

IT32063 Wireless Networking

Assignment 2

Index No: ITBNM-2110-0074

J.P.H. KAVINDHYA

a)

i. Exposed terminals

Exposed terminal is one such widely recognized problem that degrades medium access control (MAC) protocol performance such as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) in wireless communications, especially in wireless local area networks (WLANs). Exposed terminal is an event in which a node is unnecessarily prevented from sending data due to an existing nearby transmit node even if the transmit event were not going to result in interference at the receiver.

To understand why, suppose we have nodes A, B, C, and D in linear topology. If B is transmitting to node A, and node C is in range with B but not with A, if node C has to transmit to node D (not in range with B), node C will realize that the channel is busy due to B's transmission and delay its own transmission. But since C's transmission to node D could not have conflicted with B's transmission to node A, this delay is avoidable but leads to under-use of the communication channel.

The exposed terminal problem decreases network throughput and efficiency, especially in high density wireless networks with lots of neighboring nodes. MAC protocols such as RTS/CTS (Request to Send / Clear to Send) have been developed in IEEE 802.11 standards to relieve this problem, but cannot eliminate it completely (Bharghavan et al., 1994). It is an important problem in wireless network protocol design, and leaving it unsolved degrades network performance considerably. Several solutions for mitigating exposed terminals have been examined by researchers, including using directional antennas, MAC protocol changes, and cross-layer designs (Romdhani, C., et al., 2003).

ii. Hidden terminals

Hidden terminals are a recurrent problem that exists in wireless communications, especially wireless local area networks (WLANs), where two or more nodes are unable to detect one another's signals because they are spatially separated from one another while their signals clash at a shared receiver. This happens where nodes are within the coverage of the same access point but out of reach from one another and are possibly prone to clashing on what they transmit while fighting for the same time to transmit. This destabilizes the performance of the network and is not resolvable using mere use of carrier sense since nodes are unable to "feel" the presence of one another (Kushalnagar et al., 2007). Solutions such as the use of RTS/CTS (Request to Send/Clear to Send) handshake in IEEE 802.11 protocols are employed to reduce the instances of collisions where the use of the medium is coordinated (IEEE 802.11-2020).

b) Wi-Fi Protected Access 2 (WPA2)

One of the strongest built-in security layers of the wireless networks is Wi-Fi Protected Access 2 (WPA2). WPA2 is a more secure data encrypting protocol that is used to transmit data across the wireless networks using the Advanced Encryption Standard (AES) scheme. This is an encryption scheme that makes the data readable and accessible to only those people who are specifically granted authorization while securing the data from an unauthorized person and from interception. WPA2 replaced weaker Wired Equivalent Privacy (WEP) and first-generation WPA and offered a groundbreaking improvement to home and enterprise wireless setup security. WPA2 is crucial to maintaining the security and privacy of the wireless communications to the IEEE 802.11i standard (IEEE, 2004).

Media Access Control (MAC) address filtering

MAC address filtering is another crucial security feature. This tool lets network admins control who can connect to the wireless network by looking at each device's unique MAC address. By keeping a list of approved devices, an admin can block access even if someone has the right login info. While it's possible to fake a MAC address, this extra step helps guard against simple break-ins. Gast (2005) points out that for smaller networks, it's pretty easy to keep track of an access list and use it to boost security.

c) True.

The actual placement of the wireless access points (APs) is critical to both coverage and performance. Different building construction materials (for example, wood versus concrete, metal, glass, etc.) can affect wireless signal propagation due to attenuation effects or reflections. Thus, it is important to understand how the structure is designed to allow for proper or expected signal propagation. In addition, aesthetics is taken in consideration to location, in particular in public or customer-facing areas, since we obviously want to hide the APs to not affect the look of a space. It is important to find this balance between technical expectations and aesthetics, which is part of network planning.