College of Computer Science
Northeastern University
Wireless Networks CS G250

Lecture 10
October 15 2008
Lecturer: R. Sundaram

Wireless LAN, Shortest Path Trees, 802.11

1 Wireless LAN

1.1 Infrared (IR)

Infrared communication is present in most homes, where it used for all sorts of remote control devices: wireless mice, wireless keyboards, remote controls.

Advantages:

- limited spectrum, meaning really high data rates
- unregulated world-wide
- does not penetrate walls, meaning secure communication and reduced interference, which enables the set up of small cells
- inexpensive equipment
- it's only line-of-sight (it bends a little)

Disadvantages:

- the ambient radiation appears as noise in an infrared receiver
- eye safety
- high power consumption

Infrared is used as:

- Directional IR
  The beam is focused from the transmitter to the receiver. It can have a range of kilometers. One use of directional IR is setting up a token ring LAN.
- Omnidirectional IR
  A base station transmits in all directions, like a flashlight.
- Diffuse IR
  It bounces off against dust particles. It has nice military applications when a lot of dust is involved.

1.2 Spread Spectrum

Unlicensed spread spectrum:

- 902-928 MHz
- 2.4 - 2.4835 GHz
- 5.725 - 5.825 GHz

Why are these frequency bands unlicensed? The reason for that is that they correspond to the resonant frequency of the water. Water absorbes energy very well. What that means is that they are low quality badwidthes.

2 Shortest Path Trees - Bellman-Ford Algorithm

Given a graph $G = (V, E)$, where E is the set of edges and V is the set of vertices, the Bellman-Ford algorithm computes the single-source shortest-path in a weighted graph (the weights of the edges can be negative). In other words the algorithm finds the shortest paths from a source vertex to every other vertex in a weighted graph. Compared to Dijkstra algorithm, Bellman-Ford handles negative weights too. The complexity of the algorithm is $O(|V| \times |E|)$.

At every step of the algorithm, each node maintains an estimate of the distance between the source vertex or the root R.

Initially, for every vertex v different than the root R, set the distance between v and R to ∞: $D_v^0 = \infty$. What that means is that all vertices v don't know how to get to the root R. The distance between the root R to itself is $D_v^0 = 0$.

At each step of the algorithm, each vertex v updates its distance to the root R in the following way: $D_v^{t+1} = \min_{u:(v,u)\in E} \left(w(v,u) + D_u^t\right)$, where t is the previous step of the algorithm, $w(v,u)$ is the weight of the egde from v to u and D_u^t is the computed distance between vertex u and the root R at the previous step of the algorithm.

Besides the initiation phase, the algorithm updates its distances a $|V|-1$ number of times.

D_v^t is the shortest path from v to R using no more than t hops.

Given the fact we have $|V|$ vertices, the maximum length of any shortest path is $|V| - 1$ hops.

Why do we get a tree? Let's look at Figure 1. Let's suppose the shortest path between A and B is though *path* 1. If the shortest path between B and

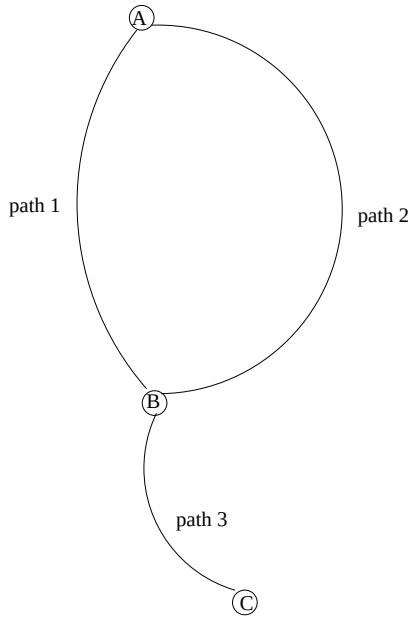

Figure 1: Why do we get a tree?

C goes through *path* 3, then the shortest path between C and A will never go though *path* 3 and then *path* 2, but it will always go through *path* 3 and then *path* 1. Thus the algorithm eliminates the possibility of having loops.

Let's apply the algorithm on the graph from Figure 2.

Here is what we get:

D	0	1	2	3	4
A	∞	∞	8C	8C	8C
B	∞	∞	5D	4D	4D
C	∞	3R	3R	3R	3R
D	∞	4R	3E	3E	3E
E	∞	2R	2R	2R	2R
R	0	0	0	0	0

The notation $3E$ for vertex D, for example, means that from D to reach R there's a distance of 3 units and the next vertex on the way from D to R is E.

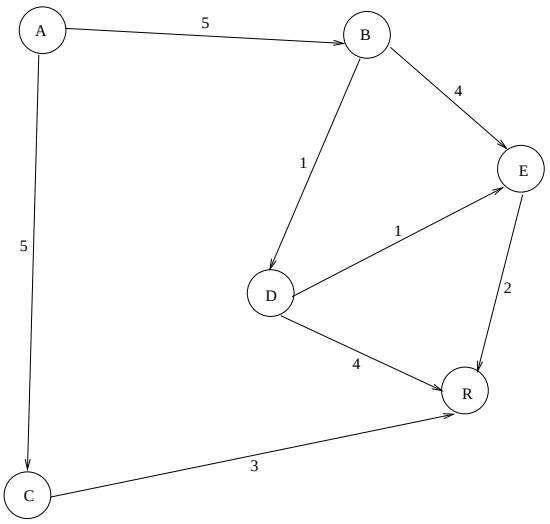

Figure 2: Graph G=(V,E)

3 802.11

802.11 is a set of standards for the wireless LANs. The 802.11 comes in 3 flavours: a (54Mbits/s and 5GHz) , b (11 Mbits/s and 2.4GHz) and g (54 Mbits/s and 2.4GHz).

Multiple Access with Collision Avoidance (MACA) is a slotted media access control protocol used in wireless LAN data transmission to avoid collisions caused by the hidden station problem and to simplify exposed station problem (Figure 3 and Figure 4)
[$http://en.wikipedia.org/wiki/Multiple\_Access\_with\_Collision\_Avoidance$].

Carrier Sense Multiple Access With Collision Detection (CSMA/CD) is a network control protocol in which a carrier sense is used. Also when a transmitting station detects that another station is also transmitting, the transmitting station stops and then attempts to transmit again after a random time. The random time is chosen between 0 and a maximum value called exponential backoff. It there is a collision, then the exponential backoff is doubled. This technique is used in Ethernet.

Hidden Node Problem

Let's take a look at Figure 3. In this situation we have 3 stations: A, B and C. Both A and C want to transmit to node B. A sees that the medium is free. At the same time C sees the medium is free. Both A and C start transmitting at the same time. What will happen is that B will get the packets from both

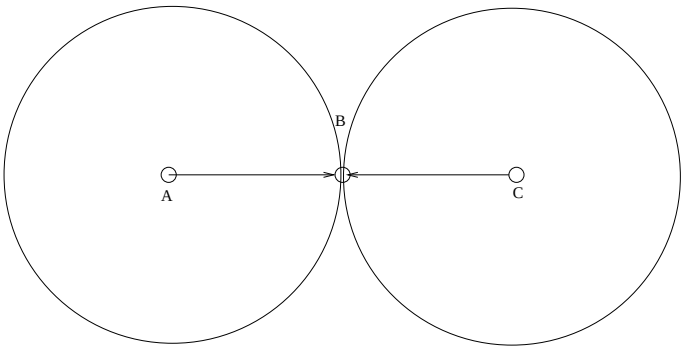

Figure 3: Hidden Node Problem

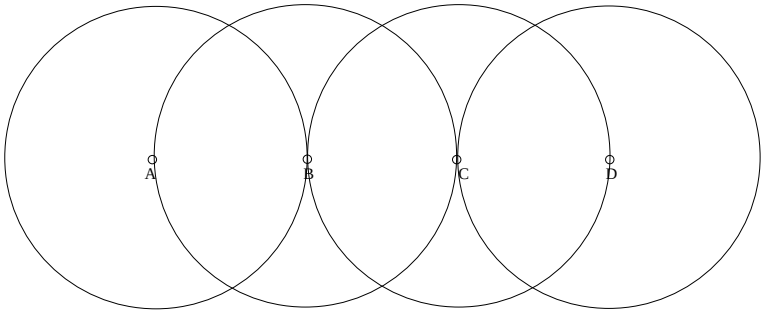

Figure 4: Exposed Node Problem

A and C at the same time and won't be able to distinguish anything out of the two transmissions.

Exposed Node Problem

Let's take a look at Figure 4. In this situation we have 4 stations: A, B, C and D. B wants to transmit to A. B sees the medium is free and it will start transmitting. C is in the range of B, therefore C will see that someone (B) is transmitting. C wants to transmit to D. A is not in the range of C and if C will start transmitting to D, A won't be influenced. But C won't transmit to D, because B is already trasmitting. The problem with this scenario is that the medium is underutilized.