Security and Cooperation in Wireless Networks

Exercise Sheet 4

WS 12/13

Youssef Shehadeh
Telematics Group,
University of Goettingen,
shehadeh@cs.uni-goettingen.de

January 18, 2013

A. **Privacy Protection**.

(1) Consider again the key-tree based approach to private authentication of RFID tags. Generalize the computation of the expected anonymity set size for key-trees that have different branching factors (b_i) at different levels of the tree.

(2) Location privacy through Mix zones: Let us consider a mix zone with three gates. Let the time slot be 0.1 unit. The discrete probability functions of the delays between gates 1 and 3, and those between 2 and 3 are given in the following table:

t	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0	1.1	1.2
$d_{13}(t)$	0.1	0.2	0.3	0.2	0.1	0.04	0.03	0.02	0.01	0	0	0
$d_{23}(t)$	0	0	0	0.1	0.2	0.3	0.2	0.1	0.04	0.03	0.02	0.01

Let us assume that the adversary observes two vehicles entering the mix zone at gates 1 and 2 at time 0, and two leaving at gate 3 at times 0.4 and 0.7. Thus we have two entering events N1=(1,0) and N2=(2,0); and two exiting events X1=(3,0.4) and X2=(3,0.7). Calculate the probabilities of the possible mutation mappings. Deduce the entropy of the system.

(3) We have seen that location privacy can be provided by coordinated changing of pseudonyms inside mix zones. This solution assumes that all nodes change pseudonyms inside mix zones

(nodes are always cooperative) which may not be a realistic assumption as changing a pseudonym has a cost (consisting of obtaining the new pseudonym, routing overhead due to changing the pseudonym, etc.). The goal of this exercise is to model, using game theory, the pseudonym changing approach for achieving location privacy under the assumption that nodes are not always cooperative (rather the nodes are rational).

a. Define a strategic-form game that represents the pseudonym changing approach (let's call that the pseudonym changing game) assuming that:

- two players meet in a mix zone and engage in the game;
- the players have two possible strategies: C - changing pseudonym (cooperating) and D – no pseudonym change (defecting);
- the achieved level of privacy L is equal to $\log_2(n)$ where n is the number of players that changed pseudonym (i.e., played C); if n = 0 the achieved level of privacy is equal to 0;
- the cost of changing the pseudonym is "γ" and the goal of each player is to maximize its utility (the level of its privacy).

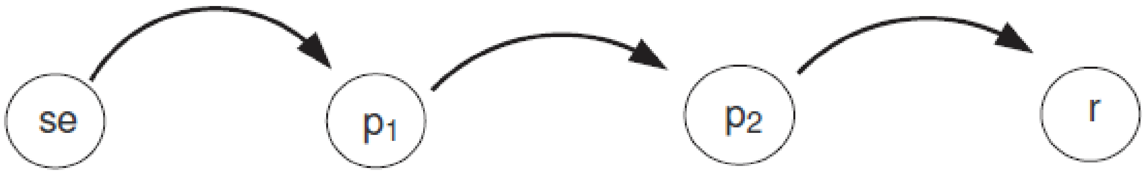
b. Identify the Nash equilibria (NE). What is the Pareto-optimal NE strategy profile?

c. Let us modify the pseudonym changing game such that the player P2 is malicious, i.e., the goal of player P2 is to minimize the utility of the rational player P1. The gain G(P2) of P2 is now defined as G(P2) = 1 - L(P1). The cost of changing pseudonym is "γ" for both players. The goal of each player is to maximize its utility, defined as the difference between the obtained gain and the incurred cost. Give the strategic-form representation of this game and identify the Nash equilibria.

d. Let us now assume that the players can be malicious with some predefined probability q. Furthermore, let us assume that the players make their moves sequentially (i.e., the game is dynamic). Player P1 moves first and then player P2 moves. The advantage of P2 is that it can observe the move of player P1. Calculate the expected gain of player 1 in case it cooperates or defers. Discuss and identify the Nash equilibria in this game.

B. Game theory for wireless networks

(1) Write the extensive form of the Joint Packet Forwarding Game. (Player P2's strategy depends on the strategy of P1, the cost of forwarding the packet is c, each gets a reward of 1 in case the packet is received at r)

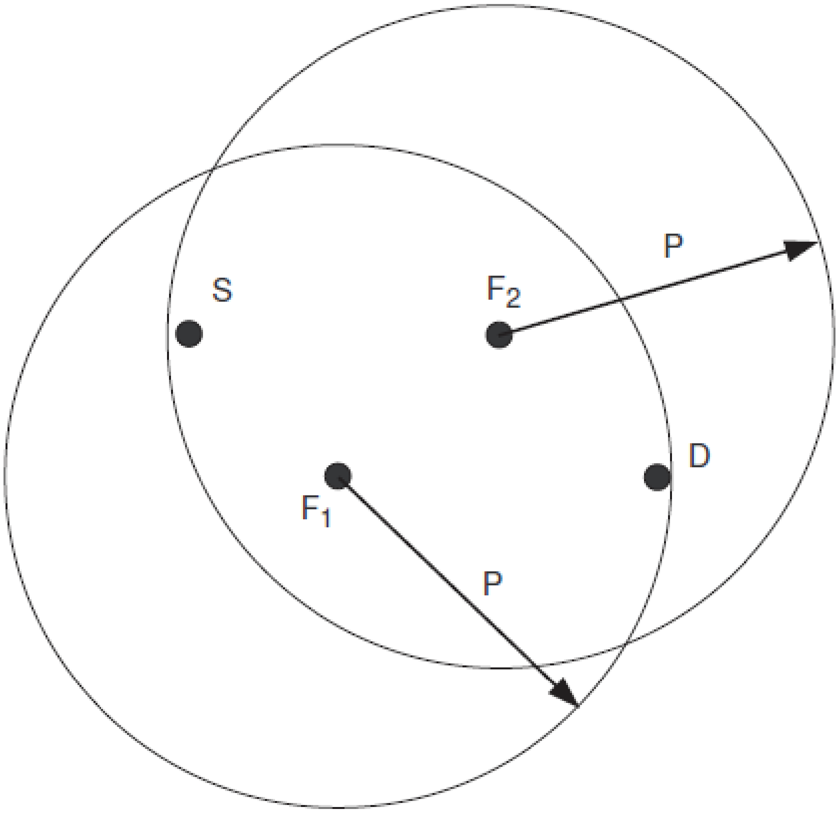


(2) Let us now consider a modified version of the Joint Packet Forwarding Game. Suppose that player p1 can reach the destination at the cost of 2c. In this case, she is the only one who receives the reward of 1. Hence, player p1 has the choice to drop (D), forward to player P2 (F'), or forward to the destination (F'').

a. Write the normal form of this modified game. Identify the Nash equilibria. Which equilibrium is Pareto-optimal?

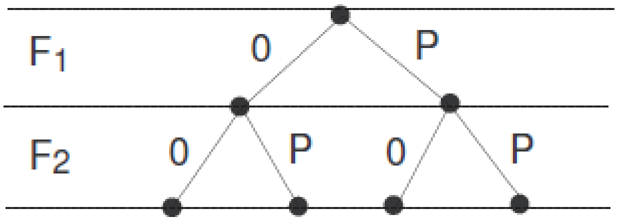
b. Write the extensive form.

(3) In this problem, we will model the connectivity between devices as a game. Consider the network presented in the following Figure:



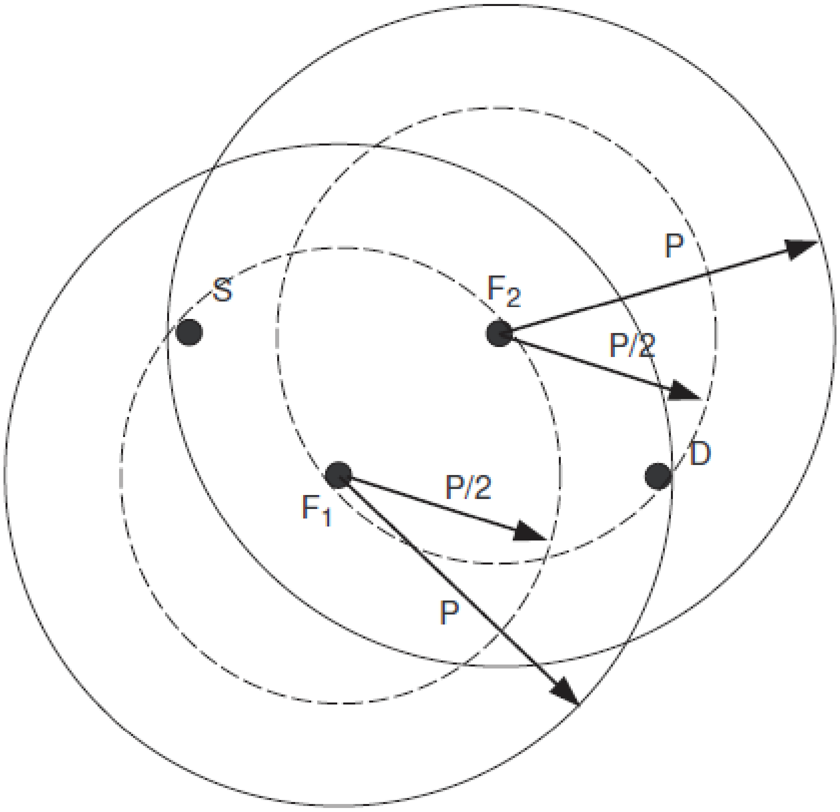
Suppose that the source S wants to send a packet to the destination D, but it needs the help of the forwarders to do this (one or both of them). Forwarder *i* has two possible moves: (a) set its power level to Pi = 0 or (b) set its power level to Pi = P. If either of the forwarders chooses P, then it connects S with D. If the connection is established, then both forwarder nodes get a reward of 1 (meaning a reward of 1 for each of them), no matter who established the connection. But forwarding has a cost: the forwarder who chooses the power level P has to pay the cost 2c. We assume that 2c < 1. Let us call this game the Connectivity Game 1.

a. Suppose that F1 chooses its power level First (F2 decides after). The extensive-form of this game is provided in the Figure below. Write the payoffs on the leaves (bottom end dots) of the tree. Given that F1 is the leader, show the Stackelberg equilibria in this game.



b. Write the corresponding normal form of the same game (in a matrix). Identify the Nash equilibria and the Pareto-optimal strategy profiles.

c. Let us now assume that the forwarders can use 3 power levels: Pi = 0, P/2, or P. With the new power level P/2 they can only reach their immediate neighbors, meaning that with P1 = P/2 the node F1 can reach only S and F2. Similarly, if P2 = P/2 , the node F2 reaches only F1 and D. Clearly, both of them have to choose a power level Pi ≥ P/2 to get the reward 1 each. Choosing P/2 costs only c. The new game (called Connectivity Game 2) is shown in the following Figure. Show the normal form of the Connectivity Game 2. Which are the Nash equilibria? Which are the Pareto-optimal strategy profiles?



d. Let us now define a variant of the Connectivity Game 2, in which the players have to share the reward of 1 proportionally to their contribution. For example, if P1 = P/2 and P2 = P, then F1 gets 1/3 and F2 gets 2/3 . Let us call this variant the Connectivity Game 3. Write the matrix representation of the normal form of the Connectivity Game 3. Show the Nash equilibria in the Connectivity Game 3 assuming that the cost is very small (for example c = 0:05). Show the Pareto-optimal states.

e. Assume now that in the Connectivity Game 3, c = 1/4. Fill the normal-form matrix numerically. Identify Nash equilibria and Pareto-optimal states.

f. Assume now that in the Connectivity Game 3, c = 1/6. Fill the normal-form matrix numerically. Identify Nash equilibria and Pareto-optimal states.

(4) Consider the RTS-based medium access contention game in wireless networks. In this game, there are a fixed number of time slots and each node tries to get access to the channel by sending an RTS (Request-To-Send) packet during a time slot. The node first sending an RTS packet (without any collision) wins the channel and gets a reward of 1. A node that hears an RTS packet quits the contention. The cost of sending an RTS packet is c ($c<1/2$).

a. Let us consider a 2-players game with two slots: S0 and S1, where each player chooses one certain slot to send its RTS packet. Write the normal form of the game. Identify the Nash equilibria and the Pareto-optimal profiles.

b. In fact, in the medium access contention mechanism, a node should choose a time slot randomly (we define this as the Cooperate strategy (C)). However, a selfish node can always send through the first slot to capture the channel (we define this as the Selfish strategy (S)). Suppose now that each node can choose between two strategies: Cooperate (selecting a random time slot) or Selfish (send always during the first slot).

   i. Calculate the probability of collision in case of (C, C), (C, S), and (S, S).

   ii. Establish the normal form of the game. Identify the Nash Equilibria and the Pareto-Optimal profiles. Note: This is a kind of mixed-strategy game, i.e. the utility function depends on the probability of transmission and the probability of success.