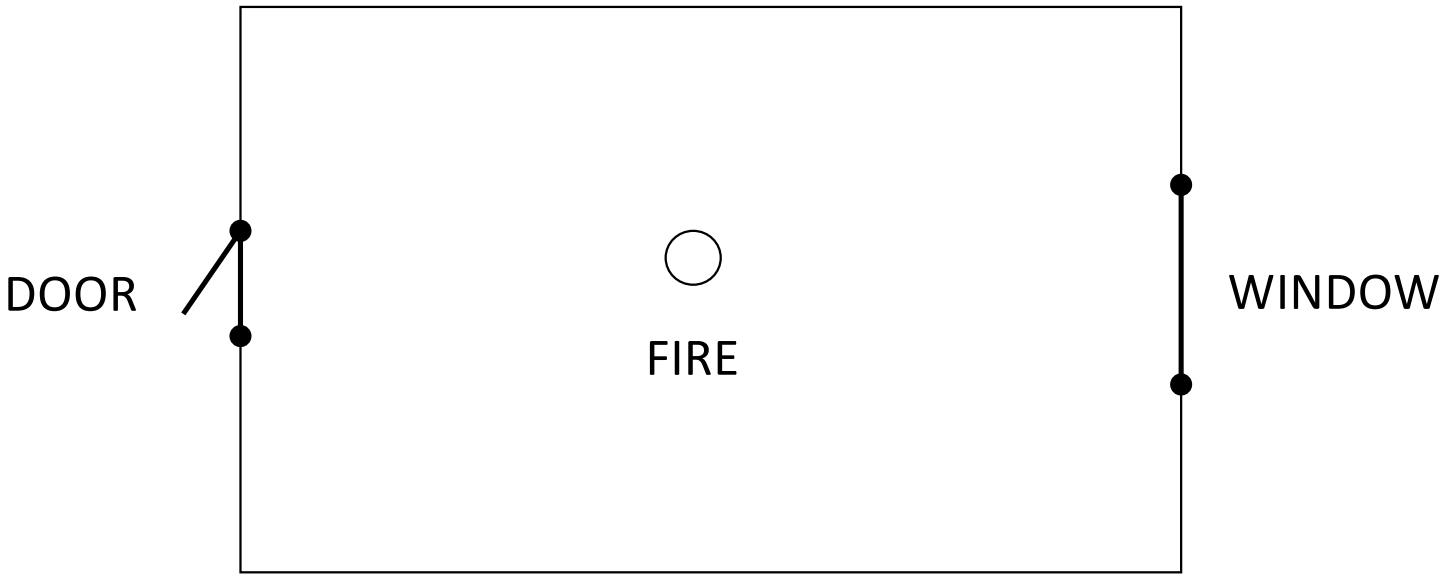
Problog Example: Encrypted IoT messaging

House alarm system



Description of the problem

- An IoT alarm system periodically tests the state of any two our of three sensors installed in the house, and uploads the message about the state of the tested sensors to a remote server using one. Here is an example message:

  DOOR_ON\n
  FIRE_OFF\n

- The system selects sensors to be tested *at random* and the result sensor state descriptions are added to the uploaded message in random order.
- The messages are protected using truly random one-time pad encryption, which is impossible to break, but it does not change the length of messages.
- The investigation team intercepted an encrypted message, which is 17 bytes in length.
- What is the probability of different message contents given that the DOOR sensor is on 90% of the time?

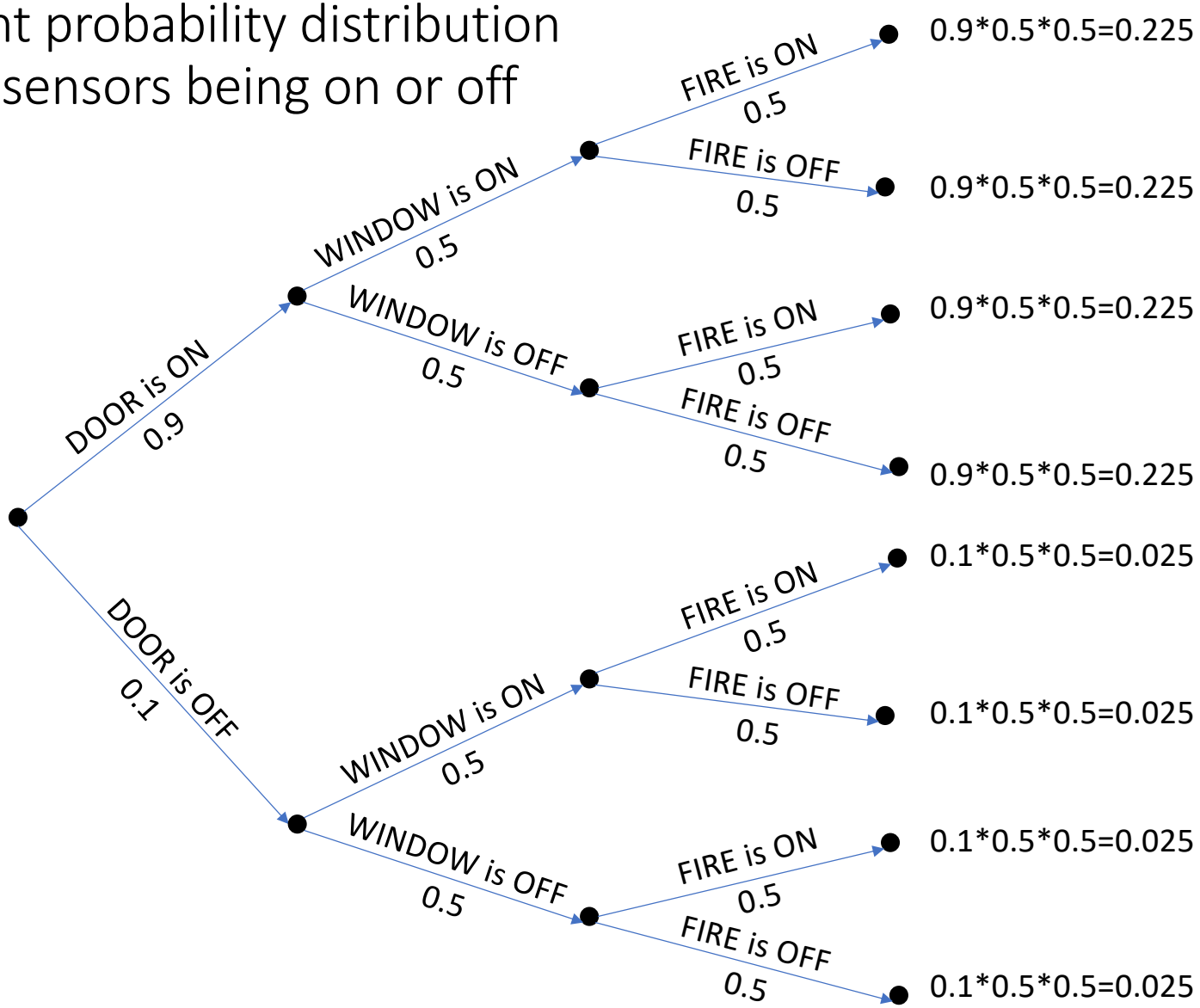
Possible sensor state texts and their lengths

Text	Length in bytes
DOOR_ON/n	8
DOOR_OFF/n	9
WINDOW_ON/n	10
WINDOW_OFF/n	11
FIRE_ON/n	8
FIRE_OFF/n	9

1. Determining probability of sensors being on or off

- According to the problem statement, the DOOR sensor is ON 90% of the time, therefore the probability of the DOOR sensor being ON or OFF is 0.9 and 0.1 respectively.
- There is **no** prior information regarding how likely WINDOW sensor being ON, therefore – by the principle of indifference - we assume equal probabilities to WINDOW sensor being ON (0.5) and the WINDOW sensor being OFF (0.5).
- There is **no** prior information regarding how likely FIRE sensor being ON, therefore – by the principle of indifference - we assume equal probabilities to FIRE sensor being ON (0.5) and the FIRE sensor being OFF (0.5).

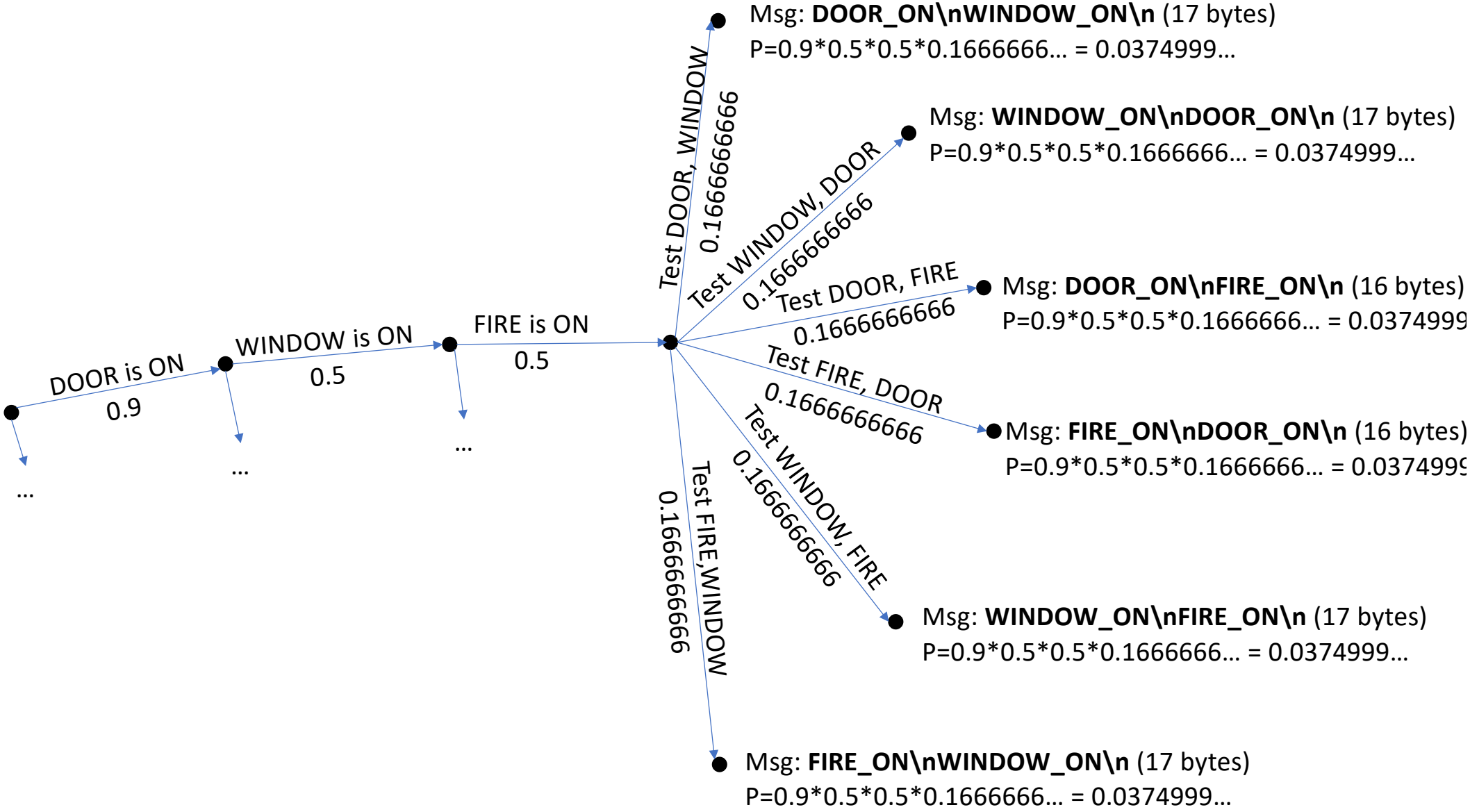
Joint probability distribution for sensors being on or off



2. Selecting sensors at random

- Selecting which sensors to test, and in which order
  a) DOOR, WINDOW
  b) WINDOW, DOOR
  c) DOOR, FIRE
  d) FIRE, DOOR
  e) WINDOW, FIRE
  f) FIRE, WINDOW

- Since we have no prior information about likelihood of specific choices and ordering, assume all equally likely (by the principle of indifference) with probability 1/6=0.16666666…


DOOR is ON
0.9
WINDOW is ON
0.5
FIRE is ON
0.5
...
...
...
Test DOOR, WINDOW
0.1666666666
Msg: DOOR_ON\nWINDOW_ON\n (17 bytes)
P=0.9*0.5*0.5*0.1666666… = 0.0374999…
Test WINDOW, DOOR
0.1666666666
Msg: WINDOW_ON\nDOOR_ON\n (17 bytes)
P=0.9*0.5*0.5*0.1666666… = 0.0374999…
Test DOOR, FIRE
0.1666666666
Msg: DOOR_ON\nFIRE_ON\n (16 bytes)
P=0.9*0.5*0.5*0.1666666… = 0.0374999
Test FIRE, DOOR
0.1666666666
Msg: FIRE_ON\nDOOR_ON\n (16 bytes)
P=0.9*0.5*0.5*0.1666666… = 0.0374999
Test WINDOW, FIRE
0.1666666666
Msg: WINDOW_ON\nFIRE_ON\n (17 bytes)
P=0.9*0.5*0.5*0.1666666… = 0.0374999…
Test FIRE,WINDOW
0.1666666666
Msg: FIRE_ON\nWINDOW_ON\n (17 bytes)
P=0.9*0.5*0.5*0.1666666… = 0.0374999…