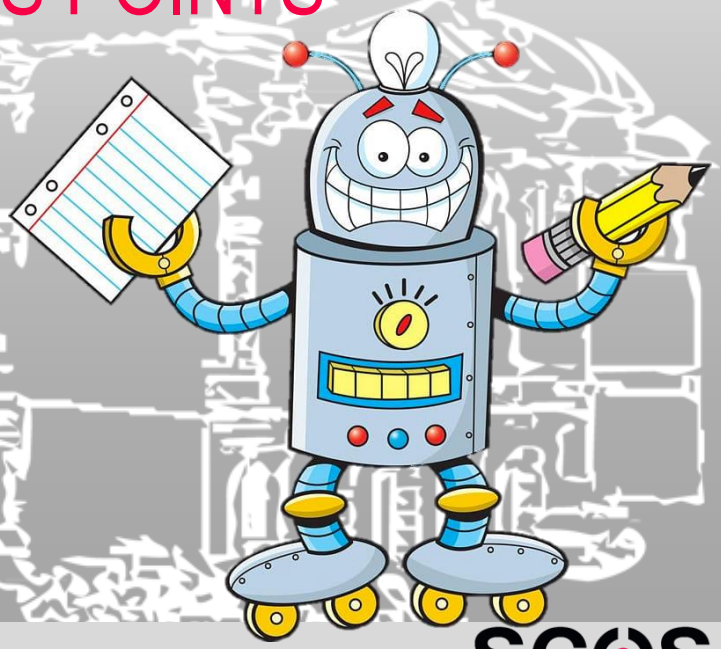
MACHINE LEARNING

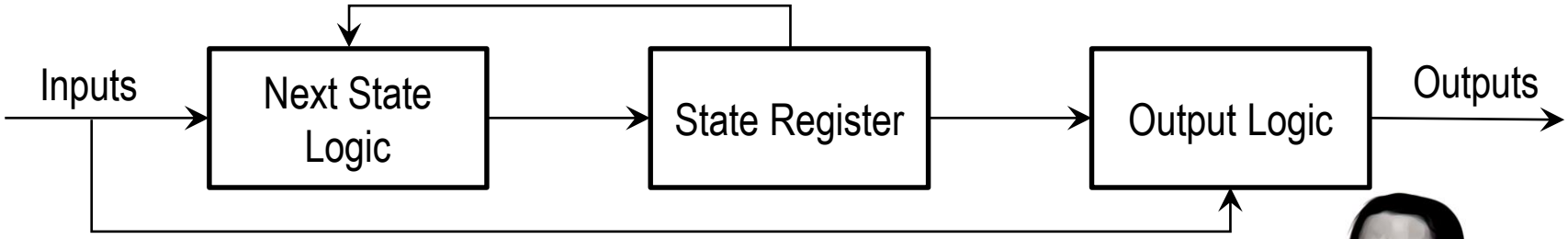
LEARNING IEEE802.11 ACCESS POINTS

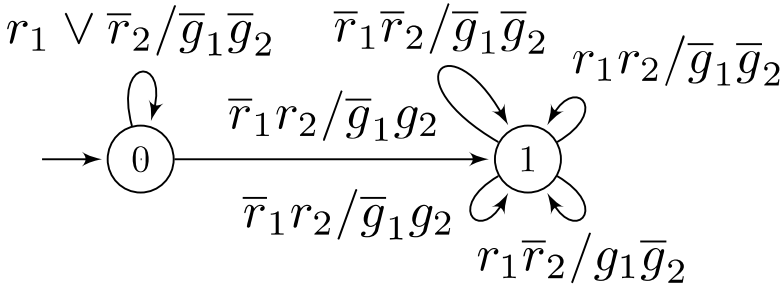
Masoud Ebrahimi
Graz University of Technology, Austria

27.01.2020

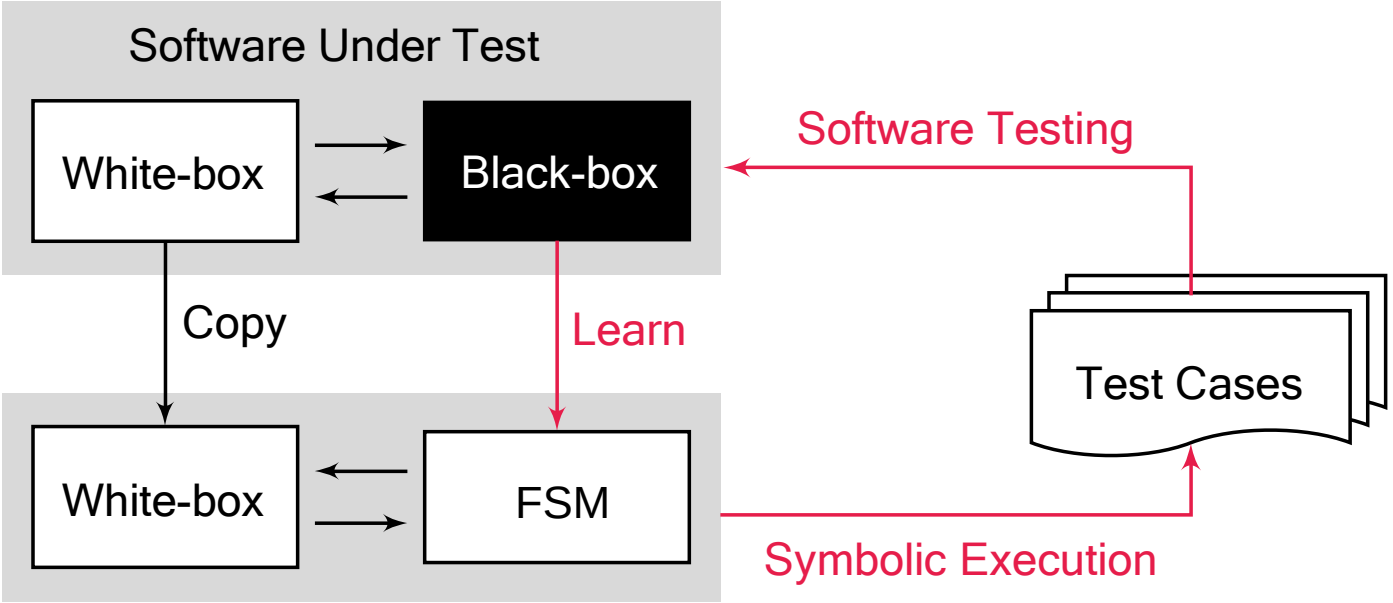


Mealy Machine Learning





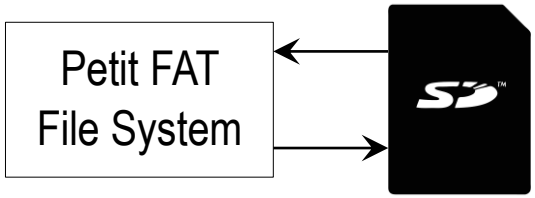
Motivation: Integration Testing



- Learn black-box by automata learning.
- Execute learned setup symbolically.
- Test software under test automatically.

Does it Work? Really!?

- We build file systems on top of disks (controller, content).
- We found the following bug automatically.

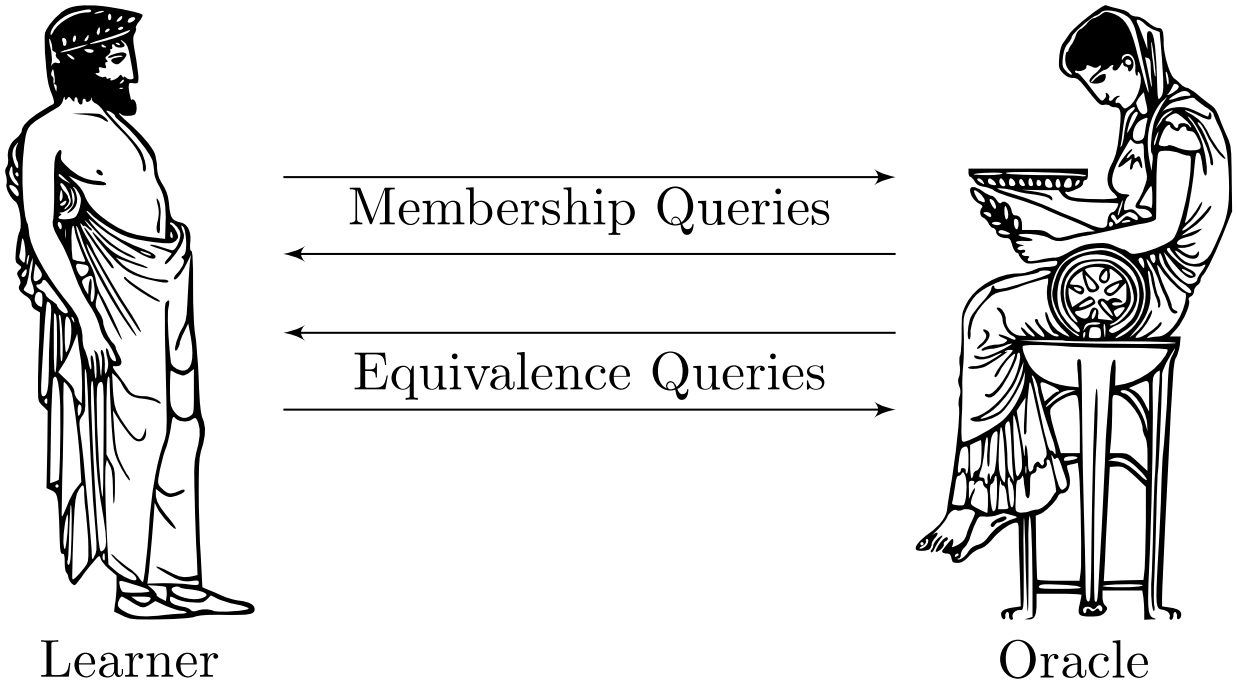


x unsigned char ← type — type → y symbolic buffer

```
fs->csize = buf[BPB_SecPerClus - 13];
fs->n_rootdir = LD_WORD(buf + BPB_RootEntCnt - 13);
tsect = LD_WORD(buf + BPB_TotSec16 - 13);
if (!tsect) tsect = LD_DWORD(buf + BPB_TotSec32 - 13);
mclst = (tsect
     - LD_WORD(buf + BPB_RsvdSecCnt - 13) - fsize
     - fs->n_rootdir / 16 ) / fs->csize + 2;
fs->n_fatent = (CLUST)mclst;
```

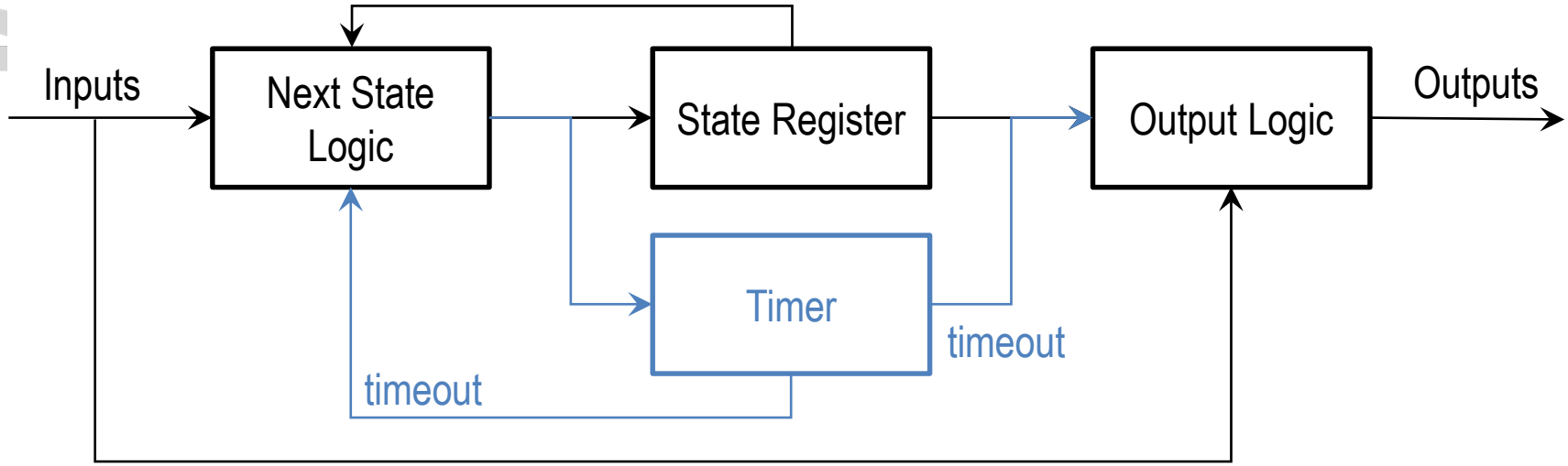
{ division by zero ← mclst; z overflow ← fsize

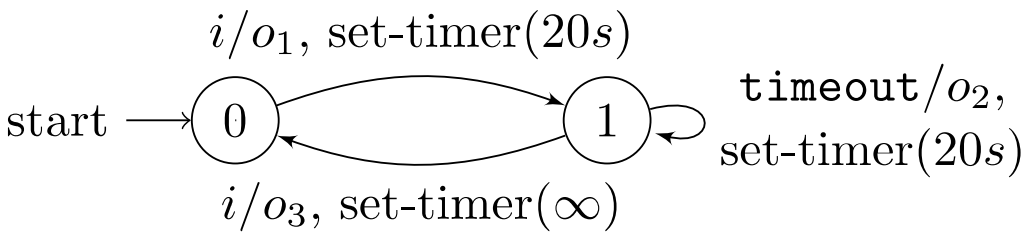
Minimally Adequate Teacher



- Membership Queries
  - What is the reaction of black-box to an input word?
- Equivalence Queries
  - Did I learn the right model? If not what is a counterexample?

Mealy Machines with One Timer

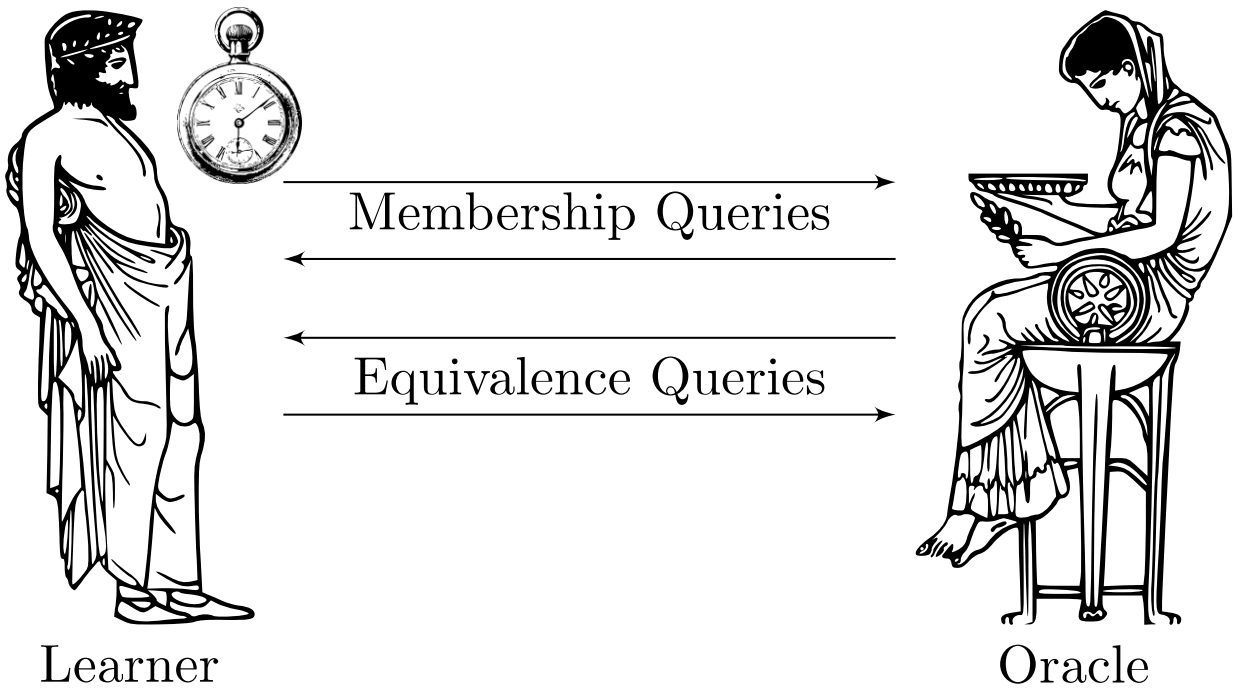




Learning Mealy Machines with One Timer

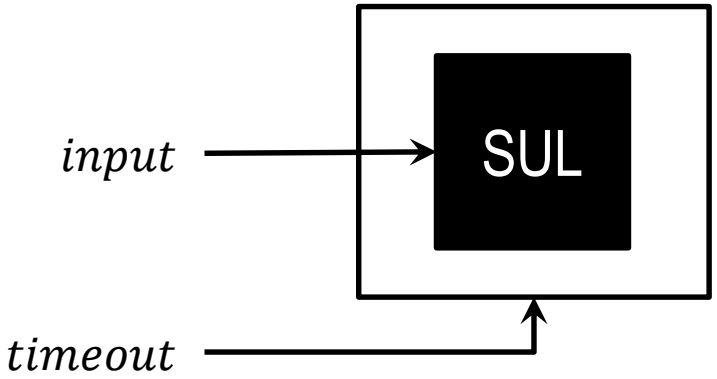
Extending Active Automata Learning

Timed Learner



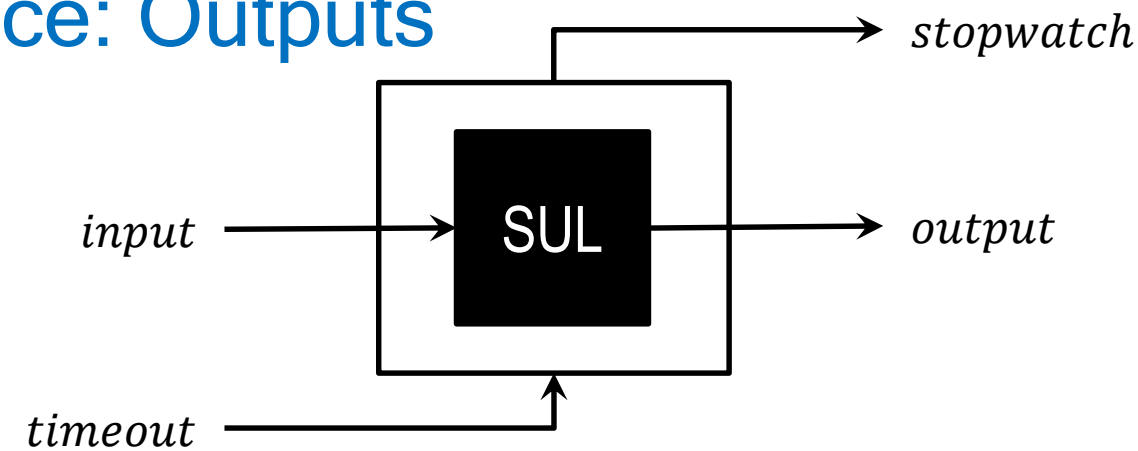
- Membership Queries
  - How long does it take for the black-box to react an input word?
- Equivalence Queries
  - Did I learn the right model? If not what is a counterexample?

Interface: Inputs and Timeout



- Input Symbols
  - Explicit inputs to the SUL
- Timeout Symbol
  - An implicit input to the SUL
  - Observe SUL's output for maximum Δ time units
  - If an output happens then a timeout has occurred

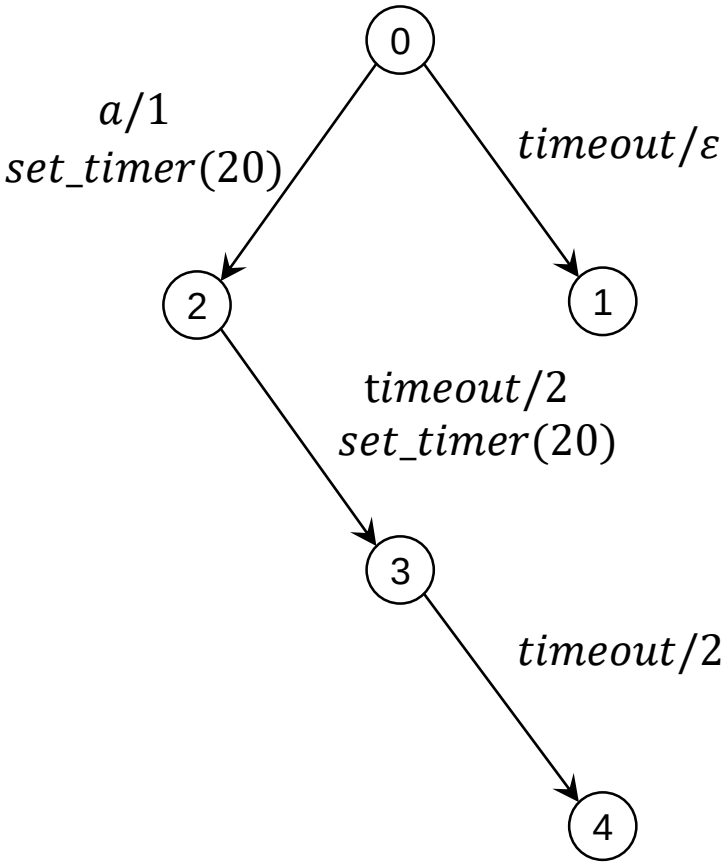
Interface: Outputs



- In Response to Inputs with a time measure of zero.
- In Response to Timeout Symbol
  - No output seen in Δ time units.
  - $output$ with a time measure $\delta \leq \Delta$ indicates a timeout occurred after δ time units.

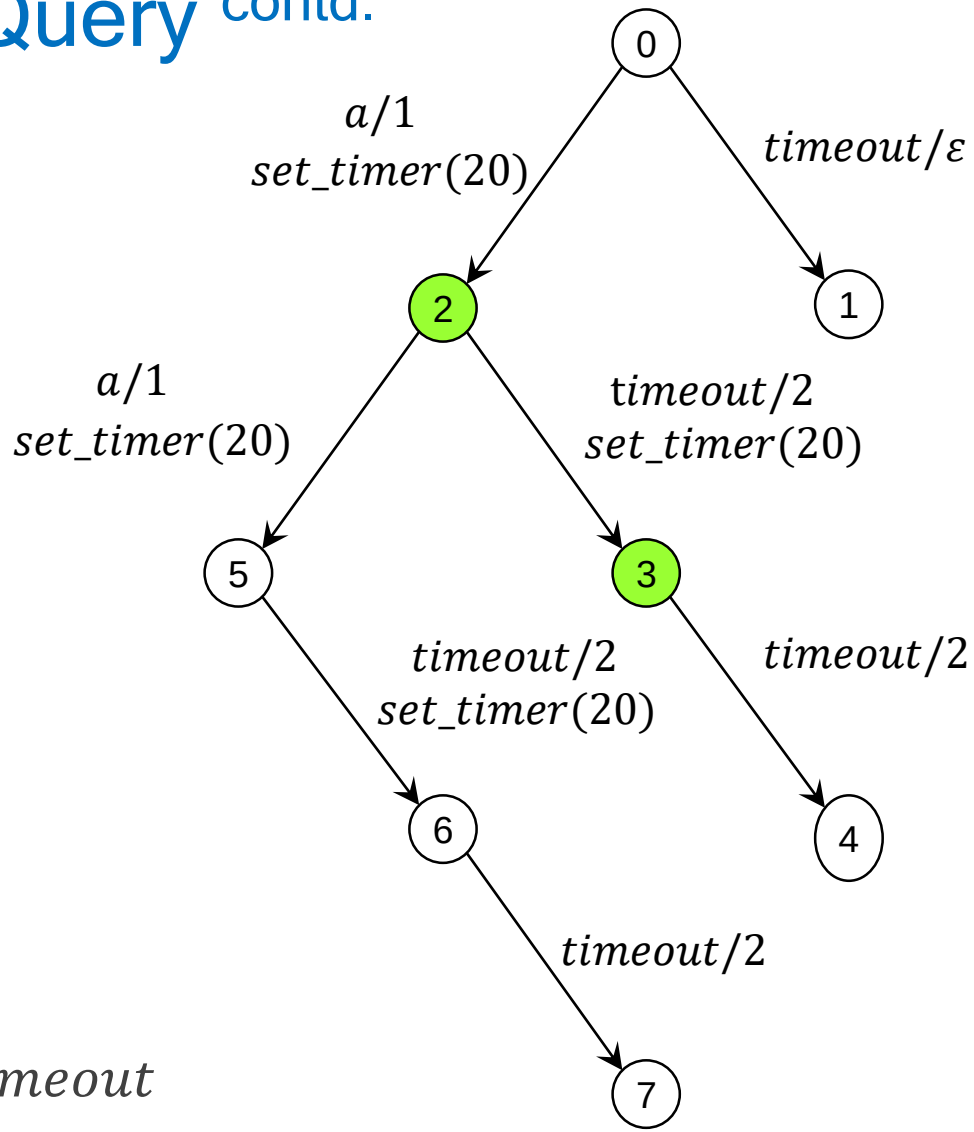
Membership Query

- Input Word
  - $a, timeout$
- Prefixes
  - ε
  - a
  - $a, timeout$
- Queries
  - $\varepsilon, timeout$
  - $a, timeout$
  - $a, timeout, timeout$

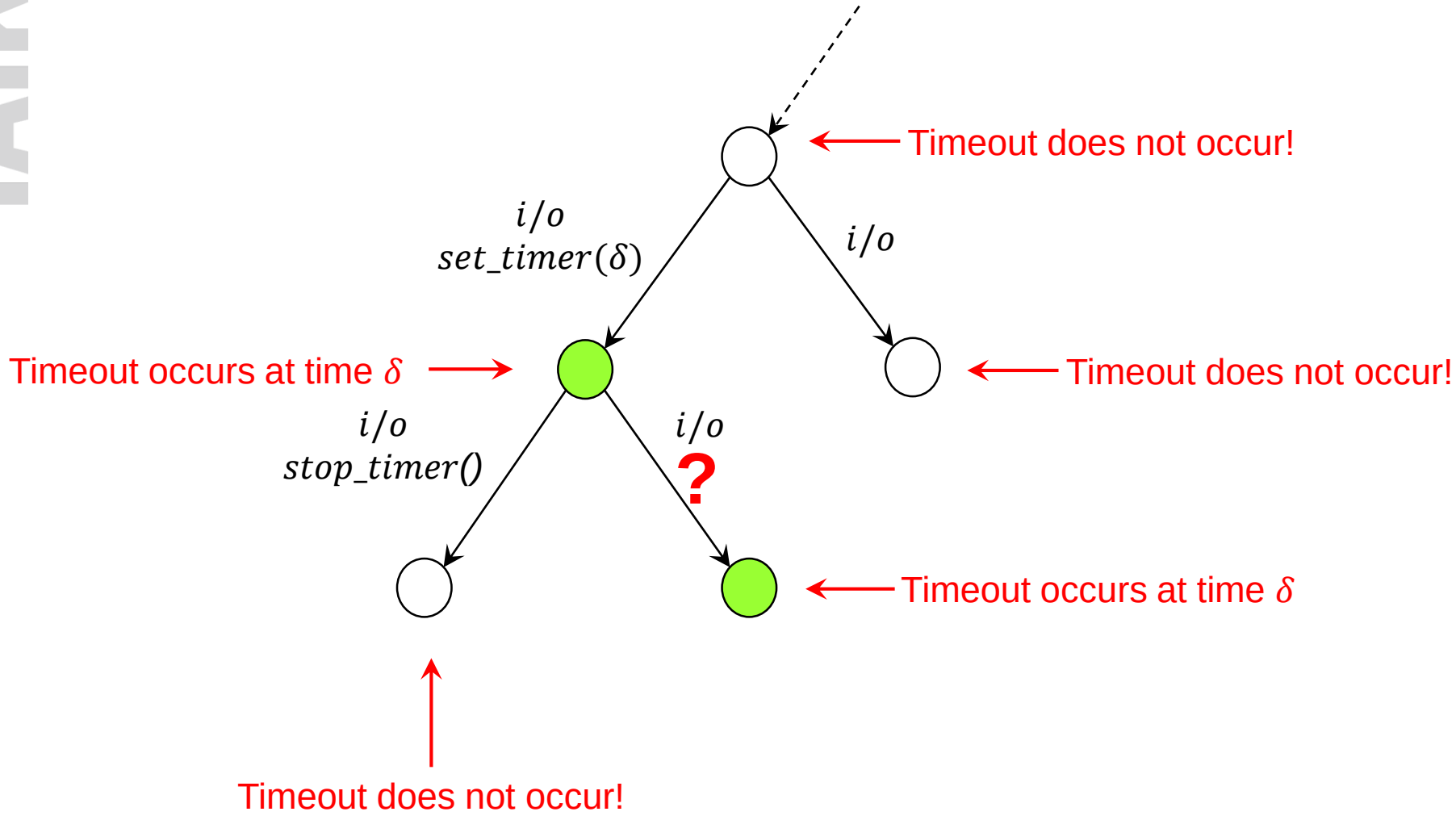


Membership Query contd.

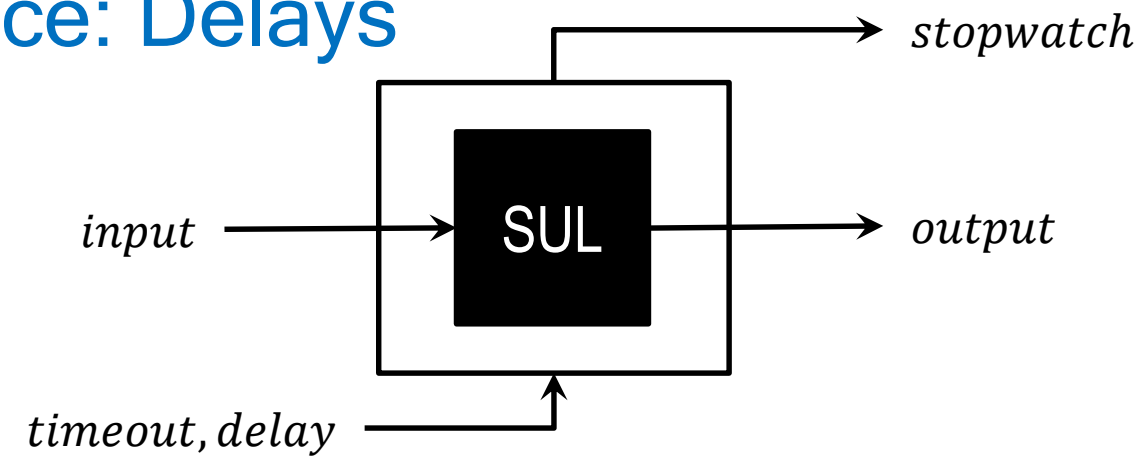
- Input Word
  - $a, a, timeout$
- Prefixes
  - ε
  - a
  - a, a
  - $a, a, timeout$
- Queries
  - $\varepsilon, timeout$
  - $a, timeout$
  - $a, a, timeout$
  - $a, a, timeout, timeout$



Practical Challenges



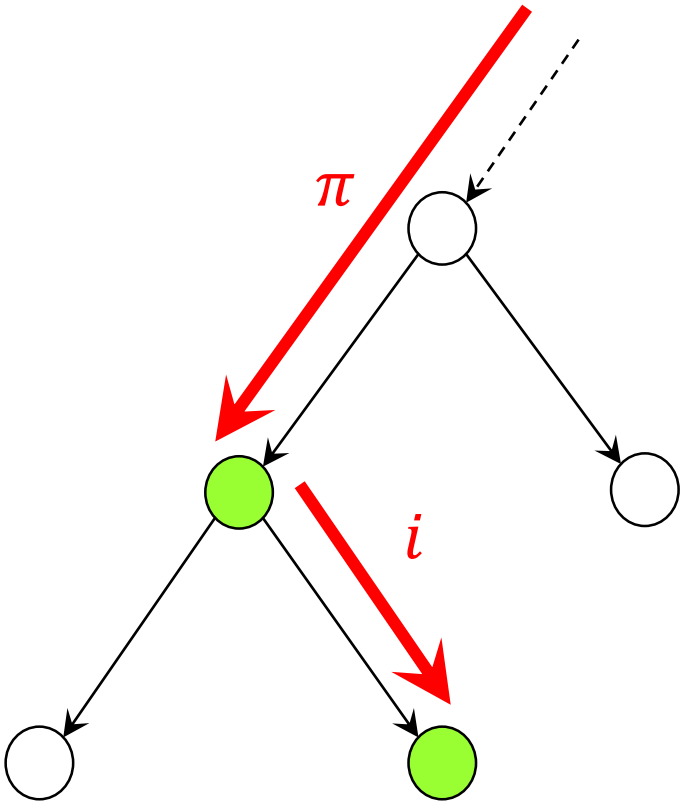
Interface: Delays



- Delay Symbol
  - Dummy input
  - Learner knows about it.
  - SUL/Oracle knows nothing about it.
  - Whenever delay occurs, learners wait for $d \leq \Delta$.

Practical Challenges contd.

- Query $\pi.i.timeout$
  Timeout occurs at time δ
- Query $\pi.delay.i.timeout$
  Timeout occurs at time δ'
- If $\delta' = \delta - d$ then timer reset does not occur, else timer is reset to δ'.



Learning IEEE802.11

Unblocking Uncontrolled Port to Initiate 4-Way Handshake

IEEE802.11 Authenticating State Machine

- IEEE802.11 Standards specifies security mechanisms for Wireless Networks.

- Often implemented as 4-Way handshake in Access Points.
- No available Implementations
  - Testing authentication step is access point specific.

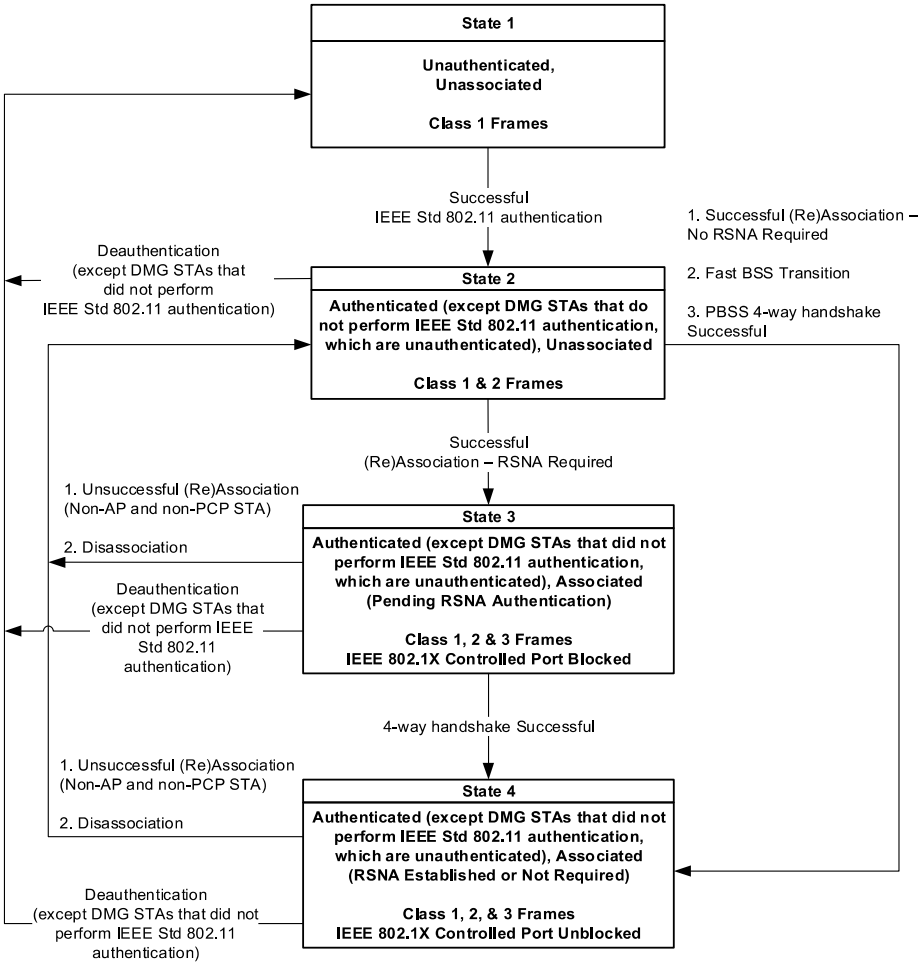


Figure 11-13—Relationship between state and services between a given pair of nonmesh STAs

Initiating IEEE802.11 4-Way Handshake

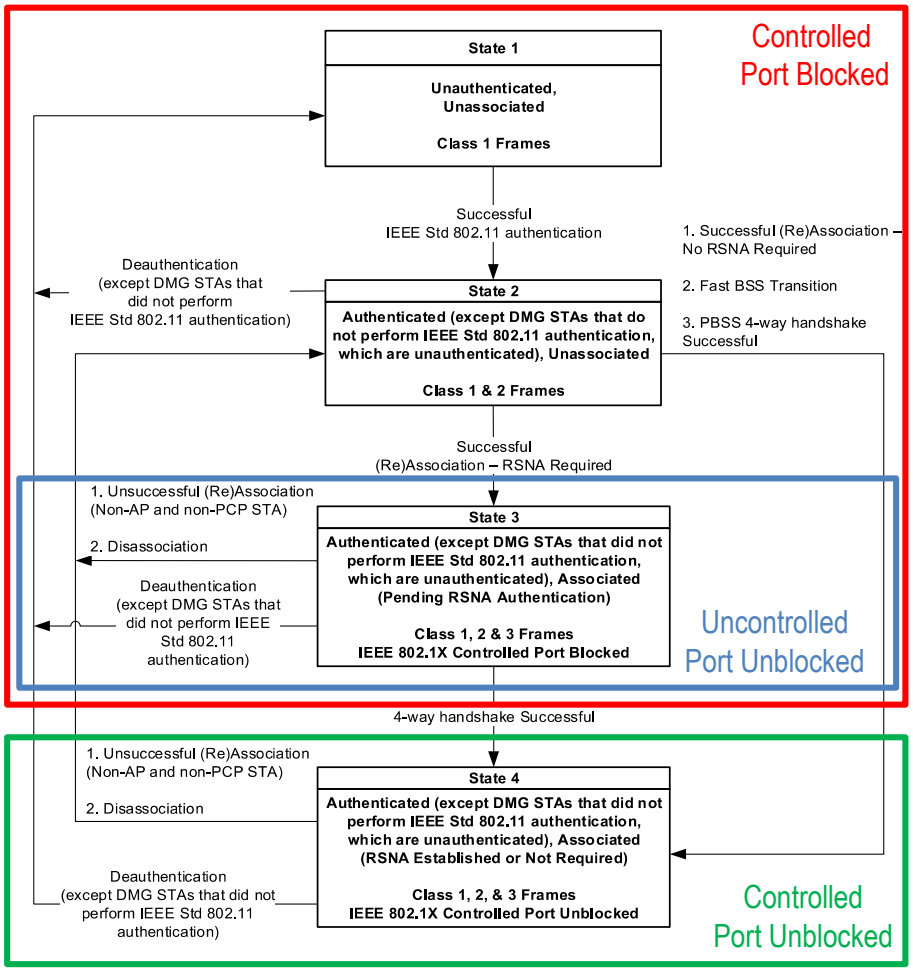


Figure 11-13—Relationship between state and services between a given pair of nonmesh STAs

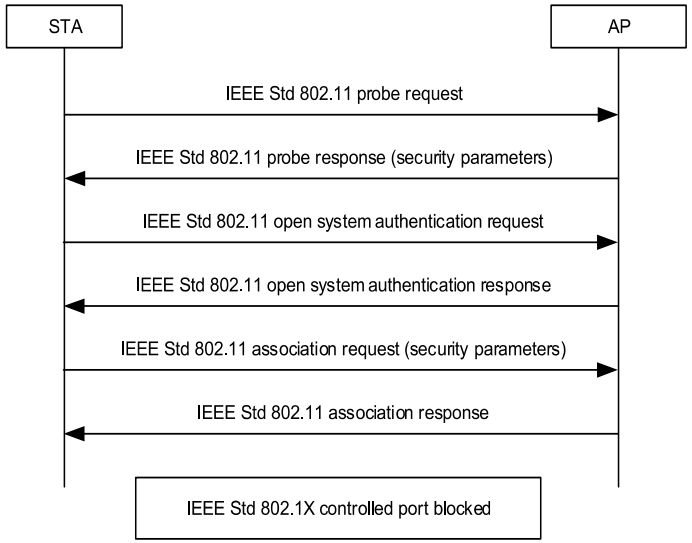
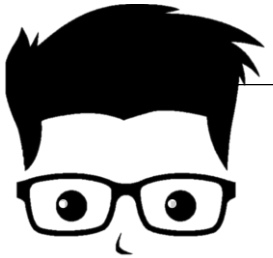


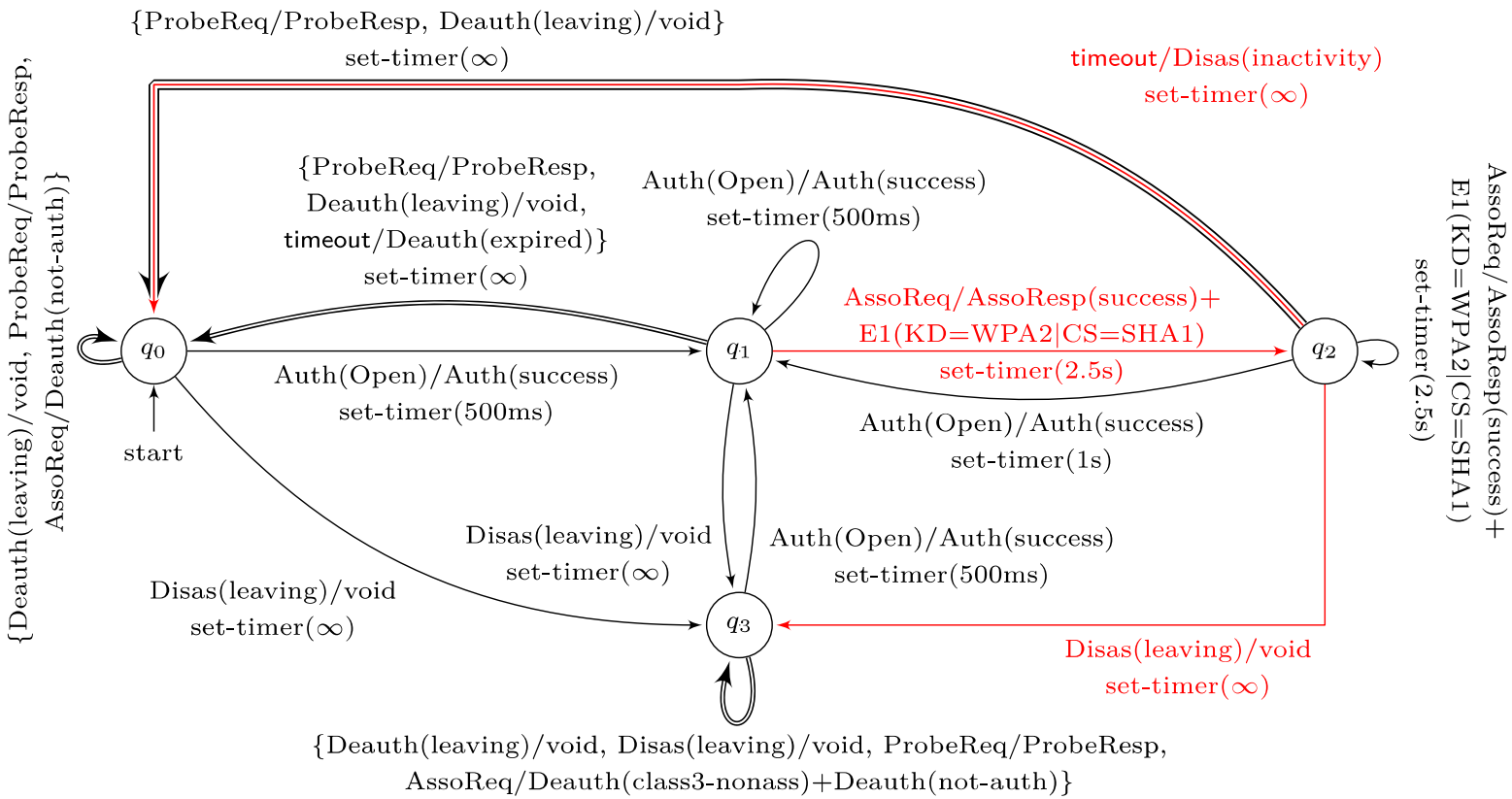
Figure 4-25—Establishing the IEEE 802.11 association



Feasible? How?

- Access Point
  - Reverse Engineer
- Transmitter STA
  - Sends inputs to AP
- Receiver STA
  - Sniffs outputs of AP

IEEE802.11 Controller in Huawei's Android



MM1T of a Huawei Mate10-lite that captures granting uncontrolled port. Double and triple edges represent a set of transitions. We rounded timer values to the nearest 500ms and marked specification violations with the color red.

Bachelor's and Master's Projects

Want to "Learn" More?

Let's do it!