Indiana Jones and the Raiders of the Lost RFID Tag

Screenshot "Indiana Jones and the Raiders of the Lost Ark" © Paramount Pictures, 1981.

Starring:
Bernhard Firner

Co-starring:
Yanyong Zhang
Richard Howard
Wade Trappe

Valuables are safe with RFID tags!

- If a tag is broken an alarm is triggered.
- You will always know where your items are!

But... perhaps not

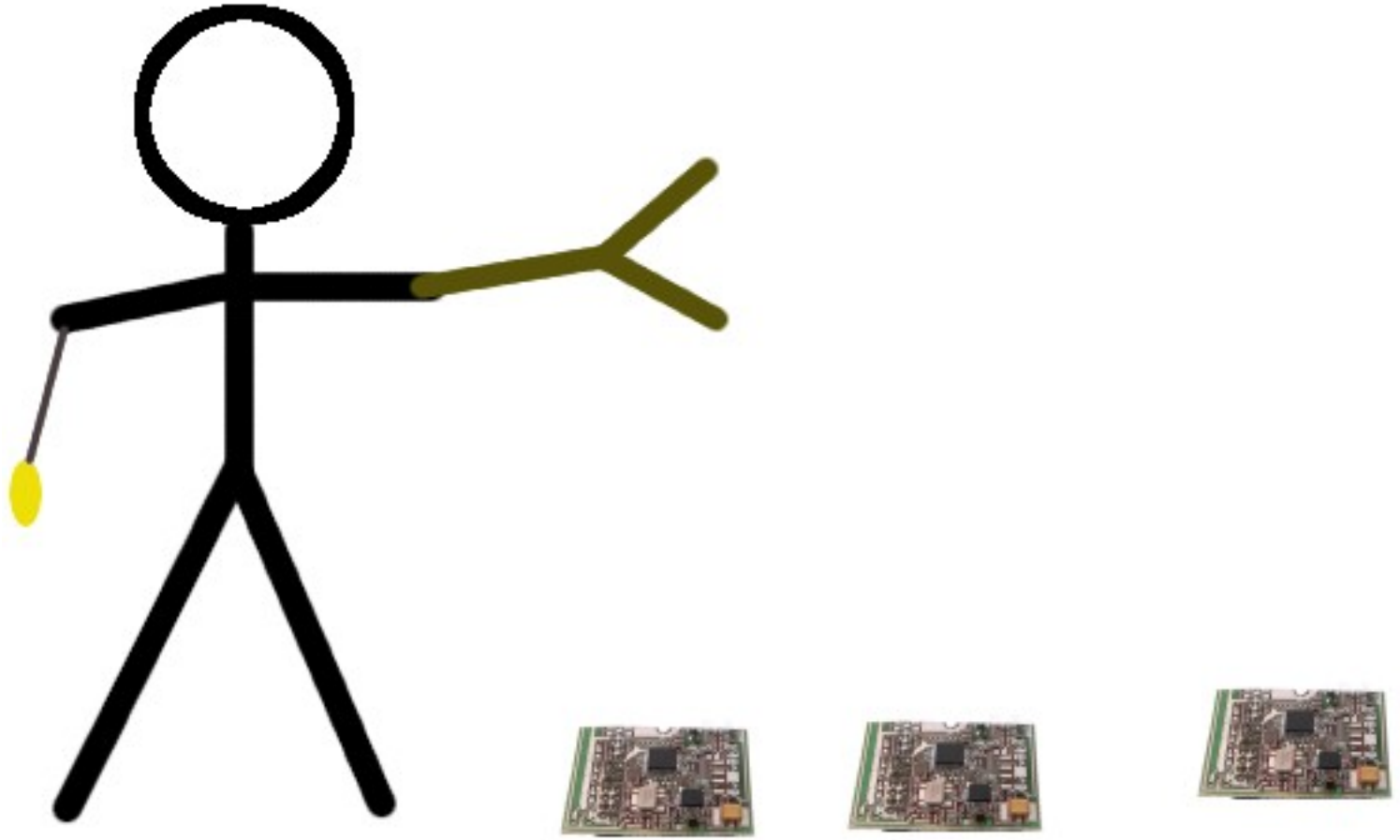
- RFID tags must be small and power efficient.
- The data and processing requirements for hash chains might be too great.
- Encryption is not helpful when every packet contains the same message (i.e. “still here”).
- RSSI “fingerprinting” is the easiest way to verify a tag's identity from one packet to the next.

We can switch a fake tag for another

- We can copy Indiana Jones and switch your item and tag with another tag that looks just like it!
- If we buy a hardware device that is identical to the target tags the copy will be nearly indistinguishable from the original.

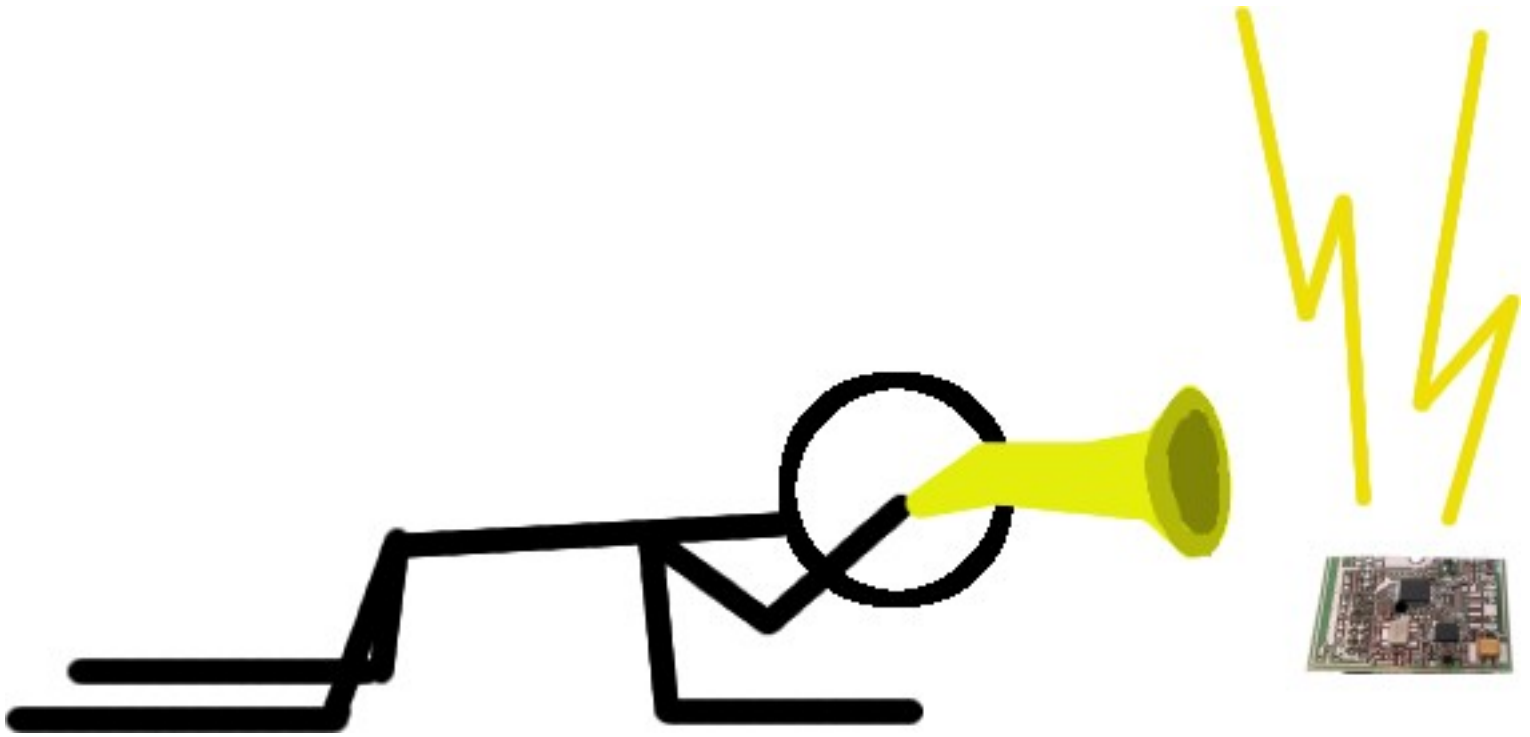
Step 1: Identify the target

- Can be done before the attack or immediately beforehand.

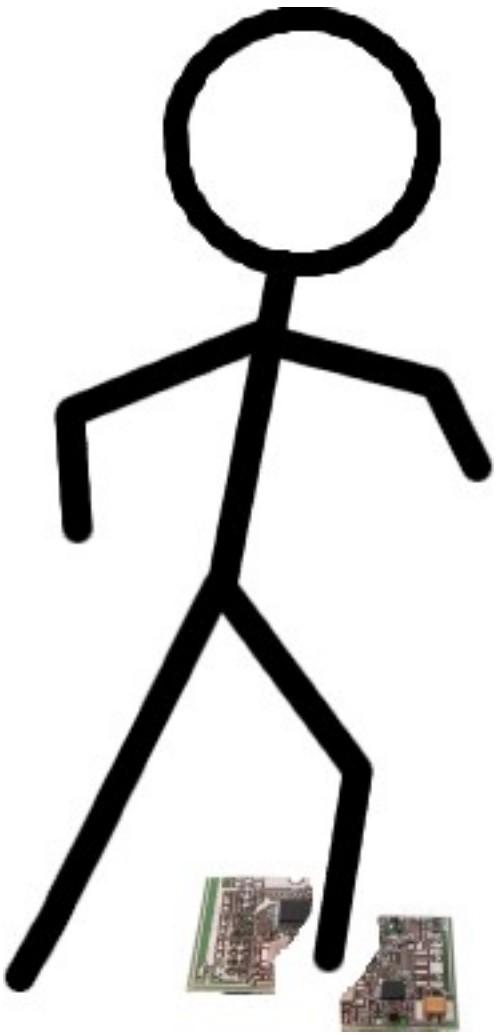


Step 2: Determine transmission schedule

- Can be done using the fake tag or with a different device. If an separate device is used it will need to program the schedule onto the fake tag.



Step 3: Silence the target

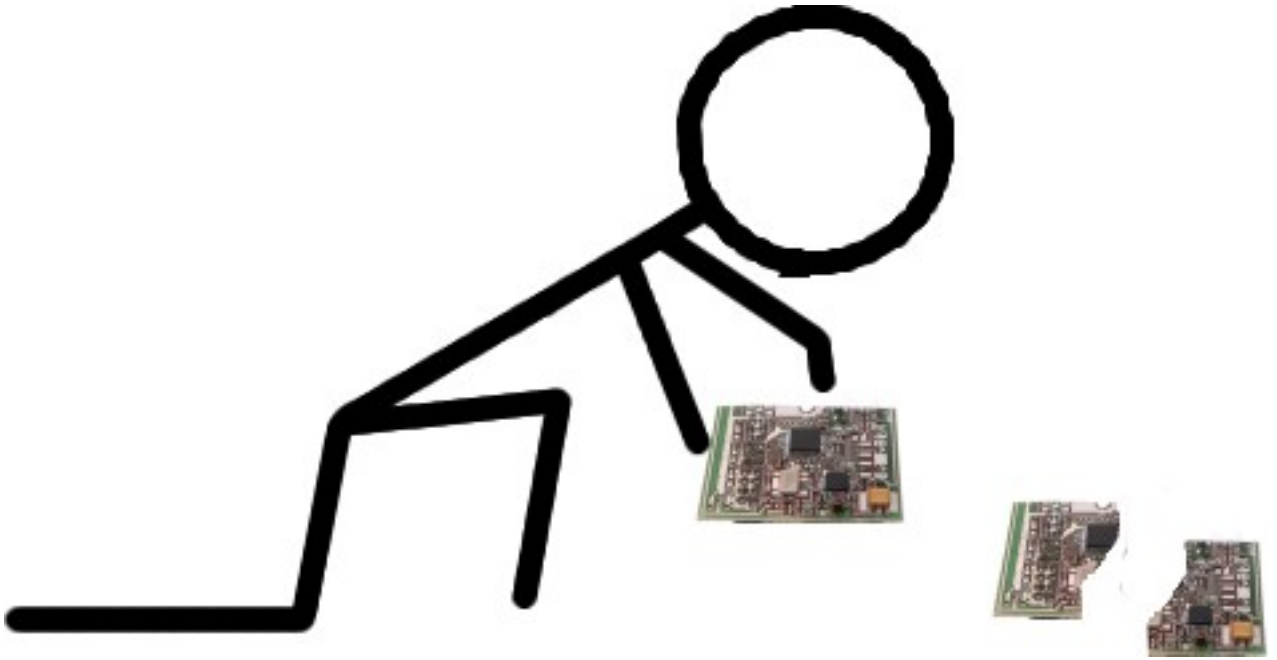


Acceptable methods may include:

- Physically breaking
- Electrically shocking
- Sealing in a faraday cage or wrapping with RF absorbing material

Step 4: Replace the target with a copy

- If a third device is used to determine the transmission schedule then it programs the copy with the schedule now.

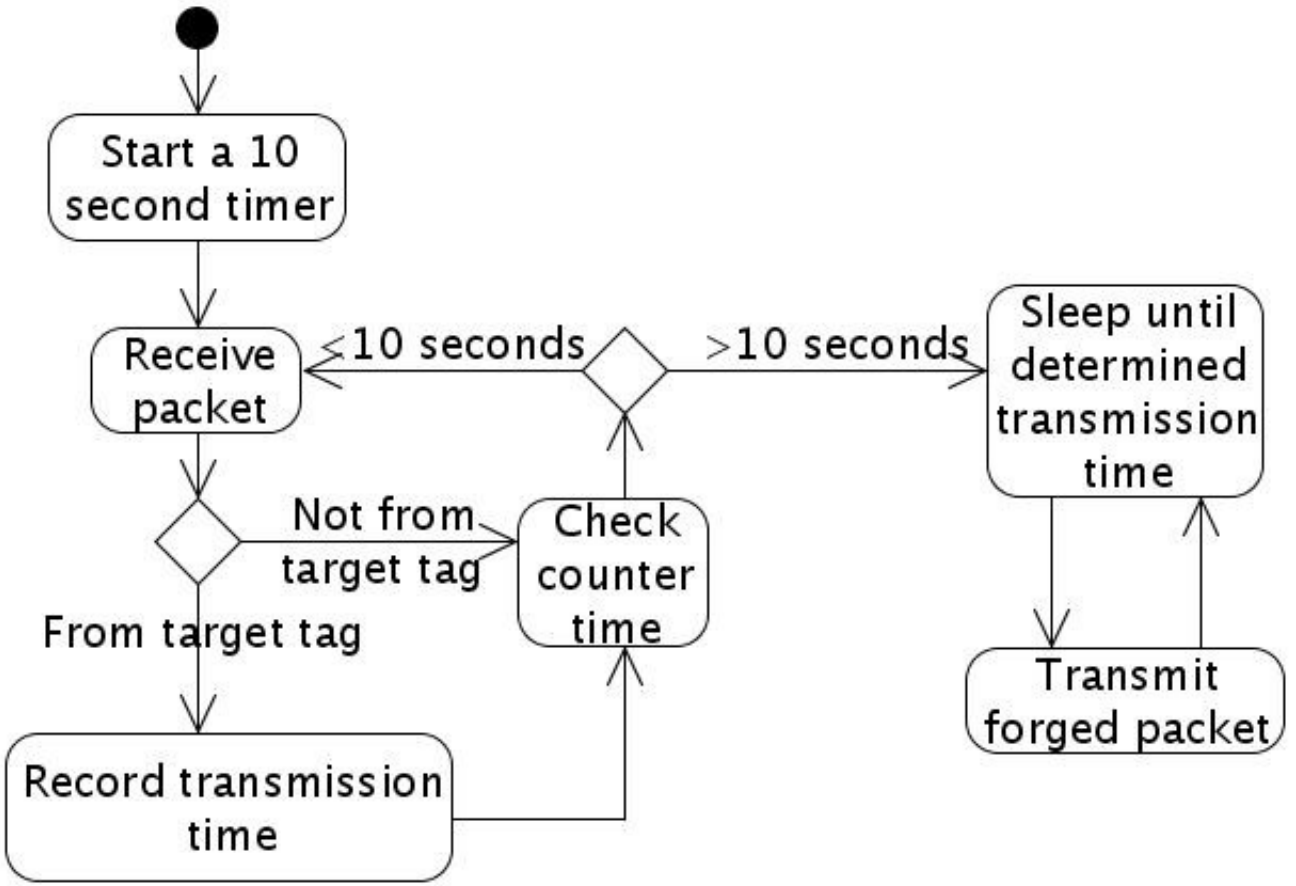


A real-life example

- We placed a target tag in the center of a square 10m on a side with 8 receivers on the outside.
- It is free to move about the area but cannot leave.
- The tag sends a heartbeat message every second showing that it is still present.
- We programmed an identical device with an Indiana Jones attack algorithm and attached a battery to it (to allow for longer use of the receiver).

Our Algorithm's State Machine

The tag is programmed with the target's ID before the attack

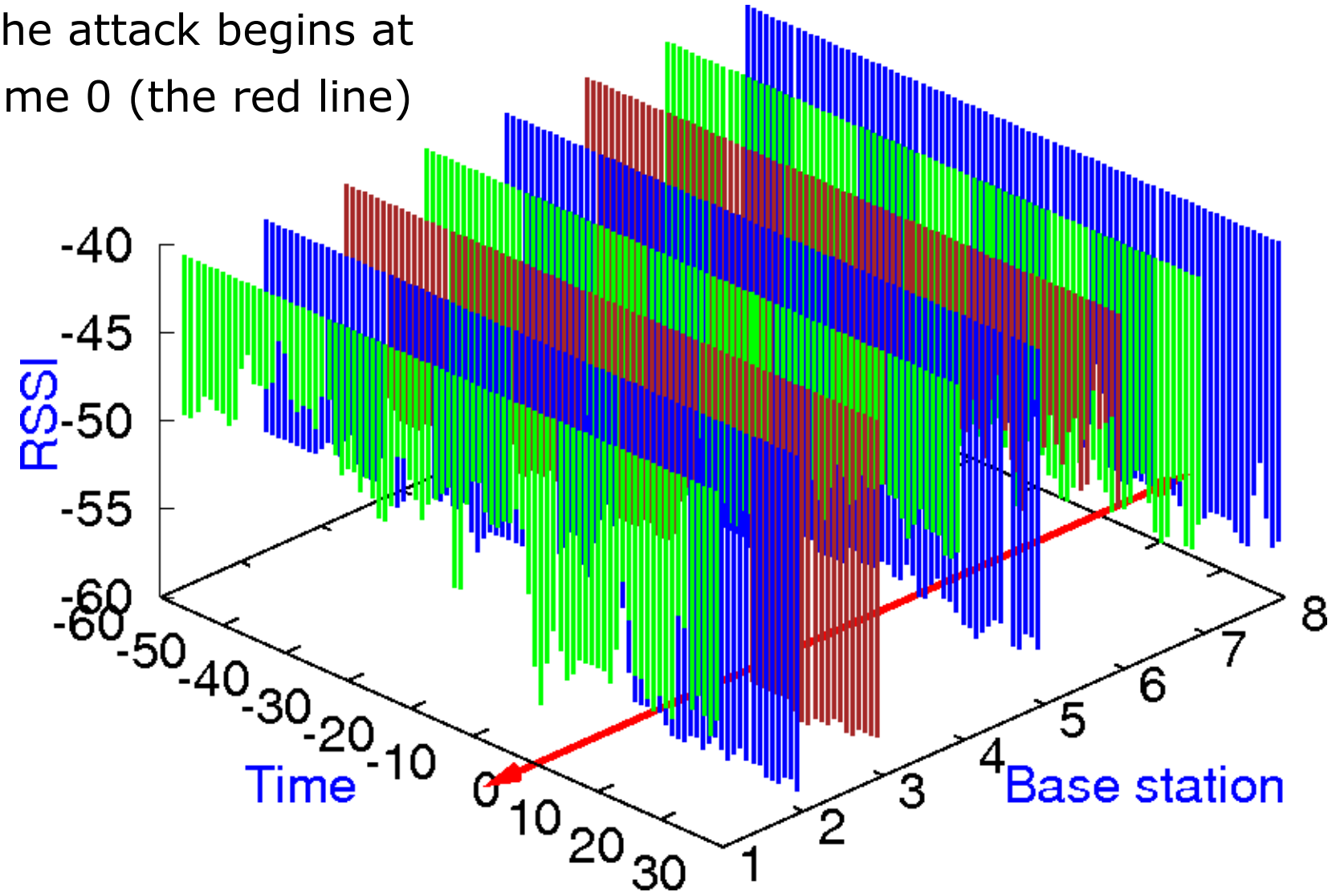


The Attack

- The malicious tag is turned on. It listens to the target and learns its transmission schedule.
  - The malicious tag is a copy of the target tag with an external battery to support extended receive times.
- Just before 10 seconds pass the target tag is silenced manually.
- After listening for 10 seconds, the replacement tag begins transmissions and is left in place of the target tag.
- The attack takes one person less than a minute to carry out.

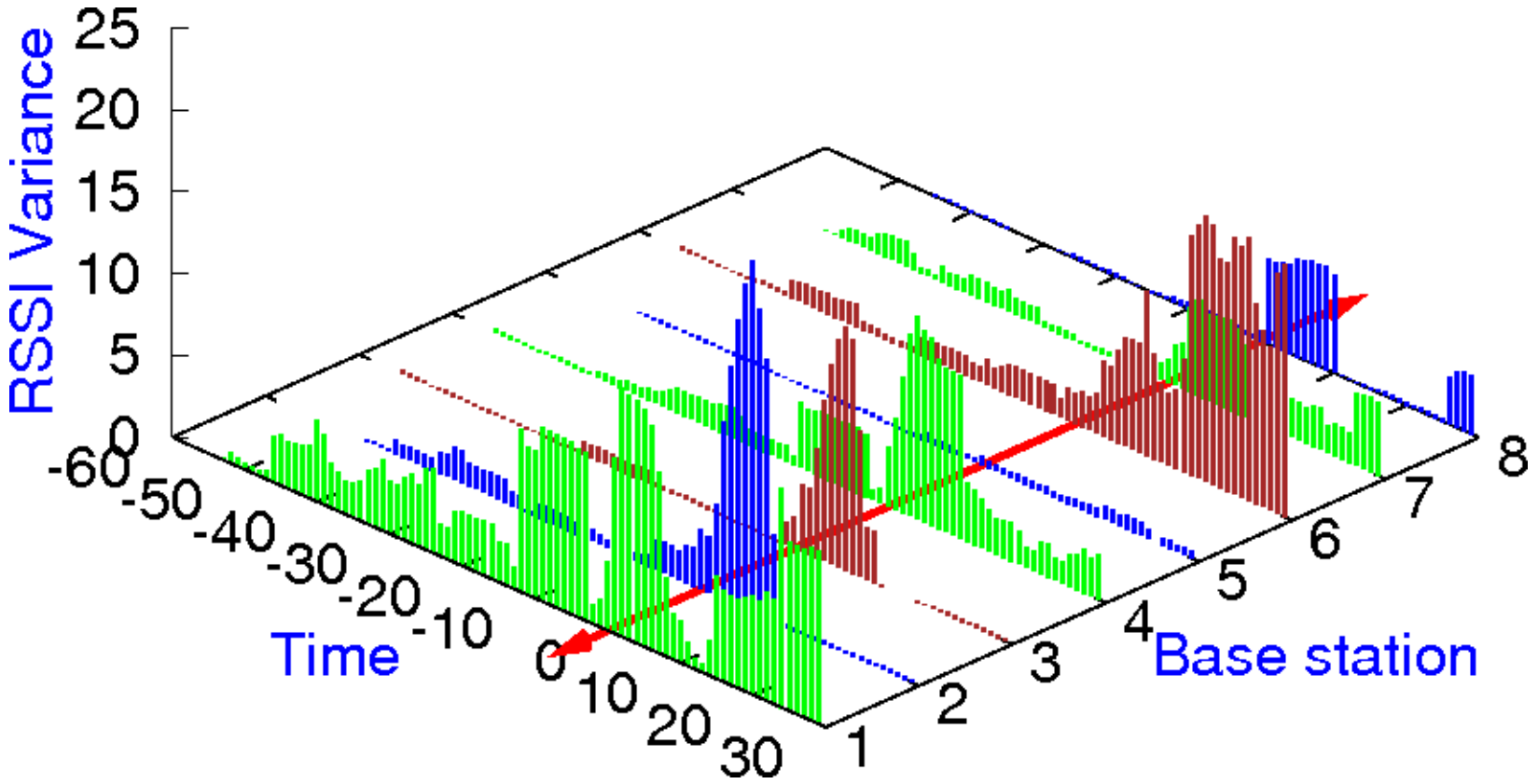
RSSI is too messy to evaluate the discreetness of the attack

The attack begins at time 0 (the red line)



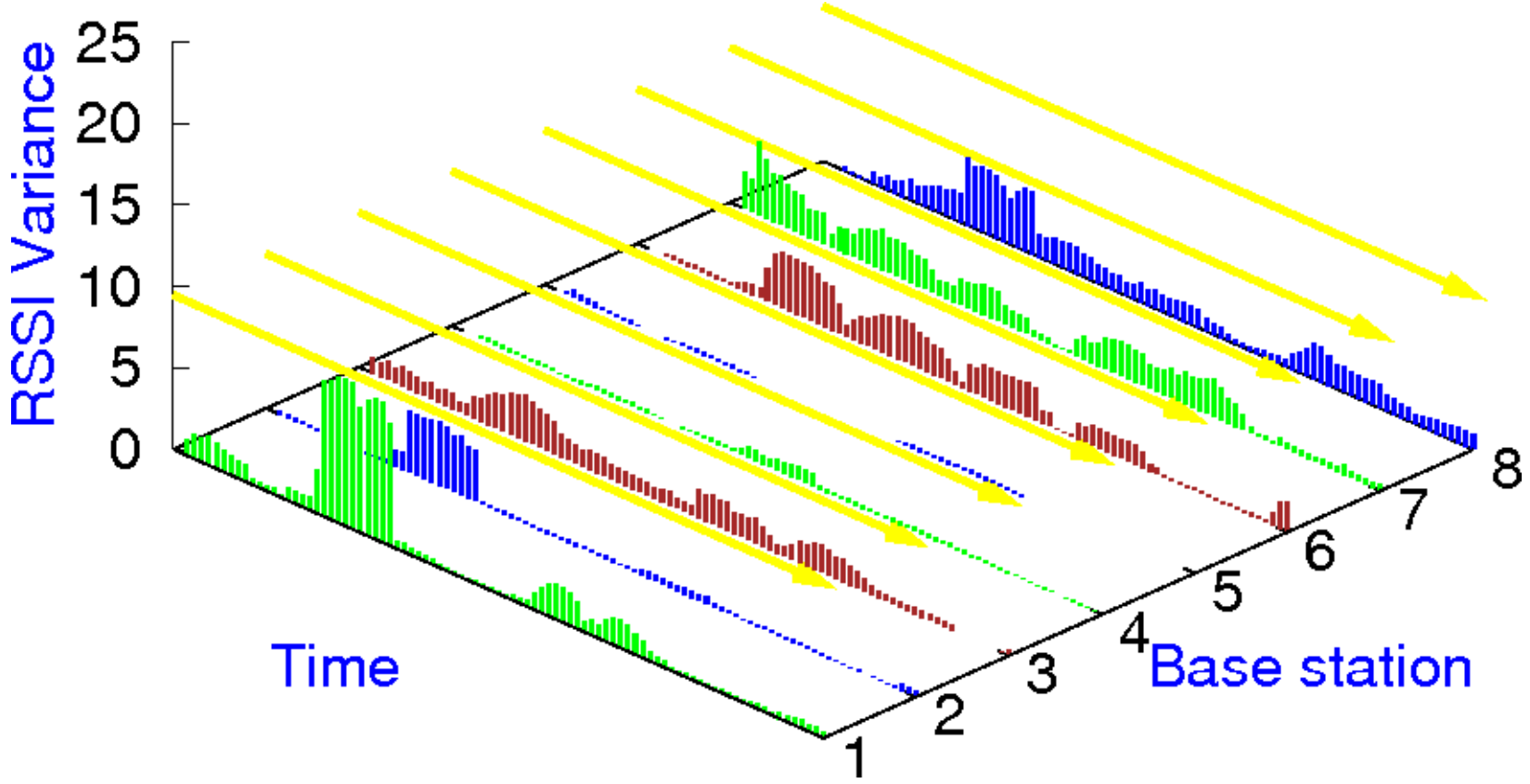
The RSSI variance clearly shows the attack

The variance of the RSSI is determined over the last 10 second interval.



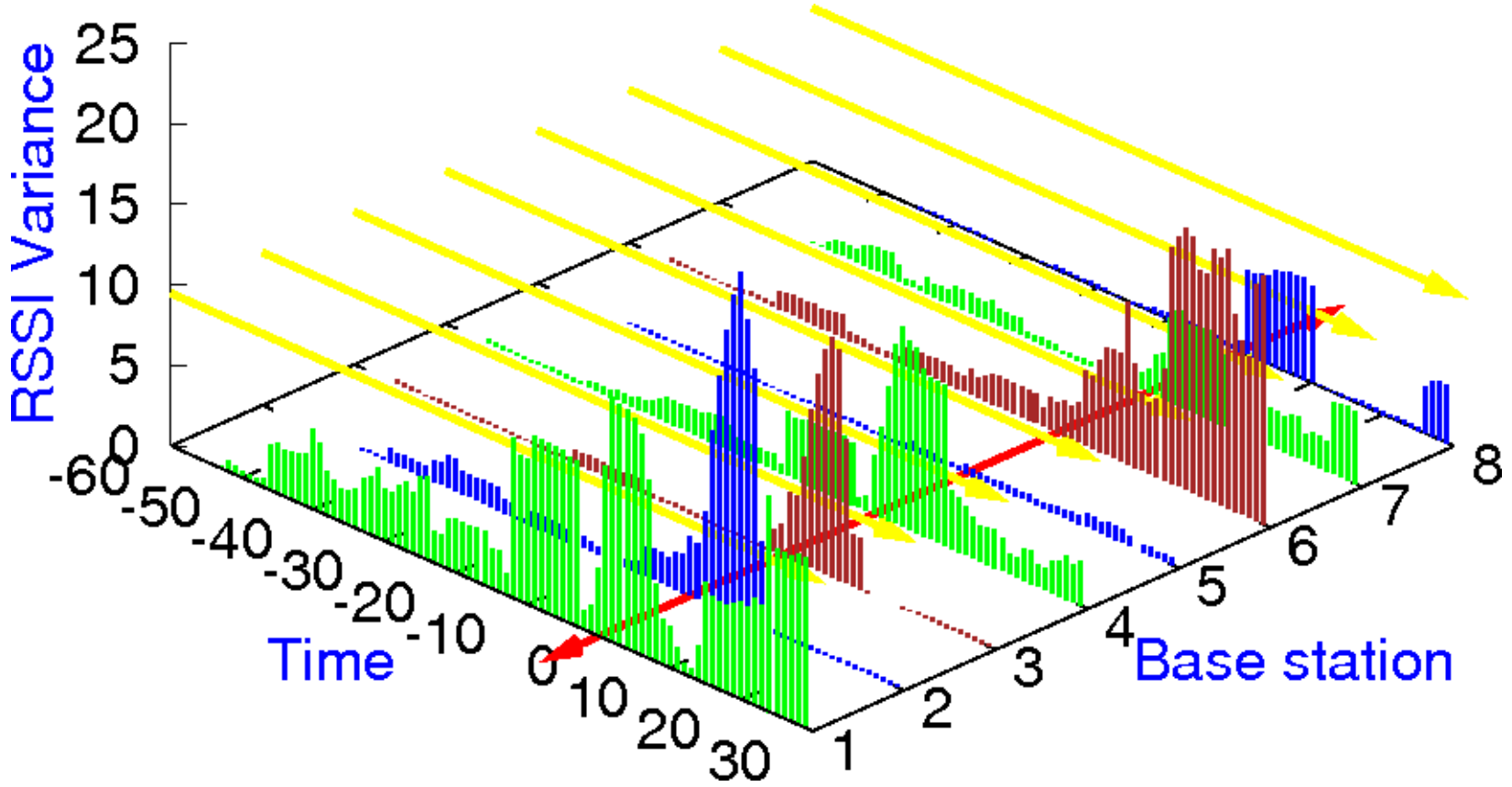
Variance thresholds are obtained from stationary data

The yellow bars indicate a maximum value for the RSSI variance in stationary data. The RSSI variance is very low in data where the tag is not moving.



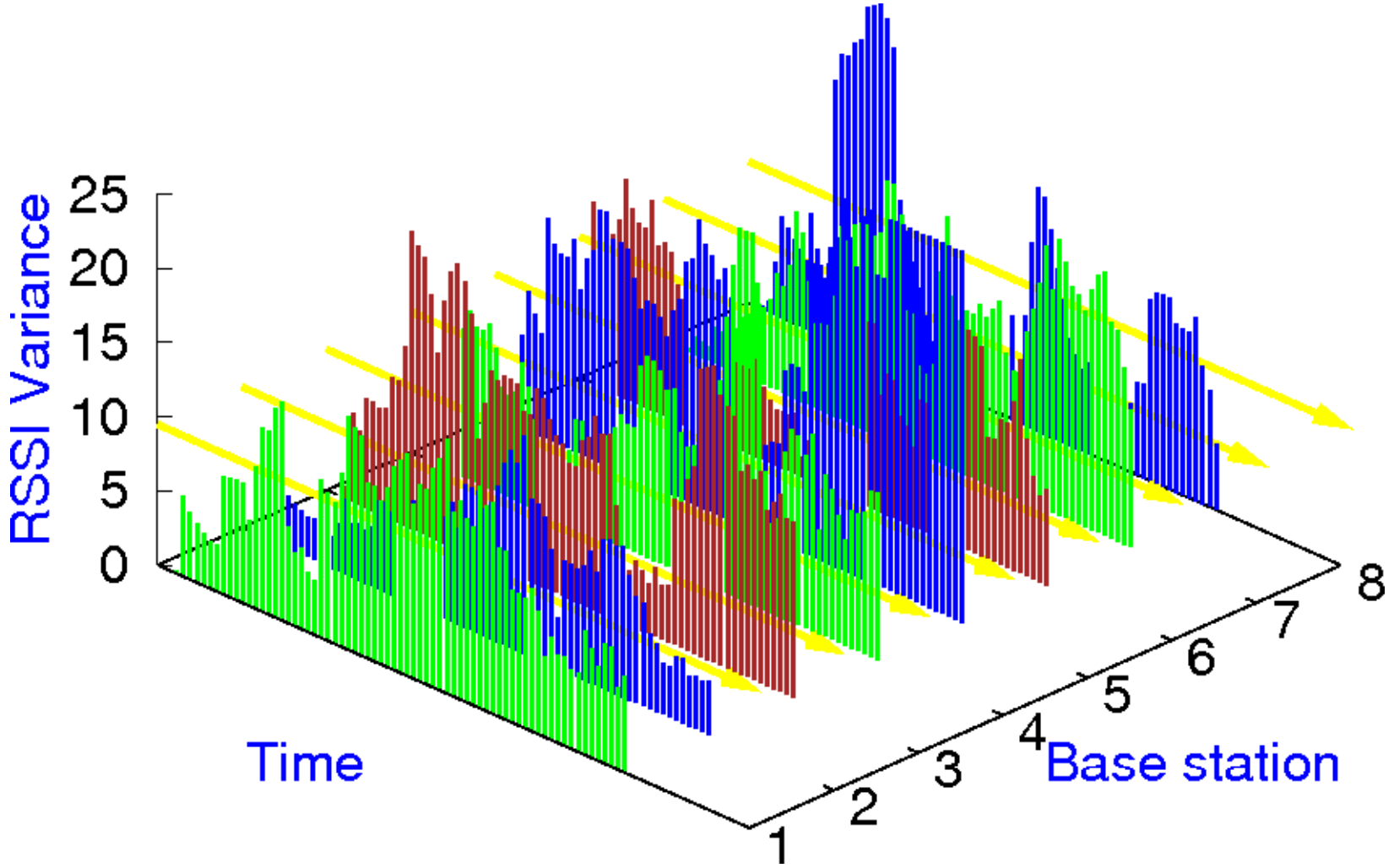
Using the threshold on the attack data clearly identifies it

The variance crosses the yellow line when the switch takes place.



Thresholding would confuse tag motion with an attack

The variance easily crosses the yellow line when the tag is moving.



An attacker can perturb RSSI readings as a smoke screen

- By jamming packets close to the attack the attacker can hide the sudden changes in RSSI
- If the attacker can move the object then the switch can be done while the tag is moving
- In dynamic environments RSSI is also in a constant state of flux – an attacker can leverage this to mask an attack by performing it in crowded places and at busy times
- Most situations will probably have fewer receivers – RSSI fluctuations can be caused at the receivers during the attack

Conclusions

- Indiana Jones can get away if conditions are right
- A high duty cycle, many receivers, and a machine learning algorithm might be a defense.
  - We have preliminary experience using RIPPER to distinguish between environmental RSSI fluctuations and RSSI fluctuations during motion
  - Systems with low cost basestations and mesh networks have more receivers and thus more data
- Fingerprints based upon hardware irregularities (such as transients) require expensive hardware
  - It might be possible to embed unique characteristics in hardware during production