Cikhaj Experiment 2013

Experimentální vývoj bezpečnostní softwarové platformy se systémem detekce průniku a režimy ochrany soukromí pro bezdrátové sensorové sítě (VG20102014031)

https://minotaur.fi.muni.cz:8443/~xsvenda/docuwiki/doku.php?id=public:cikhaj2013

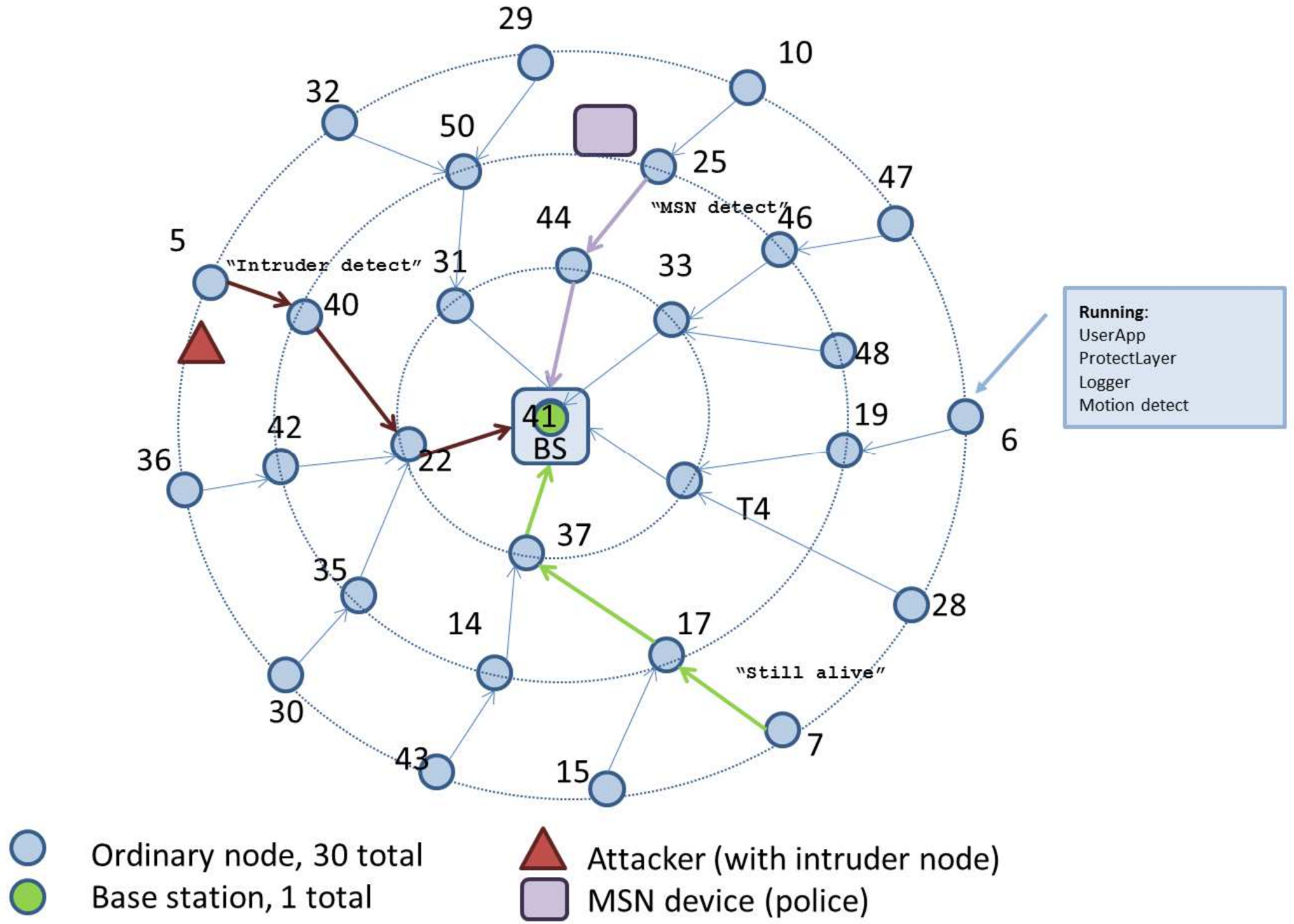
Petr Švenda svenda@fi.muni.cz

CROCS
Centre for Research on Cryptography and Security

Motto:
In theory, theory and practice are the same…

Goals

- Test of first version of prototype
- Capture traffic data (at least some) and analyze later
- Find bugs in existing code
- Obtain results from different environment
- Make some progress towards final prototype ☺

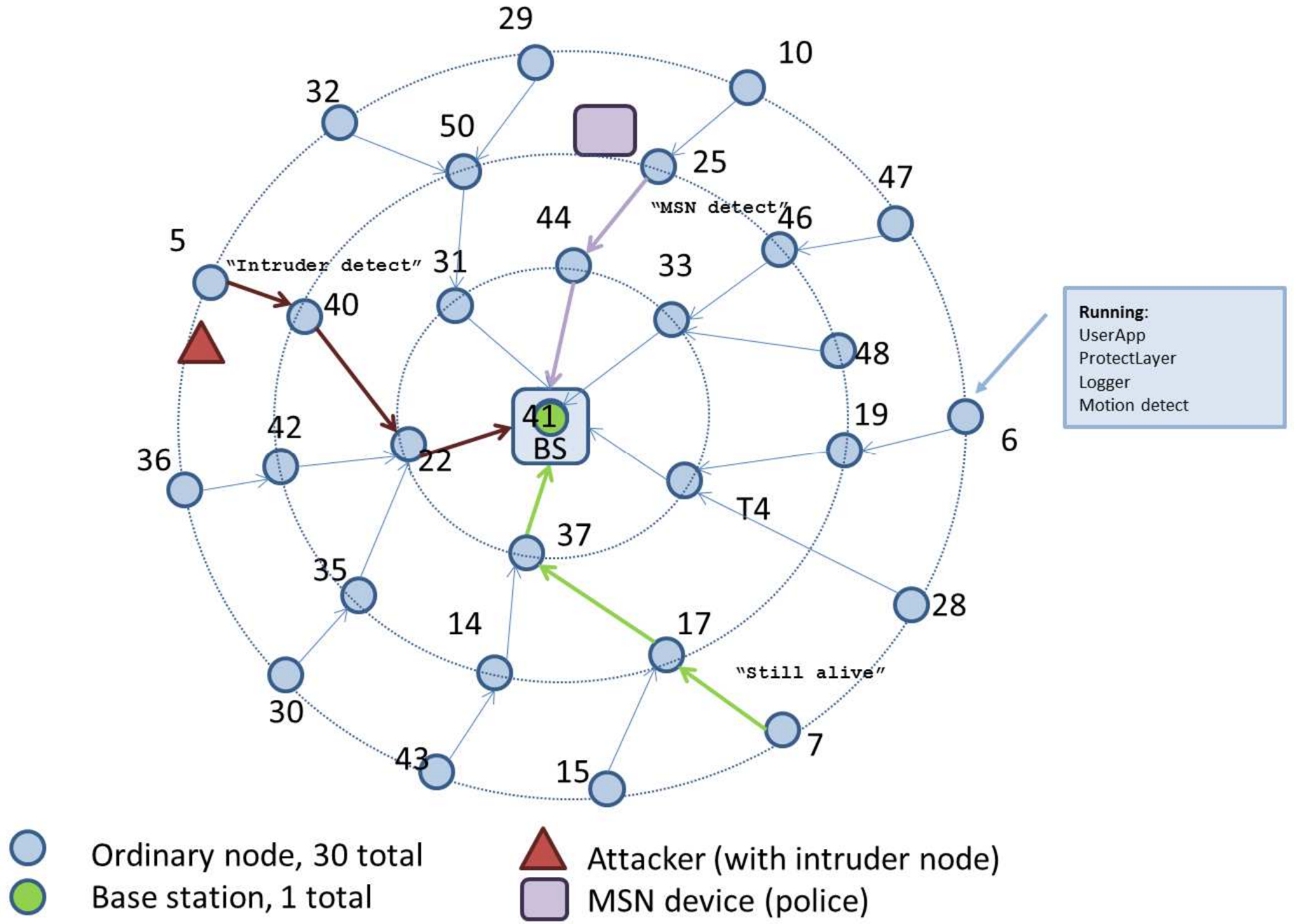

29
10
32
50
25
47
"MSN detect"
44
46
5
"Intruder detect"
31
33
40
48
41
BS
19
6
42
36
22
T4
37
35
28
14
17
"Still alive"
30
7
43
15
Running:
UserApp
ProtectLayer
Logger
Motion detect
Ordinary node, 30 total
Base station, 1 total
Attacker (with intruder node)
MSN device (police)

Settings

- 30 nodes in network, snow towers
- “Still alive” message every 5 seconds
- Fixed static routing tree (only packets to BS)
- Attacker movement detection simulated by radio proximity
  - Will result in “Movement detected” message

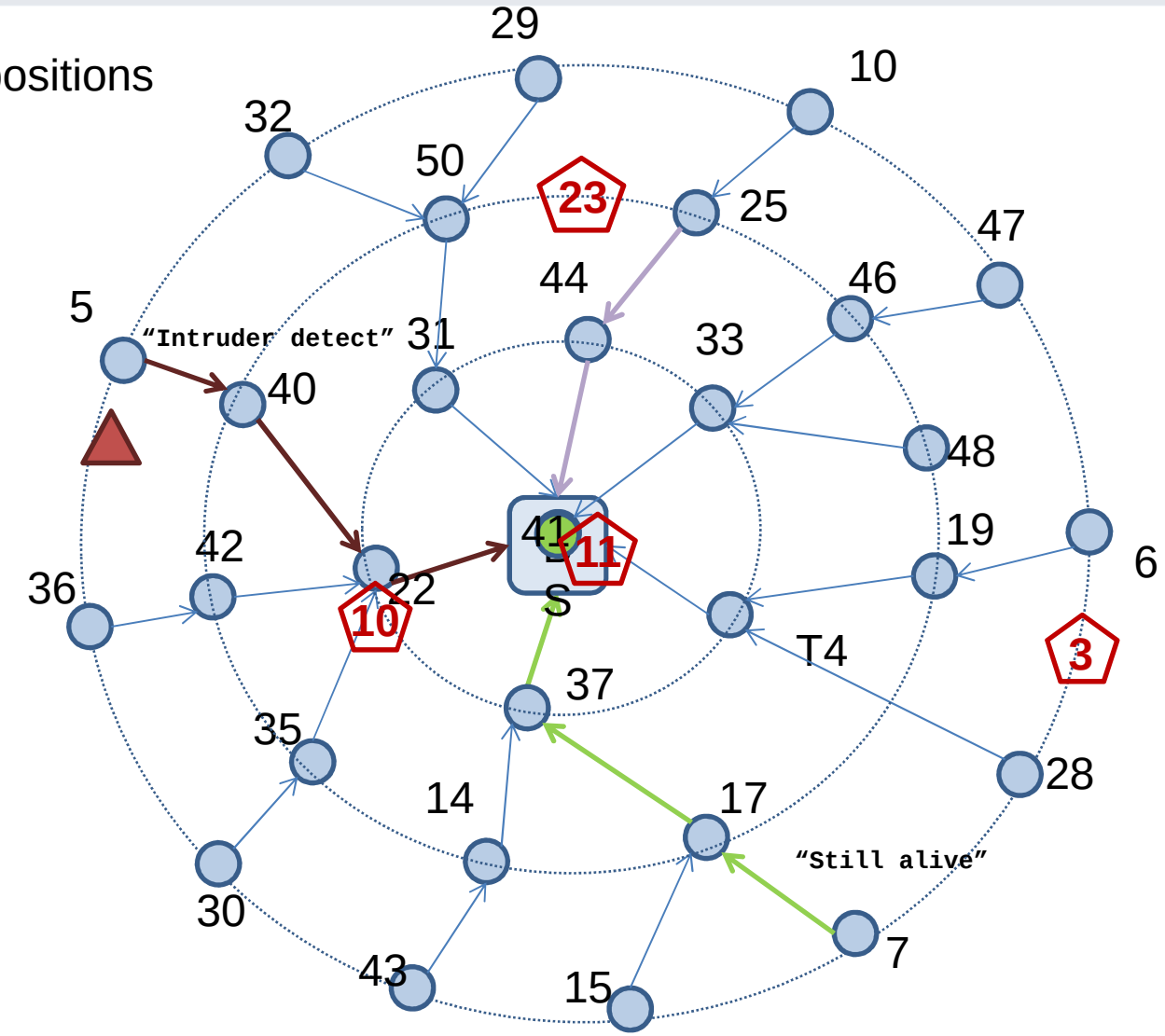
Components

- Transparent layer (AMSend)
- Privacy component (routing, encryption)
- Intrusion detection component (logging)
- Key distribution component (pairwise keys, simulated encryption)


29
10
32
50
25
47
"MSN detect"
44
46
5
"Intruder detect"
31
33
40
48
41
BS
19
6
42
36
22
T4
37
35
28
14
17
"Still alive"
30
7
43
15
Running:
UserApp
ProtectLayer
Logger
Motion detect
Ordinary node, 30 total
Base station, 1 total
Attacker (with intruder node)
MSN device (police)

Scenarios

Sniffer positions



Ordinary node, 30 total

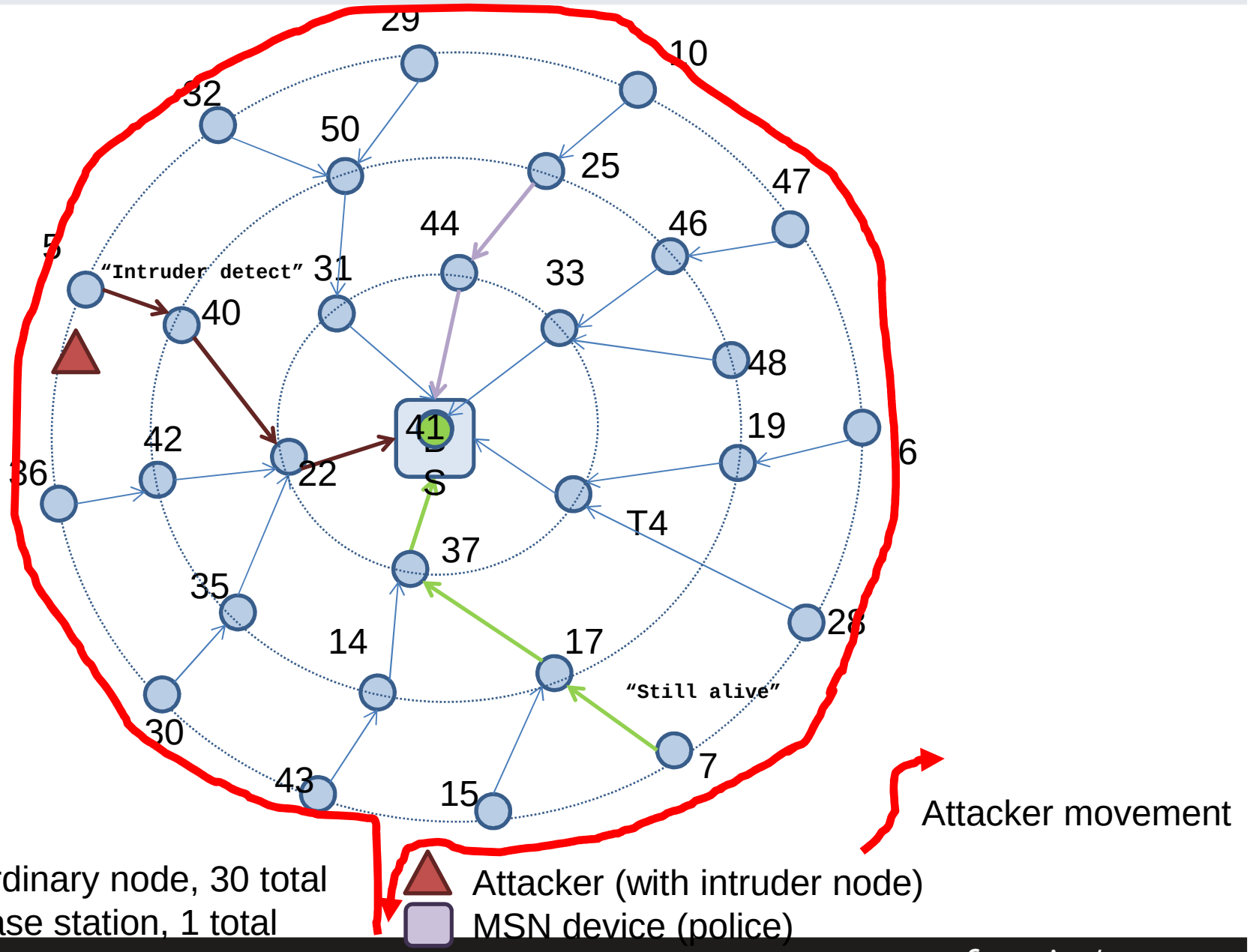
Base station, 1 total

Attacker (with intruder node)

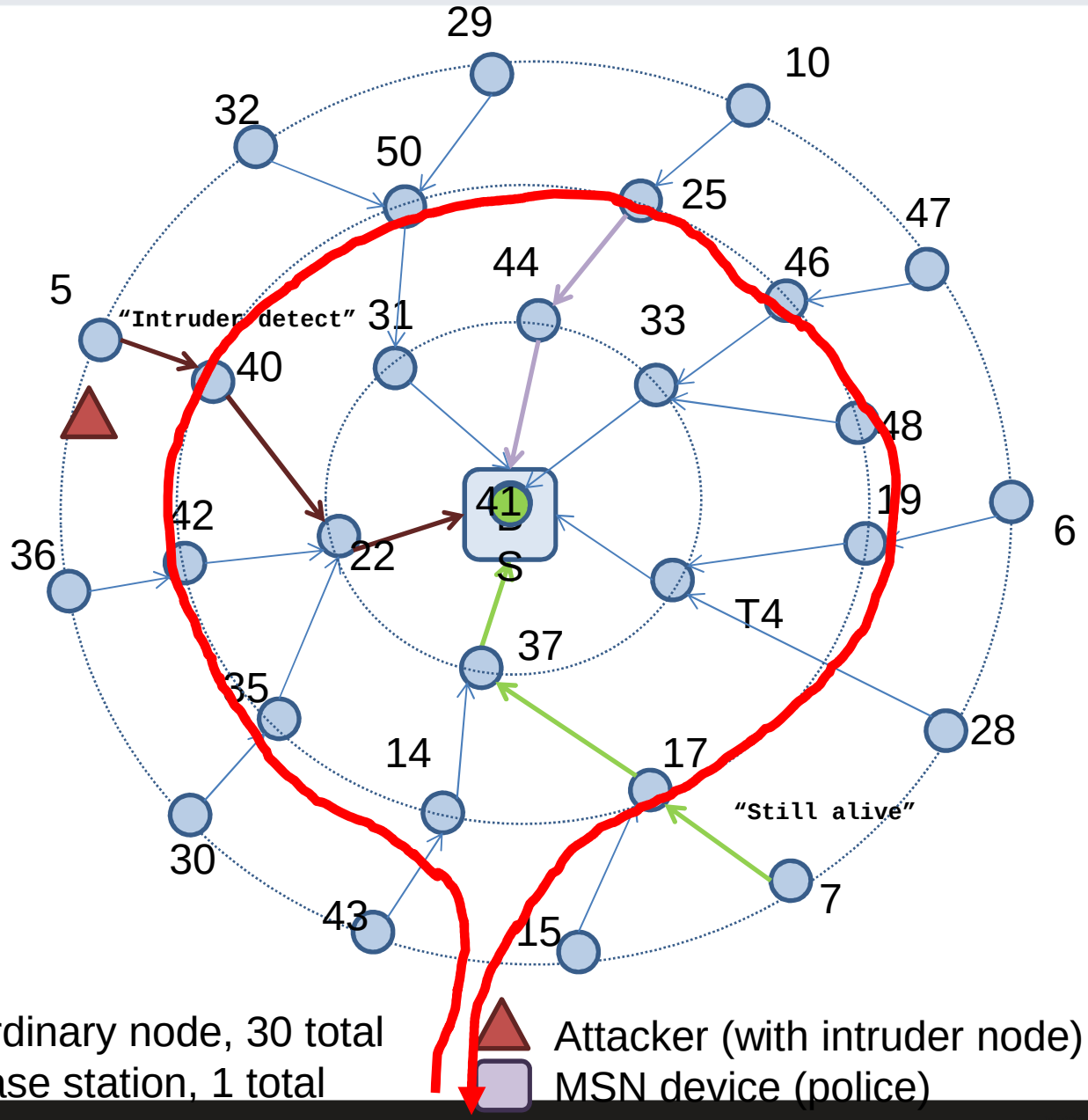
MSN device (police)

sniffer

Attacker1: outer circle, slow movement



Attacker2: fast run, entering from nodes 15, 14, 22, run around inner circle, leave around node 15



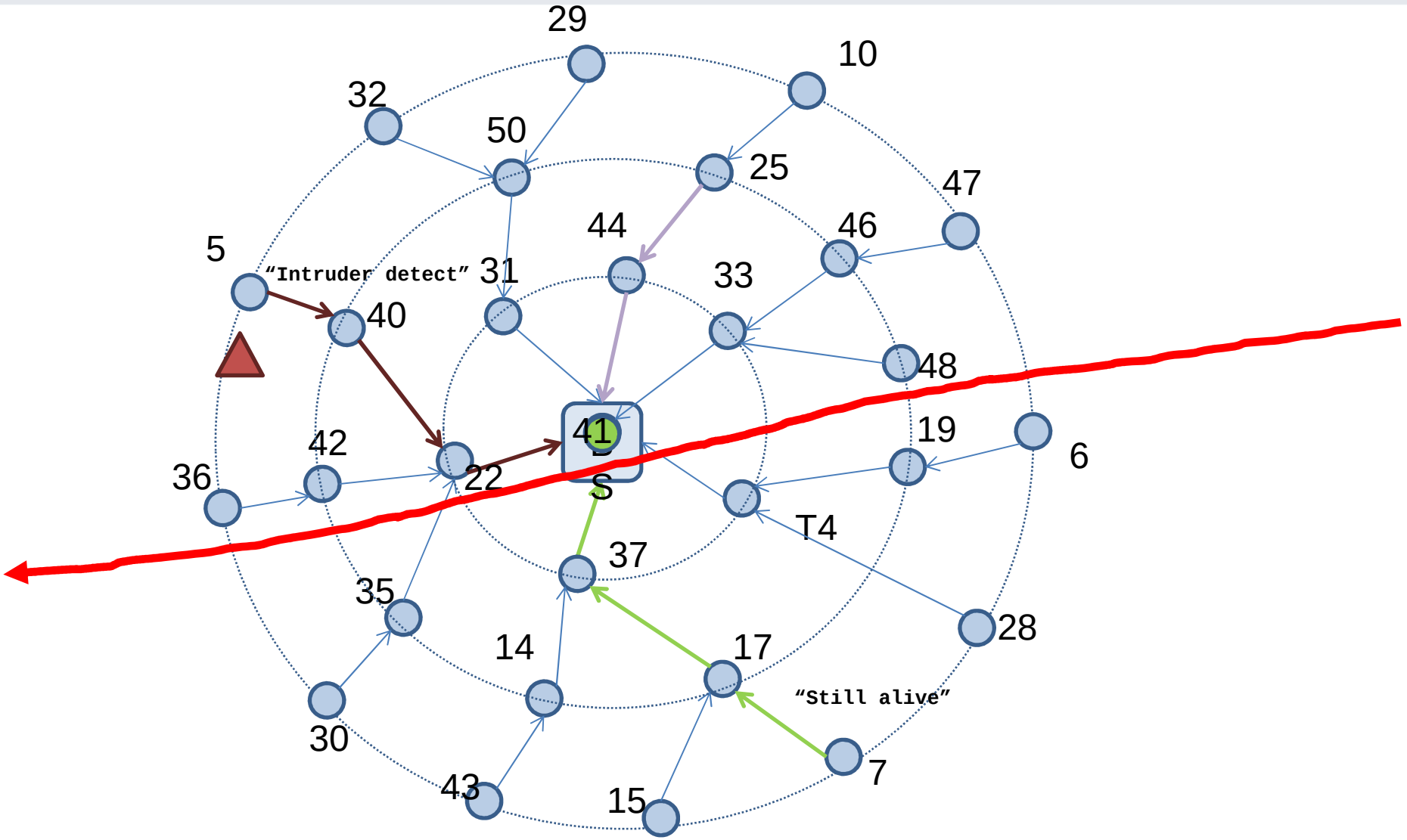
Ordinary node, 30 total

Base station, 1 total

Attacker (with intruder node)

MSN device (police)

Attacker3: fast run throw the middle, starting at 6, ending 36



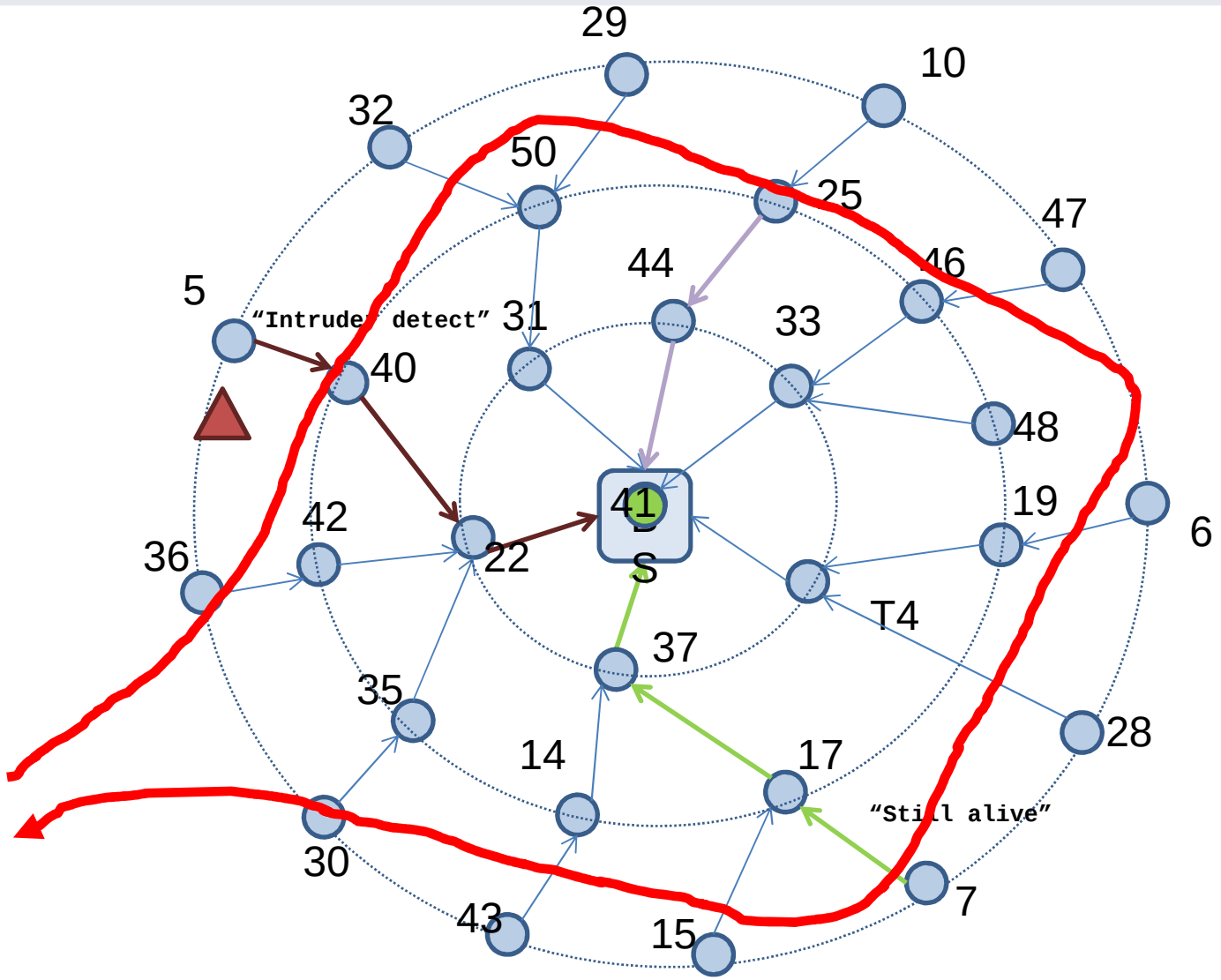
Ordinary node, 30 total

Base station, 1 total

Attacker (with intruder node)

MSN device (police)

Attacker4: fast run in square pattern



Ordinary node, 30 total
Base station, 1 total
Attacker (with intruder node)
MSN device (police)

Datasets

- https://minotaur.fi.muni.cz:8443/~xsvenda/docuwiki/doku.php?id=public:cikhaj2013
- Logs from nodes (total 28 nodes)
  - One single file for each node (whole experiment)
  - All messages received by particular node (including messages for other neighbors)
- Logs from sniffers (total 4 sniffers)
  - 5 different files for each sinffer
    - Network without attack (~60 min)
    - attacker1…attacker5 (2-5 minutes)
  - All messages received by sniffer
  - (sniffer close to node should yield similar logged data)

Content of log

- Sender, receiver, counter, + weak ordering (position in file)
- Counter incremented
  - after every message send from originating node
  - not changed during routing to base station
- “Still alive” and “Movement detected” messages share same counter!
  - (better to have two separate counters - future)

Topics for data analysis

- What section of network was captured by sniffers?
  - Does it corresponds to antenna properties?
  - How to make orientation of sniffers in future?
- How many packets were lost?
- Were there communication bottlenecks?
  - ~ higher ratio of message dropping in nodes close to BS
- How fast and reliably was attacker detected?
- What logging functionality should be improved for future?
- …?