**System and Threat model:**

1. Set a practical setting, nodes arriving periodically.
2. Adversary could have some actual devices on site and large number of emulated ones.

The adversariel device could be physical (laptop, phone, cloud?), fully emulated and hybrid, how many virtual nodes can be booted?

1. What if the adversarial devices have more laptops? This can actually be seen as a colluding attack. This could be discussed in the thesis. 3 laptops with 50 devices. Discussing the weaknesses of the model.
2. Clear on \*Many\* devices. 10 phones? We should not say vague terms. We make simple model assumption then define why we say 10-20 emulators bc our computer can run 6-7 so lets assume 2 laptops etc.
3. We have to be careful. 1 node 10 sybils all by themselves. As long as we are clear. You register but initiate a protocol, discovering, what you are actually finding, we decide whether you are in or not. We can take a mark on such nodes and may give half trusts to them.
4. Other guys join the system while in the rounds begin, shall we allow them. Let’s algorithmically show that this works.sla

**Details of the model:**

1. Discuss the effort on root device and modify emulators.
2. Be sure why 2 log(n) rounds really work. Why not more or less.
3. Whitewash and punish -> Eliminate, whitewash and punish
4. REcord structure does not make sense actually.
5. Be clear if some nodes do not submit/transmit. Define a complete round. What is a complete round. What if nodes dropout? We say null to them
6. There should be a conclusive round, the attacker cannot prevent others from participating unless they jam. You are registered with a question mark (?), you are additionally evaluated.
7. What would be the negative outcome, if there is D\_i of region R, as a result of replay by an attacker, is now classified as sybil. False negatives, false positives: We explain this clearly. Each time in different region, a device would be classified as a new device. Therefore it’s useless to replay in different areas.
8. Assignment of roles, communication, you should operate as such, be detectors.
9. What about the scoring method. Is it the best one, effective one, immune to misbehaviour itself? Does it depend on the actual values, their granulanity, depend on the number of total nodes.
10. Threshold selection: Different ones

**Others:**

1. In the writeup, what is same and what is different from the other works
2. Secure neigbor discovery from NSS papers
3. Step 1 includes everything in the Niki’s paper
4. Title of the poster

**System model detail:**

Situation: nodes come, but server-side detection has already started or a single node want to join the system.

Nodes can do client-side detection whenever they want. After client-side detection, they can try to provide data to the system. However, this kind of data will be marked doubted and be partially accepted. However, nodes could choose to wait for several minutes and join the next round of process.

The system will record participation population at different time. Unusual abrupt in total number of registered nodes may be the reason of existence of large number of Sybil nodes.