Hunting Sybil paper question

Doubts:

**In section 4 we have the following information:**

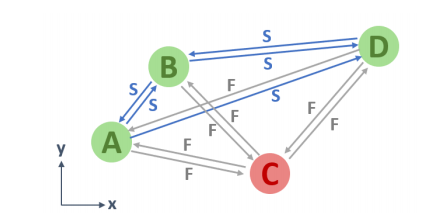
Definition: e\_i,j stands for Vi can see Vj

“Suppose that A did not see k8, and that C is a Sybil node that

could neither have seen any keys, nor could have any of its own

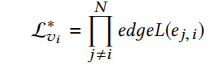
keys seen by others. This situation would have the Server produce

the following proximity graph shown in Fig. 3 below: ”

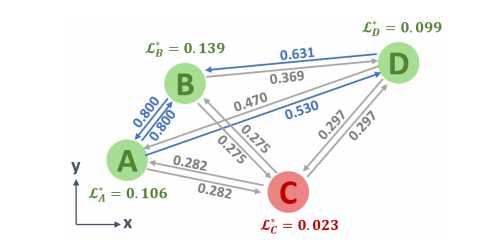


K8 is the signal broadcasted from D. We could see there is an ‘F’ on the gray line pointing from D to A. Which means A could not see D, and direction of such line is from D to A .

However in section 5, I’m confused by the deduction:

we are going to use this formula to calculate L\*vi respectively.

Here e\_j,i infers Vj can see Vi. We know from the previous graph that the arrow direction means “being seen by someone”.



Therefore, if we want to calculate L\*v value of node A, we should take 0.800, 0.530, and 0.282 as the parameter, which are outgoing lines of node A.

However, according to the paper, we should take incoming lines instead of outgoing ones.

This makes me confused.

Questions:

1. What if some benign nodes enter and quit the network frequently?
2. How can we get the distance between two nodes?
3. What would happen if malicious nodes help sybil nodes broadcast its secret key as soon as it enters the network?

This work is based on an assumption that a malicious node can impersonate one Sybil nodes.

The distance may be calculated from wifi signal strength.

~~If the laptop or PC are with the range of a proximity graph, then the attacker would no longer need a malicious node to impersonate for Sybil nodes. And by changing the wifi signal strength, the ‘distance’ of different emulators vary.~~

The exact location can be calculated with RSSI and triangulation.

The work is based on the assumption that a malicious node may not have enough time to impersonate several Sybil nodes. Otherwise it may not be able to validate its own presence.

However, with strong calculation ability, laptop of PCs can impersonate several Sybil nodes at the same round, letting Sybil infiltration successful.

Strengthen the assumption:

**Paper: An RSSI-based scheme for sybil attack detection in wireless sensor networks**

Based on ratio of RSSI, we could determine whether two nodes are at the same position.

Each round, two nearest listeners would be selected as Sybil detectors.

123 are three nodes broadcasting this round, ij are two nodes

|  |  |
| --- | --- |
| R\_1i | R\_1j |
| R\_2i | R\_2j |
| R\_3i | R\_3j |

Each column represents the RSSI value.



If we could found any two ratio value have the variance less than delta, then these two nodes are consider to be Sybils.

**Thought 1:**

The paper said only two nodes are sufficient.

To prevent both two nodes happen to be sybils, we ask all receiving nodes to update their RSSI.

Put all the nodes into three-node groups. Every group is in decreasing order of one ratio. With the help of dist(e\_ij), we could calculate the ratio of dist and validate the authenticity of RSSI ratio.

Since the sybil node doesn’t have the knowledge of other nodes location, it cannot spoof data according to the distance. Those spoofed data would not be validated.

(some problems here)

**Thought 2:**

All honest nodes are honest. Two sybils can report false positive( frame honest nodes). One sybil and one honest node can report false negative( whitewash sybil nodes).

Two nodes together report two sybils. Those two sybils would get -1 points

All groups’ results corresponding to these two sybils would be examined.

Turned out n groups would report these two sybils. Sybils would get -n points then.

The idea is that all honest groups would report sybils. But only few sybil groups report honest nodes. In the end, Sybil nodes would get minus points outweight honest nodes.

On the client side, each group report their own suspects.

(This idea might be still to extreme)

**Thought 3:**

Trade off: the more a sybil node exposes itself in the system, the higher ***l*** value would the node get, though detected by more honest nodes and being reported as sybils.