**Mick Zaatra – Peer Review**

1. Define wordings suggested; What are: “Nodes”, “Base Stations”, “RFiD”? Descriptions added
2. System seems to detect a jamming attack at a node by simple connection comparison to other nodes, if all nodes are blocked simultaneously or within a short period of one another and are all reading similarl PDR’s & RSS’s there wouldn’t be an effective comparison change between them to trigger the event that a jamming attack is taking place. Good point but we’re gonna ignore it for the sake of our test.
   1. There should be a definitive threshold for what a significant attack is. Ex. 50% packet loss would be the threshold that a jamming attack is present. Sometimes there could be packet losses that are less significant that don’t actually mean a jamming attack is present, for example if there is a 5% packet loss in transmission due to obstacles or signal strength. I actually did make changes according to this. Added a section to the Measurable success paragraph.
   2. Which also leads to saying that the packet loss percentage should scale accordingly with your received signal strength, because a lower signal strength should theoretically have a higher packet loss and shouldn’t be flagged as a jamming attack, but rather due to a signal strength issue. Stated in goal B already
   3. Having a way to also check that all nodes are experiencing same signal strength/packet loss before jamming tests, so that threshold packet losses aren’t falsely triggered as an attack and can be calibrated/zeroed. Would help to test in a controlled environment with little variables that impact signal strengths (ex. Wifi, Radio, Bluetooth, Cellular, ect).
3. Instead of Pass/Fail checkboxes, maybe add a packet loss number or percentage for different runs, and then evaluate if that packet loss is a pass or fail. We have PDR average boxes
4. Good Verification and Validation Notes & Goals Thanks

SOURCE:

Interference Test Plans

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Goals** | **Run 1** | **Run 2** | **Run 3** | **Run 4** | **Run 5** | **Did it succeed 3/5 times?** |
| A) Functional communication network is established between all 3 nodes (Raspberry Pis) and the base station (Linux computer) |  |  |  |  |  |  |
| B) Base station identifies jamming attack and sends an alert when network connectivity changes |  |  |  |  |  |  |
| C) Network transmission frequency is shifted to a designated value outside of the jammer’s range and communicate effectively |  |  |  |  |  |  |
| **Data Collection** |  |  |  |  |  |  |
| Average RSS |  |  |  |  |  | N/A |
| Average PDR |  |  |  |  |  | N/A |
| Attack Detection Speed  (mS) |  |  |  |  |  | Avg: |
| Countermeasure Deployment Speed (mS) |  |  |  |  |  | Avg: |

**Notes for verification and validation:**

1. **Goal A:** Nodes in the system are executed as Pi Boards equipped with Software Defined Radio (SDR) and Tx/Rx capabilities working in conjunction with a personal laptop operating a countermeasure software designated as the Base Station. Network connectivity will be verified by the transfer of Packet Delivery Ratio (PDR) and Received Signal Strength (RSS) between nodes.
2. **Goal B:** The countermeasures software that is executed at the Base Station will run procedural checks using RSS and PDR between nodes. In theory, during a jamming attack significant changes would be made to these values outside of expected changes due to movement or environmental factors. This significant change will be flagged at the base station for review. To emulate a jamming attack (because jamming is deemed illegal by FCC regulation) Radio-Frequency Identification (RFiD) bags will be used to prevent a node from further communications.
3. **Measurable Success:** The completion of goals A and B for all intents and purposes will deem this project to be a success. Again, due to FCC regulation, the scope of this project must be limited to detection and localization of the “attack” which will be emulated using RF blocking materials rather than a signal emitting jammer. The outcome of this project, though modified to work without proper research permits, in theory will predict results seen in real-world testing. One extra factor that we will be taking into effect is the natural interruptions that the signal may run into. There can be random interferences that can cause the PDR to change slightly and part of this project’s success relies on its ability to recognize that these minor interferences are not attacks and ignore them.
4. **Goal C (Optional):** This goal can still be accomplished in a modified sense, however the jammer (RFiD bag) would have to be physically removed from the attacked node to see the network’s ability to reconnect and communicate after the operational change. This goal is strictly here to provide additional insight to the plausibility of this countermeasure system if it were able to operate under FCC research guidelines. The base station will inform all nodes still in contact to operate at a new designated frequency, while the jammed node will change via pseudo-random sample once it realizes that it is no longer connected to the network. Once removing the RFiD bag the network should in theory be able to communicate effectively in the new operational range.