**Contiki Cooja Assignment 3**

**Network Attacks Their Detection And Mitigation**

Group Members:

Noman Anjum 17K-3755

Hassan Ahmed 17K-3654

Muhammad Ahsan 17K-3650

Submitted To : Sir Abdullah Zarshaid

Information System and Security

**Which resources gets effected after attack is held**

A DOS Or Flood Attack can keep nodes or the system busy in receiving and processing the malicious packets and in mean time useful packets and information can be lost due to buffer overflow or critical information can be expired due to time out. Due to DOS attack system or nodes remains busy replying to malicious client and its ram, storage and battery in case of sdn devices are consumed heavily, resulting system or nodes to shut down or stop entertaining other clients or nodes.

A sinkhole attack becomes a gateway to all devices in a system and attackers can use this attack to to sniff or masqueraded information being sent between nodes and controller. An integrity attack hence can cause extreme disturbance in the system.

**Any other or better way to Attacking network through selective forwarding attack.**

1) In DOS and Flood attack if we hide our identity, or just change id with id of other motes In network with certain interval, system will be unable to detect malicious mote and rather will remove normal motes.

2) Sink hole attack can be improved by sending values of hops and distance with certain threshold, rather than 0 so any rule base detection which detects with rule of 0 wont’ detect malicious mote.

**Any other or better way to Detect and mitigate against selective forwarding attacks**

1) Detection of Sinkhole checks the rssi and compares it with 0, however there is a chance that malicious mote sends hops or distance a small value other than zero,hence through analysis we can find some lower bound for motes distance.

2) Detection of Flood needs track of beacon packets send by a particular mote. A malicious node can alter this count to avoid detection. A better way to cope this is to get a new packet from all nodes which tells controller how many beacons they are receiving from each node, hence a malicious node could easily be detected by this functionality.

Above all, we can apply machine learning algorithms which are not rule based rather they learn the behavior of normal and malicious nodes, and if any suspicious activity is observed they will detect it in more efficient way, along with this AI can help system detect new attacks without inclusion of rules for every single new attack.

Mitigation in my opinion follows very straightforward algorithm and is working good.