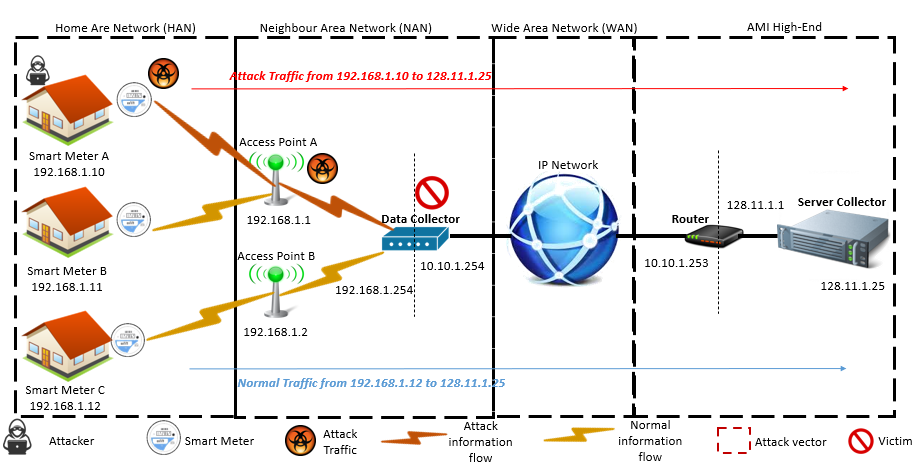
**ARP Spoofing Implementation in NetSim**

ARP spoofing (also known as ARP poisoning) is a type of cyber-attack where an attacker sends fake ARP messages onto a local network. The goal is to associate the attacker’s MAC address with the IP address of another device, effectively tricking other devices into sending traffic to the attacker instead of the intended recipient.

How ARP Spoofing Works:

1. Normal ARP Behaviour: Devices on a LAN use ARP to map IP addresses to MAC addresses.
2. Spoofing: The attacker sends forged ARP replies to the victim/gateway, associating the attacker’s MAC with the IP of the gateway or target.

Example case:



Here, Smart Meter A attempting False Data Injection Attack to falsify data from Smart Meter C to Server Collector.

To initiate this attack, Smart Meter A will have to poison Data Collector to spoof the IP address of Smart Meter C and send falsified traffic to Server Collector as Smart Meter C.

**Network Scenario:**

A diagram of a planet

AI-generated content may be incorrect.

**Source code changes:**

Source codes of ARP protocol is modified

* The attacker/malicious node (Smart Meter A) and the legitimate/attacked node (Smart Meter C) are defined in the GenerateArpRequest.c file of the ARP project.
* The attacker node sends falsified ARP packets mapping the attackers MAC address with IP address of Smart Meter C.

A screenshot of a computer program

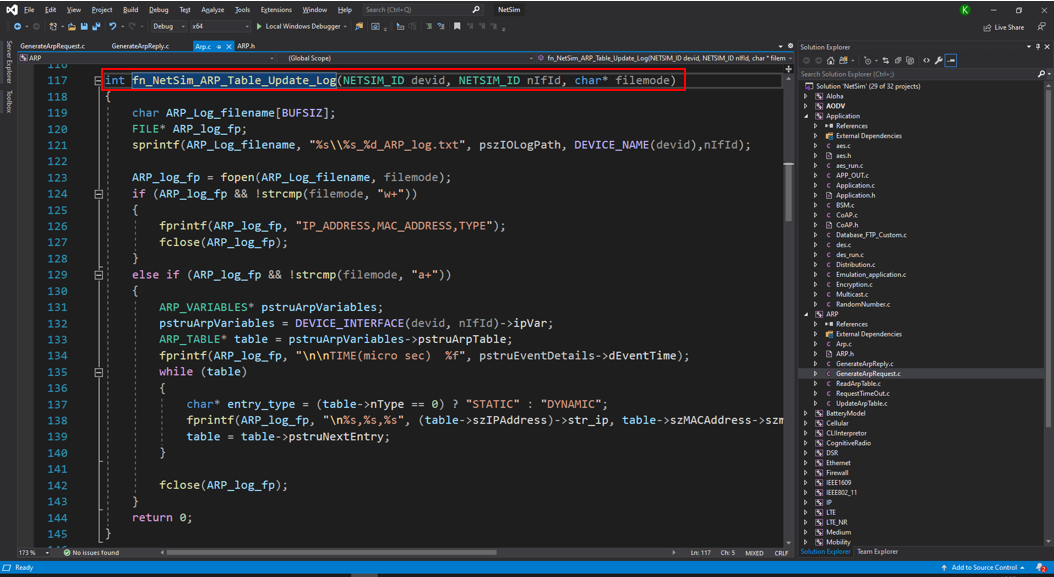
AI-generated content may be incorrect.

* Further, in the function fn\_NetSim\_Generate\_ARP\_Request() which is part of the GenerateArpRequest.c file, code has been added to include a false IP address in the ARP packet generated from the attacker/malicious node.

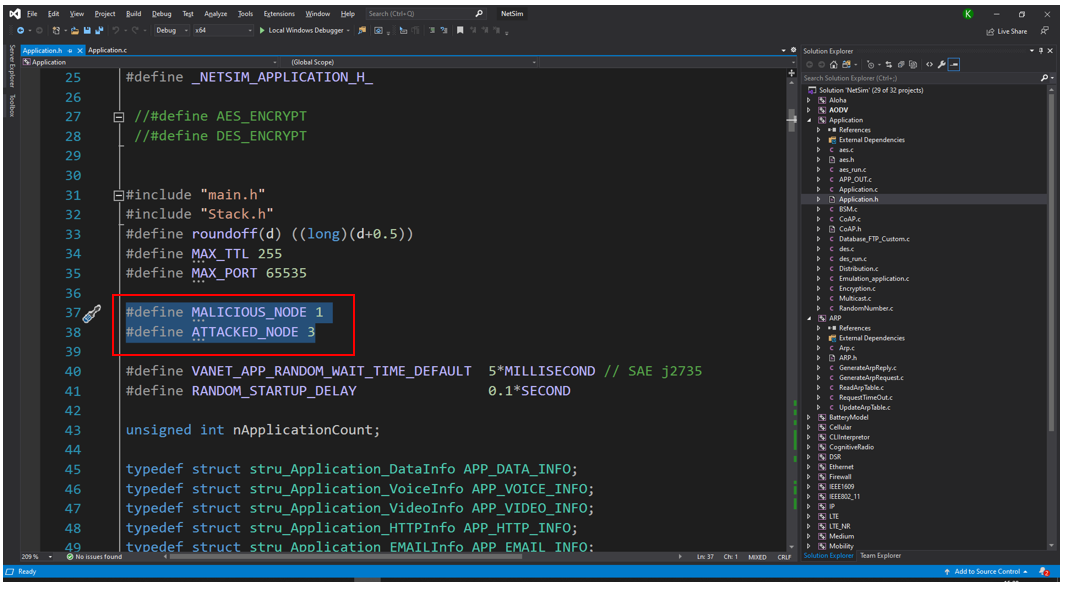
A screenshot of a computer program

AI-generated content may be incorrect.

* In the ARP.c file, an additional function fn\_NetSim\_ARP\_Table\_Update\_Log() has been added to generate ARP table logs for each node in the network that runs the ARP protocol. This function is called from various parts of the ARP protocol source code where ARP table updates occur.



* The source code of the Application project was modified to enable the attacker/malicious node to send spoofed data packets using the IP address of the legitimate/attacked node as the source IP address. The attacker/malicious node (Smart Meter A) and the legitimate/attacked node (Smart Meter C) are defined in the Application.h file of the Application project



* In the function fn\_NetSim\_Application\_StartDataAPP(), which is part of the Database\_FTP\_Custom.c file, code was added to include a false IP address in the data packet generated from the attacker/malicious node.

A screenshot of a computer program

AI-generated content may be incorrect.

* In the function fn\_NetSim\_Application\_StartDataAPP(), which generates the first packet of an application and is part of the Database\_FTP\_Custom.c file, code was added to include a false IP address in the data packet generated from the attacker/malicious node.
* Further, in the function fn\_NetSim\_Application\_GenerateNextPacket(), which generates subsequent packets of an application and is part of the Application.c file, similar code was added to include a false IP address in the data packets generated from the attacker/malicious node.

A screenshot of a computer program

AI-generated content may be incorrect.

**Network setting:**

* Enable packet trace prior to the simulation, by clicking on configure reports on top ribbon and disable the static ARP table by clicking on Options > Static ARP > Disable.
* Run the simulation for 10 seconds.

**Results:**

The screenshot below displays the NetSim packet trace with packets filtered to show Smart Meter A (the attacker node) as the transmitter. Both the ARP request and the data packets sent from the attacker node have a spoofed source IP address (192.169.0.2) instead of its actual IP address (192.169.0.3).

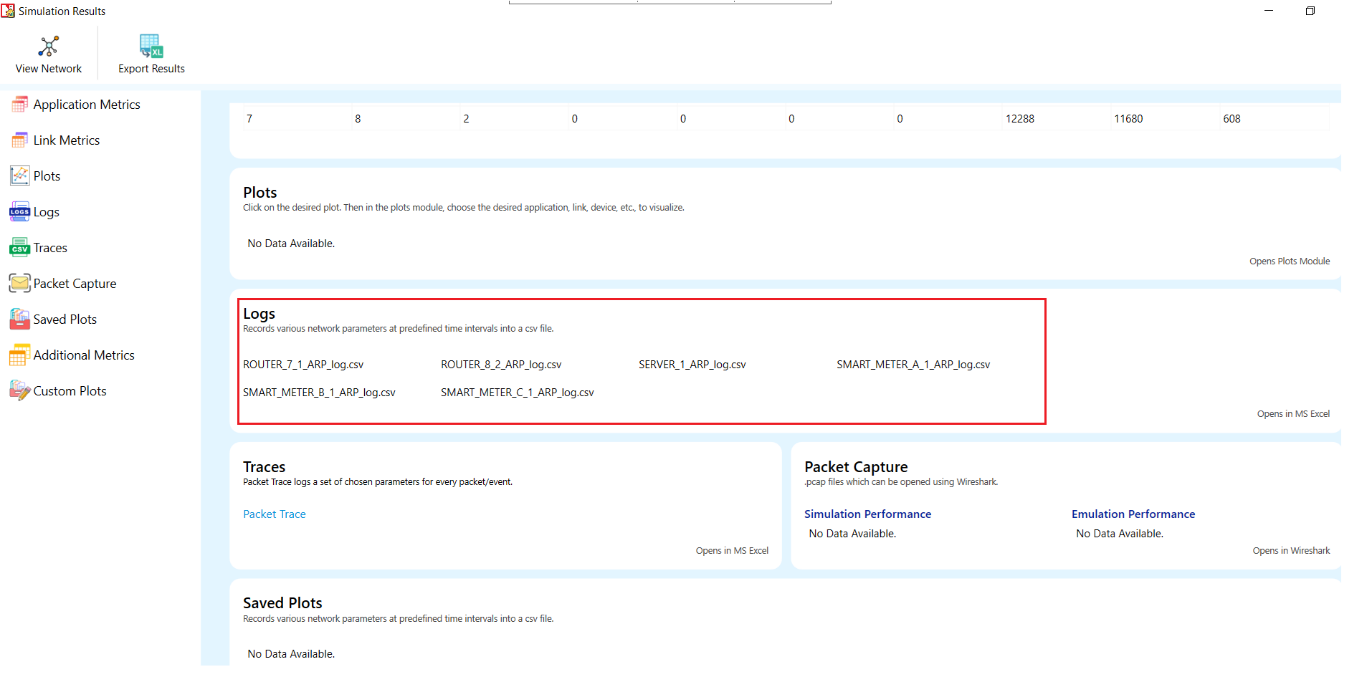
A screenshot of a computer

AI-generated content may be incorrect.

A diagram of a diagram

AI-generated content may be incorrect.

Additionally, ARP logs generated for each node can be accessed from simulation results window under logs. Each log file contains ARP table entries, including the IP-to-MAC address mappings and the type of each entry in the table.



A screenshot of a computer

AI-generated content may be incorrect.