DNP3, MMS : Issue Analysis

Modbus

Replay

▼ **Retransmission Flag**

TCP Protocol Retransmissions: A spurious retransmission happens when Wireshark detects a packet being re-sent by a system, but the original packet was likely received successfully by the destination. This can occur due to delays in acknowledgment (ACK) messages or network congestion.

Why Wireshark Flags It:

Wireshark flags packets as **"suspected retransmission"** when the sequence number of the packet matches that of a previously seen packet, and the acknowledgment for the first packet hasn't arrived within a certain window of time. This is normal TCP behavior, and Wireshark is helping you diagnose potential network performance or reliability issues.

▼ Tried Approach

attack from a different IP which seems master to the slave

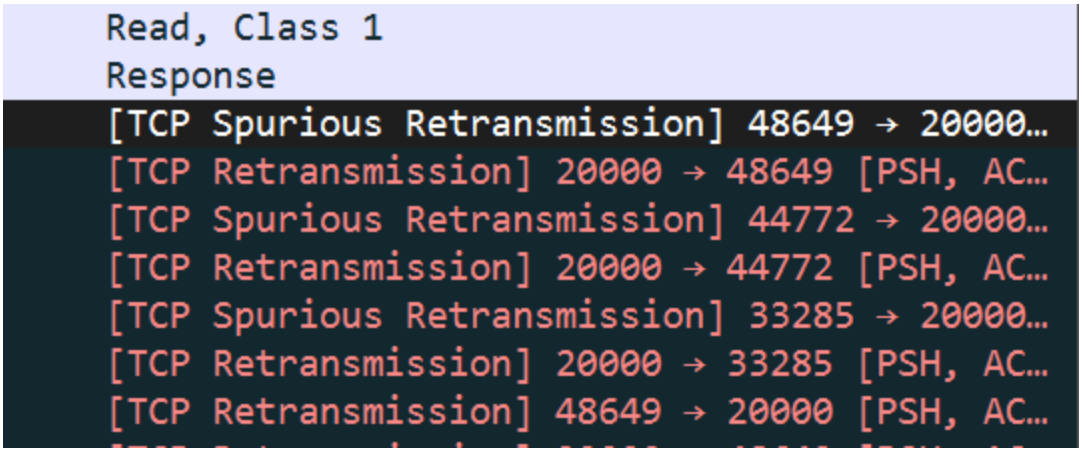
DOS

Approach

⇒ Attack the slave device from different IPs to exhaust it's resources

DNP3

Replay



The "suspected spurious retransmission" flag in the TCP analysis typically indicates that the packet Wireshark is seeing appears to be a retransmission of an earlier packet, but the retransmission might be unnecessary or unexpected based on the normal flow of the TCP conversation. This can happen for a few reasons:

Breakdown of Key Fields in the Frame:

- **Flags: 0x018 (PSH, ACK):**
  - The PSH flag tells the receiver to push the data to the application layer as soon as possible, while the ACK flag acknowledges the receipt of previous data.
- **Sequence Number: 70, Acknowledgment Number: 69:**
  - These numbers suggest the ongoing flow of data, with a sequence number that corresponds to the byte stream being transferred. A retransmission would typically have the same sequence number as the original packet.

- **Expert Info (Sequence): Suspected Spurious Retransmission:**
    - Wireshark flags this packet as a suspected spurious retransmission because it may have already seen the same data earlier in the conversation, but the packet is being retransmitted unexpectedly.

Short Summary :

TCP re-sends packets after a fixed RTO until it gets an ack flag, so when Wireshark sees and a same packet with same data it considers it a false retransmitted packet and flags it with a retransmission.

As all these protocols utilizes TCP i.e. Modbus/Tcp , DNP3 & MMS the same apply for them as well.