EE 418 Project Report

Members:
Simon Chen (1832768),
Kejin Li (1978130),
Andres Guerrero-Guzman (1066684),
Khoa Tran (1861460)

Contribution of Each Member:

Simon Chen:
- Management jobs: setting up communication, formatting all files
- Assisted with coding simulations

Kejin Li:
- Assisted with coding IDS
- Worked on additional questions

Andres Guerrero-Guzman:
- Implemented simulation_masquerade_attack and simulation_cloaking_attack

Khoa Tran:
- Assisted with IDS and simulations
- Worked on questions in 4.1

Additional Questions:

1. Briefly explain how the adversary chooses ΔT for the cloaking attack on the clock skew detector. In the cloaking attack, the adversary manipulates the message inter-transmission times of spoofed messages by adding delays to the clock to match the targeted clock skew detector to avoid detection.

   The inter-arrival time observed by R:

$$\hat{T}'' = \frac{\tilde{T}}{1 + S_A} = \frac{T + \Delta T}{1 + S_A}$$

   The transmitter's clock skew estimated by R:

$$\hat{S}'' = \frac{T - \hat{T}''}{\hat{T}''} = \frac{S_A \cdot T - \Delta T}{T + \Delta T}.$$

To pass the IDS, the adversary needs to choose ΔT such that Sˆ`` = Sˆ, or equivalently let Tˆ`` = Tˆ, which means:

$$\Delta T = \frac{(S_A - S_B)}{1 + S_B} \cdot T = S_{AB} \cdot T = \frac{-S_{BA}}{1 + S_{BA}} \cdot T,$$

2. What is the Maximum Slackness Index (MSI), and what does it measure? Based on Fig. 8 of [3], briefly comment on the performance of cloaking attack on an IDS in terms of MSI.

   The Maximum Slackness Index is used to quantify the effectiveness of an IDS in detecting masquerade attacks. Based on the fig, it can tell that it is easier for the cloaking attack to bypass the state-of-the-art IDS than the NTP-based IDS. On the CAN bus prototype n(attack) = 20 and e = 0.05, the MSI value for the state-of-the-art IDS is 22.5μs; the e-MSI value is 11.5μs for the NTP-based IDS. Moreover, the increase on n(attack) has a very small impact on MSI for the state-of-the-art IDS, but it has significant impacts on the MSI of the NTP-based IDS. Thus, in the real vehicle, as in the CAN prototype, the NTP-based IDS is more effective in detecting masquerade attacks than the state-of-the-art IDS.
3. Based on [2], explain under what circumstances, two messages are likely to be highly correlated. Based on the analysis in Section IV-C and Fig. 10 in [3], explain under what circumstances, two messages are likely to be highly correlated.

   Based on [2], If the two messages M1 and M2 are periodically sent by an ECU A, the correlation coefficient between their average clock offsets (derived per step) would show a high value close to 1, which means they are correlated since these messages originate from the same transmitter (instantaneous average clock offsets are likely equivalent). On the other hand, if the two messages were sent by different ECUs, they are uncorrelated. Based on Section IV-C and Fig. 10 in [3], Consecutive messages from the same ECU are highly correlated, while others are less correlated. However, not all pairs of messages from the same ECU have a high correlation, and such pairs and confirmed that their messages are always consecutively received.

4. Based on [3], describe how to launch the cloaking attack on the correlation detector, and briefly explain why it works.

   To launch the cloaking attack on the correlation detector: the attacker observes the targeted message over a period and identifies any sibling messages before the attack. Once the sibling messages are detected, the cloaking attack would be launched. The strong attacker-controlled ECU A begins transmitting the targeted message immediately after the sibling the message is completed. It will succeed because the transmission from ECU A begins once the sibling message transmission ends, the average offset of the targeted and sibling messages will be equivalent and show a high correlation. It also implies that their accumulated offsets, as well as estimated clock skews, will be equivalent, thus bypassing the clock skew detector at the same time to remain undetected.