Clock Skew-Based Intrusion Detection System in Controller Area Networks

Hunter North, Ethan Sepa, Logan Aikus

EE 418: Network Security and Cryptography

Due: December 10, 2021

Task Questions

1. **Compare the slopes of the curves from Tasks 2 and 3, and comment on the similarity of the three messages in terms of estimated clock skew from the perspective of the IDS.**

   The clock skew of each ECU is calculated as the slope of each message in Fig 1 and 2. Note that for calculating the slopes, we are using the endpoints.

Message	State-Of-The-Art (N = 20)	NTP (N = 20)
184	$\frac{0.7*10^{-6} sec}{12000\, sec} * 10^{6} = 5.8 * 10^{5} ppm$	$\frac{0.24*10^{-6} sec}{12000\, sec} * 10^{6} = 2 * 10^{5} ppm$
3d1	$\frac{0.52*10^{-6} sec}{12000\, sec} * 10^{6} = 4.3 * 10^{5} ppm$	$\frac{0.02*10^{-6} sec}{12000\, sec} * 10^{6} = 2 * 10^{6} ppm$
180	$\frac{0.63*10^{-6} sec}{12000\, sec} * 10^{6} = 5.3 * 10^{5} ppm$	$\frac{0.2*10^{-6} sec}{12000\, sec} * 10^{6} = 1.7 * 10^{5} ppm$

   The State-Of-The-Art IDS observes the clock skew of the different ECUs to be larger than what the NTP IDS observes. However, the relationship between each message's clock skew is maintained (in both forms of the IDS: 184 is the largest, then 180, and then 3d1 is the smallest). Additionally, it is important to note that the physical value of the estimated clock skew value isn't the deciding factor in recognizing an attack. Instead, it is the sudden change in that value, so the differing clock skew values (between the State-of-The-Art and NTP systems) are okay.

2. **Comparing the four figures from Tasks 2 through 3, comment on the consistency of clock skew estimation (i.e, the slope of the curve for the same message should be the same regardless of N) for the state-of-the-art and the NTP-based IDSs.**

   We are able to observe that the NTP based IDS is less sensitive to different batch sizes and therefore provides more consistent clock skew estimations. For example, in the estimated skew of message 184 in the state-of-the-art IDS, we see that the estimated clock skew drops from 5.8*10^6 ppm to 2.3*10^6 ppm when we adjust the batch size from 20 to 30. Alternatively, the NTP based IDS returns almost an identical estimated clock skew for message 184 of 2*10^5 ppm when the batch size changes by the same amount (20 to 30).

3. **Which IDS can detect the masquerade attack? Why?**

   The NTP IDS can detect the masquerade attack. An IDS determines if there is an attack by comparing the control limits (L^+ and L^-) to the detection threshold (Γ). If either control limit exceeds the detection threshold the IDS declares an intrusion. Our Γ is set at 5, so we determine there is an attack if L^+ or L^- is greater than 5. Looking at Fig. 5 (State of the Art IDS) we see that both the upper and lower control limit are 0 for the entire time span, so State of the Art IDS does not detect the masquerade attack. Looking at Fig. 6 (NTP IDS) we see that while the lower limit stays constant at 0, our upper limit increases exponentially and surpasses the detection threshold value of 5. For this reason, the NTP IDS detects the masquerade attack.

4. **Which IDS can detect the cloaking attack? Why?**

   Neither IDS can detect the cloaking attack. An IDS determines if there is an attack by comparing the control limits (L^+ and L^-) to the detection threshold (Γ). If either control limit exceeds the detection threshold the IDS declares an intrusion. Our Γ is set at 5, so we determine there is an attack if L^+ or L^- is greater than 5. Looking at Fig. 5 (State of the Art IDS) we see that both the upper and lower control limit are 0 for the entire time span, so the State of the Art IDS does not detect the cloaking attack. Looking at Fig. 6 (NTP IDS) we see that while the upper limit stays constant at 0, our lower limit spikes twice to approximately the values of 0.5 and 0.7. Both of these spikes are below the threshold value of 5, so the NTP IDS does not detect the cloaking attack. Although we do not detect the cloaking attack in this instance, if the spikes were greater it would be possible for an NTP IDS to determine the cloaking attack.

5. **Comparing masquerade and cloaking attacks, comment on the limitations of a clock-skew based IDS.**

   The limitations of clock-skew based IDS is that they can be mimicked by an attacker and are not very secure, especially compared to something such as a fingerprint which is hard to mimic and is very secure. From the previous two questions we determined that only a quarter of the attacks were caught by a clock-skew based IDS, which was the masquerade attack on the NTP IDS. From both the masquerade and cloaking attacks we can clearly see the flaws in the clock-skew based IDS security as the data can be fully compromised without the IDS detecting an attack.

Additional Questions

1. **Briefly explain how the adversary chooses delta(T) for the cloaking attack on the clock skew detector.**

   An IDS is going to estimate the clock skew of a “safe” or “legitimate” transmitting ECU and constantly be on an alert for a sudden change in the ECU’s estimated clock skew. If the ECU’s slew is quickly changed, it is a sign that said ECU has become compromised or an adversary is trying to mimic it. This shift in skew occurs because the adversary begins transmitting messages at a different frequency relative to the original ECU.

   Unfortunately, it is possible for an adversary to cloak their clock skew so that it matches the original ECU. This is done through the following steps:

   a. The adversary begins by compromising two different ECUs and delegating one to be a strong attacker and the other to be the weak attacker.

   b. The strong attacker will estimate the period of the target message through its local clock. This period is calculated in such a way that the IDS will be unable to notice a difference in the clock skew of the hijacked ECU.

      i. $T_{adv,\, transmit} = T + \Delta T$

      ii. $T_{adv,\, inter-arrival} = \frac{T_{transmit}}{1+S_a} = \frac{T + \Delta T}{1+S_a}$

      iii. $S_{adv,\, transmit} = \frac{T_{transmit} - T_{inter-arrival}}{T_{inter-arrival}} = \frac{S_a * T - \Delta T}{T + \Delta T}$

      iv. Adversary must now choose a ΔT such that $S_{adv,\, transmit} = S_{orig,\, measured}$ which also means that $T_{adv,\, inter-arrival} = T_{orig,\, inter-arrival}$

      v. $\Delta T = T * \frac{S_A - S_B}{1 + S_B} = S_{AB} * T = T * \frac{-S_{BA}}{1 + S_{BA}}$

      vi. Combining ΔT calculated in step v into step i, we can then determine the final transmission period for the adversary’s hijacked ECU

      vii. $T_{adv,\, transmit} = T + \Delta T = T + T * \frac{-S_{BA}}{1 + S_{BA}}$

   c. The strong attacker will then transmit its own messages at a rate equivalent to $T_{adv,\, transmit}$(calculated in previous step) to produce a clock skew that is very similar to the uncompromised ECU -- which therefore hides the attack from the IDS.

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

   The Maximum Slack Index is a term used to quantify the effectiveness of an IDS in detecting masquerade attacks. This calculation of this term comes from the amount of variance in transmission time that can be attributed to random delays and quantization errors occurring in our IDS. For example, if our IDS is normally experiencing a large amount of random delays in safe transmissions, then our clock skew will have lots of variance, and we will want to avoid flagging these transmissions as dangerous. As this variance increases, we give our adversary a wider range of acceptable clock skews to produce without being caught.

   Looking at Fig. 8 of [3], we see that the width of the plots in each graph corresponds to the Maximum Slack Index of the given detector. In the charts with greater width, there is a much larger range of added delay values that the adversary can utilize to have a successful attack probability of nearly 100%. So, we can summarize the chart by stating that minimizing our MSI will decrease the probability that an added delay value will produce an undetected attack.

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.**

   In order for messages to be considered highly correlated, the correlation coefficient (ρ) must be greater than 0.8. Messages that come from the same transmitter are likely to show some sort of repetition and have equivalent instantaneous average clock offsets [2]. This would lead to a ρ close to 1 and make said messages highly correlated. Also, messages that are received with a constant delay between them will generally be highly correlated according to Section IV-C in [3]. This is shown by the data in Fig. 10 in [3] as all of the highly correlated messages are from the same transmitter and are consecutively received. In the case of a cloaking attack, the strong attacker-controlled ECU begins transmitting the targeted message as soon as the sibling message is completed. This leads to the average offset of the targeted and sibling messages being equivalent and therefore having high correlation [3].

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

In order to effectively launch a successful cloaking attack on the correlation detector, it is important to understand different transmission scenarios and how an IDS would interpret the correlation between incoming transmissions (originating from the same ECU) $v_{k,i}$ and $w_{k,i}$ occurring at $t^{(v)}_{k,i}$ and $t^{(w)}_{k,i}$

Scenario One:

a. $w_{k,i}$ is transmitted directly after $v_{k,i}$ with no interfering arbitration.

   i. $a^{(w)}_{k,i} = a^{(v)}_{k,i} + \Delta t + (d_w - d_v)$

      1. Where $d_w$and d_v are are constant network delays

   ii. $t^{(w)}_{k,i}$=$t^{(v)}_{k,i} + \Delta T$

b. Calculating estimated average offsets:

   i. $O^{(v)}_{avg}[k] = T - \frac{1}{N}(a^{(v)}_{k,N} - a^{(v)}_{k,o}) = -O^{(v)} - \frac{1}{N}(\epsilon^{(v)}_{k,N} - \epsilon^{(v)}_{k,o})$

   ii. $O^{(w)}_{avg}[k] = T - \frac{1}{N}(a^{(w)}_{k,N} - a^{(w)}_{k,o})$

   iii. However, $O^{(v)}_{avg}[k]$ and $O^{(w)}_{avg}[k]$ are the k-th instance of random variables $O^{(v)}_{avg}$ and $O^{(w)}_{avg}$ which implies for equation 2 that:

   iv. $O^{(v)}_{avg}[k] = O^{(v)}_{avg}[k]$

c. Since $O^{(v)}_{avg}[k] = O^{(v)}_{avg}[k]$ the correlation between the two messages is said to be 1

Scenario Two:

a. $w_{k,i}$ is transmitted directly after $v_{k,i}$ with interfering arbitration (with a delay greater than zero marked by $d_{k,i}$) in between.

b. Accounting for arbitration:

   i. $a^{(w)}_{k,i} = a^{(v)}_{k,i} + \Delta t + (d_w - d_v) + d_{k,i}$

c. The relationship between $O^{(v)}_{avg}[k]$ and $O^{(w)}_{avg}[k]$ now becomes:

   i. $O^{(w)}_{avg}[k] = O^{(v)}_{avg}[k] - \frac{1}{N}(d_{k,N} - d_{k,0})$

d. Note that the second term is the k-th realization of a random variable, so the equation from part c becomes:

   i. $O^{(w)}_{avg}[k] = O^{(v)}_{avg}[k] + D$

e. The correlation between these two values is:

   i. $\rho(O^{(v)}_{avg}, O^{(w)}_{avg}) = \frac{\sqrt{Var(O^{(v)}_{avg})}}{\sqrt{Var(O^{(v)}_{avg}) + Var(D)}} \prec 1$

f. Therefore, the correlation in this scenario is less than one

Scenario Three:

a. The two messages are now arriving from two unique ECUs so that

   i. $O^{(w)}_{avg}[k] =- O^{(w)} - \frac{1}{N}(\epsilon^{(w)}_{k,N} - \epsilon^{(w)}_{k,0})$

   ii. $O^{(v)}_{avg}[k] =- O^{(v)} - \frac{1}{N}(\epsilon^{(v)}_{k,N} - \epsilon^{(v)}_{k,0})$

b. However in this instance $\epsilon^{(v)}_{k,i}$ and $\epsilon^{(w)}_{k,i}$ are completely independent so that the correlation between $O^{(w)}_{avg}[k]$ and $O^{(v)}_{avg}[k]$ is zero

If an adversary is observing a set of transmissions taking place around the target ECU they can group the relationships between our target ECUs into each of the scenarios described above. If said relationship falls into scenario two or three (low correlation), the adversary doesn't need to worry about triggering the correlation detector with their message. However, if scenario one is identified, the spoofed message will need to maintain proper correlation with its sibling message. This is executed by simply waiting for the sibling message to be completed and then immediately sending the spoofed message. This technique will maintain the average offset of the spoofed and siblining messages will be equivalent and maintain high correlation (thus, thwarting the correlation detector).

Figures

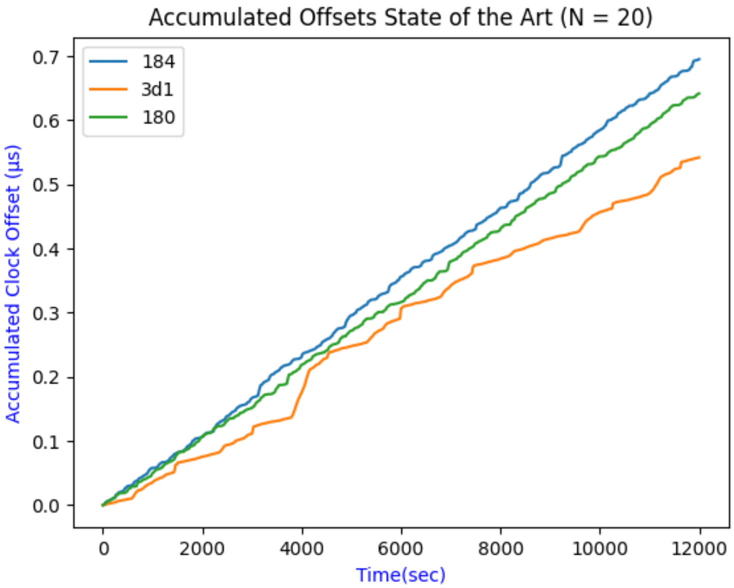

Fig.1. (Task 2) Plot of the Accumulated Offsets for the State of the Art IDS when N = 20.

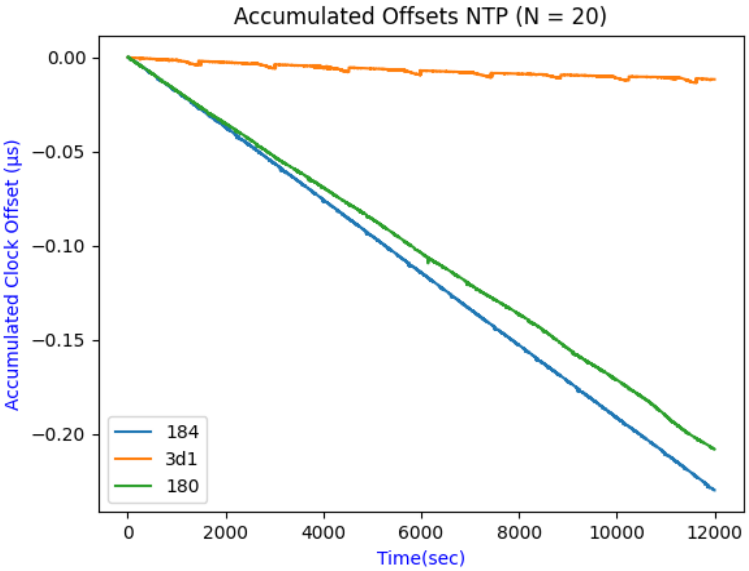

Fig.2. (Task 3) Plot of the Accumulated Offsets for the NTP IDS when N = 20.

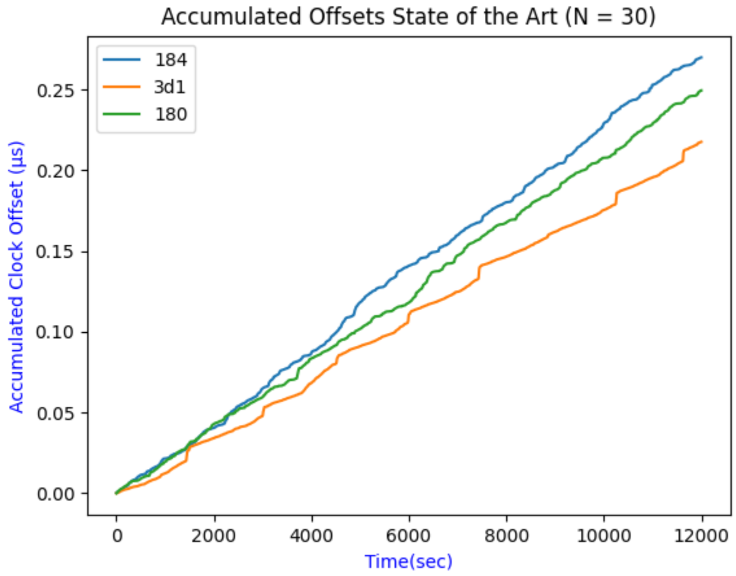

Fig.3. (Task 4) Plot of the Accumulated Offsets for the State of the Art IDS when N = 30.

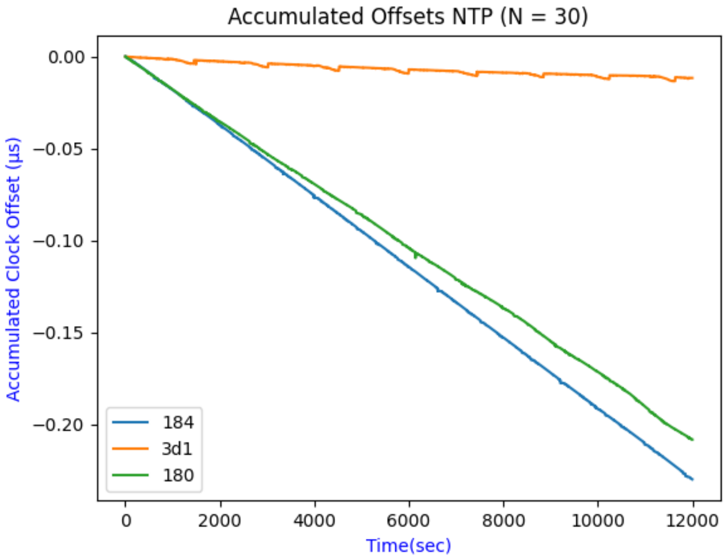

Fig.4. (Task 4) Plot of the Accumulated Offsets for the NTP IDS when N = 30.

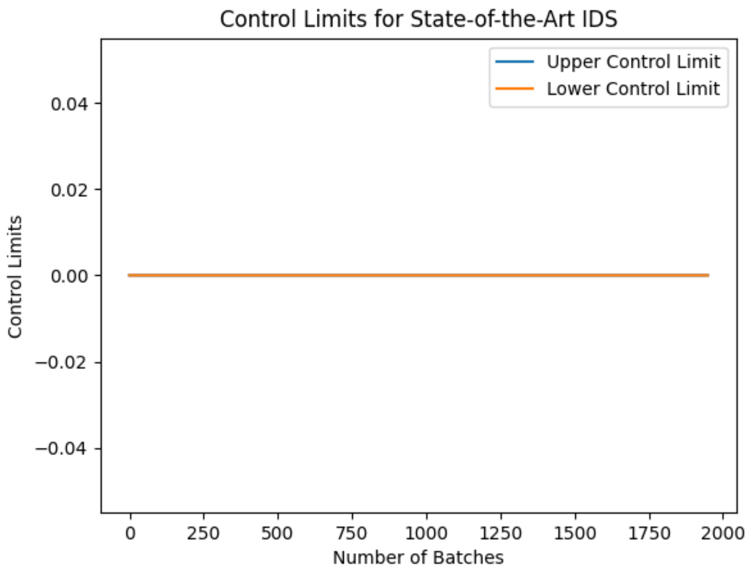

Fig.5. (Task 5) Plot of the Control Limits for the State of the Art IDS during a Masquerade Attack.

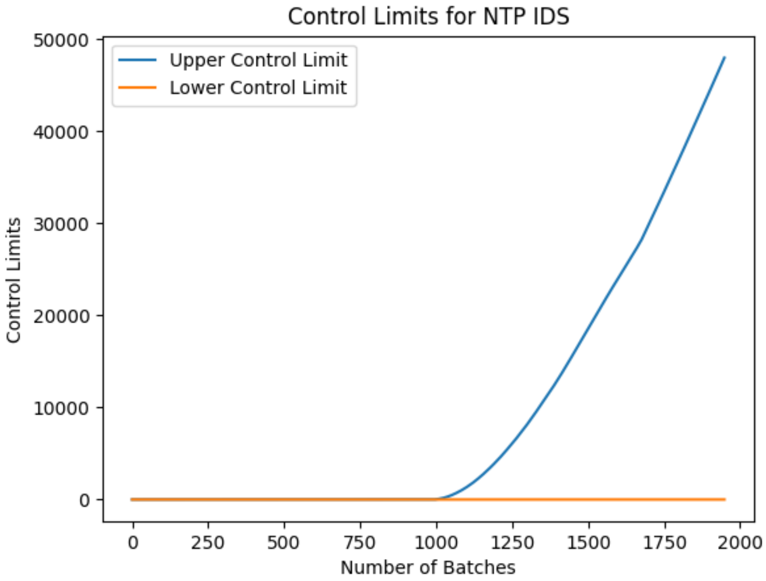

Fig.6. (Task 5) Plot of the Control Limits for the NTP IDS during a Masquerade Attack.

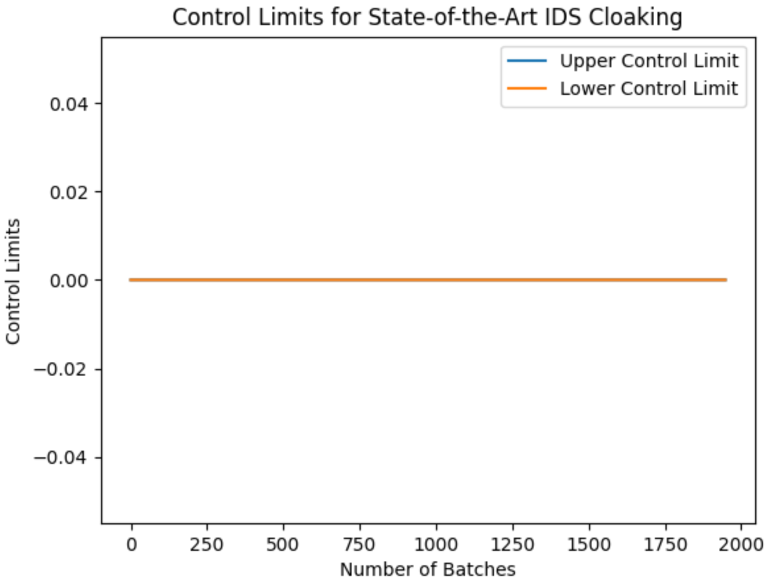

Fig.7. (Task 6) Plot of the Control Limits for the State of the Art IDS during a Cloaking Attack.

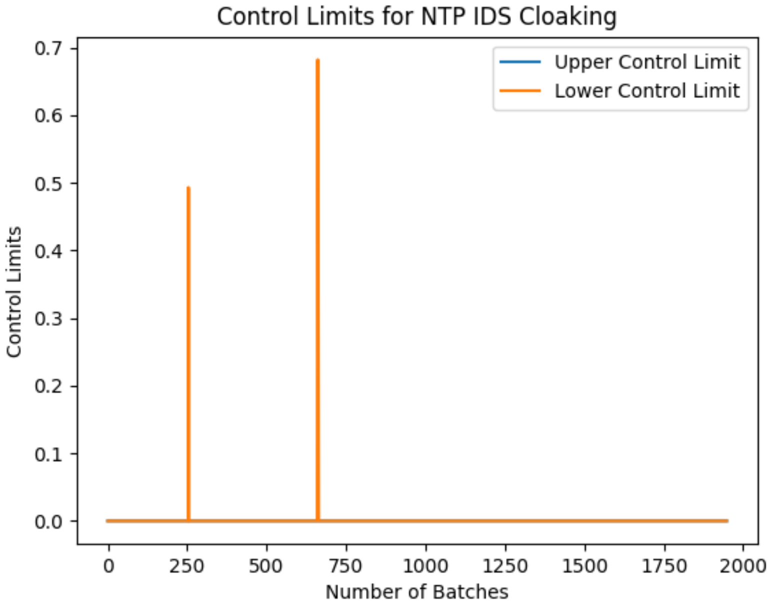

Fig.8. (Task 6) Plot of the Control Limits for the NTP IDS during a Cloaking Attack.