Detecting and Mitigating Spoofing Attack against an Automotive Radar

Prateek Kapoor, Ankur Vora, Kyoung-Don Kang
State University of New York at Binghamton, NY, USA.
{pkapoor2, avora4, kang}@binghamton.edu

***Abstract*— Applying cyber security mechanisms, such as cryptography, trusted computing, and network intrusion detection, is insufficient to secure cyber-physical systems (CPS) such as smart vehicles, because most sensors (and actuators) are designed without security considerations and remain vulnerable to sensor spoofing attacks in the analog domain. To address this problem, we present a new approach to detect and handle sensor spoofing attack against automotive radars—a key component for assisted and autonomous driving—by extending multiple beamforming in an automotive multi-input multi-output (MIMO) radar. In a simulation study for adaptive cruise control based on the car following model, our approach significantly outperforms three state-of-the-art baselines in terms of attack detection and ranging accuracy.**

I. Introduction

Cyber-physical systems (CPS) integrate computing, communication, and control to enhance the safety, convenience, and quality of life in important applications, such as smart automotive, energy, and health care systems. Unfortunately, securing CPS is very challenging. A variety of approaches have been explored to enhance the security of CPS [1], [2], [3], [4], [5], [6], [7]; however, just leveraging cyber security mechanisms, e.g., cryptography, trusted computing, and intrusion detection, is largely insufficient. Notably, most sensors and actuators consisting CPS are not designed considering security and, therefore, remain highly vulnerable. For example, a self-driving car based on Lidar has recently been compromised by a remote attack that simply generated more echoes of objects and cars [8]. Sensor spoofing in the physical analog domain is a serious threat in autonomous and driver-assisted vehicles envisioned to transform transportation and other CPS.

Broadly, there are two types of sensors: passive and active. Passive sensors, e.g., temperature and humidity sensors, sense pre-existing physical signals. Passive sensors are listening devices that naively relay the signal/data to the upper-layer software without checking the integrity, although they can reduce noise via filtering and post-processing [9]. In contrast, active sensors, e.g., a radar or Lidar, actively probe the surroundings by emitting a self-generated signal to evoke a physical response, e.g., a reflected signal, from some measured entity, such as cars on the road. They can be used to enhance the security of CPS. A novel approach, called physical challenge-response authentication (PyCRA) [9], challenges the surroundings via randomized probing in the time domain. In principle, it turns off the active sensing signal at random times, called challenge periods. PyCRA assumes that an attacker cannot detect a challenge immediately due to its hardware and signal processing latency. Given that, PyCRA detects an attack signal that continues to be higher than a noise threshold during a challenge period using the Chi square method. In this way, it effectively detects physical attack in the analog domain for magnetic sensors and RFID tags. However, PyCRA has a drawback in safety-critical systems with high availability requirements. For example, an automotive radar used for safety-critical applications, e.g., adaptive cruise control and collision warning, should be turned off at random times to detect possible attack. As a result, the availability of the radar system can be decreased, potentially affecting the safety.

A recent work by Dutta et al. [10] attempts to address this issue in the automotive radar system. The authors use the same method as PyCRA to detect spoofing attack by turning the radar off at random times. In addition, during a challenge period, they apply the recursive least square (RLS) method to provide the estimated distance to (or relative velocity of) the lead vehicle by minimizing the sum of the squared errors, which is defined as the difference between the predicted distance to the lead vehicle and the radar measurement under attack. A key challenge of this approach not addressed in [10] is that the ground truth, e.g., the actual distance to the lead vehicle, is unknown during the attack period. Performing regression based on the difference between the predicted distance and the radar measurement compromised under attack can result in large errors, raising safety concerns.

To address the problem, in this paper, we propose a new approach, called **spatio-temporal challenge-response (STCR)**, to detect and thwart sensor spoofing attack against an automotive radar system by effectively verifying physical signals in the analog domain. The key idea behind our approach is, via simultaneous multiple beamforming, for the automotive MIMO radar to send synchronized narrow beams to several directions randomly selected out of a larger number of the total directions available in the MIMO antenna array each time when the radar system probes the surroundings. In this way, STCR detects the direction of attack with high confidence when a reflected signal exceeding the noise threshold arrives from an un-probed angle. Notably, STCR is significantly different from PyCRA [9] and Dutta et al. [10] in that it never turns the radar off to maintain the availability. Neither does it apply a learning algorithm, e.g., RLS, based on distance measurements potentially inaccurate under attack. Instead, probing directions are randomly selected at different challenge periods in time to detect any attack from different directions previously unexplored or

978-1-5386-6358-5/18/$31.00 ©2018 IEEE

attack from a moving attacker. Essentially, our approach physically challenges the environment in the spatial and temporal domains to **enhance the security of automotive radars with no downtime or mis-learning**. By filtering signals with suspicious angles of arrival, our approach supports highly accurate distance (and velocity) estimates even under spoofing attack. Thus, STCR supports **not only attack detection but also resilience**.

For performance evaluation, a simulation study for adaptive cruise control based on the car following model is undertaken in Matlab [11]. Specifically, we thoroughly compare the attack detection latency and distance estimation accuracy of the vanilla state-of-the-art radar system with no spoofing attack detection/mitigation mechanism, PyCRA [9], Dutta et al. [10] and our approach. Clearly, the vanilla system fails to detect or eliminate any attack signal. The distance error, i.e., the difference between the actual and calculated distance, is near zero in STCR. However, the largest distance error in PyCRA and [10] is approximately 35m and 40m, respectively.

The key contributions of this paper are summarized below:

- We show that PyCRA [9] and Dutta et al. [10] have serious security vulnerabilities in the context of automotive radar systems.[1]
- We propose a new spatio-temporal challenge-response scheme, STCR, to significantly enhance security and accuracy of distance calculation in automotive radars under attack. Especially, STCR both detects and quickly thwarts distance attack that intends to falsely increase or decrease the distance from a host car to the lead vehicle. The key features of STCR are essential to avoid a traffic incident, e.g., a traffic jam or accident, due to attack.
- The accuracy and robustness of distance estimation to the lead vehicle provided by the vanilla radar system, PyCRA [9], Dutta et al. [10] and STCR are thoroughly evaluated and compared with each other using the car-following model and adaptive cruise control (ACC) package in Matlab.

The remainder of this paper is organized as follows. Section II gives background for the automotive MIMO radar and car-following model, while demonstrating the limitations of [9], [10] via simulation to motivate our work. In Section III, the proposed method, STCR, is described. In Section IV, the performance of the proposed approach is thoroughly evaluated in comparisons to the vanilla system and advanced methods [9], [10]. Finally, Section V concludes the paper.

II. Background and Motivation

In this section, background information regarding automotive radars and the car-following model is given. The threat model is described to specify the scope of our work for enhancing the security of automotive radars presented in this paper. Further, important limitations of representative approaches are discussed.

A. Automotive MIMO Radar

In this paper, we adopt a state-of-the-art MIMO frequency-modulated continuous wave (FMCW) radar system such as [12], because a 12 element MIMO FMCW arrays can offer performance equivalent to that provided by 32 phase array elements. 77GHz MIMO FMCW radars provide effective spectral reuse important to detect and track a large number of cars on the road at the same time. Also, a MIMO FMCW radar offers other advantages compared to a phase array antenna, e.g., lower energy consumption, higher angular resolution, faster scanning time, narrower beams, and simultaneous search and track. Thus, MIMO array radars are more suitable for numerous automotive applications, such as cruise control, speed control, collision detection, pedestrian/object detection, and parking aid [13].

To operate over a wide angular area, a radar system needs either mechanical or electrical scanning. The effectiveness of conventional analog scanning is limited, while mechanical scanning is unacceptable for most personal or commercial automotive systems. An effective solution is **digital beamforming** (DBF) [14]. Via DBF, multiple narrow beams can be generated to detect and track multiple targets. In principle, a MIMO FMCW radar system uniformly excites a linear antenna array to transmit multiple narrow beams in such a way that the received power of different targets is equalized [12]. Each receive antenna element down-converts the received multiple signals, performs A/D conversion, and stores them in memory. They are then processed in parallel for the entire coverage of the MIMO antenna elements via phase shifting and weighted amplitude conversion/correlation. In this paper, we leverage DBF to generate multiple narrow beams in different directions selected randomly within a specified range for STCR when the radar transmits a set of narrow directional beams to detect any spoofing attack as well as the distance to the vehicles in the same lane in a synchronized manner.

B. Car Following Model

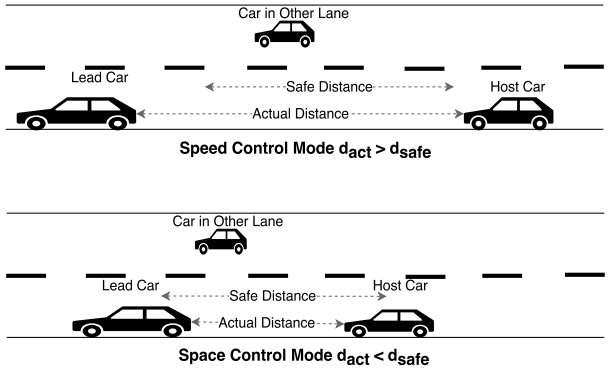


Fig. 1: Car Following Model

[1]One may argue that PyCRA is not designed for securing automotive radar systems. Although the claim is true, the basic design objective of PyCRA in a broader sense is to enhance the security of active sensors that emit signals to measure the environment. Therefore, comparing PyCRA to STCR is essential.

In this paper, we use car-following model provided by the adaptive cruise control (ACC) package of Matlab [11] as shown in Figure 1. The car-following model provides an optimal control of distance d, velocity v and acceleration a between the host and lead car over time t. To ensure safe driving of the host car, ACC optimizes the speed and space based on the actual distance d_{act} and safe distance d_{safe} to the lead car. As illustrated in Figure 1, ACC optimizes the speed if $d_{act} \geq d_{safe}$ and spacing if $d_{act} < d_{safe}$ by controlling the acceleration of the host car. Also, the ACC package is equipped with an FMCW antenna array for object detection and ranging. It supports multiple beamforming using the frequency division multiple transmitter-beamforming (FDMB) technique [15]. We have extended the FMCW antenna array scheme to support STCR.

C. Threat Model

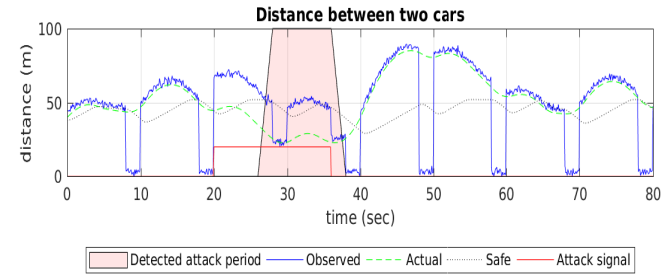
For security research, a threat model is required to define the scope of the work, because perfect security is nearly impossible. Our threat model considered in this paper is summarized as follows:

- We assume that the cyber component of an automotive system is secured via, for example, cryptography, network intrusion detection, and trusted computing. Thus, we focus on physical radar spoofing attack in the analog domain.
- We do not consider jamming attacks since modern radars are designed to minimize the impact of jamming. Also, jamming is relatively easy to detect. Thus, we focus on spoofing attack that is non-intrusive and stealthier.
- We assume that an attacker is in the same lane. Especially, we assume that a lead vehicle can spoof the radar system of the following car to deceive the distance (or velocity) and affect traffic flow or safety as a result. A signal from a different lane is detectable due to the wider angle of arrival. Further, spoofing attack from a different lane can be detected by the same STCR principle. A thorough investigation is reserved for future work.

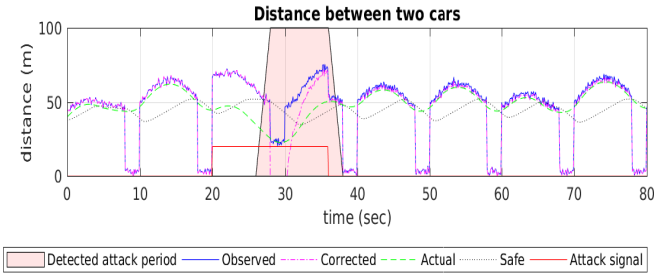
D. Limitations of Existing Approaches

In this subsection, we model a spoofing attack, in which the lead vehicle transmits a signal to the following vehicle to make it believe that it is farther away than it actually is from the lead vehicle, to demonstrate limitations of PyCRA [9] and [10]. Figure 2 plots the simulation results in Matlab in terms of the accuracy of ranging under spoofing attack launched between 20s–36s (the red rectangle in Figure 2). As shown in the figure, PyCRA and [10] keep the radar on for 8s and turns it off for 2s, and repeats this pattern for high availability of the radar system.

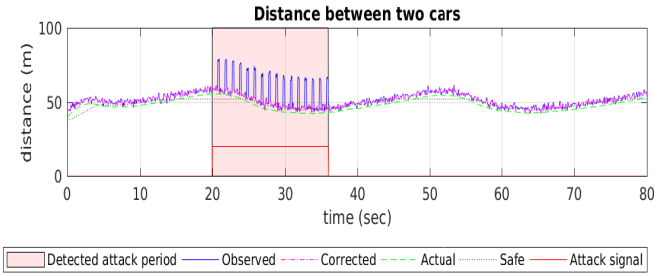
As shown in Figure 2a, PyCRA detects the attack in the challenge period undertaken between 28s–30s, since the attack is still on-going during the challenge period. It also cancels the attack signal and derives accurate distance measurement; that is, the actual distance (green curve) and



(a) PyCRA [9]



(b) Dutta et al. [10]



(c) STCR

Fig. 2: Impact of Radar Spoofing Attack (Short-Term Attack)

measured distance (blue curve) are nearly identical in the challenge period. However, when the challenge period is over, it cannot detect attack and filter the attack signal out. Thus, when the attack is launched between 20s–36s, except for the challenge period between 28s–30s, the actual distance is continuously shorter than the measured distance. It is shorter than the safe distance (black curve) by up to approximately 20m (meters). Further, the distance measurement becomes zero in the challenge periods when there is no attack as shown in Figure 2a despite the relatively infrequent challenge-response for high availability of the radar system.

Dutta et al. [10] attempts to support distance estimation when an attack is detected via a physical challenge-response scheme of PyCRA. Using the recursive least square (RLS) method, it provides distance estimates when attack is detected. In Figure 2b, however, the distance estimate (magenta curve) converges to the measured distance affected by the attack, since it performs regression based on the difference between the predicted distance via RLS and the radar's distance measurement compromised under spoofing attack without knowing the ground truth, i.e., the actual distance,

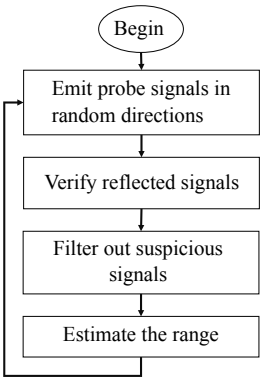


Fig. 3: Flowchart of STCR

as discussed in Section I.

In contrast, STCR has important advantages. First, both the radar system and STCR scheme are never turned off and always available. Thus, it detects attack during the entire attack period between 20s–36s with virtually no latency. On the other hand, PyCRA and [10] can detect attack only in a challenge period. Attack cannot be detected until the next challenge period. In addition, the corrected distance (magenta curve) is almost identical to the actual distance (green curve) in Figure 2c. STCR detects attack signals with wrong angle of arrival from un-probed directions—the blue spikes between 20s–36s in Figure 2c—and eliminates them when it computes the distance to the lead vehicle. A more detailed description of STCR follows.

III. SpatioTemporal Challenge Response

In this section, we describe a new spatio-temporal challenge response (STCR) scheme. The flowchart and block diagram of STCR are illustrated in Figures 3 and 4. Figure 3 depicts the overall logical flow in STCR to detect and dodge spoofing attacks against the automotive radar system. In Figure 3, STCR emits probing signals in a number of randomly selected directions in a synchronized manner, verifies the reflected signals based on the emitting and arriving directions of the signals, detects and filters suspicious signals out based on the verification results and estimates the distance from the host car to the lead vehicle using the verified signals only.

STCR divides the available bandwidth B into N narrow beams. The width of each beam is w and, therefore, $N = \frac{B}{w}$. These narrow beams are grouped into b buckets, where each bucket has p beams. Thus, the total number of buckets $b = \frac{N}{p}$. At each time, only one narrow beam out of p beams in each bucket is selected randomly by the synchronized challenge-response-authentication (CRA) module in Figure 4. To transmit b randomly selected narrow beams in different directions using the MIMO array shown in Figure 4, we use a MIMO beamforming technique based on the FDMB technique presented in [15]. It allows simultaneous multiple narrow beam transmissions using a MIMO FMCW radar as depicted in Figure 4.

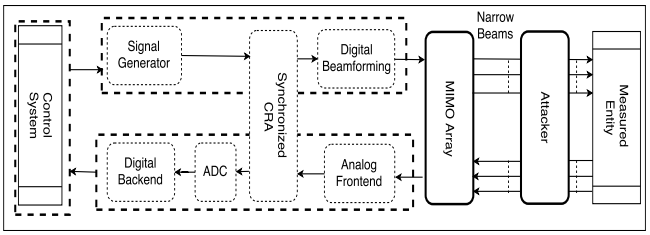
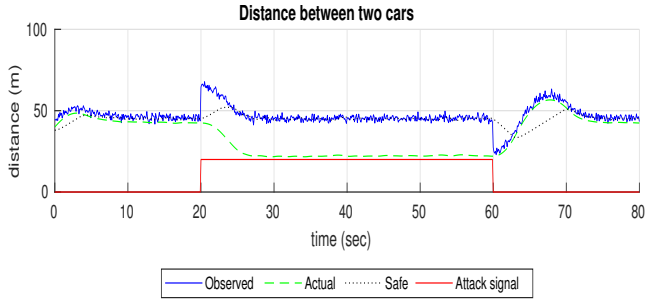


Fig. 4: Block Diagram of STCR

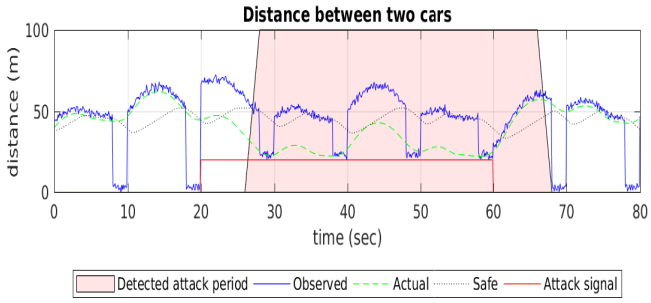
When the transmitted signal gets reflected off the lead car and arrives at the receive (Rx) end of the radar, the proposed system, STCR, determines the delay, velocity and direction of arrival (DoA) as per [16]. Further, it converts them back into the corresponding bucket. If the reflected signal that belongs to a bucket is outside the bounded physical limits determined by the DoA in relation to the direction of the beamforming of the original narrow beam, STCR considers it an attack and excludes the specific signal when it computes the distance from the host car to the lead vehicle. Thus, dropped signals are eliminated and not processed by the ADC and digital back-end in Figure 4 to avoid unnecessary distance miscalculation or signal processing overhead due to attack. This way, STCR only uses the trustworthy reflected signals with the directions of arrival verifiable based on fundamental physics to calculate the distance to the lead car, while randomly selecting a beam in each bin over time. STCR avoids an ongoing attack by simply varying the phase-angle of a victim beam, if any, to take the system out of attack in its subsequent probe signal transmission. In case of attack, the system facilitates a randomized angular phase change discussed above via MIMO beamforming in FDMB [15] to thwart attack and make long-term attack difficult. By physically verifying the trustworthiness of the radar data and enhancing the robustness of the system, the proposed system can significantly enhance the accuracy of distance calculation under attack, while offering consistent availability of the radar system with zero down-time.

IV. Performance Evaluation

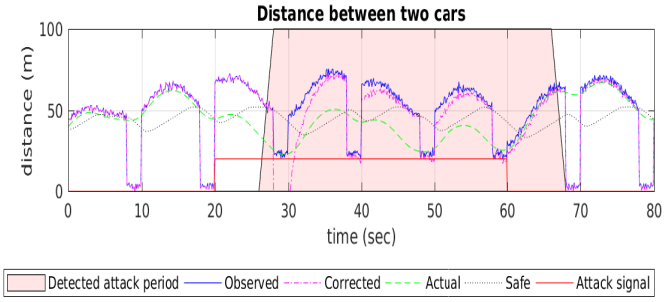
To evaluate STCR, we use the car-following model included in the ACC package of Matlab as discussed before. To articulate the attack environment, the car-following model has been extended to inject attack signals. The performance has been evaluated under three scenarios: 1) a short-term static attack scenario, 2) a long-term static attack scenario and 3) a sinusoidal attack scenario. In the short-term static attack scenario, a constant attack signal is transmitted to the radar's receive end between 20s–36s as discussed in Section II-D. In the long-term static attack scenario, we have the attacker transmit a constant attack signal to the radar system between 20s–60s to observe the impact of a long-term attack. On the other hand, an increasing ramp-like sinusoidal attack signal is transmitted to the radar system in the sinusoidal scenario. STCR is compared to the state-of-the-art baselines: 1) PyCRA [9], 2) Dutta et al. [10] and



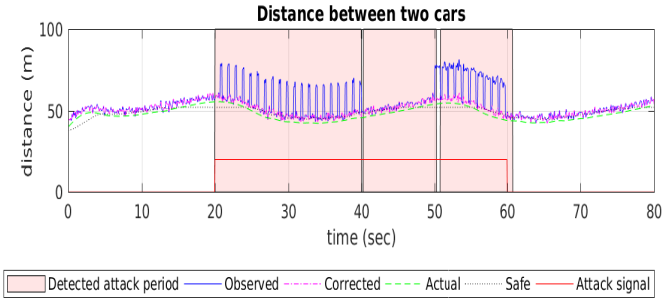
(a) Vanilla Method



(b) PyCRA Model [9]

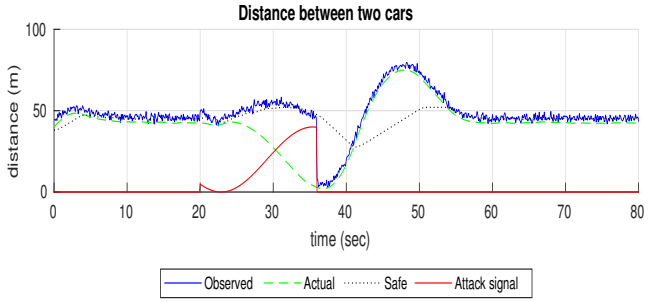


(c) Dutta et al Model [10]

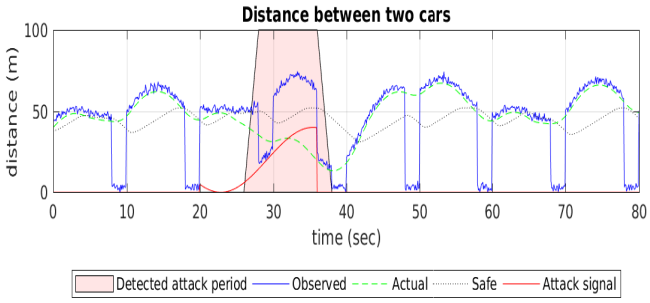


(d) STCR Model

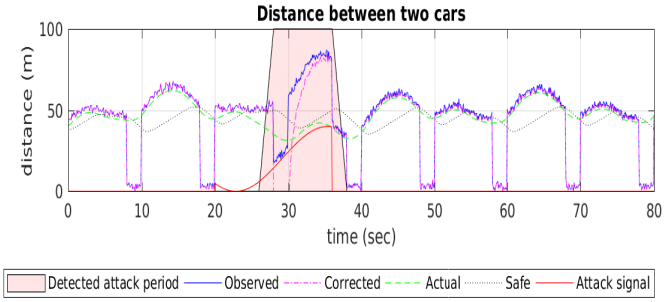
Fig. 5: Simulation Results for Long-Term Static Attack Scenario



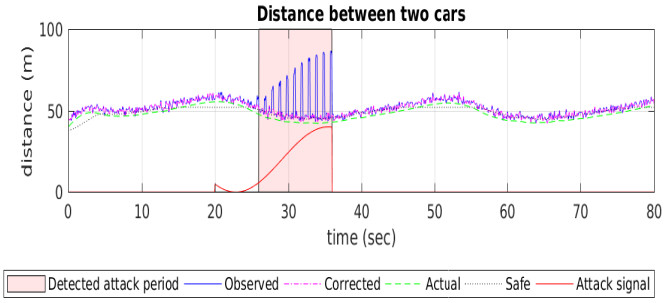
(a) Vanilla Method



(b) PyCRA Model [9]



(c) Dutta et al.Model [10]



(d) STCR Model

Fig. 6: Simulation Results for Sinusoidal Attack Scenario

3) vanilla ACC system with neither attack detection nor recovery via attack signal filtering [17].

The performance evaluation results are shown in Figures 2, 5 and 6. Figures 5a, 5b, 5c and 5d show the results under the long-term attack launched between 20s-60s, while Figures 6a, 6b, 6c and 6d plot the results under the sinusoidal attack between 20s–36s. Each figure shows the calculated/observed distance that can be affected by attack (blue curve), actual ground-truth distance (green curve), corrected distance by RLS in Dutta [10] and by eliminating incoming signals from suspicious directions in STCR (magenta curve), and the required safe distance (black curve), similar to Figure 2. Clearly, the vanilla system fails to detect or filter out any attack signal as shown in Figures 5a and 6a. In Figure 5a, its distance error is almost constant and equivalent to the attack signal. In Figure 6a, the actual distance decreases down to near zero, raising a serious safety concern. Thus, we focus on the results of PyCRA, [10] and STCR.

Similar to the results in Figures 2 discussed before, STCR significantly outperforms the baselines in terms of detection accuracy and latency as well as robustness. As shown in Figure 5d and 6d, the distance calculated by STCR (magenta curve) is nearly identical to the actual distance (green curve) even under attack. Also, the actual distance is never shorter than the safe distance unlike PyCRA and [10] whose actual distance is shorter than the actual distance by up to approximately 20m as plotted in Figure 5b and Figure 5c. Between 20s–40s in Figure 5d, STCR detects attack, spikes in the figure, based on the DoA. As the attacker keeps sending the attack signal from the same direction, STCR has no spike between 40s–50s until the attacker sends the attack signal from a different direction after 50s till 60s. However, STCR detects attack based on the DoA and excludes the attack signal.

In Figure 6d, STCR shows similar results under the sinusoidal attack too; the distance error, i.e., the difference between the distance calculated by STCR (magenta curve) and the actual distance (green curve) is near zero even under attack. Further, the actual distance is not shorter than the safe distance unlike PyCRA and [10] whose distance error increases up to approximately 35m and 40m, respectively. Notably, under the sinusoidal attack, the distance error of [10] is higher than that of PyCRA, since its RLS method converges to the attack signal that is increased incrementally between 20s–35s, which is hard to detect than a constant attack signal is.

V. Conclusions

Applying cyber security mechanisms, such as cryptography, trusted computing, and network intrusion detection, is insufficient to secure CPS, since most sensors (and actuators) are designed without security considerations and remain vulnerable to non-intrusive sensor spoofing attacks in the analog domain. To address this problem, we present a new approach to not only detect but also thwart sensor spoofing attacks against automotive radars essential for assisted and autonomous driving by effectively applying multiple beamforming in an automotive MIMO radar. Our approach, called spatio-temporal challenge-response (STCR), transmits probe signals in several randomly selected directions over time. STCR identifies reflected signals from untrustworthy directions that fail to be verified based on the direction of arrival, and excludes them when computing the distance to the lead vehicle. By doing this, it verifies the trustworthiness of sensor data, while significantly enhancing the robustness under spoofing attack. Unlike the advanced approaches representing the state of the art [9], [10], it does not suffer from any downtime or mis-learning. Therefore, not only STCR itself for improving automotive radar security but also the basic design principle is desirable to enhance the security of safety-critical CPS with high accuracy and availability requirements. In a simulation study performed using the car-following model in the adaptive cruise control package in Matlab, STCR's distance error—the difference between the actual distance (ground truth) and calculated distance—is near zero. In contrast, the largest distance error in [9] and [10] is approximately 35m and 40m, respectively. In the future, we will continue to explore how to further enhance the detection performance and resilience in automotive radar systems, while investigating the applicability of STCR to enhance sensor fusion in automotive systems. Moreover, we will investigate whether it is feasible to apply and extend STCR to enhance security or privacy in other cyber-physical systems, such as intelligent health care systems and smart grids.

Acknowledgement

This work was supported, in part, by NSF Project CNS-1526932. We appreciate anonymous reviewers for their help to enhance the paper.

References

[1] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," in *Proceedings of the 3rd Conference on Hot Topics in Security*. USENIX Association, 2008.

[2] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *International Conference on Cryptographic Hardware and Embedded Systems (CHES'13)*, 2013.

[3] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems," in *ACM Design Automation Conference (DAC '10)*, 2010.

[4] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, 2014.

[5] Song Han, Miao Xie, Hsiao-Hwa Chen, and Yun Ling, "Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges," *IEEE Systems Journal*, vol. 8, no. 4, pp. 1052–1062, 12 2014.

[6] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network," *Journal of Network and Computer Applications*, vol. 37, pp. 380–392, 1 2014.

[7] R. Liu and M. Srivastava, "PROTC: PROTeCting Drone's Peripherals through ARM TrustZone," in *Workshop on Micro Aerial Vehicle Networks, Systems, and Applications (DroNet '17)*, 2017.

[8] M. Harris, "Researcher Hacks Self-driving Car Sensors," *IEEE Spectrum*, 9 2015.

[9] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA," in *ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*, 2015.

[10] R. G. Dutta, X. Guo, T. Zhang, K. Kwiat, C. Kamhoua, L. Njilla, and Y. Jin, "Estimation of Safe Sensor Measurements of Autonomous System Under Attack," in *Annual Design Automation Conference (DAC '17)*, 2017.

[11] mathworks.com, "Model Predictive Control Toolbox Documentation."

[12] D. Bliss, K. Forsythe, and G. Fawcett, "MIMO Radar: Resolution, Performance, and Waveforms," *14th Annual Adaptive Sensor Array Processing Workshop,*, 2006.

[13] Constantine A. Balani, *Antenna Theory Analysis And Design*, 3rd ed. Wiley, 2005.

[14] W. Wiesbeck, L. Sit, M. Younis, T. Rommel, G. Krieger, and A. Moreira, "Radar 2020: The future of radar systems," in *2015 IEEE International Geoscience and Remote Sensing Symposium (IGARSS)*. IEEE, 2015.

[15] C. Pfeffer, R. Feger, C. Wagner, and A. Stelzer, "FMCW MIMO Radar System for Frequency-Division Multiple TX-Beamforming," *IEEE Transactions on Microwave Theory and Techniques*, vol. 61, no. 12, pp. 4262–4274, 12 2013.

[16] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Transactions on Antennas and Propagation*, vol. 34, no. 3, pp. 276–280, 3 1986.

[17] "Simulate adaptive cruise control using model predictive controller - Simulink," mathworks.com.