Literature Review

David R Crow, 2d Lt, USAF

May 31, 2019

Intrusion Detection

In cybersecurity, an intrusion detection system (IDS) is a device or software program that monitors a network for malicious activity. There are two primary types of IDS: misuse detection and anomaly detection [1]. Misuse detection systems compare network traffic to predefined attack signatures stored in large databases; a match indicates an attack on the network. Anomaly detection systems, on the other hand, compare traffic to a predetermined baseline to identify anomalies. In an environment of ever-increasing numbers of malicious actors, the United States Air Force (USAF) requires an IDS in each of its vital systems. Because we do not have significant access to USAF airplanes, this research concerns intrusion detection systems in passenger vehicles.

Cyber-Physical Systems & Time-Series Data

The Association of Computer Machinery (ACM) Transactions on Cyber-Physical Systems (TCPS) defines cyber-physical systems (CPS) as follows:

> Cyber-Physical Systems (CPS) has emerged as a unifying name for systems where the cyber parts, i.e., the computing and communication parts, and the physical parts are tightly integrated, both at the design time and during operation. Such systems use computations and communication deeply embedded in and interacting with physical processes to add new capabilities to physical systems. These cyber-physical systems range from miniscule (pace makers) to large-scale (a national power-grid). [2]

Often, the output of CPS monitoring is a time series representing the value of some process over time. One example of a time series in a passenger vehicle is the engine's revolutions per minute (RPM) over time, as measured by the vehicle's Electronic Control Unit (ECU). "Time series *analysis* is the process of extracting meaningful non-trivial information and patterns from time series [and time series] *forecasting* is the process of predicting the future value of time series data based on past observations and other inputs" [3]. Time series plots relate the value of the measurement for some given process to the relative or absolute time at measurement. These plots are used to increase interpretability of time series data, and they can be used to illustrate time series analysis and forecasting.

The CPSs present in passenger vehicles are capable of generating large quantities of time series data. One must only collect the data present on the vehicle's Controller Area Network bus to construct human-readable time series plots.

Causality

Causality is the relationship between cause and effect. For two processes a and b that exhibit a highly-causal relationship, we can expect that some set of parameters for a predicts some other set of parameters for b. If a and b are not highly-causal, modifying

a is not likely to elicit a predictable response in b. In passenger vehicles, causality is ever-present. The engine's RPM, for example, directly affects the vehicle's speed. Brake position indirectly affects engine RPM and thus the vehicle's speed. If one has access to a vehicle's brake position and engine RPM at time $t = 0$ and to the vehicle's brake position at time $t = 1$, one can estimate the vehicle's engine RPM at time $t = 2$.

Causal relationships also hold in the reverse direction. Some perceived value for vehicle speed implies that the vehicle must have had an engine RPM in some predetermined range at some previous point in time. This research shows that the significant presence of causal relationships in vehicles can serve as the foundation for an intrusion detection system.

Controller Area Network (CAN)

Before identifying causal relationships, we need data. The CAN protocol is a link-layer protocol commonly used in the automotive, manufacturing, and healthcare industries due to its low-cost, low-weight, and architectural simplicity. United States federal regulations require that all passenger vehicles manufactured after 2007 provide an on-board diagnostics (OBD)-II interface connected to the CAN bus. Consumers, mechanics, and original equipment manufacturers (OEMs) can utilize this OBD-II port to monitor some of the car's communications [4]. In 2018, [5] showed that data collected via an OBD-II port can be automatically reverse engineered, processed, and converted into time series data. Additionally, [5] hypothesized that one can quantify the causal relationships present in these time series with Empirical Dynamic Modeling (EDM).

Although auto manufacturers are required to provide the OBD-II interface, they

are not entirely required to abide by a message protocol. Often, OEMs develop proprietary packet frames and to obfuscate data traveling on the car's network. However, the Society of Automotive Engineers (SAE) J1979 diagnostic protocol is a federally-mandated diagnostic standard for information requests from light-duty passenger vehicles [6]. Even if OEMs deliberately misconfigure or obfuscate the CAN bus data, J1979 guarantees some truth data. Specifically, J1979 allows those with access to a vehicle's OBD-II interface to request specific information from the car; response data is standardized and must contain the truth. This protocol allows better interpretability of the time series plots given by the reverse engineering pipeline [5] developed.

Empirical Dynamic Modeling (EDM)

To identify causal relationships in a system, we use EDM, which is focused on modeling nonlinear dynamic systems using time series data. Univariate time series data can be converted to a higher dimensional representation by using time-lagged versions of itself as additional dimensions. We call the resulting manifold a shadow manifold. In 1981, Floris Takens showed that shadow manifolds created in this manner are diffeomorphic to the original attractor manifold [7].

Sugihara et al demonstrated that this diffeomorphic property of shadow manifolds can be leveraged to determine whether two time series belong to the same dynamic system [8]. If they do belong to the same system, we can quantify the causal relationship between them by examining the various manifolds and attractors.

References

[1] P. Shirani, M. A. Azgomi, and S. Alrabaee, "A method for intrusion detection in web services based on time series," *Canadian Conference on Electrical and Computer Engineering*, vol. 2015-June, no. June, pp. 836–841, 2015.

[2] ACM TPS, "Cyber-Physical Systems (TCPS): About," 2018.

[3] V. Kotu and B. Deshpande, *Time Series Forecasting*. 2019.

[4] ISO, "ISO 27145-1:2012(en), Road vehicles — Implementation of World-Wide Harmonized On-Board Diagnostics (WWH-OBD) communication requirements — Part 1: General information and use case definition," 2012.

[5] B. Stone, S. Graham, B. Mullins, and C. Schubert Kabban, *Enabling Auditing and Intrusion Detection for Proprietary Controller Area Networks*. Dissertation, Air Force Institute of Technology, 2018.

[6] SAE International, "Sae j1979: E/e diagnostic test modes," 2017.

[7] F. Takens, "Detecting strange attractors in turbulence," *Dynamical Systems and Turbulence*, pp. 366–381.

[8] Sugihara Lab, "Empirical Data Modeling: Quantitative Ecology and Data-Driven Theory," 2019.