学习周汇报

周 佳

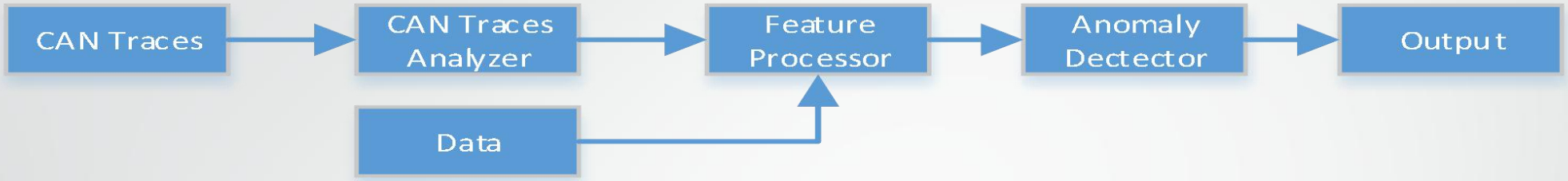
指导老师：李仁发 教授

- 提出一个，适用于车内网的，基于异常的入侵检测系统。
- 关键：找到一个feature；找到一个模型；-》区分正常与异常。

- 汽车：长生命周期；容易被物理接触；多场景（高速、低速、雨雪风霜天气等）；与人交互（误操作等）；

- 检测攻击；
- 溯源；
- 发生攻击后怎么办；

预期目标：



- First, analyze CAN traces to characterize the normal behaviors of the vehicle operation(CAN Matrix). we also need specific content of CAN messages, such **as speed, torque of engine**. We need to find **appropriate features** that can be helpful to find deviations. These combined data are fed into anomaly detection algorithm as selected feature.

- Then, design **adaptive anomaly detection algorithm**. An attack detector is just a classifier: it distinguishes system states reached when the system is operating under normal conditions from the states reached when the system is under attack. choose safety envelopes

- Next, compute the safety envelopes. As every in-vehicle network can have its own characteristics and the characteristics are even subject to change over time, there is no single equation that covers the entire variety of in-vehicle network behaviors. Therefore, I will employ **statistical methods to compute safety envelopes**. For example, **modified PCA or neural network** can be applied to compute an anomaly score.

- Real-Time Computing Lab (RTCL) in the EECS at The University of Michigan
- [1] Cho K T, Shin K G. Viden: Attacker Identification on In-Vehicle Networks. 24th ACM Conference on Computer and Communications Security (CCS'17)
- [2] Cho K T, Shin K G. Error handling of in-vehicle networks makes them vulnerable. 23rd ACM Conference on Computer and Communications Security (CCS'16)
- [3] Cho K T, Shin K G. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection. 25th USENIX Security Symposium (Sec'16)
- [4] Cho K T, Shin K G. CPS Approach to Checking Norm Operation of a Brake-by-Wire System. ACM/IEEE ICCPS'15
- [5] Tiwari A, Dutertre B, Jovanović D, et al. Safety envelope for security[C]//Proceedings of the 3rd international conference on High confidence networked systems. ACM, 2014: 85-94.

- Cho K T, Shin K G. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection. 25th USENIX Security Symposium (Sec'16)
- Clock-based Detection :

定义:

Let $\mathbb{C}_{true}$ be a "true" clock which reports the true time at any moment and $\mathbb{C}_i$ be some other non-true clock. We define the terms "clock offset, frequency, and skew" as follows.

- **offset:** difference in the time reported by clock $\mathbb{C}_i$ and the true clock $\mathbb{C}_{true}$. We define *relative offset* as the offset between two non-true clocks.
- **frequency:** the rate at which clock $\mathbb{C}_i$ advances. Thus, the frequency at time t is $\mathbb{C}_i'(t) \equiv d\mathbb{C}_i(t)/dt$.
- **skew:** difference between the frequencies of clock $\mathbb{C}_i$ and the true clock $\mathbb{C}_{true}$. We define *relative skew* as the difference in skews of two non-true clocks.

CIDS: Clock-based IDS

CIDS: Clock-based IDS

	Node 1	Node 2	Node 3
Clock Offset	-1 min	+1 min	0 min
Clock Skew	-1/60	+1/60	0

- Cho K T, Shin K G. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection. 25th USENIX Security Symposium (Sec'16)
- Clock-based Detection :

定义：

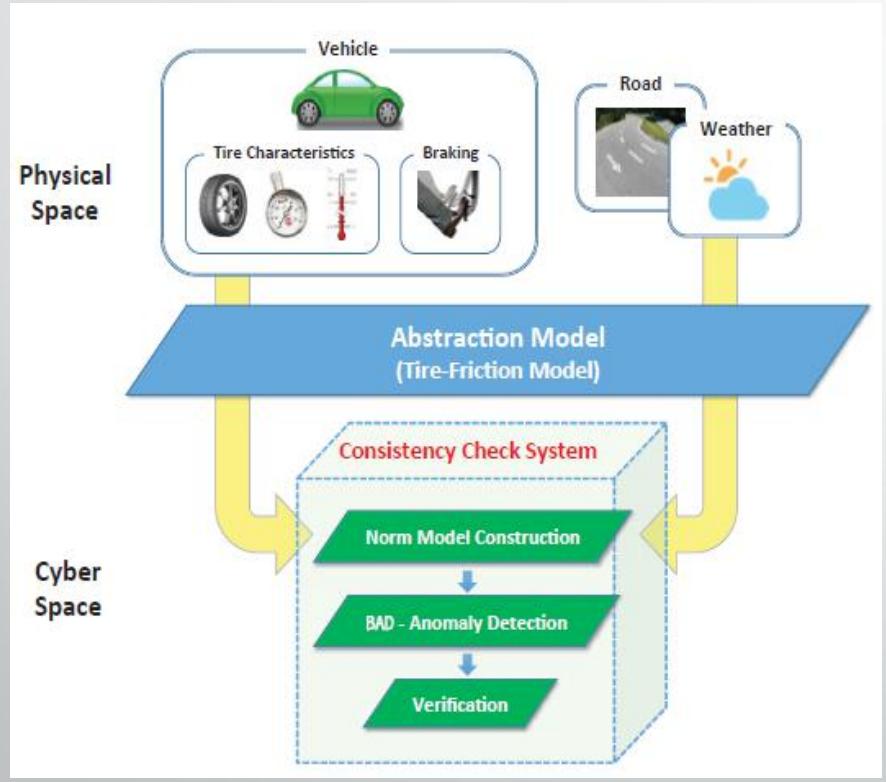
Let $\mathbb{C}_{true}$ be a "true" clock which reports the true time at any moment and $\mathbb{C}_i$ be some other non-true clock. We define the terms "clock offset, frequency, and skew" as follows.

- **offset:** difference in the time reported by clock $\mathbb{C}_i$ and the true clock $\mathbb{C}_{true}$. We define *relative offset* as the offset between two non-true clocks.
- **frequency:** the rate at which clock $\mathbb{C}_i$ advances. Thus, the frequency at time t is $\mathbb{C}_i'(t) \equiv d\mathbb{C}_i(t)/dt$.
- **skew:** difference between the frequencies of clock $\mathbb{C}_i$ and the true clock $\mathbb{C}_{true}$. We define *relative skew* as the difference in skews of two non-true clocks.

相关工作：

- 不少学者利用时钟偏移作为指纹信息加密物理设备。
- 前文的工作并不适用车内网络
  - -》 CAN网络消息包并不携带timestamp
  - -》 还有些依赖网络特定的拓扑结构（多跳特性，大网络拓扑）
- 本文利用**消息的周期特性（message periodicity）**来提取和估计transmitter的时钟漂移，作为指纹信息加密ECU。

- [4] Cho K T, Shin K G. CPS Approach to Checking Norm Operation of a Brake-by-Wire System. ACM/IEEE ICCPS'15
- 文章研究汽车线控刹车系统的安全问题。
- 文章认为数据之间存在关联性，利用关联属性可以判断汽车线控刹车系统是否受到了攻击。(本质：检查数据之间的一致性)



Cyber-physical approach to checking the norm operation of braking

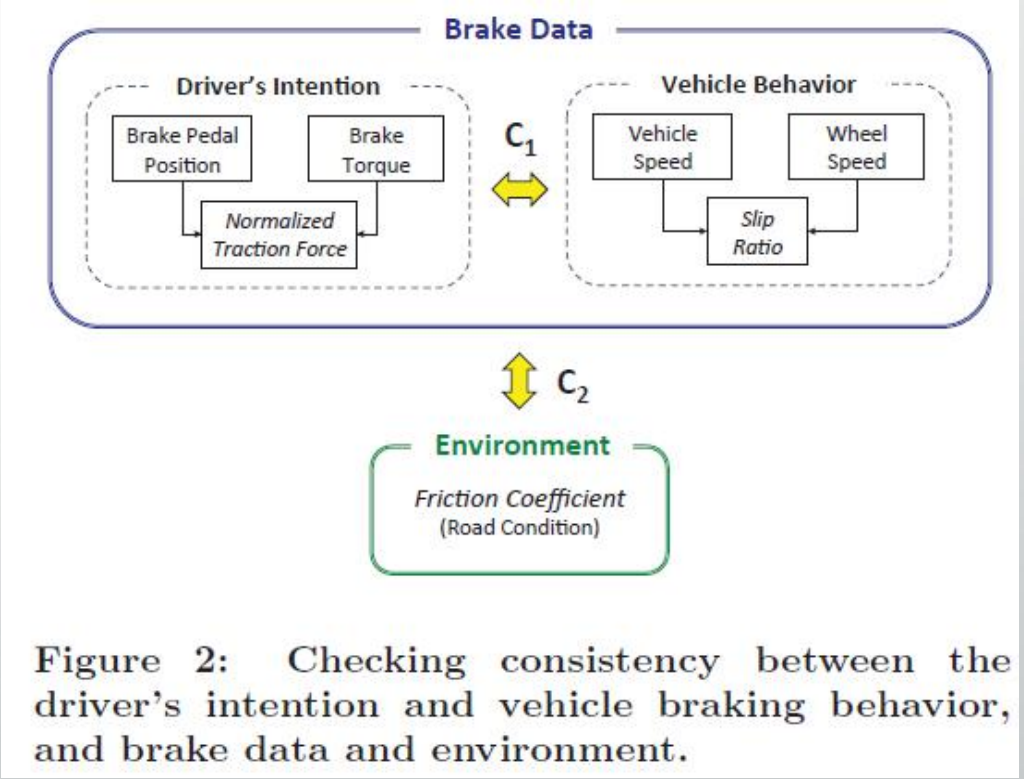


Figure 2: Checking consistency between the driver's intention and vehicle braking behavior, and brake data and environment.

- [4] Cho K T, Shin K G. CPS Approach to Checking Norm Operation of a Brake-by-Wire System. ACM/IEEE ICCPS'15
- 文章是显示建立模型：选择Brush Tire-Friction Model
  - E. Bakker, L. Nyborg, and H. Pacejka, "Tyre modelling for use in vehicle dynamics studies," in SAE Technical paper 870421, Feb. 1987.

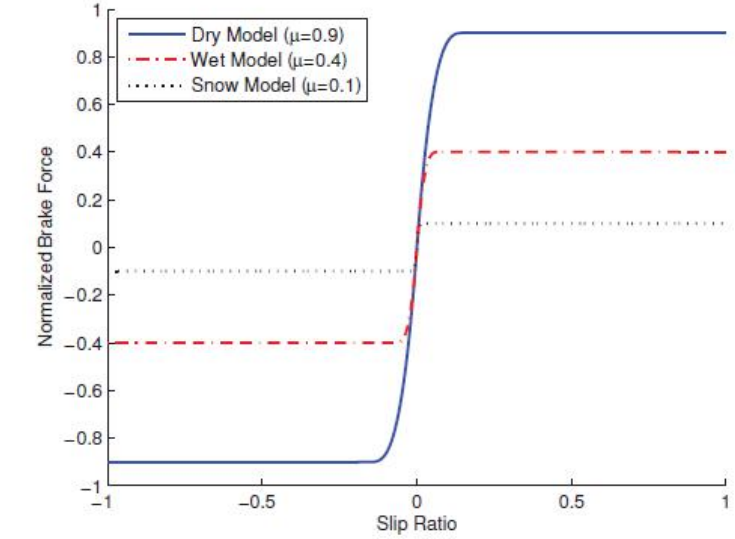


Figure 3: Norm braking models, which are based on the Brush tire-friction model and constructed by extrapolating low slip measurements.

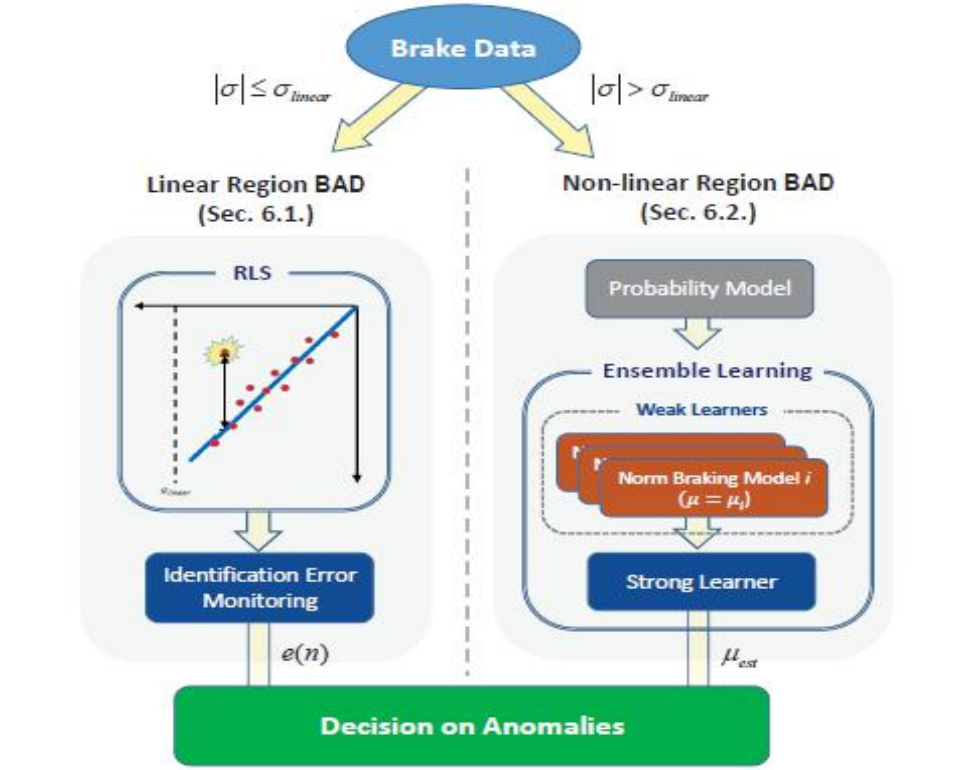


Figure 4: Overview of the proposed BAD (Brake Anomaly Detection).

低slip region（线性）和中高slip region（非线性）。

- [1] Cho K T, Shin K G. Viden: Attacker Identification on In-Vehicle Networks
- 24th ACM Conference on Computer and Communications Security (CCS'17)
- 研究入侵检测系统，解决现有入侵检测系统很难定位被攻击ECU的问题（fingerprint问题，研究背景类似之前介绍的使用时钟漂移fingerprint ECU的文章）。
- This paper proposes a novel scheme, called Viden (Voltagebased attacker identification), which can identify the attacker ECU by measuring and utilizing voltages on the in-vehicle network.

- 前提：The rationale behind using voltage for fingerprinting ECUs is the existence of small inherent discrepancies in different ECUs' voltage outputs when they inject messages.
- 文章假设一个ID的message只来自同一个ECU。
- 通过测量同一ID的message的总线电平，获得ECU的电压特性。

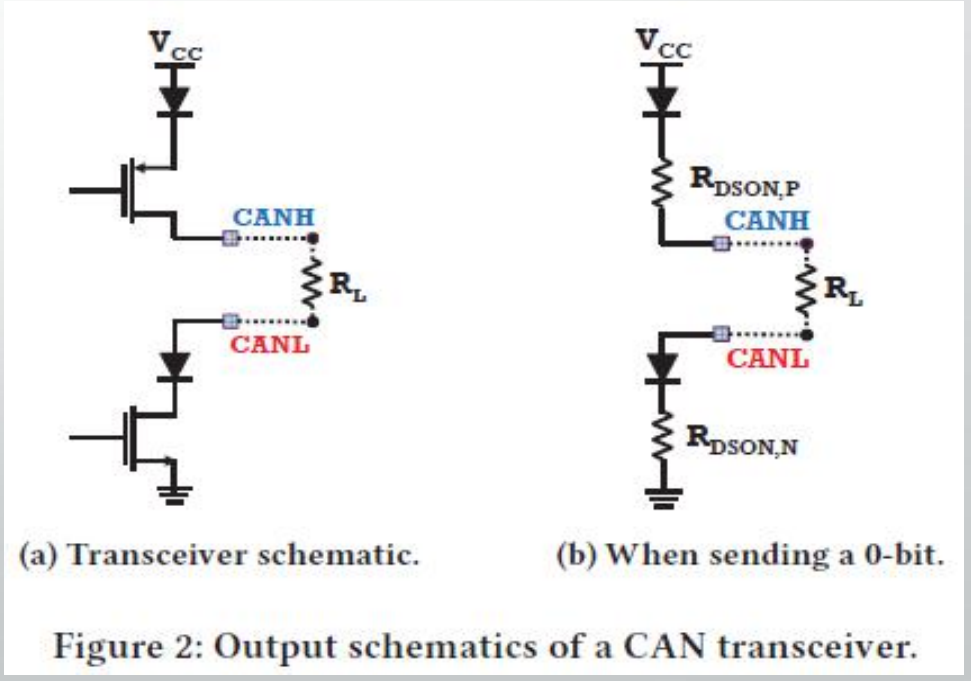


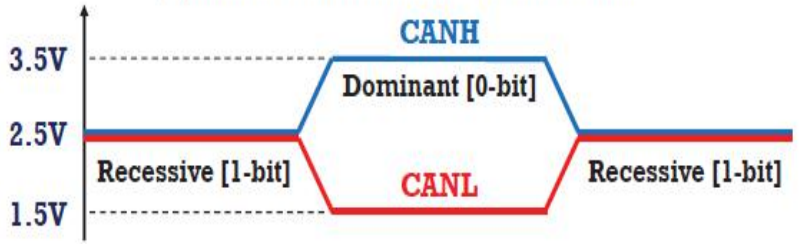
Figure 2: Output schematics of a CAN transceiver.

- [1] Cho K T, Shin K G. Viden: Attacker Identification on In-Vehicle Networks. 24th ACM Conference on Computer and Communications Security (CCS'17)
- 指纹信息需要满足：稳定，唯一，不可复制。
- 稳定：存在transient change，如何抑制以减少transient change的影响。
- 唯一：根据如下公式，CANH and CANL dominant voltages of each ECU are different from each other.

$$V_{CANH(i)} = V_{CC(i)} - V_D - I_{(i)}R_{DSON,P(i)},$$
$$V_{CANL(i)} = V_{G(i)} + V_D + I_{(i)}R_{DSON,N(i)}.$$

- 不可复制：攻击模型只有远程攻击，故不能通过精确调节电压或接入节点的方式伪装。

(a) Format of a standard CAN data frame.



(b) CAN output voltages when sending a message.

Figure 1: Message transmission via outputting voltages.

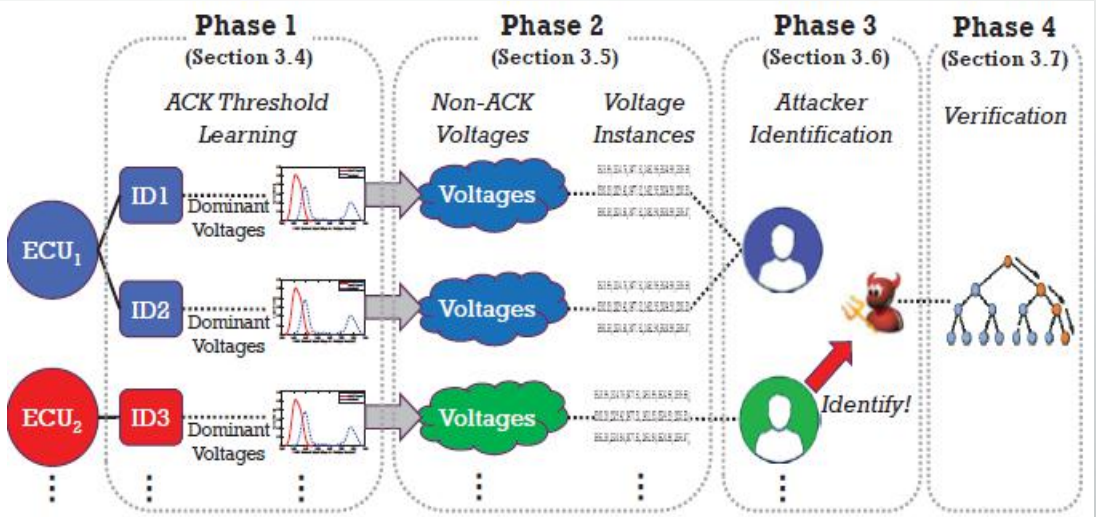


Figure 3: An overview of Viden.

Thanks!