

基于通信特征的 CAN 总线泛洪攻击检测方法

季一木^{1,2,3,4}, 焦志鹏^{1,3}, 刘尚东^{1,2,3,4}, 吴飞^{3,5}, 孙静^{1,3}, 王娜^{1,3}, 陈治宇^{1,3}, 毕强^{1,3}, 田鹏浩^{1,3}

- (1. 南京邮电大学计算机学院, 江苏 南京 210023;
2. 南京邮电大学江苏省无线传感网高技术研究重点实验室, 江苏 南京 210023;
3. 南京邮电大学高性能计算与大数据处理研究所, 江苏 南京 210023;
4. 南京邮电大学高性能计算与智能处理工程研究中心, 江苏 南京 210023;
5. 南京邮电大学自动化学院, 江苏 南京 210023)

摘要: CAN 由于其突出的可靠性和灵活性, 已成为当代汽车应用最广泛的现场总线。但是标准 CAN 协议没有提供足够的安全措施, 易遭受窃听、重放、泛洪、拒绝服务攻击。为了有效检测 CAN 总线是否遭受到攻击, 并在遭受泛洪攻击时将恶意报文滤除。对车载 CAN 总线报文通信特征进行了分析, 提出一种入侵检测方法, 该方法可以有效进行入侵检测、恶意报文滤除。通过实验验证, 该方法可以 100%检测出 CAN 总线是否遭受攻击, 恶意报文过滤的准确率可达 99%以上。

关键词: CAN 总线; 通信特征; 入侵检测; 恶意报文过滤

中图分类号: TP336

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2020005

CAN bus flood attack detection based on communication characteristics

Ji Yimu^{1,2,3,4}, Jiao Zhipeng^{1,3}, Liu Shangdong^{1,2,3,4}, Wu Fei^{3,5}, Sun Jing^{1,3},
Wang Na^{1,3}, Chen Zhiyu^{1,3}, Bi Qiang^{1,3}, Tian Penghao^{1,3}

1. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
2. Jiangsu Key Laboratory of High-Tech Research on Wireless Sensor Networks,
Nanjing University of Posts and Telecommunications, Nanjing 210023, China
3. Institute of High Performance Computing and Big Data Processing, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
4. Research Center for High Performance Computing and Intelligent Processing Engineering,

收稿日期: 2019-05-02; 修回日期: 2019-07-29

通信作者: 焦志鹏, 1577869867@qq.com

基金项目: 国家重点研发计划基金资助项目 (No.2017YFB1401302, No.2017YFB0202200); 国家自然科学基金资助项目 (No.61572260, No.61872196); 江苏省自然科学基金优秀青年基金资助项目 (No.BK20170100); 江苏省重点研发计划基金资助项目 (No.BE2017166)

Foundation Items: The National Key R&D Program of China (No.2017YFB1401302, No.2017YFB0202200), The National Natural Science Foundation of China (No.61572260, No.61872196), The Jiangsu Natural Science Foundation Excellent Youth Fund Project (No.BK20170100), The Jiangsu Provincial Key R&D Program (No.BE2017166)

论文引用格式: 季一木, 焦志鹏, 刘尚东, 等. 基于通信特征的 CAN 总线泛洪攻击检测方法[J]. 网络与信息安全学报, 2020, 6(1): 27-37.

Ji Y M, Jiao Z P, Liu S D, et al. CAN bus flood attack detection based on communication characteristics [J]. Chinese Journal of Network and Information Security, 2020, 6(1): 27-37.

Nanjing University of Posts and Telecommunications, Nanjing 210023, China

5. School of Automation, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Abstract: CAN has become the most extensive fieldbus for contemporary automotive applications due to its outstanding reliability and flexibility. However, the standard CAN protocol does not provide sufficient security measures and is vulnerable to eavesdropping, replay, flooding, and denial of service attacks. In order to effectively detect whether the CAN bus is attacked, and to filter malicious messages when subjected to flooding attacks. The characteristics of vehicle CAN bus message communication were analyzed, and an intrusion detection method was proposed, which could effectively perform intrusion detection and malicious message filtering. Through experimental verification, the method can detect whether the CAN bus is attacked by 100%, and the accuracy of malicious packet filtering can reach over 99%.

Key words: CAN bus, communication characteristics, intrusion detection, malicious message filtering

1 引言

现代汽车依靠电子控制单元(ECU, electronic control unit)实现对许多子系统的控制^[1],这些ECU通过总线连接进行通信^[2]。由BOSCH于20世纪80年代早期开发的车载控制器局域网(CAN, controller area network)总线是一种串行总线,CAN总线使用双绞线电缆两根电线之间的电压差异进行串行通信,速率可达1 Mbit/s,现已成为现代汽车总线标准协议。每个连接在CAN总线上的ECU通过设置两条双绞线之间的电压差作为信号来传输数据,同时,CAN总线上的其他ECU通过检测电压差来接收数据。由于ECU直接控制汽车的大部分传感器与执行模块,因此对车载CAN总线上的报文进行干扰、欺骗可能使ECU接收错误信息而造成严重的安全事故。2016年,在拉斯维加斯举办的黑帽大会上,Miller和Valasek演示了使用笔记本通过接入汽车CAN总线,并向CAN总线发送一些恶意报文,使汽车方向盘失控,而在此之前,他们的攻击使Jeep切诺基在高速公路上骤停,这也导致了140万辆汽车的召回。而随着智能驾驶的发展,车载诊断(OBD, on-board diagnostics)接口、辅助媒体端口等车载网络外部接口的普及,以及车联网技术的进步也使车载网络的攻击面变大,增加了车载网络对安全性的需求。文献[3]系统地分析了车辆可能遭受攻击的途径(如蓝牙、Wi-Fi、蜂窝网络等),以及ECU遭受攻击的表现。

车载CAN网络有别于传统的互联网,互联网中广泛应用的网络防御方法无法在车载CAN

网络中很好的应用。本文在分析了车载CAN网络的攻击模型和通信特征之后,提出一种基于车载CAN网络通信特征的泛洪攻击入侵检测、恶意报文滤除系统,该系统适用于车载CAN网络,并能在检测到攻击后将攻击报文滤除,提升车载CAN网络的安全性。

2 相关工作

车载网络是利用传输介质将汽车内部ECU、传感器和执行模块连接起来的通信网络,其中,应用最广泛的是CAN总线。由于CAN总线通信协议缺乏必要的安全保护措施,使其容易遭受嗅探、重放、泛洪、拒绝服务攻击。在文献[4]提出的3种攻击中,攻击方式都是泛洪地注入恶意报文到车载CAN总线上。

目前主要有两种应对车载网络攻击的防御方式:消息认证和入侵检测。消息认证是发送者在消息中添加鉴别码并加密,接收者按照约定的算法解密、鉴别运算检验消息可靠性的方法。入侵检测系统对网络传输进行实时监控,发现可疑的数据传输时发出警报或采取相应措施。

Andreaa等^[5]提出了一种轻量级认证协议,该协议允许车载CAN网络中的ECU相互认证。文献[6]提出了一种消息认证的方法来加强车载CAN总线的安全性,将CAN报文的时间间隔和时钟偏移隐藏到最低有效位中进行认证。消息认证可以提供一定安全性,并且在互联网领域广泛使用,但在CAN消息数据段长度最大为8 byte,添加认证码的可用空间有限,以及车载CAN网络通信的实时性要求,导致了消息认证很少在

CAN 总线入侵防御方面应用。

入侵检测系统广泛应用于车载 CAN 总线的安全防护, Hoppe 等^[7]首次提出车载网络入侵检测系统的概念, 并将 CAN 总线的周期性特征作为检测 CAN 总线注入式攻击的重要特征, 但没有给出具体算法、代码和实验。由于车载 CAN 报文的周期、内容恒定或者范围可预测, 因此这一特征可以作为检测车载 CAN 网络是否遭受到攻击的有力依据, 文献[8-9]已经验证这种方法有效。Muter 等^[10]提出一种入侵检测系统, 它监视两帧报文之间的时间间隔并计算它们的熵。除了报文的时间间隔, 一些研究者还验证报文的内容来检测 CAN 总线是否遭受攻击, 文献[11]验证了报文数据的取值范围。Moore 等^[12]同样利用 CAN 总线周期性作为检测依据, 首先观察总线一段时间, 估算出总线的通信周期, 以及周期的最大误差, 以此为依据, 当实时检测过程中周期性误差大于观测时的最大误差则认为遭受到注入式攻击。

现有的入侵检测系统可以以很高的精度辨别 CAN 总线是否遭受到攻击。但 CAN 报文不发送携带 ECU 的信息, 这些入侵检测系统无法辨别哪些报文是攻击报文, 以及攻击报文是由哪个 ECU 发出。这些入侵检测系统检测到攻击后一般采用发出警报的方式提醒驾驶者, 但驾驶者一般没有专业知识来处理攻击, 反而可能因为检测系统的

提醒分心而导致事故。因此, 本文提出一种入侵检测系统, 这种入侵检测系统在基于报文周期性特征检测出攻击之后, 再根据恶意报文和正常通信报文内容的区别将攻击报文滤除。

3 CLAD 检测方法

本文提出一种基于车载 CAN 总线报文通信特征的入侵检测系统 (CLAD), 该系统工作流程如图 1 所示。

1) 攻击者向攻击模型输入攻击报文, 攻击模型输出混杂着攻击报文和正常通信报文的报文序列。

2) 检测模块接收一段时间内的报文序列, 计算正常通信报文预期到达的合法时间段, 在这个合法时间段之外到达的报文, 可直接视为攻击报文, 而在这个时间段之内接收到多帧报文也认为遭受到攻击, 一旦检测到攻击, 这个模块向过滤模块输入合法时间段内所有的报文序列。

3) 过滤模块接收到检测模块输出的合法时间段报文后, 根据报文类型, 采用聚类或者霍夫变换的方法, 判别哪一帧为正常通信报文并输出。

3.1 通信特征

很多研究者以车载 CAN 总线报文的周期性作为注入式攻击检测的主要依据。当总线上流量激增, 或者周期紊乱的时候可以肯定 CAN 总线

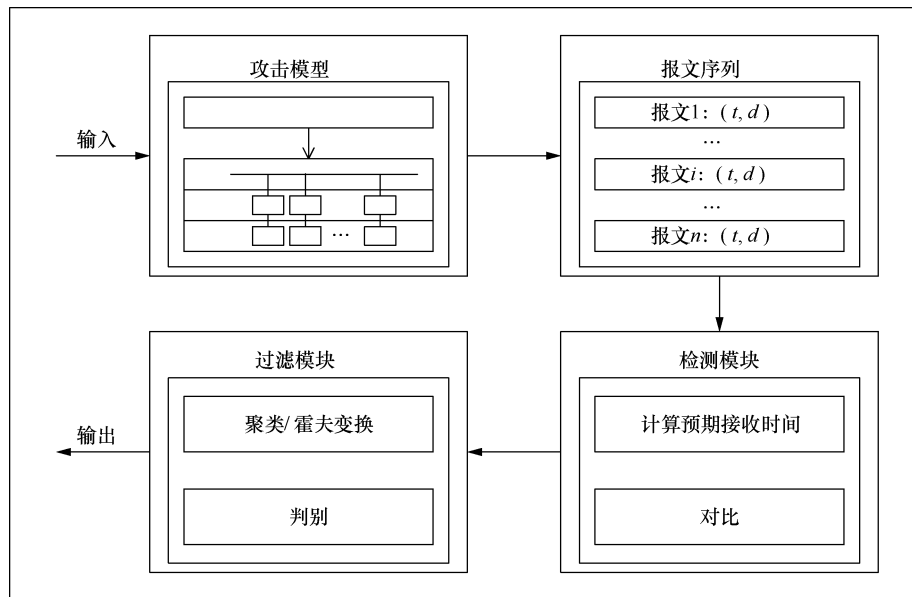


图 1 CLAD 检测流程

Figure 1 Detection process of CLAD

遭受到了注入式估计, 但仅凭借这一特征还不能达到将注入总线上的报文过滤掉的目的。经过实车报文采集、分析, 研究发现, 车载 CAN 总线报文还有稳定性特征。车载 CAN 总线报文有两个重要的通信特征详细描述如下。

(1) 周期性

为保证系统的实时性与稳健性, 连接在 CAN 总线上的 ECU 周期性地发送报文到 CAN 总线上。设有函数 $f(t)$, 参数 t 为时间, 若在 t 时刻接收到某 ID 的报文, 则 $f(t)=1$, 否则 $f(t)=0$ 。且函数 $f(t)$ 满足 $f(t+p)=f(t)$, 其中, p 为周期。

(2) 稳定性

由于报文的周期短, 同一 ID 的相邻两帧数据帧携带的数据一般保持不变或者变化量很小。设有函数 $g(t)$, 参数 t 为时间, $g(t)$ 为 t 时刻接收到报文的数据, 且函数 $g(t)$ 满足 $|g(t+p)-g(t)| \leq \Delta$ 。一般情况下, 离散型报文, 如车灯状态在一段时间内保持打开或者关闭, 在这个时间段内报文保持不变。连续型报文, 如车速, 在相隔几十毫秒的两帧报文之间数据变化量一般非常小。

本文将以上两个特征为重要依据, 进行车载 CAN 总线报文的注入式攻击检测, 并将恶意报文分离出来。

3.2 攻击模型

在车载 CAN 总线上, 当 ECU 接收到报文便根据其携带的数据执行相应的指令, 直到接收到下一帧报文根据下一帧报文内容执行相应动作。本文假设攻击者可以通过接触或者非接触的方法, 操控汽车上的 ECU, 向车载 CAN 网络注入带有伪造的 ID、数据的欺骗报文来实施攻击。攻击的方式是向 CAN 发送恶意报文, 尽可能快地覆盖关键 ECU 定期发出的正常通信报文, 使接收报文的 ECU 执行合法指令的时间趋向于 0, 而其他时间执行攻击者发送的恶意指令。

目前研究中, 攻击后果最严重的攻击方式为泛洪攻击: 攻击者伪造 ID 以较高的频率向 CAN 执行发送恶意报文, 当其他节点接收到合法数据, 很快就会被恶意 ECU A 发送的攻击报文覆盖。文献[8,11,13-14]详细描述了这样的攻击, 文献[11]以原有报文 10 倍的频率向 CAN 总线注入恶意报文来进行攻击, 可以实现操控仪表盘显示预期的里程计数值、发动机转速等攻击。

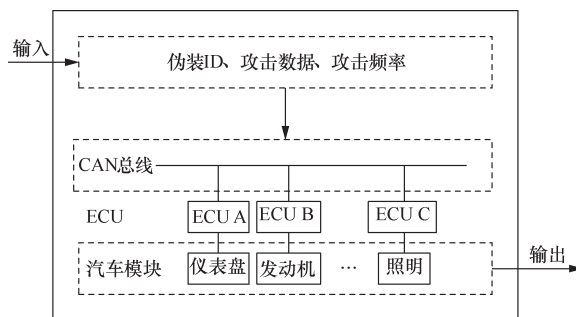


图2 攻击模型
Figure 2 Attack model

上述理论已经通过了本文的实验验证, 实验利用嵌入式设备单片机、CAN 收发器等设备模拟了车灯攻击实验, 通过恶意节点以高频率向总线注入恶意消息, 可以达到操纵 LED 灯开关的效果。因此, 本文的检测方法针对的攻击模型中, 输入为攻击报文的 ID、攻击数据以及攻击频率。其中, 伪造的 ID 决定攻击者的攻击目标, 攻击数据决定受到攻击的模块执行的虚假指令, 攻击频率越高则会导致模块执行虚假指令的时间占总时间的百分比越高。最终, 模型的输出为遭到攻击的汽车模块遭到攻击后的表现。

3.3 检测模块

利用车载 CAN 总线报文的周期性, 在接收到一帧正常通信的报文之后可以预测下一帧报文的接收时间。设周期为 p , 第 $i-1$ 帧报文的接收时间为 t_{i-1} , 则接收到第 i 帧报文的大致时间为 $t_i = t_{i-1} + p$ 。检测模块一次处理接收时间在 $\left[t_i - \frac{p}{2}, t_i + \frac{p}{2}\right]$ 范围内的所有报文, 由车载 CAN 总线报文的周期性, 第 $i+1$ 帧报文的接收时间 $t_{i+1} = t_i + p$, 且 $t_i \in \left[t_i - \frac{p}{2}, t_i + \frac{p}{2}\right]$, 所以这个范围内有且只有一帧正常通信的报文。一旦检测模块一次接收的报文大于一帧, 则可以判定车载 CAN 总线遭受攻击。

利用车载 CAN 总线报文的周期性不但可以有效检测出 CAN 总线是否遭受到注入式攻击, 并且可以详细给出恶意攻击报文的数量。假设检测模块一次接收到 n 帧报文, 则恶意攻击报文数量为 $n-1$ 。

虽然利用车载 CAN 总线报文的周期性可以有效检测出 CAN 总线是否遭受到注入式攻击和恶意攻击报文的数量, 但无法将正常通信的报文

和恶意攻击报文区分开，当需要将恶意攻击报文滤除的时候，就需要用到以车载 CAN 总线的稳定性特征为依据的过滤模块。

3.4 过滤模块

当检测模块检测到在 $\left[t_i - \frac{p}{2}, t_i + \frac{p}{2}\right]$ 范围内遭受到攻击，便将这些报文交由过滤模块处理，过滤模块将这些报文中唯一的一帧正常通信报文甄别出来，作为系统的输出。

车载 CAN 总线报文类型分为离散型报文和连续型报文。其中，控制某个模块状态信息的报文属于离散型报文，如控制车灯开或关的报文，离散型报文的数据段 d 属于一个有限的集合，即 $d \in S$ ；携带某个模块数值信息的报文输入连续型报文，如表示当前车速的报文，连续型报文的数据段可能的取值范围为一个区间内的全体实数，即 $d \in [d_{\min}, d_{\max}]$ 。

过滤模块根据报文类型采用不同的过滤策略，当 CAN 总线离散型报文遭受到攻击，在预测范围内接收到多帧报文时，首先根据报文的数据段这些报文聚类，由于一个周期一般只有几十毫秒，在这个时间段内攻击者发送的报文也趋向稳定，所以，分类之后最可能有如下两种情况：

1) 一个周期时间内的报文被分成多类，其中，一类只有一帧报文并且和上一帧正常通信报文数据相同，则这一帧是正常通信报文；

2) 如果预测范围内接收到的多帧报文数据段全部相同，并且只分为一类，由于预测范围内肯定有一帧正常通信的报文，那么可以根据上一帧接收时间和平均周期计算出一个时间点，选择接收时间与这个时间点误差最小的报文作为正常通信的报文。

而当攻击者的攻击意图刚好在预测范围内发生改变时，会发生超出上述两点之外的分类情况，但一个周期之后，聚类结果就会再次回归到上述两种主要的分类情况。一旦聚类结果发生这些情况时，在数据段与上一帧正常通信报文数据段相同的一类中，根据上一帧接收时间和平均周期计算出一个时间点，选择接收时间与这个时间点误差最小的报文作为正常通信的报文。

对于连续型报文，假设报文的接收时间为 t_i ，

报文携带的数据为 d_i ，则报文可以表示为 $t-d$ 坐标系上的一个点 (t_i, d_i) 。而当 CAN 总线连续型报文遭受攻击时，在预测时间内同时可以接收到攻击者发送的多帧恶意报文，以及一帧正常通信报文。由于报文的周期一般只有几十毫秒，这个时间段内接收到的多帧恶意报文数据段变化量很小，对应的 $t-d$ 坐标系中的多个点可以看做一条线段，而这个范围内唯一的一帧正常通信报文在 $t-d$ 坐标系映射成一个点。这样，恶意攻击报文组成的线段与正常通信报文表示的点的关系有两种：

① 点在直线之外；② 点在线段上。

通常来说，恶意报文携带的数据与正常通信报文的数据差异较大，出现第一种情况的概率较大，要将恶意报文滤除，本文首先利用霍夫变换拟合出这些报文对应的线段，再找到离线段距离最远的点即为正常通信报文。

霍夫变换可以检测出坐标系中可能存在的直线，输入坐标系中多个点坐标，输出这些点组成的直线方程。设有

$$t \cdot \cos \theta + d \cdot \sin \theta = r \quad (1)$$

由式(1)可得出如下推理。

推理1 将 t 和 d 作为常量， θ 和 r 作为变量，则将 $t-d$ 空间中一点 (t, d) 代入式(1)，式(1)可表示 $\theta-r$ 空间中的一条曲线 l 。

推理2 将 θ 和 r 作为常量， t 和 d 作为变量，则将 $\theta-r$ 空间中一点 (θ, r) 代入式(1)，式(1)可表示 $t-d$ 空间中一条直线 l' 。

假设有 $t-d$ 坐标系内点集 $P: \{p_i: (t_i, d_i), i=1, 2, \dots, n\}$ ，由推理1可得出 $\theta-r$ 空间中曲线集 $L: \{l_i: t_i \cdot \cos \theta + d_i \cdot \sin \theta = r, i=1, 2, \dots, n\}$ ，若这 n 条曲线在 $\theta-r$ 空间交于一点 $p: (\theta', r')$ ，且满足

$$\begin{cases} t_1 \cdot \cos \theta' + d_1 \cdot \sin \theta' = r' \\ t_2 \cdot \cos \theta' + d_2 \cdot \sin \theta' = r' \\ \vdots \\ t_n \cdot \cos \theta' + d_n \cdot \sin \theta' = r' \end{cases} \quad (2)$$

由 $p: (\theta', r')$ 以及推理2可得出 $t-d$ 空间中一条直线 $l': t \cdot \cos \theta' + d \cdot \sin \theta' = r'$ ，由式(2)可知，点集 $P: \{p_i: (t_i, d_i), i=1, 2, \dots, n\}$ 中所有的点都在直线 l' 上。于是，将 $t-d$ 空间中点集经由霍夫变换后得出直线方程 $l': t \cdot \cos \theta' + d \cdot \sin \theta' = r'$ 。

如图 3 所示, $t-d$ 坐标系内的点集 $S' = \{(1,3),(2,2),(3,1)\}$, 由推理 1 得出 $\theta-r$ 空间中的三条曲线交于点 $p\left(\frac{\pi}{4}, 2\sqrt{2}\right)$, 由推理 2 可得, $t-d$ 空间中经过 3 点的直线方程为 $\frac{\sqrt{2}}{2}t + \frac{\sqrt{2}}{2}d = 2\sqrt{2}$ 。

在本文应用场景中, $t-d$ 空间内 n 个点 $P\{p_i:(t_i, d_i), i=1,2,\dots,n\}$, 其中, t_i 为一个周期内第 i 帧报文的接收时间, d_i 为第 i 帧报文携带的数据。由推理 1 得出的 $\theta-r$ 空间中曲线集 $L\{l_i:t_i \cdot \cos\theta + d_i \cdot \sin\theta = r, i=1,2,\dots,n\}$ 不一定交于一点, 无法得出一条精确的直线。因此将 $\theta-r$ 空间划分成多个网格, 每个网格作为累加器, 每两条曲线在某个网格相交, 则网格对应的累加器增 1, 最终取数值最大的累加器中心点作为结果, 如图 3, 取交点最多的网格中心点 $p'(0.75, 2.5)$, 由推理 2 得出近似拟合直线为 $p': 0.73t + 0.68d = 2.5$ 。

由霍夫变换拟合出直线 l' 之后, 计算 $P\{p_i:(t_i, d_i), i=1,2,\dots,n\}$ 中每个点 p_i 到直线 l' 的距离, 若点 p_k 到直线 l' 的距离最远, 则第 k 帧报文为正常通信报文。

4 实验

4.1 通信特征与攻击模式

本文以知豆 D2S 为例验证 CAN 总线报文通信特征, 利用 USB-CAN 设备连接知豆 D2S 汽车的 OBD 接口采集了汽车 36 486 帧 CAN 总线报文进行分析。USB-CAN 设备主要记录了接收时间、报文 ID, 以及 0~7 总计 8 个字节的报文数据, 如表 1 所示。

从采集到的报文看, 车载 CAN 总线上的 ECU 总是周期性地发送报文, 即其他连接在 CAN 总线上的 ECU 从接收到某一 ID 的报文起, 到下一次接收到相同 ID 的报文的时间间隔大致是一个常量。这个时间间隔大小因报文 ID 而异, 观察采集到的 CAN 报文发现, 时间间隔常量从 20 ms 到 2 000 ms 不等, 时间轴上的点表示在该时刻接收到 ID 为 0X400 的报文, 可以看出接收到报文的时间呈现明显的周期性如图 4 所示, 报文两帧之间时间间隔大约为 210 ms, 最大误差为 0.558 ms。

ECU 周期性地向 CAN 总线发送报文的好处主要有两个: 首先, 每个传感器的数据可以被及时连接在 CAN 总线上的其他 ECU 接收, 因此保证了车载 CAN 网络的实时性; 其次, 即使一帧报文出现故障, 这一故障报文很快就会被而后接收到的正常报文覆盖掉, 增强了车载 CAN 网络的稳健性。

攻击者必然要周期性地发送恶意报文到 CAN 总线上, 否则将会被正常的周期性报文所覆盖。因此, 在攻击者进行攻击时, 恶意报文与正常报文混合在一起出现在总线上, 导致两帧报文之间的时间间隔变短。如图 5 所示, 在 CAN 总线正常通信时, 以 100 ms 为周期注入恶意报文进行攻击, 于是原本 CAN 总线信道上任意两帧之间时间间隔由稳定的 210 ms 变为从 0.2 ms 到 100 ms 不等的时间间隔。

CAN 总线报文的 ID 表示发送节点身份, 而报文的数据段通常代表节点发送的传感器感知信息或者节点的控制指令。通常情况下, 离散型报

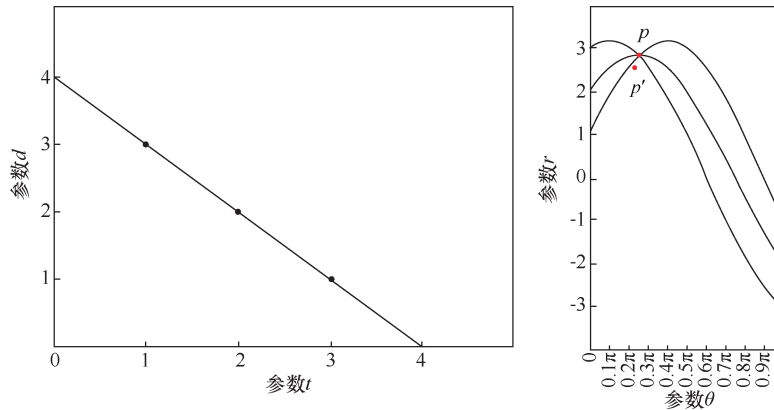


图 3 霍夫变换示例
Figure 3 Examples of Hough transform

表 1 采集到的部分车载 CAN 总线报文
Table 1 Some collected messages on CAN bus

索引	接收时间	发送/接收	ID	帧类型	帧格式	长度	字节 0	字节 1	字节 2	字节 3	字节 4	字节 5	字节 6	字节 7
1	000.001.335	接收	OCFF01DC	数据帧	扩展帧	8	0	0	0	0	8	0	0	128
2	000.016.289	接收	18C00301	数据帧	扩展帧	8	186	13	150	78	0	66	72	1
3	000.019.992	接收	18C00301	数据帧	扩展帧	8	186	13	150	78	0	66	72	1
4	000.002.463	接收	08FF01DD	数据帧	扩展帧	8	8	152	0	0	0	0	0	0
5	000.010.220	接收	OCFF00DC	数据帧	扩展帧	8	132	12	69	0	0	0	0	16
6	000.007.359	接收	18C00301	数据帧	扩展帧	8	186	13	150	78	0	66	72	1
7	000.019.993	接收	18C00301	数据帧	扩展帧	8	186	13	150	78	0	66	72	1
8	000.000.560	接收	17COEEF4	数据帧	扩展帧	8	209	14	14	166	14	15	58	1
9	000.000.568	接收	17COEEF4	数据帧	扩展帧	8	150	0	186	13	4	78	0	0
10	000.000.584	接收	17FF00F4	数据帧	扩展帧	8	0	0	0	0	0	0	0	0
11	000.000.607	接收	18C00501	数据帧	扩展帧	8	0	0	3	0	0	0	0	0
12	000.009.985	接收	08FF00DD	数据帧	扩展帧	8	0	0	171	1	0	0	0	0
13	000.007.689	接收	18C00301	数据帧	扩展帧	8	186	13	150	78	0	66	72	1
14	000.003.654	接收	0CFF01DC	数据帧	扩展帧	8	0	0	0	0	8	0	0	144
15	000.000.578	接收	401	数据帧	扩展帧	8	0	2	0	0	0	0	0	0
16	000.015.782	接收	18C00301	数据帧	扩展帧	8	186	13	150	78	0	66	72	1

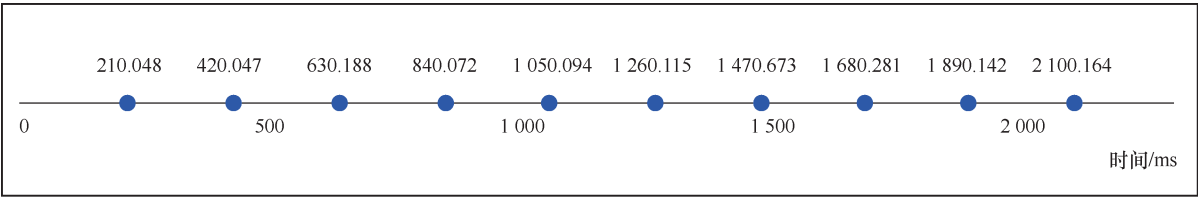


图 4 CAN 总线信道
Figure 4 CAN bus channel

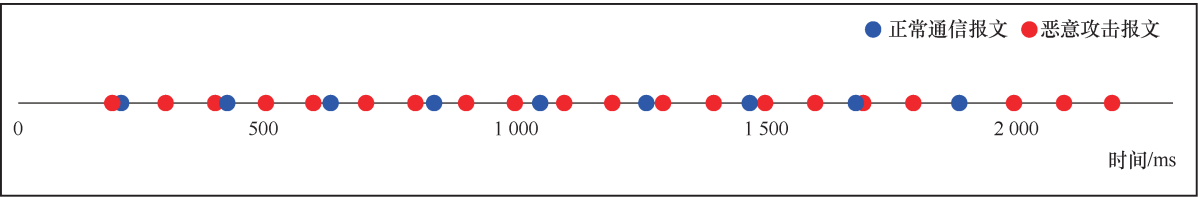


图 5 受到攻击的 CAN 总线信道
Figure 5 CAN bus channel under attack

文数据段以较大的概率保持原状态。以车灯状态为例，假如表示车灯的报文 ID 为 0X00，周期为 100 ms，驾驶员将车灯打开 10 min 再关闭。则这 10 min 内 CAN 总线上可以接收到 6 000 帧 ID 为 0X00 的报文，其中车灯状态变化了两次，即由关闭到打开，再由打开到关闭。所以在这 6 000 帧报文中，有 5 998 帧报文的数据段与上一帧保持不变，保持原状态的概率超过 99.96%。ID 为 0XCFF01DC 的报文信息如表 2 所示。其数据段

长度为 8，第 1 字节到第 7 字节数据保持不变，每帧报文的最后一个字节自增 16 用来校验是否丢帧。

而连续型报文数据段反映的一般是汽车上某传感器的感知数据，如压力数据、发动机转速数据，温度数据等。车载 CAN 总线报文周期一般为几十毫秒，两帧报文的数据变化量非常小。

可见，实验采集到的这些 CAN 报文符合第 3.1 节提出的周期性特征和稳定性特征。

表2 ID为0XCFF01DC的报文信息
Table 2 Message information with ID 0XCFF01DC

接收时间	ID	字节0	字节1	字节2	字节3	字节4	字节5	字节6	字节7
32.016	CFF01DC	0	0	1	0	8	0	0	32
132.845	CFF01DC	0	0	1	0	8	0	0	48
232.033	CFF01DC	0	0	1	0	8	0	0	64
332.203	CFF01DC	0	0	1	0	8	0	0	80
432.096	CFF01DC	0	0	1	0	8	0	0	96
532.469	CFF01DC	0	0	1	0	8	0	0	112
632.033	CFF01DC	0	0	1	0	8	0	0	128
732.047	CFF01DC	0	0	1	0	8	0	0	144
832.423	CFF01DC	0	0	1	0	8	0	0	160
932.861	CFF01DC	0	0	1	0	8	0	0	176
1032.065	CFF01DC	0	0	1	0	8	0	0	192
1132.058	CFF01DC	0	0	1	0	8	0	0	208
1232.251	CFF01DC	0	0	1	0	8	0	0	224
1332.487	CFF01DC	0	0	1	0	8	0	0	240
1432.079	CFF01DC	0	0	1	0	8	0	0	0
1532.063	CFF01DC	0	0	1	0	8	0	0	16
1632.116	CFF01DC	0	0	1	0	8	0	0	32
1732.500	CFF01DC	0	0	1	0	8	0	0	48
1832.062	CFF01DC	0	0	1	0	8	0	0	64

4.2 检测与过滤

本文主要借鉴文献[9]的实验方法,在文献[9]的实验中,作者在40 min内持续检测车载CAN总线报文,并在随机时间向总线注入恶意消息,每次攻击注入30条消息,持续5~10 s,随后在40 min的样本中随机抽样获得100个1 min的样本,这些样本有两种状态,包含攻击消息或者纯净的正常通信报文,经过该研究提出的检测方法检测后,结果显示,该方法可以有效检测注入式攻击。

本文的实验环境与文献[15]类似,利用单片机驱动CAN总线收发模块MCP_2515CAN作为一个节点连接在CAN总线上。如图6所示,模拟网络中有A、B、C3个节点,其中节点B每隔200 ms向CAN总线发送ID为0X17C0EFF4的报文,C负责接收ID为0X17C0EFF4的报文,而节点A作为攻击节点,向总线发送恶意攻击消息。正如文献[9,11,14]中表明,攻击者的发送速度应该为正常通信ECU的5~100倍,使正常通信的

ECU发出的报文尽快被攻击报文覆盖,使接收节点执行攻击节点发出的指令。因此本文中A节点以B节点5倍、10倍的频率随机向CAN总线发送恶意攻击报文,每次攻击持续2 s,同时利用USB-CAN设备监听所有总线消息,将监听到的消息序列保存至PC后,随机采样出100个20 s的样本,利用检测程序进行检测、过滤。

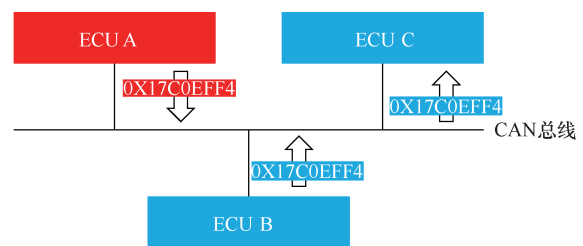


图6 实验CAN总线架构
Figure 6 CAN bus architecture in experiment

首先,节点B发送模拟车灯开关状态的离散型报文,节点A以5倍、10倍速度向CAN总线

发送ID相同的恶意报文，C节点接收并对接收到的报文进行检测。本文创建了100个5倍攻击速度的待检测样本，每个样本通信时间为20s，其中有39个样本包含2s的攻击，61个样本正常通信，创建了100个10倍攻击速度的待检测样本，每个样本通信时间为20s，其中有63个样本包含2s的攻击，37个样本正常通信。实验结果显示，检测系统可以100%测出是否遭受到攻击，进行攻击信号滤除时，100个10倍攻击速度样本中共有16314帧正常通信报文，将攻击报文滤除后得出10014帧正常通信报文，其中有9帧攻击报文被误判为正常通信报文，准确率为99.94%。

然后，节点B发送模拟车速的连续型报文，节点A以5倍、10倍速度向CAN总线发送ID相同的恶意报文，C节点接收并对接收到的报文进行检测。本文创建了100个5倍攻击速度的待检测样本，每个样本通信时间为20s，其中有45个样本包含2s的攻击，55个样本正常通信，创建了100个10倍攻击速度的待检测样本，每个样本通信时间为20s，其中有54个样本包含2s的攻击，46个样本正常通信。与离散型样本一样，检测系统可以100%测出是否遭

受到攻击，进行攻击信号滤除时，100个10倍攻击速度样本中共有15418帧正常通信报文，将攻击报文滤除后得出10037帧正常通信报文，其中有105帧攻击报文被误判为正常通信报文，准确率为99.31%。拟合检测过程直线拟合实例如图7所示，由于正常通信节点B发送的车速与攻击节点发送的车速有差别，检测系统对接收到的报文进行检测之后正常通信报文明显在拟合出的直线之外。

从实验结果来看，本文提出的入侵检测系统可以有效进行入侵检测、恶意报文过滤，本文实验结果与其他同类研究使用结果的对比如表3所示。

5 结束语

在第4.1节中发现，同一ID的车载CAN总线报文具有明显的周期性，遭受恶意报文攻击时两帧报文之间的时间间隔明显变短，这一特征可以作为是否遭受到攻击的检测依据。同时，由于报文的周期性，可以预测下一帧正常通信报文接收时间的大致范围，在这个范围之外的报文为攻击报文可以过滤掉，由于这个预测时间范围很短，在这个范围内如果遭受攻击，

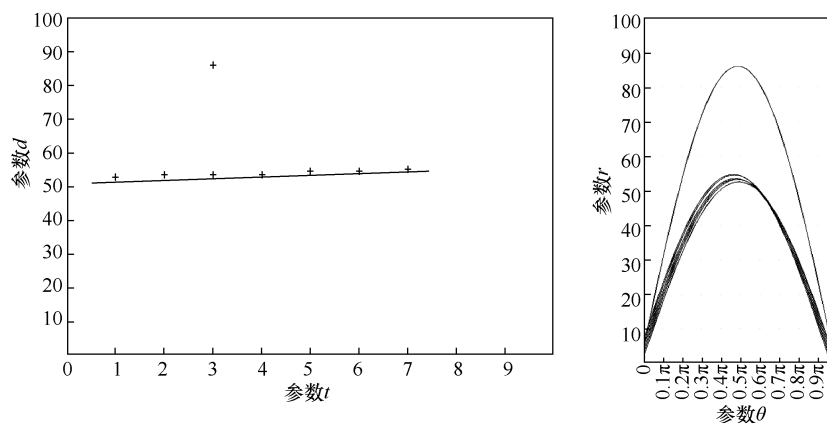


图7 检测实例
Figure 7 Example of detection

表3 本文提出的入侵检测系统检测效果与同类研究对比
Table 3 Comparative data between CLAD and related research

检测系统	攻击检测准确率	恶意报文过滤准确率
CLAD	100.00%	大于99.00%
IDS based on the analysis of time intervals ^[9]	100.00%	—
IDS based on anomaly frequency ^[12]	99.98%	—

一连串攻击报文序列携带的数据基本保持不变或者变化量很小，在时间坐标轴上基本形成一条直线。攻击者发送的数据一般与车辆正常数据不同，正常通信报文在坐标轴上的点一般在此直线之外，这一特征可以作为攻击报文滤除的依据。

因此，本文在分析了车载 CAN 总线周期性和报文携带的数据稳定性的基础上，提出了一种入侵检测系统，该系统可以成功检测出车载 CAN 总线是否遭受攻击，并在受到攻击时将恶意攻击报文滤除。在第 4.2 节检测与过滤中，该系统在入侵检测时，检测精度达 100% 并且没有误判。在进行恶意报文滤除时，准确率达 99% 以上，产生误差的原因很大程度是攻击报文携带的数据与正常通信报文的数据误差很小，这种情况下对车辆的安全不会造成太大威胁。

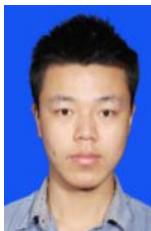
参考文献:

- [1] WOLF M, WEIMERSKIRCH A, WOLLINGER T, et al. State of the art: embedding security in vehicles[J]. EURASIP Journal on Embedded Systems, 2007(5): 1-16.
- [2] NOLTE T, HANSSON H, BELLO L L, et al. Automotive communications-past, current and future[C]//IEEE International Conference on Emerging Technologies and Factory Automation. 2005: 19-22.
- [3] CHECKOWAY S, MCCOY D, KANTOR B, et al. Comprehensive experimental analyses of automotive attack surfaces[C]//USENIX Security Symposium. 2011.
- [4] AVATEFIPOUR O, MALIK H. State-of-the-art survey on in-vehicle network communication can-bus security and vulnerabilities[J]. Comput Sci Netw, 2017, 6: 720-727.
- [5] ANDREEA R, FLAVIO D. LeiA: A lightweight authentication protocol for CAN[C]//Computer Science-ESORIC, 2016: 283-300
- [6] YING X, BERNIERI G, CONTI M, ET AL. TACAN: transmitter authentication through covert channels in controller area networks[J]. arXiv preprint arXiv.1903.05231, 2019.
- [7] HOPPE T, KILTZ S, DITTMANN J, et al. Security threats to automotive can networks practical examples and selected short term countermeasures[J]. Reliability Engineering and System Safety, 2011(96): 11-25.
- [8] TAYLOR A, JAPKOWICZ N, LEBLANC S, et al. Frequency-based anomaly detection for the automotive CAN bus[C]//World Congress on Industrial Control Systems Security. 2015: 45-49.
- [9] SONG H M, KIM H R, KIM H K, et al. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network[C]//2016 International Conference on Information Networking (ICOIN). 2016: 63-68.
- [10] MUTER M, ASAJ N. Entropy-based anomaly detection for in-vehicle networks[C]. IEEE Intelligent Vehicles Symposium. 2011: 1110-1115.
- [11] MUTER M, GROLL A, FRELING F, et al. A structured approach to anomaly detection for in-vehicle networks[C]//International Conference on Information Assurance and Security. 2010: 92-98.
- [12] MOORE M R, BRIDGES R A, COMBS F L, et al. Modeling inter-signal arrival times for accurate detection of can bus signal injection attacks: a data-driven approach to in-vehicle intrusion detection[C]//Annual Conference on Cyber and Information Security Research. 2017: 11.
- [13] MILLER C, VALASEK C. Adventures in automotive networks and control units[C]//Def Con. 2013: 260-264.
- [14] MILLER C, VALASEK C. A survey of remote automotive attack surfaces[C]//BlackHat USA, 2014: 94.
- [15] SAGONG S U, YING X, BUSHNELL L, et al. Exploring attack surfaces of voltage-based intrusion detection systems in controller area networks[C]//ESCAR Europe 2018. 2018: 1-13.

[作者简介]



季一木（1978—），男，江苏南京人，南京邮电大学教授、博士生导师，主要研究方向为 P2P 网络、云计算和大数据安全等。



焦志鹏（1994—），男，江苏淮安人，南京邮电大学硕士生，主要研究方向为总线安全。



刘尚东（1979—），男，甘肃永靖人，南京邮电大学讲师，主要研究方向为网络行为分析，大数据处理等。



吴飞（1989- ），男，江苏常州人，博士，南京邮电大学讲师，主要研究方向为人工智能、模式识别。



陈治宇（1994- ），男，江苏徐州人，南京邮电大学硕士生，主要研究方向为视觉与激光雷达的传感器融合。



孙静（1993- ），女，江苏南京人，南京邮电大学博士生，主要研究方向为机器学习。



毕强（1995- ），男，江苏宿迁人，南京邮电大学硕士生，主要研究方向为计算机视觉。



王娜（1995- ），女，安徽芜湖人，南京邮电大学硕士生，主要研究方向为计算机视觉。



田鹏浩（1996- ），男，江苏连云港人，南京邮电大学硕士生，主要研究方向为路径规划。