汽车控制器区域网络入侵检测系统综述

S191000849　李然　计算机工程系

1 前言

随着物联网技术的不断融合和针对车载网络的网络攻击的不断显现，汽车网络安全的需求日益迫切。由于现代汽车中互联技术的引入，基于网络的攻击在汽车中相对较新。如图 1 所示，现代交通工具包含多个接口，即车载诊断(OBD)-II 端口，使车辆暴露于网络攻击下。随着全自动汽车的出现，汽车安全的需求将大大增加，这些车辆必须表现得安全、可靠并且可预测。汽车网络攻击会导致灾难性的后果，包括造成生命或财产损失。

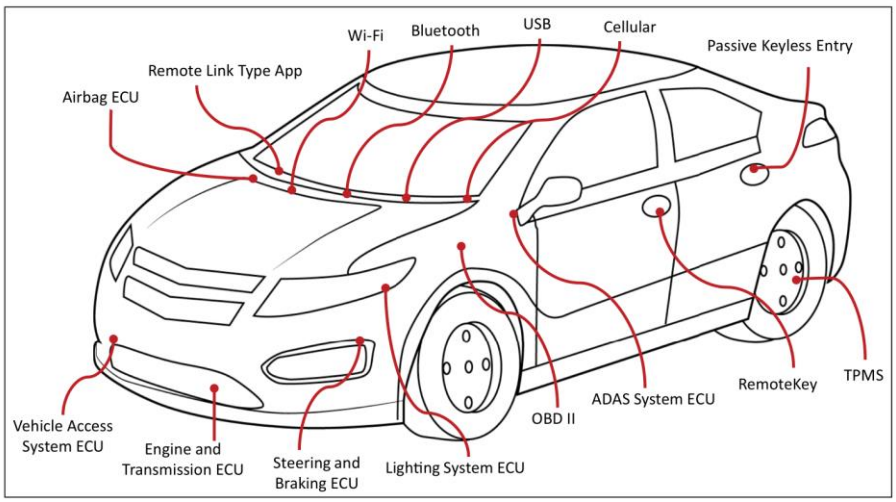

图 1 智能网联汽车安全威胁

提高车载网络安全性的一种方法是采用入侵检测和预防技术。入侵检测系统(IDSs)是用来减少入侵的计算机网络系统。然而许多传统的网络安全技术不能直接应用于车载网络，因此为车载网络设计一种高效的入侵检测系统是非常必要的。

本文探讨了目前识别车辆威胁的方法，并分析了如何使用 IDS 方法来解决这些威胁。

2 漏洞和威胁

2.1 CAN 漏洞

控制器区域网络(CAN)是一种异步串行的多机通信网络协议，连接电子控制单元(ECUs)。车辆、飞机和工业机械利用 CAN 来降低网络复杂性和布线成本。为使 CAN 消息可以自由地进出每个 ECU，CAN 体系结构是轻量级和健壮的，且无分段、未加密和缺乏身份验证。然而这些属性却直接导致了 CAN 的安全漏洞。

1) 缺乏消息认证：每个 ECU 在 CAN 总线上广播和接收所有数据，然后再确认这些信息是否是发送给它们的。在 CAN 的设计中，是无法防止未经授权的

设备加入总线并广播恶意消息到所有 ECU。通过访问总线，黑客可以向网络上的任何 ECU 发送伪造的消息。

2) 无分段网络：所有 ECU 都连接在一个公共网络上。这是 CAN 被用于汽车网络，以满足减少汽车系统之间点对点连接需求。然而，这种减少意味着一个处理信息娱乐的系统组件可以与安全关键的车辆系统通信。

3)未加密信息：加密会减慢 CAN 消息的速度并阻塞网络，然而未加密的流量很容易被嗅探、欺骗、修改和重放。

2.2 威胁和攻击

近年来，由于汽车系统出现了几起安全漏洞，因此对 CAN 总线安全性的研究有所增加。Koscher 等人通过嗅探 CAN 总线网络并对 ECU 代码进行反向工程，演示了对一系列功能的完全控制：禁用刹车、停止引擎以及控制其他车辆功能；Checkoway 等人他们在没有实际接触的情况下获得了访问权限，并通过广泛的攻击载体对车辆进行了攻击；Miller 和 Valasek 演示了通过 CAN 总线对多辆汽车进行的实际攻击。在一辆切诺基吉普车行驶在高速公路上时，作者远程控制了它的刹车，结果把车开进了沟里。

3 入侵检测系统的背景

入侵检测系统（IDS）是软件或硬件系统，通常通过传感器和报告系统实现来自动化攻击检测过程。现代大多数的 IDSs 通过监控主机或网络来捕获入侵相关数据。本文总结了传统 IDSs 的实现方法，以及如何将这些原则应用于汽车安全。

3.1 基于主机

基于主机的 IDS (HIDS)驻留在主机系统中并对其进行监视。在汽车中，基于主机的 IDS 驻留在单独的 ECU 中，它监视进出的流量包，并检查这些包是否带有恶意。为检测入侵行为，HIDS 还监视 ECU 本身。

3.2 基于网络

基于网络的 IDS (NIDS)是通信系统的一部分，它监视所有通过网络的流量，包括每个消息或包的标题和内容。自动 NIDS 使用充当 ECU 的 NIDS 监视网络上的所有流量，以便它可以接收和监视所有消息广播。

3.3 入侵检测方法

入侵检测方法可分为两大类：基于特征的入侵检测方法和基于异常的入侵检测方法。

1) 基于特征的方法使用捕获和创建的攻击特征的预定义知识库检测攻击，并监视当前具有这些特征的网络流量。该检测机制对已知的攻击具有较高的检测精度和较低的误码率，但它无法检测出数据库中未定义的攻击，因此无法检测到新的以及与已知攻击的任何偏差的攻击，需频繁地更新和维护知识库。

2) 基于异常的入侵检测通常从系统活动的训练或正常模型开始，然后 IDS 将当前系统的活动与之前捕获的正常模型相比较，以检测行为中的变化并将其标记为异常，任何未在常规配置文件中捕获的偏差都有可能被正确或错误地识别为

入侵。因此拥有完整的正常配置文件会有效地降低系统的误报率，其优点在于可以识别新的攻击。

4 汽车安全的入侵检测系统

4.1 消息时间

在正常的车辆操作中，由 ECU 生成的每个消息 ID 都有一个固定的频率。在攻击者注入消息时，ECU 仍然定期发送消息，最终根据攻击者的注入速度，网络上的消息速率将增加 2~100 倍。由于原始 ECU 仍在传输其消息，攻击者需要以足够快的速度发送消息，以覆盖具有相同 ID 的正常消息。

检测基于以下原则：当在 CAN 总线上传输新消息时，IDS 将检查该 ID 并计算从最新消息到达时间开始的时间间隔；如果新消息的时间间隔比正常模型短，则表明这是一个异常消息，因为消息比预期到达的要早。

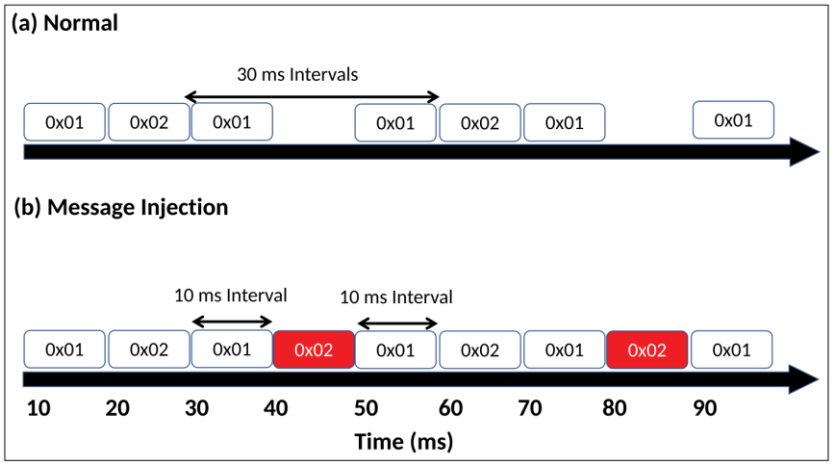

图 2 消息注入攻击对正常流量影响概念图

图 2 显示了消息注入攻击对正常流量影响的概念图， (a)正常状态下和(b)消息注入攻击下的 CAN 总线上传输的消息，消息 CAN ID 0x02 的时间间隔因注入攻击消息而缩短。

Miller 和 Valasek 引入了一个分析车载网络入侵检测消息率的概念，通过分析消息的分布率，可以检测到异常消息；Gmiden 等人提出了一种简单的 CAN 总线入侵检测方法，他们提出的算法不需要对 CAN 总线进行任何修改，且方法基于对 CAN 消息的时间间隔的分析；Moore 等人提出了一种基于 CAN 报文频率规律性的异常检测方法，他们观察到信号频率的规律性，并假设一个简单的异常检测系统监控 CAN 总线通信的信号等待时间，将提供对规则频率信号注入攻击的准确检测；Song 等人还提出了一种轻量级的入侵检测算法，用于检测 CAN 消息的时间间隔，他们确定时间间隔是一种特征，它可以通过显示正常状态和攻击状态的消息的时间间隔之间的明显差异来检测 CAN 总线流量中的消息注入攻击。

4.2 基于特征

Larson 等人提出了一种基于特征的攻击检测方法，即在每个 ECU 中都放置了一个检测器，它可以根据来自协议栈和 CAN 协议在预期 ECU 上的对象目录的信息来分析传入和传出的网络流量。结果表明，通过理论仿真可以从提取的信

息轨迹中检测出潜在的攻击。

4.3 基于异常

ECUs 的计算能力限制了复杂的 IDSs 的实现，从简单的座椅控制单元（到复杂的发动机控制单元，ECU 的复杂性和复杂程度都在不断变化。以下一些技术需要大量的计算：

1) 网络物理：定义了不同的 ECU 特性以区分单个车辆 ECU，每个 IDS 都使用车辆上每个 ECU 的特定特性。与消息定时异常检测类似，当这些属性与捕获的正常属性不同时，将检测出异常。Cho 和 Shin 引入了一个基于时钟的 IDS，它使用时钟偏移来验证 ECU，IDS 记录 CAN 总线上的通信并创建网络上每个 ECU 的指纹，每个 ECU 都根据其特定的时钟偏移分配一个指纹以对其区分；Ji 等人研究了一种基于时钟偏移的检测方法，他们的方法考虑到每个 ECU 都有一个固定的时钟偏差，可以建立一个正常的 ECU 时钟行为模型来检测异常测量，结果表明，该检测方法能够检测到 CAN 网络中传输的数据包的小范围变化；Choi 等人提出了一种新的汽车 IDS：VoltageIDS，该系统利用电子 CAN 信号特性作为 ECUs 的指纹，可以区分错误以及总线攻击，结果表明该方法能够检测到最近引入的总线攻击。

2) 熵：基于熵的入侵检测已经被应用到传统的基于网络的系统中，但由于典型的流量变化，通常具有很高的误报率。由于汽车网络流量的周期性越来越强，基于熵的检测已经被证明能够以较低的误报率检测异常。Muter 和 Asaj[24]利用正常运行时车载网络通信记录的数据计算香农熵值，偏离该熵值的区域被认定为潜在入侵。Marchetti 等人提出了一种基于熵的算法来检测未修改车辆中的 CAN 消息异常，他们根据在公共高速公路上驾驶期间捕获的数小时 CAN 流量进行了广泛的评估。实验结果表明，基于熵的异常检测器是识别攻击者注入消息引起的 CAN 总线异常的一种有效方法。

3) 报文速率：与报文定时检测相类似，Hoppe 等人提出了一种基于异常的 IDS，将其放置在 CAN 总线上，使其能够监听网络流量。它们的 IDS 检查特定消息的传输速率，并将其与检测其他消息或丢失消息的正常速率进行比较。这种方法不同于前面所研究的方法，因为它计算的是包的传输速率，而不是包的时间间隔，偏离预期正常传输的消息数被视为异常。

4) CAN 字段：利用 CAN 报文的组成和数据字段进行异常检测。Matsumoto 等人提出了一种防止 CAN 中未经授权的数据传输的方法，每个 ECU 监视总线上的所有数据，并在未经授权的消息完全传输之前，如果它识别出带有自己 ID 的欺骗消息，则广播错误消息。Markovitz 和 Wool 提出了一种新的 CAN 总线领域感知异常检测系统。他们通过对真实 CAN 通信的检测发现了语义上有意义的字段，开发了一种贪婪算法，将 CAN 消息分割成字段，并将这些字段分类为他们观察到的特定类型，异常检测系统使用分类器来描述字段并根据学习阶段的字段类型为消息建立模型，在执行阶段，系统会检测与模型的偏差。

Kang 和 Kang 提出了一种基于机器学习的 IDS 方法，使用深度神经网络结构来监视 CAN 数据包。它们的 IDS 由两个模块组成，监控模块根据已知攻击的

训练特征来确定 CAN 数据包的类型，一旦监控模块识别出新的攻击，分析模块就会记录该攻击模型并更新系统。他们使用了无监督的深层信任网络来捕获 CAN 数据的基本统计特征，并使用它们将消息分类为正常或异常，结果显示了99%的检出率，同时通过软件模拟可将误报率保持在 1%-2%以下。

这些研究表明，车辆的入侵检测具有多重 CAN 和车辆 ECU 特征。因为有些方法还没有经过评估，所以很难确定哪种方法更好，但最佳方法可能是其中一些方法的组合。

5 结论

本文研究了将 IDSs 应用于汽车系统安全的方法，对这些技术进行了概述并讨论了它们的优缺点。从技术角度看，IDSs 可以很好地检测到 CAN 总线上的入侵，不同的异常检测方法可以检测到不同类型的异常，目前的方法主要集中在消息注入攻击检测上，它是攻击者常用的攻击手段。

随着 FlexRay、局域网(LIN)和以太网等通信协议的引入，车载网络的复杂性不断增加，这些新的协议为车辆引入了新的漏洞。下一步的工作应该研究这些的 IDS 方法是否可以应用于这些新协议。然而随着这一领域的研究不断取得进展，攻击者及其攻击也会不断进步，所以需要不断更新威胁模型以识别新的漏洞和攻击，并对 IDS 进行调整以应对它们。

参考文献

[1] S. Checkoway et al., “Comprehensive experimental analyses of automotive attack surfaces,” in Proc. USENIX Security Symp., 2011.

[2] F. Koushanfar, A. R. Sadeghi, and H. Seudie, “EDA for secure and dependable cybercars: Challenges and opportunities,” in Proc. 49th ACM/EDAC/IEEE Design Autom. Conf., 2012.

[3] T. Zhang, H. Antunes, and S. Aggarwal, “Defending connected vehicles against malware: Challenges and a solution framework,” IEEE Internet Things J., vol. 1, no. 1, pp. 10–21, Feb. 2014.

[4] S. Corrigan, “Introduction to the Controller Area Network (CAN),” Texas Instruments Application Report, 2016.

[5] B. Carnevale et al., “An implementation of the 802.1AE MAC Security Standard for in-car networks,” in IEEE Proc. 2nd World Forum Internet Things, Dec. 2015.

[6] P. Mundhenk et al., “Lightweight authentication for secure automotive networks,” in IEEE Proc. 2015 Design Autom. Test Euro. Conf. Exhibition, 2015.

[7] C.-W. Lin and A. Sangiovanni-Vincentelli, “Cyber-security for the controller area network (CAN) communication protocol,” in IEEE Proc. Int. Conf.Cyber Security, 2012.

[8] K. Koscher et al., “Experimental security analysis of a modern automobile,” in IEEE Proc. Symp. Security Privacy, 2010.

[9] C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle,” BlackHat USA, 2015.

[10] D. Puthal et al., “Building security perimeters to protect network systems against cyber threats,” IEEE Consum. Electron. Mag., vol. 6, no. 4, Oct. 2017.

[11] F. M. Tabrizi and K. Pattabiraman, “Flexible intrusion detection systems for memory-

constrained embedded systems," in IEEE Proc. Depend. Comput. Conf., 2015, pp. 1–12.
[12] M.-K. Yoon et al., "Securecore: A multicore-based intrusion detection architecture for real-time embedded systems," in IEEE Proc. Real-Time Embedded Technol. Appl. Symp., 2013, pp. 21–32.
[13] C. Zimmer et al., "Time-based intrusion detection in cyber-physical systems," in IEEE Proc. 1st ACM/IEEE Int. Conf. Cyber Phy. Syst., 2010.
[14] L. Portnoy, E. Eskin, and S. Stolfo, "Intrusion detection with unlabeled data using clustering," in IEEE Proc. ACM Workshop Data Mining Appl. Secur., 2001.
[15] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network," in IEEE Proc. Int. Conf. Inf. Netw., 2016.
[16] C. Miller and C. Valasek, A Survey of Remote Automotive Attack Surfaces, 2014.
[17] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive can networks—Practical examples and selected short-term countermeasures," SAFECOMP, 2008.
[18] M. Gmiden, H. Mohamed, and H. Trabelsi, "An intrusion detection method for securing in-vehicle CAN bus," in Proc. Sci. Tech. Autom. Cont. Comput. Eng., 2016.
[19] M. Moore et al., "Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks," in IEEE Proc. 12th Ann. Conf. Cyber Inf. Security Res., 2017.
[20] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in IEEE Proc. Intell. Veh. Symp., 2008, pp. 220–225.
[21] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in IEEE Proc. USENIX Security Symp., 2016.
[22] H. Ji et al., "Investigating the effects of attack detection for in-vehicle networks based on clock drift of ecus," in Proc. IEEE Access, 2018.
[23] W. Choi et al., "Voltageids: Low-level communication characteristics for automotive intrusion detection sys-tem," in Proc. IEEE Trans. Inf. Forensics Security, 2018.
[24] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in 2011 IEEE Intell. Veh. Symp., Jun. 2011, pp. 1110–1115.
[25] M. Marchetti et al., "Evaluation of anomaly detection for in-vehicle networks through information- theoretic algorithms," in IEEE Proc. Int. Forum Res. Technol. Soc. Ind. Leveraging a Better Tomorrow, 2016.
[26] T. Matsumoto et al., "A method of preventing unauthorized data transmission in controller area network," in IEEE Proc. Veh.Techn. Conf., 2012, pp. 1–5.
[27] M. Markovitz and A. Wool, "Field classification, modeling and anomaly detection in unknown can bus networks," in IEEE Proc. Veh. Commun., 2017.
[28] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in IEEE Proc. Inf. Assurance Security, 2010.
[29] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," PLoS One, vol. 11, no. 6, 2016.
[30] S. Otsuka et al., CAN Security: Cost-Effective Intrusion Detection for Real-Time Control Systems, Tech. Rep., 2014.