(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109257358 B
(45)授权公告日 2020.08.04

(21)申请号 201811137466.0

(22)申请日 2018.09.28

(65)同一申请的已公布的文献号
申请公布号 CN 109257358 A

(43)申请公布日 2019.01.22

(73)专利权人 成都信息工程大学
地址 610225 四川省成都市西南航空港经济开发区学府路一段24号

(72)发明人 李飞 廖祖奇 张鹏飞

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 谈杰

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 108200042 A,2018.06.22
CN 108521410 A,2018.09.11
CN 106792681 A,2017.05.31
CN 105871830 A,2016.08.17
CN 106059987 A,2016.10.26
CN 107454117 A,2017.12.08
WO 2017173087 A2,2017.10.05
张子键等,.“一种应用于CAN总线的异常检测系统”,.《信心安全与通信保密》.2015,(第8期),第92-96页.

审查员 陈赞

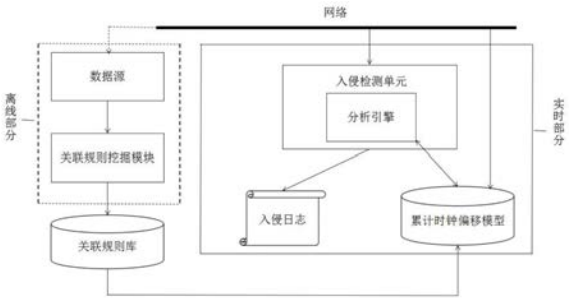
权利要求书2页 说明书11页 附图4页

(54)发明名称

一种基于时钟偏移的车载网络入侵检测方法及系统

(57)摘要

本发明属于汽车网络通信及其汽车安全技术领域,公开了一种基于时钟偏移的车载网络入侵检测方法及系统,挖掘车载网络中各个ECU之间的关联方式以及关联度,找到这些ECU的一些关联信息,并分析出关联信息的规律,建立关联规则;将建立的关联规则正常的数据加入汽车的累计时钟偏移模型;当ECU接收报文出现异常时,通过对比相关的关联数据,发现入侵行为。本发明利用CUSUM(累计和)算法,从目标值的偏差的累计和来检测突变;因为采用累计的方法,即使是轻微地偏离目标值也会持续地增加或减少累加值。因此,它是最佳的检测小的持久性变化的方法,目前已广泛用于变点检测。



CN 109257358 B

1.一种基于时钟偏移的车载网络入侵检测方法,其特征在于,所述基于时钟偏移的车载网络入侵检测方法包括:挖掘车载网络中各个ECU之间的关联方式以及关联度,找到ECU的关联信息,并分析出关联信息的规律,建立关联规则;将建立的关联规则正常的数据加入汽车的累计时钟偏移模型;

当ECU接收报文出现异常时,通过对比相关的关联数据,发现入侵行为;

建立关联规则中,利用消息的周期性去提取和估计发送器的时钟偏差,时钟偏差作为ECU的标记;具体包括:

先从安全的标准网络中采集数据,获得一个数据源;

再从数据源中挖掘出各个ECU之间的关联度,得到ECU之间的固定时钟偏差,

再将这些固定的ECU时钟偏差作为标准放入关联标准库中;

将固定的ECU时钟偏差作为标准放入关联标准库中,需先对时钟偏差进行估计与分析;

具体包括:

假设ECUA每隔Tms广播一条报文消息,ECU R周期性地接受那条报文消息;从R的角度,把报文消息到达的那一刻的时钟看成C_{true};当t=0时,表示ECUA发送第一条报文消息,O_i表示ECUA从t=0时发送第i条报文消息的时钟偏移;

在一段网络延迟d_i过后,ECU R将会接受相应的报文消息并记录到达的时间戳$iT+O_i+d_i+n_i$,其中n_i表示R的时间戳量化时产生的噪音;每个到达时间戳的时钟间隔用$T_{rx,i}=T+\Delta O_i+\Delta d_i+\Delta n_i$表示,其中$\Delta X_i$表示第i个与i-1个变量$X_i$之间的差值并且规定$O_0=0$;在一小段时间内,$O_i$变化很微小,忽略不计,$n_i$是一个零均值高斯噪声项,T是通过关联数据挖掘得到的的常数,周期性报文信息的数据长度DLC又是一个常量,$E[\Delta di]=0$,间隔的期望值用公式(1)表示:

$$\begin{aligned}&\mu_{Trx}=E[T_{rx,i}]\\&\mu_{Trx}=E[T+\Delta O_i+\Delta d_i+\Delta n_i]\\&\mu_{Trx}=T+E[\Delta O_i+\Delta d_i+\Delta n_i]\\&\mu_{Trx}\approx T\end{aligned}\quad(1)$$

基于第一条报文消息到达的时间戳d_0+n_0和时间戳间隔的期望值μ_{Trx},推断第i条报文信息到达时的时间戳为$i\mu_{Trx}+d_0+n_0$,实际测量到达时间戳为$iT+O_i+d_i+n_i$;通过估计到达的时间,μ_{Trx}由过去的测量值决定;T是一个常量并且$\mu_{Trx}\approx T$,估计值与真实测量值之间的差的期望值用公式(2)表示:

$$E[D]=E[i(T-\mu_{Trx})+O_i+\Delta d+\Delta n]\approx E[O_i]\quad(2)$$

从报文的周期性角度估计出不同发送器的时钟偏移$E[O_i]$。

2.如权利要求1所述的基于时钟偏移的车载网络入侵检测方法,其特征在于,当ECU接收报文出现异常时,通过对比相关的关联数据,发现入侵行为,具体包括:

利用关联规则库里的关联规则在量上的值,构建累计时钟偏移模型,作为与异常行为的校对标准,实时对车载网络里的数据进行检测,判别是否存在入侵行为;

对于给定ID的报文消息,运行RLS算法去估计相应ECU发送器的时钟偏差,构建相应的标准的时钟行为模型并验证测量值是否偏离正常值;利用CUSUM累计和算法,从目标值的偏差的累计和检测突变。

3.如权利要求2所述的基于时钟偏移的车载网络入侵检测方法,其特征在于,

CUSUM累计和算法包括：

在估计时钟偏差的每一步过程中，分别地更新累计时钟偏移的平均值μ_e和识别误差的方差σ_e^2；μ_e和σ_e^2只有当满足$\left|\frac{e-\mu_e}{\sigma_e}\right|<3$时，才被更新；每个得到的识别误差e以及累计和的上限L^+，下限L^-更新如公式(3)所示；

$$L^+ \leftarrow \max[0, L^+ + (e-\mu_e)\div\sigma_e - \kappa]$$
$$L^- \leftarrow \max[0, L^- - (e-\mu_e)\div\sigma_e - \kappa] \quad (3)$$

其中κ是一个反映标准偏差的参数并且κ通过监视正常车载网络情况从而离线训练得出；如果L^+或者L^-的任何一个超出了阈值Γ_L，突然改变的值都会分别被察觉出，报告有入侵；累计和的方式阈值为4或5。

4.一种实现权利要求1～3任意一项所述基于时钟偏移的车载网络入侵检测方法的信息数据处理终端。

5.一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行如权利要求1-3任意一项所述的基于时钟偏移的车载网络入侵检测方法。

6.一种实现权利要求1～3任意一项所述基于时钟偏移的车载网络入侵检测方法的基于时钟偏移的车载网络入侵检测系统，其特征在于，所述基于时钟偏移的车载网络入侵检测系统包括：

关联规则建立模块，挖掘车载网络中各个ECU之间的关联方式以及关联度，找到这些ECU的一些关联信息，并分析出关联信息的规律，建立关联规则；

累计时钟偏移模型构建模块，将建立的关联规则正常的数据加入汽车的累计时钟偏移模型；

入侵检测模块，当ECU接收报文出现异常时，通过对比相关的关联数据，发现入侵行为。

7.一种搭载有权利要求6所述基于时钟偏移的车载网络入侵检测系统的车载网络变点检测设备。

一种基于时钟偏移的车载网络入侵检测方法及系统

技术领域

[0001] 本发明属于汽车网络通信及其汽车安全技术领域，尤其涉及一种基于时钟偏移的车载网络入侵检测方法及系统。

背景技术

[0002] 目前，业内常用的现有技术是这样的：

[0003] 随着现代信息科学技术和汽车技术的融合，目前汽车的控制都是基于ECU(Electronic Control Unit:电子控制单元)的控制，并且汽车的发展趋势是越来越数字化、智能化、无人化。由于汽车各个设备器件的功能都是由ECU控制，不同的汽车型号根据需求的不同，ECU的数量也是不同的，但通常情况下汽车内平均含有20个到100个ECU，每个ECU负责自己相应器件设备的功能。目前，汽车车载网络中占主导作用的总线是CAN总线，自1986年德国博世公司开发出面向汽车的CAN总线通信协议开始，CAN总线成为了汽车车载网络的标准。由于车载网络里普遍应用最多的是标准车载网络是CAN总线网络，所以本发明是基于CAN总线网络对于ECU入侵检测的研究。

[0004] BOSCH公司在设计CAN总线之初考虑的只是为了实现功能，而没有考虑车载网络的信息方面的安全性问题。例如CAN总线网络不安全性的方面表现在，CAN总线协议规则只规定了CAN报文的协议内容和报文格式，并且CAN总线上的数据没有通过加密的措施，而是通过明文的方式来进行传输，同时CAN总线也没有相应的身份验证机制，只要挂载到CAN总线上的设备，就可以给其他的设备发送消息，因此CAN总线很容易被黑客进行攻击和监听。最近几年来针对车载网络的攻击，国外已有一些白帽黑客通过实际案例进行了实证。

[0005] 车内T-Box系统是通过在汽车的内部集成了GPS定位模块、RFID(射频技术)识别模块、传感器模块等电子元件，根据通信协议和数据交换的标准，进行无线通信和数据交换的系统，也是实现车辆智能化控制和智能动态信息服务的关键部件。黑客攻击T-Box，可以实现了对汽车的本地和远程控制，通过向CAN总线发送相关命令，可以使行驶的车辆断油、加速、减速和制动。本发明可以及时发现来自T-Box的攻击。

[0006] 车载娱乐系统可以包含导航、辅助驾驶、故障检测、车身控制、基于在线的娱乐功能等，极大的提升了汽车的电子化、网络化和智能化水平。车载娱乐系统由于通过无线可以连接外部，因此也是黑客攻击的重点对象。通过攻击车载娱乐系统，然后向CAN总线发送相关命令，也可以使行驶的车辆变向、断油、加速、减速和制动等。因此本发明可以及时发现来自车载娱乐系统的攻击

[0007] 综上所述，现有技术存在的问题是：

[0008] (1)现有技术中，没有考虑车载网络的信息方面的安全性问题。

[0009] CAN总线上的数据没有通过加密的措施，只是通过明文的方式来进行传输；同时CAN总线也没有相应的身份验证机制，只要挂载到CAN总线上的设备，就可以给其他的设备发送消息，因此CAN总线很容易被黑客进行攻击和监听。

[0010] (2)现有技术中由于T-Box没有防护措施，容易遭受来自互联网的黑客攻击，进而

攻击CAN总线，导致行驶的汽车出现异常现象。

[0011] (3)现有技术中由于车载娱乐系统没有防护措施，容易遭受来自互联网的黑客攻击，进而攻击CAN总线，导致行驶的汽车出现异常现象。

[0012] 解决上述技术问题的难度和意义：

[0013] 难度在于，对汽车车载网络信息安全问题不能进行妥善的解决；原因在于，

[0014] 由传统汽车向数字化、智能化、无人化汽车演变的过程中，汽车车载网络的信息安全问题不可忽视，因为汽车车载网络的信息安全问题跟互联网信息安全问题相比较，汽车车载网络的信息安全导致的危害更重要，一旦汽车车载网络被攻击，不仅会带来财产损失而且严重情况下会威胁车内人员的生命。而且，目前很多汽车的对外通信的防护基本没有，加上汽车对外通信的信道有多种。

[0015] 解决现有技术的问题后，带来的意义为：，针对汽车车载网络的攻击，本发明在CAN总线上，通过数据包的时钟偏移，可以及时发现攻击行为，进行入侵检测，有助于保障整个汽车载体的安全，进而保障生命和财产的安全。

发明内容

[0016] 针对现有技术存在的问题，本发明提供了一种基于时钟偏移的车载网络入侵检测方法及系统，本发明很好的解决了上述问题，并增强了汽车内部网络的安全性，也提高了汽车网络中入侵检测的能力。

[0017] 本发明是这样实现的，一种基于时钟偏移的车载网络入侵检测方法，所述基于时钟偏移的车载网络入侵检测方法包括：挖掘车载网络中各个ECU之间的关联方式以及关联度，找到这些ECU的一些关联信息，并分析出关联信息的规律，建立关联规则；将建立的关联规则正常的数据加入汽车的累计时钟偏移模型；

[0018] 当ECU接收报文出现异常时，通过对比相关的关联数据，发现入侵行为。

[0019] 进一步，建立关联规则方法中，利用消息的周期性去提取和估计发送器的时钟偏差，时钟偏差作为ECU的标记；具体包括：

[0020] 首先，先从安全的标准网络中采集数据，获得一个数据源；再从数据源中挖掘出各个ECU之间的关联度，得到ECU之间的固定时钟偏差，再将这些固定的ECU时钟偏差作为标准放入关联标准库中。

[0021] 进一步，建立关联规则中，将这些固定的ECU时钟偏差作为标准放入关联标准库中前，需先对时钟偏差进行估计与分析；

[0022] 具体包括：

[0023] 假设ECUA每隔Tms广播一条报文消息，ECU R周期性地接受那条报文消息；从R的角度，把报文消息到达的那一刻的时钟看成C_{true}；当t＝0时，表示ECUA发送第一条报文消息，O_i表示ECUA从t＝0时发送第i条报文消息的时钟偏移；

[0024] 在一段网络延迟d_i过后，ECU R将会接受相应的报文消息并记录到达的时间戳$iT+O_i+d_i+n_i$，其中n_i表示R的时间戳量化时产生的噪音；每个到达时间戳的时钟间隔用$T_{rx,i}=T+\Delta O_i+\Delta d_i+\Delta n_i$表示，其中$\Delta X_i$表示第i个与i-1个变量$X_i$之间的差值并且规定$O_0=0$；在一小段时间内，$O_i$变化很微小，忽略不计，$n_i$是一个零均值高斯噪声项，T是通过关联数据挖掘得到的的常数，周期性报文信息的数据长度DLC又是一个常量，$E[\Delta d_i]=0$，间隔的期望值用

公式(1)表示：

[0025]
$$\begin{aligned}&\mu_{Trx}=E[T_{rx,i}]\\&\mu_{Trx}=E[T+\Delta O_i+\Delta d_i+\Delta n_i]\\&\mu_{Trx}=T+E[\Delta O_i+\Delta d_i+\Delta n_i]\\&\mu_{Trx}\approx T\end{aligned}\quad(1)$$

[0026] 基于第一条报文消息到达的时间戳d_0+n_0和时间戳间隔的期望值μ_{Trx}，推断第i条报文信息到达时的时间戳为$i\mu_{Trx}+d_0+n_0$，实际测量到达时间戳为$iT+O_i+d_i+n_i$；通过估计到达的时间，μ_{Trx}由过去的测量值决定；T是一个常量并且$\mu_{Trx}\approx T$，估计值与真实测量值之间的差的期望值用公式(2)表示：

[0027] $E[D]=E[i(T-\mu_{Trx})+O_i+\Delta d+\Delta n]\approx E[O_i]$ (2)

[0028] 从报文的周期性角度估计出不同发送器的时钟偏移$E[O_i]$。

[0029] 进一步，当ECU接收报文出现异常时，通过对比相关的关联数据，发现入侵行为，具体包括：

[0030] 利用关联规则库里的关联规则在量上的值，构建累计时钟偏移模型，作为与异常行为的校对标准，实时对车载网络里的数据进行检测，判别是否存在入侵行为；

[0031] 对于给定ID的报文消息，运行RLS算法去估计相应ECU发送器的时钟偏差，构建相应的标准的时钟行为模型并验证测量值是否偏离正常值；利用CUSUM累计和算法，从目标值的偏差的累计和检测突变。

[0032] 进一步，CUSUM累计和算法包括：

[0033] 在估计时钟偏差的每一步过程中，分别地更新累计时钟偏移的平均值μ_e和识别误差的方差σ_e^2；μ_e和σ_e^2只有当满足$\left|\frac{e-\mu_e}{\sigma_e}\right|<3$时，才被更新；，每个得到的识别误差e以及累计和的上限L^+，下限L^-更新如公式(3)所示；

[0034]
$$\begin{aligned}&L^+\leftarrow\max[0,L^++(e-\mu_e)\div\sigma_e-\kappa]\\&L^-\leftarrow\max[0,L^--(e-\mu_e)\div\sigma_e-\kappa]\end{aligned}\quad(3)$$

[0035] 其中κ是一个反映标准偏差的参数并且κ通过监视正常车载网络情况从而离线训练得出；如果L^+或者L^-的任何一个超出了阈值Γ_L，突然改变的值都会分别被察觉出，报告有入侵；累计和的方式阈值为4或5，或根据实际情况设置阈值。

[0036] 本发明的另一目的在于提供一种实现所述基于时钟偏移的车载网络入侵检测方法的计算机程序。

[0037] 本发明的另一目的在于提供一种实现所述基于时钟偏移的车载网络入侵检测方法的信息数据处理终端。

[0038] 本发明的另一目的在于提供一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行所述的基于时钟偏移的车载网络入侵检测方法。

[0039] 本发明的另一目的在于提供一种实现所述基于时钟偏移的车载网络入侵检测方法的基于时钟偏移的车载网络入侵检测系统，所述基于时钟偏移的车载网络入侵检测系统包括：

[0040] 关联规则建立模块，挖掘车载网络中各个ECU之间的关联方式以及关联度，找到这些ECU的一些关联信息，并分析出关联信息的规律，建立关联规则；

[0041] 累计时钟偏移模型构建模块，将建立的关联规则正常的数据加入汽车的累计时钟

偏移模型；

[0042] 入侵检测模块，当ECU接收报文出现异常时，通过对比相关的关联数据，发现入侵行为。

[0043] 本发明的另一目的在于提供一种搭载有所述基于时钟偏移的车载网络入侵检测系统的车载网络变点检测设备。

[0044] 综上所述，本发明的优点及积极效果为：

[0045] 本发明为了建立一个有效的入侵检测方法并且能够识别出各种类型的攻击，系统应该能够验证每条消息的发送器。然而，CAN报文信息中是不包含发送器信息的，所以必须用其他信息来标记。本发明利用消息的周期性去提取和估计发送器的时钟偏差，即把这个时钟偏差作为ECU的标记。

[0046] 首先，先从安全的标准网络中采集数据，获得一个数据源。再从数据源中挖掘出各个ECU之间的关联度，得到ECU之间的固定时钟偏差，再将这些固定的ECU时钟偏差作为标准放入关联标准库当中，这样就是一个完整的离线部分的设计。

[0047] 因为要用ECU的时钟偏差来进行标记，所以首先需要对时钟偏差进行估计与分析。在真实系统中影响时钟偏差的因素有时钟偏移、网络传输延时、时间戳量化时产生的噪音，由于这些因素对于消息的周期来说都很小，可以忽略不计。

[0048] 实时部分设计

[0049] 离线部分已经解决了标记ECU发送器的问题，即通过报文消息之间的时间间隔得出时钟偏差可以用来标记ECU发送器。本发明利用这个特征设计了累计时钟偏移模型和入侵检测单元两大模块，其中入侵检测单元包含了一个判断是否属于入侵行为的分析引擎。

[0050] 实时部分是为了适应汽车车载网络对入侵检测实时的要求而设计的，它的作用是利用关联规则库里的关联规则在量上的值比如报文时间周期性，从而构建累计时钟偏移模型，作为与异常行为的校对标准，从而实时对车载网络里的数据进行检测，从而判别是否存在入侵行为。

[0051] 累计时钟偏移模型构建，相当于建立一个标准库，也就是俗称的白名单，只有符合这个模型的期望数据值才能通过入侵检测。

[0052] 入侵检测则是将实时数据与离线部分的所挖掘出的固有值(即ECU的时钟偏差)进行比对，如果与期望的ECU时钟偏差出现较大差异，那么可以判定异常或者有入侵行为(如：注入攻击、暂停攻击、伪装攻击等)。

[0053] 考虑到恶意攻击者对以固定周期发送报文信息的ECU进行注入攻击，注入攻击会显著增加估计和测量到达时钟之间的绝对平均差值。其结果就是累计时钟偏移量的变化率会突然增加，识别误差也会很大。类似的是暂停攻击也会让绝对平均值增加，也会产生很高的误差。如果存在伪装攻击，因为恶意攻击者通过恶意的ECU发送报文消息而不是原本的ECU发送报文消息，累计时钟偏移即时钟偏差的增加率会突然变化，从而也导致很高的识别误差。总之，当ECU不是恶意的话，那么它也相应具有标准的时钟行为，那么它的识别误差的平均值通常趋于0，当有入侵时，它的值会突然变成非0值。

[0054] 本发明的入侵检测方法这里利用CUSUM(累计和)算法，从目标值的偏差的累计和来检测突变。因为采用累计的方法，即使是轻微地偏离目标值也会持续地增加或减少累加值。因此，它是最佳的检测小的持久性变化的方法，目前已广泛用于变点检测。

[0055] 本发明的仿真验证有：

[0056] 在入侵检测验证这个环节，本发明采用的实验软件是CANoe7.1，这款软件工具不仅具有仿真车载网络ECU发送和接收的过程，而且也可以与真实的车载网络相连进行真实的操作。

[0057] 注入和暂停攻击入侵检测验证：

[0058] 为了验证注入和暂停攻击，用CANoe软件设计了如图5所示这样的仿真网络，其中，首先为了验证注入攻击，向ECU B中编入程序，让它在时钟为400s的时刻注入以ID为0x11的报文消息，但实际上如果没有注入攻击的话，0x11的报文消息应该是由ECU A周期性发送的，也就是说ECU B对ECU A进行了注入攻击。同时，也让ECU R中编入我们的入侵检测程序，把它作为入侵检测系统的一个检测点，让它去推导0x11报文消息的累积时钟偏移(O_{acc})，识别误差(e)以及目标值的累积上下限L^+,L^-。对于暂停攻击来说的话，ECU A可以编入暂停的程序，使它在400s的时刻暂停发送0x11的报文消息。如图6(a)展示了在有注入攻击和没有注入攻击的情况下，O_{acc}，e等这些值是怎样变化的。只要ECU B发动了注入攻击，那么累积时钟偏移就会有一个突变点，从而也会产生一个较大的识别误差。由于这样的变化，目标值累积和的上限L^+也突增并且超过了阈值Γ_L，从而可以判定发生了入侵。同理，图6(b)也展示了暂停攻击的情况下，累积时钟偏移也会突增，从而也可以判定发生了入侵行为。

[0059] 伪装攻击入侵检测验证：

[0060] 伪装攻击用CANoe设计了如图7所示的仿真网络。其中ECU A扮演强攻击者的角色，ECU B扮演弱攻击者的角色，ECU C作为非攻击者的角色，ECU R作为入侵检测系统的检测点。其中ECU A没被植入恶意程序时，默认它是发送0x11的报文消息，ECU A编入恶意程序使它在T_{masq}为250秒的时候伪装发送ID为0x55报文消息的ECU B，也即中断ECU B发送报文消息，反而让ECU A代替ECU B发送相同ID的报文消息。

[0061] 如图8(a)展示了攻击前和攻击后，ID为0x55的报文消息的PMF(概率质量函数)。在ECU A伪装过后，还是以ECU B同样的频率发送报文消息，因此，相当于攻击前，分布没有明显的偏离。然而，因为在T_{masq}时刻的时候，发送0x55的报文消息的ECU B被阻止了，由ECU A代替发送，在ECU切换的过程中会有一段延迟时钟。从图中可以看出在没发动伪装攻击时，报文消息之间的时钟间隔是50ms，然而在第一次发动伪装攻击时，相对于发动伪装攻击前一次发送的报文消息结束时，此时报文消息的时钟间隔为51.04ms。由于在T_{masq}出现了伪装攻击，PMF图中就显示出了偏离正常情况下的异常的报文消息时钟间隔。由此，这种变化也导致了检测点ECU R跟踪的O_{acc},L^+,L^-的变化，如图8(c)所示。从图8(b)可以看出，在250秒的时候，由于发动了伪装攻击，所以造成了0x55报文消息累积时钟偏移的斜率产生了变化也即时钟偏差产生了变化。由于在T_{masq}过后，O_{acc}的测量值相对于T_{masq}之前正常情况下的期望值产生了明显的偏离并且目标值的累积和下限也超出了阈值，从而入侵检测系统可以报告这是一次入侵。由于在T_{masq}之后，发送ID为0x55的报文消息的ECU变成了A，它的时钟偏差与0x11的时钟偏差相等，从而也可进一步判定攻击源为A。

附图说明

[0062] 图1是本发明实施例提供的报文消息到达时序分析图。

[0063] 图2是本发明实施例提供的累计时钟偏移图。

[0064] 图3是本发明实施例提供的时钟偏差估计算法流程图。

[0065] 图4是本发明实施例提供的入侵检测方法流程图。

[0066] 图5是本发明实施例提供的注入攻击和暂停攻击仿真网络图。

[0067] 图6是本发明实施例提供的入侵检测系统检测注入攻击和暂停攻击图。

[0068] 图中：(a)注入攻击；(b)缓冲攻击。

[0069] 图7是本发明实施例提供的伪装攻击网络仿真网络图。

[0070] 图8是本发明实施例提供的入侵检测系统检测伪装攻击图。

具体实施方式

[0071] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0072] 现有技术中，没有考虑车载网络的信息方面的安全性问题。

[0073] CAN总线上的数据没有通过加密的措施，只是通过明文的方式来进行传输；同时CAN总线也没有相应的身份验证机制，只要挂载到CAN总线上的设备，就可以给其他的设备发送消息，因此CAN总线很容易被黑客进行攻击和监听。

[0074] 下面结合具体分析对本发明作进一步描述。

[0075] 本发明实施例提供的基于时钟偏移的车载网络入侵检测方法，包括：

[0076] 首先挖掘车载网络中各个ECU之间的关联方式以及关联度，找到这些ECU的一些关联信息，并分析出其中的规律，建立关联规则，将这些正常的数据加入汽车的白名单。当ECU接收报文出现异常时，通过对比相关的关联数据，则可以发现入侵行为，从而避免安全问题的发生。

[0077] 1)其中，关联规则，包括：

[0078] 以油门踏板ECU、节气门ECU、转速ECU、车速ECU为例。从实际层面出发这4个ECU存在相互关联的关系(油门踏板的变化造成节气门的变化，节气门的变化造成发动机转速的变化，发动机转速的变化造成车速的变化)。并且根据多次的实验，发现车载网络内部大多数ECU都存在单一线性关联关系，并且ECU发送报文信息都存在时间间隔的周期特性。从而设计出每个ECU之间的关联规则。

[0079] 2)入侵检测方法原理：

[0080] 对于挂载在CAN总线网络上的ECU传输报文信息的频率是由它们自己的晶振时钟所决定的。这里本发明采用了NTP(网络时间协议)命名规范，用C_{true}表示ECU通过数据关联挖掘后得到的接收信号的期望时间，用C_i表示ECU实际接收到信号的时间。定义了时钟偏移、时钟增量、时钟偏差这些术语。

[0081] 时钟偏移：一段时间内，C_{true}与C_i的差异。

[0082] 时钟增量：一段时间内，C_i的改变量。

[0083] 时钟偏差：一段时间内，累计时钟偏移与这段时间的比值。

[0084] 为了建立一个有效的入侵检测方法并且能够识别出各种类型的攻击，系统应该能够验证每条消息的发送者信息。然而，CAN报文信息中是不包含发送信息的，所以必须用其他信息来标记。本发明利用消息的周期性去提取和估计发送器的时钟偏差，即把这个时钟

偏差作为ECU的标记。

[0085] 如图1所示，假设ECU A每隔Tms广播一条报文消息，ECU R周期性地接受那条报文消息。从R的角度来看，只有报文消息到达它那一时刻的时间戳可以利用，所以可以把报文消息到达的那一刻的时钟看成C_{true}。由于时钟偏差，有时在发送周期性的报文消息的时候会与理想的时钟(T,2T,3T…)产生微小的时钟偏移。当t＝0时，表示ECU A发送第一条报文消息，O_i表示ECU A从t＝0时发送第i条报文消息的时钟偏移。然后，在一段网络延迟d_i过后，ECU R将会接受相应的报文消息并记录到达的时间戳$iT+O_i+d_i+n_i$，其中n_i表示R的时间戳量化时产生的噪音。因此，每个到达时间戳的时钟间隔可以用$T_{rx,i}=T+\Delta O_i+\Delta d_i+\Delta n_i$表示，其中$\Delta X_i$表示第i个与i-1个变量$X_i$之间的差值并且规定$O_0=0$。由于在一小段时间内，$O_i$变化很微小，可以忽略不计，$n_i$是一个零均值高斯噪声项，T是通过关联数据挖掘得到的的常数，周期性报文信息的数据长度DLC又是一个常量，即$E[\Delta d_i]=0$，所以间隔的期望值可以用公式(1)表示：

[0086]
$$\begin{aligned}&\mu_{Trx}=E[T_{rx,i}]\\&\mu_{Trx}=E[T+\Delta O_i+\Delta d_i+\Delta n_i]\\&\mu_{Trx}=T+E[\Delta O_i+\Delta d_i+\Delta n_i]\\&\mu_{Trx}\approx T\end{aligned}\quad(1)$$

[0087] 基于第一条报文消息到达的时间戳d_0+n_0和时间戳间隔的期望值μ_{Trx}，从而可以推断第i条报文信息到达时的时间戳应该为$i\mu_{Trx}+d_0+n_0$，而实际测量到达时间戳为$iT+O_i+d_i+n_i$。正如估计到达的时间，μ_{Trx}是由过去的测量值决定的。因为T是一个常量并且$\mu_{Trx}\approx T$，所以估计值与真实测量值之间的差的期望值可以用公式(2)表示：

[0088] $E[D]=E[i(T-\mu_{Trx})+O_i+\Delta d+\Delta n]\approx E[O_i]$ (2)

[0089] 也即从报文的周期性角度本发明可以估计出不同发送器的时钟偏移$E[O_i]$，因为时钟偏移的变为很缓慢并且非零，$E[O_i]\neq 0$，而$E[\Delta O_i]=0$。从而以此为依据作为区分不同的发送器。如果把ECU R接受到的n条报文信息去估计平均时钟偏移量的话，则仅仅代表了新产生的平均时钟偏移，因为接受的报文信息都是由第一条报文消息派生出来的。因此，为了获得全部产生的时钟偏移，则需要把平均时钟偏移进行累加。根据定义，累加的时钟偏移应该是一个常量而且累计的时钟偏移的倾斜程度表示了相应的时钟偏差。

[0090] 如图2累计时钟偏移图所示，本发明用时钟偏差估计去验证了标记ECU的有效性，验证采用的数量级是ppm(百万分之几)。分别用了0x11,0x13,0x55报文消息的累计时钟偏移去作图，其中图中曲线倾斜的程度代表了相应的时钟偏差。通过图中可以看出，所有时钟偏移得到的曲线都是一条直线，从而相应的时钟偏差应该是一个常量。报文消息0x11,0x13都是从ECU A发送的，它们的报文消息时钟偏移曲线几乎是重合的而且时钟偏差为11.4ppm(最小二乘法得到)。另一方面，报文消息0x55是由ECU B发送的并且时钟偏差为25.2ppm。因此，时钟偏差的确可以区分不同的ECU。

[0091] 上面已经解决了标记ECU发送器的问题，即通过报文消息之间的时间间隔得出时钟偏差可以用来标记ECU发送器。

[0092] 本发明利用这个特征设计了累计时钟偏移模型和入侵检测单元两大模块，其中入侵检测单元包含了一个判断是否属于入侵行为的分析引擎。下面对这两大模块进行详细描述。

[0093] 通过前面的铺垫,对于给定的ID的报文消息,可以通过接受报文消息时间戳得出相应的累计时钟偏移。由于时钟偏差是恒定的,所以累计时钟偏移呈线性回归分布。因此,入侵检测方法可以把累计时钟偏移模型建模为线性回归模型。其相应的线性回归模型定义用公式(3)表达:

[0094] $O_{acc}[k]=S[k]\cdot t[k]+e[k]$ (3)

[0095] 其中k表示k个阶段,$O_{acc}[k]$表示在k个阶段的累计时钟偏移,t[k]表示在k个阶段消耗的时间,S[k]表示线性回归模型的斜率也是要估计的时钟偏差,e[k]表示识别误差即不能被模型解释的残差。其中O_{acc},S,t,e会随着每N个报文消息数目的改变而进行更新,直到达到本发明预期设定的k。

[0096] 本发明为了获得累计时钟偏移模型未知参数S,使用了最小二乘法(RLS)算法为基础设计了时钟偏差估计算法程序和图3的时钟偏差估计算法流程。其中以残差为目标函数,目的是最小化建模误差的平方和。因此在RLS算法中,识别误差的偏差最好趋近于0,这样能更精确的表达模型。

[0097] 算法描述了怎样使用RLS算法去估计时钟偏差。首先,入侵检测方法测量给定ID的报文消息的接受时的时间戳以及利用关联规则库里报文消息之间的时间周期值。如果长期没有收到预期的报文消息,那么很可能是暂停攻击,如图3的13,14行所示,那么势必造成剩余的时间戳和时间间隔增大。一旦N个值被测量完,入侵检测方法就可以决定累计时钟偏移和相应的识别误差。基于导出的值,那么增益G和协方差P就可以用RLS算法去更新线性回归模型参数S即时钟偏差。时钟偏差估计的这个过程是一个迭代的过程,如果ECU没有被攻击的话,那么输出的识别误差应该趋近于0而且时钟偏差也应该是一个常量。这样,ECU发送器的标准时钟行为可以被描述为时钟偏差为线性回归模型的斜率。在RLS算法中,为了保证样本的新鲜度,以指数的方式给出遗忘因子λ,目的是给予老样本较少的权重,本发明把λ的值设为0.9995。

[0098] 下面结合入侵检测方法对本发明作进一步描述。

[0099] 基于上述分析设计入侵检测方法如图4所示。该入侵检测方法分离线部分和实时部分。

[0100] 1.离线部分设计(关联建立)

[0101] 为了建立一个有效的入侵检测方法并且能够识别出各种类型的攻击,系统应该能够验证每条消息的发送器。然而,CAN报文信息中是不包含发送器信息的,所以必须用其他信息来标记。本发明利用消息的周期性去提取和估计发送器的时钟偏差,即把这个时钟偏差作为ECU的标记。

[0102] 首先,先从安全的标准网络中采集数据,获得一个数据源。再从数据源中挖掘出各个ECU之间的关联度,得到ECU之间的固定时钟偏差,再将这些固定的ECU时钟偏差作为标准放入关联标准库当中,这样就是一个完整的离线部分的设计。

[0103] 因为要用ECU的时钟偏差来进行标记,所以首先需要对时钟偏差进行估计与分析。在真实系统中影响时钟偏差的因素有时钟偏移、网络传输延时、时间戳量化时产生的噪音,由于这些因素对于消息的周期来说都很小,可以忽略不计。

[0104] 2.实时部分设计

[0105] 离线部分已经解决了标记ECU发送器的问题,即通过报文消息之间的时间间隔得

出时钟偏差可以用来标记ECU发送器。本发明利用这个特征设计了累计时钟偏移模型和入侵检测单元两大模块，其中入侵检测单元包含了一个判断是否属于入侵行为的分析引擎。

[0106] 实时部分是为了适应汽车车载网络对入侵检测实时的要求而设计的，它的作用是利用关联规则库里的关联规则在量上的值比如报文时间周期性，从而构建累计时钟偏移模型，作为与异常行为的校对标准，从而实时对车载网络里的数据进行检测，从而判别是否存在入侵行为。

[0107] 累计时钟偏移模型构建，相当于建立一个标准库，也就是俗称的白名单，只有符合这个模型的期望数据值才能通过入侵检测。

[0108] 入侵检测则是将实时数据与离线部分的所挖掘出的固有值(即ECU的时钟偏差)进行比对，如果与期望的ECU时钟偏差出现较大差异，那么可以判定异常或者有入侵行为(如：注入攻击、暂停攻击、伪装攻击等)。

[0109] 考虑到恶意攻击者对以固定周期发送报文信息的ECU进行注入攻击，注入攻击会显著增加估计和测量到达时钟之间的绝对平均差值。其结果就是累计时钟偏移量的变化率会突然增加，识别误差也会很大。类似的是暂停攻击也会让绝对平均值增加，也会产生很高的误差。如果存在伪装攻击，因为恶意攻击者通过恶意的ECU发送报文消息而不是原本的ECU发送报文消息，累计时钟偏移即时钟偏差的增加率会突然变化，从而也导致很高的识别误差。总之，当ECU不是恶意的话，那么它也相应具有标准的时钟行为，那么它的识别误差的平均值通常趋于0，当有入侵时，它的值会突然变成非0值。

[0110] 3.分析引擎

[0111] 对于给定ID的报文消息，入侵检测方法运行RLS算法去估计相应ECU发送器的时钟偏差，从而也构建了相应的标准的时钟行为模型并验证测量值是否偏离了正常值，即入侵。考虑到恶意攻击者对以固定周期发送报文信息的ECU进行注入攻击，注入攻击会显著增加估计和测量到达时钟之间的绝对平均差值。其结果就是累计时钟偏移量的变化率会突然增加，识别误差也会很大。类似的是暂停攻击也会让绝对平均差值增加，也会产生很高的误差。如果存在伪装攻击，因为恶意攻击者通过恶意的ECU发送报文消息而不是原本的ECU发送报文消息，累计时钟偏移即时钟偏差的增加率会突然变化，从而也导致很高的识别误差。总之，当ECU不是恶意的话，那么它也相应具有标准的时钟行为，那么它的识别误差的平均值通常趋于0，当有入侵时，它的值会突然变成非0值。本发明的入侵检测方法这里利用CUSUM(累计和)算法，从目标值的偏差的累计和来检测突变。因为采用累计的方法，即使是轻微地偏离目标值也会持续地增加或减少累加值。因此，它是最佳的检测小的持久性变化的方法，目前已广泛用于变点检测。本发明的入侵检测方法通过累计和方式进行入侵检测的方式如下。

[0112] 由于在估计时钟偏差的每一步过程中，入侵检测方法都要分别地更新累计时钟偏移的平均值μ_e和识别误差的方差σ_e^2，所以这些值代表了e的累计目标值，因此需要适当的追踪这些变量。因此，作为从攻击中产生的异常值的防范措施需要把它反映到目标值，μ_e和σ_e^2只有当满足$\left|\frac{e-\mu_e}{\sigma_e}\right|<3$时，才被更新。然后，每个得到的识别误差e以及累计和的上限L^+，下限L^-更新如公式(3)所示。

[0113] $$\begin{aligned} L^{+} &\leftarrow \max[0, L^{+} + (e - \mu_e) \div \sigma_e - \kappa] \\ L^{-} &\leftarrow \max[0, L^{-} - (e - \mu_e) \div \sigma_e - \kappa] \end{aligned} \quad (3)$$

[0114] 其中κ是一个反映标准偏差的参数并且κ可以通过监视正常车载网络情况从而离线训练得出。如果L^{+}或者L^{-}的任何一个超出了阈值Γ_L，突然改变的值都会分别被察觉出，因此入侵检测方法就可以报告有入侵。一般规律，累计和的方式都有一个阈值，并且阈值通常为4或5，可以根据实际情况设置阈值。

[0115] 下面结合仿真实验对本发明作进一步描述。

[0116] 在入侵检测验证这个环节，本发明采用的实验软件是CANoe7.1，这款软件工具不仅具有仿真车载网络ECU发送和接收的过程，而且也可以与真实的车载网络相连进行真实的操作。

[0117] 1、注入和暂停攻击入侵检测验证

[0118] 为了验证注入和暂停攻击，用CANoe软件设计了如图5所示这样的仿真网络，其中，首先为了验证注入攻击，向ECU B中编入程序，让它在时钟为400s的时刻注入以ID为0x11的报文消息，但实际上如果没有注入攻击的话，0x11的报文消息应该是由ECU A周期性发送的，也就是说ECU B对ECU A进行了注入攻击。同时，也让ECU R中编入我们的入侵检测程序，把它作为入侵检测系统的一个检测点，让它去推导0x11报文消息的累积时钟偏移(O_{acc})，识别误差(e)以及目标值的累积上下限L^{+}，L^{-}。对于暂停攻击来说的话，ECU A可以编入暂停的程序，使它在400s的时刻暂停发送0x11的报文消息。如图6(a)展示了在有注入攻击和没有注入攻击的情况下，O_{acc}，e等这些值是怎样变化的。只要ECU B发动了注入攻击，那么累积时钟偏移就会有一个突变点，从而也会产生一个较大的识别误差。由于这样的变化，目标值累积和的上限L^{+}也突增并且超过了阈值Γ_L，从而可以判定发生了入侵。同理，图6(b)也展示了暂停攻击的情况下，累积时钟偏移也会突增，从而也可以判定发生了入侵行为。

[0119] 图5注入攻击和暂停攻击仿真网络图。

[0120] 图6入侵检测系统检测注入攻击和暂停攻击图。

[0121] 2、伪装攻击入侵检测验证

[0122] 伪装攻击用CANoe设计了如图7所示的仿真网络。其中ECU A扮演强攻击者的角色，ECU B扮演弱攻击者的角色，ECU C作为非攻击者的角色，ECU R作为入侵检测系统的检测点。其中ECU A没被植入恶意程序时，默认它是发送0x11的报文消息，ECU A编入恶意程序使它在T_{masq}为250秒的时候伪装发送ID为0x55报文消息的ECU B，也即中断ECU B发送报文消息，反而让ECU A代替ECU B发送相同ID的报文消息。

[0123] 如图8(a)展示了攻击前和攻击后，ID为0x55的报文消息的PMF(概率质量函数)。在ECU A伪装过后，还是以ECU B同样的频率发送报文消息，因此，相当于攻击前，分布没有明显的偏离。然而，因为在T_{masq}时刻的时候，发送0x55的报文消息的ECU B被阻止了，由ECU A代替发送，在ECU切换的过程中会有一段延迟时钟。从图中可以看出在没发动伪装攻击时，报文消息之间的时钟间隔是50ms，然而在第一次发动伪装攻击时，相对于发动伪装攻击前一次发送的报文消息结束时，此时报文消息的时钟间隔为51.04ms。由于在T_{masq}出现了伪装攻击，PMF图中就显示出了偏离正常情况下的异常的报文消息时钟间隔。由此，这种变化也导致了检测点ECU R跟踪的O_{acc}，L^{+}，L^{-}的变化，如图8(c)所示。从图8(b)可以看出，在250秒的时候，由于发动了伪装攻击，所以造成了0x55报文消息累积时钟偏移的斜率产生了变化也

即时钟偏差产生了变化。由于在T_{masq}过后，O_{acc}的测量值相对于T_{masq}之前正常情况下的期望值产生了明显的偏离并且目标值的累积和下限也超出了阈值，从而入侵检测系统可以报告这是一次入侵。由于在T_{masq}之后，发送ID为0x55的报文消息的ECU变成了A，它的时钟偏差与0x11的时钟偏差相等，从而也可进一步判定攻击源为A。

[0124] 图7伪装攻击网络仿真网络图。图8入侵检测系统检测伪装攻击图。

[0125] 在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用全部或部分地以计算机程序产品的形式实现，所述计算机程序产品包括一个或多个计算机指令。在计算机上加载或执行所述计算机程序指令时，全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL)或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输)。所述计算机可读取存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，(例如，软盘、硬盘、磁带)、光介质(例如，DVD)、或者半导体介质(例如固态硬盘Solid State Disk(SSD))等。

[0126] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

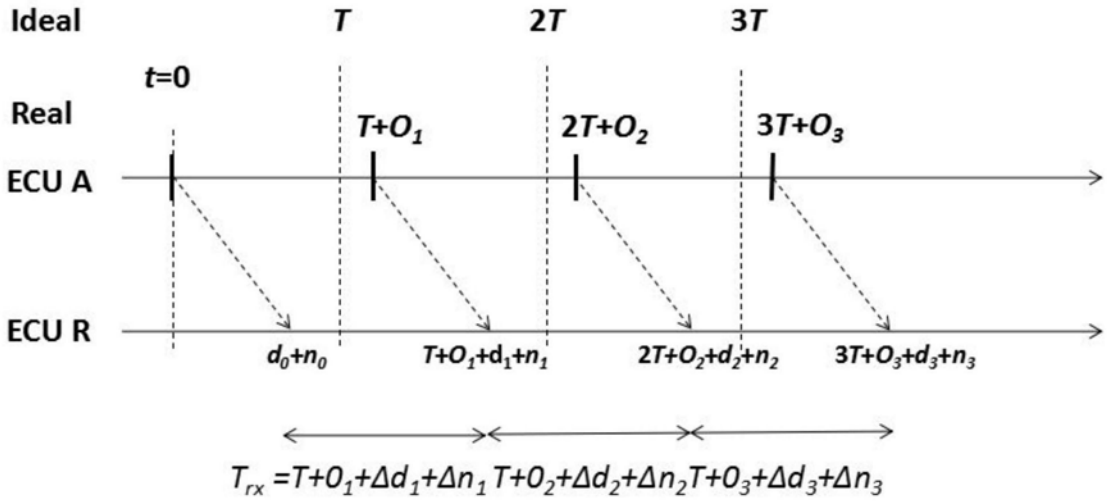

Ideal
T
2T
3T
t=0
Real
T+O1
2T+O2
3T+O3
ECU A
ECU R
d0+n0
T+O1+d1+n1
2T+O2+d2+n2
3T+O3+d3+n3
Trx =T+O1+Δd1+Δn1 T+O2+Δd2+Δn2T+O3+Δd3+Δn3

图1

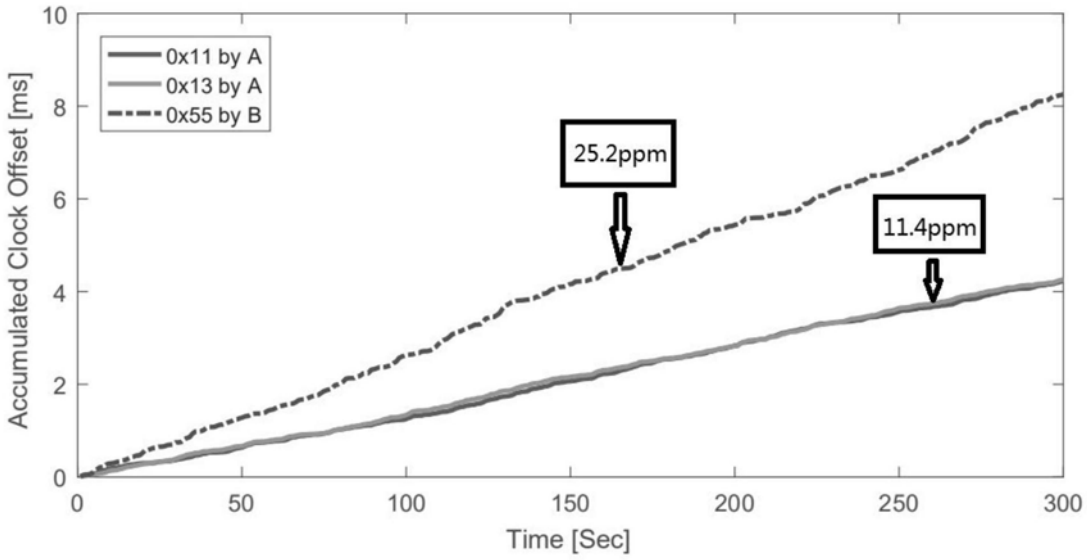

0x11 by A
0x13 by A
0x55 by B
25.2ppm
11.4ppm
Accumulated Clock Offset [ms]
Time [Sec]
0
2
4
6
8
10
0
50
100
150
200
250
300

图2

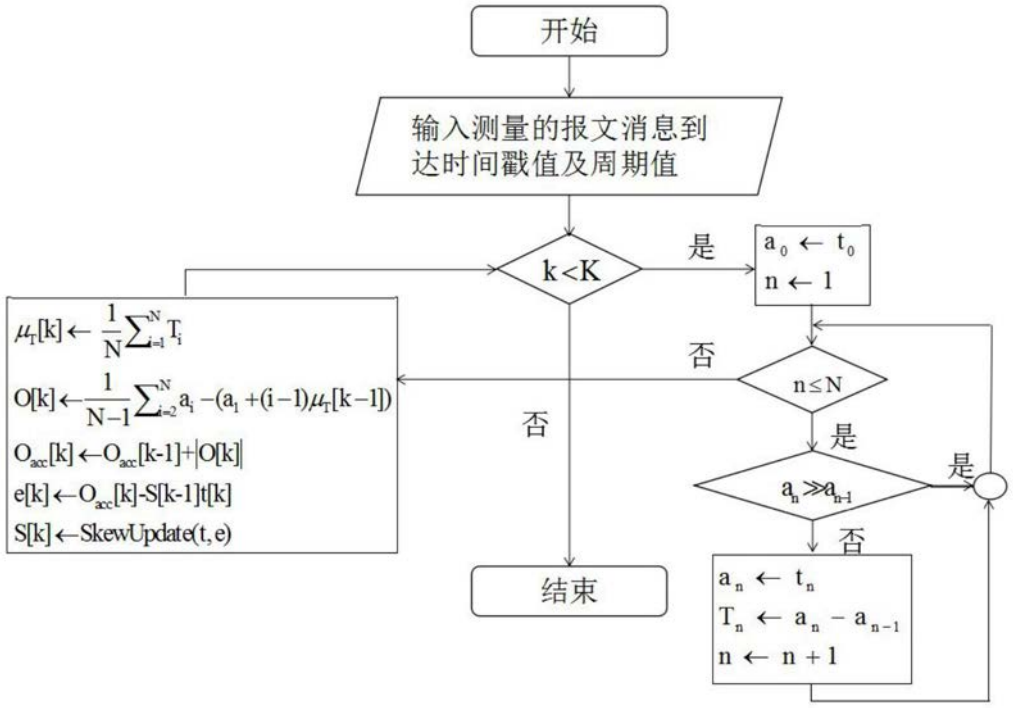

开始
输入测量的报文消息到达时间戳值及周期值
k<K
是
否
$a_0 \leftarrow t_0$
$n \leftarrow 1$
$n \le N$
否
是
$a_n \gg a_{n-1}$
是
否
$a_n \leftarrow t_n$
$T_n \leftarrow a_n - a_{n-1}$
$n \leftarrow n+1$
$\mu_T[k] \leftarrow \frac{1}{N}\sum_{i=1}^{N} T_i$
$O[k] \leftarrow \frac{1}{N-1}\sum_{i=2}^{N} a_i - (a_1 + (i-1)\mu_T[k-1])$
$O_{acc}[k] \leftarrow O_{acc}[k-1] + |O[k]|$
$e[k] \leftarrow O_{acc}[k] - S[k-1]t[k]$
$S[k] \leftarrow SkewUpdate(t,e)$
结束

图3

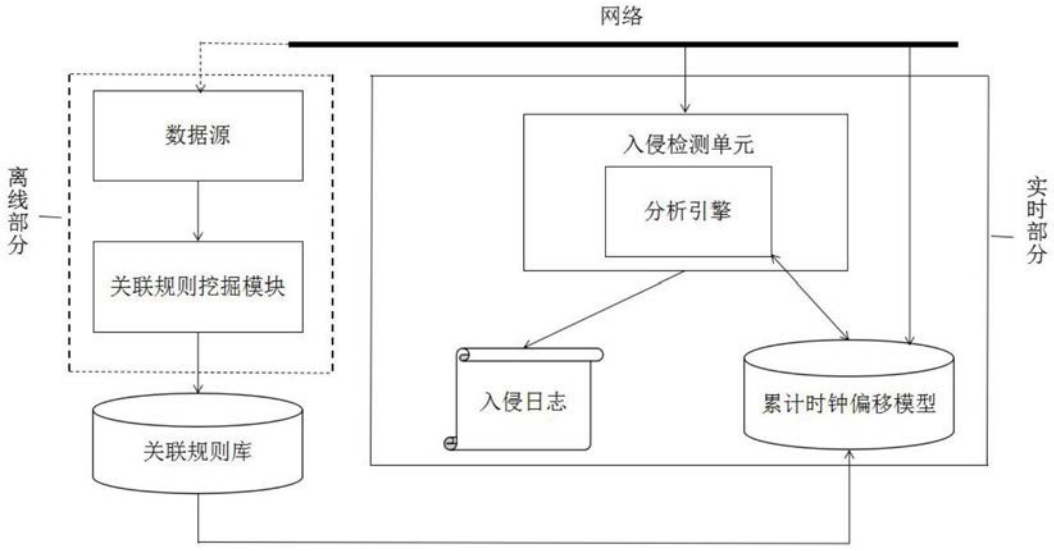

网络
离线部分
数据源
关联规则挖掘模块
关联规则库
入侵检测单元
分析引擎
入侵日志
累计时钟偏移模型
实时部分

图4

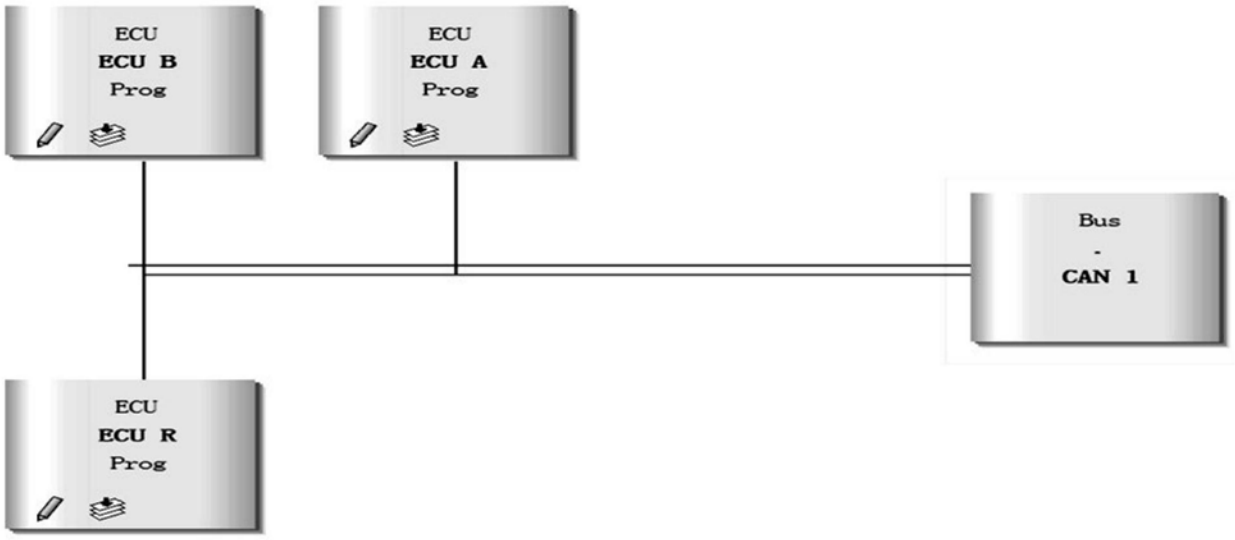

ECU
ECU B
Prog
ECU
ECU A
Prog
Bus
-
CAN 1
ECU
ECU R
Prog

图5

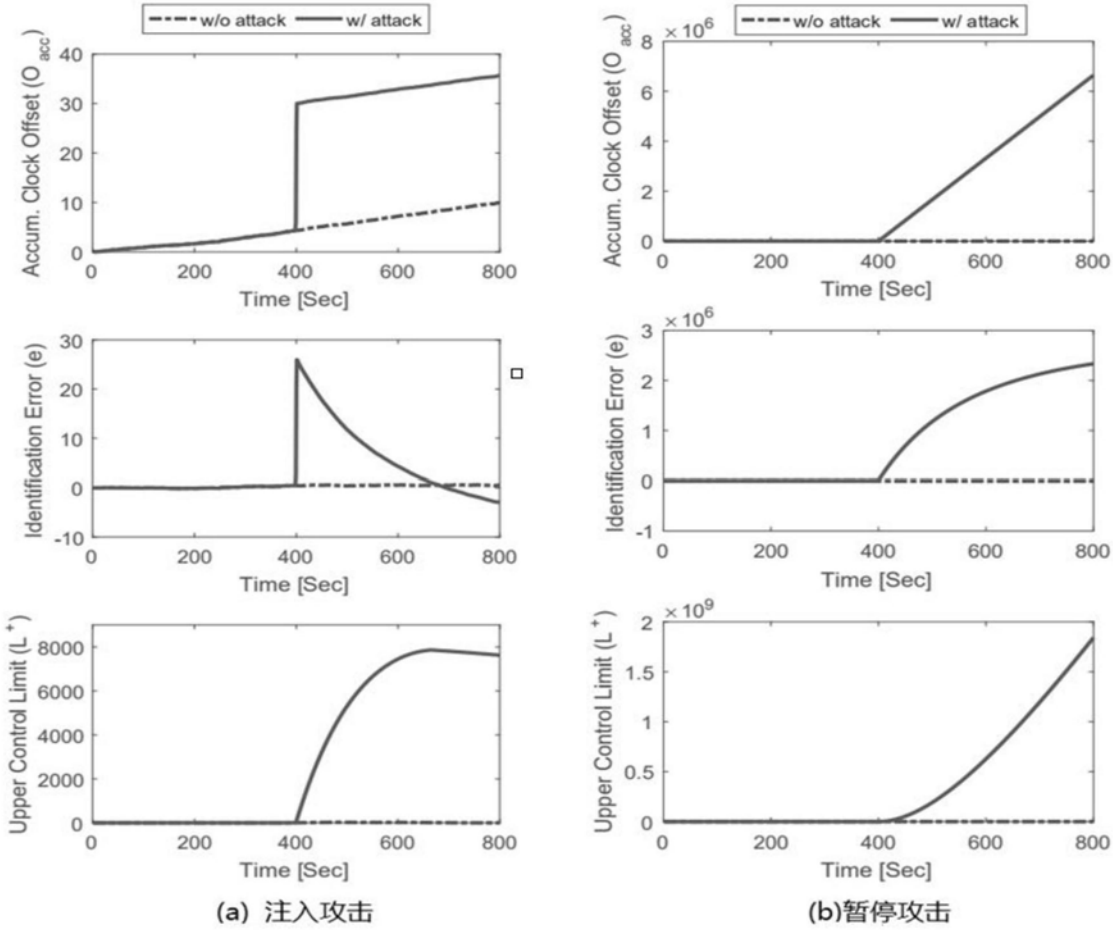

w/o attack
w/ attack
Accum. Clock Offset (O_{acc})
Identification Error (e)
Upper Control Limit (L^+)
Time [Sec]
(a) 注入攻击
(b)暂停攻击

图6

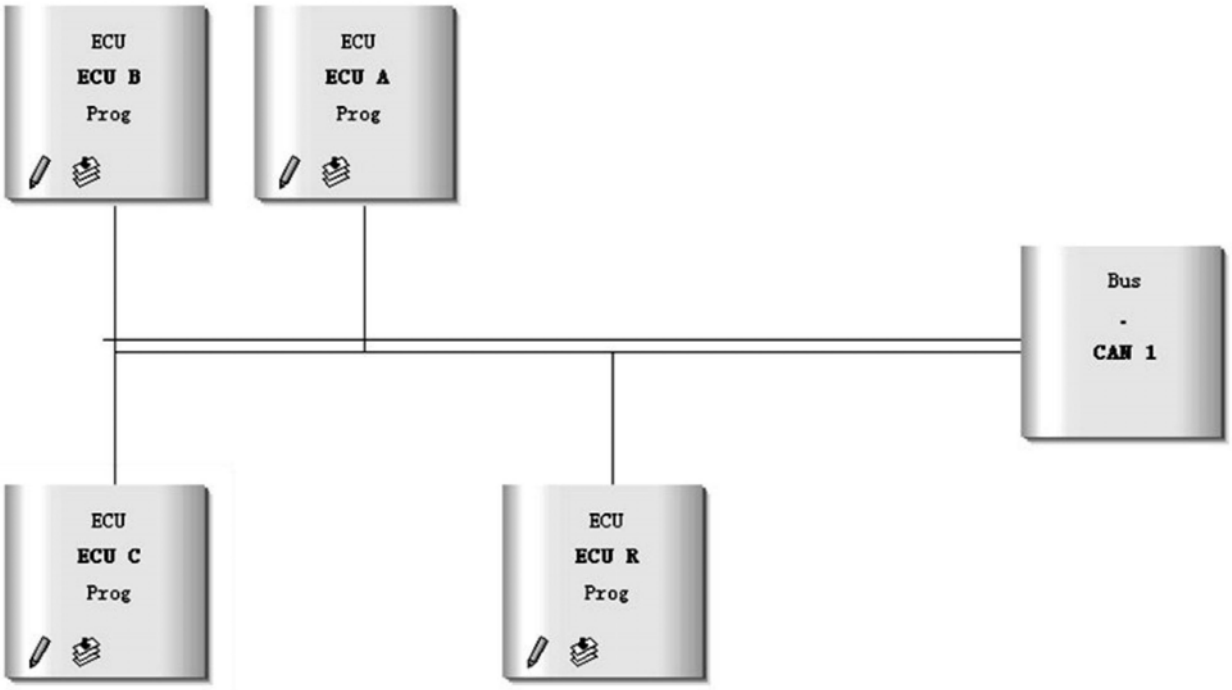

ECU
ECU B
Prog
ECU
ECU A
Prog
Bus
-
CAN 1
ECU
ECU C
Prog
ECU
ECU R
Prog

图7

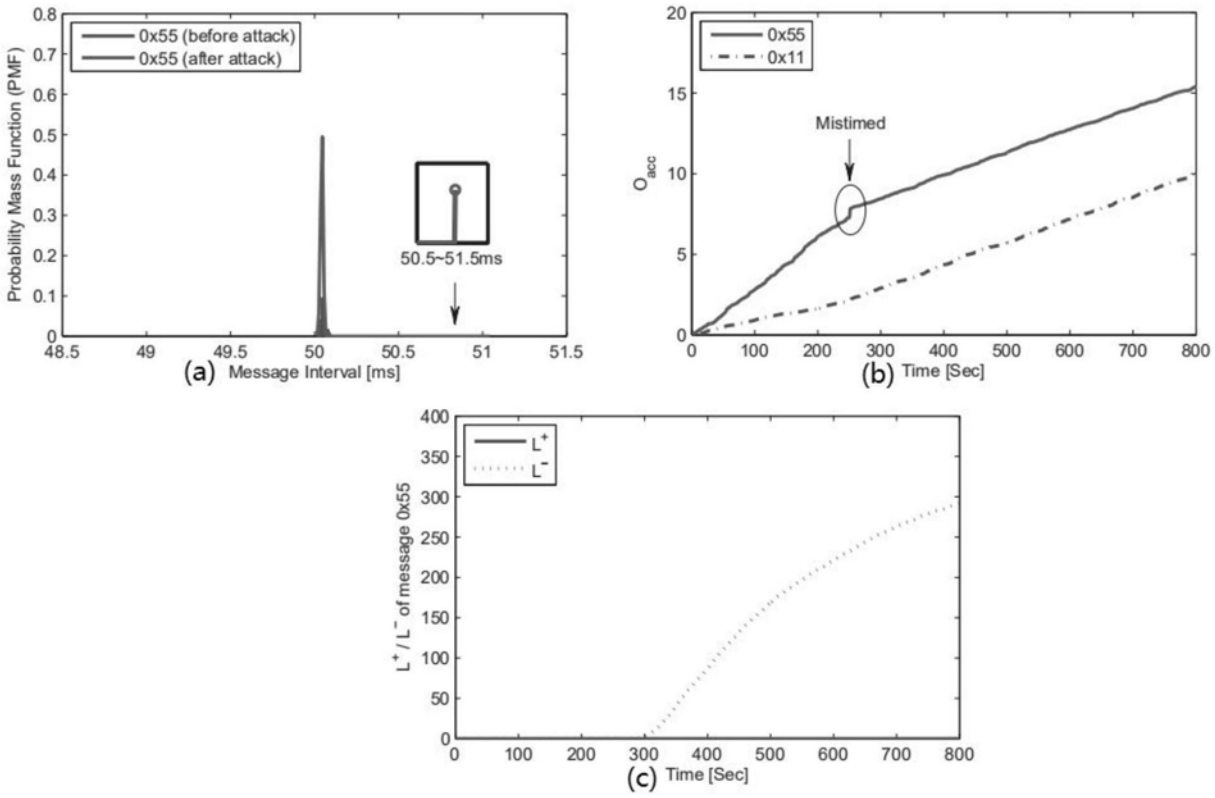

0x55 (before attack)
0x55 (after attack)
Probability Mass Function (PMF)
50.5~51.5ms
(a) Message Interval [ms]
0x55
0x11
Mistimed
O_{acc}
(b) Time [Sec]
L^+
L^-
L^+ / L^- of message 0x55
(c) Time [Sec]

图8