计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2018.20180123
55(7):1488-1497,2018

高效物联网虚假数据融合结果检测机制

许志伟　　张玉军
(中国科学院计算技术研究所　北京　100190)
(中国科学院大学　北京　100049)
(xuzhiwei2001@ict.ac.cn)

Efficient Detection of False Data Fusion in IoT

Xu Zhiwei and Zhang Yujun
(*Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100190)
(*University of Chinese Academy of Sciences, Beijing* 100049)

Abstract　Data fusion is the critical process for data transmission in the Internet of things (IoT). In data fusion process, the original sensing data is processed and aggregated in the network, and only the aggregated results of data fusion are sent to the application layer, which effectively reduces the resource consumption and alleviates the workload on the sink node. Since no network node caches the aggregated data in the data fusion process, it is impossible to detect and locate the false data injection attack against data fusion results. In order to mitigate this significant vulnerability, an efficient detection scheme of false data fusion is proposed in this paper. By modeling the data fusion process, we discover and model the relationship between the input data and the fusion results, and apply the obtained model to detect abnormal data fusion results. In this way, we can mitigate malicious data fusion and optimize the IoT transmission security. In detail, we first collect input data and the relevant data fusion results for each node, and a compressed feature representation mechanism is designed to improve the data collection efficiency and reduce the resource consumption. In addition, a data fusion model based on probabilistic graph model is proposed to depict the spatial and temporal relationship between the input data and the data fusion results. Ultimately, we take the model to detect the abnormal data fusion results in an efficient way. The experimental results demonstrate that the proposed detection scheme can detect malicious data fusion operations efficiently and accurately and thus guarantee IoT transmission security.

Key words　Internet of things (IoT); in-network data fusion; data fusion model; lightweight; efficiency; detection of false data injection

摘　要　数据融合(data fusion)是物联网数据传输和处理的关键步骤之一,在传输过程中提前汇总和处理中间数据,仅将逐层融合的结果发送到应用层,有效降低了中间节点的功耗和负载.然而,在这一过程中,各节点没有保存被融合数据,因此,无法发现和定位针对数据融合结果的数据伪造或篡改攻击.为了

收稿日期:2018-02-09;**修回日期**:2018-05-03
基金项目:国家自然科学基金项目(61402446,61572474,61672500);国家重点研发计划项目(2016YFE0121500);内蒙古自治区自然科学基金项目(2017MS(LH)0601)
This work was supported by the National Natural Science Foundation of China (61402446, 61572474, 61672500), the National Key Research and Development Program of China (2016YFE0121500), and the Natural Science Foundation of Inner Mongolia Autonomous Region of China (2017MS(LH)0601).

杜绝这一安全隐患,提出一种高效的物联网数据融合安全检验机制,通过对数据融合过程建模,发现并刻画被输入数据和融合结果之间的联系,并利用这一模型发现异常的数据融合结果,杜绝恶意数据融合,优化物联网传输安全.首先,在节点/网络的输入端和输出端分别进行数据收集,构建了基于被融合数据的特征压缩摘要机制,提升了数据收集效率并优化了节点资源消耗;其次,提出了基于概率图概率模型的数据融合模型,描述被融合数据和融合结果的时空域关系,并基于这一模型高效检测异常数据融合结果.实验结果表明:所提出的方法能够高效、准确地发现恶意数据融合操作,优化物联网传输安全.

关键词 物联网;网内数据融合;数据融合模型;轻量级;高效;数据篡改攻击检测

中图法分类号 TP393.08

作为互联网的延伸和扩展,物联网是信息技术领域的又一次重大变革.物联网的基本特征是信息的全面感知、可靠传送和智能处理.通过传感设备获取实体信息,并通过网络传输到相关服务节点,实现人-物、物-物互联,实现物理世界实体的智能化识别、定位、跟踪、监控和管理.物联网是由各种不同支撑技术组合而成的异构体系结构,如面向实物的RFID通信、面向智能终端的移动计算、面向感知节点的传感器网络,以及面向Internet用户的数据共享、应用服务等.物联网在不同的逻辑层面部署了这些技术和相应的实体.在物联网的感知层(sensing layer)和网络/接入层(core layer),智能终端、传感器以及RFID阅读器和标签的数据经过汇总和融合提交给应用层(application layer).应用层中,相应的应用服务收集从网络/接入层收到的数据融合结果,在融合结果基础上更新服务状态,为用户提供服务.

数据融合(data fusion)是对物联网多源异构数据进行综合处理获取确定性信息的过程.在物联网感知网络中,对感知数据进行融合处理,只将少量有意义的信息传输到汇聚节点,有效减少数据传输量,降低中间节点功耗,提升相关节点的在线时间.在这一数据融合过程中,为了保证融合效率和压缩数据传输,物联网接入层节点对收到的数据进行数据融合时,仅针对上层服务需求汇总数据,同时最大程度地去除无用数据的影响,整个数据融合过程是一个有损处理过程[1-4].这就在数据融合过程中留下了关键的隐患,攻击者可以在物联网覆盖的区域内配置恶意节点,或捕获合法节点发动针对数据融合结果的恶意篡改攻击.由于下游节点不保存融合前的数据,即使融合结果被篡改,这些节点也无法发现和定位这一针对数据融合结果的篡改攻击.面向物联网应用,如何解决数据融合的安全问题,特别是有损数据融合背景下的安全性问题,是影响物联网数据传输和未来发展的关键问题.

目前在实现物联网安全数据融合方面主要有2种途径:

1)提高数据传输安全性,即通过加密传输等机制保证收到数据的真实性[1-3],鉴于高强度的加密机制带来的大量时间和能量开销,目前这一途径还很难在资源受限的物联网中应用.

2)构建安全数据融合机制,文献[4-6]利用相邻节点相似和冗余的感知结果,利用多个融合结果对抗可能出现的对融合结果的恶意修改,这一方案只能在数据冗余的情况下展开.

上述2类构建安全数据融合的方案仍然无法彻底杜绝物联网数据融合过程中的安全问题,需要构建全新的物联网数据融合安全机制,全面保障数据融合过程的可靠性,提升物联网数据传输的安全性.

物联网的感知层和接入层节点资源有限,无法应用现有互联网中的安全机制抵御和检测攻击[4-5],需要构建资源消耗小且可以广泛部署的安全机制.同时,物联网节点众多,感知层数据更新频繁,因此数据传输量巨大,如何在如此高的负载下高效完成攻击的检测和防范,这是实现物联网数据融合安全的另一个关键难点.

为了杜绝数据融合的安全隐患,本文提出物联网数据融合安全检验机制,通过对相关节点/网络的数据融合过程建模,发现并刻画被输入数据和融合结果之间的联系,发现异常的数据融合结果,杜绝恶意数据融合,优化物联网传输安全.本文的主要贡献有3个方面:

1)在节点/网络的输入端和输出端分别进行数据收集,构建了基于被融合数据Hash结果的特征压缩摘要机制,提升了数据收集效率并优化了节点资源消耗.

2)提出了基于Markov概率模型的数据融合模型,根据被融合数据和融合结果的时域关系为正常的数据融合过程建立统一模型,并通过吉布斯采样

完成模型学习,有效刻画节点/网络数据融合过程,为后续异常数据融合的发现和定位提供前提.

3) 应用不同数据集构建实验,验证了本文提出的安全数据融合检验机制,该机制可以有效发现异常数据融合,防范针对数据融合结果的恶意篡改,提升了物联网数据传输的安全性.

1 相关工作

目前,国内外研究人员针对物联网数据融合安全问题进行了广泛的研究.

在加密传输方面,Hu 等人[1]利用无线网络的特性以及设备和基站之间的功率不对称性,提出了基于 μTesla 轮密钥的数据融合算法,一个为无线网络提供安全的汇聚机制,对入侵者设备和单个设备密钥泄露具有鲁棒性;Bagaa 等人对文献[2]中的数据融合算法进行了优化和改进,提出了一种新的安全数据融合方案 SEDAN,使用点到点的对数据机密性和隐私性提供了完全分布的安全传输方案,保证数据不被篡改;Ozdemir 等人[3]对 2-DNF 密码机制进行了优化和改进,该方案利用不同的加密密钥加密的数据包进行聚合,提出的数据聚合方案采用基于椭圆曲线密码的同态加密算法,保证了数据的完整性和机密性.但是,上述安全机制存在运行效率低、额外资源消耗高等问题.

在挖掘数据融合本身特性抵御篡改攻击方案方面,Cam 等人[4]提出了基于簇型融合网络的安全数据融合方案,该方案使用模式识别码技术,簇头在执行数据融合时不需要知道传感器的数据,这使得传感器节点与基站能够建立安全的端到端通信链路.He 等人基于将原始数据碎片化、无序化,然后通过节点间的协调操作来完成数据融合过程的思想,提出了基于簇型融合网络的安全数据融合方案 PDA[5],该方案通过簇内节点间的协同操作来完成数据融合运算,具有很好的抗节点合谋能力,有效地保证了网络中数据的机密性和隐私性,在文献[6]进一步优化了 PDA 方案,通过生成双树形融合网络来为数据融合结果的安全性提供多源验证机制.上述方案对网络数据的分布情况具有较严格要求,限制了方案的有效使用.

Mukhopadhyay 等人[7]通过一个线性回归模型实现了接入层数据篡改/伪造攻击的检测,方案对初始训练数据的敏感性影响了模型的可用性;文献[8]提出了另一种信任系统,该系统综合实验证据推理和贝叶斯推理,通过定期评估节点行为确定可信节点;Sun 等人[9]通过科尔曼滤波算法发现潜在的数据篡改/伪造攻击,然而该方案高度依赖于前期数据输入,无法抵御初始攻击强度较低的攻击;为了检测并防范数据融合过程中的数据包伪造、篡改攻击,Yang 等人[10]采用二阶差分过滤器(second-order divided difference filtering)发现可疑数据包并通过序贯概率比检测法(sequential probability ratio testing)估计可疑数据包是否对数据融合结果具有负面影响,从而保证了攻击检测的准确性,在连续多批次采样后,攻击检测的准确性可以进一步提高.攻击检测过程应用的二阶方差计算和序贯概率比检测的计算量较大,降低了方案在物联网这一资源受限及高数据流量应用场景下的可用性.

2 物联网数据融合安全分析

本节将对物联网数据融合安全问题进行分析.首先对物联网数据融合过程的安全隐患进行描述和分析,给出了数据融合过程中的数据篡改/伪造攻击的分析;在攻击分析的基础上,给出数据融合安全规约,规范安全数据融合的必要条件.

2.1 针对数据融合过程的数据伪造/篡改攻击

作为物联网数据传输的关键步骤,接入层各汇聚节点将收集感知层数据并进行融合,将融合结果发送给应用层服务.数据融合过程是一个有损数据汇聚过程,汇聚节点根据输入数据通过计算和推导给出相应的融合结果,输入的数据和融合结果不存在一对一的对应关系,无法从融合结果得出输入数据信息,这为攻击者伪造/篡改融合结果提供了便利之门.

攻击者分步骤在数据融合过程中发动伪造数据或者篡改数据攻击,包括 3 个步骤,如图 1 所示:

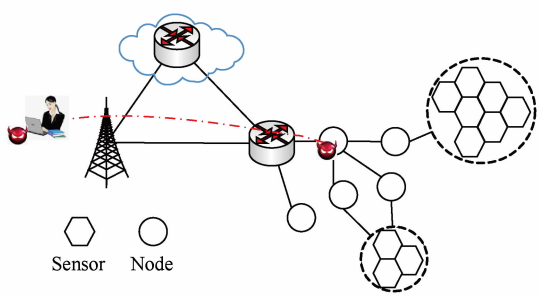

Fig. 1 The threat for information fusion in IoT

图 1 物联网数据融合安全威胁

1) 发动融合数据篡改攻击前,攻击者需要侵入

一个感知子网内的实体节点或者汇聚节点.同互联网相比,在物联网中对这些节点的侵入更容易,因为这些节点容易在物理上被攻破或被复制[11],同时节点的无线广播信道也容易发动物理层或链路层攻击.在开放的物联网环境中这一入侵过程将更为常见,很多物联网通过将多个机构的感知节点互连构成的网络,这种环境中的安全威胁更大,因为互联的感知节点分属于不同机构,这些机构间可能存在竞争关系,感知节点容易被对手控制的节点攻击,这种情况下节点间只能确保有条件的信任.

2) 发动融合数据篡改攻击时,如果攻击者仅控制了实体节点,那么攻击者将控制这些实体节点伪造恶意数据包,或者篡改上游节点传来的数据包填充恶意数据,将这些恶意数据包发往汇聚节点,汇聚节点的数据融合过程在一定程度上受到这些恶意数据的影响,受影响程度同数据融合机制对被控制节点数据的依赖有关.另外一种情况,如果攻击者控制了汇聚节点,攻击者可以直接篡改或伪造数据融合结果.

3) 发动融合数据篡改攻击后,被毒化的数据融合结果通过网络被传送到应用层服务节点,节点服务将受到影响,造成服务瘫痪或者导致负面操作,损害用户利益.

2.2 安全规约

为了应对数据融合过程中的数据伪造和篡改攻击,需要根据 2.1 节攻击过程,有针对性地构建攻击防范机制.因为物联网实体节点容易在物理上被攻破或被复制[11]物联网中针对实体节点的攻击更容易,同时这些实体节点的处理能力较差,很难支撑现有加密算法,因此数据篡改和隐私破解攻击将很难防范[12].感知层实体节点的这些弱点,成为了物联网的安全瓶颈,因此,需要研究非加密传输情况下如何有效识别和防范数据伪造/篡改攻击.同时在构建相应攻击检测机制的同时需要考虑上述物联网节点特点,优化相关机制的效率和资源消耗,按照 2 个规约构建安全检测机制:

1) 为了在无法保证节点/网络是否可信的情况下分析其可靠性并检测攻击,需要通过高效、低资源消耗的方式收集相关节点/网络数据融合前后的输入数据和融合结果;

2) 学习功能类似的可信节点的数据输入与融合结果的关系(假设在初始阶段,通过长时间使用可以根据应用层反馈判断数据输入对应的融合结果是否正常).基于这些对应关系构建高效、低资源消耗的攻击检测机制,保证检测机制的可用性,实时发现潜在的恶意数据融合结果.

3 高效数据融合安全检验机制

为了构建高效的数据融合安全检测机制,检测数据融合过程中的数据伪造和篡改攻击,本节首先梳理数据融合安全检验步骤,明确了相关操作;其次,为了收集和分析感知层数据,定义了一套高效的感知层数据特征摘要机制;最后,在数据特征摘要的基础上利用概率图模型刻画融合结果和输入的关系.

3.1 基本安全检验过程

在物联网数据融合过程中,每个实体感知终端对周期性感知数据进行初步处理,规范数据格式,并将其发往汇聚节点,由汇聚节点融合收到的感知数据完成相关合成处理.为了优化数据传输效率、减少网络资源开销、优化网络节点能耗,数据融合过程中只保留支撑应用需求的关键信息,基本感知数据在被融合后将不再保留,整个融合过程包括一系列数据合并、计算和推导操作.其中涉及的计算和推导主要包括建立在基本运算结果基础上的贝叶斯推导[13]、Markov 随机场[14]和 Dempster-Shafer 证据推导[15]等处理过程.

为了规范这一过程,Llinas 等人提出了实验室联合主任(Joint Directors of Laboratories, JDL)模型[16],JDL 模型是美国国防部实验室理事数据融合专家组提出的标准数据融合模型.JDL 模型规定了融合经历的阶段,包括从输入到输出的推导层次.在不同的处理阶段数据具有不同的形式,逐层规约,指导得到确定的融合结果.整个数据过程可以通过确定的状态机模型进行描述,在确定的状态空间上(取决于输入和当前状态)推导形成融合结果.初期的数据处理为后续高层推导提供数据,可以通过划分取值空间建立初步计算得到的数值结果同推导结果的关系,详见 3.2 节,不同的输入数据经过分阶段处理,最终得到 2 个不同的融合结果.

综上,数据融合过程中,汇聚节点将针对一定范围内节点的感知或数据读取结果进行简单的合并、计算和分析,逐层规约,得到最终的融合结果,并将融合结果发送给上层汇聚节点或者远端服务节点.为了保证这一过程的安全性,检验融合结果的合理性,需要对已有汇聚节点数据融合的输入和结果进行学习、建立模型,然后基于模型检测和识别数据融合过程中的恶意数据伪造和篡改.其基本的检验步骤包括 3 个步骤:

1) 为了能够发现输入和融合结果的关系,首先需要部署检验节点,从待检验的汇聚节点的输入端和输出端获取数据,例如图 2 中,检测节点从被检测的节点 a 的输入端(连接 b,c,d 的链路)和输出端(连接 sink 节点的链路)分别获取融合过程涉及的输入数据和融合结果.

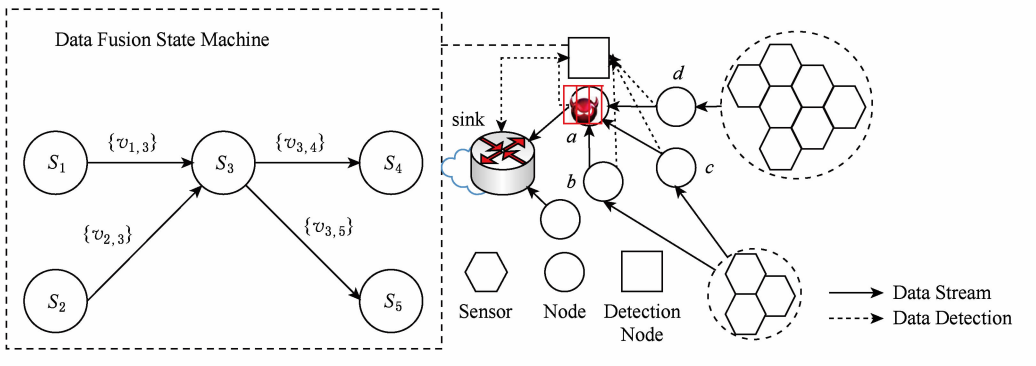

Fig. 2 Attack detection with traffic monitoring nodes

图 2 基于流量监控的攻击检测框架

2) 为了能够统一刻画数据融合过程中的输入数据,需要构建高效的输入数据汇总表示机制,以便统一分析输入数据及融合结果之间的关系.

3) 构建模型描述输入数据及融合结果之间的关系,为检测和发现数据融合过程中的数据伪造和篡改攻击提供依据.

为此,本节后续部分将首先提出一种统一的输入数据表示机制——感知层数据特征摘要机制. 在这一输入数据表示机制基础上,利用随机图理论构建高效数据融合模型,高效检测数据融合过程中的恶意数据伪造和篡改攻击.

3.2 感知层数据特征摘要机制

在物联网这一资源受限、大数据流量、高时效性的应用场景下,数据融合安全检测方案需要建立在高效的数据收集和建模基础之上,在提升检测准确性的同时,最大程度地优化攻击检测效率和资源消耗. 为了实现这一目标,本文构建了一种高效的输入数据表示机制——感知层数据特征摘要机制,如图 3 所示. 压缩表示感知层节点待融合数据,为高效挖掘和发现待融合数据同融合结果之间的关系,构建相应的数据融合模型提供了前提,同时也为构建高效的数据伪造/篡改攻击检测机制奠定了基础.

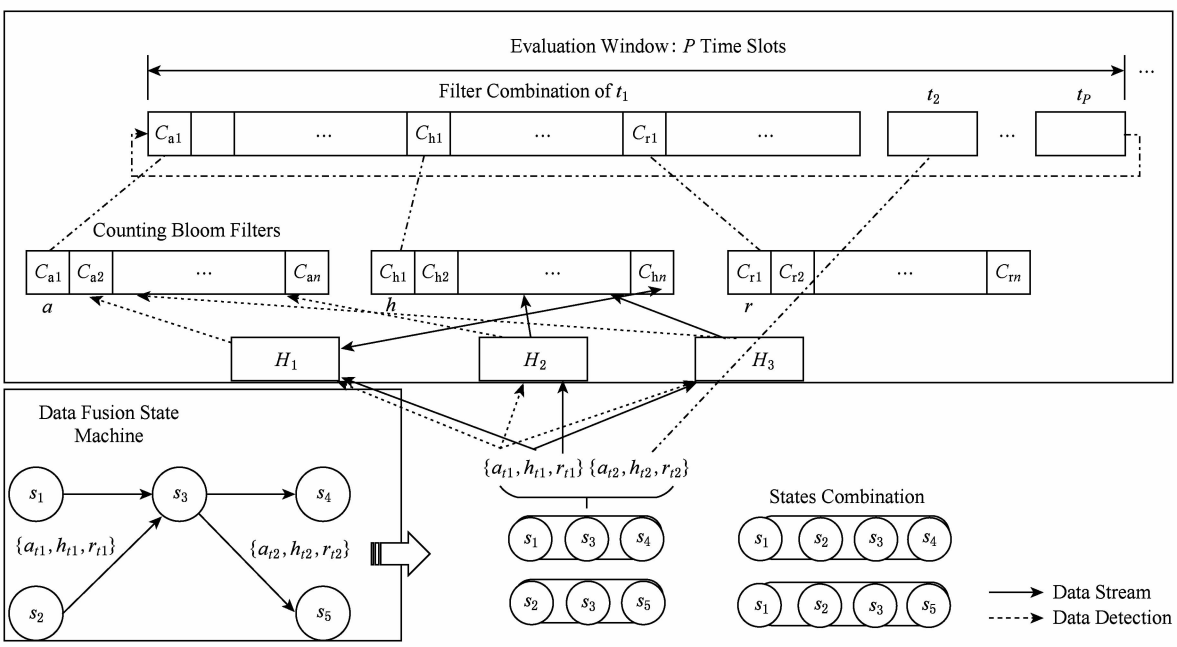

Fig. 3 Data finger point generation

图 3 感知层数据特征摘要机制

这一输入数据表示机制,需要满足3个条件:

1) 准确性. 可以准确表征输入数据,捕获并利用数据关键特征描述输入数据及其分布.

2) 效率. 归并和约简输入数据的同时,需要保证数据特征摘要和应用过程的高效性,提升输入数据分析的效率,以满足物联网高效海量数据处理的要求.

3) 可用性. 能够统一表示各类数据,便于在各类场景下刻画数据融合过程涉及的输入数据.

为此,本文在3.1节对感知层数据融合过程的分析的基础上,应用目前广泛使用的数据压缩表示技术、布隆过滤器技术,通过优化组合各输入数据的特征构建输入数据特征摘要,保留数据融合结果对应输入数据的时空关系的同时优化数据表示效率及开销,整个数据特征摘要机制如图3所示.

首先,为了能高效描述融合结果对应的数据输入并减少资源消耗,本文采用布隆过滤器技术获取单一感知层数据的压缩表示,图3中,原始数据输入及对应融合过程利用右下状态机模型表示,当时刻 t_1 汇聚节点收到一组来自3类实体的感知层数据 a_{t1},h_{t1},r_{t1},经过处理到达状态 s_3 对应步骤,当汇聚节点在下一时刻 t_2 收到数据 a_{t2},h_{t2},r_{t2} 后,进过推导得到状态 s_4 对应的数据融合结果,完成数据融合操作. 这个融合过程对应的操作状态序列为 s_1,s_3,s_4,对应的输入为 $\{a_{t1},h_{t1},r_{t1}\}$ 和 $\{a_{t2},h_{t2},r_{t2}\}$. 每个时隙3个感知实体的数据分别记录到相应的计数布隆过滤器中,利用对应数据的不同Hash结果(Hash函数 H_1,H_2,H_3 的结果)定位布隆过滤器中的单元,每次命中单元取值加1. 根据输入数据取值范围设置布隆过滤器单元数量,以保证数据表示精度[17],能够准确刻画输入数据特征. 同时根据重复的采样数据的统计情况设置单元最大计算值,实现对重复数据的记录和统计. 然后将不同实体对应布隆过滤器的表示结果组合在一起,作为本时隙数据表示结果.

为了全面收集影响数据融合结果的输入数据,需要将相关时隙对应实体的数据全部加入分析,因此需要收集不同时隙的数据表示结果,例如图3中将当前时刻之前 P(图3例子中,$P=2$)个时隙作为1个检测周期,收集对应的表示结果序列,关联融合结果(序列 s_1,s_3,s_4). P 的设置根据新的融合结果的平均生成时隙确定. 为了充分利用之前的表示结果,每个时隙结束后,将利用最旧的数据记录对应的布隆过滤器记录下一个时隙的数据. 这一感知层数据特征摘要机制通过数据压缩表示机制高效保留数据特征,全面收集数据融合结果相关的数据输入,为构建数据融合模型提供了前提条件.

3.3 高效数据融合模型

构建高效合理的数据融合模型是实现物联网数据融合过程中数据伪造和篡改攻击的关键. 本文通过支持增量融合结果发现随机图模型发现并刻画输入数据同数据融合结果之间的关系,实现高效的异常数据融合结果检测.

首先利用中国餐馆过程[18]对待融合数据能够覆盖的融合结果数量进行估计;其次利用概率图模型,确认各融合操作对应的数据特征摘要及其相关度,作为续数据融合过程中异常融合结果检测的依据.

中国餐馆过程定义了一种随机的类别产生过程. 在界定数据融合结果的数量时,用从小到大的自然数标记各个融合结果,然后将输入数据特征摘要随机分配到这些融合结果上:

1) 第1个数据特征摘要分配给1号融合结果;

2) 第 n 个数据特征摘要或者按照概率 $\alpha/(n-1+\alpha)$ 选择分给一个新融合结果(α 为先验系数),或者依概率 $m_k/(n-1+\alpha)$ 选择已经分配了数据特征摘要的第 k 个融合结果,其中 m_k 为当前分配到第 k 个融合结果的数据特征摘要的数量. 中国餐馆过程是一个稳态的随机过程,因此,可以获得明确的数据融合结果数.

在此基础上,构建概率图模型刻画 K 个数据融合结果和输入数据特征摘要之间的联系. 如3.1节相关文献所述,数据融合过程是针对输入数据的多个阶段的处理,融合结果可以表示为多个中间状态的序列. 在旁路获得融合结果及相应的输入数据特征摘要后,在中间状态未知的情况下刻画融合结果同输入数据数据摘要之间的关系. 因此,我们首先利用Dirichlet分布刻画中间状态作用下第 t 个检测周期内输入数据摘要 $F_t=\{f_{t,1},f_{t,2},\cdots,f_{t,P}\}$ 对应的融合结果的先验分布.

$$\theta_t=Dir(\lambda), \tag{1}$$

其中,λ 为分布Dirichlet分布的超参数.

基于 θ_t 可得检测周期 t 的数据特征摘要序列 $F_t=\{f_{t,1},f_{t,2},\cdots,f_{t,P}\}$ 对应的融合结果 $S_t=\{s_1,s_2,\cdots,s_K\}$ 的多项分布:

$$S_t=multi(\theta_t). \tag{2}$$

同样利用Dirichlet分布刻画特定融合结果 s_i 相关的数据摘要 f_j 的先验分布:

$$\beta_k = Dir(\eta), \tag{3}$$

其中,η 为这一 Dirichlet 分布的超参数.

根据 β_k 得到第 i 个输入数据摘要 $f_{t,i}$ 的概率分布为

$$f_{t,i} = multi(\beta_k). \tag{4}$$

至此已经构建出从输入数据序列到融合结果集的 Dirichlet-multi 共轭,可以根据采集得到先验分布得到相应的后验分布. 同样基于从特定融合结果到相关输入数据的 Dirichlet-multi 共轭可以得到 $f_{t,i}$ 的后验分布.

利用 Gibbs 采样[19],可以不断迭代推导生成当前输入序列同下一时刻 $t+1$ 的输入的关系,直到收敛(推导同实际数据吻合),得到最终的描述融合结果 s_k 同输入数据 $f_{t,i}$ 的关系的概率图模型,从中选择显著的关系,将其中融合结果对应的输入数据特征摘要(计数布隆过滤器)按照显著性排列,构成基于输入验证融合结果是否正常的依据.

$$P(F_{t+1}|F_t) = \sum_{k=1}^{K} P(f_{t+1,i}|\beta_k) Dir(\eta) P(\theta_t|F_t) Dir(\lambda). \tag{5}$$

算法 1. 概率图模型生成算法.

输入:中国餐馆过程参数 α、输入特征摘要序列 $\{F_t\}$、Dirichlet 先验分布的参数 λ 和 η、收敛阈值 ε;

输出:描述融合结果 s_k 同输入数据 $f_{t,i}$ 的关系的概率图模型.

① for 每个时隙 t

② $CRP(F_t,\alpha)$; /* 中国餐馆过程 */

③ $\theta_t = Dir(\lambda)$;

④ $S_t = multi(\theta_t)$;

⑤ $\beta_k = Dir(\eta)$;

⑥ $f_{t,i} = multi(\beta_k)$;

⑦ $P(F_{t+1}|F_t) = \sum_{k=1}^{K} P(f_{t+1,i}|\beta_k) Dir(\eta) \times P(\theta_t|F_t) Dir(\lambda)$;

⑧ if $P(F_{t+1}|F_t) \leqslant \varepsilon$

⑨ break; /* 收敛后 break */

⑩ end if

⑪ end for

算法收敛速度同具体输入数据有关,输入数据比较单一(潜在融合结果较少),模型收敛较快,第 5 节给出了模型的收敛速度的实验结果.

最后,在数据融合模型基础上,根据 s_k 同输入数据 $f_{t,i}$ 关联度的概率分布,验证某一时刻 t 之前 P 个时隙的数据输入(对应特征摘要为 $F_t = \{f_{t,1}, f_{t,2}, \cdots, f_{t,P}\}$)是否可以驱动数据融合过程得到输出的融合结果集合 S_t,具体检测步骤如下:

1) 按照 3.1 节感知层数据特征摘要机制收集时刻 t 之前的 P 个时隙的数据特征摘要.

2) 分析收集到的数据融合结果,根据模型中该融合结果对应的输入特征摘要序列 $\langle f_{k,1}, f_{k,2}, \cdots, f_{k,n}\rangle$ 及其概率分布 $\langle w_{k,1}, w_{k,2}, \cdots, w_{k,n}\rangle$,计算当前输入数据的特征摘要的匹配度 d_t,具体步骤如下:

① 计算模型中特征摘要和输入的特征摘要间的相似度:

$$f_k - f_t = \sum_{i=1}^{M} |b_{k,i} - b_{t,i}|, \tag{6}$$

其中,M 为数据特征摘要对应的布隆过滤器的单元数,$b_{k,i}$ 和 $b_{t,i}$ 分别为任一模型特征摘要 f_k,和任一输入特征摘要 f_t 的布隆过滤器相同位置上的单元;

② 计算当前输入数据的特征摘要同模型特征摘要序列的匹配度 d_t:

$$d_t = \sqrt{\sum_{i=1}^{N} w_{k,i} \sum_{j=1}^{p} (f_{k,i} - f_{t,j})^2}; \tag{7}$$

3) 如果匹配度高于 d_t 检测阈值 μ 则为正常融合结果,否则为恶意数据篡改.

攻击检测的计算复杂度:单位时间内采集的感应数据有限,因此 M 为确定常数,同时检测周期长度 P 同数据融合操作时延有关,具有上界,因此,上述攻击检测的计算复杂度为 $O(KN)$,其中,数据融合结果数量 K 和每个数据融合结果涉及的输入数据个数 N 由相关融合过程决定.

4 实验与结果分析

在本节中,我们实现了本文提出的攻击检验机制,并且通过对比验证了其准确性和效率.

4.1 实验实现

4.1.1 数据集

论文中在文献[20]的智能家居数据集基础上,构建了用于验证数据融合过程中攻击检测效果的数据. 原始数据集中包括多个城市、家庭的设备数据. 主要包括热水器、空调和家居机器人 3 类设备获取的水温、气温和耗电量等信息,数据最大采样间隔为 10 s. 同时数据中给出了设备相应的可选决策,如开始加热、停止加热等操作. 为了能够有效评估本文安全验证模型对节点数据融合的准确性,通过对该数据集中相关数据的收集和整理,本文提取并采用了 200 个实体(70 台空调、70 台热水器和 60 台家居

机器人)为期 10 min 至 1 h 的不同时间规模的多个实验数据集,每项数据都包括设备报告的水温、气温和现有电量数据同相关决策状态的组合,数据集具体信息如表 1 所示:

Table 1 The Information of Datasets

表 1 实验数据集信息

Datasets	Time Period/min	Datasets Size
DS-10	10	12 000
DS-20	20	24 000
DS-30	30	36 000
DS-40	40	48 000
DS-50	50	60 000
DS-60	60	72 000

数据集中单个实体产生重复数据的概率为 50%. 同时,为了评估攻击检测方案有效性,本文在上述背景数据中按照参数 $\lambda=20$ 的泊松分布篡改了部分时隙的数据融合结果,每次攻击持续时间服从参数 $1/\lambda=0.2$ 的指数分布,平均攻击持续时间为 5 个时隙,因此包括攻击的时隙数为各数据集总时隙数的 1/100.

4.1.2 方案及对比方案实现

为了验证本文方案的准确性和效率,本文基于文献[10]实现了基于采用二阶差分过滤器和序贯概率比检测法的攻击检测机制,并根据文献仿真部分的参数优化了该方案的参数设置,其中用户设定假阳性率为 10%,检测周期为 5 个时隙,保证了该方案验证结果的有效性.

同样,本文方案(EDIoT)的参数均依照第 2.2 节中的安全规约配置,其中,考虑到检测准确率和假阳性率之间的制约关系,基于实验经验值,单次攻击检测阈值设为 $\mu=0.8$,在避免过高的假阳性率的前提下通过多时隙(检测周期 P 为 5 个时隙)检验保证检验准确性. 基于 5 个时隙的数据规模,将布隆过滤器的长度为 500 个单元,每个单元一个字节,采用 3 个 32 为 murmur Hash 函数[17]. 根据多项分布共轭的凸函数特性,基于实验经验值优化相关概率图模型参数,其中超参数 $\lambda=0.2$,$\eta=0.1$,模型生成收敛阈值 $\varepsilon=0.005$.

4.2 实验和结果

4.2.1 攻击检测准确性评估

本节通过准确率(P_R)和假阳性率(FP_R)来评估数据融合过程安全检验的准确性. 准确率用于衡量攻击检测的准确程度:

$$P\_R=\frac{A}{N}, \tag{8}$$

其中,A 为正确检验攻击次数(时隙数),N 为总攻击检测次数.

本文分别对比了本文方案与对比方案在单时隙及 5 时隙后检测攻击的准确率 P_R,结果如图 4 所示. 单时隙下 2 个检测机制的检测准确性均大于 60%,其中对比方案的准确性略高于本文方案,究其原因是基于输入压缩表示(布隆过滤器)的检测过程引入了额外的可控误差,对检测准确性有所影响. 同时当经过 5 个时隙的检测后,2 方案的检测准确性均超过 98%,均能准确发现攻击,5 个时隙作为检查周期比较合理.

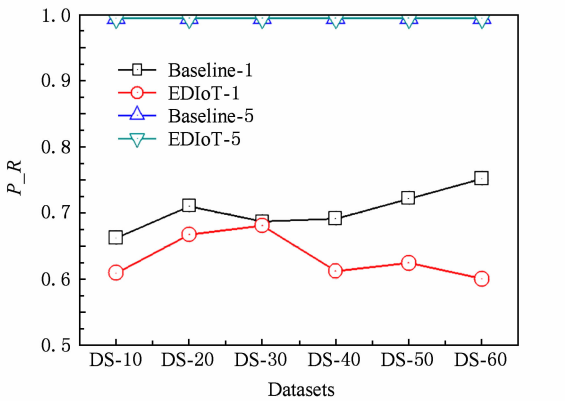

Fig. 4 Comparison of precision rate (P_R)

图 4 准确率对比

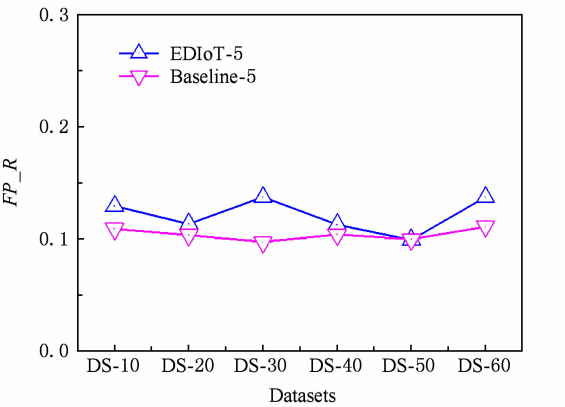

Fig. 5 Comparison of false positive rate (FP_R)

图 5 假阳性率对比

为了衡量攻击检测过程中误判的情况,我们引入了假阳性率 FP_R:

$$FP\_R=\frac{B}{N}, \tag{9}$$

其中,B 为将正常数据融合被检验为攻击的次数. 从图 5 可以看出,本文方案虽然由于数据压缩表示引入

了少量误判,但是通过合理设置布隆过滤器长度,有效控制了攻击检测中的假阳性,假阳性率同对比方案相近,均小于 13%,在数据 DS-50 上平均假阳性率为 9.95%,略小于对比方案的假阳性率 9.97%,本文方案在攻击检测中的误判可以控制在较小范围.

4.2.2 检测效率评估

首先,为了评估本文模型生成效率及其影响因素,在不同数据集上,利用 3.3 节算法构建模型,模型中包含的融合结果及模型生成过程中的迭代次数如图 6 所示. 可以看出模型中数据融合结果的数量同数据采集次数(总数据量)无关,融合结果的数量会对模型收敛时的经历的迭代次数产生影响,融合结果较多的数据集上模型收敛速度较慢.

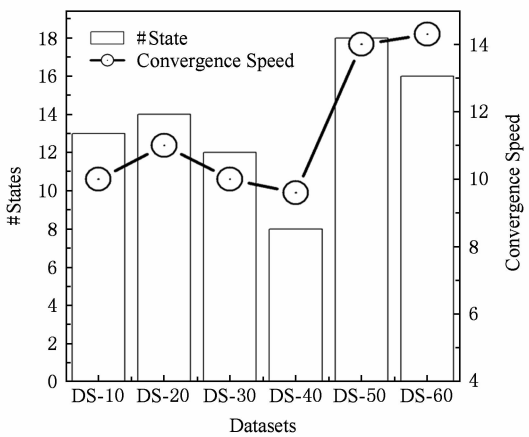

Fig. 6 The states of the generated models and their convergence

图 6 模型数据融合结果数量及模型收敛情况

检测时延是衡量攻击检测效率的关键因素,本文检测时延是指攻击发生到攻击被检测到的时延的平均值. 本文检测机制和对比方案在检测攻击过程中的检测时延如图 7 所示:

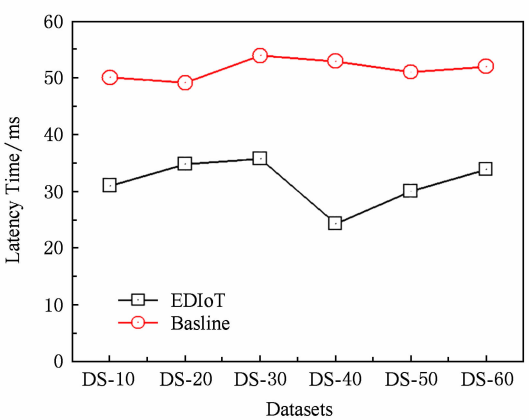

Fig. 7 Comparison of detection latency

图 7 检测时延对比

从图 7 可以看出,为了检测攻击,本文攻击检测机制时延相对较小,本文实验均小于 37 ms,对比方案时延在 50 ms 左右,时延差异主要是由检测机制本身计算复杂度的差异所导致,相对于二阶差分过滤器和序贯概率比检测法的运算复杂度,本文检测过程仅包括基本运算,复杂度较低.

5 总 结

物联网数据融合过程中存在的数据伪造、篡改攻击会扰乱甚至损害物联网的正常使用. 在物联网资源受限、大数据流量、高时效性的特性对攻击检测机制提出了新的挑战,本文提出了一套高效的数据收集和建模方案,在提升攻击检测准确性的同时,最大程度地优化攻击检测效率和资源消耗. 本文方案通过对压缩表示的数据及其融合过程建模,发现并刻画被输入数据和融合结果之间的联系,并利用这一模型快速发现异常的数据融合结果,防范恶意数据融合操作,优化了物联网传输安全. 方案采用压缩表示机制处理输入数据,屏蔽了不同数据类型的差异性,可以广泛应用于各类新型物联网数据融合场景.

参 考 文 献

[1] Hu Lingxuan, Evans D. Secure aggregation for wireless networks [C] //Proc of the 1st IEEE Applications and the Internet Workshops. Piscataway, NJ: IEEE, 2003: 384-391

[2] Bagaa M, Lasla N, Ouadjaout A, et al. Sedan: Secure and efficient protocol for data aggregation in wireless sensor networks [C] //Proc of the 32nd IEEE Conf on Local Computer Networks. Piscataway, NJ: IEEE, 2007: 1053-1060

[3] Ozdemir S, Yang Xiao. Integrity protecting hierarchical concealed data aggregation for wireless sensor networks [J]. Computer Networks, 2011, 55(8): 1735-1746

[4] Çam H, Özdemir S, Nair P, et al. Energy-efficient secure pattern based data aggregation for wireless sensor networks [J]. Computer Communications, 2006, 29(4): 446-455

[5] He Wenbo, Liu Xue, Nguyen H, et al. Pda: Privacy-preserving data aggregation in wireless sensor networks [C] //Proc of the 26th IEEE Int Conf on Computer Communications. Piscataway, NJ: IEEE, 2007: 2045-2053

[6] He Wenbo, Nguyen H, Liu Xue, et al. iPDA: An integrity-protecting private data aggregation scheme for wireless sensor networks [C] //Proc of the 27th IEEE Military Communications Conf. Piscataway, NJ: IEEE, 2008: 1-7

[7] Mukhopadhyay S, Panigrahi D, Dey S. Model based error correction for wireless sensor networks [C] //Proc of the Annual IEEE Communication Society Conf on Sensor, Mesh and Ad Hoc Communication and Networks. Piscataway, NJ: IEEE, 2004: 575-584

[8] Liu Yanbing, Gong Xuehong, Feng Yanfen. Trust system based on node behavior detection in Internet of things [J]. Journal on Communications, 2014, 35(5): 8-15

[9] Sun Bo, Shan Xuemei, Wu Kui, et al. Anomaly detection based secure in-network aggregation for wireless sensor networks [J]. IEEE Systems Journal, 2013, 7(1): 13-25

[10] Yang Lijun, Ding Chao, Wu Meng, et al. Robust detection of false data injection attacks for data aggregation in an Internet of things-based environmental surveillance [J]. Computer Networks, 2017, 129: 410-428

[11] Tan Chiuchiang, Sheng Bo, Li Qun. Severless search and authentication protocols for RFID [C] //Proc of the 5th Annual IEEE Int Conf on Pervasive Computing and Communications. Piscataway, NJ: IEEE, 2007: 3-12

[12] Zhu Ming, Bian Jinian, Wu Weimin. A novel collaborative scheme of simulation and model checking for system properties verification [J]. Computers in Industry, 2006, 57 (8/9): 752-757

[13] Jones G D, Allsop R E, Gilby J H. Bayesian analysis for fusion of data from disparate imaging systems for surveillance [J]. Image and Vision Computing, 2003, 21(10): 843-849

[14] Mohan C K, Mehrotra K G, Varshney P K, et al. Temporal uncertainty reasoning networks for evidence fusion with applications to object detection and tracking [J]. Information Fusion, 2007, 8(3): 281-294

[15] Haenni R, Hartmann S. Modeling partially reliable information sources: A general approach based on Dempster-Shafer theory [J]. Information Fusion, 2006, 7(4): 361-379

[16] Llinas J, Bowman C, Rogova G, et al. Revisiting the JDL data fusion model Ⅱ [C] //Proc of the 7th Int Conf on Information Fusion. Stockhol, Sweden: P Svensson & J Schubert, 2004: 36-78

[17] Fan Li, Cao Pei, Almeida J, et al. Summary cache: A scalable wide-area Web cache sharing protocol [J]. IEEE/ACM Trans on Networking, 2000, 8(3): 281-293

[18] Blei D M, Griffiths T L, Jordan M I. The nested chinese restaurant process and Bayesian nonparametric inference of topic hierarchies [J]. Journal of the ACM, 2010, 57(2): 17-24

[19] Geman S, Geman D. Stochastic relaxation, Gibbs distributions, and the Bayesian restoration of images [J]. Journal of Applied Statistics, 1984, 20(5-6): 25-62

[20] Fioretto F, Yeoh W, Pontelli E. A multiagent system approach to scheduling devices in smart homes [C] //Proc of the 16th Conf on Autonomous Agents and MultiAgent Systems. New York: ACM, 2017: 981-989

Xu Zhiwei, born in 1979. PhD candidate in Institute of Computing Technology, Member of CCF. His main research interests includes future Internet, dependable and secure computing.

Zhang Yujun, born in 1976. Professor and PhD supervisor of Institute of Computing Technology, Chinese Academy of Sciences, China. Member of CCF. His main research interests includes future Internet, Internet security assessment and verification (zhmj@ict.ac.cn).