

基于语义的物联网电子商务网购商品溯源算法

张婷婷¹, 葛 静²

- (1. 安徽机电职业技术学院 信息工程系, 安徽 芜湖 241000;
2. 安徽交通职业技术学院 管理工程系, 安徽 合肥 230051)

摘 要:电子商务网购产品的假货、水货现象严重,如何利用现有的物联网实现产品溯源是个重要的研究课题。文中将传统溯源算法、公共密钥加密算法、语义路由的思想相结合,提出一种基于语义的电子商务网购产品溯源算法。配合查询算法,可快速判断网购商品身份。该算法中,一个感知节点只需要关心自己通信范围内的邻居节点,不需要知道整个网络的状况。仿真结果表明,算法具有冗余数据少、能耗小、响应快速、实现简单等特点。

关键词:电子商务;物联网;语义路由;溯源算法;公共密钥加密算法

中图分类号:TP301.6

文献标识码:A

文章编号:1673-629X(2013)05-0213-03

doi:10.3969/j.issn.1673-629X.2013.05.055

Traceback Algorithm for E-Commerce Goods in Internet of Things Based on Semantic Thought

ZHANG Ting-ting¹, GE Jing²

- (1. Department of Information Engineering, Anhui Technological College of Machinery and Electricity, Wuhu 241000, China;
2. Department of Management Engineering, Anhui Communication Vocational & Technical College, Hefei 230051, China)

Abstract: The problem of that E-Commerce goods are smuggled or fake is serious. How to trace the back of the E-Commerce goods using Internet of Things is an important research problem. In this paper, a traceback algorithm based on semantic thought combining traditional traceback algorithm, public key encryption is proposed. With the query algorithm, it can judge the identity of the E-Commerce goods. In this algorithm, every perception node only concerns the nodes in its own communication range instead of knowing all the nodes in net. The simulation results show that the algorithm is less redundant data, lower query consumption, quick response and easier implementation.

Key words: E-Commerce; Internet of Things; semantic routing; traceback algorithm; public key encryption algorithm

0 引 言

电子商务近年来发展迅速,网络销售成为商品的又一主要销售模式。但网上市场充斥的大量假货、水货现象比较严重,这在一定程度上降低了网络零售企业的诚信度^[1],给消费者带来了损失。因此,怎样高效快速地对网购商品进行溯源,确定其是否为真货、行货是目前面临的紧迫挑战。

物联网是继计算机、互联网与移动通信网之后的世界信息产业第四次技术革命,指的是将各种信息传

感设备,如射频识别 RFID 装置、红外感应器、全球定位系统、激光扫描器等装置与互联网结合起来而形成的一个巨大网络^[2],可实现物物互联,实时地对物体进行识别、定位、追踪、监控等目的,符合溯源系统的技术要求^[3]。

物联网是一种资源受限的无线网络。目前,国内外已经提出一些基于资源受限无线网络的溯源算法。文献[4]中提出 CAPTRA (Coordinated Packet Traceback) 方法,利用广播特性,转发节点和监听节点交换信息,构造整条路径;文献[5]中提出 CTrace (Contact-based Traceback in Wireless Sensor Networks) 方法,通过联系人列表使得每个节点都能够构造出一条连通某个联系人的路径,最终追溯到数据源节点;文献[6]中提出 FBT (an efficient traceback scheme in hierarchical wireless sensor network),利用分层的标记方式可以迅

收稿日期:2012-08-13;修回日期:2012-11-16

基金项目:2010 年高校省级优秀青年人才基金项目(2010SQRL205)

作者简介:张婷婷(1983-),女,安徽芜湖人,讲师,硕士,研究方向为计算机应用、电子商务、无线网络;葛 静,硕士,副教授,研究方向为电子商务、企业管理。

速构造出由分簇头节点构成的路径主干部分,还可以再重构造出每个分簇内的详细路径;文献[7]提出 PNM (Probabilistic Nested Marking) 溯源算法,通过嵌套式存储经过加密的节点信息,解决多节点协同攻击带来的溯源问题。这些溯源算法各有优缺点,但都不适合电子商务网购商品的溯源。

文中结合了传统溯源算法、公共密钥加密算法、语义路由的思想,在物联网环境下,提出一种基于语义的电子商务网购商品溯源算法,可以防止不法商家篡改、伪造商品信息,帮助消费者快速判断所购商品是否为真货、行货。该算法中,一个感知节点只需要关心自己通信范围内的邻居节点,不需要知道整个网络的状况,算法具有冗余数据少、能耗小、响应快速、实现简单等特点。

1 数据的存储

1.1 相关定义

(1) 感知节点。

物联网感知层负责监测、处理、中短距离传输数据,具体可以选用 WSN 技术、RFID 技术^[8]等。文中,装置感知层设备的商品统称感知节点,记为 Node。

(2) 商品 ID。

ID 号是同类商品的唯一编号,出厂时已经指定,不能更改。

(3) 公共密钥和私有密钥。

公共密钥和私有密钥分别记为 PubK 和 PriK,成对出现,相互不能推算出,且加密解密必须一一对应。

(4) 销售中转地。

销售中转地是商品的预定销售区域路径,有层次关系,记为 TA (ta1, ta2, ta3, ..., tan), 实际商品若符合预订销售路径,即可认为是行货。

(5) 邻居列表。

邻居列表用于记录当前感知节点通信距离为 1 范围内的所有其他感知节点的 ID,用于构建逻辑覆盖网络,记为 List_Neighbor(1, 2, ..., n)。

(6) 当前所在地。

感知节点到达中转地时,通过自身感知设备定位所在地,记为 TA_Now。

(7) 邻居节点中转地。

邻居节点中转地是当前感知节点邻居列表 List_Neighbor 中的某一个节点的销售中转地 TA,记为 TA_Neighborn(ta1, ta2, ta3, ..., tan)。

(8) 写入标识。

记为 Flag,当 Flag 值为 1 时,动态属性 TA_Neighborn(ta1, ta2, ta3, ..., tan) 允许被写入,当值为 0 时,拒

绝写入。

1.2 感知节点的数据结构模型

感知节点的属性分为静态属性和动态属性。静态属性是出厂时已经固化的信息,不能被修改,动态属性可以动态更新和维护。文中,感知节点动态属性用二维表 List_D 表示,静态属性用二维表 List_S 表示。

(1) 静态属性表(List_S)。

静态属性包括:节点唯一编号(ID)、销售中转地 TA (ta1, ta2, ta3, ..., tan)、公共密钥 I (PubK I)、私有密钥 II (PriK II)、私有密钥 III (PriK III) 和商品基本信息(Inf)。List_S 格式见表 1。

表 1 静态属性表 List_S

ID	TA (ta1, ta2, ta3, ..., ta n)	PubK I	PriK II	PriK III	Inf
----	-------------------------------	--------	---------	----------	-----

(2) 动态属性表(List_D)。

动态属性包括:邻居列表(List_Neighbor)、邻居节点中转地(TA_Neighborn(ta1, ta2, ta3, ..., tan))、当前所在地(TA_Now)、写入标识(Flag)。List_D 格式见表 2。

表 2 动态属性表 List_D

List_Neighbor(1)	TA_Neighbor ₁ (ta1, ta2, ta3, ..., ta n)	TA_Now ₁	Flag ₁
List_Neighbor(2)	TA_Neighbor ₂ (ta1, ta2, ta3, ..., ta n)	TA_Now ₂	Flag ₂
.....			
List_Neighbor(n)	TA_Neighbor _n (ta1, ta2, ta3, ..., tan)	TA_Now _n	Flag _n

2 基于语义路由的电子商务商品溯源算法

2.1 语义表示

语义路由就是利用查询关键字与节点的映射关系,将查询请求转发给一部分被认为最有可能满足请求的节点。这种方法类似于前缀匹配,但它是直接将资源关键字映射到资源索引位置,查询关键字采用与资源关键字相同的语义表示形式。这样,查询关键字就与索引位置产生对应关系^[9]。文中,要建立查询关键字与感知节点索引位置的对应关系,这样,就可以通过查询关键字将查询数据包路由到相应的感知节点,完成相应操作。

确定合适的查询关键字是文中算法的关键。对于 1.2 中的数据结构,可选择每个感知节点的 List_D、List_S 中的内容可作为资源关键字,即资源关键字为 RK (Neighbor(n)_ID, TA_Neighborn(ta1, ta2, ta3, ..., tan), TA_Nown, Flagn)。查询关键字 QK 采用与资源关键字相同的语义表示 QK (Neighbor(n)_ID, TA_Neighborn(ta1, ta2, ta3, ..., tan), TA_Nown, Flagn)。这样,查询关键字就与索引位置(感知节点位置)有了对应关系。

2.2 溯源算法

设生产厂家生成三对密钥,这三对密钥符合公共

密钥算法的要求,一一对应,且彼此不能推导。植入商品感知设备中的为公共密钥 I (PubK I)、私有密钥 II (PriK II)、私有密钥 III (PriK III),而 PubK I 和 PubK II 通过官方渠道发布,可被消费者查询。感知节点出厂前静态属性表 List_S 均被 PriK I 加密。感知节点每新到一个销售中转地启动感知设备,执行溯源算法,其余时间均处于休眠状态,最大程度地节约资源。溯源算法描述如下:

1) 所有非深度睡眠的节点苏醒, Nodex 感知自己路径 1 范围内的所有邻居节点,构造 Nodex. List_D [List_Neighbor]。//深度睡眠节点能被其他节点读取和写入,但不能对其他节点执行操作,只有在执行 2.3 查询算法时才能苏醒,最大程度上节约资源。

2) 设置 Nodex. List_D [Flag] 为 1。

3) 感知当前所在地 Nodex. List_D [TA_Now]。

4) 按照 Nodex. List_D [List_Neighbor] 的顺序,依次用 Nodex. List_S [PubK I] 对 List_Neighbor (n). List_D 解密,发送查询关键字 QK (Neighbor (n)_ID, TA_Neighbor (ta1, ta2, ta3, ..., tan), TA_Nown, Flag), 并返回查询结果。

5) 从 QK 返回结果中读取内容 TA_Nown, 并和自己检测到的 TA_Nowx 对照,若一致,构造 Nodex. List_D [TA_Nowx], 若不一致, Node (x) 和 Node (n) 重新检测。//通过核对 Node (x) 和 Node (n) 检测到 TA_Now, 最大程度保障当前所在地信息的准确性。

6) 从 QK 返回结果中读取内容 Flag, 依次检测 List_Neighbor (n). List_D [flag], 若为 0, 继续检测下个节点,直到找到 List_Neighbor (n). List_D [flag] = 1 的节点,执行 7), 若一直没找到,则进入休眠状态。

7) 从 QK 返回结果中读取内容 TA_Neighbor (ta1, ta2, ta3, ..., tan), 比较 Nodex. List_D [TA_Nowx] 是否存在于 List_Neighbor (n). List_D [TA_Nown] 中,若存在,则表示目前 n 节点为行货。将 List_Neighbor (n). List_D [flag] 改为 0, 阻止再次写入,并用 Nodex. List_D [PriK II] 加密,防止非法商家修改 List_D。销毁 List_D [PriK II], 防止非法商家获得。转入深度睡眠状态。//非法商家无法获得 PriK II, 不能对伪造或篡改的商品信息进行合法加密,2.3 中的查询算法可以轻松察觉商品信息是否已经被修改。

8) 若不存在,则表示 n 节点为水货,用 Nodex. List_D [PriK III] 加密。转入深度睡眠状态。// PukK III 没有公布,所以用 Nodex. List_D [PriK III] 加密的信息在 2.3 中无法解密,可认为标识为水货。

2.3 查询算法

消费者收到所购商品后,通过官方途径获得 PubK 和 PubK II, 启动感知节点中的查询算法,可以确定所

购商品是否为真货、行货。查询算法描述如下:

1) 用 PubK I 解密 Nodex. List_S, 若解密失败,则说明该商品静态信息被非法中间商篡改或伪造,查询结果显示 Nodex 为假货,停止下面步骤。

2) 若成功解密,获取 Nodex. List_S [ID] 上官网查询,若一致,结果显示 Nodex 为真货,否则为假货。

3) 用 PubK II 解密 Nodex. List_D, 可能需要解密多次,若解密失败,说明商品动态信息被非法中间商篡改或伪造,或被其他节点识别为水货,查询结果显示 Nodex 为水货。若解密成功,获取 Nodex. List_S [TA (ta1, ta2, ta3, ..., tan)], 上官网查询,若一致,结果显示 Nodex 为行货,否则为水货。

3 性能分析

从 2.2 的溯源过程可以看出,查询节点将请求 QK (Neighbor (n)_ID, TA_Neighbor (ta1, ta2, ta3, ..., tan), TA_Nown, Flag) 发送到周围路径为 1 的节点上,因为被查询信息都是自身已存储信息,所以可以直接回应查询节点,耗时 $O(1)$, 可忽略不计。

设感知节点总数为 N 。在信息写入阶段,写入节点依次寻找路径为 1 的邻居节点中满足条件的目的节点。一次溯源算法中,每个节点只被写入一次。写入延时忽略不计,平均寻找次数为 $O(\log_2 N)$ 。

OMNET++ 是开源的基于组件的模块化的开放网络仿真平台,可以对溯源算法进行很好的仿真^[10,11]。文中分别从网络延时、路由跳数两个方面,对文中溯源算法进行性能分析。网络延时计算公式为: $\text{delay} = (\text{receive_time} - \text{send_time}) / \text{num}$, 其中, receive_time 表示接收包的时间; send_time 表示发送包的时间; num 表示发包的数量; delay 的单位是 s。

从图 1 可以看出,文中溯源算法的网络时延大部分分布在 0 ~ 0.045s 之间,这是因为节点之间的路由跳数为 1, 再加上文中溯源算法的简单性,传输延时很小,符合物联网的实时性要求。

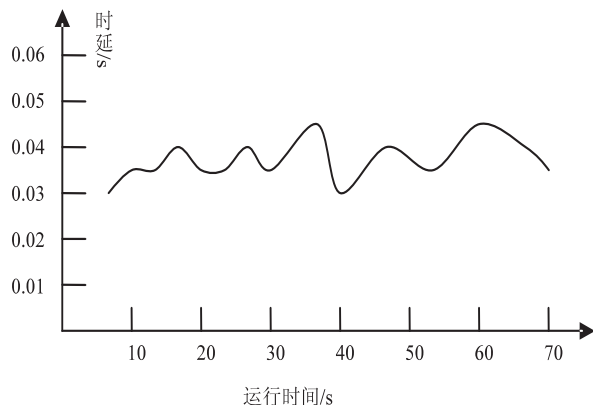


图1 文中算法的网络时延曲线

控人员评估安全提供量化的依据。

表2 系统管理 Agent 消息——动作映射表(部分)

消息号	系统管理 Agent 所做动作
1	将此消息通知事故处理 Agent,新建一个井控事故处理任务,任务标识为 JK+事故标识,报告新事故到达消息,其中包括事故相关信息,将任务 OPP 状态改为正执行
2	将消息通知事故处理 Agent,报告事故处理已初步处理信息,将任务 OPP 状态改为完成,任务 OD 状态改为正执行
3	将消息通知事故处理 Agent,同时将任务 OD 状态改为完成,因为任务 JKAD 的子任务完成,将 JKAD 的状态改为已完成,任务 JGCZ 改为正执行
4	将消息通知司钻 Agent,执行 XXCD 任务,启动 QDXH(关井信号)
5	将消息通知司钻 Agent,增加 open 任务置设备液动防喷闸 Agent 状态为开;同时执行 XXCD 任务,启动 LLSS(开),并将消息通知副司钻 Agent
6	副司钻 Agent 读取远程控制台 Agent 状态;同时执行 XXCD 任务,启动 LLSS(开),并将消息通知司钻 Agent
7	将消息通知司钻 Agent,增加 close 任务置设备环形防喷器 Agent 状态为关;同时执行 XXCD 任务,启动 LLSS(关),并将消息通知副司钻 Agent
8	副司钻 Agent 读取远程控制台 Agent 状态;同时执行 XXCD 任务,启动 LLSS(关),并将消息通知司钻 Agent

参考文献:

[1] 周长虹. 井控安全技术 在钻井企业的重要应用[J]. 科技资讯,2012(3):99-99.

[2] Dziurzynski W, Roszkowski J, Tobiczyn J. Monitoring and con-

trol of ventilation in polish coal mines[C]//Proc of 8th International Mine Ventilation Congress. [s. l.]:[s. n.],2005:309-315.

[3] Mironowicz W, Wasilewski S. Monitoring of natural hazards in the underground hard coal mines[C]//Proc of International Mining Forum on New Technological Solutions in Underground Mining. [s. l.]:[s. n.],2006:87-94.

[4] Cotton S, Dennison-Johnson A, Giraldo L. Mine Escape Vehicle (MEV) Concept Development[C]//SME Annual Meeting and Exhibit 2010. [s. l.]:[s. n.],2010:206-209.

[5] 王武礼,王延江,杨华,等. 钻井井控仿真中多 Agent 系统建模研究[J]. 石油天然气学报,2008,30(5):120-123.

[6] 李慧琴,薛霄. 多 Agent 系统仿真平台[J]. 计算机系统应用,2012,21(5):8-11.

[7] Nwana H S, Ndumu D T, Lee L C, et al. ZEUS: A Toolkit for Building Distributed Multi-Agent System[J]. Applied Artificial Intelligence Journal, 1999, 13(1):129-185.

[8] 王武礼. 钻井井控仿真中多 Agent 系统建模研究[D]. 北京:中国石油大学,2007.

[9] 尹全军. 基于多 Agent 的计算机生成兵力建模与仿真[D]. 长沙:国防科技大学,2005.

[10] 耿建鲁. 基于黑板系统的多智能体系统实现方法的研究[D]. 哈尔滨:哈尔滨工程大学,2003.

[11] 张俊瑞,陈立潮,潘理虎,等. 基于 Agent 的井下透水事故逃生模型研究[J]. 计算机技术与发展,2012,22(7):197-200.

(上接第 215 页)

4 结束语

文中提出一种在物联网环境中基于语义的电子商务网购商品溯源算法,这种溯源算法的创新在于结合传统溯源算法、公共密钥加密算法、语义路由的思想,可以防止不法商家篡改、伪造商品信息,帮助消费者快速判断所购商品是否为真货、行货。新算法具有冗余数据少、能耗小、响应快速、实现简单等优点。但是该算法是在假设所有感知节点都能至少被邻居节点访问一次的情况下提出的,对于极少数没有被访问过的感知节点,查询结果可能会出现错误,这是今后要研究的重点问题。

参考文献:

[1] 徐秋丽. 水货假货严重危害电子商务发展[EB/OL]. 2012 [2012-02-11]. <http://news.163.com/12/0211/04/7PV3304U00014AED.html>.

[2] 胡清,詹宜巨,黄小虎. 基于 RFID 企业物联网及中间件技术研究[J]. 微计算机信息,2009(20):158-160.

[3] 李园园,毕晓冬,张永胜,等. 物联网框架安全威胁及相应策略研究[J]. 计算机技术与发展,2011,21(12):149-150.

[4] Sy D, Bao Lichun. CAPTRA: Coordinated Packet Traceback[C]//Proceedings of 5th International Conference on Information Processing in Sensor Networks. [s. l.]:[s. n.],2006:152-159.

[5] Zhang Qiyuan, Zhou Xuehai, Yang Feng. CAPTRA: Coordinated Packet Traceback[C]//Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing. [s. l.]:[s. n.],2007:2487-2490.

[6] Cheng Bochao, Chen Huan, Liao Guotan. FBT: an efficient traceback scheme in hierarchical wireless sensor network[J]. Security and Communication Networks, 2009, 2(2):133-144.

[7] Ye Fan, Yang Hao, Liu Zhen. Catching "Moles" in Sensor Networks[C]//IEEE International Conference on Distributed Computing Systems. [s. l.]:[s. n.],2007.

[8] 叶东海,吕捷. 考虑安全与公平的电子市场[J]. 南京师范大学学报(工程技术版),2010(4):84-86.

[9] 张婷婷,周鸣争,许金生,等. 无线传感器网络中基于语义路由的事件查询算法[J]. 仪器仪表学报,2008,29(6):1661-1662.

[10] 李占波,邵金华,刘冬冬. 基于 Chord 算法的物联网信息查询机制[J]. 计算机工程,2011,37(23):108-109.

[11] 张靖,景旭,孙晓波,等. AODV 协议的简单智能化研究[J]. 哈尔滨理工大学学报,2005(1):115-117.

基于语义的物联网电子商务网购商品溯源算法



作者：[张婷婷](#)，[葛静](#)
作者单位：[张婷婷\(安徽机电职业技术学院 信息工程系, 安徽 芜湖 241000\)](#)，[葛静\(安徽交通职业技术学院 管理工程系, 安徽 合肥 230051\)](#)
刊名：[计算机技术与发展](#)
英文刊名：[Computer Technology and Development](#)
年，卷(期)：2013(5)

本文链接：http://d.g.wanfangdata.com.cn/Periodical_wjtz201305057.aspx