



工业无线传感云中面向移动机器人的自适应信任演化机制

刘建华^{1,2}, 李明禄², 李大志^{2,3}, 李鲁群³

(1. 嘉兴学院数理与信息工程学院, 浙江 嘉兴 314001;

2. 上海交通大学计算机科学与工程系, 上海 200240;

3. 上海师范大学信息与机电工程学院, 上海 200234)

摘要: 在智能制造系统中, 工业无线传感器网络和生产设备以分散的、无人值守的方式运行。传感云作为一种潜在的技术能有效地集成分散的设备为云服务并提供给移动机器人使用。当移动机器人通过传感云平台访问远程云设备时, 由于潜藏的攻击者容易通过无线信道截获密钥并窃听设备操作内容, 这使得密钥管理和设备操作权限的控制成为其安全、可靠运行的关键。形式化了博弈参与者的效用函数, 对自适应信任度更新过程进行了分析, 提出了基于演化博弈的自适应信任管理机制。仿真结果显示, 提出的方法能有效提高传感云网络系统和设备的安全性。

关键词: 云计算; 无线传感器网络; 博弈论; 信任管理

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2017125

Adaptation trust evolution scheme for mobile robot in industrial wireless sensor-cloud

LIU Jianhua^{1,2}, LI Minglu², LI Dazhi^{2,3}, LI Luqun³

1. College of Mathematics Physics and Information Engineering, Jiaxing University, Jiaxing 314001, China

2. Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

3. College of Information, Mechanical and Electrical Engineering, Shanghai Normal University, Shanghai 200234, China

Abstract: Industrial wireless sensor networks and production equipments are deployed in unattended and distributed intelligent manufacturing system (IMS). Sensor-cloud as a potential technology can effectively integrate distributed equipments as a service and provide it to mobile robots. However, when the mobile robots access the remote devices via sensor-cloud platform, because potential attackers easily intercept keys and eavesdrop equipment operation contents through wireless channels, which makes the key management and the control of equipment operation permission become crucial to the safe and reliable operation of IMS. Therefore, the utility function of game players were formalized, the adaptive trust update process was analyzed, and an adaptive trust management mechanism based on evolutionary game was proposed. Simulation results show that the proposed method can effectively improve the security of sensor-cloud network systems and equipments.

Key words: cloud computing, wireless sensor network, game theory, trust management

收稿日期: 2016-11-21; 修回日期: 2017-05-06

基金项目: 国家自然科学基金资助项目 (No.61572014); 浙江省自然科学基金资助项目 (No.LY16F020028)

Foundation Items: The National Natural Science Foundation of China (No.61572014), The Natural Science Foundation of Zhejiang Province of China (No.LY16F020028)

1 引言

在智能制造系统中,工业无线传感器网络和生产设备以分散的、无人值守的方式运行。传感云作为一种潜在的技术能有效地集成分散的设备为云服务并提供给移动机器人使用,例如自动化生产工厂中的多个移动机器人可以通过传感云平台使用云设备服务。工业无线传感云平台被认为是提高智能制造效率的关键网络系统之一,智能制造企业的工业机器人通过无线网络接入传感云平台后,使用远程云设备生产和制造零部件,充分提高了空闲机床和生产设备的利用率,为企业节约了生产成本。这种协作生产模式已广泛应用于各种智能制造系统中,例如军工制造和机械加工系统。因此,面向机器人的工业无线传感云技术逐渐成为实现机器换人的一项新技术^[1]。然而,当部署云制造系统时,由于工业生产现场恶劣的电磁环境,云平台和无线传感器网络防御攻击的脆弱性,给云制造系统带来了一定的安全威胁。例如工业无线机器人被部署在自动化生产企业时,容易被攻击者伪造成一个合法机器人来访问和控制远程云设备,从而使远程云设备停机,给企业造成重大经济损失。参考文献[2]对公有云的安全现状进行梳理,总结了目前公有云面临的主要的安全技术问题,分析了每种技术的优缺点,并对公有云的安全防范策略提出建议。

虽然传统的加密技术能够增强传输信息的保密性,密钥的长度也可以增加攻击者解码的困难。例如参考文献[3]介绍了同态加密在云计算机密性保护及其他方面的应用,重点介绍了各种代数部分同态加密方案和电路全同态加密方案的优缺点,对同态加密未来的研究问题进行了分析,同时简单介绍了云安全中的明文保密计算概念。但是,由于智能制造系统的资源约束性,使得生产线上的智能机器人持有较短的密钥,这很容易被攻击者在较短的时间内解码。其次,加密技术不

能解决合法节点的验证问题。研究表明可信管理机制能解决以上问题,并增强云制造设备的安全性。参考文献[4]提出一种云可信赖性模型,并系统分析了模型的可信赖特性,给出了云系统可信赖性的定义及可信赖性的度量指标,并进行了量化分析。参考文献[5]基于评价支持度和评价一致性因子提出了一种适用于开放分布式网络环境下的基于信任领域和评价可信度的信任模型。

典型的云制造平台的认证系统由移动机器人、云认证服务提供者、云设备服务提供者组成,其访问控制问题实质上是移动机器人、云认证服务提供者和云设备服务提供者之间的信任演化问题。参考文献[6]分类了无线传感器网络的信任模型,包括贝叶斯信任模型、主观逻辑信任模型、熵信任模型、模糊理论信任模型和博弈论信任模型,为开发信任模型提供了借鉴作用。参考文献[7]针对社会网络中动态可靠的服务组合,提出了基于信任的联盟形成博弈,根据信任度进行服务组合响应查询过程。通过信任度的演化构建多点防护安全网,这比仅依靠加密来增加安全性的单点防护有着天然的优势。

同时,由于工业无线传感器网络的无线广播特性,使得无线介质能够被合法和恶意的用户同时访问,当移动机器人和远程云设备服务接入云平台时,潜藏的攻击者容易通过无线信道截获密钥并窃听设备操作内容,导致了工业无线传感器网络易受到窃听攻击。参考文献[8]建立了云服务提供商和云终端用户之间的重复博弈模型,使用动态贝叶斯博弈理论分析了用户的行为,并对恶意的行为给出了控制机制。参考文献[9]针对已有基于轻量云模型的节点信誉安全方案中存在的决策困难问题以及推荐节点的恶意行为识别问题,提出了优化的轻量云模型,用云隶属度函数计算推荐信任值,在涉及推荐节点信任值计算时可以提高恶意节点识别的准确度。参考文献[10]面向智能设备提出了一种基于云计算的安全服务机制,



在云平台中分析入侵节点,从而为智能设备提供好的安全性。参考文献[11]根据社会物联网节点间的交互建立信任模型来限制恶意节点的攻击。参考文献[12]分析了当前云服务系统的认证需求,提出了一种基于指纹识别的云安全认证系统。通过更加安全的认证方式防止恶意用户的非法访问,保证云环境下用户数据的访问安全。参考文献[13]为了防止恶意攻击者和云计算数据外包中心提供商窃取数据,利用基于证书的信任演化博弈思想研究了移动云用户和云计算数据外包中心动态认证的信任建立问题,为移动云用户提供一种安全高效的数据保护措施。参考文献[14]针对异构移动云网络的安全和私有性,提出了一种切换认证机制。

面对窃听攻击,节点可以通过检测保密容量来确定密钥是否泄露,如果泄露,认证系统立刻升级密钥和设备操作权限,从而有效地防止攻击者掌握所有的权限密钥。参考文献[15]针对工业无线传感器网络中信道的窃听攻击,从物理层角度,提出了优化调度方法提高系统的保密容量,降低窃听攻击者截获信息的概率。

由以上分析可知,针对面向无线传感云的智能制造环境下的信任管理和认证技术的研究成为热点,目前已有的参考文献研究了云环境中恶意行为识别^[8-11]、公有云和私有云访问的认证机制^[12-14]、可信云模型^[4,5]、无线传感器网络信任模型^[6,7]、云数据同态加密^[3]和保密容量^[15]等。在智能制造系统中,密钥管理和设备操作权限的控制成为其安全、可靠运行的关键。如何对移动机器人、云认证服务提供者和云设备服务提供者提供有效的信任管理成为了智能制造系统新的安全挑战。与已有的工作相比,本文基于无线传感云智能制造环境下移动机器人远程操作特点,考虑密钥分发、信任度分配和保密容量等问题,提出了一种面向工业无线传感云的移动机器人自适应的信任演化机制,在机制中使用演化博弈来提高无线传感云设备的安全性。本文的贡献主要包

括:首先,根据工业无线传感云拓扑,提出了一个信任度管理架构和信任度量模型;其次,使用演化博弈论提出了信任度分配框架,给出了信任演化交互过程的效用函数,分析了移动机器人之间的信任演化阶段、移动机器人和云认证服务提供者之间自适应信任度分配阶段;最后,提出了移动机器人自适应信任演化算法。

2 面向移动机器人的信任度量模型

在制造工厂中移动机器人之间信任博弈及移动机器人与云认证服务提供者之间的博弈过程,考虑了动态密钥和设备操作权限的保密程度,提出了信任度分配框架。定义了移动机器人、云认证服务提供者、云设备服务提供者之间信任演化博弈的效用函数。

2.1 信任度量函数

信任度量模型用来测量云设备服务提供服务时,使用云设备服务的移动机器人身份的合法性。为了增加远程生产设备的安全性,本文根据移动机器人通过传感云平台访问远程云设备的特性,提出了信任度量模型。令移动机器人从云认证服务提供者获得的信任度为 d 。信任度量函数有如下特性:

$$H(d) = \begin{cases} h_{\max}, & d > d_{\max} \\ \text{lb}d, & d_{\min} < d < d_{\max} \\ h_{\min}, & d < d_{\min} \end{cases} \quad (1)$$

其中, $h_{\max}$ 表示移动机器人获得信任度的最大值, $h_{\min}$ 表示移动机器人获得信任度的最小值。

2.2 信任度分配框架

本文提出工业传感云中面向移动机器人的信任度分配机制,信任度分配网络架构如图1所示。信任度分配框架有两个目标:一是使得移动机器人能分配足够的信任度来获得设备操作权限;二是云认证服务提供者使用优化的信任度最大化远程云设备的安全性。在信任度分配框架中,博弈参与者分别是移动机器人、云认证服务提供者和

云设备服务提供者。云设备服务提供者决定设备的操作权限, 经由密钥验证后发放给云认证服务提供者。每个云认证服务提供者决定云设备服务权限所需的密钥个数, 然后发布操作云设备服务权限所需的验证请求。每个移动机器人选择一个云认证服务提供者连接并获得信任度及云设备的操作权限。同一工厂的移动机器人一方面共享信任度信息, 实现协同工作; 另一方面能够获得其他移动机器人连接的云认证服务提供者信任度的高低。

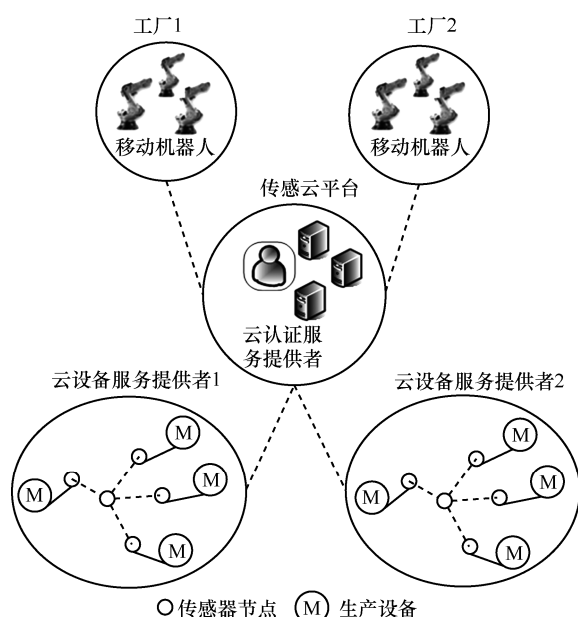


图1 工业无线传感云中面向移动机器人的信任度分配网络架构

移动机器人优先选择信任度高的云认证服务提供者连接, 这有利于移动机器人连接到合法的云认证服务提供者并获得更多的云设备服务操作权限。远程云设备的操作权限由云设备服务提供者决定。对于操作权限级别较高的远程云设备, 云认证服务提供者将提高移动机器人的认证级别。如果云认证服务提供者发布较高的认证级别, 那么合法的移动机器人为了获得较高认证级别的操作权限, 将发送多个密钥来获得较高的信任度。而非法移动机器人由于没有足够的权限密钥而选择那些低认证级别的

设备操作权限进行攻击。这样即使攻击者攻破了低认证级别的设备操作权限, 也不会对企业的安全生产造成大的影响。为了协调三方博弈参与者选择合适的策略, 增强系统的安全性, 本文提出的信任度分配框架分为3个步骤: 云设备服务提供者决定远程云设备操作权限的认证级别, 并发布给云认证服务提供者; 云认证服务提供者接收到订阅的远程云设备操作权限认证级别后, 根据认证等级, 把操作权限转换成所需的密钥对应的信任等级, 然后向准备连接到云认证服务提供者的移动机器人发布信任等级; 生产工厂中的每个移动机器人将根据云认证服务提供者发布的信任等级, 发送权限密钥进行验证, 并获得云认证服务提供者的信任度分配和远程云设备操作权限。

2.3 信任演化博弈参与者的效用函数

假设有 J 个工厂, n 个移动机器人, v 个云认证服务提供者, m 个云设备服务提供者。

2.3.1 移动机器人的效用函数

通过密钥验证的移动机器人连接到传感云平台向云设备服务提供者发送控制命令, 由传感器节点对所连接的设备执行相应的操作。移动机器人发送密钥并通过验证后将获得云认证服务提供者分配的信任度。移动机器人的收益 $f(d)$ 与对应的传感云平台的信任度有关, d 越大, 移动机器人的收益越大, 同时传感云平台的信任度也与服务质量的大小成正比, 服务质量一般使用对数函数来描述, 因此, 本文也使用对数作为效用函数来描述移动机器人的收益与信任度之间的关系。移动机器人的效用考虑了获得设备操作权限所需的密钥和认证服务提供者分配的信任度。移动机器人的收益表示如下:

$$f(d) = \lambda \ln(1 + \eta(d)) \quad (2)$$

其中, λ 表示云认证服务提供者的信任度参数, λ 越大, 云认证服务提供者的信任度越高。



$\eta(d)$ 表示移动机器人从云认证服务提供者获得信任度量函数。在生产工厂 j 的移动机器人为了最大化其安全效用, 选择 λ 较大的云认证服务提供者进行连接。因此生产工厂 j 的移动机器人的效用函数为:

$$u_{i,j}(d_i) = f_{i,j}(d_i) - c_{i,j}(d_i) \quad (3)$$

其中, $f_{i,j}(d_i)$ 表示工厂 j 的移动机器人发送权限密钥后获得云认证服务提供者 i 分配的信任收益。 $c_{i,j}(d_i)$ 表示获得云认证服务提供者分配的信任收益所需的权限密钥成本, 由式 (2) 可得:

$$f_{i,j}(d_i) = \lambda_{i,j} \text{lb} \left(1 + H_{i,j} \left(\frac{d_i}{n_i} \right) \right) \quad (4)$$

其中, $H_{i,j} \left(\frac{d_i}{n_i} \right)$ 表示工厂 j 的移动机器人获得云认证服务提供者的信任度量。云认证服务提供者 i 把从云设备服务提供者获得的认证等级中的远程云设备操作权限转换为信任等级中的信任度 d_i 。 n_i 表示工厂 j 需要认证的移动机器人的个数。由于在同一工厂中的机器人共享信任度, 选择云认证服务提供者 i 进行认证的移动机器人的信任度量表示为:

$$H_{i,j} = \alpha_{i,j} \text{lb} \left(\theta_{i,j} \frac{d_i}{n_i} \right) \quad (5)$$

其中, $\alpha_{i,j}$ 表示移动机器人发送给云认证服务提供者密钥的保密程度。 $\theta_{i,j}$ 表示远程云设备操作权限的保密程度。这两个参数值可以通过移动机器人和云认证服务提供者之间的保密容量来衡量。工厂 j 的移动机器人从云认证服务提供者获得信任度收益前, 需要发送的密钥数为:

$$c_{i,j}(d_i) = \sum_i k_i \quad (6)$$

其中, k_i 表示移动机器人发送的权限密钥策略数, $k_i = 1$ 表示发送权限密钥; $k_i = 0$ 表示不发送权限密钥。工厂 j 的移动机器人通过认证时, 获得效用定义如下:

$$u_{i,j}(d_i) = \lambda_{i,j} \text{lb} \left(1 + H_{i,j} \left(\frac{d_i}{n_i} \right) \right) - \sum_i k_i \quad (7)$$

因此, 工厂 j 的移动机器人连接到云认证服务提供者 i 的信任度优化问题, 可形式化为:

$$\begin{aligned} & \max_{d_i} u_{i,j}(d_i) \\ \text{s.t. } & d_i \geq 0, \text{lb} \left(\theta_{i,j} \frac{d_i}{n_i} \right) > 0 \end{aligned} \quad (8)$$

2.3.2 云认证服务提供者的效用函数

云认证服务提供者使用转换密钥来变换云设备服务提供者发送的认证等级为信任等级中的信任度。因此, 云认证服务提供者的效用是从移动机器人获得的密钥数减去转换为信任等级中的信任度所需的密钥数, 其效用函数为:

$$u_i(k_i, o_i) = r_i(k_i) - c_i(o_i) \quad (9)$$

其中, $r_i(k_i)$ 表示接收到移动机器人发送的密钥数, $c_i(o_i)$ 表示转换认证等级中的设备权限为信任等级中的信任度时所需转换密钥个数。工厂 j 的移动机器人选择 $k_i = 1$ 时, 发送给云认证服务提供者的密钥数为:

$$r_i(k_i) = n_i \sum_j k_j \quad (10)$$

云认证服务提供者转换认证等级中的设备权限为信任等级中的信任度时, 使用的转换密钥数为:

$$c_i(o_i) = \sum_j k_j \cdot (o_i + e_i) \quad (11)$$

其中, $\sum_j k_j$ 表示转换需要的密钥数, o_i 表示

远程云设备的基本操作权限数, e_i 表示基本操作的关联操作权限数。因此, 云认证服务提供者 i 的效用函数为:

$$u_i(k_i, o_i) = n_i \sum_i k_i - \sum_j k_j \cdot (o_i + e_i) \quad (12)$$

云认证服务提供者的目标是, 使用少的转换密钥获得较多的设备操作权限。即:

$$\begin{aligned} & \max_{k_i, o_i} u_i(k_i, o_i) \\ \text{s.t. } & k_i, o_i > 0 \end{aligned} \quad (13)$$

2.3.3 云设备服务提供者的安全效用

云设备服务提供者获得权限密钥后, 发放一定的设备操作权限。云设备服务提供者的效用函数为:

$$u_d(k) = r_d(k) - c_d \quad (14)$$

其中, $r_d(k)$ 表示云设备服务提供者获得的权限密钥数, c_d 表示发放的远程云设备操作权限数。

云设备服务提供者获得的权限密钥数为:

$$r_d(k) = \sum_{i=1}^v \left(\sum_j k_j \cdot (o_i + e_i) \right) \quad (15)$$

云设备服务提供者发放的远程云设备操作数为:

$$c_d = \sum_{i=1}^v (o_i + e_i) \quad (16)$$

因此, 云设备服务提供者的效用为:

$$u_d(k) = \sum_{i=1}^v \left(\sum_j k_j \cdot (o_i + e_i) \right) - \sum_{i=1}^v (o_i + e_i) \quad (17)$$

为了防护设备的安全性, 云设备服务提供者的目标是获得较多的权限密钥, 发放较少的操作权限, 即:

$$\begin{aligned} & \max_k u_d(k) \\ & \text{s.t. } k > 0, o_i > 0, e_i > 0 \end{aligned} \quad (18)$$

3 信任演化博弈分析及其自适应信任演化算法

3.1 移动机器人之间的信任演化阶段

在工厂 j 的移动机器人能相互通信并且共享信任度。因此, 同一工厂的机器人能观察到与其协作完成工作任务的其他移动机器人选择云认证服务提供者认证的策略选择, 然后相互比较云认证服务提供者的信任等级, 调节他们选择连接云认证服务提供者的策略。本文提出了基于演化博弈的移动机器人之间共享信任度演化机制, 使得移动机器人选择高信任等级的云认证服务提供者的认证服务。在演化博弈中, 移动机器人作为博弈参与者, 工厂 j 的所有移动

机器人作为一个种群, 使用动态复制方程分析演化博弈平衡。同一工厂中协作的移动机器人获得相同的信任度后, 共享远程云设备的操作权限。根据密钥的保密程度, 移动机器人不断变化其密钥发送策略, 因此, 在工厂 j 中, 选择连接到高信任等级的云认证服务提供者时发送密钥的比例数为:

$$x_{i,j} = \frac{n_{i,j} \sum_j k_j}{N_j} \quad (19)$$

其中, $n_{i,j}$ 为连接到信任等级高的云认证服务提供者的移动机器人的个数, $\sum_j k_j$ 表示每个移动机器人发送密钥的个数, N_j 表示工厂 j 的所有机器人持有的密钥个数。移动机器人为了实现信任度的共享, 在动态复制方程中, 信任度的演化率为:

$$\dot{x}_{i,j}(t) = x_{i,j}(t) (u_{i,j}(t) - \bar{u}_j(t)) \quad (20)$$

其中, $\bar{u}_j(t)$ 是整个工厂 j 移动机器人种群的平均效用, 它可以由式 (21) 计算, 即:

$$\bar{u}_j(t) = \sum_{i=1}^n x_{i,j} \cdot u_{i,j}(t) \quad (21)$$

在演化平衡点, 工厂 j 所有移动机器人选择相同的云认证服务提供者, 获得相同的信任度。通过解 $\dot{x}_{i,j}(t) = 0$ 能获得稳定点。在演化平衡状态, 移动机器人的信任度状态如下:

$$d_j^* = (d_{1,j}^*, d_{2,j}^*, \dots, d_{i,j}^*, \dots, d_{n,j}^*) \quad (22)$$

3.2 移动机器人和云认证服务提供者之间自适应信任度

根据演化博弈结果, 一方面, 云认证服务提供者根据获得的密钥, 选择信任度分配策略来最大化自己的效用; 另一方面, 由于在认证过程中, 无线信道容易受到恶意节点的窃听攻击, 并截获权限密钥和远程云设备的操作权限, 因此, 认证服务提供者将根据信道的保密容量自适应变化其信任度分配。此时, 云认证服务



提供者的效用为:

$$u_i(k_i, d_i) = n_i \sum_i k_i^* - \sum_{i=1}^n d_{i,j}^* (o_i + e_i) \quad (23)$$

当保密容量 $C_{\text{secrecy}}(i) = C_s(i) - C_e(i) > 0$ 时, 恶意的节点未截获权限密钥, 这里 $C_s(i)$ 表示信道容量, $C_e(i)$ 表示窃听容量。此时, 使用响应函数 $\varphi(k_i, d_i)$ 可以获得其最大安全效用时的策略, 即:

$$\varphi(k_i, d_i) = \arg \max_{k_i, d_i} u_i(k_i, d_i) \quad (24)$$

令 $k^* = (k_1^*, k_2^*, \dots, k_n^*)$ 且 $d^* = (d_1^*, d_2^*, \dots, d_n^*)$ 表示纳什均衡时, 接收到移动机器人优化的密钥策略和分配给移动机器人优化的信任度策略。当 $C_{\text{secrecy}}(i) < 0$ 时, 移动机器人发送的密钥被恶意节点截获。此时, 为了保持网络的安全效用, 云认证服务提供者变化信任度的分配, 并且升级信任度所对应的密钥, 即:

$$\begin{aligned} k(t+1) &= k^*(t) \oplus \text{random}(i) \\ d(t+1) &= d^*(t) - \sigma \cdot (C_s(i) - C_e(i)) \end{aligned} \quad (25)$$

其中, σ 表示信任度损失因子。当移动机器人得到降低的信任度值后, 将不能驱动其执行远程云设备操作, 以免泄露更多的操作内容。同时, 由于云认证服务提供者已升级信任度对应的密钥, 攻击者即使获得部分密钥, 也不能通过下一步的认证。云认证服务提供者把更新后的密钥发送给云设备服务提供者, 对新的密钥进行操作权限升级。

3.3 移动机器人自适应信任演化过程

根据以上分析, 在演化博弈中, 移动机器人选择信任等级高的云认证服务提供者发送密钥来最大化自己的信任度并获得远程云设备的操作授权。如果在工厂 j 的一个移动机器人的效用低于整个种群的平均效用, 表明这个移动机器人是不安全或不可信的, 必须发送权限密钥以提高其效用, 当达到平均效用后, 与其他的移动机器人共

享信任度, 并协作使用远程云设备的操作权限。由于移动机器人和云认证服务提供者之间的无线信道容易受到恶意节点的攻击, 截获密钥, 云认证服务提供者必须更新密钥, 根据保密容量的变化自适应信任度分配。移动机器人自适应信任演化过程如算法 1 所示。

算法 1 移动机器人自适应信任演化过程
初始化所有机器人的信任度。

for 每个时间隙 t_1

云认证服务提供者转换认证等级为信任度。

repeat

for 每个时间隙 t_2

每个移动机器人选择信任等级高的云认证服务提供者连接, 并选择发送密钥策略。

repeat

使用式 (7) 计算移动机器人的效用。

工厂的所有移动机器人交换云认证服务提供者的信任等级。

使用式 (21) 计算整个工厂 j 移动机器人种群的平均效用。

if $u_{i,j} < \bar{u}_j(t)$

不共享信任度。

else

共享信任度。

end if

until 所有机器人达到平均效用。

end for

if $C_{\text{secrecy}}(i) < 0$

使用式 (25) 更新密钥和信任度。

until 直到分配给移动机器人的信任度增大为 $d^*(t)$ 。

end for

算法收敛时间与密钥个数 k 、移动机器人个数 n 及操作权限数 o 有关, 因此算法空间复杂度为 $O(k \cdot n + o)$ 。时间复杂度为 $O(t_1 \cdot n \cdot t_2 \cdot v)$, v 表示云认证服务提供者个数。

4 实验仿真与分析

本文使用 MATLAB 工具对博弈效用和自适应信任度进行仿真, 主要评估了移动机器人的信任演化行为、不同的密钥数和不同的信任等级对移动机器人效用的影响、云认证服务提供者自适应信任度分配过程。首先仿真了移动机器人的信任演化行为。

在实验中设定工厂 1 移动机器人发送的密钥数 $K_1=3$, 工厂 2 移动机器人发送的密钥数 $K_2=5$, 云认证服务提供者 1 的信任等级为 $D_1=100$, 云认证服务提供者 2 的信任等级为 $D_2=150$, 移动机器人信任行为的演化过程如图 2 所示。从图 2 中可看出, 在工厂 1 和工厂 2 中的移动机器人经过 5 步迭代后, 其效用收敛于优化值 0.85。从图 2 中还可以看出, 在演化稳定状态所有的移动机器人的信任度是相同的。由此可见, 通过信任的演化使得所有的移动机器人变为可信的合法节点, 共享远程云设备的操作权限。这可以有效地防止恶意节点与合法节点协作访问远程云设备。

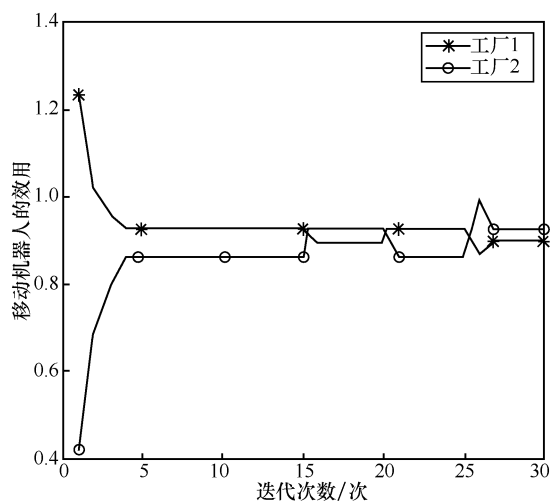


图2 移动机器人信任行为的演化过程

图 3 给出了云认证服务提供者 2 的信任等级为 $D_2=150$ 且受到窃听攻击时, 移动机器人发送不同的密钥数为 $K_1=3$ 、 $K_2=5$ 、 $K_3=4$ 和 $K_4=1$

时, 对其效用的影响。从图 3 中可看出, 移动机器人发送的密钥越少, 其效用越高。例如, 当 $K_2=5$ 时, 移动机器人的效用趋向于 0。当 $K_4=1$ 时, 移动机器人的效用最终稳定在 4 左右。由此可见, 在云认证服务提供者信任等级较高的情况下, 为更有效地提高其持有密钥的安全性, 移动机器人应变化其连接云认证服务提供者策略, 选择信任等级高且保密容量大的云认证服务提供者接入。

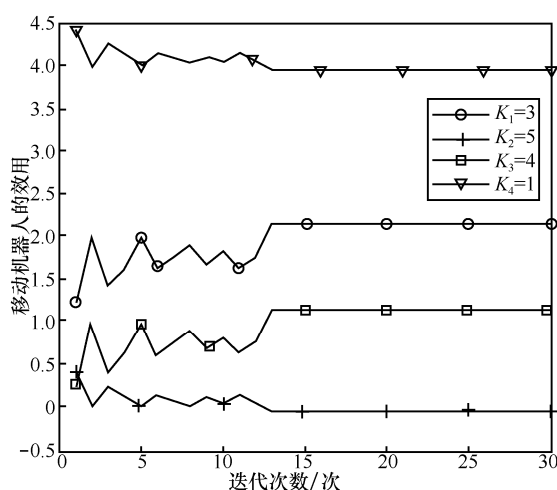


图3 不同密钥数对移动机器人效用的影响

图 4 给出了不同的云认证服务提供者的信任等级和移动机器人发送密钥数对移动机器人效用的影响。面对窃听攻击时, 根据式 (25) 进行密钥和信任度更新, 使得密钥数和信任度发生变化, 从图 4 中可看出, 当发送密钥数适中, 且云认证服务提供者的信任等级适中时, 移动机器人获得的效用最大。当发送密钥数较多, 且云认证服务提供者的信任等级较大时, 移动机器人获得的效用最小。例如, 当 $K_1=3$ 、 $D_1=110$ 时, 移动机器人获得最大效用为 1.7; 当 $K_1=5$ 、 $D_1=170$ 时, 移动机器人获得最大效用为 0.25。由此可见, 面对窃听攻击时, 在云认证服务提供者的信任等级和移动机器人发送密钥数都变化的情况下, 为更有效地提升移动机器人的效用, 移动机器人应选择发送密钥数和信任等级适中的云认证服务提供



者接入, 增强其自身的安全性。

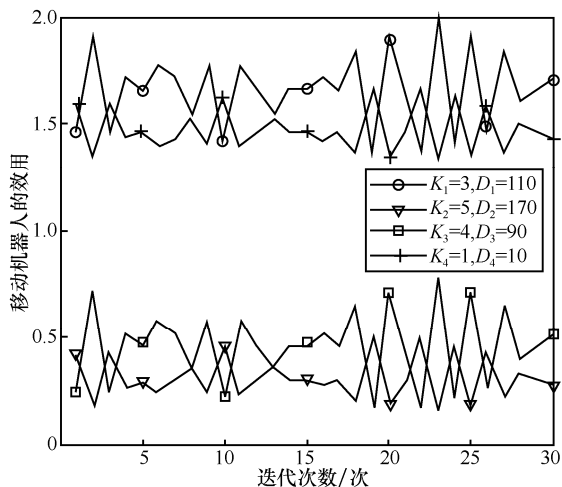


图4 不同信任等级和密钥数对移动机器人效用的影响

图5给出了当 $D_1 = D_2 = D_3 = D_4 = 110$ 时, 面对窃听攻击时, 云认证服务提供者自适应信任度分配过程。可以看出, 当密钥个数 ≤ 4 时, 信任度收敛于较高水平。例如, 当 $K_1 = 3$ 、 $K_3 = 4$ 时, 云认证服务提供者自适应信任度分配达到较好水平。这主要由于此时密钥数适中, 分配的信任度也处于中等水平。

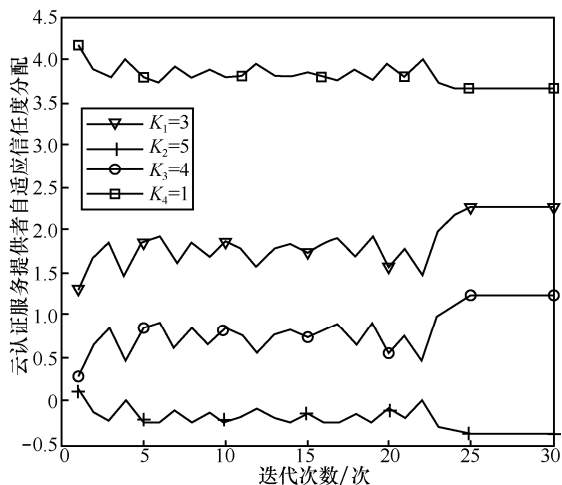


图5 云认证服务提供者自适应信任度分配过程

当 $K_4 = 1$ 时, 虽然信任度达到较高水平, 但由于云认证服务提供者发送的密钥数较少时, 只能获得认证等级低的云设备操作权限。当 $K_2 = 5$ 时, 虽然密钥较多, 但是被攻击者截获的密钥较多, 因此信任度较低。通过算法1, 自适应调节信

任度, 使得密钥泄露概率减少。

图6给出了自适应信任演化算法与其他认证方法的比较。从图6可以看出, 在无线传感云智能制造环境下的信任管理和认证机制中, 自适应信任演化算法表现出较高的效用。这主要是由于基于信任模型的认证机制通过信任度来识别可信的节点, 在授权远程设备操作时不进行操作权限验证, 使得移动机器人的效用下降。基于单密钥的认证机制使用密钥过滤非法节点, 但受到窃听攻击时, 密钥容易泄露, 降低移动机器人的效用。本文提出的自适应信任演化算法能根据移动机器人之间的信任演化分析、移动机器人和云认证服务提供者之间自适应信任度分析选择密钥发送策略, 当检测到保密容量降低时, 说明无线信道受到窃听攻击, 通过自适应更新信任度所对应的密钥及分配新的信任度, 提高了移动机器人远程操作云设备的效用及安全性。

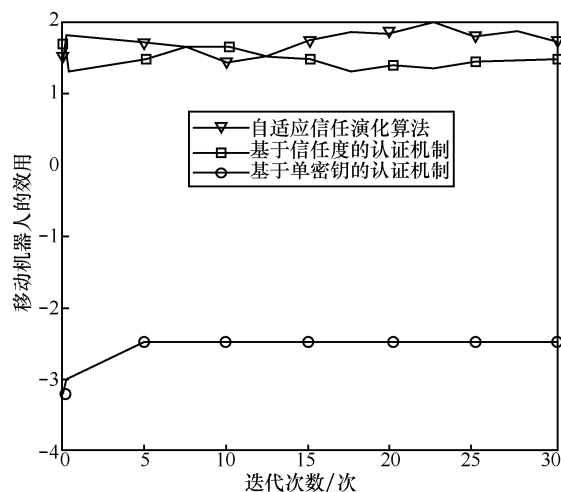


图6 自适应信任演化算法与其他认证方法的比较

无线信道受到攻击时, 不同的安全机制对云设备安全等级的影响如图7所示。在单密钥认证方法中, 开始时, 受窃听攻击云设备的安全等级较高, 为4.25, 随着单个密钥的泄露, 受窃听攻击云设备的安全等级有所降低, 最终保持在3.5, 这主要是由于移动机器人发送的是单个密钥, 只能获得认证等级要求低的云设备服务, 也只访问

云设备而不对设备进行操作, 密钥泄露对云设备安全性影响不大。在基于信任度的认证机制中, 开始时, 由于信任度的增加, 受窃听攻击云设备的安全等级也随之升高, 最高达到 0.87, 随后由于信任机制不对设备操作权限进行认证, 于是受窃听攻击云设备的安全等级降低至 0.6, 这比单密钥认证机制中受窃听攻击云设备的安全等级低。在自适应的信任演化算法中, 为了获得认证等级要求高的云设备服务, 在开始时, 由于进行多个密钥的发送和认证, 受窃听攻击云设备的安全等级升高至 1.75, 接着多个密钥泄露造成受窃听攻击云设备的安全等级降低至 1.5, 通过更新信任度所对应的密钥以及对新的密钥进行操作权限升级, 使得受窃听攻击云设备的安全等级升高至 2.8。由此可见, 自适应的信任演化方法与基于信任度的认证方法相比能显著提高受窃听攻击云设备的安全等级。与单密钥的认证方法相比, 不仅可以获得认证等级要求高的云设备服务, 而且在无线信道受到攻击时, 还能自适应提高云设备的安全等级。

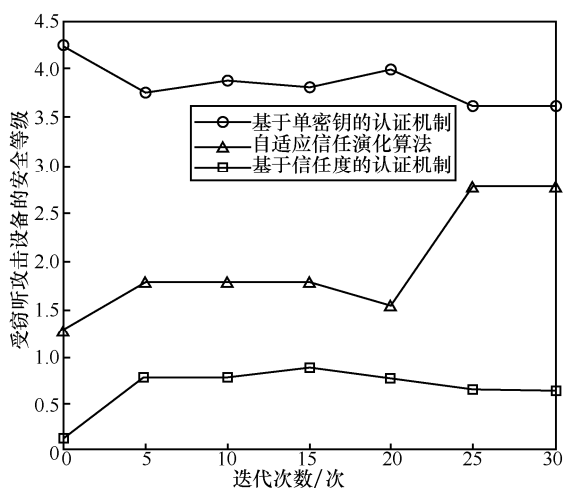


图7 不同的安全机制对云设备安全等级的影响

5 结束语

在本文中, 面向工业无线传感云中的移动机器人访问远程云设备提出了基于演化博弈的自适应信任演化机制。在提出的机制中, 移动机器人

通过发送密钥获得执行远程云设备的操作权限, 云认证服务提供者分配信任度给移动机器人, 在同一工厂中的移动机器人通过演化博弈共享分配的信任度, 从而过滤不可信和非法的节点访问远程云设备。移动机器人为了获得最大化效用, 选择发送密钥适中且信任等级高的云认证服务提供者接入, 这有利于移动机器人获得所需的设备操作权限。通过模型化自适应信任度分配系统框架为一个演化博弈, 分析了移动机器人之间的信任演化阶段、移动机器人和云认证服务提供者之间自适应信任度分配阶段。在博弈达到纳什均衡时, 存在使博弈参与者最大化其安全效用的最优策略, 面对窃听攻击时, 博弈参与者平衡效用被打破, 本文通过更新密钥和信任度的自适应机制使得博弈参与者的效用再次达到平衡。数值仿真显示, 在面对窃听攻击时, 使用本文提出的自适应信任演化机制能提高网络及远程云设备的安全性。

参考文献:

- [1] 李伯虎, 张霖, 任磊, 等. 云制造典型特征、关键技术与应用[J]. 计算机集成制造系统, 2012, 18(7): 1345-1356.
LI B H, ZHANG L, REN L, et al. Typical characteristics, technologies and applications of cloud manufacturing[J]. Computer Integrated Manufacturing Systems, 2012, 18(7): 1345-1356.
- [2] 江家仁. 虚拟化安全—公有云安全的核心关键问题探讨[J]. 电信科学, 2015, 31(12): 121-124.
JIANG J R. Virtualization security, discussion on key issues of public cloud computing security[J]. Telecommunications Science, 2015, 31(12): 121-124.
- [3] 李顺东, 窦家维, 王道顺. 同态加密算法及其在云安全中的应用[J]. 计算机研究与发展, 2015, 52(6): 1378-1388.
LI S D, DOU J W, WANG D S. Survey on homomorphic encryption and its applications to cloud security[J]. Journal of Computer Research and Development, 2015, 52(6): 1378-1388.
- [4] 郭强, 孙大为, 常桂然, 等. 一种基于虚拟化技术增强云安全的可信模型[J]. 东北大学学报(自然科学版), 2011, 32(6): 786-790.
GUO Q, SUN D W, CHANG G R, et al. A virtualization techniques based dependability model to enhance security of cloud computing environments[J]. Journal of Northeastern University(Natural Science), 2011, 32(6): 786-790.
- [5] 蔡红云, 田俊峰, 李珍, 等. 基于信任领域和评价可信度量的信任模型研究[J]. 计算机研究与发展, 2011, 48(11): 2131-2138.



- CAI H Y, TIAN J F, LI Z, et al. Trust model based on trust area and evaluation credibility[J]. Journal of Computer Research and Development, 2011, 48(11): 2131-2138.
- [6] YU Y, LI K, ZHOU W, et al. Trust mechanisms in wireless sensor networks: attack analysis and countermeasures [J]. Journal of Network & Computer Applications, 2012, 35(3): 867-880.
- [7] LOUATI A, HADDAD J E, PINSONP S. Trust-based coalition formation for dynamic service composition in social networks[M]//Web Information Systems Engineering WISE 2015. Heidelberg: Springer, 2015: 570-585.
- [8] 陈亚睿, 田立勤, 杨扬. 云计算环境下基于动态博弈论的用户行为模型与分析[J]. 电子学报, 2011, 39(8): 1818-1823.
CHEN Y R, TIAN L Q, YANG Y. Model and analysis of user behavior based on dynamic game theory in cloud computing[J]. Chinese Journal of Electronics, 2011, 39(8): 1818-1823.
- [9] 肖云鹏, 姚豪豪, 刘宴兵. 一种基于云模型的 WSN 节点信誉安全方案[J]. 电子学报, 2016, 44(1): 168-175.
XIAO Y P, YAO H H, LIU Y B. A WSN node reputation security scheme based on cloud model[J]. Chinese Journal of Electronics, 2016, 44(1): 168-175.
- [10] ZONOUZ S, HOUMANSADR A, BERTHIER R, et al. Secloud: a cloud-based comprehensive and lightweight security solution for smart phones[J]. Computers & Security, 2013, 37(9): 215-227.
- [11] NITTI M, GIRAU R, ATZORI L. Trustworthiness management in the social internet of things[J]. IEEE Transactions on Knowledge & Data Engineering, 2014, 26(5): 1253-1266.
- [12] 汤雅妃, 张云勇, 张尼. 基于指纹识别的云安全认证技术[J]. 电信科学, 2015, 31(8): 166-172.
TANG Y F, ZHANG Y Y, ZHANG N. Cloud security certification technology based on fingerprint recognition[J]. Telecommunications Science, 2015, 31(8): 166-172.
- [13] 沈士根, 刘建华, 曹奇英. 博弈论与无线传感器网络安全[M]. 北京: 清华大学出版社, 2016: 114-132.
SHEN S G, LIU J H, CAO Q Y. Game theory meets wireless sensor networks security[M]. Beijing: Tsinghua University Press, 2016: 114-132.
- [14] YANG X, HUANG X, LIU J K. Efficient handover authentication with user anonymity and untraceability for mobile cloud computing[J]. Future Generation Computer Systems, 2015, 62(C): 190-195.
- [15] ZOU Y, WANG G. Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack[J]. IEEE Transactions on Industrial Informatics, 2016, 12(2): 780-787.

[作者简介]



刘建华 (1978-), 男, 博士, 嘉兴学院数理与信息工程学院讲师, 主要研究方向为无线传感器网络、云计算、网络与信息安全、博弈论。



李明禄 (1965-), 男, 博士, 上海交通大学计算机科学与工程系教授, 主要研究方向为无线传感器网络、云计算与大数据、物联网。



李大志 (1977-), 男, 上海交通大学计算机科学与工程系博士生, 上海师范大学信息与机电工程学院讲师, 主要研究方向为云计算与大数据、物联网。



李鲁群 (1967-), 男, 博士, 上海师范大学信息与机电工程学院教授, 主要研究方向为无线传感器网络、群体智能算法。