

引用格式:石乐义,刘娜,崔雯迪,等.基于联盟链的可信工业控制网络访问控制机制[J].微电子学与计算机,2020,37(11):24-28. [SHI L Y, LIU N, CUI W D, et al. Trusted access mechanism of industrial control network based on alliance chain [J]. Microelectronics & Computer, 2020, 37(11): 24-28.]

基于联盟链的可信工业控制网络访问控制机制

石乐义¹, 刘娜², 崔雯迪², 李晓雨¹, 朱红强¹

(1 中国石油大学(华东) 计算机科学与技术学院, 山东 青岛 266580;

2 中国石油大学(华东) 海洋与空间信息学院, 山东 青岛 266580)

摘 要: 针对工业控制网络高度中心化、数据安全和访问控制等问题, 优化基于属性的访问控制模型, 引入多维信任度量技术作为访问控制判决因素来解决网络内部节点攻击问题, 采用联盟链技术优化工业控制网络模式, 解决控制系统中心化的问题. 进一步提出了基于联盟链的可信工业控制网络访问控制模型 TurstAC-ABAC. 采用 LabVIEW 仿真软件和 HyperLedger Fabric 平台分别实现对工业控制系统和联盟链系统的仿真环境, 验证了本文所提出框架的可行性和安全性.

关键词: 工业控制网络; 联盟链; 多维信任度量; 访问控制

中图分类号: TP311

文献标识码: A

文章编号: 1000—7180(2020)11—0024—05

Trusted access mechanism of industrial control network based on alliance chain

SHI Le-yi¹, LIU Na², CUI Wen-di², LI Xiao-yu¹, ZHU Hong-qiang¹

(1 College of Computer Science and Technology, China University of Petroleum(EastChina),

Qingdao 266580, China; 2 College of Oceanography and Space Informatics,

China University of Petroleum (East China), Qingdao 266580, Chian)

Abstract: Aiming at the problem that is highly centralized, data security and access control of industrial control network, this paper puts forward some solutions, which improve the model of Attribute based access control (ABAC), introduce multi-dimensional trust measurement as access control decision factors to solve the problem of node attack, use the alliance chain technology to optimize industrial control network model and solve the problem of control system centralization. A TurstAC-ABAC model is proposed, which is a highly trusted access control mechanism model of industrial control network based on the alliance chain. The industrial control system and alliance chain system is simulated using LabVIEW and the HyperLedger Fabric platform. The simulation results verify the feasibility and security of the proposed framework.

Key words: industrial control network; alliance chain; multi-dimensional trust measurement; access control

1 引言

随着两化的深度融合,传统的工业控制网络模式面临着很大的安全问题,系统一旦被攻击,不仅会

导致信息泄露、系统不能正常使用等问题,还会对现实的世界造成影响. 访问控制技术可以保障系统资源 and 数据只被合法授权的用户进行访问控制和操作^[1]. 因此,访问控制是工控网安全研究的重要内容

之一。

现有访问控制方法有基于角色的访问控制(RBAC)、基于属性的访问控制(ABAC)和基于权限的访问控制(CapBAC)等。在大规模的环境下,ABAC模型表现出更好的优势,能够做到对节点细粒度的授权管理。传统的ABAC模型虽然解决了节点的访问权限问题,但是不能有效防御网络内部节点的攻击。

区块链是一种将分布式账本、加密算法、智能合约等技术融合在一起,从而实现防篡改、去中心、可追溯的新型系统架构^[2]。区块链根据去中心化的程度,可分为公有链、私有链和联盟链三种。其中,联盟链是一种可以对成员身份和权限进行限制的区块链,是部分去中心化的链,其数据仅可被联盟内已授权的节点进行访问操作。国内外学者在工控网安全上主要围绕加密计算^[3-4]、身份认证^[5-7]和访问控制^[8-12]三个方向进行研究。

本文创新地提出 TrustAC-ABAC 模型,将有效地保证分布式协作下的工业控制网络访问控制策略、数据管理操作及系统使用的合法性。

2 TrustAC-ABAC 模型

TrustAC-ABAC 模型是对 ABAC 的改进,引入信任值作为访问权限分配的属性,并将此策略同系统重要参数一同存于联盟链当中,依据合约的自动执行实现模型的自治,实现对工业控制网络节点行为的监控,保障系统最重要数据的不可篡改,提升了访问控制的安全性。

2.1 模型框架

系统模型框架包括工业控制网络及联盟链网络两部分,主要涉及工业控制网络与联盟链网络的数据交互模块、智能合约模块和数据存储模块,如图 1 所示。

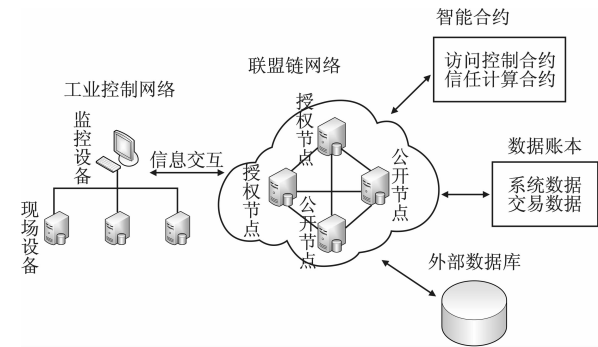


图 1 TrustAC-ABAC 模型图

在 TrustAC-ABAC 模型中,工业控制网络节点首先将现场控制设备数据发送给联盟链网络,联盟链网络根据收集到的数据运行智能合约中的多维信任度量和访问控制策略,并将判决结果反馈给工业控制网络,实现对工业控制网络节点的实时监控和访问授权。由于此模型策略均存于联盟链网络当中,并且采用联盟链来实现对节点的分级分层控制,攻击者难以针对工业控制网络发起攻击,因此模型具有良好的隐私性与抗攻击性。

2.2 关键策略

TrustAC-ABAC 模型采用访问控制策略和多维信任度量策略,前者为工业控制系统中节点的分层分级控制问题而提出,后者为解决模型网络内节点在系统执行过程中的实时可靠性问题而提出。

2.2.1 多维信任度量策略

信任度量即评估节点 i 对被评估节点 j 的信任度进行量化的过程。为保证度量结果的真实有效,本文采用多维度的可信度量因素,来全面的度量工控网节点的可信状态,即多维信任度量。

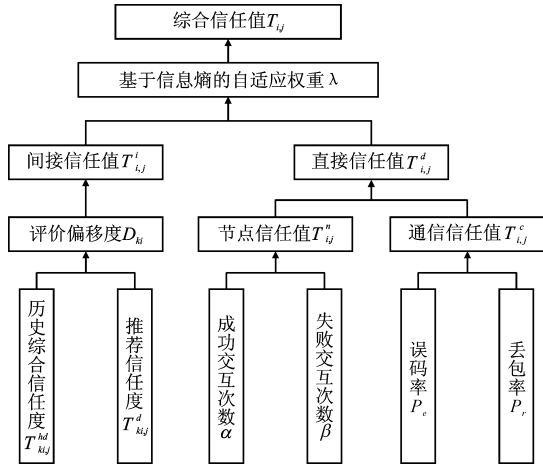


图 2 信任模型框架

如图 2 所示,节点的综合信任 $T_{i,j}$ 由直接信任 $T_{i,j}^d$ 和间接信任 $T_{i,j}^i$ 因素构成,并使用信息熵自动调节权重 λ 。其中, $T_{i,j}^d$ 由通信信任 $T_{i,j}^c$ 和节点信任 $T_{i,j}^n$ 因素构成, $T_{i,j}^i$ 由相邻节点 k 的推荐意见 $T_{ki,j}^{rd}$ 和历史信任值 $T_{ki,j}^{hd}$ 构成,并根据评价偏移度 D_{ki} 设置权重。

多维信任度量包括信任因素获取模块、信任度量模块和信任评估模块。

(1) 信任获取模块

根据信任度量过程中所涉及到的度量因素进行收集,包括通信信任、节点信任、历史综合信任等因素。

(2) 信任度量模块

信任度量模块根据定义的各个信任因素,分别在计算周期内计算出当前直接信任值和间接信任值,然后计算出综合信任值,可描述为:

$$T_{i,j} = \lambda_1 T_{i,j}^d + \lambda_2 T_{i,j}^i \quad (1)$$

根据直接信任和间接信任的信息熵确定合成权重,计算可得:

$$\lambda_1 = (1 + T_{i,j}^d \ln T_{i,j}^d) / [(1 + T_{i,j}^d \ln T_{i,j}^d) + (1 + T_{i,j}^i \ln T_{i,j}^i)] \quad (2)$$

$$\lambda_2 = (1 + T_{i,j}^i \ln T_{i,j}^i) / [(1 + T_{i,j}^d \ln T_{i,j}^d) + (1 + T_{i,j}^i \ln T_{i,j}^i)] \quad (3)$$

若节点 i 与 j 的交互次数中,成功和失败交互次数分别为 α 和 β ,且发包数为 m ,收包数为 p ,码元数为 a ,正确的码元数为 b ,则节点 i 关于 j 的信任度服从 Beta 分布,即有 $T_{i,j}^d = \text{Beta}(\alpha_{ij} + 1, \beta_{ij} + 1)$,则节点信任值 $T_{i,j}^d$ 和通信信任值 $T_{i,j}^c$ 可分别为:

$$T_{i,j}^d = (\alpha + 1) / (\alpha + \beta + 2) \quad (4)$$

$$T_{i,j}^c = 1/2 * \log_2(1 + p/m) + 1/2 * \log_2(1 + b/a) \quad (5)$$

则直接信任值 $T_{i,j}^d$ 为:

$$T_{i,j}^d = 1/2 T_{i,j}^c + 1/2 T_{i,j}^n \quad (6)$$

考虑到节点间可能存在恶意推荐的问题,节点 i 需要对相邻节点 k 的推荐可靠性进行判别,这里采用直接信任值 $T_{i,ki}^d$ 作为判别指标,若其 $T_{i,ki}^d$ 小于相对应的阈值则认为其推荐信任度不可靠,不予采纳。 k_i 对 j 的推荐权重由其自身信任值占有所有推荐信任值的比重确定。

假设 k_i 对 j 直接信任度的期望和邻居节点 k_i 的评价差异度可分别表示为 $\overline{E_k^d}$ 和 D_{ki} ,则 D_{ki} 为:

$$D_{ki} = (T_{ki,j}^d - \overline{E_k^d}) / \sum_{i=1}^k (T_{ki,j}^d - \overline{E_k^d}) \quad (7)$$

则间接信任值为:

$$T_{ki,j}^i = \sum_{i=1}^n (1 - D_{ki}) * T_{ki,j}^c \quad (8)$$

(3) 信任评估模块

根据多维信任度量计算得到的综合信任值与其相对应的信任阈值 $T_{\min}$ 进行对比,得到节点的可信状态。

2.2.2 访问控制策略

为解决工控网内部节点的可靠性问题,引入信任度量策略实时的监控节点的行为,保证访问节点的诚实度。本文在访问控制策略中加入信任值作为访问控制策略的判决因子,并使用联盟链实现访问控制的分层分级控制,可描述为:

$$\text{TrustAC-ABAC} = \{S, O, P, E, T\}$$

式中, S 表示发起访问控制请求的节点所具有的属性信息,如节点 ID 信息、节点证书、随机数等信息; O 表示请求访问节点及被访问资源具有的属性信息; P 表对被访问资源所要执行的查询和增加等操作行为; E 表示请求时间、系统网络位置等访问控制过程中所归属的环境属性。 T 表示多维信任属性集合,即节点直接信任值、间接信任值、对其他节点的推荐信任值等信息。

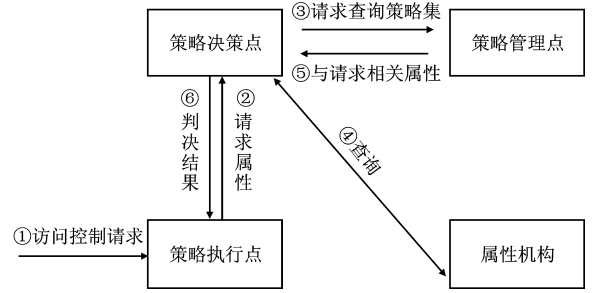


图3 访问控制模型框架

如图3所示,访问控制模型框架包括四个组成要素,其中,策略执行点、策略决策点、策略管理点用智能合约来实现,策略执行点负责联盟链系统与工业控制系统进行交互。

当节点想要对网络中其他节点进行操作时,需发送访问控制请求,策略执行节点收到请求时会根据属性信息生成基于属性的访问请求并发送给策略决策点;策略决策点向策略管理点请求访问控制策略集查询,并将结果反馈给策略节点进行判决。

3 安全性分析

3.1 方案结构特点

(1) 分层分级控制。访问控制策略对工控网节点身份权限进行了有效的限制,并且本文 TrustAC-ABAC 机制采用联盟链来进行部署,根据不同节点的实际现场需求,制定不同的节点权限。

(2) 实时信任度量。访问控制策略引入信任度量算法,对节点的行为进行监控,实时度量访问节点的可靠性,保障工业控制网络的安全性。

(3) 协同自治。本方案所提策略和系统重要参数均存于联盟链中,利用区块链防篡改保障数据安全,并依据智能合约自动执行实现模型的自治。

3.2 安全性分析

(1) DDos 攻击。由于工控网当中存在很多资源受限的节点,很容易受到 DDOS 攻击来消耗节点资源。本方案采用联盟链进行节点权限分配,只有在节

点间建立共享密钥才能进行通信,且采用信任度量算法来进行节点行为监控,防止内部节点攻击。

(2)追加攻击. 此类攻击是攻击者通过伪造交易和创造虚假共识生成区块,本方案中工业控制网络节点可以根据联盟链网络中账本的所有者等信息检测出虚假区块。

(3)设备注入攻击. 攻击者将虚假节点注入到工业控制网络中,以获取访问隐私信息的能力. 由于本地通信需要对节点身份权限进行核实,所以节点注入的设备会被隔离。

(4)修改攻击. 由于工业控制网络中包含的数据均存于联盟链当中,联盟链中存储的数据所包含特定的哈希值可以记录数据存储的时间及其他信息,可以以此检验数据是否被修改过。

4 实验测试与分析

本节通过仿真实验对 TrustAC-ABAC 模型进行测试,主要对时延和系统稳定性进行了实验,实验

设计分为联盟链模块和水位控制模块,以验证其有效性和可行性。

联盟链系统模块负责运行高可信的访问控制策略,存储控制系统重要参数. 仿真系统采用 Fabric 平台进行设计和实现,系统在 Intel Core i7-6700U 3.40 GHz,16 G 内存,Ubuntu16.04 操作系统下运行. 联盟链系统使用 Docker 虚拟化部署,采用 4 个节点共同维护一个超级账本,每两个节点归属于一个组织并选取一个为 CA 节点. 水位控制仿真模块主要负责模拟水位控制系统的执行过程,采用 LabVIEW 仿真平台设计实现,系统在 Intel Core i7-8550U 1.80 GHz,Windows10 操作系统下运行. 水位控制系统主要实现对下位机的控制,包括水位水压采集命令、水阀控制命令等,并水位控制系统的水位设定值和其他重要参数使用 Go 语言编写存于区块链中,使用命名为“Fabric”控件与联盟链网络进行信息交互,后面板设计如图 4 所示。

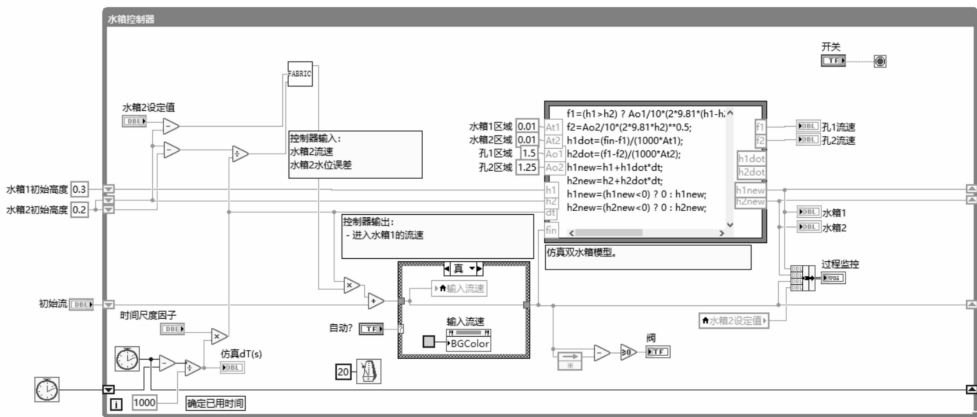


图 4 基于 Labview 的水位控制系统程序后面板

仿真实验时,工控系统模块模拟水位变化过程,并持续向联盟链发送访问控制请求,联盟链模块执行改进后智能合约,将策略执行结果返回水箱控制系统中对其节点进行实时监控及访问控制操作。

4.1 时延

时间延迟分为高可信访问控制合约时延和请求控制参数时延,高可信访问控制合约时延为仿真系统执行智能合约中的多维信任度量和访问控制策略所用时间,请求控制参数时延为工业控制网络从联盟链中获取水位设定值等重要参数所需时间。

由图 5、图 6 可知,随着节点访问控制次数的增

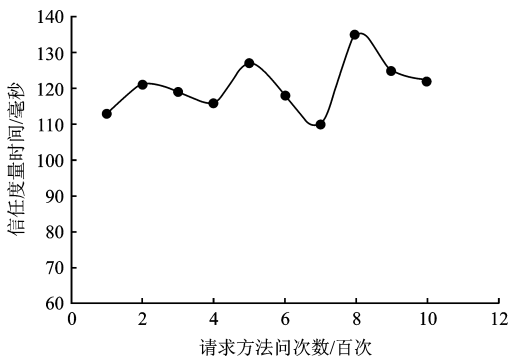


图 5 高可信访问控制合约时延

加,高可信访问控制合约执行的平均时延稳定在 120 ms,请求控制参数平均时延稳定在 35 ms,两者

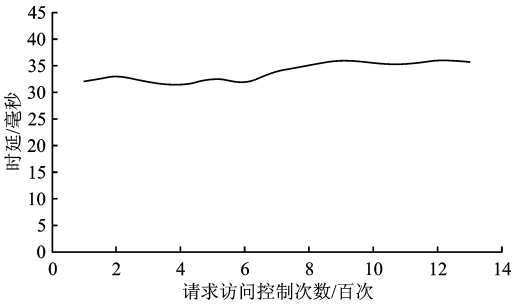


图 6 请求控制参数时延

都为毫秒级的时延,可以保障在可接受的时间延迟内,对工业控制网络行为进行度量并实现有效监控,可以被大多数的工业控制网络场景接受.

4.2 系统稳定性

系统稳定性是指水位控制系统在外界影响下表现出的稳定状态. 本实验设定水箱初始水位为 0.2 L,初始进水流速为 0.3 L/s,同时以 0.3 L/s 的出水速度进行排水,水箱水位目标设定值为 0.3 L.

水位控制系统通过从联盟链中获取预先存储的水位设定值进行水位控制,由图 7 可以看出,水箱水位、水流变化过程平稳,能够按照既定的目标运行,在从而证明了本文所提出框架的系统稳定性.

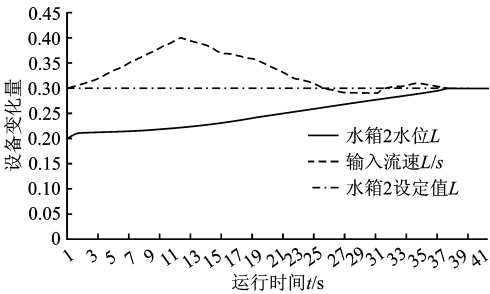


图 7 水箱控制系统过程监控图

5 结束语

针对 TrustAC-ABAC 模型,分别从时间和系统稳定性的两个方面进行了实验测试,实验结果表明了本文所提模型的安全性与可行性,为进一步研究工业控制网络安全问题提供了新的思路. 然而,在具体的工业控制网络应用时,其性能还需提高,下一步,将重点研究区块链网络的高并发和索引性能等问题,进一步提高框架的实用性.

参考文献:

[1] 房梁,殷丽华,郭云川,等. 基于属性的访问控制关键技术综述[J]. 计算机学报, 2017, 40(7):

1680-1698. DOI: 10. 11897/SP. J. 1016. 2017. 01680.
FANG L, YIN L H, GUO Y C, et al. A survey of key technologies in attribute-based access control scheme[J]. Chinese Journal of Computers, 2017, 40 (7): 1680-1698. DOI: 10. 11897/SP. J. 1016. 2017. 01680.
[2] 袁勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494. DOI: 10. 16383/j. aas. 2016. c160158.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42 (4): 481-494. DOI: 10. 16383/j. aas. 2016. c160158.
[3] AITZHAN N Z, SVETINOVIC D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams [J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 840-852. DOI: 10. 1109/ TDSC. 2016. 2616861.
[4] 谢辉,王健. 区块链技术及其应用研究[J]. 信息安全, 2016(9): 192-195. DOI: 10. 3969/j. issn. 1671-1122. 2016. 09. 038.
XIE H, WANG J. Study on block chain technology and its applications[J]. Netinfo Security, 2016(9): 192-195. DOI: 10. 3969/j. issn. 1671-1122. 2016. 09. 038.
[5] AXON L, GOLDSMITH M. PB-PKI: a privacy-aware blockchain-based PKI[C]//International Conference on Security & Cryptography. Madrid: University of Oxford, 2017: 311-318. DOI: 10. 5220/0006419203110318.
[6] KUOTT, OHNO-MACHADOL. ModelChain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks [EB/OL]. arxiv: PaulKingsbar. (2018-02-06). [2020-01-16]. https://arxiv.org/ftp/arxiv/papers/1802/1802.01746.pdf.
[7] ZHANG F, CECCHETTI E, CROMAN K, et al. Town crier: an authenticated data feed for smart contracts[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna: ACM, 2016: 270-282. DOI: 10. 1145/ 2976749. 2978326.
[8] MAESA DDF, MORI P, RICCI L. Blockchain based access control[C]//17th IFIP International Conference on Distributed Applications and Interoperable Systems. Neuch? tel: Springer, 2017: 206-220. DOI: 10. 1007/978-3-319-59665-5_15.

- tus; how often should one update? [C]//2012 Proceedings IEEE INFOCOM. Orlando: IEEE, 2012. DOI: 10.1109/INFOCOM.2012.6195689.
- [2] KAUL S, GRUTESER M, RAI V, et al. Minimizing age of information in vehicular networks[C]//2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. Salt Lake City, IEEE, 2011. DOI: 10.1109/SAHCN.2011.5984917.
- [3] COSTA M, CODREANU M, EPHREMIDES A. On the age of information in status update systems with packet management[J]. IEEE Transactions on Information Theory, 2016, 62(4): 1897-1910. DOI: 10.1109/TIT.2016.2533395.
- [4] HUANGL B, MODIANO E. Optimizing age-of-information in a multi-class queueingsystem [C]//2015 IEEE International Symposium on Information Theory. Hong Kong, China: IEEE, 2015. DOI: 10.1109/ISIT.2015.7282742.
- [5] TALAK R, KARAMAN S, MODIANO E. Minimizing age-of-information in multi-hop wireless networks [C]//2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton). Monticello: IEEE, 2017. DOI: 10.1109/ALLERTON.2017.8262777.
- [6] LENG S Y, YENER A. Age of information minimization for an energy harvesting cognitive radio[J]. IEEE Transactions on Cognitive Communications and Networking, 2019, 5(2): 427-439. DOI: 10.1109/TCN.2019.2916097.
- [7] HSUY P, MODIANO E, DUAN L J. Age of information: design and analysis of optimal scheduling algorithms[C]//2017 IEEE International Symposium on Information Theory. Aachen, IEEE, 2017. DOI: 10.1109/ISIT.2017.8006590.
- [8] HSU Y P, MODIANO E, DUAN L J. Scheduling algorithms for minimizing age of information in wireless broadcast networks with random arrivals [J]. IEEE Transactions on Mobile Computing, 2019. DOI: 10.1109/TMC.2019.2936199.
- [9] LIU K Q, ZHAO Q. Indexability of restless bandit problems and optimality of whittle index for dynamic multichannel access[J]. IEEE Transactions on Information Theory, 2010, 56(11): 5547-5567. DOI: 10.1109/TIT.2010.2068950.
- [10] LIU Y, LIU K Q, ZHAO Q. Learning and sharing in a changing world: non-Bayesian restless bandit with multiple players [C]//2011 Information Theory and Applications Workshop. La Jolla, IEEE, 2011. DOI: 10.1109/ITA.2011.5743588.
- [11] WHITTLEP. Restless bandits: activity allocation in a changing world[J]. Journal of Applied Probability, 1988, 25(A): 287-298. DOI: 10.2307/3214163.
- 作者简介:**
赵悦超 男, (1995-), 硕士研究生. 研究方向为 5G、无线通信、高可靠低时延通信.
杨 涛(通讯作者) 男, (1970-), 博士后, 副教授. 研究方向为无线通信信号处理. E-mail: taoyang@fudan. edu. cn.
胡 波 男, (1968-), 博士, 博士生导师. 研究方向为天线通信.
-
- (上接第 28 页)
- [9] OUADDAH A, ELKALAM A A, OUAHMAN A A. Towards a novel privacy-preserving access control model based on Blockchain technology in IoT[M]//ROCHA, SERRHINI M, FELGUEIRAS C. Europe and MENA Cooperation Advances in Information and Communication Technologies. Cham: Springer, 2017: 523-533. DOI: 10.1007/978-3-319-46568-5_53.
- [10] DAGHER GG, MOHLER J, MILOJKOVIC M, et al. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology[J]. Sustainable Cities and Society, 2018(39): 283-297. DOI: 10.1016/j. scs. 2018.02.014.
- 作者简介:**
石乐义 男, (1975-), 博士, 教授. 研究方向为信息安全、博弈论. E-mail: shileyi@upc. edu. cn.
刘 娜 女, (1992-), 硕士. 研究方向为工控安全、区块链.
崔雯迪 女, (1995-), 硕士. 研究方向为工控安全、风险评估.
李晓雨 女, (1995-), 硕士. 研究方向为区块链、共享计算.
朱红强 男, (1993-), 硕士. 研究方向为工控安全、深度学习.