DOI 10.15302/J-SSCAE-2020.06.016

信息中心物联网节点状态监测技术研究

崔立群，伍军

（上海交通大学网络安全技术研究院，上海 200240）

摘要：为了管理信息中心物联网（IC-IoT）不断变化的网络状态信息，本文针对 IC-IoT 提出一种节点状态监测方案，以更好适应未来网络的发展。首先提出一种新的管理信息库结构用于记录各种网络节点状态信息，采用信息中心网络（ICN）的命名格式，以网络节点状态内容本身为中心。在此架构上采用跟踪路由方法，结合基于数据块重要性的自适应数据放置策略来获得所需的网络状态信息，提高网络节点状态信息检索效率，同时设计了安全防护机制来达到保证数据机密性与对管理用户进行访问控制的目的。搭建网络仿真测试环境评估了上述跟踪路由机制、自适应数据放置策略、访问控制安全防护带来的时延影响，仿真结果表明此方案能够有效地提高数据获取效率，访问控制模型提供了数据机密性和其他安全性功能，仅附加了少量的计算成本。

关键词：信息中心网络；物联网；节点监测；访问控制

中图分类号：TP3　　**文献标识码：**A

Node Status Monitoring of Information-Centric Internet of Things

Cui Liqun, Wu Jun

(Institute of Cyber Science and Technology, Shanghai Jiao Tong University, Shanghai 200240, China)

Abstract: To manage the constantly changing network status information of the information-centric Internet of Things (IC-IoT), this study proposes a node status monitoring program for the IC-IoT. It first proposes a new management information base structure for recording various network node status information, and adopts the naming format of information-centric networking (ICN), centering on the content of the network node status. In this architecture, we combine the trace route method and adaptive data placement strategy according to the importance of the data block, to obtain the required network status information and improve the retrieval efficiency. At the same time, this scheme designs a security protection mechanism to achieve the purpose of ensuring data confidentiality and access control for management users. Finally, through the establishment of a network simulation test environment, time delay brought by the above-mentioned trace routing mechanism, adaptive data placement strategy, and access control security protection is evaluated. The simulation results show that this scheme can effectively improve the efficiency of data acquisition. The access control model provides data confidentiality and other security functions for the solution, while only brings a small amount of computational cost.

Keywords: information-centric networking; Internet of Things; node status monitoring; access control

收稿日期：2020-09-15；**修回日期：**2020-10-25

通讯作者：伍军，上海交通大学网络安全技术研究院教授，研究方向为物联网及其安全、云计算 / 雾计算及其安全、下一代互联网及其安全、大数据与人工智能安全等；E-mail: junwuhn@sjtu.edu.cn

资助项目：中国工程院咨询项目“网络空间安全保障战略研究”(2017-XY-45)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

信息中心网络（ICN）为未来的物联网（IoT）网络体系结构设计提供了新的思路，已经出现了许多基于 ICN 的物联网解决方案，这些方案进一步验证了 ICN 对 IoT 的适用性。尽管有很多相关 ICN 架构的研究，但目前的评估和验证方法仍然停留在对 ICN 本身的仿真和理论探讨层面，如缓存优化等。Lee H 等 [1] 提出了 ICN-OMF 框架用于可扩展内容中心网络（CCN）测试平台的控制和管理，包括对分散在不同地理位置的多个 CCN 节点的控制和管理。除此之外，ICN 节点的监测与管理研究较少，大多数关联研究专注于实现单个 IoT 应用领域。本文侧重于构建用于控制和监视信息中心物联网（IC-IoT）系统各设备节点的完整框架。

二、相关背景技术

（一）信息中心网络

ICN 以“信息”作为网络核心而不是 IP 协议栈结构，将“信息”作为唯一标识。当用户请求某一信息时，请求的对象是该信息本身，而“信息”就是请求过程中的凭据，相当于 IP 网络中的 IP 地址，信息提供端按照信息名字查找相应数据并返回给请求用户端。ICN 被视为是一种革命性的体系结构，通过直接命名数据使数据占据网络中的首要地位，既不是一种 IP 模式，也不是覆盖 IP 的模式，而是未来全新的网络模式 [2]。国内外的 ICN 研究已有较多成果，且由于在设计上缺乏共识，到目前为止提出了相当多种类的 ICN 结构，使用最多且被认可的主要有 DONA、PSIRP、NetInf、CCN 等数种典型的 ICN。

命名数据是 ICN 的基本思想，但不是完整的架构设计。此外，ICN 架构还通过网内缓存机制来实现高效的数据分发，使得数据不仅只存在生产者中，还可能被缓存在其他网络路由器中，以便再次出现对该数据的请求时消费者能够从更方便的位置获取到该数据。这种从“基于位置”转变为“基于内容”的网络提高了内容传播效率，带来了可扩展性、安全性、移动性、多接入点等特性 [3]。

与 ICN 类似，在 IoT 中消费者感兴趣的是数据内容而不是他们的位置，也就是说 IoT 实际上是以内容为中心的。因此 ICN 的设计理念也适用于 IoT，不再需要维持点到点的通信。已有研究提出了 IC-IoT 概念，近年来出现了许多基于 ICN 的 IoT 机制研究，未来 IoT 也将朝着信息中心的方向发展 [4,5]。

（二）物联网节点监测

随着互联网的不断扩展，适当的互联网管理（包括网络分析和诊断）的重要性也日益增加，应进行监测和控制，管理各种网络设备，实现状态信息的集中管理。IoT 有许多应用领域，如智能家居和城市、交通系统、工业控制系统、医疗保健监测系统等。许多研究采用无线传感器网络（WSN）将与物理域关联的信息、IoT 驱动的计算系统相互关联，可以无处不在地访问位置、环境中不同实体的状态，进行数据采集，以进行长期的 IoT 监视。同样为使网络有效运行，IoT 也需要监测、控制、记录网络性能和设备资源的使用情况，而设备的管理者负责收集网络设备信息，包括设备特性、数据吞吐量、通信超载和错误等。未来 IoT 架构将朝着以内容为中心的方向发展，运用 IoT 技术的网络节点监测系统也将随之改变，在 IC-IoT 的应用场景下，网络节点监测具有较大的研究空间。

三、信息中心物联网节点状态监测架构

（一）基于命名的信息管理库整体架构

在 ICN 原理的启发下，本文基于简单网络管理协议基础，为 IC-IoT 节点监测与管理设计了一个以内容为中心的管理信息库结构。以“统一维护所有网络节点设备”为基本思想，遵循 ICN“以内容为中心”的原则，保存所有正在运行的设备的相关信息，响应管理工作站的查询请求。相应的总体结构如图 1 所示。

与传统的简单网络管理协议中管理信息库的树状结构不同，数据对象经过命名后按类型划分为一系列数据块。一个企业或组织可以定义为数据块，一个协议甚至功能模块也可以定义为数据块，将这些数据块的名称内容放在一起，形成一个中心数据块。在每个数据块中，数据对象按内容名称存储，

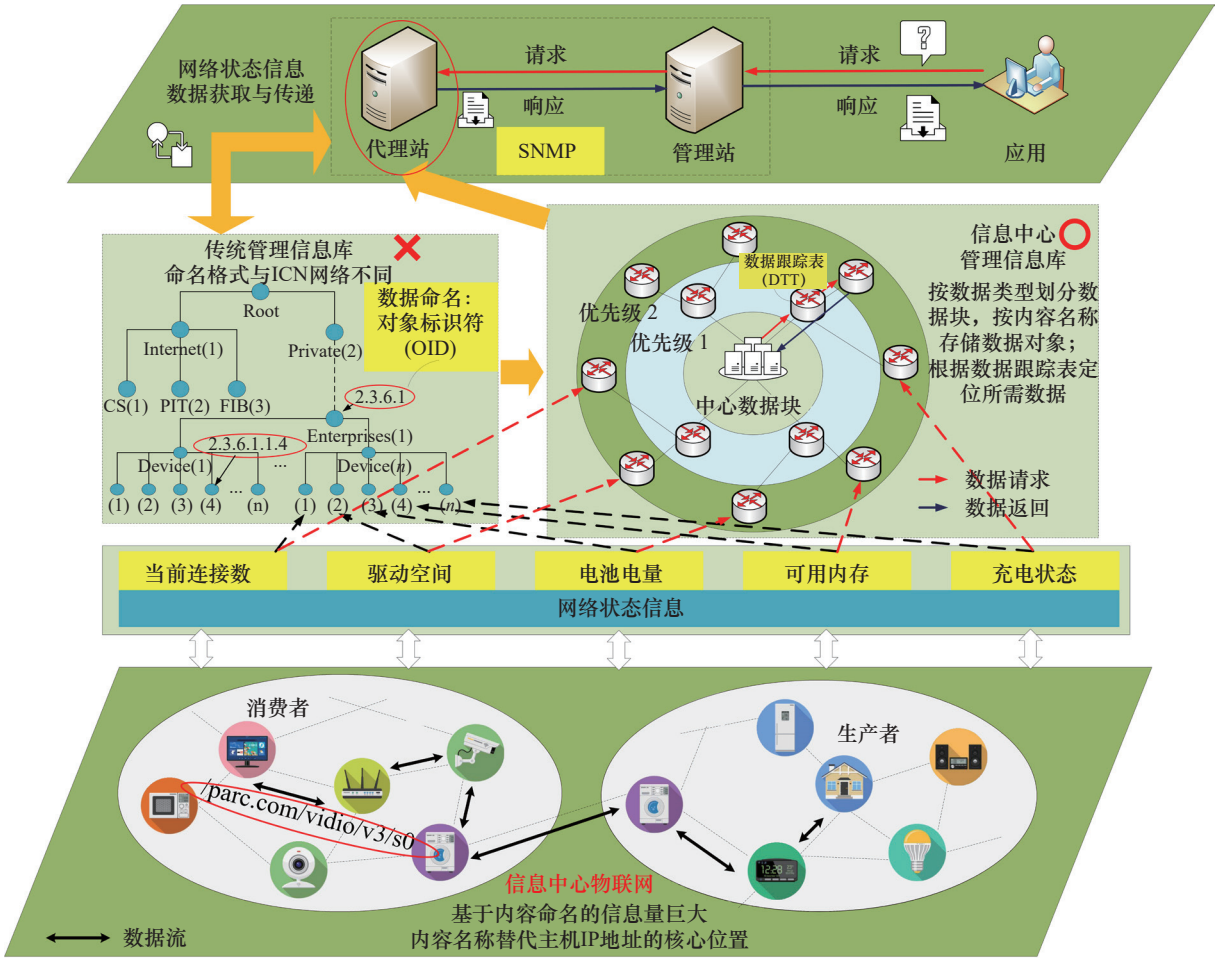

图 1　内容中心命名的管理信息库架构

注：SNMP 为简单网络管理协议；CS 为内容存储；PIT 为未决兴趣表；FIB 为转发信息库。

为了体现被管理网络节点的信息，内容名称主要考虑网络节点的状态，还可包括其访问权限、状态、默认值、历史访问次数和其他属性。当代理需要一个数据对象时，首先在中心数据块中搜索数据所在的子块，然后在该子块中获取所需的数据。通过这个方法简要介绍了目标数据的快速定位原理，从而更好支持数据更新，如块动态加载和卸载等。监测网络节点的状态需要考虑节点的工作状态和接入状态，传统网络系统的节点接入状态分为节点身份、节点接入位置：前者指该设备的类型，体现了该节点在网络中心作用以及在网络拓扑中的位置；后者可以是由子网划分决定的逻辑位置，也可以是由节点端口之间的物理连接所决定的真实物理位置。由于 ICN 并不关心节点位置，因此与命名相关的网络节点状态只需描述节点工作状态（如系统信息、接口信息、运行参数等）和节点身份。

（二）基于名称的节点状态数据获取

ICN 中的每个路由器都有 3 个功能模块用于路由和转发内容：内容存储（CS）、未决兴趣表（PIT）、转发信息库（FIB）。基于这种转发策略，在 ICN 中信息的分配更加高效、准确。这与 IC-IoT 的有效管理机制设计目标一致。同样定义 3 个表：数据块重要性表、数据块结构表、数据跟踪表。数据块重要性表记录每个数据块的重要性，数据块结构表记录数据块间的拓扑信息，它们都存储在中心数据块中；数据跟踪表存储在各子数据块中，包含了内容名称和下一个存有该内容的数据块名称。

如图 2 所示，当代理接收到来自管理站的数据请求时，首先检查请求名称中是否包含数据对象所在的数据块名称。如果存在，直接从中心数据块获取数据并返回管理站；否则从中心数据块开始，在第一优先级的所有子数据块中搜索数据；如果发现某一子数据块的数据跟踪表中存在的内容名称与所

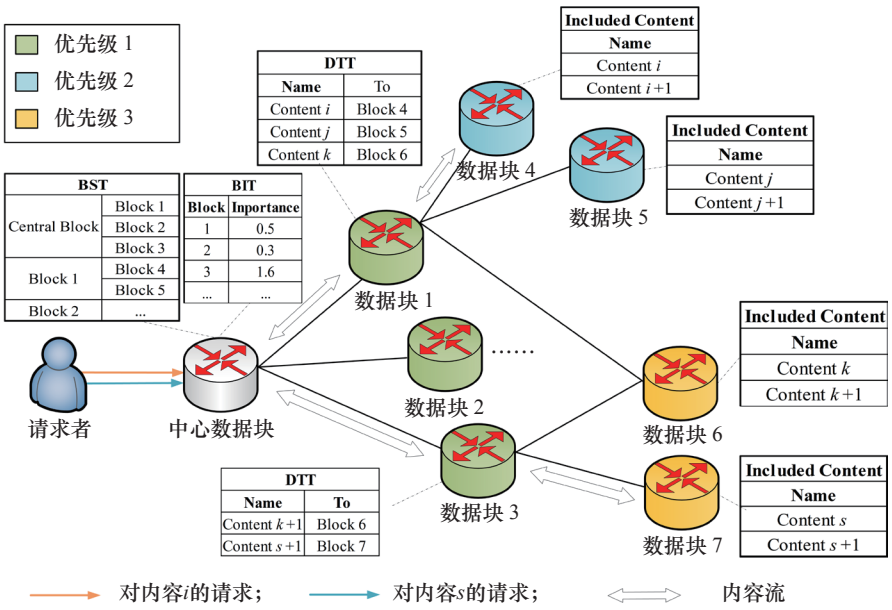

图 2　基于名称的节点状态数据获取过程

注：BIT 为数据块重要度表；BST 为数据块结构表。

需的数据内容名称相匹配，则根据数据跟踪表中的信息将请求转发到下一个子数据块；如此随优先级递减，直到找到所需数据存在的数据块为止。

对于数据块的放置，本文采用基于优先级的边缘放置策略。首先将数据块重要性定义为一个参数，与仅考虑流行度的传统替换策略不同，本文根据数据块重要性来实时更改数据块的放置，即数据块越重要，其优先级越高。将优先级高的数据块放在靠近中心数据块的位置，使得相较于传统的管理信息库（MIB）结构，代理能更快检索到所需数据，进而提高网络节点监测的实时性。

四、信息中心物联网节点状态监测安全防护

（一）节点状态监测中的安全问题

与 IP 网络技术相比，ICN 凭借网内缓存、支持移动性等特性更适合 IoT 应用，但也带来了一些安全性挑战。首先，因为内容占据着网络核心位置，易遭受兴趣泛洪攻击和内容中毒攻击；其次，ICN 中存在最重要的安全问题，即内容和缓存隐私 [6]。从网络监测与管理的角度来看，ICN 存在访问控制、身份验证、数据安全、隐私性等诸多安全挑战。本文着力解决 IC-IoT 节点状态监测过程中的两个安全问题：内容隐私保护、管理站访问控制。

（二）基于命名的信任机制

在不考虑内容本身的情况下，消费者与生产者之间的信任是从双方事先约定好的凭据中获得的；遵循的原则是直接从公开的身份或内容名称中获得信任。如果选择信任身份，那么也就对与该身份关联的内容具有某种程度的信任，这种关联应该是易于验证的。

当名称中包含有关该实体真实身份的有效信息时，可确保该实体身份，但需要一种机制来验证信息的有效性。同样，公共密钥应与其所有者的真实世界身份绑定在一起，因为此密钥将用于生产者身份验证。为了提供数据机密性，必须采用基于加密的模型来命名，授权实体必须知道解密密钥。为了验证生产者的身份并保证数据的有效性，所有内容均需要采用初始内容提供者的私钥进行数字签名。如果内容名称没有包含有关生产者身份的足够有效信息，则按以下方式发起攻击：通过监听兴趣包，攻击者会构建虚假内容并将之与合法内容名称绑定在一起；向请求者发送一个数据包，包含相同的名称、错误的内容、有关他自己的密钥信息（在已签名的信息字段中）、关联的数字签名；接收此内容后，请求者根据公用密钥和攻击者的证书来认为该数据是正常数据，由于数据包看起来合法并且带有合法签名，请求者将无法感知受到攻击。

（三）面向节点监测的访问控制

访问控制是 ICN 中保障安全的重要手段。如果未应用访问控制，则合法用户和恶意用户之间将没有区别，代理在任何名称空间下都将发布数据，并且请求者可以访问任何内容。这种安全方面的重要性要求采用访问控制模型，本文建议在代理处理密钥管理和数据内容发布的同时，还应为管理用户设置最大访问时间 [7]，根据附加在管理站发送的兴趣包上的用户签名，执行身份验证和审查。一旦合法用户试图超过其有限的访问时间，代理就会感知这种欺骗性的行为。

本文设计方案中，内容提供者（即代理站）根据配置的安全策略将其存储内容划分为具有唯一群体身份（GID）的不同组，并将 GID 添加到内容名称中。此外，利用特权掩码表示用户的特权，一个用户可以访问多个组的内容；特权掩码是位映射，每个位表示用户是否可用于相应组中的内容。例如，如果用户权限掩码的第二位是“1”，则表示用户有权访问 GID 为 2 的组中内容。

管理用户首先向代理注册，当被限制访问时间的管理用户注册到代理中时，代理生成管理用户的特权掩码，根据用户身份设置其最大访问时间。然后，用户发送附加签名的兴趣包来获取所需数据，代理根据获得的用户信息对请求进行身份验证，成功认证之后兴趣包被允许进入并返回对应的内容数据包。为了保证数据的机密性，代理在返回数据包给管理站之前对内容进行加密。具体访问控制模型如图 3 所示，利用哈希链提高认证过程的效率，以降低代理站的负担。一般来说，用户会持续不断地请求一系列数据，代理可以利用哈希链的单向属性，通过对文件的第一请求签名来对用户进行认证，并利用哈希链来认证后续请求的与哈希链相同的文件。

五、实验测试与评估

本文使用 ns-3 和 ndnSIM2.5 对 IC-IoT 节点状态监测架构进行建模仿真并分析结果。整个仿真分为两部分：一是对跟踪路由数据获取机制和基于重要度的数据放置策略的评估；二是对访问控制模型的评估，获得参数对监测数据获取的时延影响。首先建立一个简单的数据块拓扑结构，假设每个数据

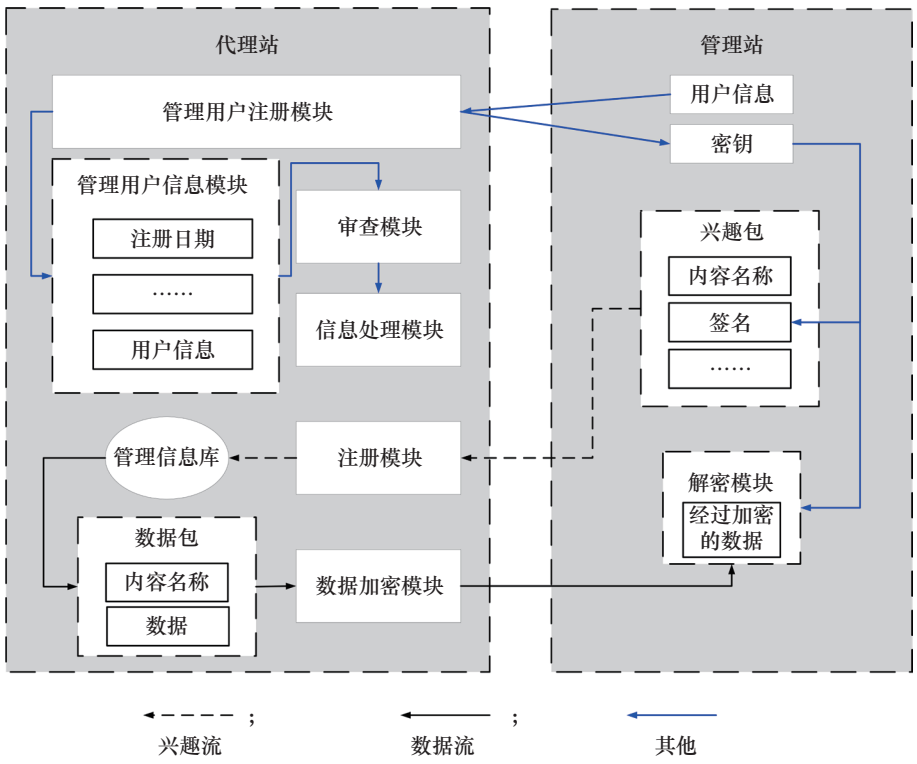

图 3　面向节点监测的访问控制模型

块中的数据量是相同的，随后为各个数据块设置不同的重要级别。

（一）数据放置策略评估

仿真过程中采用一个具有 37 个可用数据块的拓扑结构，除中央数据块外，其余数据块的优先级在 1~6 之间变化。期望结果是：在这种信息管理库结构中获取数据所需的时间与块的重要性成反比，如果请求中没有数据块名或没有跟踪路由策略，则获取数据的时间延迟将有显著差异。

由图 4 可以直观地看到，与仅基于请求数量或内容流行度的替换策略相比，采用基于数据块重要度的替换策略后，请求访问所需数据的平均跳数在一段时间内显著减少。这是因为在基于数据块重要度的数据放置策略中，频繁请求的数据将被放置在一个更高优先级的数据块中，因此数据块自适应替换策略是有必要的。

（二）数据获取模型评估

根据定义的 ICN 数据对象命名规则，应用于 IC-IoT 节点状态监测场景，在基于内容命名的新型管理信息库结构中所定义的内容名称，包含其所在的数据块的名称（即资源主体名称）；管理用户有时并不知道他所请求内容的具体完整名称，因此在这些请求中有时将不包含数据块名称。为此考虑 3 种情况。场景 1：请求兴趣包中含有数据块名称；场景 2：请求中不含数据块名称，并且在数据采集过程中没有跟踪路由策略；场景 3：请求中不含数据块名称，但在数据采集过程中有跟踪路由策略。本文对这 3 个场景下获取设备状态信息数据的延迟时间进行了测试，当优先级罗高时，跟踪路由策略所产生的时延减少效应更为明显（见图 5）。

（三）访问控制机制评估

在 ndnSIM 2.5 中访问控制模型进行了模拟，并与基本内容中心网络（NDN）的性能进行了比较。此时管理信息库中数据块大小不同，仿真设置了 5 种类型节点：10 MB，100 MB，300 MB，700 MB、1 GB，由每个拓扑节点来代表各个数据块，管理节点每次请求的数据包大小设为 1 MB，请求时间间隔设为 2 s。每个管理站节点的请求到达数据提供节点时，都要对该请求进行身份验证，在此过程中，通过分析网络获取数据包的时延来进行评估访问控制模型带来的时间开销。在管理站路由器请求带有正确前缀的内容，且始终连续请求同一数据块中的数据的情况下，图 6 显示了不同数据块大小的数据检索延迟，基本 NDN 带来了较低的延迟。当网络中加入访问控制机制后，如果数据块的大小不太大，它的性能依然很好。随着数据块大小的增加，带有访问控制机制的网络与基本 NDN 之间的区别变得很明显，因为更多的数据块意味着身份验证和解密需要进行更多次。整体来看，基本 NDN 与引入访问控制机制的网络在数据获取时延之间的差距是可以接受的。

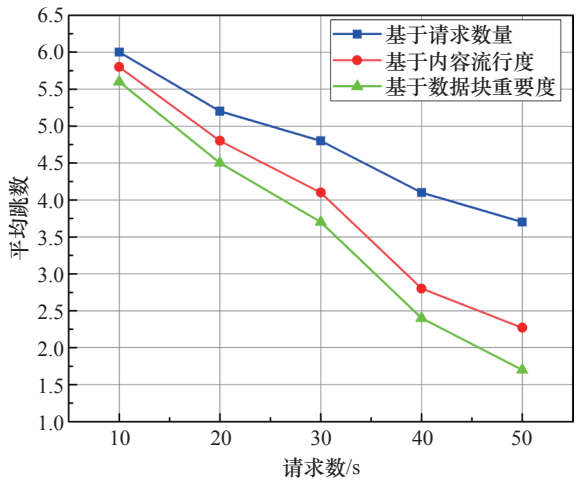

图 4　不同数据替换策略的结果比较

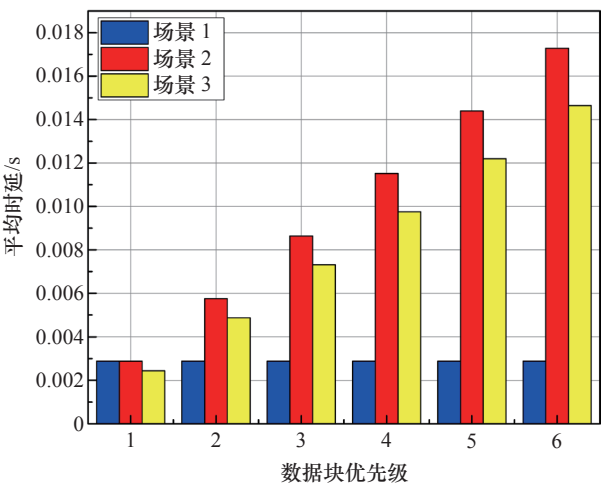

图 5　数据获取模型的评估结果

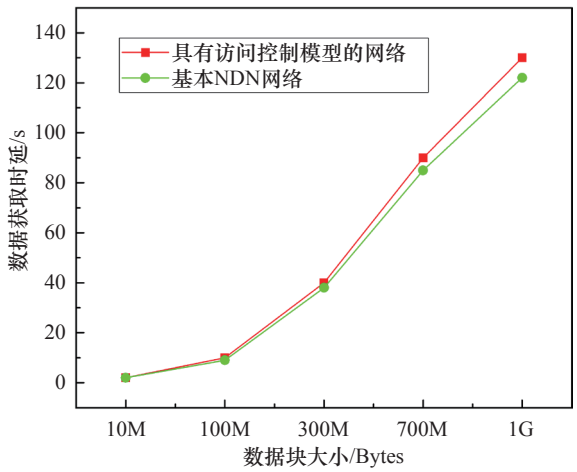

图 6　访问控制机制对数据获取时延的影响

六、结语

本文重点研究面向 IC-IoT 的节点状态监测架构及其安全防护技术设计。从监测架构方面来说，仅提出了与传统网络管理协议不同的新型管理信息库结构，以适应未来 ICN 的发展，但监测过程仅在本地管理站中进行。后续研究可以将智能管理延申到网络边缘，采用分层架构执行本地管理决策，以扩大网络覆盖率并对网络节点实施更加精准的监测；也可进一步增强架构安全防护机制，从访问控制和简单数据加密拓展到更高级的、独立于服务的安全机制；还可以考虑在安全防护中加入去中心化的区块链技术，使数据交换过程中的数据机密性与完整性得到更多保护，且不损害未来移动设备和支持第五代移动通信的互联网所必需的功能。

参考文献

[1] Lee H, Kim D, Suh J, et al. ICN-OMF: A control, management framework for Information-Centric Network testbed [C]. Gwangiu: International Conference on Information Networking (ICOIN), IEEE, 2015.

[2] 孙彦斌, 张宇, 张宏莉. 信息中心网络体系结构研究综述 [J]. 电子学报, 2016, 44(8): 2009–2017.
Sun Y B, Zhang Y, Zhang H L. Survey of research on information-centric networking architecture [J]. Acta Electronica Sinica, 2016, 44(8): 2009–2017.

[3] 杨若冰, 马严. 命名数据网络中的转发策略研究 [J]. 新型工业化, 2015, 5(10): 63–71.
Yang R B, Ma Y. Research on forwarding strategies in named data networking [J]. The Journal of New Industrialization, 2015, 5(10): 63–71.

[4] Amadeo M, Campolo C, Quevedo J, et al. Information-centric networking for the internet of things: Challenges and opportunities [J]. IEEE Journals and Magazines, 2016, 30(2): 92–100.

[5] Arshad S, Azam M, Rehmani M. Recent advances in Information-Centric Networking-Based Internet of Things (ICN-IoT) [J]. IEEE Internet of Things Journal, 2019, 6(2): 2128–2158.

[6] 霍跃华, 刘银龙. 内容中心网络中安全问题研究综述 [J]. 电讯技术, 2016, 56(2): 112–120.
Huo Y H, Liu Y L. Survey on security issues in content-centric networking [J]. Telecommunication Engineering, 2016, 56(2): 112–120.

[7] He P, Wan Y, Xia Q, et al. LASA: Lightweight, auditable and secure access control in ICN with limitation of access times [C]. Kansas City: IEEE International Conference on Communications, IEEE, 2018.