基于时间自动机的物联网网关安全系统的建模及验证

王国卿，庄雷，王瑞民，宋玉，张坤丽
（郑州大学信息工程学院，河南 郑州 450001）

摘 要：物联网是一个多网异构融合网络，其感知层常面临各类安全威胁。物联网网关作为感知层和网络层的桥梁，应当具备安全管理功能，防止安全问题向上层扩散。针对物联网网关目前安全方面的不足，以物联网网关中间件技术为平台，设计一个通用的物联网网关安全系统。该系统可以嵌入不同的安全协议或算法，然后进行建模与分析，能够辅助安全网关的设计和具体实现。利用时间自动机对系统进行形式化建模与验证，验证结果表明物联网网关安全系统满足机密性、可用性、真实性、顽健性、完整性和新鲜性 6 项安全需求。

关键词：物联网网关；安全系统；中间件；时间自动机；模型检测
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000-436x.2018042

Modeling and verifying based on timed automata of Internet of things gateway security system

WANG Guoqing, ZHUANG Lei, WANG Ruimin, SONG Yu, ZHANG Kunli
School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China

Abstract: The Internet of things (IoT) is a multiple heterogeneous network, and its perception layer is often faced with various security threats. As the bridge between the perception layer and the network layer, the IoT gateway should have the security management function to prevent the security issue from spreading to the upper layer. According to the current security deficiencies in IoT gateway, a universal IoT gateway security system was proposed based on the IoT gateway middleware technology. Various security protocols or algorithms can be embedded in IoT gateway security system, and the modeling and analysis can help the design and implementation of IoT gateway. The formal modeling and verification of the IoT gateway security system was performed by timed automata. The results show that the IoT gateway security system satisfies the security properties of confidentiality, availability, authenticity, robustness, integrity and freshness.

Key words: IoT gateway, security system, middleware, timed automata, model checking

1 引言

随着第 4 次工业革命的到来，人类社会正逐步进入一个万物互联的时代，物联网（IoT, Internet of things）应运而生。物联网是继计算机、互联网和移动通信之后的又一次革新发展，是信息化时代的重要发展阶段[1]。物联网是由具有自我标识、感知和智能的物理实体基于通信技术相互连接而成的网络，这些物理实体可以自发地进行协同和互动，以实现智能的识别、定位、监控和管理，

收稿日期：2017-10-12；**修回日期**：2018-02-20
通信作者：庄雷，ielzhuang@zzu.edn.cn
基金项目：国家自然科学基金资助项目（No.61379079）；河南省科技攻关计划基金资助项目（No.172102210478）；河南省国际科技合作计划基金资助项目（No.152102410021）
Foundation Items: The National Natural Science Foundation of China (No.61379079), The Science and Technology Key Project of Henan Province (No.172102210478), The International Cooperation Program of Henan Province (No.152102410021)

从而将人类社会、信息空间和物理系统进行有机的融合[2]。

物联网的体系结构如图 1 所示，共分为 3 层。其中，感知层负责随时获取物理实体的信息，并将应用层指令反馈给物理实体；网络层负责实时传输各类信息、数据和指令；应用层负责对海量数据和信息进行分析、处理及决策，接收用户的服务定制。3 个层次并不是相互独立的，而是相互支撑、相互影响的，进而搭建起整个体系架构。

网关技术在传统互联网中的运用比较成熟，应用到物联网体系中，将成为连接感知网络与传统通信网络的纽带。作为物联网网关，可以实现感知网络与通信网络以及不同类型感知网络之间的协议转换[3]。物联网网关还可以提供管理功能和安全策略[4]。通过物联网网关设备可以管理底层的感知节点和运行设备，监测各物理实体的运行状态，实现远程控制；带有安全策略的物联网网关可以屏蔽传感器网络和移动通信网的异构性，实现从协议级到应用级的保护。

在物联网网关的体系结构方面，许多学者设计并实现了网关的基本功能[5~8]，主要包括感知接入、协议适配、协议转换、消息传输等，解决了物联网网关的关键问题，即对异构网络的不同通信协议进行转换和底层通信协议到上层通信协议的转换，并在物联网网关的管理与控制时，建立可统一识别指令及标准。但在网关安全方面没有详细设计，或默认安全策略已经完备，或只是简单说明而没有具体实现。

关于物联网网关安全方面的研究，文献[9]针对 IoT 中机器对机器（M2M, machine to machine）通信，设计了一个安全网关应用（SGA, security gateway application），其中，包括对称密钥加密协商功能、安全密钥交换生成功能和信息安全传递功能，能够满足 M2M 服务层的基本安全需求；文献[10]设计了一种基于动态优先级调度算法的异构物联网网关，可支持 RS485、蓝牙、ZigBee 等协议，通过实现高层协议保证了物联网网关的数据安全性和可靠性；文献[11]提出了一种结合物联网智能设备与控制系统网关的实时响应模型，通过加强身份验证与授权的控制，以提高系统的安全性；文献[12]讨论了传感器网络、家庭网关和应用终端的安全问题及相应的解决方案，通过对这 3 个部分安全性进行有机整合，实现信息传输和用户隐私的安全保护，最大限度地保护智能家居的安全；文献[13]设计实现了基于 Modbus 协议的物联网汇聚安全网关，通过在应用层构建网关覆盖网，提供网关信任管理，有效解决了网关海量数据的拥塞控制问题，

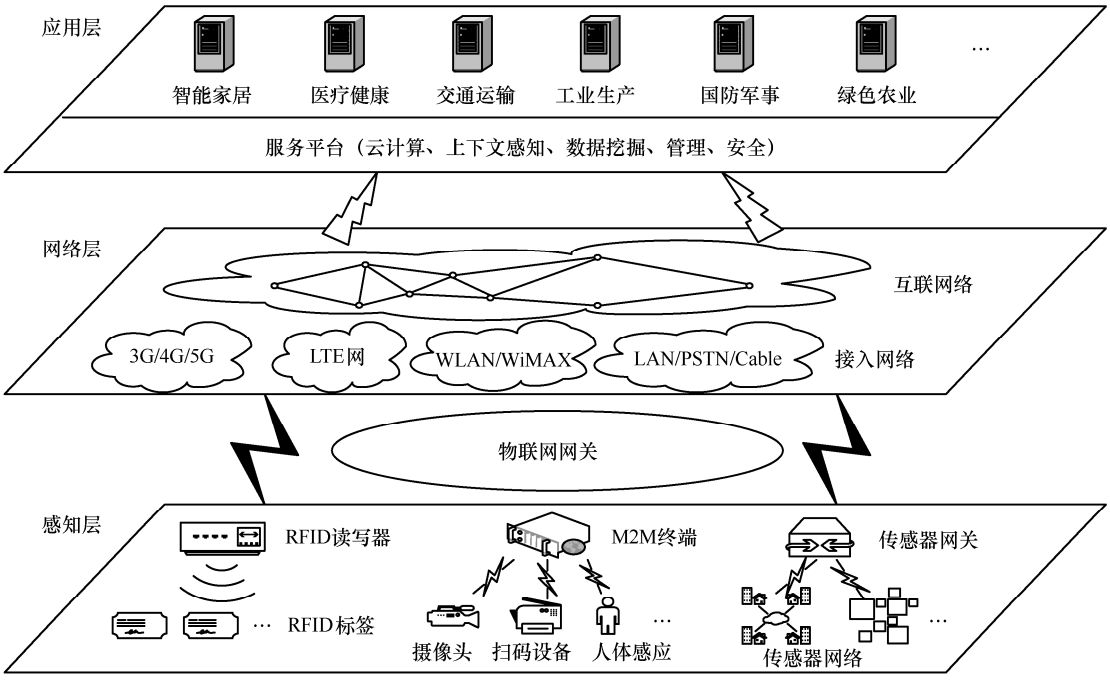

图 1 物联网体系结构

保证了网关虚拟网络的安全性。上述研究成果大多针对某一特殊场景，例如，文献[11,13]主要应用于工业物联网，文献[12]主要应用于智能家居。文献[9,10]虽然应用场景更宽泛一些，但在安全体系的设计上存在一些不足。文献[9]集中考虑了密钥管理体系，对其他安全技术没有涉及；文献[10]的安全网关在应用层级，没有考虑连接感知层和网络层的网关安全性。

基于对当前研究现状的分析，针对物联网网关安全方案存在的不足，利用物联网安全常用的密钥管理、身份认证、入侵检测等技术，设计了一个通用的物联网网关安全系统。通过对系统的形式化分析与验证，保证了系统的机密性、可用性、真实性、顽健性、完整性、新鲜性等相关安全特性，为网关中间件的设计和实现提供了理论框架。物联网网关安全系统可以嵌入各类安全协议或算法，然后进行建模与分析，验证系统是否正确与可靠，对网关的具体设计和实现具有指导意义。

2　物联网网关安全系统的设计

物联网是信息技术发展的趋势，物联网应用在给人们生活带来便利的同时，也带来了很多安全隐患。尤其物联网感知层作为物联网体系结构的底层，直接面向现实环境，承担着信息感知和命令执行的重任，其安全问题尤为重要。

物联网网关作为感知层和网络层的桥梁，由于硬件设备的迅猛发展，其功能不再局限于单一的协议转换，可以向服务提供、设备管理、安全检测等功能扩展[14]；中间件技术可屏蔽底层硬件细节，对外提供统一抽象接口，使用跨层设计的思想，在满足应用动态性的同时可满足应用异构性，为安全系统的实现提供了平台[15]。

2.1　物联网网关安全需求

物联网感知层的安全异常重要，作为底层感知和执行设备，所有物联网应用能否正常运行全部依赖于感知层是否安全可靠。由于感知层自身有限的存储空间和计算能力、有限的带宽和通信能量以及网络协议安全形式的多样，感知层经常面临通信信道攻击、拒绝服务攻击、节点捕获、假冒攻击、路由协议攻击等安全威胁[16]，如表 1 所示。

针对上述安全威胁，物联网网关需要弥补感知层能力的不足，避免安全缺陷从感知层通过网关传递到网络层，应满足以下 6 个方面的安全需求[17]。

1) 机密性：消息对非授权方是保密的。
2) 可用性：按约定向合法用户提供服务。
3) 真实性：消息认证能够核实来源的真实。
4) 顽健性：面对不确定因素具有强适应性。
5) 完整性：收到的信息与源信息完全一致。
6) 新鲜性：保证消息的时效性。

网关技术具有有效的安全隔离、灵活的业务代理、成熟的技术积累等特点。为了应对感知层安全威胁，避免感知层安全问题向上扩散，信息加密、认证与访问控制、入侵检测等信息安全技术可以综合运用到物联网网关安全系统中，能够和其他相关技术实现较好的衔接，从而满足物联网网关安全需求。基于网关中间件及安全支撑平台构建的物联网网关安全技术框架如图 2 所示。

2.2　网关安全系统的逻辑流程

在传感器网络中，节点通过各种方式大量部署在被感知对象内部或附近，这些节点通过自组织方式构成无线网络，以协作的方式感知、采集和处理网络覆盖区域中特定的信息，可以实现对任意地点信息在任意时间的采集、处理和分析。对于新加入或退出的节点，自组织网络可设定生存时间检测，通过多跳的方式连接至汇聚节点，节点收到数据连接安全网关，整个系统通过任务管理器来管理和控制。

根据所设计的物联网网关安全技术框架，物联

表 1　　**物联网感知层面临的安全威胁**

名称	说明
通信信道攻击	消息的截取、篡改、重放及注入，攻击者通过长时间占据信道导致合法通信无法传输
拒绝服务攻击	污水池（sinkhole）攻击、虫洞（wormhole）攻击、洪泛攻击等，DoS 攻击会耗尽节点资源，使节点丧失运行能力
节点捕获	网关等关键节点被攻击者控制，可能导致通信密钥、广播密钥、配对密钥等被泄露，进而威胁网络的通信安全
假冒攻击	恶意节点假冒合法节点发起女巫（sybil）攻击，利用多身份与其他节点通信，并配合其他攻击手段达到攻击目的
路由协议攻击	通过欺骗、篡改或重发路由信息，攻击者可创建路由循环，形成虚假错误消息，增加端到端时延，耗尽关键节点能源等

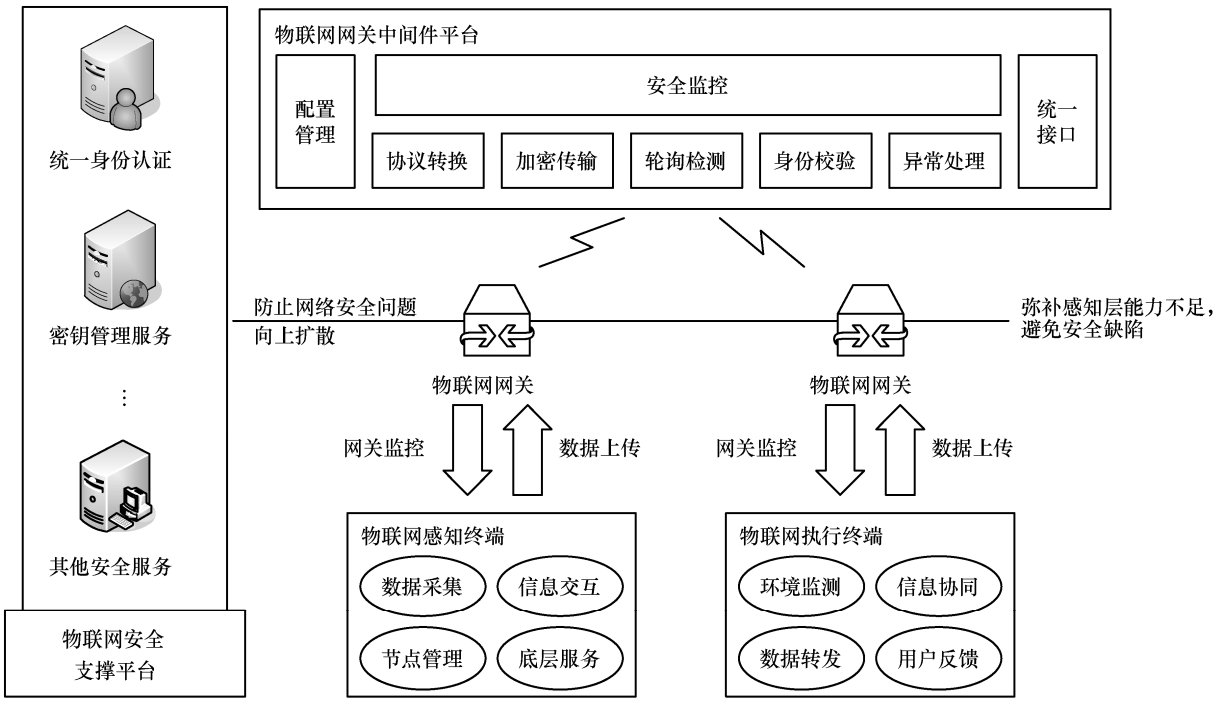

图 2 物联网网关安全技术框架

网网关安全系统实现在物联网网关中间件平台上，其在完成物联网网关基本功能的基础上，添加了加密传输、轮询检测、身份校验、异常处理等子模块。物联网网关安全系统的逻辑流程如图 3 所示。

为了便于建模与检测，仅抽取主要流程分析并进行适当假设。物联网网关安全系统的顶层主模块在网关进行消息转发等基本功能的基础上实现了网关合法性认证及入侵检测，以确保网关的安全启动和运行，然后进入中间层轮询模块。终端在轮询时一般处于工作状态，需要安全系统发出控制指令检测终端状态。对于感知终端，由于感知节点的大规模和随机性，安全系统主要连接汇聚节点进行监测，汇聚节点的处理能力、存储能力、通信能力相对较强，在实现通信协议栈转换的同时，可发布网关的监测任务。对于执行终端，如果设备正在运行，则令设备在合法时间内运行一段时间，如果在规定时间内设备状态能正确返回到安全系统，则认为轮询成功，设备处于正常状态，生成监控信息。底层主要提供了密钥算法、统一认证、入侵检测、异常处理等安全服务，应用于顶层和中间层的各个环节，以保证安全系统整体的安全可靠。

若暂不考虑底层安全服务模块所选策略，设网关安全系统所需管理的终端数为 n，则顶层主模块的时间复杂度为 $O(n)$，中间层轮询模块的时间复杂度为 $O(n^2)$，所以网关安全系统的时间复杂度为 $O(n^2)$。若进一步考虑底层安全服务模块，则时间复杂度受到底层所选策略的影响可能会提高，但由于底层所选策略通常是成熟的算法，因此，应用到网关安全系统中的总时间复杂度是可以接受的。

3 基于时间自动机的网关安全系统建模

由于物联网网关安全系统不仅需要满足运行结果的逻辑正确性，部分功能还需要满足时间的正确性，因此，选择时间自动机进行形式化分析，可有效刻画物联网网关安全系统的时间属性，并可借助模型检测工具 UPPAAL 进行验证。

3.1 预备知识

定义 1 时钟约束。假设时钟变量集为 C，时钟约束 τ 的定义为

$$\tau ::= c \sim n \mid \tau_1 \wedge \tau_2$$

其中，$c \in C$，$n \in \mathbb{N}$，$\sim$ 表示二元关系{<，≤，=，≥，>}中的一种，时钟约束集 $T(C)$ 是时钟约束 τ 的集合。

时钟解释 v 是从 C 到 $\mathbb{R}^+ \cup \{0\}$ 的一个映射，$\mathbb{R}^+$ 为正实数集，即时钟变量集 C 中每个时钟的变量赋值。对于时钟变量集 C 的子集 X，$X := 0$ 表示 X 的

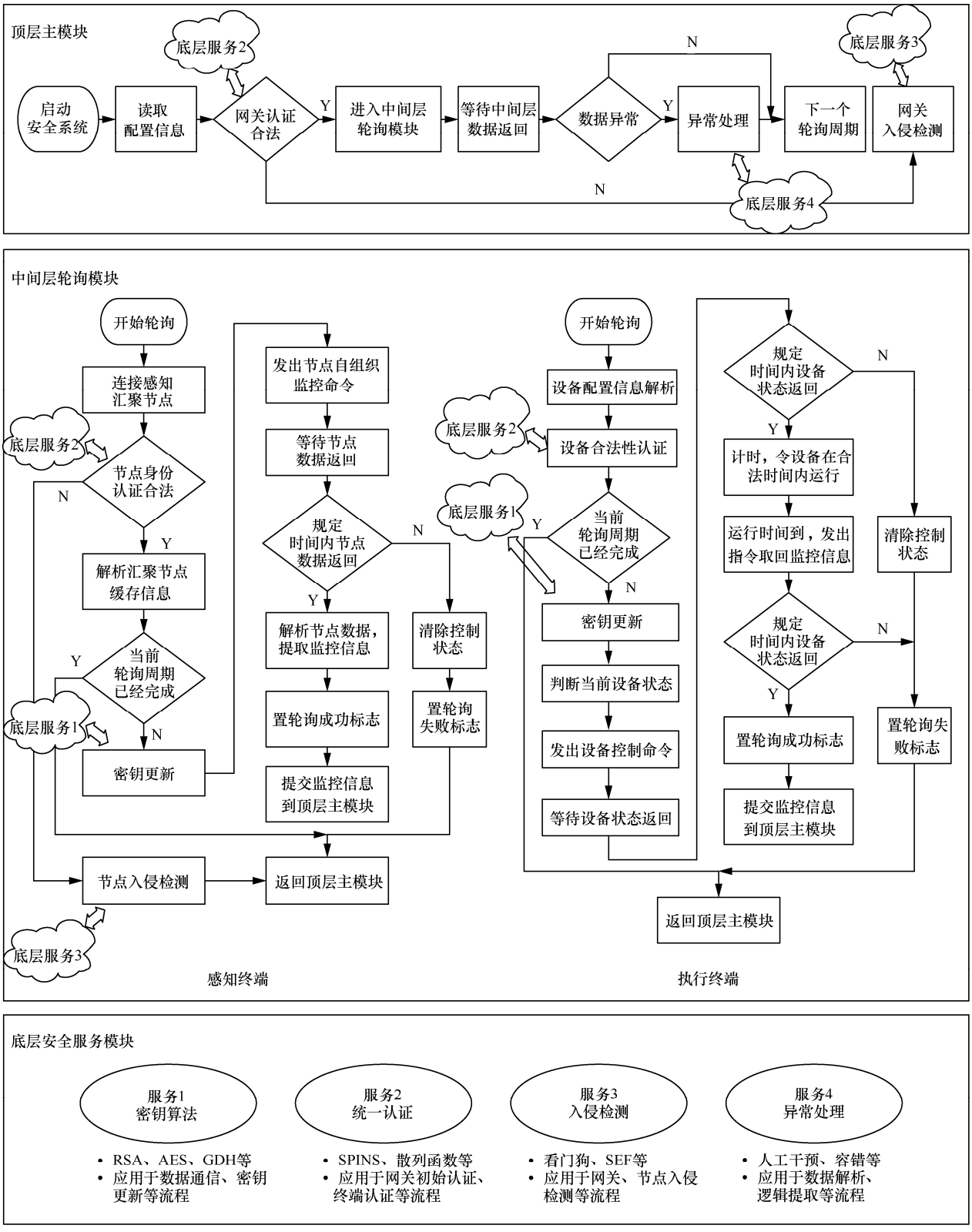

图 3　物联网网关安全系统的逻辑流程

所有时钟变量 c 赋值为 0（即时钟复位），而对集合 $C-X$ 的时钟变量没有影响。

定义 2　时间自动机[18]。时间自动机定义为一个六元组 (C,L,l_0,A,I,E)，其中，C 是时钟变量集，L 是有穷的状态位置集，$l_0 \in L$ 是起始位置，A 是有穷的动作事件集合，I 是一个映射使每一个状态位置

$l \in L$ 都有一个时钟约束，$E \subseteq L \times A \times T(C) \times 2^C \times L$ 是边界的规则转换集合。

一个规则转换 (l,a,τ,λ,l') 表示当状态位置 l 的时钟满足时钟约束 τ，则系统可以完成动作事件 a 从状态位置 l 转移到状态位置 l'，并完成 λ 中的全部时钟复位。

根据物联网网关安全系统流程的分层设计，可考虑引入层次时间自动机进行建模，它以层次方式对时间自动机进行了扩展，能有效解决建模时的复杂流程与蕴含逻辑。

定义 3 层次时间自动机[19]。层次时间自动机定义为一个八元组 $(L,L_0,\delta,V,C,Ch,I,E)$。

1) L 是有穷的状态位置集，描述系统中的不同位置状态。

2) $L_0 \in L$ 是起始位置集合。

3) $\delta: L \to 2^L$ 是一个从位置 l 到 l 所有可能的子状态映射函数。

4) V、C、Ch 分别是变量、时钟及通道的集合。

5) $I: L \to Invariant$，使每一个状态位置 $l \in L$ 都有一个时钟不变量。

6) $E \subseteq L \times (Guard \times Ch \times Reset \times \{\text{true,false}\} \times L)$ 是边界的规则转换集合，其中，$Guard$ 是卫式集合，$Reset$ 是时钟重置集合。当紧急标记为 true 时，转移立即进行；若为 false，边界各约束可以忽略。

3.2 形式化表示

使用层次时间自动机建模，整个系统表示为 3 个层次。

$$\text{SecuritySystem} \equiv \text{Top} \parallel \text{Middle} \parallel (\text{KMS} \parallel \text{AC} \parallel \text{IDS} \parallel \text{Exception})$$

其中，Top 表示顶层主模块，Middle 表示中间层轮询模块，底层安全服务模块包括 KMS 密钥管理系统、AC 认证中心、IDS 入侵检测系统及 Exception 异常处理。模型中状态位置、同步通道、变量等符号的含义如表 2~表 4 所示。

表 2 模型中状态位置的含义

状态位置	含义	状态位置	含义
Start	启动安全系统	CheckCategory	检查终端类别
Configuration	读取网关配置信息	Connect	连接感知汇聚节点
Authentication	统一身份认证	ReadCache	解析汇聚节点缓存信息
WaitAC	等待认证信息返回	CheckAP	检查轮询周期完成标识
CheckGS	检查网关状态	UpdateKey	密钥更新
CheckTS	检查终端状态	WaitKMS	等待密钥管理系统工作
IntrusionDetection	入侵检测	SelfMonitoring	发出自组织监控命令
WaitIDS	等待入侵检测系统处理完成	WaitNode	等待节点数据返回
Idle	空闲状态	CheckRF	检查返回标识
Restart	网关重新启动	Clear	清除控制状态
EnterMiddle	进入中间层轮询模块	MonitoringInfo	准备提交监控信息至顶层主模块
WaitData	等待中间层返回监控信息	ReadConInfo	读取执行设备配置信息
CheckData	检查是否有监控信息返回	DeviceControl	发出设备控制命令
Verify	数据是否异常	WaitDevice	等待设备状态返回
WaitHE	等待异常处理	Keep	令设备在合法时间内运行一段时间
DataAnalysis	解析监控信息	RetrieveData	发出取回监控信息命令
Record	记录监控信息或轮询失败的信息	Failure	轮询失败
CheckPolling	当前轮询周期是否完成	End	该逻辑流程结束

表 3　模型中同步通道的含义

同步通道	含义
StartIDS	开始进行入侵检测
FinishIDS	入侵检测完成
StartAC	开始进行身份认证
FinishAC	身份认证完成
StartMiddle	开始执行中间层轮询模块
FinishMiddle	中间层轮询模块执行完成
StartKMS	开始进行密钥管理
FinishKMS	密钥管理完成
HandlingException	开始进行异常处理
Return	异常处理完毕返回
Decryption	解密
DReturn	解密完成
Encryption	加密
EReturn	加密完成

表 4　模型中变量的含义

变量	含义
c	全局时钟
x, y, z	KMS 时钟，中间层时钟，IDS 时钟
Category	类别标识：1-网关，2-感知终端，3-执行终端
GatewayStatus	网关认证合法状态
TerminalStatus	终端认证合法状态
SubmitData	监控信息提交至顶层标识位
AlreadyPolling	轮询周期完成标识位
PollingSuccess	轮询成功标识位
AuthenticationFlag	认证标识
KMSType	密钥管理功能类别：1-更新密钥，2-验证密钥
KeyUpdateFlag	密钥更新标识
KeyVerificationFlag	密钥验证标识
ReturnFlag	返回标识
ExceptionLevel	数据异常等级：0-无异常，1-容错机制，2-人工干预

顶层主模块形式化模型为 Top = $(L_0, L_{00}, \delta_0, V_0, C_0, Ch_0, I_0, E_0)$，其中，

L_0 = {Start, Configuration, Authentication, WaitAC, CheckGS, IntrusionDetection, WaitIDS, Idle, Restart, EnterMiddle, WaitData, CheckData, Verify, WaitHE, DataAnalysis, CheckPolling, Record}

L_{00} = {Start}

δ_0 是一个映射函数，将状态位置映射为卫式，其具体表示如图 4 所示。

V_0 = {*Category*, *GatewayStatus*, *SubmitData*, *AlreadyPolling*}

C_0 = {c}

Ch_0 = {StartAC!, FinishAC?, StartMiddle!, FinishMiddle?, HandlingException!, Return?, StartIDS!, FinishIDS?}

I_0 = {Record→c≤600, Restart→c≤300}

E_0 = {(Start, ∅, ∅, c := 0, Configuration), (Configuration, c≥90, ∅, *Category*=1, Authentication), (Authentication, ∅, StartAC!, ∅, WaitAC), (WaitAC ∅, FinishAC?, ∅, CheckGS), (CheckGS, !*GatewayStatus*, ∅, *Category*=1, IntrusionDetection), (IntrusionDetection, ∅, StartIDS!, ∅, WaitIDS), (WaitIDS, ∅, FinishIDS?, ∅, Idle), (Idle, ∅, ∅, c := 0, Restart), (Restart, c≥180, ∅, ∅, Start), (CheckGS, *GatewayStatus*, ∅, ∅, EnterMiddle), (WaitData, ∅, FinishMiddle?, ∅, CheckData), (CheckData, !*SubmitData*, ∅, ∅, CheckPolling), (EnterMiddle, ∅, StartMiddle!, ∅, false, WaitData), (CheckPolling, *AlreadyPolling*==1, ∅, ∅, CheckGS), (CheckData, *SubmitData*, ∅, ∅, Verify), (CheckPolling, *AlreadyPolling*==0, ∅, c := 0, Record), (Verify, ∅, HandlingException!, ∅,

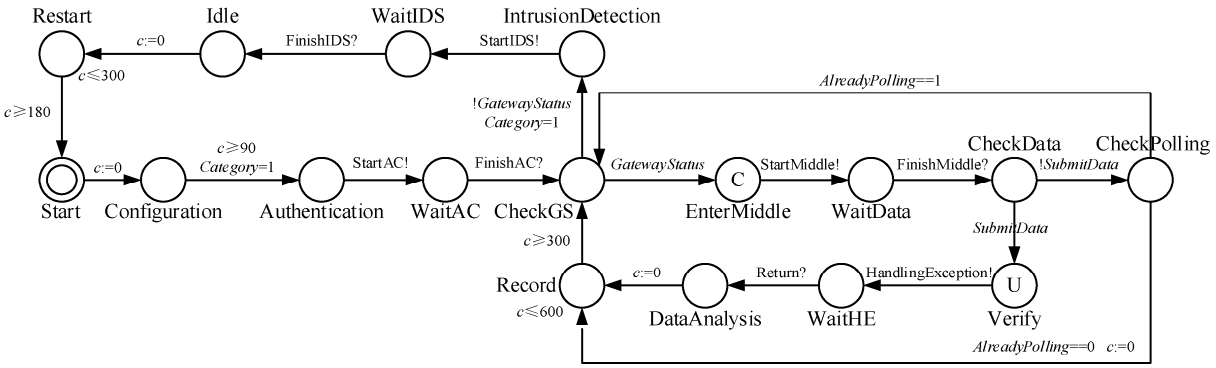

图 4　顶层主模块模型（Top）

true, WaitHE), (DataAnalysis, ∅, ∅, $c:=0$, Record), (WaitHE, ∅, Return?, ∅, DataAnalysis), (Record, $c\geqslant 300$, ∅, ∅, CheckGS)}

中间层及底层各模块形式化模型依据顶层主模块模型，结合图例较容易得出，限于篇幅不再详述。

3.3 层次化建模

根据层次时间自动机的定义，首先建立顶层主模块模型，如图 4 所示。

物联网网关从 Start 开启运行，读取配置信息并进行网关身份认证，通过通道 StartAC 调用底层统一认证服务进行安全认证，认证结束返回网关认证状态 *GatewayStatus*。如果 *GatewayStatus*= false，进入 IntrusionDetection 状态，进行入侵检测，然后在等待一段时间后重启物联网网关，重新启动网关安全系统，这里对重启网关的时间约束为 180~300 个时间单位；如果 *GatewayStatus*= true，进入 EnterMiddle 状态，通过通道 StartMiddle 进入中间层轮询模块，待中间层数据返回后，判断是否有监控信息提交至顶层主模块。如果 *SubmitData*= false，进一步检查当前轮询周期是否已经完成，若完成则直接进入下一周期，反之，则记录轮询失败信息后进入下一周期；如果 *SubmitData*= true，进入 Verify 状态，通过通道 HandingException 处理数据异常，最终记录有效的监控信息，然后进入下一轮询周期。这里对信息记录 Record 状态同样设置了时间约束，以确保安全系统的周期性运转，时间约束为 300~600 个时间单位。

对于中间层轮询模块，通过通道 StartMiddle 开启轮询，并由通道 FinishMiddle 返回顶层主模块。CheckCategory 状态控制轮询逻辑的终端是感知终端还是执行终端，两者有不同的流程处理。所建立的中间层轮询模块模型如图 5 所示。

当 *Category*=2 时，对感知终端进行轮询；当 *Category*=3 时，对执行终端进行轮询。在 2 个轮询流程中，根据不同的需求通过同步通道调用底层安全服务，具体过程可由状态位置、同步通道、变量的含义解读，在此不再赘述。特别地，在等待计时阶段和设备保持运行状态阶段也添加了时间约束，例如，执行终端需在 5 个时间单位内返回运行状态，持续运行需保持 25 个时间单位以上，以此来保证安全需求的新鲜性。

顶层主模块模型和中间层轮询模块模型是物

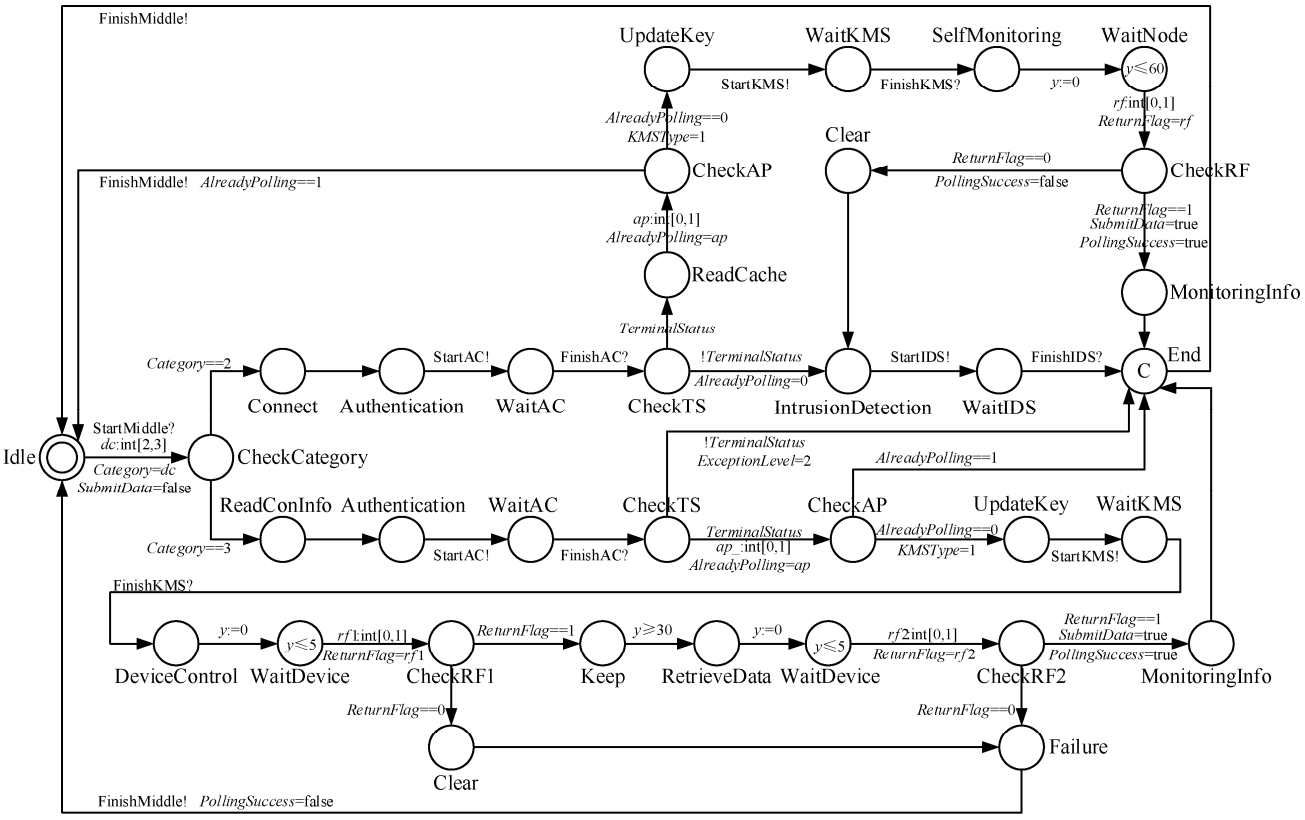

图 5 中间层轮询模块模型（Middle）

联网网关安全系统的通用框架，其安全性的实现最终依赖于底层的安全服务模块，因此，需要完善底层安全服务模块的模型构建。图 3 中给出了底层各个安全服务子模块的常用算法或协议，用户可根据实际场景和需要选择适合的算法协议，然后在此框架下进行相应的建模分析，从而指导网关安全系统在网关中间件平台的设计与实现。

为了验证所设计的物联网网关安全系统是否满足安全需求，拟选取基于时间标签的 AES 密码算法[20]为核心，建立密钥管理、身份认证、入侵检测及异常处理模型。需要说明的是，加、解密是密钥管理系统常用的逻辑流程，为使结构更加清晰，分别对加、解密进行了单独建模。底层安全服务模块建模如图 6~图 11 所示。

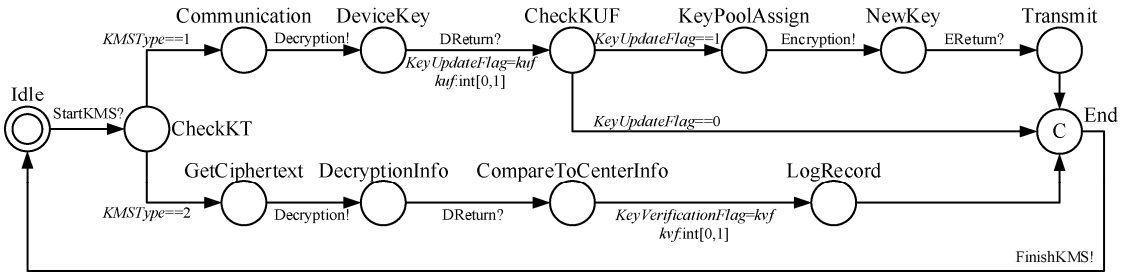

图 6　密钥管理系统模型（KMS）

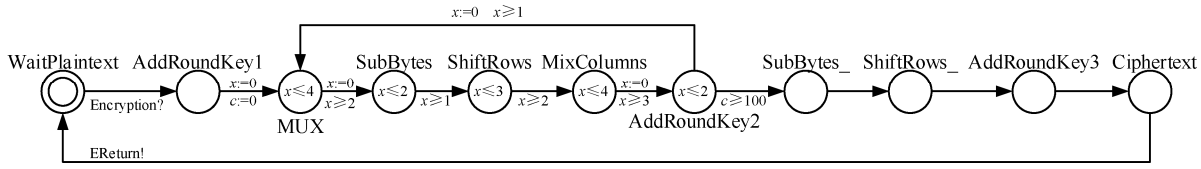

图 7　AES 算法加密模型（AESEncryption）

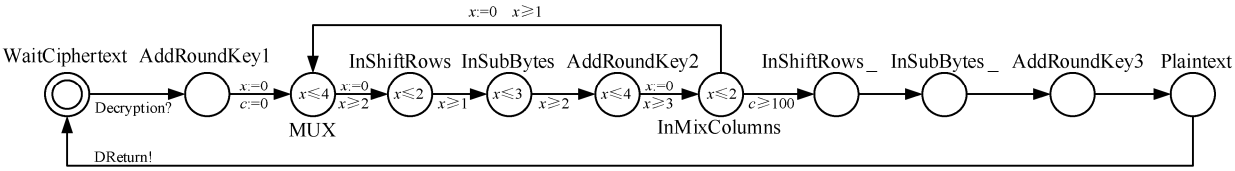

图 8　AES 算法解密模型（AESDecryption）

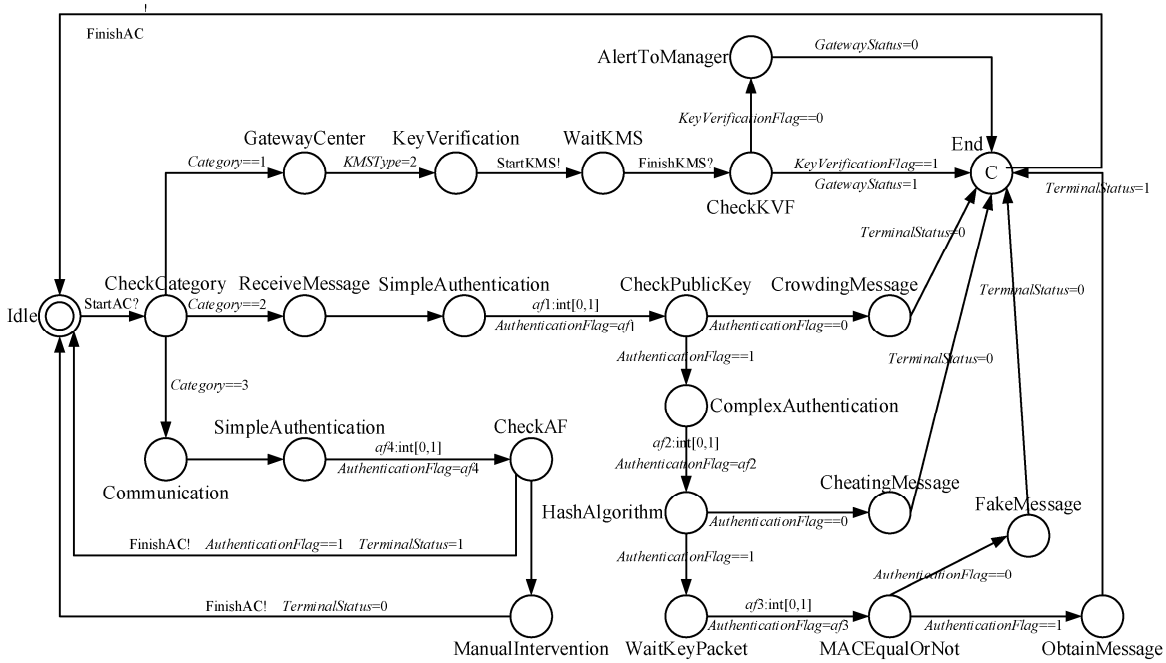

图 9　认证中心模型（AC）

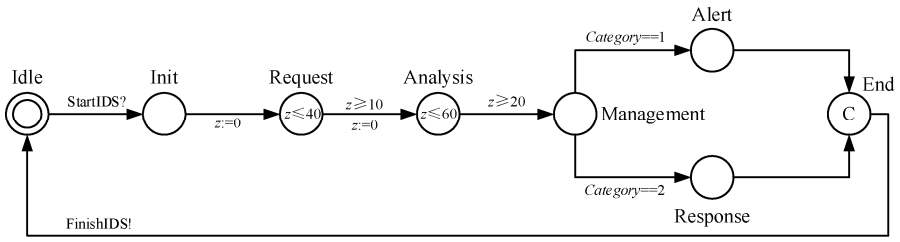

图 10　入侵检测系统模型（IDS）

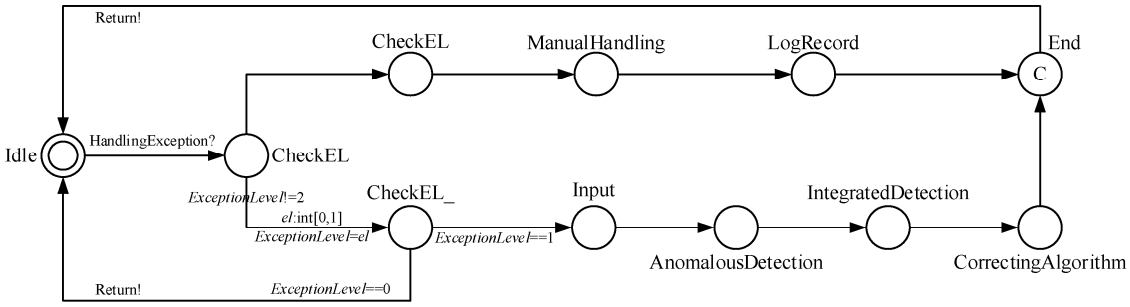

图 11　异常处理模型（Exception）

简要对密钥管理系统模型和基于时间标签的 AES 密码算法进行介绍，其他安全服务模型限于篇幅不再赘述。密钥管理系统首先检测 *KMSType*，如果 *KMSType*=1，则更新密钥，与终端通信获取终端密钥信息进行解密校验，判断是否需要更新，若需要更新则通过数据中心密钥池分配新的密钥，然后加密传送回终端；如果 *KMSType*=2，则验证密钥，将终端传来的密文进行解密，然后提交数据中心比对处理，最后记录数据中心反馈的验证信息。

AES 密码算法包括加密过程、解密过程和密钥扩展过程。其加密过程共 10 轮（或 12 轮、14 轮），前 9 轮（或前 11 轮、前 13 轮）由字节代换、行移位、列混合和加轮密钥等 4 种变换迭代完成，最后一轮没有列混合变换；解密过程与加密过程的轮数一致，并且前若干轮变换是加密过程的逆变换，依次是逆字节代换、逆行移位、逆列混合和加轮密钥变换，最后一轮没有逆列混合变换。基于时间标签的 AES 密码算法是在密钥扩展阶段引入时间标签，使轮密钥可随时间的变化进行动态更新，进而实现密文的变化，可以更有效地保证机密信息的安全性。因此，在建模过程中对加、解密模型的部分状态位置和边界添加了时间约束，以体现时间标签属性。

4　网关安全系统的形式化验证

可以对建立好的物联网网关安全系统的层次时间自动机模型使用模型检测工具 UPPAAL 进行验证，能够有效发现模型的错误，并验证模型的安全性质是否满足。

4.1　UPPAAL 工具简介

UPPAAL[21] 是瑞典 Uppsala 大学和丹麦 Aalborg 大学于 1995 年联合发布的基于时间自动机的自动化验证工具，其名字的由来是 2 所学校名称的前 3 个字母组合。UPPAAL 的操作界面包含编辑器（editor）、模拟器（simulator）、验证器（verifier）3 个部分。编辑器用于对要分析的问题进行建模和编辑，是一个图形化交互界面，可进行自定义及编程；模拟器用于模拟模型的执行过程，可选择步进执行或随机执行，工具将生成时序图和消息控制序列，以帮助设计者发现错误原因和路径；验证器用于验证给定性质是否满足，在每个性质验证结束后给出验证结果、验证时间和内存消耗，性质的表示使用巴科斯范式（BNF, Backus-Naur form）描述。

4.2　安全需求性质的验证

本文通过编辑器建立物联网安全系统模型，可以在模拟器模拟各层次的交互情况。时序图详细展示了各层次对象间的交互情况及各时间自动机模型的执行情况，消息控制序列以图文形式展示了各对象的运行流程和通信状态，它们对于模型的分析和调试有极大帮助。

模拟器的模拟运行，其择路条件随机，不一定能够完全遍历模型状态，因此，需要使用验证

器进行全面验证。2.1 节提到，物联网网关的安全需求需要满足机密性、可用性、真实性、顽健性、完整性、新鲜性 6 个性质，使用 BNF 语法对上述性质进行公式化表示，然后利用验证器进行验证。

1) 机密性验证

A[] AC.AlertToManager imply *KeyVerificationFlag*==0

加密信息通过网关时，若密钥验证失败，则安全监控逻辑进行报警，拒绝消息继续传输。

2) 可用性验证

在顶层模型，检测网关认证状态可达，可确保网关的合法身份和轮询周期的不断进行；中间层及底层各模型入口状态可达，可确保为用户提供相应服务。待验证性质表示如下。

E<> Top.CheckGS

E<> Top.EnterMiddle imply Middle.CheckCategory

E<> Middle.UpdateKey imply KMS.CheckKT

E<> Top.Authentication imply AC.CheckCategory

E<> Middle.IntrusionDetection imply IDS.Init

E<> Top.Verify imply Exception.CheckEL

3) 真实性验证

E<> *TerminalStatus*==1 imply AC.*AuthenticationFlag*==1

在消息认证时，需要同步验证消息来源节点的私钥以认证身份的合法性。如果认证中心的认证成功，则认为终端状态正常，说明源节点是系统内节点，而不是外部伪造的。

4) 顽健性验证

A[] not deadlock

系统不存在死锁，即面对任何情况都有处理路径可执行。

5) 完整性验证

A[] AC.ObtainMessage imply AC.*AuthenticationFlag*==1

消息认证码（MAC, message authentication code）可同时提供基于校验和的数据完整性和基于秘密密钥的数据源完整性。如果接受的消息最终通过 Hash 运算处理后，2 次计算的 *MAC* 值相等，则认为数据未被篡改，解密并获取发送方的信息。

6) 新鲜性验证

整个模型中设置了多处时间约束，目的就是保证消息的时效性。待验证性质表示如下。

A[] Top.Restart imply $c \leqslant 300$

A[] Top.Record imply $c \leqslant 600$

A[] Middle.RetrieveData imply Middle.$y \geqslant 30$

A[] Middle.WaitDevice imply Middle.$y \leqslant 5$

A[] IDS.Analysis imply IDS.$z \leqslant 60$

A[] AESEncryption.MUX imply AESEncryption.$x \leqslant 4$

A[] AESDecryption.InShiftRows_ imply $c \geqslant 100$

UPPAAL 验证器对上述 6 个性质的全部语句逐条进行验证，验证结果如表 5 所示。

表 5　　模型检测结果

性质	验证时间/s	内存消耗/KB	验证结果
机密性	0.034	9 096	满足该性质
可用性	0.001	9 116	满足该性质
真实性	0.001	9 116	满足该性质
顽健性	0.060	9 508	满足该性质
完整性	0.034	9 504	满足该性质
新鲜性	0.062	9 516	满足该性质

验证结果表明，所有性质均通过验证，所设计的物联网安全系统满足机密性、可用性、真实性、顽健性、完整性、新鲜性等安全需求。

5　结束语

物联网作为新一代信息技术的重要组成部分，安全问题应当得到足够重视。物联网感知层直面真实环境，其底层感知和执行设备常常面临各类安全威胁。物联网网关负责连接感知层与网络层，可弥补感知层能力的不足，避免安全问题的进一步扩散。目前，对物联网网关体系结构的研究主要解决了基本功能的实现，安全策略涉及不多；对物联网网关安全措施的研究一般都有实际应用背景，可借鉴性与通用性不强。

基于上述分析，结合现有的密钥管理、身份认证、入侵检测等安全技术，设计了一个通用的物联网网关安全系统，可在网关中间件平台部署。利用时间自动机对系统 3 个层次进行形式化建模，并使用模型验证工具 UPPAAL 进行性质验证，结果表明

网关安全系统满足机密性、可用性、真实性、顽健性、完整性、新鲜性等安全性质。物联网网关安全系统还可以根据实际需要调整底层安全协议或算法，然后重新进行建模分析，有助于发现设计漏洞，辅助网关的设计和实现。

下一步研究工作的重点有 2 个方面。

1) 进一步研究其他安全协议或算法的建模方法，以便有效嵌入物联网网关安全系统，从而提升系统的普适性。

2) 结合物联网网关的硬件设备及中间件技术，在实际环境中具体实现物联网网关安全系统。

参考文献：

[1] 王良民, 熊书明. 物联网工程概论[M]. 北京: 清华大学出版社, 2011:45-52.
WANG L M, XIONG S M. The introduction of IoT engineering[M]. Beijing: Tsinghua University Press, 2011:45-52.

[2] 钱志鸿, 王义君. 物联网技术与应用研究[J]. 电子学报, 2012, 40(5):1023-1029.
QIAN Z H, WANG Y J. IoT technology and application[J]. Acta Electronica Sinica, 2012, 40(5):1023-1029.

[3] MORABITO R, BEIJAR N. A framework based on SDN and containers for dynamic service chains on IoT gateways[C]//The Workshop on Hot Topics in Container Networking and Networked Systems. 2017:42-47.

[4] SATHYADEVAN S, VEJESH V, DOSS R, et al. Portguard an authentication tool for securing ports in an IoT gateway[C]//IEEE International Conference on Pervasive Computing and Communications Workshops. 2017:624-629.

[5] SCHRICKTE L F, MONTEZ C B, OLIVEIRA R S D, et al. Design and implementation of a 6LoWPAN gateway for wireless sensor networks integration with the internet of things[J]. International Journal of Embedded Systems, 2016, 8(5/6):380-390.

[6] 陈琦, 韩冰, 秦伟俊, 等. 基于 Zigbee/GPRS 物联网网关系统的设计与实现[J]. 计算机研究与发展, 2011, 48(s2):367-372.
CHEN Q, HAN B, QIN W J, et al. Design and implementation of the IoT gateway based on Zigbee/GPRS protocol[J]. Journal of Computer Research and Development, 2011, 48(s2):367-372.

[7] ZHANG L, ALHARBE N R, ATKINS A S. A self-adaptive distributed decision support model for Internet of things applications[J]. Transactions of the Institute of Measurement and Control, 2017, 39(4): 404-419.

[8] 罗俊海, 周应宾, 邓霄博. 物联网网关系统设计[J]. 电信科学, 2011, 27(2):105-110.
LUO J H, ZHOU Y B, DENG X B. Design for gateway system in Internet of things[J]. Telecommunications Science, 2011, 27(2): 105-110.

[9] CHEN H C, YOU I, WENG C E, et al. A security gateway application for end-to-end M2M communications[J]. Computer Standards & Interfaces, 2016, 44(C):85-93.

[10] MIN D, XIAO Z, SHENG B, et al. Design and implementation of heterogeneous IoT gateway based on dynamic priority scheduling algorithm[J]. Transactions of the Institute of Measurement and Control, 2014, 36(7):924-931.

[11] CONDRY M W, NELSON C B. Using smart edge IoT devices for safer, rapid response with industry IoT control operations[J]. Proceedings of the IEEE, 2016, 104(5):938-946.

[12] LI F, WAN Z, XIONG X, et al. Research on sensor-gateway-terminal security mechanism of smart home based on IoT[C]//IoT Workshop 2012, CCIS 312. 2012: 415-422.

[13] 石希, 陈震, 汪东升, 等. 物联网汇聚安全网关关键技术研究[J]. 信息网络安全, 2012(6):85-89.
SHI X, CHEN Z, WANG D S, et al. A research of the key technology of the aggregative security gateway of Internet of things[J]. Netinfo Security, 2012(6):85-89.

[14] SERDAROGLU K C, BAYDERE S. WiSEGATE: wireless sensor network gateway framework for Internet of things[J]. Wireless Networks, 2015, 22(5):1-17.

[15] 罗娟, 顾传力, 李仁发. 基于角色的无线传感网络中间件研究[J]. 通信学报, 2011, 32(1):79-86.
LUO J, GU C L, LI R F. Researches on role-based middleware in wireless sensor networks[J]. Journal on Communications, 2011, 32(1):79-86.

[16] 杨光, 耿贵宁, 都婧, 等. 物联网安全威胁与措施[J]. 清华大学学报(自然科学版), 2011, 51(10):1335-1340.
YANG G, GENG G N, DU J, et al. Security threats and measures for the Internet of things[J]. Journal of Tsinghua University (Science and Technology), 2011, 51(10):1335-1340.

[17] 王浩, 郑武, 谢昊飞, 等. 物联网安全技术[M]. 北京: 人民邮电出版社, 2016:5-17.
WANG H, ZHENG W, XIE H F, et al. IoT security technology[M]. Beijing: Posts & Telecom Press, 2016:5-17.

[18] ALUR R, DILL D L. A theory of timed automata[J]. Theoretical Computer Science, 1994, 126(2):183-235.

[19] DAVID A, OLIVER M M. From HUPPAAL to UPPAAL: a translation from hierarchical timed automata to flat timed automata[R]. BRICS Report Series RS-01-11, Department of Computer Science, University of Aarhus, 2001.

[20] YIN A, WANG S. A novel encryption scheme based on timestamp in gigabit ethernet passive optical network using AES-128[J]. Optik, 2014, 125(3):1361-1365.

[21] BEHRMANN G, DAVID A, LARSEN K G. A tutorial on UPPAAL[M]//Formal Methods for the Design of Real-Time Systems. Springer Berlin Heidelberg, 2004:200-236.

[作者简介]

王国卿（1989-），男，山东临沂人，郑州大学博士生，主要研究方向为模型检测、形式化分析、物联网安全等。

庄雷（1963-），女，山东日照人，博士，郑州大学教授、博士生导师，主要研究方向为模型检测、未来网络架构、网络虚拟化等。

王瑞民（1974-），男，河南安阳人，博士，郑州大学副教授，主要研究方向为密码学、信息安全、物联网安全等。

宋玉（1969-），男，河南邓州人，郑州大学副教授，主要研究方向为数据挖掘、物联网体系结构、人工智能等。

张坤丽（1977-），女，河南巩义人，郑州大学讲师，主要研究方向为人工智能、自然语言处理等。