

异构传感网密钥管理协议分析模型与性能评测*

马春光^{1,2,3}, 钟晓睿¹⁺, 王九如¹

¹(哈尔滨工程大学 计算机科学与技术学院, 黑龙江 哈尔滨 150001)

²(网络与交换技术国家重点实验室(北京邮电大学), 北京 100876)

³(哈尔滨工程大学 国家保密学院, 黑龙江 哈尔滨 150001)

Analysis Model of Key Management Protocols and Performance Evaluation for Heterogeneous Sensor Networks

MA Chun-Guang^{1,2,3}, ZHONG Xiao-Rui¹⁺, WANG Jiu-Ru¹

¹(College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)

²(State key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications), Beijing 100876, China)

³(College of National Secrecy, Harbin Engineering University, Harbin 150001, China)

+ Corresponding author: E-mail: zhongxiaorui@hrbeu.edu.cn

Ma CG, Zhong XR, Wang JR. Analysis model of key management protocols and performance evaluation for heterogeneous sensor networks. *Journal of Software*, 2012, 23(10): 2817-2832 (in Chinese). <http://www.jos.org.cn/1000-9825/4193.htm>

Abstract: The traditional ways of estimating key management schemes, which only test one, or a few communications, are not comprehensive. With the increase of heterogeneous strength, static analysis will become more and more complex, and finally lose its referential value. First, a key management framework in this paper is summarized. According to the strategy layer of this framework and based on the classical cluster model of the entity layer, a key management logic (KML) model is proposed. This KML model involving colored hierarchical Petri net and generalized stochastic Petri net extended the energy place. Next, by making the Top layer key management strategy and Button layer energy consumption model as the core, a KML model for key management is built to support and represent heterogeneity with tokens to help the analysis and decisions. Finally, the performance analysis methods are discussed, including energy consumption, latency and lifetime. The experimental results show that KML model is effective for analyzing the short-term and long-term performance and can help scheme designers to improve their schemes by discovering the bottlenecks and hidden perils.

Key words: key management; model; energy consumption analysis; Petri net

摘要: 传统的以单次或几组通信过程为目标进行的密钥管理性能分析的方法具有片面性,且随着网络异构程度的增加将越发复杂,分析结果的参考价值也相对较低.针对该问题,首先概括了异构传感网密钥管理框架,细化了其策略层逻辑结构,并结合 Petri 网理论,通过对库所进行能耗扩展,提出分簇结构下的密钥管理逻辑(key management

* 基金项目: 国家自然科学基金(61073042); 北京邮电大学网络与交换技术国家重点实验室开放课题(SKLNST-2009-1-10)

收稿时间: 2011-06-15; 定稿时间: 2012-02-15

logic,简称KML)模型.随后,以带吸收壁的Top层密钥管理策略和Button层能耗模型为核心,建立了密钥管理协议的KML模型,该模型支持多种异构性以token的形式参与分析和决策.最后,以低能耗协议为例,讨论了所提模型的能耗、时延和寿命的分析方法.实验结果表明,KML模型能够有效地对协议进行仿真和分析,提供了对协议的短期性能和长期性能的合理估测,从而帮助设计者发现协议瓶颈和性能隐患,为协议改进提供参考.

关键词: 密钥管理;模型;能耗分析;Petri网

中图法分类号: TP393 文献标识码: A

与其他许多网络技术一样,无线传感网的安全性主要由密码技术来保障.作为密码技术不可分割的一部分,传感网密钥管理方案也逐渐受到社会各界的广泛关注,但对于其性能的分析一直是学术界研究的热点与难点.在协议能耗分析方面,文献[1]分析了信息收发过程中节点所处状态,并根据状态的不同,将传感网节点通信过程的能耗进行分步建模.该能量模型在后续研究中被频繁引用.Arvindpal等人^[2]在8bit的微控制平台上对基于公钥的无线传感网认证协议和密钥交换协议的能耗情况进行了实际测试和分析,并证明了公钥算法在8bit能量受限节点上的可用性.2010年,基于能耗的虚加密和密钥方案被提了出来^[3],该方案以通信次数作为能耗的衡量标准,以减少通信次数的方式来减少密钥更新代价.最近,文献[4]也对密钥管理技术进行了分类,并按照协议操作的类别来计算协议的总能量开销.在协议时延分析方面,文献[5]分析对比了PMIPv6和其他一些已经存在的IP移动管理协议的交付时延,这对传感网密钥管理协议的时延分析具有很好的借鉴作用.从国内外的研究现状来看,安全协议的性能分析还处在计算单次或几次通信开销的阶段,这对于同构对等传感网来说是可行且有效的.但是随着异构传感网以其明显提高网络性能的优势,已经逐步替代了同构传感网,成为了更贴近实际的传感网经典模型^[6].而在异构传感网中,节点的能力差异、职能差异,使得不同节点单次能耗量不同、能耗速率不同、消耗同样能量以后节点的残留执行能力也不同,这就意味着简单的从能耗次数的角度进行协议能耗和寿命分析的评估方法对异构传感网不再适用.与此同时,这种计算一次通信或一组通信能耗的方式虽然能够反映协议的短期静态性能,却无法衡量协议的长期动态性能,对异构性的适应能力也极其薄弱.

2010年开始,我们利用Petri网来对密钥管理协议的更新开销进行仿真分析^[7],为本文奠定了知识基础.为了适应异构传感网中多类型节点在网络中各自分工合作的情况,本文首先提出了异构传感网密钥管理框架,明确界定所研究问题的思路、范围、内容和作用.随后,基于有色随机Petri网提出了层级密钥管理逻辑(hierarchical key management logic,简称HKML)形式化模型,并根据第1节所提框架的核心策略模型建立起密钥管理的Top层KML模型,依据文献[1]的能耗模型建立Button层KML模型.同时,将框架的物理层所限定的不同类型传感节点替换为HKML网模型的token.第3节以低能耗密钥管理协议为例,对所提HKML网模型进行实例化.实例化后的HKML网模型可以利用第4节所介绍的方法进行包括能耗、时延、网络寿命等在内的综合性能分析.第5节展示相关性能分析的实验结果.第6节是对全文的总结与展望.

1 异构传感网密钥管理框架

密钥管理框架的研究一直是学术界关注的重点,近年来最具代表性的密钥管理框架由文献[8,9]提出.前者提出的框架主要针对异构传感网中的分布式密钥管理方案,后者则提出了包含周期认证机制和新注册机制的密钥管理框架.与这些框架不同,本文提出的异构传感网密钥管理框架从整体上融合了各种异构性因素(如节点能力异构、链路异构和网络协议异构等),对HSN(heterogeneous sensor network)密钥管理机制的结构特征进行规范的细粒度刻画,如图1所示.密钥管理框架的3层结构,可形式化为一个七元组:

$$KMM = \langle E, S, P; K, M; f_{es}, g_{sp} \rangle,$$

其中, E 是实体层; S 是策略层; P 是评价层; K 是整个网络系统的知识集,包括实现密钥管理策略的所有方法; M 是指标集; f_{es} 和 g_{sp} 分别是实体层到策略层和从策略层到评价层的层间映射.密钥管理框架的3层结构是一个交互模型:其实体层的构建将限制策略层密钥管理解决方案的提出;反过来,策略层密钥管理解决方案的设计,又可能为实体层引入新的实体元素,构建更完善的物理网络.同样地,策略层解决方案的侧重点不同,评价层设定

的分析指标和方法也会相应改变;而评价层的评测结果,将进一步优化策略层的方案设计;三者从下到上提供依据,起支撑作用;从上到下提供反馈,起调控作用.各层相辅相成,共同组成 HSN 密钥管理框架结构.

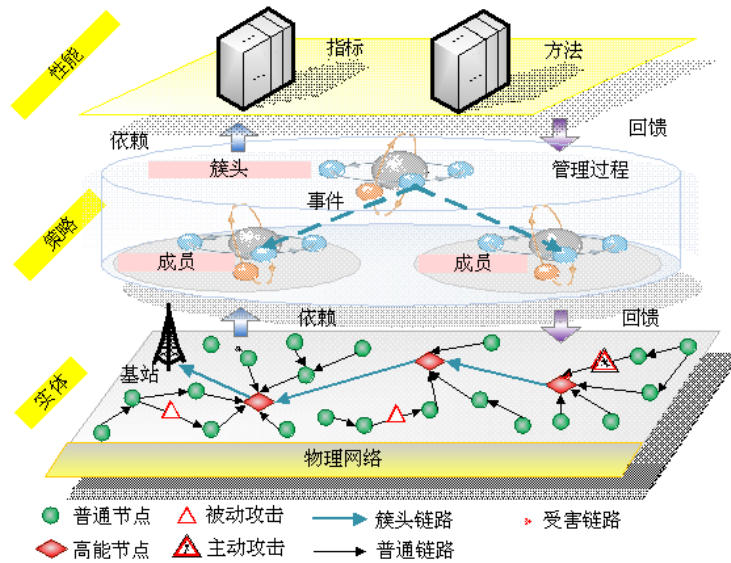


Fig.1 HSN key management framework

图 1 HSN 密钥管理框架

(1) 实体层

网络实体层 E 是对应用密钥管理机制的异构传感网中物理网络实体和网络环境的客观描述,是整个密钥管理框架的物理基础.由于异构性既是传感网的本质属性,又可以人为地、有目的地添加到网络中,因此,网络通常形成典型的“基站-簇头-簇成员(BCM)”的 3 层拓扑结构.能力较弱的节点作为簇成员节点,安全级别最低,负责感知任务,并将感知信息在规定的时间内传送给能力较高的簇头节点.簇头节点对簇内节点进行管理,对信息作进一步的检验、融合等处理,并经由簇头链路传递给基站,安全能力高于普通节点.基站是信息的最终处理者和用户,向网络提出感知需求,管理整个网络,并接收评测感知结果,安全级别最高.网络中链路异构、底层协议异构还可能使网络发生局部划分,而使得簇间节点通信完全或不完全独立.同时,在整个网络的运行过程中,既存在不易发现的被动攻击,又存在危害性极强的主动攻击,安全条件恶劣,安全需求迫切.

(2) 策略层

基于实体层所决定的典型分簇物理网络结构,策略层 S 描述了解决各类密钥在簇间和簇内节点间生成、分配和维护等一系列问题的技术流程,为实现密钥管理提供实际的解决方案.策略层的实例化结果为若干密钥管理协议,它们均遵循管理策略所规范的、为授权各方之间实现密钥关系建立和维护所奉行的基本思想,并实现对策略所描述的各个步骤的进一步细化.

图 2 给出了 HSN 密钥管理策略的逻辑模型.密钥管理周期涵盖 6 个过程:密钥产生、密钥存储、密钥分配、密钥使用、密钥撤销和密钥更新.密钥产生是一个密钥从无到有的过程,既包括节点部署前、密钥池中预分配密钥的生成,也包括在节点布撒之后、会话密钥的生成.密钥产生的结果可能有对称密钥,也可能产生非对称密钥.如果称预分配的密钥是静态密钥,网络部署后才动态确立的有固定使用期限的密钥为动态密钥,则在安全链路建立期,会不断地由静态密钥通过密钥共享等方式直接建立动态密钥(直接密钥),或者通过路径密钥等间接方式建立动态密钥(间接密钥).密钥产生阶段所产生的密钥将用于组内通信(组密钥)、簇内成员通信(簇内对密钥)以及簇间通信(簇间对密钥),并受整个密钥管理过程的完全管理.

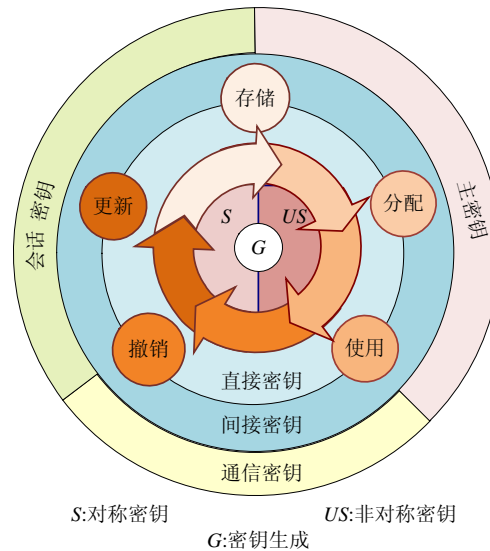


Fig.2 Strategy model for key management

图2 密钥管理策略模型

(3) 评价层

显然,能够适应所有需求的密钥管理协议是不存在的,一项协议通常在某些性能之间寻求多目标平衡,这就需要密钥管理协议进行性能评测,以寻求满足特定需求的适当方案.评价层 P 描述了采用什么方法对密钥管理协议的哪些性能进行评价.评测层严格依赖于策略层与实体层,换句话说,对 HSN 密钥管理的评测实际上是评测特定的密钥管理策略应用于某种实体特性的网络所能达到的某种性能效果.常见的性能评测指标包括能量开销、时间开销、抗毁性、连通性、前后向安全性、可扩展性等.

2 密钥管理策略模型

2.1 密钥管理逻辑

1962年,联邦德国的 Carl Adam Petri^[10]在其博士论文中首次提出了 Petri 网的数学定义,后经 Peterson 等人^[11]的不断研究,逐渐发展成为一套兼具图形与数学理论的形式化分析模型,且善于描述与分析系统的并发同步行为.作为对其描述功能的一种扩充,时间概念被引入到 Petri 网中,由此产生了时间 Petri 网、随机 Petri 网 (SPN)以及广义随机 Petri 网(GSPN).随着应用需求和复杂度的增加,Petri 网已经从最初的 P/T 系统逐渐演化为许多高级 Petri 网系统,加强了其模型描述和分析能力.ZENIE^[12]在 1985 年为随机 Petri 网的 token 添加了不同的颜色,提出了有色随机 Petri 网(colored stochastic Petri net,简称 CSPN),其库所、变迁和弧都受到了颜色集的约束,因此可以看作是一种语义受限的随机高级 Petri 网^[13].类似地,融入了 token 颜色集的广义随机高级 Petri 网^[14]也逐渐登陆到历史的舞台上.国内也有林闯^[15]、吴哲辉等人一直在研究 Petri 网理论及其应用.发展至今, Petri 网理论不仅可以更准确、形象地对网络异构元素和密钥管理行为进行形式化描述,更能有效地压缩模型规模,提供合理的模型性能量化分析,非常适合具有异构特性的传感网动态行为建模.为了评测密钥管理协议的能耗性能,本文首先结合 CGSPN,给出一些相关定义.

定义 1. 非空有限颜色集 S 上的多重集(multi-set) ms 是一个函数表达式:

$$\sum_{s \in S} m(s) \cdot s \quad (1)$$

其中, $m(s)$ 为有限集 S 中的颜色 s 在多重集 ms 里的重复个数,或称为 s 的重复度. S 上的所有多重集记为 S_{MS} . ms 中所有元素的重复度组成的集合 $\{m(s)|s \in S\}$ 称为多重集 ms 的系数.

密钥管理协议消耗的能量除了电路的固定能耗以外,还有节点信息交换产生的通信能耗.通信能耗在网系统中常常表现为一个与通信距离有关的随机变量.虽然有许多方法可以用来在 Petri 网中表示能量,本文选择将随机能耗、固定能耗加载到变迁中,使其语义更明确、更清晰.

定义 2. 将密钥管理逻辑(key management logic,简称 KML)定义为一个 10 元组:

$$KML=(N,CS,V;D,ND,C,W;M_0,\lambda,r),$$

其中,

- $N=(P,T;F)$ 是一个网^[15,16], $P \cup T \neq \emptyset, P \cap T = \emptyset$, 保证了网的非空二元性.本文定义 $P = P_c \cup P_n$ 且 $P_c \cap P_n = \emptyset$, $T = T_t \cup T_v$ 且 $T_t \cap T_v = \emptyset$, 其中, P_c 为消耗库所集, P_n 为普通库所集, T_t 为消耗变迁集, T_v 为控制变迁集. $F \subseteq (P \times T) \cup (T \times P)$ 是库所与变迁之间的有向流关系;
- $CS = \{c_1, c_2, \dots, c_n\}$ 是有限非空的颜色集^[16];
- $V = \{v_1, v_2, \dots, v_n\}$ 是有限变量集合;
- $D: V \rightarrow CS$ 是变量的色彩实例化函数, 返回变量绑定的颜色值;
- $ND: F \rightarrow (P \times T) \cup (T \times P)$ 是弧 F 的节点函数. 规定 ND_P 和 ND_T 分别为其中的库所集和变迁集, 其反函数 ND^{-1} 返回对应节点周围的弧;
- $C: P \cup T \rightarrow CS_{MS}$ 是节点颜色函数, 特别地,

$$C(T) = \bigcup D(\text{Var}(ND^{-1}(t) \cup t)),$$

其中, $\text{Var}(x)$ 表示 x 中的所有变量 v . 即, 任意变迁的颜色函数是其周围弧上的颜色变量和其自身谓词集上变量的绑定;

- $W: F \rightarrow CS_{MS}$ 是流关系上的损益函数, 它规定了每次流的形成必须消耗或产生的 token 类型和数目的限制. 它既可以是一个多重颜色集, 也可以是映射到某个多重颜色集的分段函数. 满足

$$\text{Type}(\text{Var}(W)) \subseteq CS.$$

- M_0 是网络初始状态, 为一个 n 元有序向量, 表示网中全部 n 个库所的颜色分布情况;
- $\lambda = \{(\lambda_t^f, \lambda_t^e, lvl) \mid t \in T\}$ 是消耗变迁 t 的属性集合, 3 个参数分别表示点火速率、能耗速率和变迁触发的优先级. 点火速率限定了单位时间内变迁能够触发的次数, 单位为次/单位时间. 能耗速率则限定了变迁触发 1 次状态转换需要消耗的能量, 单位为焦耳/次. 根据耗能方式的不同, 能耗速率可以细分为固定能耗和随机能耗两种, 分别对应传感器节点的电路能耗和放大器能耗. 若 $\exists t_i, t_j \in T, t_i.lvl = i, t_j.lvl = j, i < j$, 则称 t_i 的优先级高于 t_j 级, 记为 $t_i.lvl > t_j.lvl$;
- r 是消耗库所的属性. 在 KML 中, 任意两个状态之间的转换都是瞬间发生的, 变迁的速率仅刻画变迁发生的频率. 这就意味着, 能量的消耗既有状态瞬间变换的变迁消耗 λ_t^e , 又可能存在因为驻留在某些状态中而产生的驻留能耗. 后者定义为特定状态下(库所中)单位驻留时间内的能耗量, 即 r .

复杂系统的模型存在大量的图元和限制条件, 平面建模复杂度大, 且容易出错. 此时, 对大规模的 KML 进行分层是一种有效的化简手段. 基于 CPN 的层次化理论^[14], 本文给出融合库所的定义.

定义 3. 若 M 为从 P 映射到非负整数集 N^* 的标识函数, 对 $FPS \subseteq P, \forall p_i \in FPS, p_j \in \{FPS - p_i\}$, 有

$$[C(p_i) = C(p_j)] \wedge [M(p_i) = M(p_j)] \wedge M(p_i)[t]M'(p_i) \Rightarrow M(p_j)[t]M'(p_j) \wedge [C'(p_i) = C'(p_j)] \wedge [M'(p_i) = M'(p_j)],$$

则称 FPG 为融合库所组, 其中的每个元素都是一个融合库所 FP . 由融合库所组成的集合称为融合库所集 FPS . 显然, FPG 中的所有融合库所在整个网络运行过程中, 始终保持行为一致, 而 FPS 则不然.

定义 4. 层级密钥管理逻辑 HKML 是以分页的方式, 按照不同的层次级别组合多级逻辑层的密钥管理逻辑网. 其定义如下:

$$HKML = \{PG; TP, IO\},$$

其中,

- $PG = KML \cup RTS \cup FPS$ 是页面集, 每个层级页面至少为一个 KML 网, 可能含有一个融合库所集 FPS 以及替换变迁 RTS ;

- RTS 是替换变迁集合,一个替换变迁 RT 可以由一个页面代替,且称 RT 所在页面为父页面(super),替换 RT 的页面为子页面(sub);
- $FPS=(P_{Socket} \times P_{Port}) \cup P_{fusion}$ 是融合库所集,属于同一个融合库所集的库所始终有相同的静态属性和动态行为.其中, P_{fusion} 是同一个页面上的融合库所集; $(P_{Socket} \times P_{Port})$ 是不在同一页面上但同组的融合库所组成的融合库所集,在父页面的融合库所称为 socket 库所,在子页面的融合库所称为 port 库所;
- $TP:RT \rightarrow PG$ 是从替换变迁到替换页面的映射函数,它决定了两个页面的父子关系,且

$$\forall p_{socket} \in \bullet RT, \exists p_{port} \in TP(RT). P \text{ s.t. } (p_{socket}, p_{port}) \in FPS;$$

- $IO:(P_{Socket} \times P_{Port}) \rightarrow IN|OUT$ 是输入输出函数,限定了一对父子融合库所的数据流向关系,满足

$$\forall t \in RT, [p_{socket} \in \bullet t, IO(p_{socket}, p_{port}) = IN \wedge p_{socket} \xrightarrow{data} p_{port}] \wedge [p_{socket} \in t^{\bullet}, IO(p_{socket}, p_{port}) = OUT \wedge p_{port} \xrightarrow{data} p_{socket}].$$

2.2 基于KML的策略模型形式化

研究表明,HSN 中传感节点的能量主要消耗在信息传递的过程中^[1].因此,将密钥管理策略和节点信息收发过程结合起来,有利于从全局的角度刻画密钥管理策略的能量消耗问题.根据密钥管理策略模型,利用 HKML 网进行密钥管理能耗模型形式化的描述,可以使整个密钥管理能耗过程具有精确的数学定义和逻辑推理能力、预测能力,便于模型检验和性能分析.

2.2.1 Top 层策略模型

图 3 给出的 HSN 密钥管理策略模型,已经从结构上对密钥管理的管理对象及管理流程进行了形象的刻画.根据该模型,密钥管理策略首先需要处理主密钥 MK 如何产生的问题,然后解决通信对密钥 CK 如何建立的问题.如果通信密钥不作为会话密钥,则还需要管理会话密钥 SK 的建立.传感节点的主密钥通常采用预分配的方式预先存储到节点中,其能耗可以忽略不计.在节点布撒后,通过信息交换建立对密钥的过程统称为耗能密钥建立.通过耗能密钥建立,节点就可以利用各自的密钥材料和既定协议对数据通信进行加、解密.与此同时,运行期密钥还面临着密钥撤销和密钥更新两大操作.造成密钥撤销的原因主要有 3 种:节点能量耗尽、可信活节点主动离开和不可信节点被迫撤离^[17].通常,为了保证网络信息的前向安全性和后向安全性,可能存在两种密钥更新方式,分别是周期性更新和触发性更新(由新节点加入操作和旧节点撤销操作触发).因此,从整个密钥管理生命周期的角度来看,可以对密钥管理策略结构模型进行如图 3 所示的形式化建模.

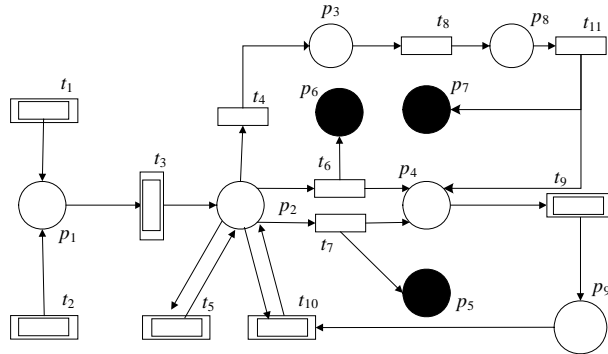


Fig.3 Top layer HKML model

图 3 Top 层 HKML 模型

设网络节点密钥材料(主密钥)已经预加载完成,且刚刚布撒完毕,则:

- (1) 准备态 p_1 中节点按需以速率 $(\lambda_3^f, \lambda_3^e, \lambda_3^c)$ 经过密钥建立事件 t_3 进入正常运行态 p_2 ;

- (2) 正常运行态 p_2 中的节点以 $(\lambda_4^f, 0, lv_4)$ 的速率被捕,进入妥协未检测态 p_3 ,转入步骤(6);
- (3) 正常运行态 p_2 中的节点以 $(\lambda_6^f, 0, lv_6)$ 的速率耗尽能量而失效,进入能竭库所 p_6 ,转入步骤(7);
- (4) 正常运行态 p_2 中的节点以 $(\lambda_7^f, 0, lv_7)$ 的速率可信离开网络,进入可信离开库所 p_5 ,转入步骤(7);
- (5) 正常运行态 p_2 中的节点以 $(\lambda_5^f, \lambda_5^e, lv_5)$ 的速率进行周期性更新,并重新回到正常运行态 p_2 ;
- (6) 入侵检测以 $(\lambda_8^f, 0, lv_8)$ 的速率发现 p_3 中的妥协节点,并将之移入妥协库所 p_7 ,转入步骤(7);
- (7) 系统进入等待撤销态 p_4 ,并以速率 $(\lambda_9^f, \lambda_9^e, lv_9)$ 触发撤销,进入等待密钥更新态,受影响的正常态节点以速率 $(\lambda_{10}^f, \lambda_{10}^e, lv_{10})$ 触发更新,更新后重新回到正常运行态 p_2 ;
- (8) 新普通节点以 $(\lambda_1^f, \lambda_1^e, lv_1)$ 的速率到达网络,进入准备态 p_1 ;
- (9) 新高能节点以 $(\lambda_2^f, \lambda_2^e, lv_2)$ 的速率到达网络,进入准备态 p_1 .

所提模型能够以有色 token 来合理刻画异构元素,例如异构数据、异构信息、异构的传感器节点等.这种优势使得我们所提出的模型能够在不改变其结构的同时,通过更改库所类型、变量类型来模拟不同对象在同一个操作中的不同行为.

2.2.2 Button 层能量模型

传感网需要考虑每个无线电过程的能耗,包括信息传输、接收和空闲状态^[18],在密钥管理过程中体现为收发密钥信息、加解密数据以及执行休眠机制产生能量消耗.而节点用于信息传输、接收的开销要远大于节点存储和计算的开销,成为了节点能耗的主要诱因^[1].为此,本文对密钥管理的信息接收过程和发送过程分别进行建模.从整体层次结构上来看,图 4 所示的收发模型是最底层的能量模型,它向上层网络提供输入、输出接口,在内部实现信息收发模拟,直接反映能量消耗情况.单位信息的传播能耗仅与信息长度和节点硬件性能有关,可以简单地划分为电路能耗和放大器能耗两部分.其中,电路能耗为固定值,放大器能耗却是与传输距离有关的随机变量.

发送方模型如图 4(a)所示,采用信息退避策略控制信息发送,其消耗的能量既包括电路能耗 t_6 ,又包括放大器能耗 t_7 .当发送方 P_1 有信息需要发送时,节点一定处于苏醒态,触发退避策略后探测信道,如果成功,则发送信息;否则,重复退避探测过程,直到信息发送出去或操作超时.

图 4(b)所示为接收方模型,采用节点本身休眠/苏醒机制应对信息接收.信息到达接收方时,接收方节点可能处于苏醒态 P_2 或者休眠态 P_4 ,并分别以 r_2 和 r_4 的驻留能耗速率消耗能量.如果处于休眠态,则需要触发高优先级的即时苏醒变迁 t_3 来唤醒沉睡节点.同样地,如果处于苏醒态,将优先执行 t_1 参与信息接收,并消耗固定能量,而非进行休眠转换 t_2 .

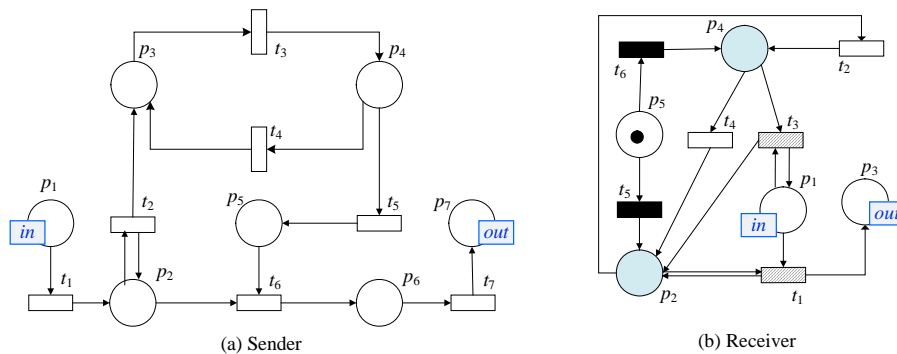


Fig.4 Button layer HKML model

图 4 Button 层 HKML 模型

库所与变迁实际映射意义见表 1 和表 2.

Table 1 Symbols for sender**表 1** 发送方符号说明

库所		变迁		
库所	意义	变迁	意义	速率
p_1	发送者	t_1	传输信息	$(\lambda_1^f, \lambda_1^e, lv_1)$
p_2	信息	t_2	退避一段时间	$(\lambda_2^f, \lambda_2^e, lv_2)$
p_3	退避状态	t_3	探测信道是否繁忙	$(\lambda_3^f, \lambda_3^e, lv_3)$
p_4	尝试状态	t_4	尝试失败	$(\lambda_4^f, 0, lv_4)$
p_5	信道准备状态	t_5	尝试成功	$(\lambda_5^f, 0, lv_5)$
p_6	尝试发送状态	t_6	电路处理	$(\lambda_6^f, \lambda_6^e, lv_6)$
p_7	输出信息	t_7	通过放大器发送数据	$(\lambda_7^f, \lambda_7^e, lv_7)$

Table 2 Symbols for receiver**表 2** 接收方符号说明

库所			变迁		
库所	意义	速率	变迁	意义	速率
p_1	信息库所	—	t_1	接收到信息	$(\lambda_1^f, \lambda_1^e, lv_1)$
p_2	激活状态	r_2	t_2	进入休眠	$(\lambda_2^f, 0, lv_2)$
p_3	接收到的信息	—	t_3	立即激活	$(\lambda_3^f, \lambda_3^e, lv_3)$
p_4	休眠状态	r_4	t_4	激活	$(\lambda_4^f, \lambda_4^e, lv_4)$
p_5	控制库所	—	t_5	进入激活或休眠态	$(\infty, 0, lv_5)$

2.2.3 变迁实施规则

在同一个标识 M 下,可能发生多个变迁同时满足实施条件,其中一个变迁的实施将抑制其他变迁的实施,从而造成变迁之间竞争资源 token 的情况.为了解决此类冲突,就需要为可实施变迁集定义实施规则,使变迁的触发公平、按序进行.假设网络中共有 n 种优先级,令标识 M 下的若干个可实施变迁组成的集合为 H ,其中最高级别的变迁组成的集合记为 TL ,则有:

(1) 若 $\exists t_i \in H \cap T_v \cap TL, \forall t_j \in H, t_j, lv_l < t_i, lv_l \vee t_j \in T$, 则

$$\begin{cases} P_f(M[t_i]) = \sum_{p_i \in t_i} M(p_i) / \sum_{t_k \in TL} \sum_{p_k \in t_k} M(p_k) \\ P_f(M[t_j]) = 0 \end{cases} \quad (2)$$

(2) 若 $\exists t_i \in H \cap T_v \cap TL \wedge \neg(\exists t_v \in H \cap T_v \cap TL), \forall t_j \in H, t_j, lv_l < t_i, lv_l$, 则

$$\begin{cases} P_f(M[t_i]) = \left(\lambda_i^f / \sum_{t_k \in TL} \lambda_k^f \right) \times 0.5 + \left(\sum_{t_k \in TL} \lambda_k^e / \lambda_i^e \right) \times 0.5 \\ P_f(M[t_j]) = 0 \end{cases} \quad (3)$$

根据上述实施规则,只有具有 TL 级别的瞬时变迁才可实施;或者在不存在可实施瞬时变迁的条件下速度最快,能耗最低的延时变迁实施概率最大.

3 模型实例

对 Top 层策略模型的替换变迁进行子页替换,可以实现对具体密钥管理协议的建模和实例化.替换顺序和内容的不同,使得对模型的实例化可以形成一棵以 Top 层页面为根的实例化树,树的叶子节点就是 Button 层收发模型的实例.以 Jolly 等人提出的低能耗密钥管理协议为例^[19],假设 Sensor 节点完全不可信,仅负责信息收集工作;高能节点为网关节点 G ,负责信息收发,所有簇头节点间能够直接通信;命令节点 C 具有无限能量,能够获取入侵检测信息并触发相应的节点撤销事件,且绝对安全.协议定义了密钥建立、密钥撤销、密钥触发性更新和新节点到达这 4 部分操作,则该协议的顶层模型如图 5(a)所示,其中声明、注释等代码全部采用标准 ML 语言,

图形风格样式由 CPN 软件 CPNTool 自动生成.

```

val n=100;
val len_im=9;
val len_m_new=8;
val len_Ask=7;
val len_GjR=6;
val len_GiR=5;
val len_rs=4;
val le_ng=3;
colorset S=with sensor;
colorset G=with gateway;
colorset NODE=union s:S:g:G;
colorset INT=int with 1,...,n;
colorset LENGTH=INT;
colorset Msg=product LENGTH*TYPE;
colorset MSG=Union e+m:Msg;
colorset TYPE=string with a,...,z and 0,...,9;
var lgth: LENGTH;
var msg: MSG;
var t: TYPE;
var sensr: S;
var gtw: G;
    
```

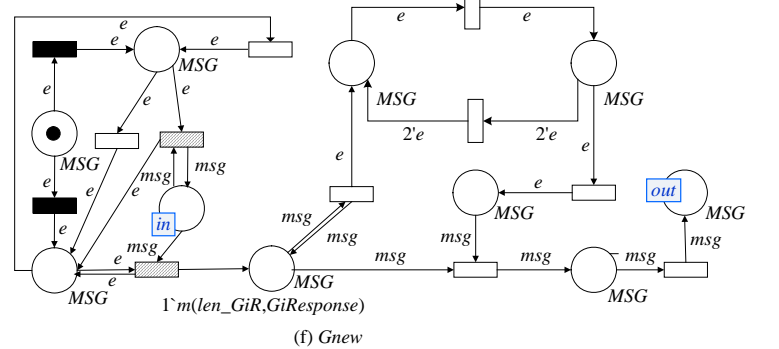
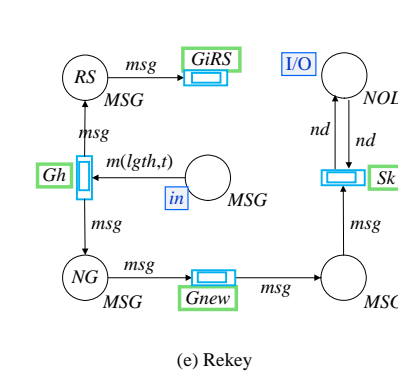
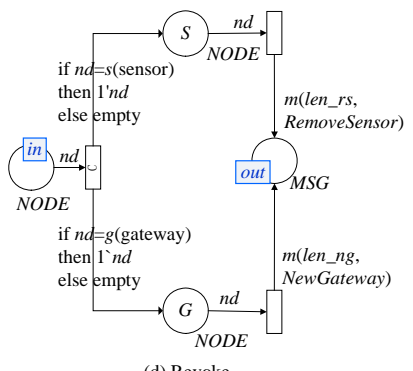
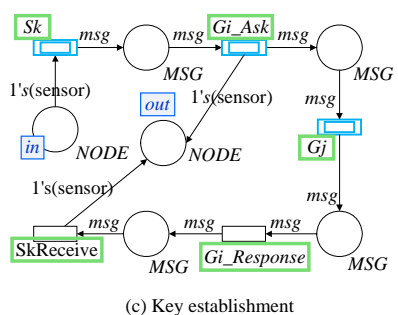
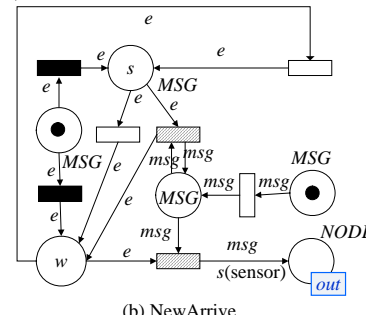
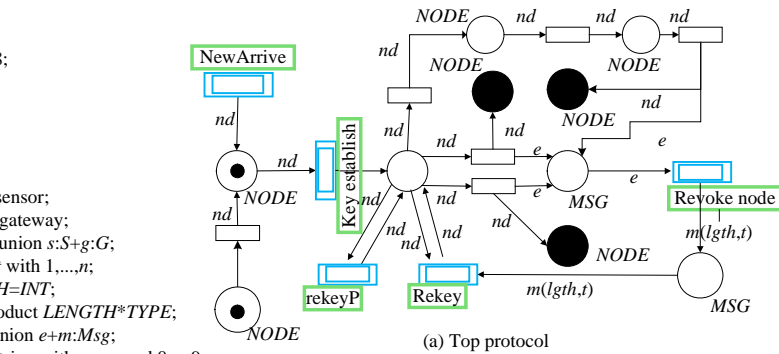


Fig.5 HKML model of low-energy key management protocol

图 5 低能耗密钥管理协议的完整 HKML 图

密钥预分配后,节点布撒到监测区域,首先执行密钥建立操作:传感节点 S 广播 *Hello* 信息,网关 G_j 检测自己是否存在与 S 的共享密钥:若有,则完成密钥建立;否则,向 S 的默认网关索取共享密钥,并告知 S 节点,如图 5(a) 所示.

密钥建立结束后,网络正常运行,当有新节点到达时,由具有无限能量的 C 节点向网中任一节点 G_0 发送其与新节点的共享密钥信息,布撒新传感节点后,重新执行密钥建立过程.因此,Top 层中的新传感节点到达的替换变迁只需对 G_0 节点接收信息的耗能过程进行建模,忽略 C 对网络的作用.而对新网节点的到达,则只需被动等待,而不需要主动建立密钥.如图 5(b)所示.

密钥撤销操作(如图 5(d)所示)和密钥更新操作(如图 5(e)所示)是关联进行的.由于触发的密钥撤销包括了对 S 节点的撤销和对 G 节点的撤销,因此,首先根据传递的信息不同对撤销对象进行分类,记录死亡节点,并向任一 G_h 节点发送更新信息.在更新操作中,如果是撤销网关操作,则 G_h 向新网关 G_{new} 发送通知, G_{new} 再通知 S 更换网关;否则, G_h 向 S 所在网关 G_i 发送通知, G_i 接收信息并作相应处理.

对信息收发替换变迁,如 G_{new} (如图 5(f)所示),都各自建立一个收发模型实例,整个层次模型共有 3 级变迁,瞬时变迁(黑色)为 1 级变迁,优先时间变迁(斜纹填充)为 2 级变迁,普通时间变迁(白色)为 3 级变迁.

应当注意,本文对新节点加入(*new*)、节点撤销(*revoke*)的定义有别于以往.通常来说,新节点加入操作是指节点加入触发对密钥建立,而本文将两者分开,新节点加入操作仅包含新节点以一定速率进入网络,并未密钥建立做准备的过程,并不包含密钥建立过程.同样地,传统的节点撤销操作是指特定节点离开并触发其他节点更新.在本文中,该过程划分为离开节点的判定及移除和触发性更新两个操作,前者为本文意义上的节点撤销.

4 模型求解和量化分析方法

对 HKML 网模型的协议实例化,为基于概率方法的协议性能分析提供了条件.HKML 网是一个连续时间系统,假设每个变迁从可实施到实施的延迟时间是一个连续随机变量 λ ,且服从指数分布,则上述 HKML 网实例可以看作是一个双参数带吸收壁的 GSPN 模型.在不考虑能耗的情况下,所建立的 HKML 模型退化为一个普通的 GSPN,且由标识的可数性和时延变迁实施速率的指数分布所导致的无记忆特性可知,该模型的可达图与一个齐次离散有穷状态、连续时间随机点过程(stochastic point process,简称 SPP)同构^[15,20],且包含 3 种类型的标识(状态):实存态、消失态和吸收态.在下述计算过程中,涉及的状态也都是 SPP 中的各个标识状态.显然,该 SPP 的嵌入马尔可夫链(embedded Markov chain,简称 EMC)的转移概率矩阵容易表示为

$$P = \begin{bmatrix} VV, VT, VS \\ TV, TT, TS \\ 0, 0, E \end{bmatrix} = \begin{bmatrix} Q, R \\ 0, E \end{bmatrix} \quad (4)$$

P 由变迁相应的随机开关分布和实施速率所决定,其中, V, T, S 分别表示消失态、实存态和吸收态, E 是单位矩阵. P 的每一个元素 P_{ij} 表示从状态 i 到状态 j 的一步转移概率,且从 i 状态转移到其他所有状态的概率之和为 1.由于非吸收态最终要进入到吸收态,故 $\lim_{n \rightarrow \infty} Q^n = 0$, 则根据等式(4)容易得到:

$$\lim_{k \rightarrow \infty} P^{(k)} = P^k = \begin{bmatrix} \lim_{k \rightarrow \infty} Q^k, \left(\sum_{m=0}^{\infty} Q^m \right) R \\ 0, E \end{bmatrix} = \begin{bmatrix} 0, (E-Q)^{-1} R \\ 0, E \end{bmatrix} \quad (5)$$

令 $M=(E-Q)^{-1}$ 是一个 $m \times m$ 的矩阵,其元素 m_{ij} 即表示从状态 i 出发进入吸收态之前、经过状态 j 的平均次数^[21].因此,在到达吸收态之前,进入状态 j 的平均次数为 M 矩阵的第 j 列元素之和,进而在状态 j 的驻留时间的均值可以通过等式(6)计算得到,其中, H_j 是在状态 j 下可实施的所有变迁组成的集合.

$$\bar{T}_j = \left(\sum_{t \in H_j} \lambda_t^f \right)^{-1} \times \sum_{i=1}^m m_{ij} \quad (6)$$

4.1 能耗和时延分析

文献[1]已经给出了基于随机距离的单次通信能耗计算公式.由于传输时间与信号传递的距离是成正比关系,因此本文采用公式(7)对具有随机能耗速率的变迁上的能耗速率求解:

$$\lambda_i^e(t \in rsend(T_e)) = c_s + c_{time} \times \left(\frac{1}{\lambda_i^f} \right)^\alpha \quad (7)$$

其中, c_s 是发送 1bit 数据的固定电路能耗, c_{time} 是 1bit 数据已经传输了 1 个单位时间的能耗, α 是传输过程的损益函数.此外,对于接收过程,仅消耗固定接收电路能耗:

$$\lambda_i^e(t \in receive(T_e)) = c_r \quad (8)$$

令耗能库所组成的集合为 ES ,则在进入吸收态 j 之前,耗能库所 s 的能耗量为

$$E_s = \sum_{s \in ES} \sum_{k \in VE(s)} \bar{T}_k \times r_s \quad (9)$$

其中, $VE(s)$ 为耗能库所 s 中 token 数不为 0 的所有状态的集合.在本实例中,耗能库所仅为节点休眠态库所.

抛开库所能耗单独来看变迁能耗.由于 HKML 网模型是层级结构,可以利用文献[22]所验证的等价公式对每个页面内的库所和变迁进行等价速率替换,同时保留瞬时变迁和能耗库所.替换库所可以替换为等价速率变迁或者一个含少量能耗库所或瞬时变迁的简单网,从而整个层级网简化为一个精简状态的有色 Petri 网.注意到,与文献[22]不同,HKML 网具有耗能库所,因此,在父页面替换变迁对子页面进行能耗参数等价时,应当加上等式(9)计算的库所驻留能耗.因此,Top 层所有替换变迁的等价变迁速率都可以通过子页面的速率等价得到.用 $V(s)$ 表示所有在库所 s 标识不为 0 的标识状态集合,则进入吸收态之前,Top 层密钥建立替换变迁的执行次数为

$$F_{establish} = \sum_{j \in V(P_2)} m_{ij} \quad (10)$$

其中, P_2 为 Top 层库所 P_2 .同理,撤销和密钥触发更新替换变迁的执行次数为

$$F_{revoke} = F_{rekey} = \sum_{j \in V(R_3)} m_{ij} \quad (11)$$

其中, P_3 为 Top 层库所 P_3 ,而周期性更新的执行次数则与网络寿命有关:

$$F_{rekeyP} = Life / \lambda_5^f \quad (12)$$

于是有各个过程的宏观总能耗为

$$E = F \times \lambda_i^e \quad (13)$$

类似地,也可以求得各个过程的时延:

$$T = F \times \frac{1}{\lambda_i^f} \quad (14)$$

4.2 寿命分析

从状态 i 出发,到达吸收态前的平均等待时间,就是进入各个非吸收态的次数之和,即矩阵 M 的第 i 行元素之和:

$$T'_i = \sum_{j=0}^m m_{ij} \quad (15)$$

再令 $B=M \times R$,其元素 b_{ij} 表示从状态 i 进入吸收态 j 的概率^[21],则网络寿命可以表示为

$$Life = \sum_{j \in A} \left(T'_{M_0} + \sum_{k \in NA} \frac{1}{r_{kj}} \right) \times b_{i,j} \quad (16)$$

其中, A 是所有吸收态组成的集合, NA 是所有非吸收态组成的集合, r_{kj} 是 R 的元素.

4.3 多色系统的单色处理

由于 token 是具有颜色的,不同的颜色代表不同能力的节点.就密钥管理来说,这些节点的能耗速率和变迁

发生速率可能不同,甚至有较大差异.因此,单纯地按照上述方法对密钥管理的能耗、时延和寿命进行分析是不合理的.本文采用极端单色方法对结果进行最终权衡处理:

- (1) 分别准备不同颜色 token 所对应的能耗和变迁速率参数.本实例中仅有高能节点和低能节点两种颜色,分别称为 a 色和 b 色;
- (2) 构建两个一步转移概率矩阵 A 和 B .对 A 来说,所有唯一色 token 可触发的变迁有与 B 相同的参数,所有不区分颜色的变迁,即 a 色 token 可以经过、 b 色 token 也可以经过的变迁,全部采用 a 色 token 所代表角色的参数; B 则刚好与之相反;
- (3) 按照上述 3 种性能分析方式,分别采用 A 和 B 矩阵进行求解,即在 a 色 token 和 b 色 token 均可触发的变迁上,采用 $A(B)$ 矩阵时仅执行 $a(b)$ 色 token;在具有色彩选择功能的结构中,也仅选择 $a(b)$ 色支路;
- (4) 按照各色 token 的初始比例分析结果进行加权求和,并作为最终结果.

5 分析

5.1 模型本身正确性分析

模型本身的正确性决定了其求解的有效性和可靠性.对于密钥管理策略来说,一定具有以下两个性质:

- (1) 任意一个传感器节点在同一时刻要么不执行任何密钥操作,要么仅执行一项密钥操作;
- (2) 任何节点都必然经历密钥建立,且可能参与密钥更新和撤销.

对于网模型来说,系统有界是 HKML 模型的正确性条件.因此本文规定,密钥管理策略正确性和 HKML 网正确性的实例模型是正确的网模型.

在第 2.2.1 节所给出的密钥管理策略模型的 Top 层模型中,令 $M'_k(p_i)$ 表示状态 M_k 下库所 i 中的 token 集合,则有以下性质成立.

性质 1. $\forall ct \in ColorTokens(node), \neg \exists p_1, p_2 \in P \text{ s.t. } \forall M_k \in M, ct \in M'_k(p_1) \wedge ct \in M'_k(p_2)$.

显而易见,性质 1 是肯定成立的,因为任何一个 token 在任何一个时刻都只可能存在于一个库所,而实例用 token 代表节点,也就是说,任何一个节点在一个时刻只可能在一项操作的某个状态或者位置中,这使得密钥管理策略正确性条件 1 成立.

性质 2. $\forall ct \in ColorTokens(node), \exists M_1, M_2 \in M, ct \in M'_1(p_{Top_1}) \wedge ct \in M'_2(p_{Top_2})$.

由于在 Top 层中,如果有满足条件的 token 处于 P_1 ,则密钥建立变迁将以概率 1 触发.而 P_1 库所是网络准备库所,是初始状态下的非空库所,即,总是可以改变初始状态标识,使得 P_1 以概率 1 触发,于是,性质 2 成立.

性质 3.

$$\begin{aligned} & \forall ct \in ColorTokens(node), \exists M_1[t_{Top_5}]M_2, M_3[t_{Top_9}]M_4, M_5[t_{Top_10}]M_6, \\ & \text{s.t. } [\Pr(ct \in M'_1(\bullet t_{Top_5})) \wedge ct \in M'_2(\bullet t_{Top_5})] > 0 \wedge [\Pr(ct \in M'_3(\bullet t_{Top_9})) \wedge ct \in M'_4(\bullet t_{Top_9})] > 0 \wedge \\ & [\Pr(ct \in M'_5(\bullet t_{Top_10})) \wedge ct \in M'_6(\bullet t_{Top_10})] > 0. \end{aligned}$$

因为竞争变迁的触发概率由变迁触发速率和随机开关决定,所以,当库所 P_2 中的标识数 $M(p_2) > 0$ 时, $\Pr(fire(t_5)) > 0$.由性质 2 可知,Top 层库所 P_2 是所有角色为传感器节点的 token 的必达库所,即 $\Pr(\exists M, M(p_2) > 0) = 1$,因此, $\forall ct \in ColorTokens(node), ct$ 触发 t_5 的概率 $\Pr(t_5) > 0$,触发前后的状态分布是 M_1 和 M_2 .类似地, $\Pr(t_6) > 0, \Pr(t_7) > 0$,使得 $\Pr(ct \in p_4) > 0$.由于 p_4 是变迁 t_9 的唯一前驱,所以 $\Pr(fire(t_9)) = \Pr(ct \in p_4) > 0$.更进一步地,当 t_9 触发, $M(p_{10}) > 0, \Pr(M(p_2) > w(p_2, t_{10})) > 0$,则 $\Pr(fire(t_{10})) > 0$,点火前后的状态分别为 M_5 和 M_6 .于是,性质 3 成立.

性质 2 和性质 3 说明了所建立 HKML 模型满足密钥管理策略正确性条件 2.

有界性是指 HKML 的所有库所的最大 token 数是有限可数的,这使得模型的状态空间有限,进一步保证了第 4 节所提出的对模型进行分析的方法是可行的.HKML 网模型的有界性可以由性质 4 提供.

性质 4.

$$\exists c, c_1 \in N^+, \forall t_1 \in T, M_1, M_2 \in M, M_1[t_1] > M_2, \text{ 有 } \sum_{p \in P} M_0(p) = c, \text{ 且}$$

$$\text{若 } \sum_{p_{a1} \in t_1} M_2(p_{a1}) - \sum_{p_{b1} \in t_1} M_1(p_{b1}) = c_1, \text{ 则 } \exists c_2 \in N^+, t_2 \in T, M_3, M_4 \in M, M_2[t_1, t_k, \dots] > M_3[t_2] > M_4,$$

$$\text{s.t. } \sum_{p_{a2} \in t_2} M_4(p_{a2}) - \sum_{p_{b2} \in t_2} M_3(p_{b2}) = c_2 \geq c_1,$$

其中, $M_i(p)$ 标识状态 i 下库所 p 中的 token 数目.

性质 3 说明, 在 HKML 模型实例中, 初始标识 token 数有限可数, 且在网络模拟过程中不会增加其数目, 而这样的系统一定是有界的. 所建立的 HKML 网模型实例所具有的上述 4 个性质决定了该网系统的逻辑正确性.

5.2 协议性能分析

为了进行能耗、时延和寿命分析, 本文主要根据文献[1]确定非随机参数的取值, 见表 3. 其他服从不同参数指数分布的时延速率和能耗速率, 本文利用 Matlab 统计工具箱计算各自的随机参数值.

Table 3 Energy consumption parameters

表 3 能耗相关参数

参数	值
传输电路能耗 c_s	1.066μJ/bit
接收电路能耗 c_r	0.533μJ/bit
1bit 数据传输单位时间能耗 c_{time}	2.293μJ/bit, s
睡眠能耗 r_s	120 pJ/s
传输的路径损益 α	2.5
密钥建立信息长度	150 bit
更新信息长度	100 bit
撤销信息长度	110 bit
平均更新数目	3% p_{top_2}
周期性更新速率	1 次/天

由 Matlab 产生的 4 组随机参数和表 1 参数对第 3 节实例模型进行仿真, 可以得到相应的可达树及状态转移概率矩阵, 并利用第 4 节所述方法, 得到 4 组参数的寿命分别为 $life_1=9.638E7, life_2=7.231E7, life_3=4.063E7$ 和 $life_4=6.452E7$. 相应的能耗和时延情况如图 6 所示. 图 6(a)~图 6(d) 分别表示在不同随机参数条件下, 执行实例协议模型的单次能耗、进入吸收态之前的能耗、单次时延和进入吸收态之前的时延. 对比图 6(a)和图 6(b)、图 6(c)和图 6(d), 虽然 4 组参数下密钥更新操作的平均单步开销远小于密钥建立操作, 但在进入吸收态之前, 密钥更新的总耗费却由于其频繁地执行而尤为突出.

类似地, 撤销操作虽然在单步能耗和单步时延中开销较低, 但与长期性能相比, 其能耗和时延开销均出现大幅上涨, 且时延开销的上涨幅度更为明显. 由此可见, 单步时延和单步能耗能够直观地反映各步密钥操作的单步能力, 但它并不能决定整个密钥管理策略的性能. 在整个密钥管理生命过程中, 各部分操作被执行次数的不同, 将导致一些小能耗的单步操作最终消耗较多的能量, 成为整个密钥管理策略的瓶颈, 这是由运行环境模拟参数所决定的. 例如, 在本文中, 密钥操作事件所服从的随机分布将决定各个单步事件的发生概率以及单步事件之间的转移概率, 从而影响策略的整体性能. 此外不难发现, 并不是能耗越多就越早进入吸收态, 这是因为能量是为系统进入吸收态做贡献的, 不仅有节点失效, 还有节点妥协和自动离开, 这说明节点的最终寿命主要是由能量消耗情况和协议安全能力共同决定的. 这也是为什么 $life_3$ 组数据总能耗小、总时延小, 却寿命最短的原因.

这种从系统运行开始到结束的全局预测与其他文献中采用的特定时刻或单一步骤的性能分析相比, 更能体现密钥管理方案整体的长期适应能力, 而且能够实现一次建模支持多对象多目标性能分析, 这也是本文选择采用 Petri 网来进行性能分析的初衷和最终目的.

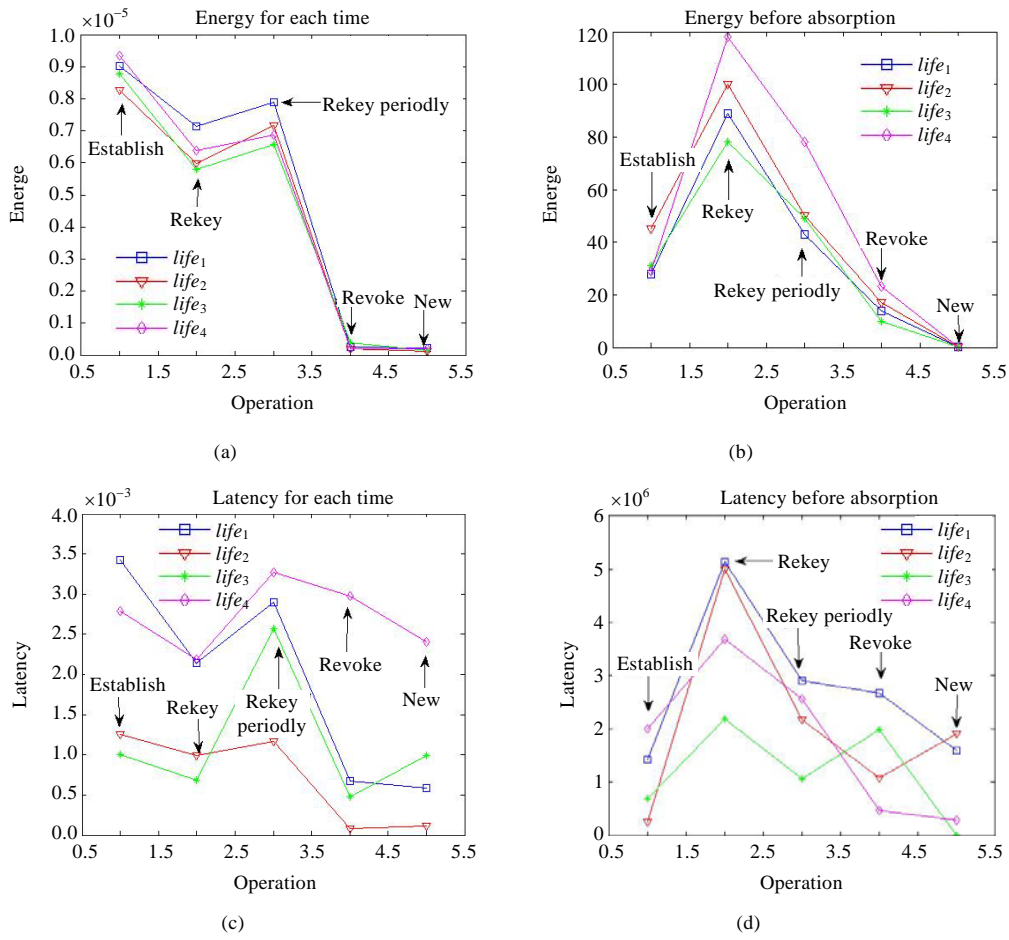


Fig.6 Experimental results

图 6 实验结果

5.3 对比分析

前两节本文已经证明了模型本身的正确性以及分析协议短期和长期性能的有效性,本节重点对所提模型方法与其他关于能耗、时延及寿命分析方法进行对比.如表 4 所示,其中,“√”表示可以,“—”表示不可以,“*”表示进一步研究后可以.

Table 4 Comparison of analyzing methods

表 4 分析方法对比

用途	KML	随机过程	随机预言机
分析连通性	*	√	—
分析单步能耗、时延	√	√	—
分析长期能耗、时延	√	√	—
分析网络寿命	√	√	—
模拟攻击场景	√	√	√
分析协议安全性	*	√	√
刻画并行策略	√	—	—
建模直观性	直观	不直观	较直观
刻画规模	有限	>KML	>KML

在 3 种密钥管理协议分析方法中,随机预言机主要实现逻辑推理,因此常见于安全性分析,在数值分析方面作用很弱.对于能耗、时延和寿命等数值性能,KML 和随机过程都可以实现,但相比随机过程的数学建模方法,KML 更加直观,能够刻画并行的策略模型,更适用于协议状态规模较小的应用.

6 结束语

本文在研究无线异构传感网密钥管理协议需求和能耗分析方案的基础上,融合并扩展了有色层级 Petri 网和广义随机 Petri 网,使得所提 HKML 模型能够适应传感网的异构特性,并能适应短期和长期性能分析,在成功扩大密钥管理协议性能分析范围的同时,降低了形式化建模和分析的复杂度.本文的主要贡献有:

- (1) 提出了异构传感网密钥管理框架,细粒度地刻画了密钥管理机制,为相应的协议设计和分析提供了一条普适思路;
- (2) 结合并扩展了有色层级 Petri 网和广义随机 Petri 网,提出了适合密钥管理协议建模的 HKML 形式化模型;
- (3) 在确定实体层物理网络的分簇结构基础上,建立了 Top 策略层和 Button 通信层 HKML 模型,确立了密钥管理协议分析模型的基本结构;
- (4) 详细介绍了密钥管理协议的 HKML 模型的能耗、时延和寿命的分析方法,为基于所提模型的密钥管理协议分析提供了坚实的数学理论支持;
- (5) 最后,通过实例说明了所提 HKML 模型在密钥管理协议建模和分析方面的应用.实验结果说明,利用所提 HKML 模型来对密钥管理协议进行建模、完成短期和长期性能分析的方法是可行且有效的.

今后,我们将继续研究 HKML 模型对密钥管理协议其他性能的分析,并探求一种以所述密钥管理框架为输入和主导思想的仿真工具的实现方法.

References:

- [1] Haapola J, Shelby Z, Pomalaza-Raez C, Mahonen P. Cross-Layer energy analysis of multi-hop wireless sensor network. In: Cayirci E, Baydere S, Havinga P, eds. Proc. of the 2nd European Workshop on Wireless Sensor Networks. Institute of Electrical and Electronics Engineers, 2005. 33–44. [doi: 10.1109/EWSN.2005.1461997]
- [2] Wander AS, Gura N, Eberle H, Gupta V, Shantz SC. Energy analysis of public-key cryptography for wireless sensor networks. In: Kawada S, ed. Proc. of the 3rd IEEE Int'l Conf. on Pervasive Computing and Communications (PerCom 2005). Los Alamitos: IEEE Computer Society, 2005. 324–328. [doi: 10.1109/PERCOM.2005.18]
- [3] Uluagac AS, Beyah RA, Li YS, Copeland JA. VEBEK: Virtual energy-based encryption and keying for wireless sensor networks. IEEE Trans. on Mobile Computing, 2010,9(7):994–1007. [doi: 10.1109/TMC.2010.51]
- [4] Majidi M, Mobarhan R, Hardoroudi AH, H-Ismail AS, Parchinaki AK. Energy cost analyses of key management techniques for secure patient monitoring in WSN. In: Kassim MRM, ed. Proc. of the 2nd IEEE Int'l Conf. on Open Systems (ICOS 2011). Malaysia: IEEE Computer Society, 2011. 117–121. [doi: 10.1109/ICOS.2011.6079269]
- [5] Kong KS, Lee WJ, Han YH, Shin MK. Handover latency analysis of a network-based localized mobility management protocol. In: Proc. of the IEEE Int'l Conf. on Communications (ICC 2008). New York: IEEE Express Conference Publishing, 2008. 5838–5843. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4534128 [doi: 10.1109/ICC.2008.1092]
- [6] Du XJ, Xiao Y, Guizani M, Chen HH. An effective key management scheme for heterogeneous sensor networks. Ad Hoc Networks, 2007,5(1):24–34. [doi: 10.1016/j.adhoc.2006.05.012]
- [7] Ma CG, Zhong XR, Chu ZJ, Zhang H. KMSPN: A key management analyze model for sensor networks. In: Proc. of the IET Int'l Conf. on Wireless Sensor Network 2010. Beijing: Institution of Engineering and Technology, 2010. 302–311. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5741113>
- [8] Lu KJ, Qian Y, Guizani M, Chen HH. A framework for a distributed key management scheme in heterogeneous wireless sensor networks. IEEE Trans. on Wireless Communications, 2008,7(2):639–647. [doi: 10.1109/TWC.2008.060603]

- [9] Alagheband MR, Aref MR. A secure key management framework for heterogeneous wireless sensor networks. In: Decker BD, Lapon J, Naessens V, Uhl A, eds. Proc. of the 12th IFIP TC-6 and TC-11 Conf. on Communications and Multimedia Security (CMS 2011). Berlin, Heidelberg: Springer-Verlag, 2011. 18–31.
- [10] Petri CA. Communication with automata [Ph.D. Thesis]. New York, 1966.
- [11] Peterson JL. Petri Net Theory and the Modeling of Systems. Englewood Cliffs: Prentice-Hall, Inc., 1981. 31–124.
- [12] Alexandre Z. Coloured stochastic Petri nets. In: Proc. of the Int'l Workshop on Timed Petri Nets. Washington: IEEE Computer Society, 1985. 262–271. <http://dl.acm.org/citation.cfm?id=670494>
- [13] Chiola G, Dutheillet C, Franceschinis G, Haddad S. Stochastic well-formed colored nets and symmetric modeling applications. IEEE Trans. on Computers, 1993,42(11):1343–1360. [doi: 10.1109/12.247838]
- [14] Chiola G, Bruno G, Demaria T. Introducing a color formalism into generalized stochastic Petri nets. In: Rozenberg G, ed. Proc. of the 9th European Workshop on Applications and Theory of Petri Nets. London: Springer-Verlag, 1988. 202–215.
- [15] Lin C. Stochastic Petri Net and System Performance Analysis. 2nd ed., Beijing: Tsinghua University Press, 2005 (in Chinese).
- [16] Jensen K, Kristensen LM. Coloured Petri Nets—Modeling and Validation of Concurrent Systems. Berlin: Springer-Verlag, 2009.
- [17] Cho JH, Chen IR, Feng PG. Performance analysis of dynamic group communication systems with intrusion detection integrated with batch rekeying in mobile ad hoc networks. In: Conner OL, ed. Proc. of the 22nd Int'l Conf. on Advanced Information Networking and Applications—Workshops. Washington: IEEE Computer Society, 2008. 644–649. [doi: 10.1109/WAINA.2008.140]
- [18] Xing GL, Lu CY, Zhang Y, Huang QF, Pless R. Minimum power configuration for wireless communication in sensor networks. ACM Trans. on Sensor Networks, 2007,3(2):1–33. [doi: 10.1145/1240226.1240231]
- [19] Jolly G, Kusc MC, Kokate P, Younis M. A low-energy key management protocol for wireless sensor networks. Nordic Journal of Computing, 2005,12:201–228.
- [20] Marsan MA, Conte G, Balbo G. A class of generalized stochastic Petri nets for the performance evaluation of multiprocessor systems. ACM Trans. on Computer Systems, 1984,2(2):93–122. [doi: 10.1145/190.191]
- [21] Xiong BB, Lin C, Ren FY. Performance analysis of stochastic delivery transport protocols in WSNs. Journal of Software, 2009, 20(4):942–953 (in Chinese with English abstract). <http://www.jos.org.cn/1000-9825/3265.htm> [doi: 10.3724/SP.J.1001.2009.03265]
- [22] Lin C, Tian LQ, Wei YY. Performance equivalent analysis of workflow systems. Journal of Software, 2002,13(8):1472–1480 (in Chinese with English abstract). <http://www.jos.org.cn/1000-9825/20020818.htm>

附中文参考文献:

- [15] 林闯. 随机 Petri 网和系统性能分析. 第 2 版, 北京: 清华大学出版社, 2005.
- [21] 熊斌斌, 林闯, 任丰原. 无线传感器网络随机投递传输协议性能分析. 软件学报, 2009, 20(4):942–953. <http://www.jos.org.cn/1000-9825/3265.htm> [doi: 10.3724/SP.J.1001.2009.03265]
- [22] 林闯, 田立勤, 魏丫丫. workflow 系统模型的性能等价分析. 软件学报, 2002, 13(8):1472–1480. <http://www.jos.org.cn/1000-9825/20020818.htm>



马春光(1974—),男,黑龙江双鸭山人,博士,教授,博士生导师,CCF 高级会员,主要研究领域为密码学,信息安全,网络编码,传感网,物联网.



王九如(1983—),男,博士生,主要研究领域为无线传感器网络,信息安全.



钟晓睿(1987—),女,博士生,CCF 学生会员,主要研究领域为无线网络安全,协议性能评测.