一种面向融合泛在网的协同防护体系设计

戚 湧 莫 璇 李千目
(南京理工大学计算机科学与工程学院 南京 210094)

摘 要 在深入分析融合泛在网功能和特征的基础上,通过增加安全接入网关和虚拟重构安全控制服务器(简称安全控制服务器)两类主要的功能实体构成协同防护的硬件体系,同时通过策略订阅实现协同防护的软件逻辑体系,并采用基于证据投影分解方法的证据理论实现安全态势评估,从而实现在融合泛在网中各种末梢网络均可通过安全接入网关,利用现有的各种异构接入网络安全接入到位于IP核心网的安全服务平台,也可将安全服务命令和数据发送到末梢节点。

关键词 融合泛在网,安全接入网关,安全控制服务器,态势评估
中图法分类号 TP393.0 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.05.018

Collaborative Protection Architecture Design Orient to Fusion Ubiquitous Network

QI Yong MO Xuan LI Qian-mu
(School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract With the in-depth analysis on the functions and features of fusion ubiquitous network, the hardware system for collaborative protection described in this paper was implemented by adding two kinds of function entities namely fusion security access gateway and virtual reconstruction security control server (security control server). Meanwhile, the software logical system was implemented by policy subscription. Additionally, an evidence projection decomposition method was used on evidence combination, which provides a security situation analysis method. Thus, in fusion ubiquitous network, various peripheral networks could use existing heterogeneous access network to access the security service platform in the IP core network by security access gateway. Meanwhile, the command and data of security service can be sent to peripheral nodes in the other direction.

Keywords Fusion ubiquitous network, Security access gateway, Security control server, Situation analysis

1 引言

泛在计算(ubiquitous computing)是施乐实验室的Mark Weiser于1991年提出的有别于传统计算的一种计算形式,其目的在于使计算资源在整个现实环境中可随处取得,用户却觉察不到计算机的存在,让人们的关注点从软硬件设备回归到要完成的任务上[1]。在此基础上,无论是日韩的泛在网络(ubiquitous network)、欧盟的环境感知智能(ambient intelligence),还是北美的普适计算(pervasive computing),其核心都是要建立一个充满计算和通信能力的环境,同时使该环境中的人们逐渐融合在一起[2]。2009年,我国政府提出加强建设"感知中国",其核心就是使信息从平面、线式交互发展为大、纵、深的融合泛在网立体交互。

随着融合泛在网研究与建设的进一步推进,作为其有机组成部分的融合泛在网防护体系研究成为一个热点。马铮等人分析移动互联网的安全特性和管控难点,设计相应的安全防护能力架构,提出各层面端到端的安全加固策略,并初步探讨了建立安全监控中心实施全网联动安全保障的思路[3]。吴东海等人提出一种基于实名认证和安全管理两项关键技术的网络空间安全防护体系[4]。赵婷等人提出涵盖物理、网络、主机和应用的智能电网物联网信息安全防护体系[5]。高昆仑等人提出基于可信计算技术的新一代智能电网调度控制系统安全主动防御体系[6]。张水平等人提出一种基于云计算和WCF技术的数据中心安全体系[7]。蒋诚智等人提出了基于智能Agent模型的电力信息网络安全态势感知模型[8]。丁鲜花等人提出了面向云计算环境的按需安全防护框架,具体说明了云计算环境下各类风险应采用的安全对策[9]。当前,在信息化建设不断推进、智能设备日益普及的同时,各类安全事件频发,安全形势不容乐观。原有针对网络中单一对象或仅适应特定网络类型的网络防护技术彼此之间相互独立,缺乏协同作用,难以形成统一的防护力量,已不能适应融合泛在网的现实需要。从以上分析可以看出,虽然针对各细分层面上的防护的研究已有很多,但在融合泛在网层面上的协同防护体系的研究还比较匮乏。为解决这一问题,本文设计一种面向融合泛在网的协同防护体系,以综合利用各种防护措施,为融合泛在网的安全提供保障。

到稿日期:2015-11-06 返修日期:2016-03-24 本文受国家自然科学基金项目(61272419)资助。
戚 湧(1970-),男,博士,教授,博士生导师,CCF高级会员,主要研究方向为网络信息安全,E-mail:790815561@qq.com;莫 璇(1992-),男,硕士生,主要研究方向为网络信息安全;李千目(1979-),男,博士,教授,博士生导师,主要研究方向为网络信息安全。

本文第 1 节介绍融合泛在概念的由来，以及当前面向融合泛在网各组成部分的安全防护体系研究；第 2 节介绍融合泛在网协同防护体系的整体构成；第 3 节介绍协同防护的硬件体系；第 4 节介绍协同防护的软件逻辑体系；第 5 节介绍基于证据投影分解方法的安全态势分析方法；最后总结全文。

2　融合泛在网协同防护体系构成

随着工业监测、智能交通、城市规划、智能物流、感知农业等众多融合泛在网应用的普及，其对象多元、交互快速、地区广域、性质多维等特点日益呈现，迫切需要融合泛在网系统具备安全交互能力、安全风险全域感知能力和适应不同规模、不同性质及不同地区的全维一体化协同防御能力。

美国等西方发达国家日益重视融合泛在网的安全技术。2009 年，美国政府就指出“目前制约融合泛在网技术军事应用的最大问题是无法保障节点系统的接入有效性、资源可信性和信息机密性”，并认为现在是关键的历史转型时刻，美国需要建立全新的、全面的、保卫赛博空间（Cyberspace）的战略，而融合泛在网是赛博空间不可割裂的组成部分。因此，迫切需要建立融合泛在网的协同防护体系。

目前泛在网处于简单、垂直的物联阶段，缺乏统一的协同融合理论基础与技术规范，每种公众服务或行业应用都要设计和建设自己的传输网络和应用平台，这增加了系统应用的成本，造成了巨大的资源浪费，并且制约了融合泛在网技术的推广使用。

融合泛在网末梢网络包括：RFID 网、传感器网（如 ZigBee）以及传统 IP 网（WiFi 或 Ethernet）；泛在网接入网络包括 WLAN、WiMax、ADSL、FTTH、3G、4G、Cable、电力线网（LPC）、卫星链路等现有的各种远程传输手段。融合泛在网的协同防护体系结构中安全接入网关位于接入适配层，向下连接感知延伸层，向上连接网络接入层，为不具有广域接入能力的各种感知网络和设备提供传输通路。接入适配层还包括在各种接入网中注册的智能终端，这些智能终端本身就具有广域接入能力，不需要借助接入网关来提供传输通路。安全控制服务器位于 IP 核心网，为服务支撑层和业务应用层提供支持。融合泛在网的协同防护体系框架如图 1 所示。

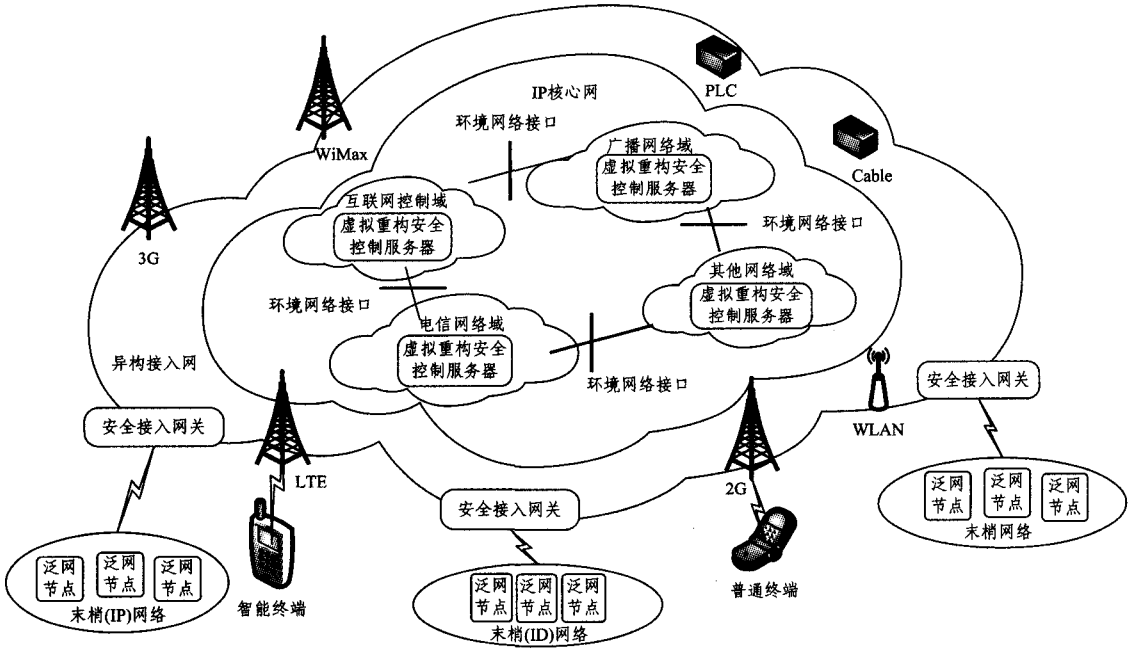

图 1　融合泛在网的协同防护体系框架

融合泛在网络主要的安全业务类型包括：安全数据监测（包括事件 Events、通知 Notification）、远程安全控制、数据安全处理以及其他安全通信业务。泛在网的安全数据的传输类型不同于物联网，后者侧重安全数据采集（单向上传）；泛在网络安全数据传输类型包括：安全数据采集类（上行）、安全广播类（下行）以及安全传输/桥接类（双向）。融合泛在网的安全接入适配模式如图 2 所示。

对于电路域，传统通信安全业务（语音、短信）直接通过所属接入网接入电路域核心网获取所需安全服务；分组域承载的通信安全业务则通过 IP 核心网中的安全控制服务器实现异构安全融合，安全接入网关负责提供到该安全服务器的 IP 层互联通道。安全协同防护在融合泛在网体系中的所属分层位置如图 3 所示。在逻辑层面上，融合泛在网的协同防护逻辑体系主要有 3 个层次，如图 4 所示。

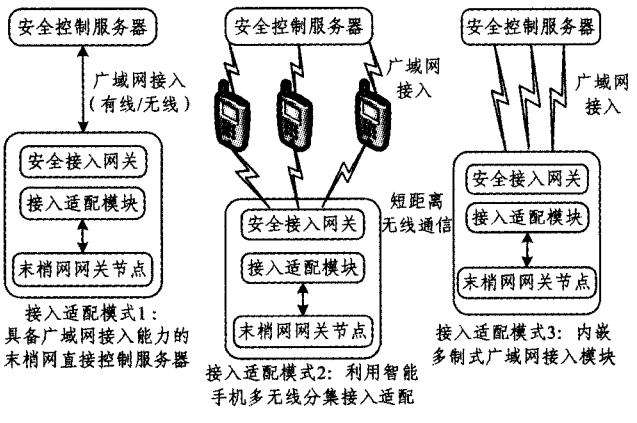

图 2　融合泛在网的安全接入适配模式

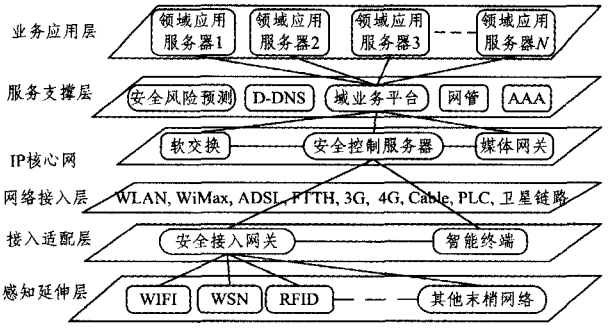

图 3 协同防护在融合泛在网体系中的所属分层

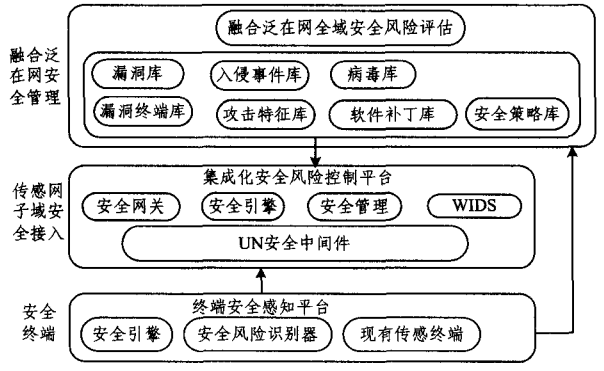

图 4 融合泛在网的协同防护逻辑体系结构

最底层是终端安全感知平台。该层在安全接入网关的基础上综合使用终端漏洞自修复和安全引擎自加载技术，运用基于 DS 的安全态势分析方法实现融合泛在网系统的安全风险识别，达到综合安全风险感知的目的，体现“防”的概念。

中间层是集成化的安全风险控制平台。该层以安全控制服务器为主要载体，包括融合泛在网系统安全风险预测与动态控制子系统，结合对安全网关、安全引擎、安全管理、UN 安全中间件等的有机集成，体现“测、控、管”的思想。其中，安全管理组件用于管理终端软件漏洞、病毒库、审计和无线定位以及瘫痪节点的隔离与修复。安全中间件则为各种各样的终端提供良定义的一致安全接口，屏蔽设备的异构性。

最上层是融合泛在网安全风险评估层。通过融合泛在网系统安全策略的层次联合建模方法，结合安全风险评估系统和基础数据库，实现融合泛在网全域安全评估的自动化，体现安全中以“评”促“管”的思想。

3 协同防护的硬件体系

融合泛在网协同防护的硬件体系由融合安全接入网关（简称安全接入网关）和虚拟重构安全控制服务器（简称安全控制服务器）两类主要功能实体共同构成。其中，安全控制服务器这个关键功能实体使用“软总线＋软构件”的方法，其组件框架如图 5 所示。

安全控制服务器实现以下功能：1）安全资源注册——存储安全接入网关标识、安全状态、能力集参数等安全信息的数据库；2）连接性管理——与安全接入网关共同管理网关与安全控制服务器应用层的数据持续性，以及安全控制服务器与外部安全应用服务器的数据持续性；3）网络的安全管理——网络内各安全接入网关与安全控制服务器等设备配置及参数设置管理；4）移动性安全管理——与安全接入网关协同管理末梢网络节点的移动性安全（加入、退出网关）以及网关的移动性安全（网关在不同接入网间漫游、切换）；5）安全域管理——统一对象间的安全交互方式，向网络合成管理模块提供可信资源及相应策略；6）MRRM 控制——融合并统一管理接入网关的各种资源；7）网络合成管理——通过在不同控制功能模块及不同泛在网络之间进行协商，能够对网络合成的过程进行管理并建立相关合成协议；8）承载及覆盖管理——通过泛在网业务接口对各种应用提供端到端的承载服务；9）QoS协商及 SLA 管理——在连接资源之上建立并维护业务级协议。

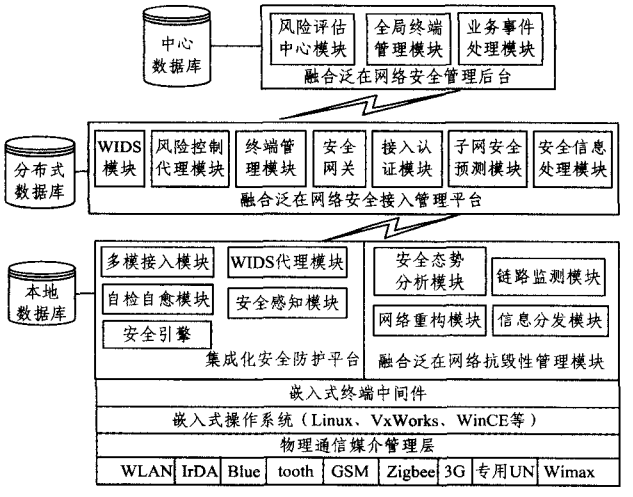

图 5 安全控制服务器的物理体系组件框架

另一个关键功能实体是协同安全接入网关，其功能结构如图 6 所示。

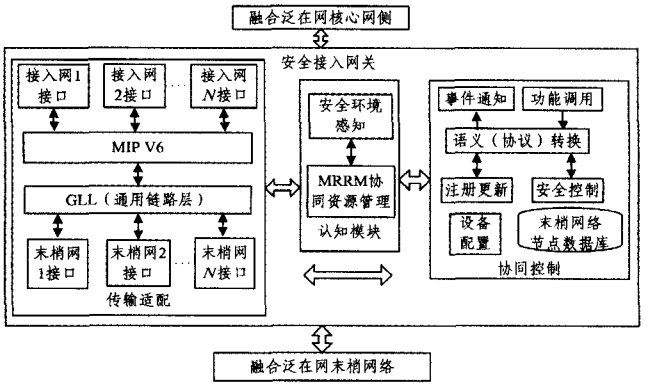

图 6 协同安全接入网关的功能结构图

协同安全接入网关的主要功能包括：1）注册更新——安全接入网关向安全控制服务器注册及更新网关安全信息，包括网关 URN/URL、末梢网络安全类型-安全标识-状态（在线/离线）列表；2）末梢网络节点数据库——存储末梢网络节点标识、安全状态等信息的数据库；3）设备配置——安全接入网关设备配置及参数管理；4）安全控制——安全接入网关与安全控制服务器的双向认证，执行泛在网架构的安全控制协议及功能；5）安全环境感知——安全接入网关对异构接入网与异构末梢网络的网络环境安全感知，以及用户应用需求的

安全感知；6）MRRM 协同资源管理——控制异构广域接入网上的安全连接，并均衡其负载；7）语义（协议）转换——泛在网应用协议到末梢网操作控制处理命令的转换，用于支持数据监测类、远程控制类和数据处理类安全业务应用的协议转换；8）通用链路层 GLL——用于异构末梢网络链路层的数据融合，向上转换为统一的 IP 分组数据，支持有 MAC 层、无 MAC 层末梢网络以及 IP 类型末梢网络旁路。

4　协同防护的软件逻辑体系

融合泛在网通过策略订阅实现协同防护的软件逻辑体系。由于融合泛在网系统具有分布式、层次化、异构性的空间特点和动态演变的时间特点，安全也具有动态、异质的时空特征，将其安全生命周期划分为防护、检测、预测、响应 4 个阶段。相应地，可将一条安全策略分解为防护、检测、预测、响应 4 个分策略。其中，防护分策略描述在整个信息交互过程中，各种可用安全技术构造的多级协同防护体系方法集；检测分策略描述对入侵和攻击的检测条件和方法集；预测分策略描述预测全网安全态势的方法集；响应分策略描述可采取的安全响应方法和调用方式。其中，检测和预测作为规则的条件，防护和响应作为规则的结论，防护是静态的，响应是动态的。4 个分策略同时完成。以此可分阶段解决整个安全周期中存在的问题。

防护分策略是从安全漏洞集 S 到元组 (C,L) 的映射，其中 C 是对策集，L 是关联集，$P:S\rightarrow C\times L$，其实例 $p=(s\rightarrow c,l)$ 表示：若要对漏洞 s 进行防护，可以采用 c 对策，涉及 l 层的安全控制技术。防护子策略不仅给出了漏洞补救方法，还包括部署何种层次安全产品的建议。如利用漏洞 CVE-2014-9034 可以进行 DoS 攻击，其对应的防护分策略为 CVE-2014-9034→patch(https://wordpress.org/news/2014/11/wordpress-4-0-1/)：B(ins-tall new software updates)。该策略表示防护漏洞 CVE-2014-9034，可以在 https://wordpress.org/news/2014/11/wordpress-4-0-1 页面下载漏洞修复补丁，部署防护措施级别中 B 级技术措施（安装软件更新）。

检测分策略是从安全漏洞集 S 到元组 (T,A) 的映射，其中 T 是检测条件，A 是攻击类型，$D:S\rightarrow T\times A$，其实例 $d=(s\rightarrow t,a)$ 表明：利用漏洞 s 的 a 型攻击，可以通过 t 方法检测。如对于 CVE-2014-9034，其检测分策略为 CVE-2014-9034→((content:|key:valuevaluevalue|;protocol:http)，DoS cpu consumption attack)。该策略表示如果以 http 协议发送的畸形报文其内容仅有一个键，冒号后有多个值，则断定为拒绝服务攻击，这种类型的攻击利用了漏洞 CVE-2014-9034。

预测分策略建立从安全漏洞集 S、攻击类型集 A 到预测方法集 M 的映射，$F:S,A\rightarrow M$，其实例 $f=(s,a\rightarrow m)$ 表示方法 m 可预测对 s 漏洞进行的 a 类攻击。如 m 可以对应一个流量测度指标来预测未知类型的攻击。如 CVE-2014-9034 对应的预测分策略为（CVE-2014-9034，DoS）→CPU utilization ration＞95% and last for 300 seconds。该策略表示，如果检测到服务器 CPU 的利用率超过 95%且持续时间超过 300s，则预测可能产生利用 CVE-2014-9034 漏洞进行的 DoS 攻击。

响应分策略定义从威胁评估值到响应方法集 W 的映射。可通过安全漏洞集 S、受保护对象集 O、安全事件集 E（由 D 或者 F 生成）进行定义。$R:S,O,E\rightarrow W$，其实例 $r=(s,o,e)\rightarrow w$ 表示对于利用安全漏洞 s 对受保护对象 o 发起的攻击产生了安全事件 e 时，可以用 w 代表的相应方法进行处理。将攻击目标和安全事件相关联，实现动态响应策略定制。例如，对于利用 CVE-2014-9034 进行的 DoS 攻击，若根据检测分策略检测出报文属于 DoS 攻击报文，第一时间可以采取的响应策略是断开该条 HTTP 连接，以封禁来自该报文源 IP 的所有 HTTP 会话请求。

5　安全态势分析方法

本文选择 DS 证据理论作为对安全态势进行分析的方法，其对应的融合泛在网安全态势分析模型如图 7 所示。

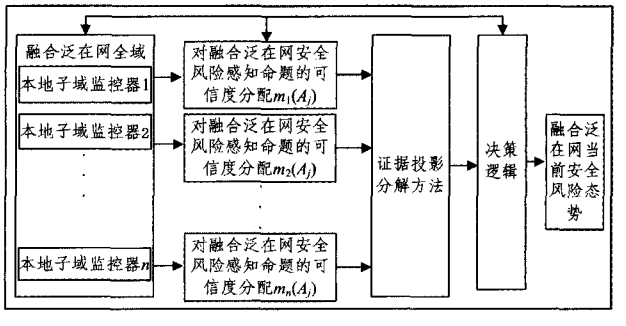

图 7　融合泛在网安全态势分析模型

目前，进行安全态势分析时，国际上普遍使用基本可信度的函数，但常规集结规则仅适用于对小规模融合泛在网安全风险的分析，规模稍大就会引起焦元“组合爆炸”，其计算量往往是不可接受的。因此，本文选择证据投影分解方法合成证据，并以此作为安全态势的决策方法，以减少计算量。

首先确定融合泛在网系统全域安全态势分析的识别框架，考虑各种可能结果，列出全部可能命题（这里的命题是指当前融合泛在网安全态势的所有可能判断，这些命题间相互排斥，互不包含）。假设对当前安全域态势的判断有 t 种可能的结果，即识别框架为 $\Theta=\{\theta_1,\theta_2,\theta_3,\cdots,\theta_t\}$。识别框架的幂集为 $2^{\Theta}=\{\varnothing,\{\theta_1\},\{\theta_2\},\cdots,\Theta\}$。令 m 为识别框架 Θ 上的基本可信度分配（mass 函数），即 $m:2^{\Theta}\rightarrow[0,1]$，其中，$m(\varnothing)=0$，对于 $A\subseteq\Theta$ 且 $m(A)\neq0$，称 A 为 m 的一个焦元，有 $\sum_{A\in 2^{\Theta}} m(A)=1$。假设提供证据的本地子域监控器有 n 个，有限个 mass 函数 $m_1,m_2,\cdots,m_n$ 的 Dempster 合成规则为：$(m_1\oplus m_2\oplus\cdots\oplus m_n)(A)=\frac{1}{K}\sum_{A_1\cap A_2\cap\cdots\cap A_n=A} m_1(A_1)\cdot m_2(A_2)\cdots m_n(A_n)$。

$$K=\sum_{A_1\cap A_2\cap\cdots\cap A_n\neq\varnothing} m_1(A_1)\cdot m_2(A_2)\cdots m_n(A_n)$$
$$=1-\sum_{A_1\cap A_2\cdots\cap A_n=\varnothing} m_1(A_1)\cdot m_2(A_2)\cdots m_n(A_n)$$

此时对于任意 mass 函数 $m(A)$，其对应的信任函数为：$bel(A)=\sum_{B|B\subseteq A} m(B)$，其对应的似然函数为：$pl(A)=\sum_{B|B\cap A\neq\varnothing} m(B)$。其为真的概率 $p(A)$ 为：$bel(A)\leqslant P(A)\leqslant pl(A)$。

从上述分析可看出，传统的 Dempster 合成规则较为复杂。因为识别框架中 t 个命题两两不同，所以可借助欧氏空间的思想将 t 个命题看成两两互相垂直的坐标轴，Θ 即为这些坐标轴组成的坐标系。定义 $m \cdot \cos \alpha_{ij}$ 为 m 在某个坐标轴的投影，其中，α_{ij} 代表焦元 i 与坐标轴 j 间的夹角，而焦元中的元素及其个数决定了 α_{ij} 的大小。接着把所有焦元在各坐标轴上的投影相加后进行归一化，可以得到一个近似概率分布函数 m'。此时 m' 中的焦元都变成了仅含一个元素的原子集。m' 为证据合成得到的最终结果的具体步骤为：

1)计算焦元与坐标轴的夹角余弦值；

2)焦元向各个坐标轴投影；

3)对各坐标轴上的投影分别求和，然后归一化。

据此，即可判断出融合泛在网当前的安全态势。

为说明上述安全态势分析方法的作用方式，以图 8 所示的电力物联网系统为例进行分析。

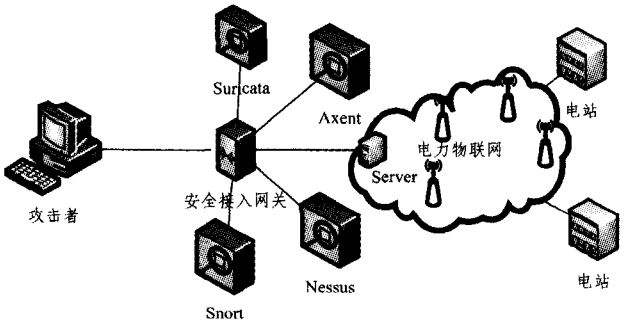

图 8 电力物联网拓扑结构图

在图 8 所示的电力物联网系统中，存在 Suricata，Snort，Axent 3 种入侵检测系统以及漏洞扫描系统 Nessus。若某时刻发生入侵，3 种入侵检测系统的检测结果如表 1 所列，3 种入侵检测系统的识别准确率分别为 0.9，0.85，0.8。

表 1 入侵行为检测结果

入侵检测系统	入侵行为
Suricata	DoS，DNS Attacks，Bots
Snort	Dos，DNS Attacks
Axent	DoS，Bots

令 θ_1 = DoS，θ_2 = DNS Attacks，θ_3 = Bots，此时可以将识别框架定义为 $\Theta=\{\theta_1,\theta_2,\theta_3\}$，有焦元 $A_1=\{\theta_1,\theta_2,\theta_3\}$，$A_2=\{\theta_1,\theta_2\}$，$A_3=\{\theta_1,\theta_3\}$。归一化后可得，$m_1(A_1)=0.353$，$m_2(A_2)=0.333$，$m_3(A_3)=0.314$。焦元 A_1 与坐标轴 $\theta_1,\theta_2,\theta_3$ 的方向余弦分别为 $\cos\alpha_{11}=\cos\alpha_{12}=\cos\alpha_{13}=1/\sqrt{3}$，$m_1'(\theta_1)=m_2'(\theta_2)=m_3'(\theta_3)=m_1(A_1)\cdot\cos\alpha_{11}=0.204$；焦元 A_2 与 $\theta_1,\theta_2,\theta_3$ 的方向余弦分别为 $\cos\alpha_{21}=1/\sqrt{2}$，$\cos\alpha_{22}=1/\sqrt{2}$，$\cos\alpha_{23}=0$，$m_2'(\theta_1)=m_2'(\theta_2)=m_2(A_2)\cos\alpha_{21}=0.235$，$m_2'(\theta_3)=0$；焦元 A_3 与 $\theta_1,\theta_2,\theta_3$ 的方向余弦分别为 $\cos\alpha_{31}=1/\sqrt{2}$，$\cos\alpha_{32}=0$，$\cos\alpha_{33}=1/\sqrt{2}$，$m_3'(\theta_2)=0$，$m_3'(\theta_1)=m_3'(\theta_3)=m_3(A_3)\cos\alpha_{32}=0.222$。此时 $m'(\theta_1)=m_1'(\theta_1)+m_2'(\theta_1)+m_3'(\theta_1)=0.661$，$m'(\theta_2)=m_1'(\theta_2)+m_2'(\theta_2)+m_3'(\theta_2)=0.439$，$m'(\theta_3)=m_1'(\theta_3)+m_2'(\theta_3)+m_3'(\theta_3)=0.426$。将上述可信度分配归一化后可得 $m'(\theta_1)=0.433$，$m'(\theta_2)=0.288$，$m'(\theta_3)=0.279$，即为最终的可信度分配。因此，该电力物联网系统存在 DoS 入侵的可信度为 0.433，存在 DNS Attacks 入侵的可信度为 0.288，存在 Bots 入侵的可信度为 0.279。此时，系统可根据上述可信度信息采取必要的防护措施。

通常优先对可信度最高的检测结果采取措施，此处为 DoS 入侵。根据 Nessus 检测结果得到系统中的 Server 上存在漏洞 CVE-2014-9034，该漏洞是 DoS 入侵发生的根源。以其为例对协同防护逻辑体系的作用过程进行分析，有：CVE-2014-9034 对应的防护分策略为 CVE-2014-9034→patch(https://wordpress.org/news/2014/11/wordpress-4-0-1/)；B(install new software updates)；CVE-2014-9034 对应的检测分策略为 CVE-2014-9034→((content:|key: valuevaluevalue|; protocol:http)，DoS CPU consumption attack)；CVE-2014-9034 对应的预测分策略为(CVE-2014-9034，DoS)→CPU utilization ration>95% and last for 300 seconds；CVE-2014-9034 对应的响应分策略为(CVE-2014-9034，Server，DoS)→close HTTP session and ban IP。

当入侵检测系统根据检测分策略检出 DoS 入侵或根据预测分策略检出服务器 CPU 利用率超过 95%且持续时间超过 300s，同时漏洞扫描系统确定了入侵利用的漏洞为 CVE2014-9034 时，则可采用响应分策略断开 HTTP 会话并封禁报文源 IP，同时执行防护分策略安装软件更新修补漏洞。

结束语 融合泛在网作为国家重要的信息基础设施，已融入生产、生活的方方面面，其安全防护体系的研究是融合泛在网建设中必不可少的一个重要方面。本文通过对融合泛在网功能和特征进行深入的分析，将策略订阅机制与安全接入网关及虚拟重构安全控制服务器相结合，实现协同防护的软硬件体系，并采用基于证据投影分解方法的证据理论实现安全态势评估，从而使融合泛在网中各种末梢网络均可通过安全接入网关，既可利用现有的各种异构接入网络安全接入到位于 IP 核心网的安全服务平台，也可将安全服务命令和数据发送到末梢节点。

参 考 文 献

[1] WEISER M. The computer for the twenty-first century [J]. Scientific America，1991，265(3)：94-104.

[2] International Telecommunication Union. Ubiquitous network societies：their impact on the telecommunication industry[EB /OL]. (2005-06-08) [2015-06-16]. https://www.itu.int/osg/spu/ni/ubiquitous/Papers/UNSImpactPaper.pdf.

[3] MA Z，WANG J Q，ZHOU G T，Analysis of mobile internet security protection system and strategy[C]// 2012 National Conference on Wireless & Mobile Communication. 2012：271-275. (in Chinese)
马铮，王健全，周光涛. 移动互联网安全防护体系及策略探析[C]//2012 全国无线及移动通信学术大会论文集(下). 2012：271-275.

(下转第 131 页)

网络威胁事件产生预警，实时检测网络攻击行为，并采用可视化的方法对结果进行呈现。可根据安全需求将其部署于信息系统安全防护，也可用于 APT 攻击检测等应用场景。

本文更多关注框架设计，给出了各个部分的主要功能和具体实现方式，未涉及过多具体分析方法，下一步的工作重点是结合此框架开展应用，并在此框架下充实完善各种算法细节。

参 考 文 献

[1] LEE Y. Toward scalable internet traffic measurement and analysis with Hadoop[J]. Acm Sigcomm Computer Communication Review, 2013, 43(1): 5-13.

[2] CHEON J J, CHOE T Y. Distributed Processing of Snort Alert Log using Hadoop[J]. International Journal of Engineering & Technology, 2013, 5(3): 2685-2690.

[3] CHARISHMA P, VENKATESH K. Big Data Security Analytic Solution using Splunk[J]. International Journal of Engineering Research & Applications, 2015, 5(4): 50-53.

[4] LI B. Network Security Monitoring and Analysis Based On Big Data Technologies[D]. Dissertations & Theses, 2013.

[5] MARCHAL S, JIANG X, STATE R, et al. A Big Data Architecture for Large Scale Security Monitoring[C]// Proceedings of the 2014 IEEE International Congress on Big Data. IEEE Computer Society, 2014: 56-63.

[6] SAURABH R. Big Data Analytics and Challenges: Network Security and Instruction Detection [J]. International Research Journal of Computers and Electronics and Engineering, 2015, 3(1): 290-295.

[7] MA Z, SMITH P. Determining Risks from Advanced Multi-step Attacks to Critical Information Infrastructures[M]// Critical Information Infrastructures Security. Sprin-ger International Publishing, 2013: 142-154.

[8] ALSERHANI F M. Knowledge-Based Model to Represent Security Information and Reason About Multi-stage Attacks[M]// Advanced Information Systems Engineering Workshops. Springer International Publishing, 2015: 482-494.

[9] LIN S, LI Y, DU X. Study and research of APT detection technology based on big data processing architecture[C]// International Conference on Electronics Information and Emergency Communication. IEEE, 2015.

[10] Opensoc[OL]. http://opensoc.github.io/

[11] XU H. Research on the Tecom Fundamental Network Information Security Awareness Based on Big Data Analyzation[J]. Journal of Information Security Research, 2015(3): 253-260. (in Chinese)
徐浩. 基于大数据分析的电信基础网安全态势研究[J]. 信息安全研究, 2015(3): 253-260.

[12] LI M G, XIAO Y, CHEN J F, et al. Big Data-based Framework for Security Event Mining[J]. Communications Technology, 2015, 48(3): 346-350. (in Chinese)
李明桂，肖毅，陈剑锋，等. 基于大数据的安全事件挖掘框架[J]. 通信技术, 2015, 48(3): 346-350.

[13] FU Y, LI H C, WU X P, et al. Detecting APT attacks: a survey from theperspective of big data analysis[J]. Journal on Communications, 2015, 36(11): 1-14. (in Chinese)
付钰，李洪成，吴晓平，等. 基于大数据分析的 APT 攻击检测研究综述[J]. 通信学报, 2015, 36(11): 1-14.

[14] SUN D W, ZHANG G Y, ZHENG W M. Big data stream computing: Technologies and instances[J]. Journal of Software, 2014, 25(4): 839-862. (in Chinese)
孙大为，张广艳，郑纬民. 大数据流式计算：关键技术及系统实例[J]. 软件学报, 2014, 25(4): 839-862.

[15] Flume[OL]. http://flume.apache.org.

[16] Kafka[OL]. http://kafka.apache.org.

[17] Storm[OL]. http://storm.apache.org.

[18] Elastic Search[OL]. https://www.elastic.co/products/elasticsearch.

(上接第 104 页)

[4] WU D H, YANG W, LONG K. Security Protection Architecture and Critical Technology for Cyberspace[J]. Information Security and Communications Privacy, 2014(7): 79-80. (in Chinese)
吴东海，杨文，龙恺. 网络空间安全防护体系及关键技术研究[J]，信息安全与通信保密, 2014(7): 79-80.

[5] ZHAO T, GAO K L, ZHENG X J, et al. Research on technical framework and cyber security protection system of IOT in smart grid[J]. Electric Power, 2012, 45(5): 87-90. (in Chinese)
赵婷，高昆仑，郑晓崑，等. 智能电网物联网技术架构及信息安全防护体系研究[J]. 中国电力, 2012, 45(5): 87-90.

[6] GAO K L, XIN Y Z, LI Z, et al. Development and Process of Cybersecurity Protection Architecture for Smart Grid Dispatching and Control Systems[J]. Automation of Electric Power Systems, 2015, 39(1): 48-52. (in Chinese)
高昆仑，辛耀中，李钊，等. 智能电网调度控制系统安全防护技术及发展[J]. 电力系统自动化, 2015, 39(1): 48-52.

[7] ZHANG S P, LI J Z, ZHANG F Q, et al. Research and implementation of data center security system based on cloud computing[J]. Computer Engineering and Design, 2011, 32(12): 3965-3979. (in Chinese)
张水平，李纪真，张凤琴，等. 基于云计算的数据中心安全体系研究与实现[J]. 计算机工程与设计, 2011, 32(12): 3965-3979.

[8] JIANG C Z, YU Y, LIN W M. Research on Electric Information Network Security Situation Awareness Model Based on Intelligent Agent[J]. Computer Science, 2012, 39(12): 98-101. (in Chinese)
蒋诚智，余勇，林为民. 基于智能 Agent 的电力信息网络安全态势感知模型研究[J]. 计算机科学, 2012, 39(12): 98-101.

[9] DING X H, ZHAO W D, JU Y, et al. On Demand Security Framework for Cloud Computing[J]. Computer Science, 2014, 41(Z11): 284-287. (in Chinese)
丁鲜花，赵卫栋，俱莹，等. 云计算的按需防护安全框架[J]. 计算机科学, 2014, 41(Z11): 284-287.