基于模糊身份密码学的机会网络身份认证方案

曹晓梅 殷 瑛
(南京邮电大学计算机与软件学院 南京 210003) (江苏无线传感网高技术研究重点实验室 南京 210003)
(南京邮电大学宽带无线通信与传感网技术教育部重点实验室 南京 210003)

摘 要 针对机会网络的自组织性、开放性、连通性差等特点以及现有的基于上下文的路由协议中可能存在的隐私泄露等安全问题,提出了一种基于模糊身份密码学的身份认证方案F-ONIAS(Identity Authentication Scheme in Opportunistic Network Based on Fuzzy-IBE)。该方案通过一个无需实时在线的PKG为用户颁发私钥来解决机会网络中因节点无法实时连通而导致的传统非对称密码学方案不适用的问题。同时,将节点的生物信息作为身份标识,避免了传统身份密码学中身份信息可能被伪造而带来的安全隐患。仿真实验表明,在存在恶意节点的网络环境下,本方案比现有的经典路由协议方案拥有更高的报文投递率和更低的路由开销率,并且未对报文平均时延造成明显影响。

关键词 机会网络,模糊身份密码学,基于社会上下文的路由
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.10.042

Identity Authentication Scheme in Opportunistic Network Based on Fuzzy-IBE

CAO Xiao-mei YIN Ying
(Department of Computer and Software, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)
(Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China)
(Key Lab of Broadband Wireless Communication and Sensor Network Technology of Ministry of Education, Nanjing 210003, China)

Abstract An identity authentication scheme in opportunistic network was proposed based on Fuzzy-IBE, which can conform to the characteristics of self-organized management, openness and intermittent connectivity in opportunistic networks. The scheme is committed to addressing the security issues such as privacy leaks in the existing social context-based routing protocols. Because of the intermittent connectivity, the traditional cryptography cannot be applied to the opportunistic networks. So in F-ONIAS, an off-line PKG is used to generate private keys for users. Meanwhile, in identity-based cryptography, identity information may be forged. To avoid such security risks, the biological information is used as a node's identifier. Simulation results show that implementing our security scheme does not induce any negative impact on the average delay, and achieves higher delivery probability and lower routing overhead rate.

Keywords Opportunistic networks, Fuzzy identity-based encryption, Social context-based routing

1 引言

机会网络是一种不需要源节点与目的节点之间存在完整链路,利用节点移动带来的相遇机会实现通信的自组织网络[1]。图1是一个机会网络的示意图。源节点S希望将消息传递给目标节点D,但它们不在通信范围之内。因此,S在移动过程中,将消息转发给合适的下一跳节点。中间节点在接收到消息后,先存储消息并在其移动过程中继续寻找机会转发,直至消息到达目的节点D,完成数据传输。机会网络的概念部分源自于早期的容忍迟延网络(Delay Torrent Networks, DTN)和移动自组织网络(Mobile Ad hoc Networks, MANET)[2],但与DTN和MANET不同的是,机会网络将网络中的不连通性看作一种传输的机会,对于实现未来的普适计算具有重大的影响。尤其是在智能终端和手持移动设备蓬勃发展的今天,利用移动来实现数据传输的现象已经非常普遍。因此,机会网络有着很好的研究和应用前景,受到了学术界和产业界广泛的关注。

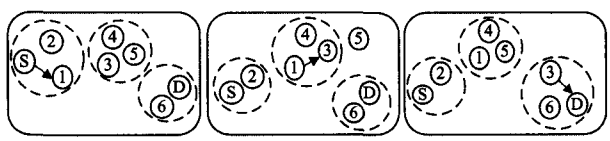

图1 机会网络示意图

机会网络中的节点很多是人们手持的移动设备,人的行为的周期性和规律性使得节点的移动也具有相似的社会属

到稿日期:2013-12-09 返修日期:2014-02-14 本文受国家自然科学基金(61202353),国家重点基础研究发展计划(973)(2011CB302903),江苏高校优势学科建设工程资助项目(yx002001)资助。
曹晓梅(1974-),女,博士,副教授,主要研究方向为计算机通信网与安全,E-mail:caoxm@njupt.edu.cn;殷 瑛(1989-),女,硕士,主要研究方向为无线网络安全。

性[3-6](例如,两个在同一公司上班的人很有可能在某一时刻相遇,从而进行消息的传输)。因此,基于节点上下文信息的路由协议受到了更为广泛的关注。现有的经典的基于社会上下文信息的机会网络路由协议主要有 Bubble[7],HiBOp[8],和 Propicman[9]这 3 种。Bubble rap 协议引入社区和中心度的概念,建立一个排名树,发送者 S 将消息从全局树底开始 bubble,直到找到与目的节点同一社区的节点 R,再将消息从本地树底部开始 bubble,直到消息到达目的节点 D。HiBOp 协议中,节点在本地维护一张"身份表"和一张"历史信息表",综合节点当前的上下文信息和相遇节点的历史信息来选择合适的转发节点。Propicman 协议利用节点档案来描述节点的属性,并通过计算节点档案匹配度来选择下一跳节点。

基于上下文的路由协议利用节点属性来预测和选择转发节点时,不可避免地面临着隐私保护的问题。上下文信息中包含着大量用户的隐私(包括地理位置、身份消息、工作地点、兴趣爱好等),当网络环境中存在恶意节点时,这些隐私消息可能会被恶意地窃取利用。因此,在选择转发节点时,有效的身份验证机制是不可或缺的。在传统的公钥密码体制(也称为基于证书的密码体制)中,节点需要在发送消息前取得目的节点的证书并验证其有效性,这在不实时连通的机会网络中显然是不切实际的[10,11]。为此,Shikfa[12]提出了基于身份密码学的安全方案,用户的公钥直接来源于他的公开身份,而私钥通过一个不必实时在线的密钥生成中心(Private Key Generator,PKG)来生成。PKG 不再需要保存或发放公钥证书,其唯一的任务就是为每个首次加入系统的用户分配一个与其身份对应的私钥。

基于身份密码学的方案简化了用户和公钥的绑定,用 PKG 取代了传统的 CA 为新加入系统的用户发送私钥,此后系统内任何两个用户之间的交互都是直接的,无需第三方参与,因此能很好地适用于不能保持实时连通性的机会网络。在身份密码学中,人们用 Email 地址或者身份证号作为身份信息,而这些信息本身也具有容易被窃取和伪造的局限性[13]。相比之下,人自身的生物信息却能保证是独一无二、不可复制的。在科技高速发展的今天,用手机等智能终端提取指纹、声纹也不再是难事。因此,本文提出一种基于模糊身份密码学的方案,将用户的身份看作是一组描述性的生物信息的属性组合,当且仅当用户私钥中的属性与密文中属性的重合率超过一个阈值时用户才可以解密密文。由于生物信息的不可伪造且唯一的特性,使得模糊密码学在进行身份认证时更加可靠和有效。

2 F-ONIAS 身份认证方案

F-ONIAS 假设网络中存在一个可信服务器。在系统初始化阶段,可信服务器产生用来加密的公共参数,并为用户产生私钥。发送者向两跳之内的节点发送用公共参数加密的消息头。中间节点在接受到加密信息后,用服务器分配的私钥解密得到节点属性值,并将其返回给发送者验证其身份。

2.1 系统架构和组成模块

假设机会网络由可信服务器和用户两个实体组成,可信服务器是一个无需实时在线的 PKG。系统由 Setup、KenGen、Encrypt、Decrypt 4 个模块组成。下面给出具体的描述:

(1)组成模块

1)Setup:给定一个阈值 d。输出一组秘密用来产生公共参数。

2)KenGen:给定一个用户的属性集 ω 和一个秘密集,输出与 ω 相关的一个私钥。

3)Encrypt:给定一个消息 M、一个公共参数集 PP 和一个属性集 ω',加密模块输出与 ω' 关联的密文。

4)Decrypt:给定一个密文 E、一个属性集 ω' 和一个属性集 ω 的私钥 PrK,当且仅当 $|\omega' \cap \omega| \geq d$ 时解密模块可以解密密文。

(2)假设机会网络系统由两个实体组成

1)可信服务器(TS)。这是一个管理属性集的授权机构,用来发行和处理密钥。它用 Setup 模块产生公共参数,并使用 KenGen 模块来为用户产生私钥。它是系统中唯一的能被所有实体信任的部分。

2)用户(User)。其分为发送者和接受者。发送者用 Encrypt 模块加密数据;接受者用 Decrypt 模块解密接收到的消息。

图 2 所示的是系统的基本架构。在初始化阶段,TS 为每一个群组给定一个组内参数 d 和一个虚拟的属性集 D,并产生秘密和公共参数 PP。秘密仅被 TS 所知,而公共参数是公开给所有成员的。TS 同时也为每个成员产生一个私钥 PrK,通过一个安全信道将其传送给每个成员。发送者使用公共参数来加密消息,接收者使用它们的私钥来解密消息。

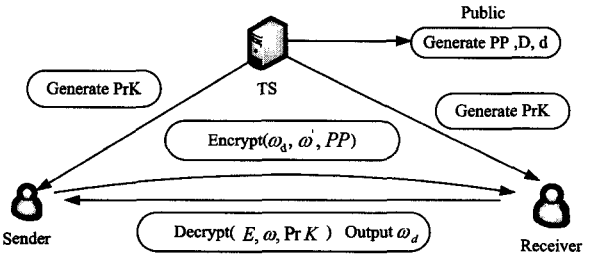

图 2 系统架构

2.2 初始化阶段

TS 首先会产生一个阈值 d,并为每个用户产生公共参数 PP 和私钥 PrK。

(1)参数的产生:TS 选择 $d-1$ 个属性来产生一个虚拟属性集 D,它是一个被所有用户知道的属性集合。所有虚拟的属性是独一无二的且不能被重复用来代表其他属性的。每个群分配一个唯一的属性,称为群 ID,每个用户也分配一个唯一的属性,称为用户 ID。D 中的第 i 个属性表示为 a_i^d,第 i 组的群属性表示为 a_i^g,第 i 个用户的属性表示为 a_i^u。对于每个属性 i,TS 选择一个随机的秘密 $t_i \in Z_p$。TS 同时选择两个主随机秘密 $\alpha, \beta \in Z_p$,α 是解密的主秘密,β 是访问控制的主秘

密。另外，TS选择一个 $d-1$ 阶的群随机多项式 $q(\cdot)$，且 $q(0)=\beta$。对于每个属性 i，令 $\beta_i=q(i)$。只有 TS 知道所有的 $q(\cdot)$。公共参数集 PP 是公开给所有成员的，定义如下：

$$PP=\begin{pmatrix} \hat{e}(P,P)^{\alpha}; \\ t_iP; \\ \beta_iP \end{pmatrix}$$

(2)私钥产生器：TS 同时也负责为每个用户产生私钥。用 ω_{ij} 表示 j 组的用户的属性集$\{a_j^g,a_i^u\}$。TS 为每个用户 i 随机选择一个 $d-1$ 阶多项式 $f(\cdot)$，并令 $f(0)=\alpha$。私钥 $PrK_i=(D_1,D_2)$。其中，$D=\begin{pmatrix} D1_k=\frac{f_i(k)}{t_k}P,\text{for } k\in\omega_{ij}\cup D \\ D2_k=(f_i(k)+\frac{\beta}{t_k})P,\text{for } k=a_i^u \\ D3_k=\frac{1}{t_k}P,\text{for } k=a_i^u \\ D4_k=\frac{\beta_k}{t_k}P,\text{for } k=a_i^u \end{pmatrix}$。

私钥通过安全信道传递给用户。

2.3 加密消息头

将加密的消息头发送给所有两跳之内的节点。ω'是黑名单中用户 ID 的属性集合。令

$$D'=\begin{pmatrix} \{a_1^d,\cdots,a_{d-1-|\omega'|}^d\}, & \text{if } |\omega'|\leqslant d-2 \\ \varphi, & \text{if } |\omega'|=d-1 \end{pmatrix}$$

密文 E 如下：

$$E=\begin{pmatrix} E1=\omega_d[\hat{e}(P,P)^{\alpha}]^r \\ E2_k=r(t_kP),\text{for all } k\in D \\ E3_k=r(\beta_kP),\text{for all } k\in\omega'\cup D' \\ E4=rP \end{pmatrix}$$

其中，$\hat{e}(P,P)^{\alpha}$，t_kP，β_kP 和 P 是公共信息，r 是一个随机数，ω_d 为目的节点属性集。

2.4 身份认证

如果接收者的用户 ID 在接收到的黑名单属性集 ω' 中，那就意味着接收者在黑名单中，则他不能解密消息。如果接收者的 ID 不在接收到的属性集 ω' 中，那就意味着接收者不在黑名单之内，则他可以解密消息。令

$$Z_k=\begin{cases} \dfrac{\hat{e}(D2_k,E4)}{\hat{e}(D3_k,\sum\limits_{x\in\omega'\cup DA'}\sigma_k(E3_k))\cdot\hat{e}(D4_k,E4_k)^{\sigma_k}}, & \text{if } k=a_i^u \\ \hat{e}(D1_k,E2_k), & \text{if } k\in D \end{cases} \tag{1}$$

其中，$k\in\omega''$ 时，$\sigma_k=\prod\limits_{l\in\omega''_i l\neq k}\frac{0-l}{k-l}$；$k\in\{a_i^u\}\cup D$ 时，$\varepsilon_k=\prod\limits_{l\in\{a_i^u\}\cup D;l\neq k}\frac{0-l}{k-l}$，以上两个是拉格朗日系数。解密过程如下：

$$\omega_d=\frac{E1}{\prod\limits_{k\in\{a_i^u\}\cup D}Z_k\varepsilon_k} \tag{2}$$

中间节点在解密得到 ω_d 后，将其发送给源节点 S。S 在收集到所有两跳之内节点的数据包后，检查数据包中的 ω_d，若发现是伪造的，则将节点 i 判断为恶意节点。

3 安全性分析

3.1 可逆性证明

由于 $\sum\limits_{k\in\{a_i^u\}\cup D}\varepsilon_kf_i(k)=f_i(0)=\alpha$ 且 $\sum\limits_{k\in\omega'}\sigma_k\beta_k=q(0)=\beta$，由式(1)，当 $k=a_i^u$ 时，

$$\begin{aligned} Z_k&=\frac{\hat{e}(D2_k,E4)}{\hat{e}(D3_k,\sum\limits_{x\in\omega'\cup D}\sigma_x(E3_x))\cdot\hat{e}(D4_k,E4)^{\sigma_k}} \\ &=\frac{\hat{e}((f_i(k)+\frac{\beta}{t_k})P,rP)}{\hat{e}(\frac{1}{t_k}P,\sum\limits_{x\in\omega'\cup D}\sigma_x(r\beta_xP))\cdot\hat{e}(\frac{\beta_k}{t_k}P,rP)^{\sigma_k}} \\ &=\frac{\hat{e}(f_i(k)P,rP)\hat{e}(\frac{\beta}{t_k}P,rP)}{\hat{e}(\frac{1}{t_k}P,rP)^{\sum\limits_{x\in\omega'\cup D}\sigma_x\beta_x}\cdot\hat{e}(\frac{1}{t_k}P,rP)^{\sigma_k\beta_k}} \\ &=\frac{\hat{e}(f_i(k)P,rP)\hat{e}(\frac{\beta}{t_k}P,rP)}{\hat{e}(\frac{\beta}{t_k}P,rP)} \\ &=\hat{e}(f_i(k)P,rP) \end{aligned} \tag{3}$$

当 $k\in D$ 时，

$$\begin{aligned} Z_k&=\hat{e}(D1_k,E3_k)=\hat{e}(\frac{f_i(k)}{t_k}P,rt_kP) \\ &=\hat{e}(f_i(k)P,rP) \end{aligned}$$

然后，根据式(2)和式(3)，我们可以得到：

$$\begin{aligned} \frac{E1}{\prod\limits_{k\in\{a_i^u\}\cup D}Z_k^{\varepsilon_k}}&=\frac{E1}{\prod\limits_{k\in\{a_i^u\}\cup D}\hat{e}(f_i(k)P,rP)^{\varepsilon_k}} \\ &=\frac{E1}{\hat{e}(P,rP)^{\sum\limits_{k\in\{a_i^u\}\cup D}\varepsilon_kf_{i(k)}}} \\ &=\frac{\hat{M}e(P.P)^m}{\hat{e}(P,P)^m}=\omega_d \end{aligned}$$

因此可逆性得到证明。

3.2 数据机密性

根据 DBDH 和 DMBDH 假设，除非一个攻击者拥有足够多的属性，否则他就不能解密数据。同时，信任服务器随机为不同的用户选择不同的多项式。每个用户持有一个唯一的私钥。因此，一个用户的私钥并不能在计算主秘密方面给其他用户任何提供帮助，即使是多个用户，也不能通过破解主秘密来解密。因此，我们提出的 FUZZY-IBE 方案可以提供数据机密性。

3.3 身份认证的不可抵赖性

由于采用了以生物信息识别为基础的模糊身份密码学理论，因此解决了传统的身份密码学所用的身份证、邮箱地址作为身份标识可能被伪造和假冒的威胁。利用手持设备提取用户的指纹、声纹等生物信息，将唯一且不可否认的身份标识作为加密解密的属性，从而可以实现身份认证的不可抵赖性。

4 仿真

为了验证 F-ONIAS 方案是否能有效地提高机会网络中

数据传输的安全性，减少恶意节点对网络性能的影响，本节将从报文投递率、报文平均时延和路由开销率3个方面对实施了F-ONIAS身份认证方案的Propicman路由协议与原Propicman和使用了身份密码学进行身份认证的Propicman路由协议进行了仿真比较。

4.1 场景设计

我们使用了ONE（opportunistic networking environment）[14]平台对基于模糊身份密码学的Propicman方案进行了仿真与实现，模拟了携带无线智能设备的行人步行于赫尔辛基的场景，并与基于身份密码学的Propicman及原Propicman协议进行了性能对比。具体设置如表1所列。

表1 仿真场景设置

类别	参数	值
场景特征	仿真时间	24h
	仿真区域范围	3400m×4500m
节点特征	移动模型	SPMBM
	移动速度	0.8～1.2(m/s)
	传输速率	250kBps
	缓存大小	40M
消息特征	生产间隔	25～35(ms)
	消息大小	500kB～1MB

4.2 仿真结果分析

(1)报文平均时延与报文生命周期的关系

图3所示的是当网络中的节点总数为600时，报文平均时延随报文生命周期的变化情况。Propicman协议在报文生命周期较长时，由于网络中的有效报文急剧增长，造成网络拥塞，导致平均时延增长。F-ONIAS Propicman和IBE-Propicman两种方案由于在制定转发策略时增加了身份认证机制，使得平均时延较原有方案略有增长。但由于两种方案中的密钥分配都不要求网络实时连通，因此时延增长幅度并不是很大。基于模糊身份密码学的方案在计算消息头时要根据访问控制计算属性集，因此其平均时延比身份密码学略长。

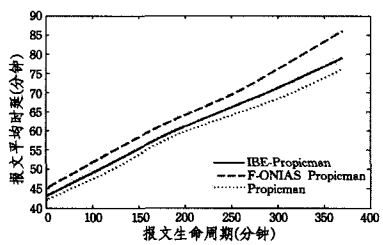

图3 报文平均时延

(2)报文投递率与恶意节点比率的关系

图4对比了Propicman协议，增加了安全机制的F-ONIAS Propicman和IBE Propicman 3个方案在网络环境中存在恶意节点时的报文投递率。正如我们前面分析的，在机会网络这样的自组织网络环境下，很有可能存在恶意节点虚报自己的节点属性来伪造自己有更高的转发概率，在获得数据后，并不按路由方案进行转发，而是直接丢弃数据包，形成数据黑洞。在我们的仿真中，恶意节点的比例设为0%～30%渐变。如图所示，没有安全机制的Propicman协议随着网络中恶意节点的增加，报文投递率急剧下降。而F-ONIAS Propicman和IBE-Propicman由于在转发前验证了节点身份，减少了数据的流失，报文得以安全的传输。在F-ONIAS Propicman方案中，由于引入了不可伪造的生物信息作为身份标识，减少了恶意节点伪造合法身份带来的危害，使得报文投递率更高。

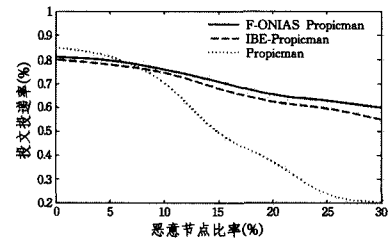

图4 报文投递率

(3)路由开销率与恶意节点比率的关系

图5所示的是Propicman与增加了安全机制的IBE-Propicman和F-ONIAS Propicman方案的路由开销率随恶意节点率变化的关系。路由开销是指一定时间内转发报文的总数。本文用路由开销率来进行评价，即所有节点转发的报文总数与成功到达目的节点的报文总数之比。路由开销率越大，说明中间节点大量转发报文，使网络中充斥大量报文副本，大量消耗节点的能量。由图中可以看出，原Propicman方案中，恶意节点伪造较大的相遇几率来不断接收数据而不转发。当网络中的恶意节点增多时，节点大量转发报文，而报文投递率却急剧下降，导致路由开销率急剧增加。而在IBE-Propicman和F-ONIAS Propicman方案中，由于加入了有效的身份认证机制，减少了节点将数据无效地传递给恶意节点的可能性，降低了路由开销率。尤其是F-ONIAS Propicman方案使用了难以伪造的生物信息作为身份标识，相较IBE-Propicman更大程度地抵御了恶意节点伪造身份接收消息而不转发造成的黑洞效应，有效地降低了路由开销率。

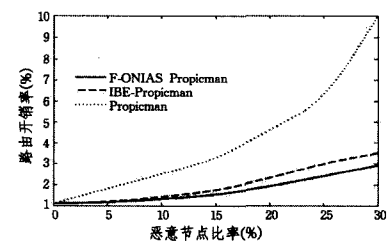

图5 路由开销率

综上所述，本方案只需要在网络初始化阶段进行参数的生成和密钥分配，不需要节点与TS进行实时交互，因而适合在非实时连通的机会网络中部署。仿真结果表明，基于模糊身份密码学的Propicman在性能上与原协议基本保持一致。而当网络环境中存在大量的恶意节点时，F-ONIAS Propicman方案能很好地保证报文的投递率并降低黑洞节点造成的路由开销。

结束语 随着智能手机和手持终端的普及，机会网络将面临着更为广阔的应用前景。在机会网络这样开放的自组织网络环境中，如何保证数据的安全传输和防止用户的隐私泄露是值得深入研究和思考的问题。本文针对这一情况，提出

了一种基于模糊身份密码学的身份认证方案，其利用用户的生物信息作为身份标识来验证中继节点的身份，使得恶意节点无法通过伪造属性来获得转发机会，从而提高了报文投递率。同时，我们以典型的基于上下文信息的转发协议 Propicman 为基础给出了具体的实施方案，并进行了仿真实验。实验表明，基于模糊身份密码学的 Propicman 在性能上与原协议基本保持一致。而当网络环境中存在大量的恶意节点时，F-ONIAS Propicman 方案具有较高的报文投递率及较低的路由开销率。

参 考 文 献

[1] 熊永平，孙利民，牛建伟，等. 机会网络[J]. 软件学报，2009，20(1)：124-137

[2] Grossglauser M，Tse D. Mobility increases the capacity of ad-hoc wireless networks[C]// Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies(INFOCOM 2001). 2001，3：1360-1369

[3] Spyropoulos T，Psounis K，Raghavendra C S，et al. Single-copy routing in intermittently connected mobile networks[C]// 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks，2004 (IEEE SECON 2004). IEEE，2004：235-244

[4] LeBrun J，Chuah C N，Ghosal D，et al. Knowledge-based opportunistic forwarding in vehicular wireless ad hoc networks[C]// Vehicular technology conference，2005. VTC 2005-Spring. 2005 IEEE 61st. IEEE，2005，4：2289-2293

[5] Jones E P C，Li L，Schmidtke J K，et al. Practical routing in delay-tolerant networks[J]. IEEE Transactions on Mobile Computing，2007，6(8)：943-959

[6] 李东生，杨志义，郭斌，等. 基于机会网络的社会性活动组织研究[J]. 计算机科学，2013，40(2)：35-39

[7] Hui P，Crowcroft J，Yoneki E. Bubble rap：Social-based forwarding in delay-tolerant networks[J]. IEEE Transactions on Mobile Computing，2011，10(11)：1576-1589

[8] Boldrini C，Conti M，Jacopini J，et al. Hibop：a history based routing protocol for opportunistic networks[C]// IEEE International Symposium on World of Wireless，Mobile and Multimedia Networks，2007(WoWMoM 2007). IEEE，2007：1-12

[9] Lindgren A，Doria A，Schelén O. Probabilistic routing in intermittently connected networks[J]. ACM SIGMOBILE Mobile Computing and Communications Review，2003，7(3)：19-20

[10] Seth A，Keshav S. Practical security for disconnected nodes [C]// 1st IEEE ICNP Workshop on Secure Network Protocols，2005 (NPSec). IEEE，2005：31-36

[11] Kate A，Zaverucha G M，Hengartner U. Anonymity and security in delay tolerant networks[C]// Third International Conference on Security and Privacy in Communications Networks and the Workshops，2007(SecureComm 2007). IEEE，2007：504-513

[12] Shikfa A，Onen M，Molva R. Privacy in context-based and epidemic forwarding[C]// IEEE International Symposium on a World of Wireless，Mobile and Multimedia Networks & Workshops，2009(WoWMoM 2009). IEEE，2009：1-7

[13] Trifunovic S，Legendre F. Trust in Opportunistic Networks[J]. 2009

[14] Keränen A，Ott J，Kärkkäinen T. The ONE simulator for DTN protocol evaluation[C]// Proceedings of the 2nd International Conference on Simulation Tools and Techniques，ICST (Institute for Computer Sciences，Social-Informatics and Telecommunications Engineering). 2009：55

(上接第 176 页)

义基础。最后，通过对网络攻击实例的有效知识获取，验证了基于本体的网络攻击案例库模型的有效性。

参 考 文 献

[1] López B. Case-Based Reasoning：A Concise Introduction[J]. Synthesis Lectures on Artificial Intelligence and Machine Learning，2013，7(1)：1-103

[2] Acorn T，Walden S. SMART：Support management automated reasoning technology for Compaq customer service[C]// Proceedings of the Tenth National Conference on Artificial Intelligence. MIT Press，1992

[3] William M. Bain Judge：a case-based reasoning system Machine learning[M]// a guide to current research. Kluwer Academic Publishers Norwell，MA，USA，1986

[4] 邓志鸿，唐世渭，张铭，等. Ontology 研究综述[J]. 北京大学学报：自然科学版，2002，38(5)：730-738

[5] 王前，冯亚军，杨兆民，等. 基于本体的网络攻击模型及其应用[J]. 计算机科学，2010，37(6)：114-117

[6] 吴林锦，武东英，刘胜利，等. 基于本体的网络入侵知识库模型研究[J]. 计算机科学，2013，40(9)：120-124，129

[7] 谢新洲，夏晨曦. 网络事件案例库建设与案例数据分析[J]. 情报学报，2012，31(1)：72-81

[8] Amailef K，Lu J. Ontology-supported case-based reasoning approach for intelligent m-Government emergency response services[J]. Decision Support Systems，2013，55(1)：79-97

[9] Akmal S，Batres R，Shih L H. An Ontology-based Approach for Product-Service System Design[M]// The Philosopher's Stone for Sustainability. Springer Berlin Heidelberg，2013：67-72

[10] McClure S，Scambray J，Kurtz G. 黑客大曝光：网络安全机密与解决方案[M]. 2006