ISSN 1000-1239/CN 11-1777/TP
50(2): 278-290, 2013

机会网络中的安全与信任技术研究进展

吴 越[1] 李建华[1] 林 闯[2]
[1](信息内容分析技术国家工程实验室(上海交通大学) 上海 200240)
[2](清华大学计算机科学与技术系 北京 100084)
(wuyue@sjtu.edu.cn)

Survey of Security and Trust in Opportunistic Networks

Wu Yue[1], Li Jianhua[1], and Lin Chuang[2]
[1](*State Engineering Laboratory of Information Content Analysis Technology (Shanghai Jiaotong University), Shanghai* 200240)
[2](*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084)

Abstract Opportunistic networks (OppNets) are one of the evolutionary mobile ad hoc networks whose communication links often suffer from disruption, while their totally different networking paradigm attracts extensive attentions from both researchers and developers. The message in OppNets is transferred only on the occasional encountering of pair-wise mobile wireless nodes, and the routing paradigm is referred to as "store-carry-and-forward" transmission characteristics to implement network communication. In such networks, continuous end-to-end connectivity may not be possible. Due to unique features of high mobility of nodes, frequent link variation and long communication delays, many opportunistic forwarding protocols present major security issues, the design of OppNets faces serious challenges such as how to effectively protect data confidentiality and integrity and how to ensure routing security, privacy and node authentication and incentive cooperation. In other words, systematic research on OppNets is still open and far from a widely-used practical system. In this paper, it first systematically describes the security threats and requirements in OppNets; then elaborates the popular research problems including secure routing, privacy protection, node authentication and incentive cooperation mechanisms in opportunistic networks; and then various security and trust schemes are comprehensively analyzed and compared. Finally it concludes and gives the future research directions.

Key words opportunistic networks; security; privacy; trust; cooperation; incentive mechanism

摘 要 机会网络是一种通信连接经常中断的移动自组织网络,是利用节点移动形成的通信机会逐跳传输消息,以"存储-携带-转发"的路由模式实现节点间通信.然而机会网络作为移动自组织网络的极端版本,其特有的节点高移动性、网络链路经常变化和延迟容忍特性,对数据的机密性和完整性、路由安全性与隐私性以及节点认证与合作性等提出了更高的要求与挑战.首先系统地描述了机会网络的安全威胁与安全需求,深入分析了机会网络中的安全路由及其隐私保护机制;其次研究了机会网络节点认证及其合作激励机制,并对各种相关安全与信任技术解决方案进行了综合比较分析;最后对未来进一步的研究工作作出了展望.

关键词 机会网络;安全;隐私;信任;合作;激励机制

中图法分类号 TP309

收稿日期:2011-10-24;**修回日期**:2012-08-24

基金项目:国家自然科学基金项目(60932003,61271220,61211130104);国家"九七三"重点基础研究发展计划基金项目(2010CB731403)

机会网络(opportunistic networks,OppNets)是一种通信连接经常中断的移动自组织网络(disconnected/disruption mobile ad hoc networks),它的最大特点在于移动节点之间即使没有一条完整的路由存在也能够保持通信.机会网络是利用节点移动形成的通信机会逐跳传输消息,以"存储-携带-转发"的路由模式实现节点间通信,这种完全不同于传统网络通信模式的新兴组网方式引起了研究界极大的兴趣[1-2].

机会网络技术有着巨大的发展前景,但是机会网络技术的应用在如存储管理、电源管理、安全机制、不同异构网络的互通互连等方面仍然面临许多重大挑战[3-4],其中安全和信任技术就是机会网络走向应用的关键问题之一.例如用户在数据传输过程中的任何恶意行为(包括报文的篡改、报文重放等)都将给其他用户带来重大损失,需要深入分析其中的安全威胁与安全需求;隐私保护要求敏感信息(包括用户身份、位置、路线和兴趣等)不被透露,需要提出完备的安全与隐私保护机制;与此同时,授权认证要求在出现事件(如交通事故、犯罪调查)时能够核实用户身份,需要设计灵活的节点认证与接入控制机制;而且由于节点的移动性和网络拓扑不断随机变化,出现异常行为的节点很难定位,节点间的信任关系很难维持等等[5-6].上述的状况可能给其他用户带来致命的威胁,因此迫切需要有一整套完备的安全理论与方法来实现机会网络的通信安全、有限的隐私保护和有效的节点认证与合作激励机制.

由于移动自组织网络 MANET 任一节点对之间存在至少一条完整的端到端通信路径,在安全理论与协议方面有过大量研究[7-12],为机会网络安全机制设计奠定了良好的基础.然而机会网络作为移动自组织网络的极端版本,是利用机会通信使得移动节点更加不可控制,其主要特性表现在以下 3 个方面:

1) 异构性.机会网络不要求网络的全连通,可能使用多种不同的通信技术而且横跨多个异构网络,这将直接导致命名问题.由于节点在不同网络中地址不惟一,必须采用新的认证和信任机制.

2) 移动性.机会网络中节点经常移动会引起路径频繁中断,不可能建立一条稳定的端到端的路由,因而安全解决方案应该是高度动态灵活而且不依赖于事先定义的路径.

3) 延迟容忍.由于消息采用的是"存储-携带-转发"策略,在提高了数据包递送率的同时引入了更大的延迟.从安全的角度来看上述策略无法假设节点之间直接交互,端到端的密钥管理不可能实现,而且所有依靠在线信任授权机构的安全协议需要重新评估与设计.

由于机会网络的以上特殊特性,要求对安全的各个方面作出根本的修正和深入的研究.

1　安全威胁与安全需求

1.1　安全威胁

由于机会网络节点的稀疏性以及不存在网络基础设施(或无法与基础设施建立实时连接),同时节点之间通信链路经常中断,因此面临着比传统有线网络和移动自组织网络更多的安全威胁和风险.主要表现在以下几个方面[13-14]:

1) 非授权访问.由于机会网络的资源稀缺,任何针对网络资源的未授权访问和利用都可能对网络造成严重的影响,如果某个未授权应用可以控制某种机会网络结构(如路由控制协议),它对网络资源的消耗将是雪崩式的.

2) 消息(或束)篡改攻击.在机会网络中,消息可能在多个异构网络中转发,因此存在对消息(或束)进行篡改的潜在风险.

3) 束注入攻击.攻击者可能尝试注入虚假的数据束以欺骗其他节点从而入侵网络,如节点未检测到的重放攻击.

4) 资源消耗攻击.由于机会网络节点的计算、通信或存储资源的有限性,使其极易受到资源消耗的攻击.如非授权应用控制机会网络运作、授权应用越权发送某类服务的数据束、非授权数据内容篡改以及被俘获的网元都会带来资源消耗的攻击风险.

5) 拒绝服务(DoS)攻击.类似于移动自组织网络,机会网络从物理层到应用层的各个层面均会遭受 DoS 攻击,尤其是经常中断的连接和较长延迟的网络特性使 DoS 攻击更加有效.例如查验证书时需要消耗较多的计算资源,因而接收节点和密钥服务器会遭受更多 DoS 攻击的可能性.

6) 机密性攻击.机会网络中数据从源节点发送至目的节点时,会经过若干中间节点的存储、携带和转发,故易遭受中间节点复制或泄露敏感数据内容,构成了数据机密性的潜在威胁.

7) 隐私泄漏.机会网络中的消息往往需要存储在中间节点上,中间节点具有信息传输路径上的上一跳及下一跳节点的信息.实际应用中并不能保证

每个中间节点都是可信的,即使对消息进行了加密,中间节点也可能违反发送端的策略,获取通信双方身份、位置或其他敏感数据等信息,侵犯用户隐私,给通信双方带来经济或其他方面的有形或无形损失.

1.2 安全需求

针对以上安全威胁,在机会网络部署和协议设计时应对网络系统有以下安全考虑:

1.2.1 认证、授权与访问控制

由于机会网络不能建立端到端的安全连接,因此它无法采用在线的中央证书颁发机构 CA 或集中式密钥服务器. 而且机会网络与移动自组织网络 MANET 相比,更着重内容分发而不是对话通信,消息从源节点发送至目的节点是基于对内容感兴趣的接收者而非明确的目的地址. 要避免恶意节点身份欺骗、非授权访问就必须针对机会网络特性建立有效的认证、授权与访问控制机制.

1.2.2 数据机密性和完整性保护

机会网络节点在转发消息过程中,由于无线信号容易被监听,数据可能被截获并被恶意篡改,数据的机密性需求确保数据在转发的过程中敏感信息不暴露给未授权的第三方;另外机会网络"存储-携带-转发"的路由机制导致中间节点有足够的时间修改或者伪造数据,数据的完整性需求确保数据在转发的过程中不被修改. 因此为阻止网络受到数据篡改攻击、伪造攻击以及重放攻击,必须实施有效的数据机密性和完整性保护.

1.2.3 隐私保护

机会网络的隐私性需求包括源节点与目的节点的身份隐私、位置隐私、中间转发节点的身份隐私和位置隐私等. 在一些应用场景中,隐私保护是一类非常重要的安全需求,然而隐私有时又是相对的,对一般用户来说应该保证其足够的隐私性,但是对特定部门来说,应该有相应的手段在必要时暴露其隐私性. 如何兼顾隐私保护与特定部门网络监管与取证是设计机会网络协议的必要考量.

1.2.4 合作激励机制

机会网络的每一个节点既是主机又是路由器,既作为一个网络终端用户又作为一个网络交换节点,故每一个节点都要承担起网络路由和包交换的功能. 但在机会网络中每个节点拥有的资源有限,在多个管理域的情况下,有些节点为了节省自己的资源,不参与网络交换,合作性缺乏保证. 节点的合作行为会在很大程度上影响到机会网络的性能,并且直接影响到路由协议和相关机制的设计,因此建立合适的合作激励机制是解决安全问题又一重要需求.

2 安全机制与隐私保护

机会网络安全与隐私问题研究主要集中在安全路由与隐私保护的设计,以及针对特定安全威胁和攻击设计相应的解决机制上,但还没有形成较为完善的体系. 现就国内外已有的相关研究详细分析如下:

2.1 网络安全架构

机会网络利用机会通信使得移动节点更加不可控制,对数据的机密性和完整性、路由安全性与隐私性等带来更大的挑战,Lilien 等人较早地描述了机会网络的安全问题,并给出了一个初步的安全架构[15]. 他们将安全分为 5 个模块,分别是安全路由、基于角色的访问控制、授权、监测中间节点行为和入侵检测,如图 1 所示:

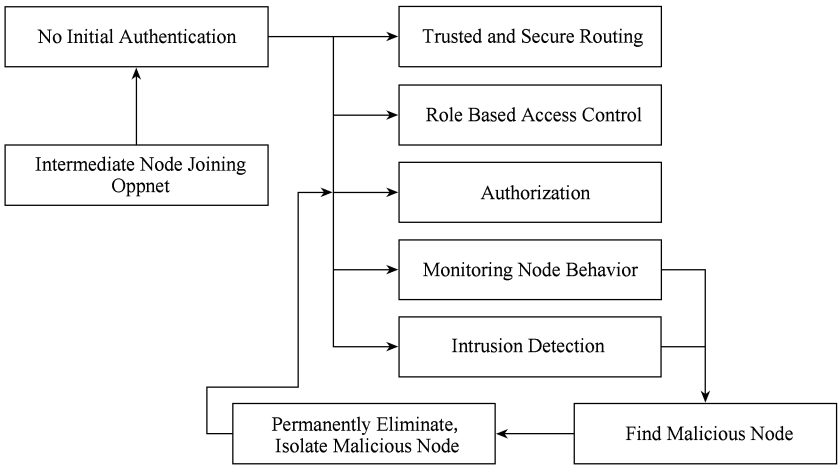


Fig. 1 The security architecture of opportunistic networks.

图 1 机会网络安全架构

首先是安全路由设计.机会网络可以维持一张可信设备列表,例如警察局、政府部门、医院、公共图书馆、大学或知名公司的设备可信度相对较高,将作为路由中间节点的首选.另外可以专门设计符合机会网络特性的安全路由协议.

其次,中间节点必须在基于角色的访问控制后才能被授权进行特定的操作,同时中间节点行为必须受到监控而且还要有入侵检测机制能及时发现恶意节点,最终采取删除、隔离等措施,将恶意节点排除在网络之外.文献[15]给出了机会网络的安全框架,但是并未提供具体的安全解决方案.

2.2　路由安全与隐私保护

2.2.1　路由认证、完整性和机密性

路由认证和完整性可在一定程度抑制一些经典机会网络路由协议的漏洞攻击,Fawal 等人首次研究了机会网络中传染转发(epidemic forwarding)机制的漏洞[16],他们将攻击分为两类:恶意攻击(malicious attack)和理性攻击(rational attack).恶意攻击包括人为制造大量高密度转发包来激发扩展控制或采用禁止机制来抑制邻居节点正常发包,通过修改 TTL 值进行攻击以及假冒正常节点身份大量发送垃圾数据包等;理性攻击包括不合作攻击以及合法节点 Sybil 攻击等.性能评估结果表明,恶意攻击所产生的影响依赖于攻击者与受害者的邻近程度、网络节点密度、业务负载量以及移动性.在静态情况下,被攻击方数据包转发能力受到明显抑制,而其他攻击方式受制于自适应禁止和注入速率控制双重机制,效果并不明显;在移动车载动态环境下,恶意攻击由于扩展控制机制的制约其影响将降至最低.因此结论是只要网络具有较好的路由认证、完整性校验以及扩展控制和自适应禁止机制,恶意攻击传染路由机制很难实现.但是对理性攻击,网络性能下降明显,攻击方可以在各种场景下获取很大的利益和性能提高,如何针对理性攻击进行防范,该文献并未提及,可能的解决方案是通过设计适当的公平合作激励机制来加以克服.

在安全路由中必须要保证传输数据的机密性和完整性,Asokan 等人研究了身份密码学(identity based cryptography,IBC)在机会网络中的适用性[17].基于身份的密码技术 IBC 是一种公钥密码体制的思想,它以用户惟一身份标识,如电子邮箱地址、手机号、车牌号等直接作为系统中用户的公钥信息,因而避免了繁琐的数字证书管理问题.

在路由认证和完整性方面,由于中间节点资源有限,要求使用认证机制作为基于策略的路由转发基础,而接收者也要求数据源认证和数据完整性校验才能保证数据内容的真实可靠性.Seth 等人认为证书废除列表不适合机会网络是因为在连接经常中断的环境中上述列表更新时间过长[18],而在 IBC 中则不存在此问题.IBC 系统可以周期性地刷新标识符和基本密钥,每个基本密钥在很短时间(如一天)内有效,当前标识符可以由长期标识符与有效时间串接,例如 Alice@example.com:30-08-2011 表示 Alice 可以在 2011 年 8 月 30 日内使用此当前标识符,校验者可以检查消息是否被最近的签名密钥签过名.故基于 IBC 的认证方案只需要接收周期性刷新后的签名密钥即可.

当然传统公钥密码中,发布签名密钥的证书也可以使用短有效期(如一天)的方案.签名者要从 CA 周期性地接收新证书,但是前提是签名密钥本身必须长期有效,校验者在获得有效期内的证书后可以检查消息是否被正确签名.因此结论是机会网络中的认证与完整性保护不必完全求助于 IBC,却可以巧妙地使用传统公钥密码技术.值得注意的是即使没有网络连接,传统的数字签名机制仍然可以实现所有必要的认证和校验.

总之,基于身份密码 IBC 和传统公钥密码的数字签名作为机会网络的路由认证机制同样有效,都要求发送者能够接收到包含 IBC 签名密钥或证书的消息(从服务器 PKG 或证书授权机构 CA 获得),而接收者即使在无网络连接时照常可以认证和校验通过机会网络发送的消息内容.

在路由机密性方面,如果缺乏到接收者或密钥服务器的连接,则使得获取加密密钥和检查其有效性变得非常困难,导致传统公钥密码方法不再适用.而身份密码 IBC 系统中,发送者只要知道接收者身份和公共系统参数就可以对消息实施加密,即使无网络连接时也不影响其加密.

为了分析路由机密性计算开销,假设机会网络中有 s 个发送者,每人发送 m 条消息给 d 个接收者;同样网络系统中有 r 个接收者,每人平均接收 e 条消息.消息收发总数应该相等,即 $smd=r\times e$.基于身份密码 IBC 技术和传统公钥密码 TC 技术的计算开销比较如表 1 所示[17].

结果表明,身份密码学 IBC 在路由机密性方面有优势,是因为其不仅对网络连接性无严格要求,而且对服务器的计算开销要求较少,因此更加有利于保护数据的机密性.

Table 1 Computational Overhead Comparison of IBC and TC Based Confidential Message Transmission

表 1 基于 IBC 和 TC 的机密消息传输计算开销比较

Type	IBC Based Cryptography	TC Based Cryptography
Server	r IBC key generation r symmetric encryptions	sm private key decryptions smd symmetric encryptions
Sender	md IBC encryptions m symmetric encryptions	m public key encryptions m symmetric encryptions
Receiver	e IBC decryptions $1+e$ symmetric decryptions	$e+e$ symmetric decryptions

2.2.2 隐私保护

机会网络中的隐私保护更多地与特定的应用场景密不可分,一般可以分为基于节点上下文的隐私保护、基于数据内容的隐私保护和基于节点社会关系的隐私保护.

对于异构的网络,尤其是机会网络,网络地址变得没有意义.源节点和目的节点之间的传统通信模式被基于报文内容的传播模式所取代,目的节点被它们共同的"内容"(如感兴趣的信息报文)或"上下文"(如环境、地理位置等)隐性地定义,而不再是被一个显性的地址定义.基于"上下文"和基于"内容"的两种转发模式都给机会网络的隐私保护问题带来挑战,因为上下文和内容都是隐私数据,需要保持机密性,但中间节点仍需要通过访问报文的"上下文"或"内容"部分来实现机会网络的有效通信.在安全路由和隐私保护间存在的冲突问题需要全新的方案加以解决,因此针对机会网络中两种主流的转发模式应该分别设计隐私保护解决方案.

在基于上下文的转发模式中,目的节点不为源节点直接所知,但源节点知道目的节点的上下文属性.由于目的节点的上下文是属于隐私的信息,必须得到有效的保护,不得在网络中公开地发送.Shikfa 等人提出了机会网络中基于上下文和传染转发的隐私解决方案[19],该方案基于身份的加密技术,用目的节点的上下文属性取代目的节点的身份.在这种转发模式中,中间节点需要将它们的上下文与目的节点的上下文信息进行比较,这就要求中间节点能够发现可以与目的节点相匹配的属性而不获知其他额外的属性信息,从而保证目的节点的隐私.他们将一种基于关键字搜索的公钥加密(PEKS)运用到机会网络,使中间节点可以搜索匹配的上下文.同时为了要满足机会网络通信的安全路由需求,需要对 PEKS 的操作模式进行修改,用一个可信第三方取代目的节点,负责提供给每个中间节点与它们上下文有关的信息.可信第三方只需要在节点加入网络之前与之连接一次,而在网络通信过程中一直处于离线状态,这恰好与机会网络的连接特性相符合.而且允许中间节点计算它们与目的节点的上下文之间的匹配程度,然后转发消息给拥有匹配程度更高的节点,从而解决了基于上下文转发模式的隐私保护问题.

在基于内容的通信模式中,发送方与接收方之间存在一个完全的解耦合关系,中间节点的路由表建立在接收方发布的兴趣基础之上.这些兴趣信息属于隐私信息,因此在中间节点建立路由表的同时保证这些信息的机密性是至关重要的.Shikfa 等人还提出了基于内容转发的隐私解决方案[20].与基于"上下文"的转发模式不同之处在于,兴趣本质上并不是与某一节点相关联的,而是频繁变化的.所以关键是使中间节点能够使用加密的兴趣信息建立路由表,并在路由表中实现对加密信息的安全查询.他们实现并验证了一种基于多层互换加密(MLCE)的解决方案,该方案通过多重加密层,使得基于内容的安全路由以一种分布式的方式有效地保护了接收方的隐私.此外尽管缺少端到端的连接,但是端到端的机密性仍能够通过本地的密钥协商协议得到保证.

以上两种通信模式都是针对机会网络的节点上下文信息或者内容隐私提出的解决方案,当然还有其他应用层隐私保护方案[21].实际上机会网络的路由可以利用社交网络信息进行信息转发[22-25],但是社交网络信息若不妥善加以保护,很容易遭受窃听者截获数据包等多种威胁侵犯用户隐私[26-27].Parris 等人在分析了基于社交网络路由隐私威胁的基础上,在消息产生时对每条消息采用修改和模糊发送者朋友列表的方法来达到社交网络路由隐私增强的目的[28-29].通过修改朋友列表引入了似是而非的可抵赖性,使每个发送列表并非真实的朋友列表;而通过模糊朋友列表使得窃听者即使截获了列表也很难读出其原先真实的内容,从而保护了用户社交信息隐私.

他们采用了两种方式,一种是统计社交网络路由 SSNR,发送者对每条即将发送的消息改变其朋友列表,即增加或者删除节点.修改后的列表在一定程度上仍然基于真实的朋友列表,故还是可以提供社交网络路由,但任何能看到此列表的节点却无法确定某一特殊节点是否确实是发送者的朋友,修改程度可以由发送者决定(如 50%,即增加 50%的节点或删除 50%的节点).性能评估显示在不同的网络规模与数据集下,即使删除了 40%的节点,网络仍能保持近乎 90%的成功递送率.另外一种是模糊社交网络路由 OSNR,它采用了 Bloom 滤波器过滤朋友列表[30].Bloom 滤波器是一种概率数据结构,可以以一定的概率查询集合成员.如果结果为负则不可能出现出错概率;而结果为正时出错概率随滤波器更加充盈而加大.

实际上 Bloom 滤波器可以视为朋友列表的不可逆 Hash 函数,尽管攻击者仍可以通过暴力破解对 Bloom 滤波器进行逆向工程分析,但其必须穷尽节点的所有标识符,并与明文种子串接来测试通过 Bloom 滤波器的匹配情况,这无疑给攻击者增加了巨大的工作量而使得其攻击成本大幅攀升,这种机制可以在路由性能无明显降低的情况下提高用户的隐私保护性能.不同转发模式下的隐私保护方案比较如表 2 所示:

Table 2　Privacy Protection Scheme Comparison of Different Transfer Modes

表 2　不同转发模式的隐私保护方案比较

Forwarding Mode	Context Based Forwarding	Content Based Forwarding	Social Based Forwarding
Known information of destination node	Partial or whole context attribute	Partial or whole interested content	Partial or whole social network information
Privacy enforcement scheme	Public encryption with keyword search (PEKS) and policy-based encryption	Multiple layer commutative encryption (MLCE)	Statisticulated social network routing (SSNR) obfuscated social network routing (OSNR)
Memory and computation overhead	Low	High	Low
Advantages	Stronger anti-attack performancethan hash function scheme	Stronger anti-attack performance than hash function scheme and less key management overhead than group security scheme	Anti-local eavesdropper and anti-partial eavesdropper
Disadvantages	Requiring offline trusted third party (TTP)	Large key maintenance overhead under collusion attack	Bad scalability for SSNR

3　节点认证与接入控制

3.1　节点认证机制

在机会网络中,针对高效的路由算法设计已经有大量的研究,但在消息转发过程中如何对数据束进行节点认证方面的研究较少.当前 DTNRG 工作组提出的"束安全协议规范"草案中提出了针对网络安全脆弱性问题的解决方案[31],其中包括消息转发时数据束的认证及网络路由器的授权,以控制节点更好地访问和利用网络中的资源,这两方面均与节点认证有关."束安全协议规范"建议采用束认证模块和负载完整模块,通过在每个数据束中添加一个数字签名实现节点的认证和路由器的授权.源节点使用私钥进行数字签名,允许目的节点和中继节点认证源节点的真实性、消息的完整性以及源节点的服务等级.

由于机会网络的特有属性,传统的 PKI 应用于节点认证将面临时空效率瓶颈,同时证书撤销列表(CRL)机制无法适用于连接经常中断、延迟较大的网络环境中,机会网络中的公钥证书管理和撤销机制仍需更深入的研究.Zhu 等人提出了机会批束认证机制(OBBA)[32],一种在线/离线协议,允许中继节点在离线阶段(即携带阶段)结合数据束并在线时(即转发阶段)同时高效认证多个数字签名.与机会路由类似,该机制在一批缓冲数据束需要认证时,在中继节点中机会实现.OBBA 机制是基于身份加密认证的批数字签名,同时结合分片认证树(FAT),可以有效地降低节点认证所需的计算时间和各种开销.

文献[33]结合(t,n)阈值密钥共享和基于身份加密技术进行机会网络的节点认证,在连接经常中断的移动自组织网络中可以有效防范节点的恶意攻击.基于 IBC 的节点主密钥由 n 个分布式私钥服务器 PKG 共享,每个节点需在移动过程中与 n 个 PKG 中的 t 个相遇才可重构自身的私钥.为了克服路由

安全相互依赖的循环问题,引入了基于面对面的节点认证机制,即服务器 PKG 与节点间的认证和密钥建立过程只有在它们直接相遇的条件下进行.

基于身份加密 IBC 技术使节点的公钥可以从其公开的个人信息(如邮箱地址)中直接获取,无需公钥证书的建立和管理,应用于机会网络的节点身份认证具有优势.当然在 IBC 基础上引入其他补充机制是机会网络节点认证的趋势[34].

3.2 节点接入控制

如果机会网络中缺乏节点的接入控制机制,恶意路由器可对数据束任意地插入错误信息,其他合法路由器转发这些伪造消息的副本,攻击者将对网络产生大量不必要的负载流量.由于机会网络资源的稀缺性,对网络资源的未授权访问和利用是机会网络安全策略的另一个重要议题[35].机会网络中的长时延、连接中断、不对称数据链路等使得传统网络中接入控制管理系统无法直接适用.节点接入控制[36]有助于网络及其资源免受未认证节点的未授权访问,其中集中式、分布式和等级式架构是不同网络环境管理节点接入控制的三大管理框架[37-38],而等级式架构是机会网络中节点接入控制的首选.

机会网络的束节点是实现网络结构"束层"(bundle layer)协议的主要组件[39],由主节点、路由器和网关组成,它们的存储空间和转发能力固定受限.束层协议在应用服务器中实现,包括束协议层代理、汇聚层适配器和应用层代理,与文献[37]中的 AAA 服务器机制类似,机会网络中的节点接入控制可借鉴其构想.文献[40]提出了基于传统加密的轻量级等级架构用于实现 AAA 概念,包括可灵活部署的授权服务、数据交换协议、AAA 概念的实现等,减少服务器的负载压力,降低目的节点网络连接的严格限制,该架构允许网络中的节点在没有即时网络连接的情况下既可以执行被赋予的决策,也可以制定独立的访问控制决策.

机会网络的节点接入控制机制需要一个简单且易扩展的框架,比如离线处理的支持、凭证和策略的有效结合、通信开销的降低以及认证与授权的分离等.而这些均建立在机会网络长时延、连接中断、异构的特性基础之上.

4 信任与合作激励机制

4.1 信任模型与分析

为了保证机会组网及其安全相关信息获取和确认的可靠性,对信任问题的研究将成为安全基础理论的重要组成部分.信任模型是解决移动机会网络中的动态性和不确定性带来的安全问题的关键.Eschenauer 等人在移动 Ad Hoc 网络中引入了信任建立的一般原理[41],而且与因特网中的信任建立进行了对比,他们描述了在节点为中心的认证过程中基本证据产生和分发的示例;Zouridaki 等人则在文献[42]中使用修正 Bayes 方法用二手信息构建信誉系统以便在路由协议中建立信任关系.许多信任管理机制允许每个节点基于自身的观察和其他节点的推荐信息建立其独立的对于其他节点的信任观点,例如 CONFIDANT[43]和 CORE[44]基于声誉系统构建节点的信任与合作机制,它们均采用监控模块监视邻居节点是否转发数据包,一旦发现异常行为就会向声誉系统(reputation system)报告.所汇报的信息是本节点直接观察到的结果,而通过其他各个组件汇报的网络中其他节点的行为,采用一定的计算方法对网络中的所有节点在声誉系统中合并后对节点行为进行评估,最终确定其是否可以信任.其信任管理架构如图 2 所示:

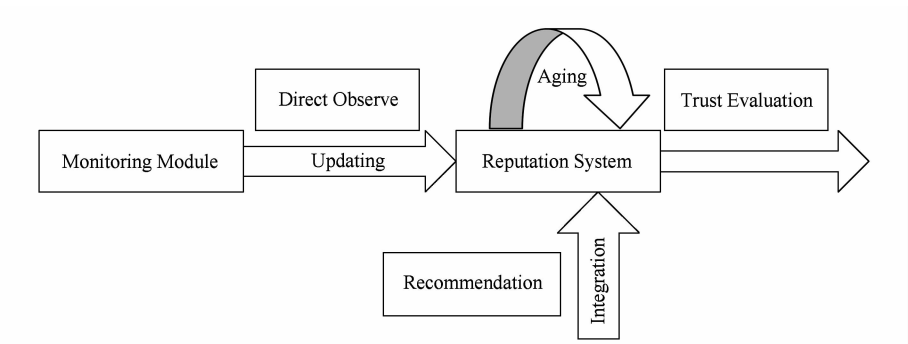


Fig. 2 Trust management architecture.

图 2 信任管理架构

Raya 等人提出针对节点逐个消息的高动态和以数据为中心的无线自组织网络信任关系建立的模型[45],而且采用了 D-S 理论(Dempster-Shafer theory, DST)[46],在具有很高不确定性的网络中对攻击更加有效灵活. Lo 等人提出了采用基于事件的声誉系统来实现车载自组织网络中信任的建立[47],该声誉系统的核心包括 4 个主要功能,即事件管理、声誉值自适应模块、事件声誉值收集以及事件信任列表收集. 不像传统的声誉系统是针对网络节点、网络实体来建立声誉,该技术是针对车载自组网中的某个事件或某些数据来建立声誉,从而为高速移动的车载自组织网络应用的信任问题提供了解决方案.

但是上述信任模型都是针对具有端到端连接的移动 Ad Hoc 网络,尽管对构建机会网络信任模型具有较高的参考价值,但是并不能直接应用于机会网络. 对于特定目的节点的机会路由转发协议[48-50]要求选取合格的转发者,即具有较高概率遇到目的节点的中间节点,实现成功的数据转发. 显然遇到目的节点概率越高,就越有竞争力进行数据的成功递送. 这种方法只适用于友好的无线环境,而不适合有攻击者的敌对场景. 例如某个恶意节点故意夸大其遇到目的节点的概率从而截获本该发往其他节点的数据包,形成"黑洞攻击"[51],严重降低网络性能.

为对付上述任意夸大遇到目的节点概率的恶意行为,Li 等人提出了相遇票据(encounter ticket, ET)作为实际遇到某个节点的证据[52],其定义为

$$ticket=A,B,t,E_{RKA}\{H(A|B|t)\},$$
$$E_{RKB}\{H(A|B|t)\}.$$

该票据包含节点 A 和节点 B 的签名以防信息篡改,式中 $H(\cdot)$为 Hash 函数,$A|B|t$ 表示 A,B,t 的串接,而 $E_{RKA}\{\cdot\}$则表示用节点 A 的私钥进行加密签名.

当目的节点正确接收到数据包时,将产生一个包含签名的确认信息,其格式如下:

$$ack=A,C,p,t,E_{RKC}\{H(A|C|p|t)\},$$

其中 A 为源节点 ID,C 为目的节点 ID,p 为数据包 ID.

由于相遇票据和确认消息只包含了节点的 ID 和签名,和数据包大小相比要小得多,因此其引入的额外开销很小,不会造成网络性能的明显降低却能够有效阻止恶意节点的黑洞攻击.

但是使用相遇票据 ET 的问题在于,自私贪婪节点可以通过一次性的尾部挡板攻击(tailgate attack)收集冗余的票据,夸大其与目的节点相遇的次数和概率;或者多次进入和移出目的节点通信范围,并在较长的时间间隔里收集票据,然后对目的节点进行数据截获,从而达到多重尾部挡板攻击. 因此单纯使用相遇票据 ET 对付以上两种攻击则无能为力.

Li 等人提出了一种机会网络中基于声誉辅助的数据转发协议 RADON(reputation assisted data forwarding in opportunistic networks)[53-54],采用肯定反馈信息(positive feedback message,PFM)的机制帮助监控节点的行为,能够将传统的看门狗(watchdog)机制扩展到机会网络. 该协议采用以前相遇次数来确定下一个合格的转发者,可以顺利将信任框架集成到单纯数据转发协议中,提升网络抵御黑洞攻击的性能.

由于在不可靠的网络环境中传递票据,可能会带来票据遭篡改的风险. RADON 采用第三方数字签名的方式,有效地防止了票据伪造的情况;同时 RADON 模型探讨了将传统基于声誉的机制扩展到机会网络中,节点之间进行相互监视并提供声誉决策.

采用 PFM 机制后 RADON 协议会产生大量的反馈数据包,尽管与普通数据包相比反馈的 PFM 包尺寸很小,但是这些数据包要作为普通流量发往信源节点,在回发过程中还会产生大量的拷贝,造成网络负担增大. 这也是 RADON 协议的不足,有待改进与提高.

不同信任模型与协议解决方案比较如表 3 所示:

Table 3　Comparison of Different Trust Models and Protocol Resolution Schemes

表 3　不同信任模型与协议解决方案比较

Protocol Type	CONFIDANT	CORE	Encounter Ticket	RADON
Core idea	Detection, alarm, response	Watchdog and reputation table updating	Encounter Ticket (ET)	Positive Feedback Message (PFM)
Anti-attack type	Anti-malicious attack and anti-selfish attack	Anti-selfish attack	Anti-blackhole attack and anti-spoofing attack	Anti-blackhole attack and anti-spoofing attack
Overhead	Low	Medium	Low	Medium
Network scenario	Mobile Ad Hoc networks	Mobile Ad Hoc networks	Opportunistic networks	Opportunistic networks
Disadvantages	Lack of explicit reputation combining and aggregation algorithm	Unable to thwart DoS attack	Unable to thwart multiple tailgating attack	Large network overhead

4.2 合作与激励机制

在数据转发过程中中间节点可能会出现自私行为,即只转发"感兴趣"的报文而忽略其他报文,加之节点资源的有限助长了这种自私行为,该情况对于小型移动设备尤其突出.对于自私行为常采用激励合作和惩罚2种方法.在无线自组织网络中,有关自私行为的问题得到了广泛的研究[55-59], Buttyan 等人提出了基于虚拟货币 Nuglet 的经济学合作激励模型[55],模型中节点通过为其他节点提供转发服务来赚取 Nuglet,然后向其他节点支付 Nuglet 来换取其他转发服务.他们首次系统地提出了许多经济学合作激励模型所必须面对的问题,如数据包的定价、虚拟货币的支付方式等等. Zhong 等人则给出了 Sprite 模型[60],Sprite 同样是该模型中虚拟货币的名字.与 Nuglet 的自由交易不同,Sprite 中的虚拟货币都有一个可信第三方 CSS 统一发放,而节点之间以一种叫作收据(receipt)的结构来证明自己确实提供过转发服务.该模型中 CSS 扮演着重要角色,监视着整个网络.通过节点提交的收据向节点兑现一定数量的 Sprite.同一张收据在不同情况下所能兑现的 Sprite 是不同的.文中引入了博弈论的概念,并通过数学分析,证明了通过合理的定价策略,甚至可以杜绝网络中恶意节点的串谋欺骗.

还有一类是基于声誉系统的合作激励模型,这类机制模型中都有看门狗机制以及声誉(reputation)机制.节点会通过监视自己的邻居节点的行为来确定其表现是否正常,并以此确定该节点的声誉评级.节点还会将这些评级信息广播到网络中.评级低的节点将会遭到惩罚措施,从而得不到中继服务.这类模型中比较典型的有 CONFIDANT, CORE, OCEAN[61],已经在 4.1 节信任模型与分析中提及,不再赘述.

节点的合作行为同样会在很大程度上影响到机会网络的性能,并且直接影响到路由协议和相关机制的设计.尽管上述无线 Ad Hoc 网络中的模型与机制对设计机会网络的合作激励具有重要参考意义,但是其解决方案同样不能直接应用于机会网络中.事实上,基于货币的合作加强解决方案不是依靠昂贵的防篡改硬件,就是依靠可信的在线第三方,而这些均与机会网络的延迟容忍特征不兼容.

针对机会网络各种激励方法与机制的研究日益受到关注和重视[62-66]. Panagakis 等人在文献[62]中研究了机会网络中存在自私节点(即非合作环境下)对传染转发路由(epidemic forwarding)、两跳中继转发路由(two hop relaying)和二进制散发与等待路由(binary spray and wait)这3种典型机会转发机制性能(主要是传输时延和网络传输开销)的影响[67-69],其中合作行为建模为接收到消息拷贝时节点的丢包概率(合作类型Ⅰ)和/或节点相遇时转发消息包的概率(合作类型Ⅱ).结果表明,以网络传输开销作为度量指标,随着自私节点数量的加大即不合作程度的增加,传染转发路由的网络传输开销急剧上升,远超过其他两种路由的增加速度,因而其对节点合作程度最为敏感,即节点自私行为严重降低其性能;若以网络传输平均时延作为度量指标,随着自私节点数量的加大,二进制散发与等待路由消息传输时延迅速增大,超过其他两种路由的增加速度,故对节点合作程度最敏感.相对而言,两跳中继转发路由对节点自私行为反应不明显.同时作者指出,如果在上述路由转发机制中增加简单的激励合作机制将会明显改善网络系统性能.

Shevade 等人提出了一种机会网络中的激励路由[70],其激励机制是互利原则(tit for tat, TFT),即每个节点为邻居节点转发消息包与邻居节点为其转发的消息包数量相同,它不是试图检测恶意行为,而是检测节点好的行为,通常采用数据包确认作为下一跳节点正常工作的证明.该肯定反馈使得节点与其邻居节点进行平衡交换,即对邻节点好的行为奖励以同样互惠的服务而不理会恶意行为.为无线自组织网络设计的看门狗机制监视邻居节点虚假的转发或不转发行为来检测节点的自私行为对机会网络不能适用,原因在于机会网络相邻节点连接经常中断以及移动模式和网络状况经常变动,故节点无法对其邻节点进行监测,而 TFT 则无需监视恶意节点因而非常适合机会网络的路由激励.该文不仅研究了节点自私行为对路由性能严重降低的影响,而且还指出了现有 TFT 机制面临无法引导和遭受剥削利用的问题,提出了一种结合慷慨(generosity)和悔悟(contrition)机制的 TFT 方案克服原有 TFT 的不足,而且设计了相应的激励路由协议.结果表明该协议能有效地促进自私节点的合作并显著提升机会网络的路由性能.

Chen 等人针对异构无线网络提出了机会网络中的基于信用(credit-based)的激励系统 MobiCent 以提供 Internet 访问服务[71].移动设备通常具有两种模式下的工作能力,即既使用长距离低带宽无线链路(如蜂窝接口)保持始终在线连接,同时又能使用短距离高带宽链路(如 Wi-Fi)在相邻区域与对等设备

进行机会性的大量数据交换.短距无线链路由于节点的移动性往往是间歇性的连接,这种间歇性接触可采用机会路由来转发数据.MobiCent使用了一种多重降低回报(multiplicative decreasing reward, MDR)算法来计算支付费用且支持两种类型客户,即希望要求最小化成本和最小化时延的客户.MobiCent为自私节点提供了激励因此无需再检测自私行为,它工作在现有机会网络路由协议之上,确保自私行为不会获得很大的回报.仿真结果表明MobiCent开销有限且能有效促进节点合作,同时可抵御边缘插入攻击(edge inserting attack)和边缘隐藏攻击(edge hiding attack).但是其需要可信第三方(trusted third party, TTP)的支持.Lu等人也提出了车载容迟网络中基于信用的激励协议Pi[72],同样需要有一个可信机构(trusted authority, TA).

不同合作与激励解决方案的比较如表4所示:

Table 4　Comparison of Different Cooperation and Incentive Resolution Schemes

表4　不同合作与激励解决方案比较

Incentive Type	Reputation Based Incentive Mechanism	Tit for Tat (TFT) Based Incentive Mechanism	Virtual Currency Based Incentive Mechanism
Typical Protocol	RADON	Pair-wise TFT	MobiCent
Core mechanism	Promoting cooperation and punishing selfishness by using reputation based trust mechanism	Tit for tat (TFT)	credit-based incentive system without requiring detection of selfish actions
Advantages	Anti-blackhole attack and anti-spoofing attack	Introduction of generosity and contrition to enable bootstrapping and reach stability after perturbation	Anti-insertion attack and anti-hiding attack
Disadvantages	Unable to thwart collusion and Sybil attack	Unsuitable for asymmetric transactions	Requiring offline trusted third party (TTP)

5　结论与展望

作为一种新的组网方式,机会网络在动物迁徙追踪、移动社交、边远地区网络通信和智能交通等领域具有巨大的发展前景,然而安全、隐私和信任技术对机会网络的广泛应用提出了挑战.本文对机会网络中安全和信任技术目前的研究进展进行了综述,系统地描述其安全威胁与安全需求,深入分析了机会网络中的安全路由及其隐私保护机制,研究了机会网络的合作激励机制,并对各种相关安全与信任技术解决方案进行了比较分析.预计机会网络安全和信任技术领域未来的重点研究方向包括以下方面:

1) 结合社交网络理论研究移动社交机会网络安全路由与隐私保护机制;

2) 设计机会网络与蜂窝网、WLAN、Zigbee等混合式网络应用系统中的安全路由协议与隐私保护机制;

3) 基于博弈论的合作激励机制探索,合作激励不仅仅只局限于节点个体理性中,而是扩展到群体理性,因此必须深入研究在机会网络合作博弈模型设计中合作联盟的存在性和稳定性问题,评估合作联盟的实现对网络吞吐量和时延等重要网络性能指标的影响;

4) 大规模测试平台的构建和相关安全与信任协议的验证.

参　考　文　献

[1] Pelusi L, Passarella A, Conti M. Opportunistic networking: Data forwarding in disconnected mobile ad hoc networks [J]. IEEE Communications Magazine, 2006, 44(11): 134-141

[2] Xiong Yongping, Sun Limin, Niu Jianwei, et al. Opportunistic networks [J]. Journal of Software, 2009, 20(1): 124-137 (in Chinese)
(熊永平, 孙利民, 牛建伟,等. 机会网络[J]. 软件学报, 2009, 20(1): 124-137)

[3] Jun H, Ammar M, Corner M, et al. Hierachical power management in disruption tolerant networks with traffic-aware optimization [C] //Proc of the ACM CHANTS'06. New York: ACM, 2006: 245-252

[4] Krifa A, Barakat C, Spyropoulos T. Optimal buffer management policies for delay tolerant networks [C] //Proc of SECON'08. Piscataway, NJ: IEEE, 2006: 260-268

[5] Hong X, Huang D, Gerla M, et al. SAT: Situation-aware trust architecture for vehicular networks [C] //Proc of MobiArch'08. New York: ACM, 2008: 31-36

[6] Miranda H, Rodrigues L. Reputation in anonymous vehicular networks [J]. Int Journal of Autonomous and Adaptive Communications Systems, 2010, 3(2): 178-197

[7] Zhou L, Hass Z. Securing ad hoc networks [J]. IEEE Network, 1999, 13(6): 24-29

[8] Hu Y, Perrig A, Johnson D. Ariadne: A secure on-demand routing protocol for ad hoc networks [C] //Proc of ACM MobiCom'02. New York: ACM, 2002: 12-23

[9] Theodorakopoulos G, Baras J. Trust evaluation in ad-hoc networks [C] //Proc of the ACM Workshop on Wireless Security (WiSe'04). New York: ACM, 2004: 1-10

[10] Yang H, Luo H, Ye F, et al. Security in mobile ad hoc networks: Challenges and solutions [J]. IEEE Wireless Communications, 2004, 11(1): 38-47

[11] Wu B, Chen J, Wu J, et al. A survey of attacks and countermeasures in mobile ad hoc networks [M] //Wireless Mobile Network Security. Berlin: Springer, 2006: 1-38

[12] Li W, Parker J, Joshi A. Security through collaboration in MANETs [C] //Proc of CollaborateCom. Berlin: Springer, 2008: 696-714

[13] Farrell S, Cahill V. Security considerations in space and delay tolerant networks [C] // Proc of 2nd IEEE Int Conf on Space Mission Challenges for Information Technology (SMC-IT'06). Piscataway, NJ: IEEE, 2006: 29-38

[14] Farrell S, Symington S, Weiss H, et al. Delay-tolerant Networking Security Overview: Draft-irtf-dtnrg-sec-overview-06 [EB/OL]. (2009-03-08) [2011-10-08]. http://tools.ietf.org/html/draft-irtf-dtnrg-sec-overview-06

[15] Lilien L, Kamal Z, Bhuse V, et al. Opportunistic networks: The concept and research challenges in privacy and security [C] // Proc of Int Workshop on Research Challenges in Security and Privacy for Mobile and Wireless Networks (WSPWN 2006). Piscataway, NJ: IEEE, 2006: 134-147

[16] Fawal A, Boudec J, Salamatian K. Vulnerabilities in epidemic forwarding [C] //Proc of the IEEE Int Symp on World of Wireless, Mobile and Multimedia Networks (WoWMoM'07). Piscataway, NJ: IEEE, 2007: 1-6

[17] Asokan N, Kostiainen K, Ginzboorg P, et al. Applicability of identity-based cryptography for disruption-tolerant networking [C] //Proc of the 1st Int MobiSys Workshop on Mobile Opportunistic Networking. New York: ACM, 2007: 52-56

[18] Seth A, Hengartner U, Keshav S. Practical security for disconnected nodes [C] //Proc of the 1st Workshop on Secure Network Protocols (NPSec'05). Piscataway, NJ: IEEE, 2005: 31-36

[19] Shikfa A, Onen M, Molva R. Privacy in context-based and epidemic forwarding [C] //Proc of the 3rd IEEE Int WoWMoM Workshop on Autonomic and Opportunistic Communications. Piscataway, NJ: IEEE, 2009: 1-7

[20] Shikfa A, Onen M, Molva R. Privacy in content-based opportunistic networks [C] //Proc of the 2nd IEEE Int Workshop on Opportunistic Networking. Piscataway, NJ: IEEE, 2009: 832-837

[21] Dóra L, Holczer T. Hide-and-lie: Enhancing application-level privacy in opportunistic networks [C] //Proc of the 2nd Int Workshop on Mobile Opportunistic Networking (MobiOpp'10). New York: ACM, 2010: 135-142

[22] Bigwood G, Rehunathan D, Bateman M, et al. Exploiting self-reported social networks for routing in ubiquitous computing environments [C] //Proc of the 1st Int Workshop on Social Aspects of Ubiquitous Computing Environments. Piscataway, NJ: IEEE, 2008: 484-489

[23] Consolvo S, Walker M. Using the experience sampling method to evaluate ubicomp applications [J]. IEEE Pervasive Computing, 2003, 2(2): 24-31

[24] Daly E, Haahr M. Social network analysis for information flow in disconnected delay-tolerant MANETs [J]. IEEE Trans on Mobile Computing, 2009, 8(5): 606-621

[25] Eagle N, Pentland A, Lazer D. Inferring friendship network structure by using mobile phone data [J]. Proceedings of the National Academy of Sciences (PNAS), 2009, 106(36): 15274-15278

[26] Belle S, Waldvogel M. Consistent deniable lying: Privacy in mobile social networks [C] //Proc of Workshop on Security and Privacy Issues in Mobile Phone Use. Berlin: Springer, 2008: 1-8

[27] Lu R, Lin X, Shen X. SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks [C] //Proc of the 29th Conf on Computer Communications (INFOCOM'10). Piscataway, NJ: IEEE, 2010: 1-9

[28] Parris I. Privacy-enhanced opportunistic networks [C] //Proc of the 2nd Int Workshop on Mobile Opportunistic Networking (MobiOpp'10). New York: ACM, 2010: 213-214

[29] Parris I, Henderson T. Privacy-enhanced social-network routing [J]. Computer Communications, 2011, 35(1): 62-74

[30] Bloom B. Space/time tradeoffs in hash coding with allowable errors [J]. Communications of the ACM, 1970, 13(7): 422-426

[31] Farrell S, Symington S, Weiss H, et al. Bundle Security Protocol Specification: RFC 6257 [EB/OL]. (2011-05) [2011-10-08]. http://tools.ietf.org/html/rfc6257

[32] Zhu H, Lin X, Lu R, et al. An opportunistic batch bundle authentication scheme for energy constrained DTNs [C] // Proc of the 29th Conf on Computer Communications (INFOCOM'10). Piscataway, NJ: IEEE, 2010: 605-613

[33] Ma Y, Jamalipour A. Opportunistic node authentication in intermittently connected mobile ad hoc networks [C] //Proc of the 16th Asia-Pacific Conf on Communication (APCC'10). Piscataway, NJ: IEEE, 2010: 453-457

[34] Kate A, Zaverucha G, Hengartner U. Anonymity and security in delay tolerant networks [C] //Proc of the 3rd Int Conf on Security and Privacy in Communication Networks (SecureComm'07). Piscataway, NJ: IEEE, 2007: 504-513

[35] Farrell S, Cahill V. DTN: An architectural retrospective [J]. IEEE Journal on Selected Areas in Communications, 2008, 26(5): 828-836

[36] Hu V, Ferraiolo D, Kuhn R. Assessment of access control systems, 7316 [R/OL]. (2006-09) [2011-10-08]. http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

[37] Laat C, Gross G, Gommans L, et al. Generic AAA Architecture: RFC 2903 [EB/OL]. (2000-08) [2011-10-08]. https://tools.ietf.org/html/rfc2903

[38] Blaze M, Feigenbaum J, Ioannidis J, et al. The Role of Trust Management in Distributed Syetems Security: Secure Internet Programming [M]. Berlin: Springer, 1999: 185-210

[39] Scott K, Berleigh S. Bundle Protocol Specification: RFC 5050 [EB/OL]. (2007-11) [2011-10-08]. http://tools.ietf.org/html/rfc5050

[40] Johnson E, Cruickshank H, Sun Z. Managing access control in delay/disruption tolerant networking (DTN) environment [C] //Proc of the 4th IFIP Int Conf on New Technologies, Mobility and Security (NTMS). Piscataway, NJ: IEEE, 2011: 1-5

[41] Eschenauer L, Gligor V, Baras J. On trust establishment in mobile ad hoc networks [C] //Proc of the 10th Int Security Protocols Workshop. Berlin: Springer, 2002: 47-66

[42] Zouridaki C, Mark B, Hejmo M, et al. Robust cooperative trust establishment for MANETs [C] //Proc of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'06). New York: ACM, 2006: 23-34

[43] Buchegger S, Boudec J. Performance analysis of the CONFIDANT protocol: Cooperation of nodes fairness in dynamic ad-hoc networks [C] //Proc of IEEE/ACM Symp on Mobile Ad Hoc Networking and Computing. Piscataway, NJ: IEEE, 2002: 226-236

[44] Molva R, Michiardi P. Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks [C] //Proc of IFIP—Communication and Multimedia Security Conference. Berlin: Springer, 2002: 107-121

[45] Raya M, Papadimitratos P, Gligor V, et al. On data-centric trust establishment in ephemeral ad hoc networks [C] //Proc of the 27th Conf on Computer Communications (INFOCOM'08). Piscataway, NJ: IEEE, 2008: 1238-1246

[46] Shafer G. A Mathematical Theory of Evidence [M]. Princeton: Princeton University Press, 1976

[47] Lo N, Tsai H. A reputation system for traffic safety event on vehicular ad hoc networks [J]. EURASIP Journal on Wireless Communications and Networking, 2009, 2009 (1): 1-10

[48] Burgess J, Gallagher B, Jensen D, et al. Maxprop: Routing for vehicle-based disruption-tolerant networks [C] //Proc of the 25th Conf on Computer Communications (INFOCOM'06). Piscataway, NJ: IEEE, 2006: 1-11

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

[50] Boldrini C, Conti M, Passarella A. Exploiting users' social relations to forward data in opportunistic networks: The HiBOp solution [J]. Elsevier Pervasive and Mobile Computing, 2008, 4(5): 633-657

[51] Hu Y, Perrig A. A survey of secure wireless ad hoc routing [J]. IEEE Security and Privacy, 2004, 2(3): 28-39

[52] Li F, Wu J. Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets [C] //Proc of the 28th Conf on Computer Communications (INFOCOM'09). Piscataway, NJ: IEEE, 2009: 2428-2436

[53] Li N, Das S. RADON: Reputation-assisted data forwarding in opportunistic networks [C] //Proc of the 2nd Int Workshop on Mobile Opportunistic Networking (MobiOpp'10). New York: ACM, 2010: 8-14

[54] Li N, Das S. A trust-based framework for data forwarding in opportunistic networks [J/OL]. (2011-02-09) [2011-10-08]. http://www.sciencedirect.com/science/article/pii/S1570870511000400

[55] Buttyan L, Hubaux J. Stimulating cooperation in self-organizing mobile ad hoc networks [J]. Mobile Networks and Applications, 2003, 8(5): 579-592

[56] Hu J, Burmester M. Cooperation in Mobile Ad Hoc Networks: Guide to Wireless Ad Hoc Networks [M]. London: Springer, 2009: 43-57

[57] Komathy K, Narayanasamy P. Best neighbor strategy to enforce cooperation among selfish nodes in wireless ad hoc network [J]. Computer Communications, 2007, 30(18): 3721-3735

[58] Altman E, Kherani A, Michiardi P, et al. Non-cooperative forwarding in ad-hoc networks [C] //Proc of the 4th IFIP-TC6 Int Conf on Networking Technologies, Services, and Protocols (NETWORKING'05). Berlin: Springer, 2005: 486-498

[59] Srinivasan V, Nuggehalli P, Chiasserini C, et al. Cooperation in wireless ad hoc networks [C] //Proc of the 22nd Conf on Computer Communications (INFOCOM'03). Piscataway, NJ: IEEE, 2003: 808-817

[60] Zhong S, Chen J, Yang Y. Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks [C] //Proc of the 22nd Conf on Computer Communications (INFOCOM'03). Piscataway, NJ: IEEE, 2003: 1987-1997

[61] Bansal S, Baker M. Observation-based cooperation enforcement in ad hoc networks [R]. Stanford, CA: Stanford University, 2003

[62] Panagakis A, Vaios A, Stavrakakis I. On the effects of cooperation in DTNs [C] //Proc of the 2nd Int Conf on Communication Systems Software and Middleware (COMSWARE'07). Piscataway, NJ: IEEE, 2007: 1-6

[63] Balasubramanian A, Levine B, Venkataramani A. DTN routing as a resource allocation problem [C] //Proc of SIGCOMM'07. New York: ACM, 2007: 373-384

[64] Zhu H, Lin X, Lu R, et al. A secure incentive scheme for delay tolerant networks [C] //Proc of the 3rd Int Conf on Communications and Networking (Chinacom'08). Piscataway, NJ: IEEE, 2008: 1-6

[65] Mahmoud M, Shen X. Stimulating cooperation in multi-hop wireless networks using cheating detection system [C] //Proc of the 29th Conf on Computer Communications (INFOCOM'10). Piscataway, NJ: IEEE, 2010: 1-9

[66] Zhu H, Lin X, Lu R, et al. SMART: A secure multilayer credit based incentive scheme for delay-tolerant networks [J]. IEEE Trans on Vehicular Technology, 2009, 58(8): 4628-4639

[67] Vahdat A, Becker D. Epidemic routing for partially connected ad hoc networks, CS-200006 [R]. Durham, NC: Duke University, 2000

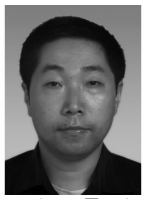
[68] Grossglauser M, Tse D. Mobility increases the capacity of ad hoc wireless networks [J]. IEEE/ACM Trans on Networking, 2008, 10(4): 477-486

[69] Spyropoulos T, Psounis K, Raghavendra C. Spray and wait: An efficient routing scheme for intermittently connected mobile networks [C] //Proc of SIGCOMM'05. New York: ACM, 2005: 252-259

[70] Shevade U, Song H, Qiu L, Zhang Y. Incentive-aware routing in DTNs [C] //Proc of the 16th IEEE Int Conf on Network Protocols (ICNP'08). Piscataway, NJ: IEEE, 2008: 238-247

[71] Chen B, Chan M. Mobicent: A credit-based incentive system for disruption tolerant networks [C] //Proc of the 29th Conf on Computer Communications (INFOCOM'10). Piscataway, NJ: IEEE, 2010: 875-883

[72] Lu R, Lin X, Zhu H, et al. Pi: A practical incentive protocol for delay tolerant networks [J]. IEEE Trans on Wireless Communications, 2010, 9(4): 1483-1492



Wu Yue, born in 1968. Received his PhD degree from the Department of Radio Engineering, the Southeast University, Nanjing, China in 2004. Associate professor in the School of Information Security Engineering at Shanghai Jiaotong University. Member of IEEE, member of IEEE Communications and Information Security Technical Committee, and member of the International Conference on Computer Sciences and Convergence Information Technology. His current research interests include wireless networks security, trust and security of future internet.

Li Jianhua, born in 1965. Received his PhD degree from the Department of Electronics, Shanghai Jiaotong University, China in 1998. Professor of the Department of Electronics at Shanghai Jiaotong University. Member of IEEE. His current research interests include information content analysis and networks security(lijh888@sjtu.edu.cn).

Lin Chuang, born in 1948. Received his PhD degree in computer science from Tsinghua University in 1994. Professor of the Department of Computer Science and Technology, Tsinghua University, Beijing, China. Fellow member of China Computer Federation. His current research interests include computer networks, performance evaluation, network security analysis, and Petri net theory and its applications (chlin@tsinghua.edu.cn).