移动 ad hoc 网络安全综述

易 平, 蒋嶷川, 张世永, 钟亦平
(复旦大学计算机与信息技术系, 上海 200433)

摘 要: 移动 ad hoc 网络是由移动节点自组织形成的网络, 由于其动态拓扑、无线通信的特点, 容易遭受各种安全威胁. 该文介绍了移动 ad hoc 网络安全研究的最新研究进展. 首先从传输信道、移动节点、动态拓扑、安全机制、路由协议几方面, 分析了移动 ad hoc 网络的安全弱点, 然后将移动 ad hoc 网络安全方面的研究分为三个方向: 密钥分配与管理、入侵检测、增强合作. 对每个方向内一些典型安全方案也进行了分类论述, 同时分析了各种方案的优点和缺点, 并进行了综合比较. 文中阐明了目前协议存在的一些问题并提出了相应的改进方法, 最后指出了下一步研究方向.

关键词: 计算机网络; 信息安全; 移动 ad hoc 网络; 密钥管理; 入侵检测; 增强合作
中图分类号: TP393 文献标识码: A 文章编号: 0372-2112 (2005) 05-0893-07

A Survey of Security for Mobile Ad Hoc Networks

YI Ping, JIANG Yi-chuan, ZHANG Shi-yong, ZHONG Yi-ping
(*Department of Computing and Information Technology Fudan University, Shanghai 200433, China*)

Abstract: In resent years, mobile ad hoc networks are a new emerging field with its potential applications in extremely unpredictable and dynamic environments. However, it is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative routing algorithms. The article surveys the state of the art in security for mobile ad hoc networks. Firstly, we analyze various possible threats to security in mobile ad hoc networks. Secondly, we illustrate representative solutions to deal with those threats, including key management, intrusion detection and cooperation enforcement. We also make a comparison and discussion of their respective merits and faults, and propose some ways to fix these problems. Finally, we also present the challenges which are still worth to further research in the area.

Key words: network; security; mobile ad hoc networks; key management; intrusion detection; cooperation enforcement

1 引言

移动 ad hoc 网络作为一种新型的移动多跳无线网络, 与传统的无线网络有很大不同, 它不依赖于任何固定的基础设施和管理中心, 而是通过传输范围有限的移动节点间的相互协作和自我组织来保持网络连接和实现数据的传递. 移动 ad hoc 网络的独特的结构, 从而产生了一些突出的特点[1]: 动态的拓扑结构、有限的资源、多跳的通信、脆弱的网络安全.

传统网络中, 主机之间的连接是固定的, 网络采用层次化的体系结构, 并具有稳定的拓扑. 传统网络提供了多种服务, 包括路由器服务、命名服务、目录服务等, 并且在此基础上实现了相关的安全策略, 如加密、认证、访问控制和权限管理、防火墙等. 而在移动 ad hoc 网络中没有基站或中心节点, 所有节点都是移动的, 网络的拓扑结构动态变化. 并且节点间通过无线信道相连, 没有专门的路由器, 节点自身同时需要充当路由器, 也没有命名服务、目录服务等网络功能. 两者的区别导致了在传统网络中能够较好工作的安全机制不再适用于移动 ad hoc 网络. 因此, 移动 ad hoc 网络比固定网络更容易遭受各种安全的威胁, 如窃听、伪造身份、重放、篡改报文和拒绝服务等等.

本文首先分析了移动 ad hoc 网络的安全弱点, 然后综述了现行的各种解决方法, 并指出了各种方案的优点和缺点.

2 移动 ad hoc 网络的安全弱点

2.1 传输信道方面

移动 ad hoc 网络采用无线信号作为传输媒介, 其信息在空中传输, 无需像有线网络一样, 要切割通信电缆并搭接才能偷听, 任何人都可接收, 所以容易被敌方窃听. 无线信道又容易遭受敌方的干扰与注入假报文.

2.2 移动节点方面

因为节点是自主移动的, 不像固定网络节点可以放在安全的房间内, 特别是当移动 ad hoc 网络布置于战场时, 其节点本身的安全性是十分脆弱的. 节点移动时可能落入敌手, 节点内的密钥、报文等信息都会被破获, 然后节点又可能以正常的

收稿日期: 2004-08-19; 修回日期: 2005-01-23
基金项目: 国家 863 计划信息安全技术主题资助项目(No. 2003AA148010); "十五"国家科技攻关计划信息安全资助项目(No. 2002DA103A03-07)

面目重新加入网络,用来获取秘密和破坏网络的正常功能.因此,移动 ad hoc 网络不仅要防范外部的入侵,而且要对付内部节点的攻击.

2.3 动态的拓扑

移动 ad hoc 网络中节点的位置是不固定的,可随时移动,造成网络的拓扑不断变化.一条正确的路由可能由于目的节点移动到通信范围之外而不可达,也可能由于路由途经的中间节点移走而中断.因此,难于区别一条错误的路由是因为节点是移动造成的还是虚假路由信息形成的.由于节点的移动性,在某处被识别的攻击者移动到新的地点,改变标识后,它可重新加入网络.另外由于动态的拓扑,网络没有边界,防火墙也无法应用.

2.4 安全机制方面

在传统的公钥密码体制中,用户采用加密、数字签名、报文鉴别码等技术来实现信息的机密性、完整性、不可抵赖性等安全服务.然而它需要一个信任的认证中心来提供密钥管理服务.但在移动 ad hoc 网络中不允许存在单一的认证中心,否则不仅单个认证中心的崩溃将造成整个网络无法获得认证,而且更为严重的是,被攻破认证中心的私钥可能会泄露给攻击者,攻击者可以使用其私钥来签发错误的证书,假冒网络中任一个移动节点,或废除所有合法的证书,致使网络完全失去了安全性.若通过备份认证中心的方法虽然提高了抗毁性,但也增加了被攻击的目标,任一个认证中心被攻破,则整个网络就失去了安全性.

2.5 路由协议方面

路由协议的实现也是一个安全的弱点,路由算法都假定网络中所有节点是相互合作的,共同去完成网络信息的传递.如果某些节点为节省本身的资源而停止转发数据,这就会影响整个网络性能.更可怕的是参与到网络中的攻击者专门广播假的路由信息,或故意散布大量的无用数据包,从而导致整个网络的崩溃.

3 密钥管理

由于移动 ad hoc 网络具有自组织和动态拓扑的特性,使得在固定网络中常用的密钥管理手段无法在 ad hoc 网络中应用,例如: Certification Authority (CA) 或 Key Distribution Center (KDC) 就无法在移动 ad hoc 网络应用,使用这些设施其一容易导致单点失败和拒绝服务,即该设施由于敌方攻击而失灵了,整个网络就不能正常运转了,其二由于无线多跳通信误码率高和网络拓扑动态变化,会大大降低服务的成功率,延长服务时间,其三,容易导致网络拥塞,本来就不充足的传输带宽,网络中各节点还都要到该节点去认证.文献[2]模拟试验了集中认证、分布认证、本地认证三种方法的可扩展性、健壮性和有效性,其中使用集中 CA 的认证性能最差,特别当网络节点数量增加、网络负载上升时,集中认证的性能明显下降.通过实验证实了集中 CA 的方法在移动 ad hoc 网络中无法应用,但是近来提出的许多 ad hoc 路由安全协议,都要求事先存在或预先分配共享密钥或公开密钥,这就要求提供适应于移动 ad hoc 网络的密钥管理手段.下面首先介绍两种具有代表性的密钥管理方案,其次介绍其他几种解决的方案.

3.1 分布式的密钥管理

Lidong Zhou 和 Zygmunt J. Haas 提出一种基于门限密码理论,实现分布式的 CA 来进行密钥管理的算法[3].所谓 (n, k) 门限密码,即将密钥分为 n 份子密钥,其中任意 k 份子密钥联合起来即可完成加解密操作,而当份数小于 k 时则不能执行加解密操作.该算法利用门限密码的特点,网络初始化时,由集中的 CA 将网络系统私钥分为 n 份,指定 n 个节点拥有,这 n 个节点就充当了分布式的 CA.当需要 CA 来发布证书时,这 n 个节点中的任意 k 个合作生成一份有效的证书.当新节点加入网络时,就可向这 n 个节点中的任意 k 个节点提出证书申请,每个节点返回部分签名证书,合起来就形成了一份完整的证书.为了防止 *mobile adversaries*[4] 攻击,即敌方攻破一个节点后转向下个节点,这样经过一段时间后会攻破很多节点,甚至达到 k 节点,采取共享更新算法,即从老的 n 份私钥中生成新的 n 份私钥.因为新的私钥独立于老私钥,所以只要更新周期合适,就能对抗 mobile adversaries 攻击.文献[5]设计了该算法的具体实现细节,并用网络模拟器检测其算法的性能.该算法的优点是将单一的 CA 服务分散到 n 个节点中去,有效地防止了单点失败,提高了网络的健壮性,只要被攻陷节点少于 k 个,整个网络仍然是安全的.缺点有两点,其一是增加了计算负载,需要指定 n 个节点充当 CA 服务器,签发证书,增加了这 n 个节点的计算负载.其二是增加了网络传输负载,因为在集中式的 CA 中,节点只需与一个 CA 联系返回一份证书,而分布式 CA,节点需要到 k 个持有系统私钥的节点去申请,返回 k 份证书,而这些节点可能遍布于网络各处,需要多跳通信才能达到,至少与 k 个节点都成功通信时,才能完成.熊焰等人[6]对门限加密算法进行了改进,提出了一种多跳步加密签名函数签名的方法,将移动密码学与门限加密分布式认证相结合,用以提高门限加密的安全性.

Jiejun Kong 等人提出了一个类似的方案[7],改进了上述方案,增强了可用性.网络系统初始化时,由集中的 CA 将系统私钥分为 k 份授权给 k 个节点,然后由这 k 个节点联合起来继续将私钥授与网络中其余各节点.这样,系统私钥不只分为 n 份由 n 个节点持有,而是网络中每个节点都持有一份系统私钥.节点加入网络时,只要向周围 k 个邻居节点提出申请,即可获得证书.该方案将分布式认证转化为本地认证,提高可用性,降低了网络负载.该方案还具有扩展性,无论网络扩大或缩小都可适用.文献[8]也提出了类似的方案,只是增加了邻居监视功能,每个节点的周围的邻居不仅联合颁发证书,而且负责监视其的行为.如果该节点有恶意行为,证书到期后将不能申请到证书.此类方案的缺点是每个节点都拥有私钥,随着系统私钥的拥有节点数目的增加,对其管理和维护的费用也在增加.

3.2 自组织的密钥管理

Jearr Pierre Hubaux 等人首先在文献[9]中提出该算法并进行了概要介绍,Srdjan Capkun 等有在文献[10]中对该算法进行了详细论述并进行了模拟实验.该算法不需要公认的 CA 来发布证书,节点自己发布并维护证书,类似于 PGP 算法,用

户通过证书链来实现认证. 与 PGP 算法不同的是, 用户证书是靠用户自己分配并分布存储于每个用户自身节点之中, 而不是存储于认证服务器之中. 在该算法分为两步, 第一步每个用户在本节点构筑一个证书数据库, 用户首先生成本节点的公钥和私钥, 然后发布自己的证书并收集其他节点的证书, 最后按一定算法形成本地证书数据库. 第二步当两个用户需要相互认证时, 他们合并他们各自拥有的证书数据库形成一张认证路径图, 并试图从该图中发现一条认证链路. 如果发现一条认证路径, 则认证成功, 否则认证失败.

本算法的优点在于完全不需要 CA 来发布和维护证书, 防止了单点失败. 缺点有三点, 其一, 由于没有 CA 来验证身份, 任何能发布证书的节点均能加入网络, 攻击者可假冒合法节点或编造节点标识发布证书加入网络. 其二因为节点存储证书信息不完全, 不能保证 100% 认证, 其认证成功率与证书数据库形成密切相关. 其三算法的扩展性不好, 当网络扩大时, 证书数据库的形成、维护和认证的花费会明显增加.

3.3　两种密钥管理方案的比较和分析

分布式和自组织的密钥管理是较为典型的两种类密钥管理方案, 表 1 对这两种方案进行了比较. 它们的特点为:

表 1　分布式密钥管理与自组织密钥管理的比较

算法分类	分布式的密钥管理	自组织的密钥管理
理论基础	门限密码	PGP 技术
前提条件	信任实体生成系统公钥和私钥, 将公钥发送给所有节点, 将私钥分为 n 份授与 n 个节点持有	各节点通过证书交换, 形成本地证书数据库
证书管理	由 n 个持有系统私钥的节点中 k 个联合颁发并管理	由节点自己生成并管理
认证方式	通过系统公钥校验节点的证书	通过证书链
优势	防止了单点失败	防止了单点失败
劣势	增加了计算负载和网络流量	攻击者可假冒合法节点发布证书、算法的扩展性不好

上述各种密钥管理方案都考虑到移动 ad hoc 网络自组织无中心的特点, 为了防止单点失败, 设计上采取各种方法代替集中的 CA, 如采用分布式的 CA、自组织的方法.

在分布式的密钥管理中, 将集中的 CA 分配到 n 个节点中去, 由 n 个节点中的 k 个节点合作签发证书. 节点必须与 k 个节点都建立通信并成功申请到 k 份证书才能合成一份有效的证书. 这 k 个节点可能分布在网络各处, 需要多跳通信才能到达. 如果与 k 个节点中任意一个节点通信失败或返回证书有误, 则无法合成证书, 整个申请失败, 必须再找 k 个节点重新开始申请. 从上述过程可以看出, 分布式的 CA 虽然防止了单点失败, 但也增加了网络负载, 延长了服务时间, 降低了申请证书的成功率.

在自组织的密钥管理方案中, 每个节点负责颁发和维护自己的证书, 由于没有 CA 来验证身份, 任何能发布证书的节点均能加入网络, 攻击者可假冒或编造节点标识发布证书加入网络. 解决该问题可采用, 首先通过检测证书的一致性来发现假冒行为, 如同一份证书代表了两个节点, 然后通过邻居监视来确定假冒者, 从而将其排除出网络.

3.4　其他一些密钥管理方案

Frank Stajano 和 Ross Anderson 提出复活鸭子的安全模式[11], 鸭子破壳而出之后, 它会把它见到的第一个移动物体作为它的母亲. 与此类似, 节点初始化时, 它将第一个发给它密钥的节点作为它的拥有者, 它只接受拥有者的控制. 这种控制一直保持到节点死亡, 节点重新复活后可产生新的拥有者. 这样就形成了一种树状的密钥分发与管理模式. 这种方案适用于低价的嵌入式设备, 如 sensor networks. 它的优点在于简单, 不需复杂的计算. 缺点是缺乏灵活性, 如果一个节点失灵了, 它所带的所有子节点和孙节点都将无法进行安全通信.

N. Asokan 和 Philip Ginzboorg 提出一种基于口令的密钥管理方案[12]. 该方案针对一群带着笔记本电脑的人在一间会议室里开会, 在没有任何安全架构的情况下, 建立各移动电脑之间的安全信息交换. 它的基本思想是从一个弱的口令字, 通过多方 Diffie-Hellman 密钥交换, 最终生成用于信息安全交换的密钥. 该方案也不需要 CA 或 KDC, 但只适用于小范围, 扩展性不好.

Zheng Yan 提出基于外部 CA 的密钥管理[13]. 外部 CA 可设立在卫星或飞机上, 采用广播加密技术来发送信息. 网络中节点嵌入专用硬件来实现密钥的存储、加密和解密操作. 该方案对硬件要求过高, 适用面不广.

Srdjan Capkun 提出通过节点的移动来建立交换密钥的方案[14]. 它认为节点的移动性能够帮助网络安全的实现. 因为移动 ad hoc 网络中节点在频繁移动中, 所以任意两节点有机会相互见面, 当它们接近到一定程度时, 通过安全旁路(如红外信道)相互交换密钥, 以此种方式实现密钥的建立和维护. 该方案也不需要 CA, 但分配密钥需要耗费一定的时间且受到节点移动模式、分布范围等因素的影响, 文献[15~17]提出组密钥管理, 它们共同的特点是将网络分为多个组, 组头负责组内各节点的密钥管理. 该方案在一定程度上防止了单点失败, 但由于节点的移动性, 组头和组员管理十分复杂.

4　入侵检测

从第 2 节可以看出, 无线信道、动态拓扑、合作的路由算法、缺乏集中的监控等都使得移动 ad hoc 网络安全更加脆弱, 特别是移动节点缺乏物理保护, 容易被偷窃、捕获, 落入敌手后重新加入网络, 导致攻击从内部产生. 而采用密码学理论的网络安全方案无法对抗此类攻击. 此外, 网络安全的发展史告诉我们没有 100% 的安全方案, 无论多么安全的方案都可能存在这样或那样的漏洞. 因此, 入侵检测就理应成为安全方案之后的第二道防护墙.

4.1　入侵检测方案

Yongguang Zhang 和 Weeke Lee 提出了一个基于 agent 的分布式协作入侵检测方案[18]. 在该方案中 IDS agent 运行于网络中每一个节点上, 拥有六大功能模块, 分为数据收集、本地检测、合作检测、本地入侵响应、全局入侵响应、安全通信. 图 1 为 IDS agent 由六大功能模块组成的示意图. 其过程为首先执行本地数据收集和检测. 如果本地节点能够确定入侵已发生,

则直接告警. 如果只是怀疑有入侵行为, 本地节点能够激发多节点的协作检测, 进一步是否发生了入侵. 如果确定有入侵则激发全网的入侵响应. 同时提出了一个检测路由进攻的异常检测模型, 通过提取正常网络运行时的数据, 进行分类训练, 实现对路由入侵的检测. 为了提高检测效率, 入侵检测并不局限于网络层, 而是多层综合检测.

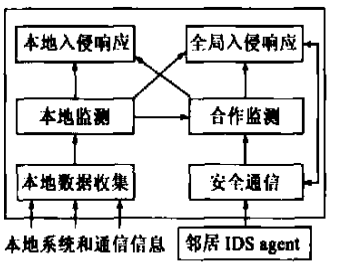

图 1 IDS agent组成

上述方案的优势有两点, 其一, 提出了分布式协作入侵检测的架构, 利用分布在每个节点的 IDS agent 独立完成本地检测, 合作完成全局检测, 适合于移动 ad hoc 网络自组织的特点. 其二, 采用多层综合入侵检测, 提高了检测效率. 缺点也有两点, 其一, 采用异常检测模式, 要事先采样数据进行训练, 不适合于移动 ad hoc 网络多变的应用场合. 其二, 每个节点都运行有 agent, 占用过多的内存和计算资源.

Oleg Kachirski 和 Ratan Guha 提出了基于移动 agent 的入侵检测方案[19]. 他们认为 Yongguan Zhang 的方案每个节点都有 agent, 过于占用网络资源, 为了节省资源, 只是在某些节点上驻留有监视网络的 agent, 并且 agent 的数量可按要求进行增减.

Chirr Yang Tseng 等有提出了基于规范(specificationr based) 入侵检测方案[20]. 该方案利用分布在网络中的监测点, 合作监视在 AODV 路由查询过程中, 被监视节点是否按路由规范进行操作. 如果发现不一致则报警. 检测过程为, 监听节点对查询报文的处理过程, 记录下来形成转发表和操作树, 然后用规范形成的有限状态机进行检查, 输出为正常状态、怀疑状态、入侵状态三种结果, 再分别进行不同的处理. 该方案优点在于采用了基于规范入侵检测, 既不需要事先提取入侵行为特征, 也不需要数据进行训练, 有较高的检测率和较低的误报率. 缺点为, 占用节点较多的计算资源, 也未用实验进行验证.

易平等人[21]提出一种基于时间自动机的入侵检测算法. 其算法为, 将整个网络划分为一个个区域, 每个区域随机选出一个节点作为监视节点. 然后, 按照路由协议构筑节点正常行为和入侵行为的时间自动机, 监视节点收集其邻居节点的行为信息, 利用时间自动机分析节点的行为, 确定入侵者. 本算法不需要事先进行数据训练并能够实时检测入侵行为.

4.2 入侵检测方案比较与分析

表 2 对四种入侵检测方案进行比较, 它们具有以下特点:

表2 四种入侵检测方案的比较

协议名称	基于 agent 的分布式协作入侵检测	基于移动 agent 的入侵检测	基于规范入侵检测	基于时间自动机的入侵检测
执行者	驻留节点上的 agent	各种移动 agent	每个节点	每个区域一个监视节点
检测模式	异常检测	异常检测	基于规范的检测	基于时间自动机的检测
检测方法	分布式监测、邻居监视	分布式监测、邻居监视	分布式监测、邻居监视	分布式监测
优点	各 agent 合作监测与响应	可动态调整 agent 数量, 降低对资源的消耗	不需要数据进行训练, 较高的检测率	实时检测, 不需要事先进行数据训练
缺点	占用过多资源	协议比较复杂	计算量大	占用监视节点资源过多

因为没有统一的监测点, 任何节点收集的信息是不完全的, 所以它们都采用分布式邻居监测, 协同检测的方法.

现行的入侵检测的架构为使用 agent 作为入侵检测的执行者, agent 驻留并运行于网络中每一个节点内, 分布式的监视网络状况, 信息共享, 合作检测入侵行为. 这种架构对于入侵检测来说是较为有效的, 但未充分考虑到网络带宽和节点计算资源有限的特点, 也许会过多占用节点资源. 我们认为在设计上应充分考虑到网络资源有限的特点, 降低其对资源的要求, 不必每一个节点都运行 agent, 可采用两种方式, 一种是分区域, 每个区域使用一个 agent 负责监控. 另一种是使用少量移动 agent 散布于网络各处, 如发现异常, 可向异常处移动, 进一步检测以确定是网络故障还是入侵行为.

5 增强合作的机制

移动 ad hoc 网络不像固定网络, 有专门的路由器和交换机来实现网络通信功能, 它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, 因此, 每一个节点要承担起网络路由和包交换的功能. 但在移动 ad hoc 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, 这就是移动 ad hoc 网络节点中的自私行为. 这种自私行为对网络性能的影响不可低估. 在文献[22] 中研究了在 DSR 协议环境下, 自私行为对整个网络吞吐量和传输延迟的影响程度, 模拟试验结果显示, 既使整个网络节点中只有一小部分节点产生自私行为, 也造成网络性能的严重下降. 自私行为和攻击者的蓄意破坏行为虽然在出发点上有所不同, 前者是为了保存和节省资源, 后者是为了破坏网络的正常功能, 但它们所造成后果相同, 都会严重影响网络性能, 所以如何对付自私行为, 增强网络节点的合作机制也应该是网络安全的一个研究方向. 在对付自私行为, 增强合作方面的论文主要分为两类, 第一类是基于激励的机制, 其基本原理为节点转发报文后, 即可得筹码或虚拟货币用于自己报文的发送. 第二类是基于惩罚的机制. 邻居相互监视, 发现不良行为的节点, 则将被排除出网络. 下面首先介绍这两类算法, 然后进行分析比较.

5.1 基于激励的机制

Levente Buttyan 和 Jearr Pierre Hubaux 在文献[23] 中, 提出了为了增强合作, 网络中的节点必须被鼓励转发报文, 但又不能滥发报文增加网络负载. 为此, 设计两种虚拟货币的解决方案. 一种是钱包方式, 需要发送报文的节点估计报文所经过的节点与所需要的花费, 将计算所得的虚拟货币数放入钱包, 钱包随报文一起发送, 途经中间的每一个转发节点从报文的钱

包中取出一定量的货币作为转发该报文的费用, 然后转发该报文, 直至到达目的节点. 这样每一个节点只有尽力转发其它节点的报文才能获得足够的货币以发送自己的报文, 从而起到一种激励合作的作用. 该方式的优点是可以防止节点滥发报文增加网络负载, 缺点有两点, 其一是源节点需要能够精确计算报文转发的费用, 如果放入钱包的费用小于实际费用报文就会被中途抛弃, 在拓扑频繁变化的移动 ad hoc 网络中估计报文所经过的节点和费用不是一件容易的事. 其二是每个报文都要携带货币, 用于中途付给转发节点, 增加了报文的长度. 另一种解决方案是购买方式, 每一个节点转发报文时, 从上游节点买下该报文, 加上本节点的转发费用后, 又把报文卖给下游节点, 依此转发直至目标节点. 该方式的优点在于无需事先估计路途转发费用, 全部费用由收方支付, 缺点为由于发方无需支付发送费用, 攻击者可滥发报文, 造成网络负载过重直至崩溃.

Levente Buttyan and Jearr Pierre Hubaux 在文献[24]中, 提出了一种基于筹码的方案. 该方案要求每个节点都安装一个防止用户修改的硬件叫安全卡. 该卡内有筹码累加器, 每当节点转发一个报文时, 该计数器就增加一个筹码值. 当节点需要发送自己的报文时, 就要将卡内筹码累加器减去 n 个筹码, n 代表报文要经过 n 个节点转发才能到达目的节点. 如果卡内筹码数小于 n, 则节点不能发送该报文. 这意味着节点要发送自己的报文, 首先必须转发其他报文, 以积累足够筹码才行. 该方案并不是用于阻止节点的不良行为, 它只是鼓励节点转发报文, 确保节点不能从不良行为中获益, 如果节点不转发报文, 它就没有筹码用于发送自己的报文. 其优点是算法简单, 只需要一个筹码累加器即可. 缺点为两点, 其一需要硬件支持. 其二不论报文长短, 转发时均增加一个筹码. 也许转发一个长报文花费相当于转发几个短报文的花费.

Sheng Zhong 等人认为在每个节点安装额外硬件是不现实的, 他们提出一个不需要在节点安装硬件的类似方案 sprite[25]. 首先设立一个集中的结算中心来存储每个节点的筹码数, 当节点发送一个报文时, 所有中间转发节点和目的节点都记下这个报文的收据, 然后与结算中心联系, 上传该收据, 结算中心根据报文转发情况付给参与转发节点相应的筹码数, 同时扣去发送节点总计筹码数. 结算时, 按照博弈理论来计算支付方案, 促使节点能够尽力诚实履行网络功能. 该方案的优点在于用统一的结算中心取代了各节点的硬件累加器, 无需在每个节点安装硬件卡. 缺点也在集中的结算中心, 若有网内节点承担则会造成过重的通信负载和单点失败. 该算法提出使用网外设备, 将结算中心放在网外, 通过移动通信中的 GPRS 来实现与结算中心的联系. 这既增加了硬件设备, 又限制了网络的应用场合.

该类方案有三个特点, 其一使用虚拟货币或筹码作为转发的回报. 其二使用硬件设备来存储筹码值, 以防用户修改. 其三采用博弈理论来促使节点合作.

5.2　基于惩罚的机制

Sergio Marti 等人提出通过 watchdog 和 pathrater 两种技术来对付不良节点的方案[26]. Watchdog 和 pathrater 运行于每一个节点上, Watchdog 负责监视邻居节点行为, 发现不良行为的节点. Pathrater 负责选择避开不良节点的路径. 该方案只是实现如何发现并避开不良节点, 并不孤立和惩罚不良节点. 不良节点仍然能够正常收发报文, 反而为其免除了正常的转发流量, 客观上奖赏了不良节点.

Sonja Buchegger 和 Jearr Yves Le Boudec 在文献[27]中提出一种利用邻居监视来发现并排除不良节点的算法 CONFIDANT. 它依靠运行于每个节点上的四个程序来实现其功能. 邻居监视器: 用于发现不履行正常网络功能的邻居节点. 信任管理: 用于发送、接收、管理其它节点的报警信息. 名誉系统: 标记并管理其它节点的名誉值. 路径管理: 路径选择时避开并孤立不良节点. 每个节点监视其邻居的行为, 如果发现不良行为则提交给名誉系统并给发送报警信息给其它节点. 名誉系统为每个节点设立一个名誉值, 当有不良行为报告时, 减少其名誉分值. 当某个节点的名誉值低于标准时, 则提交路径管理. 路径管理将删除与不良节点有关的路径存储信息, 并拒绝其路由申请. 该方案的优点是不仅发现不良节点, 而且用孤立方法来惩罚它们, 以促使它们履行正常网络功能.

Pietro Michiardi 和 Refik Molva 也提出一种通过监视技术和名誉机制来激励合作的算法 CORE[28]. 网络中每一个节点监视其邻居的行为, 观察其是否履行正常网络功能, 如转发报文、处理路由请求等. 如果观察结果与预期的一致, 则增加该节点的名誉分值, 否则减去一定分值. 节点通过一个综合公式来计算某个节点总名誉分值, 公式的参数有直接观察结果、其他节点的报告等, 还考虑到通信线路状况和以前的名誉分值. 当某个节点出现自私行为或其他恶意行为时, 其名誉分值会逐渐下降, 当低于某个值时, 其他节点会拒绝为其提供服务, 那样就会将自私节点排除出网络.

这类方案有三个特点, 其一采用本地监视技术来发现不良节点. 其二通过名誉值来评价节点. 其三通过惩罚不良节点来促使节点合作.

5.3　两类算法的比较与分析

为了实现共同的目标, 限制节点的自私行为, 增强节点合作, 提高网络性能, 上述两类算法采用完全不同的方法, 一种是激励的方法, 另一种是惩罚的方法, 表 3 对两类算法进行了比较. 它们具有以下特点:

表 3　基于激励的机制算法与基于惩罚的机制算法的比较

算法分类	基于激励的机制	基于惩罚的机制
理论基础	博弈论	
实现手段	虚拟货币	邻居监视
主要思想	以虚拟货币作为节点合作的奖赏, 鼓励转发报文	以被排出网络作为不合作的惩罚, 鞭策节点参与网络功能
基本原理	节点转发报文后, 即可得筹码或虚拟货币用于自己报文的发送	邻居相互监视, 发现不良行为的节点, 则将被排除出网络
优点	算法简单	纯软件实现, 无需硬件支持
缺点	需要硬件支持	邻居监视并不完全有效

基于激励的机制算法存在的主要问题是需要额外的硬件

支持其协议的执行. 前两种方案需要在每一个节点安装安全卡用来存储信息,以防用户修改,这些设备的使用会限制网络的扩展性和应用范围. 例如多个管理域的网络中用户若不同意安装安全卡,就无法运行前两种协议.

基于惩罚的机制算法中存在邻居节点监视的有效性问题. 基于惩罚的机制主要使用本地邻居监视的方法发现不良行为,但移动 ad hoc 网络具有多变的拓扑和不稳定的无线通信的特征,这使得有效检测自私节点变得十分困难. 节点可能由于线路和电源等故障而无法转发报文,被认定为自私节点.

标识的有效性问题. 移动 ad hoc 网络中节点可不断变动位置. 当在某处被邻居认定为自私的节点而被排除出网络,它可移动到新的地点,通过改变节点标识,又可重新加入网络.

6 总结与展望

由于移动 ad hoc 网络的独特结构,使得常规的安全方案无法应用,必须针对其特点设计专门的安全解决方案. 本文从密钥管理、入侵检测、增强合作几个方面介绍了应用于移动 ad hoc 网络的安全解决方案. 首先讨论了密钥管理,主要介绍了自组织的密钥管理和分布式的密钥管理两类算法,指出了其优点和缺点. 接下来说明了基于 agent 的分布式监视合作检测的入侵检测体系结构. 最后讨论了基于激励和基于惩罚的两种增强合作的机制.

移动 ad hoc 网络安全的研究是一个年轻而又迅速发展的领域,总体来说,下一步发展应包括以下几个方面:

进一步提高性能,降低算法对资源的要求. 移动 ad hoc 网络中节点本身的计算能力和电池能量都十分有限,还要参与网络交换. 网络安全作为网络正常运行的一种保障,不应该也不允许占用节点大量的资源,不能因为增加了安全措施,降低了网络性能,影响了网络的正常运行. 应该设计和采用一些对资源要求少的算法,如:使用本地认证取代分布式的认证,用对称密钥取代公开密钥等.

增强协议的可扩展性. 有些协议在节点数目较少时,性能还可以,当节点数目增加时,其性能会明显下降. 如:自组织的密钥管理当网络扩大时,证书数据库的形成、维护和认证的花费会明显增加. 算法在设计时,就应考虑到其可扩展性.

安全方案应具有自适应可调整的特性. 安全方案不应该是固定的,它应该具有自适应的性能,根据网络的资源状况调整其功能,资源充足时,功能强一些,反之则功能减少一些,也可以将一些占有资源较多的功能模块分布到一些资源多性能好的节点上去,使得整个网络负载均衡. jiejun kong 等人在这方面进行了一些研究,提出了一种自适应的安全方案[29]. 平时,利用无人飞机上的节点来实现集中的 CA 或 KDC,因为飞机上的节点资源相对充足. 战时,当无人飞机被摧毁时,集中的 CA 或 KDC 自动转化为分布式的,由 n 个移动节点承担. 虽然性能会有所降低,但仍然能保证整个网络的安全运行.

提供对组播的安全保护. 组播的应用能够有效地减少网络流量,特别适用于军事指挥网络. 现行大多数的安全方案只停留在如何保护路由信息的完整性,如何实现对单个节点的认证,没有考虑如何实现对组播的安全支持. 只有少数文献[30,31]论述了安全的组播. 对移动 ad hoc 网络环境下的安全组播的研究还很不完善,需要进一步发展.

移动 ad hoc 网络安全应该是一个综合的解决方案. 它应该融合密钥管理、路由安全、入侵检测等各方面的内容,形成一个整体的安全方案. 本人在此方面进行了一些研究,提出了基于免疫机制的安全架构[32],该架构引入免疫系统的原理,将入侵检测和主动响应结合起来,形成一个整体的安全架构.

在移动 ad hoc 网络安全的研究领域内,除了本文论述的几个主要的研究方面,还有许多新领域有待于去拓展:

(1)如何保护节点通信量和位置的信息. 通过通信量的分析能够确定网络中节点的角色,再确定节点的位置,就可将攻击指向网络的要害,如:网控中心、集中的 CA 或军事指挥网中指挥员等.

(2)各种针对中路由协议的攻击及对策. 如:wormhole[33]、rushing[34]、flooding[35]攻击等,因为移动 ad hoc 网络的复杂性,也许还存在许多新类型的攻击尚未发现.

(3)链路层和高层的安全协议的研究.

(4)如何实现网络的存取控制.

参考文献:

[1] Corson, J Macker. Mobile Ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations[S]. RFC 2501, 1999.

[2] L Buttyan, J P Hubaux. Report on a working session on security in wireless Ad Hoc networks[J]. Mobile Computing and Communications Review, 2003, 7(1): 74-94.

[3] Lidong Zhou, Zygmunt J Haas. Securing ad hoc networks[J]. IEEE Networks Special Issue on Network Security, 1999, 13(6): 24-30.

[4] R Ostrovsky, M Yung. How to withstand mobile virus attacks[A]. Proc of the 10th ACM Symposium on Principles of Distributed Computing[C]. ACM press, New York, 1991. 51-59.

[5] Seung Yi, Robin Kravets. MOCA: Mobile certificate authority for wireless Ad Hoc Networks[A]. Proc of 2nd Annual PKI Research Workshop Program (PKI 03)[C]. Gaithersburg, Maryland, April, 2003. 65-79.

[6] 熊焰, 苗付友, 张伟超, 王行甫. 移动自组网中基于多跳步加密签名函数签名的分布式认证[J]. 电子学报, 2003, 31(2): 161-165.

[7] Jiejun Kong, Petros Zerfos, et al. Providing robust and ubiquitous security support for mobile Ad-Hoc networks[A]. IEEE 9th International Conference on Network Protocols (ICNP' 01)[C]. Riverside, California, 2001. 251-260.

[8] Haiyun Luo, Jiejun Kong, et al. Self-securing Ad Hoc wireless networks[A]. Proc of the Seventh IEEE Symposium on Computers and Communications (ISCC' 02)[C]. Italy, 2002. 567-574.

[9] Jearr Pierre Hubaux, Levente Buttyan, Srdjan Capkun. The quest for security in mobile Ad Hoc networks[A]. Proc of the 2001 ACM International Symposium on Mobile ad hoc networking & computing 2001[C]. Long Beach, CA, USA, 2001. 146-155.

[10] Srdjan Capkun, Levente Nuttyan, Jearr-Pierre Hubaux. Self-organized public-key Management for mobile ad hoc networks[J]. IEEE Transactions on mobile computing, January-March, 2003, 2(1): 52-64.

[11] Frank Stajano, Ross Anderson. The resurrecting duckling: security is

sues for Ad-hoc wireless networks[A]. Proc of the 7th International Workshop on Security Protocols[C]. LNCS 1796, Springer-Verlag, Berlin Germany, April 1999. 172- 194.

[12] N Asokan, Philip Ginzboorg. Key agreement in ad hoc networks[J]. Computer Communications, 2000, 23(17): 1627- 1637.

[13] Zheng Yan. Security in Ad Hoc Networks[DB/OL]. http://citeseer.nj.nec.com/536945.html.

[14] Srdjan Capkun, Jean-Pierre Hubaux, Levente Buttyan. Mobility helps security in Ad Hoc networks[A]. The Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing[C]. Annapolis, Maryland, USA, June 1- 3, 2003. 46- 56.

[15] Tuomas Aura1, Silja Mäki. Towards a survivable security architecture for ad-hoc networks[A]. Proc of 9th International Security Protocols Workshop[C]. Cambridge, UK, 2001. 63- 73.

[16] P Dasgupta, S Gokhale. Distributed authentication for Peer to Peer networks[A]. IEEE Workshop on Security and Assurance in Ad hoc Networks[C]. Orlando, FL, January 28, 2003. 347- 353.

[17] Lakshmi Venkatraman, Dharma P Agrawal. A novel authentication scheme for Ad hoc networks[A]. Wireless Communications and Networking Confernce (WCNC 2000)[C]. Chicago, 2000. 1269- 1273.

[18] Yongguang Zhang, Wenke Lee. Intrusion detection in wireless Ad-Hoc networks[A]. Proc of The Sixth International Conference on Mobile Computing and Networking (MobiCom 2000)[C]. Boston, MA, 2000. 275- 283.

[19] Oleg Kachirski, Ratan Guha. Intrusion detection using mobile agents in wireless Ad Hoc networks[A]. IEEE Workshop on Knowledge Media Networking (KMN'02)[C]. Kyoto, JAPAN, 2002. 153- 158.

[20] Chirr-Yang Tseng, Poornima Balasubramanyam, et al. A specification-based intrusion Detection system for AODV[A]. 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03)[C]. Fairfax, VA, USA, October 2003.

[21] Ping Yi, Yiping Zhong, Shiyong Zhang. Real-time protocol analysis for detecting routing attacks in mobile Ad Hoc networks[A]. Fifth IEEE International Symposium and School on Advance Distributed Systems (ISSADS2005)[C]. Lecture Notes in Computer Science, Guadalajara, Jalisco, México, January 2005.

[22] P Michiardi, R Molva. Simulation-based analysis of security exposures in mobile ad hoc networks[A]. Proc of European wireless conference[C]. Firenze, Italy, 2002.

[23] Levente Buttyan, Jean-Pierre Hubaux. Enforcing service availability in mobile Ad-Hoc WANs[A]. Proc of the IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)[C]. Boston, MA, USA, August 2000. 87- 96.

[24] L Buttyán, J - P Hubaux. Stimulating cooperation in self-organizing mobile Ad Hoc networks[J]. Mobile Networks and Applications, 2003, 8(5): 579- 592.

[25] Sheng Zhong, Jiang Chen, Yang Richard Yang. Sprite: A Simple, Cheat-proof, Credit-based system for mobile Ad-Hoc networks[A]. Proc of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)[C]. San Francisco, CA, April 2003. 1987- 1997.

[26] Sergio Marti, T J Giuli, et al. Mitigating routing misbehavior in mobile ad hoc networks[A]. Proc of the Sixth International Conference on Mobile Computing and Networking (Mobicom2000)[C]. Boston, August 2000. 255- 265.

[27] Sonja Buchegger, Jean-Yves Le Boudec. Performance analysis of the CONFIDANT protocol: Cooperation of nodes-fairness in distributed Ad-hoc networks[A]. Proc of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC2002)[C]. EPFL Lausanne, Switzerland, 2002. 226- 236.

[28] Pietro Michiardi, Refik Molva. Core: A collaborative reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks[A]. Sixth IFIP conference on security communications and multimedia (CMS 2002)[C]. Portoroz, Slovenia, 2002. 107- 121.

[29] Jiejun Kong, Haiyun Luo, et al. Adaptive security for multilevel ad hoc networks[J]. WIRELESS COMMUNICATIONS AND MOBILE COMPUTING. Wirel Commun Mob Comput, 2002, 2(5): 533- 547.

[30] T Kaya, G Lin, et al. Secure multicast groups on Ad Hoc networks[A]. Proc of the 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03)[C]. Fairfax, VA, USA, 2003. 94- 102.

[31] Loukas Lazos, Radha Poovendran. Energy-aware secure multicast communication in Ad-hoc networks using geographic location information[A]. Proc of IEEE International Conference on Acoustics Speech and Signal Processing[C]. Hong Kong, China, 2003. 201- 204.

[32] Ping Yi, Yiping Zhong, Shiyong Zhang. An immunity- based security architecture for mobile ad hoc networks[J]. Journal of Electronics(China), accepted to appear.

[33] Y-C Hu, A Perrig, D B Johnso. Wormhole Detection in Wireless Ad Hoc Networks[R]. Technical Report TR01- 384, Department of Comrputer Science, Rice University, December 2001.

[34] Yih-Chun Hu, Adrian Perrig, David Johnson. Rushing attacks and defense in wireless Ad Hoc network routing protocols[A]. Proc of the ACM Workshop on Wireless Security (WiSe 2003)[C]. San Diego, California, U. S. A. 2003. 30- 40.

[35] 易平, 钟亦平, 张世永. 移动 ad hoc 网络中 DOS 攻击及其防御机制[J]. 计算机研究与发展, 2005. 42(4): 697- 704.

作者简介:

易　平　男, 1969 年生, 复旦大学计算机与信息技术系博士生, 1991 年毕业于南京通信工程学院计算机系, 获工学学士学位, 2003 年毕业于同济大学计算机系, 获工学硕士学位, 主要研究领域为网络安全、移动计算. E-mail: pyi_edu@yahoo.com.cn.

蒋嶷川　男, 1975 年生, 复旦大学计算机与信息技术系博士生, 2002 年毕业于北方交通大学计算机系, 获工学硕士学位, 主要研究领域为网络安全, 人工智能.