移动自组网安全技术研究

张 鹏[1] 孙 磊[2] 崔 勇[1] 韩秀峰[3]
(清华大学计算机科学与技术系 北京 100084)[1] (海军海洋测绘研究所 天津 300061)[2]
(首都经济贸易大学 北京 100070)[3]

摘 要 移动Ad Hoc网络由于其动态拓扑和无线通信等特点,容易受到安全威胁。将现有的移动Ad Hoc网络的网络安全技术分为入侵检测与防范、安全路由协议技术、架构模型技术、密钥技术和其他技术。其中,入侵检测与防范主要基于移动Ad Hoc网络的特点,在一定数学模型的基础上对于网络节点的行为进行分析和监测,以保证整个移动网络的网络安全。安全路由协议技术包括全新的安全路由协议技术和现有路由协议的安全化改进技术。密钥技术主要是基于移动Ad Hoc网络的特点对现有密钥技术进行改造。对上述移动Ad Hoc网络的网络安全技术分别进行了介绍和分析。

关键词 移动自组织网络,动态性,入侵检测与防范,安全路由协议,密钥
中图法分类号 TP301 **文献标识码** A

Review of Security Techniques for Mobile Ad Hoc Networks

ZHANG Peng[1] SUN Lei[2] CUI Yong[1] HAN Xiu-feng[3]
(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)[1]
(Navy Marine Charting Institute, Tianjin 300061, China)[2]
(Financial College, Capital University of Ecnomics and Business, Beijing 100070, China)[3]

Abstract Mobile Ad Hoc networks are particularly vulnerable due to their features of dynamic changing topology, and wireless communication. Current security techniques for mobile Ad Hoc networks are divided into five categories: intrusion detection, securing routing protocols, architecture and models, key management techniques and others. Using intrusion detection, nodes' behaviors were analyzed and detected based on particular mathematics modules. Securing routing protocols include novel securing routing protocols and security enhancements of current routing protocols. The security techniques were introduced and analyzed.

Keywords Mobile ad hoc network, Dynamic, Intrusion detection, Securing routing protocols, Key

1 引言

随着社会的发展,人们对于移动通信的需求日益增长,移动通信技术迅猛发展,移动自组网技术应运而生。移动自组网,又称移动Ad Hoc网络,是不依赖于任何固定基础设施的移动节点的动态联合体[1],其中每个节点动态发现与之通信的其他节点[2]。移动Ad Hoc网络与传统计算机网络相比,其主要特点在于无稳定的拓扑结构、节点离散、无线通信、能量有限。正是基于这一点,移动自组网作为一种不需要基础设施支持的直接通信形式,在很多领域得到广泛的应用,例如军事应用、紧急救助、灾难援助、医疗应用、电子商务[3]等。

计算机网络自产生之初就伴随着网络安全的问题,传统网络在层次化结构和拓扑稳定的基础上实现了一系列安全策略,例如加密、认证等[4]。而移动Ad Hoc网络具有自组织性、无线性、离散性、动态性、能量有限的特性,所以现有网络安全技术在移动Ad Hoc网络中通常不能适用[5]。另外,移动Ad Hoc网络节点在不安全的环境中使用共享的无线介质,节点动态重组,节点物理保护有限,因此容易受到各种网络攻击[6]。因此,移动Ad Hoc网络的网络安全是一个很大的挑战。

学者对于移动Ad Hoc网络的网络安全进行了深入的研究。本文就移动Ad Hoc网络安全技术进行综述,分析和比较现有的多种移动Ad Hoc网络安全技术,并对未来的研究做出展望。根据移动Ad Hoc网络安全技术所针对的安全威胁,将现有的移动Ad Hoc网络的网络安全技术分为入侵检测与防范、安全路由协议技术、密钥技术、架构模型技术和其他技术。

本文第2节介绍入侵检测与防范,该部分的研究热点在

到稿日期:2008-08-29 返修日期:2008-11-02 本文受国家自然科学基金(No. 60403035),国家高技术研究发展计划(863)项目,国家重点基础研究计划(973)项目(No. 2007CB307105,2007CB307100)资助。

张 鹏(1981—),男,硕士,主要研究领域为Ad Hoc网络、移动通信和XML数据库,E-mail:zhangp@tsinghua.org.cn;孙 磊(1981—),男,硕士,工程师,主要研究领域为计算机网络、水声工程;崔 勇(1976—),男,博士,副教授,主要研究领域为计算机网络体系结构、无线网络;韩秀峰(1981—),女,主要研究领域为金融数据分析、移动计算和信息处理。

于提出一种适于入侵检测与防范的数学模型；第 3 节介绍安全路由协议技术，该部分的研究热点在于提出一种支持网络安全的路由协议；第 4 节介绍密钥技术，该部分的研究热点在于结合移动 Ad Hoc 网络的特点设计密钥方案；第 5 节介绍其他技术；第 6 节对于各种技术进行比较分析；在现有各种技术的基础上，最后就未来移动自组网安全技术的发展提出展望。

2 入侵检测与防范

入侵检测与防范主要基于移动 Ad Hoc 网络的特点，在一定数学模型的基础上对于网络节点的行为进行分析和检测，以保证整个移动网络的网络安全。该类方法的关键在于基于移动 Ad Hoc 网络的离散性和动态性的特点建立用于网络检测的特定数学模型。有些入侵检测与防范技术主要针对各个移动节点的行为进行检测，而有些入侵检测与防范技术则主要针对由移动节点所构成的整体系统的行为进行检测，即节点级的入侵检测与防范、系统级的入侵检测与防范。

2.1 节点级的入侵检测与防范

该类方法主要基于节点行为的分析，判断节点是否为恶意节点，从而保障移动 Ad Hoc 网络的网络安全。该方法的关键在于基于适宜的数学模型对于节点行为进行分析。学者提出了基于纳什平衡等式的博弈分析技术、基于图论的关键节点探测技术，以及基于隐式马尔可夫模型的侵入探测技术等等。

为了防止移动 Ad Hoc 网络中具有合法标识符的攻击者的侵入，文献[7]采用博弈分析技术，基于纳什平衡等式识别攻击者。该文献提出，纳什平衡(Nash equilibrium)方案表明，节点对于相对节点提供的帮助不应当多于相对节点对该节点提供的帮助，这样的节点被称为自私性节点(selfish node)。该文献将节点之间的相互作用定义为安全路由和包转发的博弈，并使用一些变量进行描述，其中参与者是指网络中用户的数量，定义为 N；类型是指每个节点 $i\in N$ 均具有类型 $\theta i\in\Theta$，其中 $\Theta=\{$自私性，攻击性$\}$，N_s 代表自私性节点的集合，并且 $N_m=N-N_s$ 代表内部攻击者的集合；成本是指对于每个节点 $i\in N$ 而言，传送包需要花费成本 C_i；收益是指对于每个节点 $i\in Ns$ 而言，如果从该节点发送的包能够成功传送到目的地，其获得收益 g_i；工具对于每个节点 $i\in N$ 而言，$S_i(t_f)$代表节点 i 在时间 t 内成功传送的包的数量，$F_i(j,t_f)$ 代表节点 i 在时间 t 内转发给节点 j 的包的数量，并且存在等式：$F_i(t_f)=\Sigma_{j\in N}F_i(j,t_f)$。另外，$T_i(t_f)$代表节点 i 在时间 t_f 内需要传送的包的数量，$W_j(i,t_f)$代表节点 i 在时间 t_f 内引发的向节点 j 的无用包的数量，基于纳什平衡方案，该工具被定义为对于任何自私性节点 $i\in N_s$ 而言，其目标在于最大化：

$$U_i^s(t_f)=\frac{S_i(t_f)g_i-F_i(t_f)c_i}{T_i(t_f)} \tag{1}$$

对于攻击者而言，其目标在于最大化：

$$U_j^m(t_f)=\frac{1}{t_f}\sum_{i\in N_s}(W_j(i,t_f)+F_i(j,t_f))c_i-F_j(t_f)c_j \tag{2}$$

式(1)中，分子代表自私性节点获得的纯利益，分母代表节点 i 需要发送的包的总数。式(2)代表节点 j 对于其他节点造成的纯损害(浪费自私性节点的时间或者能量等等)。综上所述，该文献中的方法模拟自私性节点间的协作，适用于防范内部攻击者(即具有合法标识符的攻击者)的侵入。该技术可以高效地防止攻击，但是运算的时间复杂度较高，会耗费较高的能量。

上述博弈分析技术基于纳什平衡等式，有学者提出了基于其他数学模型的节点级入侵检测与防范技术：基于隐式马尔可夫模型的侵入探测技术。为了解决入侵检测的问题，文献[8]提出使用隐式马尔可夫模型(HMM)基于相关数据的观察(系统参数的变化、错误频率等)预测潜在的攻击。受到观察的行为用统计量和统计模型描述。统计量是代表一定时期内积聚的定量测量的变量。使用统计模型从审计数据记录中获得的观察资料来分析偏离标准状态的情况并且触发侵入状态标识。隐式马尔可夫模型使用原始数据和连续性的配置信息进行训练，主要包括下述步骤：首先，测量从侵入标识分析得出或者逻辑推导得出的观察状态，该标识是分布在整个系统中的测试点；然后，根据隐式状态，使用多元高斯模型或者其他模型估算瞬时观察的可能性矩阵；接着，通过将一个或者多个组件的同时行为聚簇在一起，估算隐式状态；最后，使用获得的知识或随机数据，估算隐式状态变换可能性矩阵。在隐式马尔可夫模型得到训练之后，当其对每个有效的观察结果进行检查和分类的时候，其首先输入生命周期状态。接着，该模型确定是将该观察结果加入到配置文件中，还是丢弃，或是将该观察结果标记为未分类。未分类的观察结果未来被检测以分类。也就是说，该技术针对 CPU 行为、系统呼叫行为、系统处理行为，网络行为和会话行为设定了配置训练器。所有这些配置与特定用户的行为紧密相关，根据这些数据可以对非法侵入进行探测。综上所述，该技术基于隐式马尔可夫模型进行侵入检测，可以高效地防止攻击，但是运算的时间复杂度较高，会耗费较高的能量。

上述两种技术能量消耗较高，有学者提出一种节省能量的节点级入侵检测与防范技术：关键节点探测技术。关键节点是指一种节点，在该节点上的失败或者恶意行为会使得网络断开或者性能显著降低。文献[9]提出一种关键点探测技术，在该技术中采用图论的方法探测顶点部分和边部分。顶点部分是顶点的集合，该顶点的移除会产生具有更多部分的子图。边部分是边的集合，该边的移除会产生具有更多部分的子图。在该方法中，首先确定特定时帧的网络拓扑结构的近似结构或者拓扑结构的一部分，然后根据上述拓扑结构进行关键节点探测，确定其失败或者恶意行为会切断网络或者显著地降低网络性能的节点，其中可以采用轻量级的触发器机制监测网络流量并确定关键节点，接着探测节点是否与邻居共享关键链接，一旦确定为关键链接，则使用更多的资源对其进行监测。总之，该技术集中资源对于关键节点进行入侵检测，可以节省有限的运算资源，但是其对于移动 Ad Hoc 网络的动态性支持不够。

2.2 系统级的入侵检测与防范

该类方法主要基于移动 Ad Hoc 网络的整体系统行为的分析，进行系统的安全管理，从而保障移动 Ad Hoc 网络的网络安全。该方法的关键在于建立系统化的安全管理机制。学者提出了基于政策的安全管理机制、基于贝叶斯方法的非法侵入探测系统，以及终端到终端的蠕虫攻击探测方法等等。

基于贝叶斯方法的非法侵入探测系统为了在系统级上防止非法侵入，在文献[10]提出的分布式协作的非法侵入探测

系统中，周围的一些节点共享本地非法探测信息，并且与邻居合作以探测周围的不正常行为。该系统包括4个组成部分：处理模块、本地探测模块、管理模块和全局处理模块。在处理模块中，审计数据得以收集和处理。在本地探测模块中，使用朴素贝叶斯分类器对记录和探测情况进行分类。管理模块负责生成警告信息并且与其他节点通信。每个节点的非法侵入探测系统定期监测包，并且收集下列信息：源地址，目的地址，源端口号，目的端口号，包大小，MAC包类型，路由控制包流向。基于上述数据，产生下列特征向量：接收到的包被丢弃的概率，接收到的包(在数量上)被传送的概率，接收到的包(在包的大小上)被传送的概率，目的地址改变的概率，目的端口改变的概率，节点位置改变的概率，节点发出路径请求的概率，节点发出路径回复的概率，标准的路由负载和包转送的丢失。基于这些特征向量，采用朴素贝叶斯方法(Naive Bayes)对记录进行分类。根据特征向量判断节点现在所遭受的攻击的类型。基于使用朴素贝叶斯方法的分类器采集的信息，如果节点感测到其邻居节点是恶意节点，该节点发出全局警告信息并且初始化合作非法侵入探测过程，从而每个节点共享该消息。综上所述，该技术基于贝叶斯方法进行非法侵入探测，可以高效地防止攻击，但是运算的时间复杂度较高，并且需要占用较大的存储空间。

上述技术时间复杂度较高，同样为了在系统级上防止非法侵入，有学者提出了一种时间复杂度较低的系统级入侵检测与防范技术：基于政策的安全管理机制[11]。在基于政策的安全管理机制下，每个节点装备有攻击检测代理，该代理持续监测网络行为和移动节点的行为级别，并且如果该级别超过特定阈值，代理将向邻居节点发送警告信息。其主要利用响应/预先防范策略和连锁反应安全政策启动机制。响应策略应用于正在遭受攻击的网络节点。利用该响应策略，在节点遭受攻击的时候启动更新的安全政策。预先防范策略应用于受到攻击的节点的邻居节点，利用该策略，当节点遭受攻击的时候，该节点更新安全级别并且将警告信息发送到邻居节点，当邻居节点接收到警告信息的时候，每个节点更新自己的安全级别并且将警告信息传送给警告范围内的自己的邻居。综上所述，该技术所具有的集成性和适应性使得该方法可以高效地防止攻击，并且运算的时间复杂度较低，但其对于移动Ad Hoc网络的动态性支持不够，并且占用较大的存储空间。

除了上述两种技术之外，有学者专门针对蠕虫攻击提出了终端到终端的蠕虫攻击探测方法。蠕虫攻击通过在网络中生成较短的路由干扰正确的网络路由，当路由协议选择网络中的最短路径时，蠕虫将导致网络的拥塞。文献[12]提出的终端到终端的蠕虫攻击探测方法的主要内容如下。一旦ROUTE REQUEST包到达目的地，其回复ROUTE REPLY，该包具有当前位置信息。发送方从ROUTE REPLY包中获得接收方的位置并且估计接收方和发送方之间的最小跳数。如果接收到的包比估计的最短路径还要短，该路由被丢弃，否则发送方选择最短路径。一旦发送方识别到蠕虫，发送方启动与蠕虫节点之间的路径并且向接收方发送TRACE包。该TRACE包被路由中的每个中间节点转送。当路由中的节点接收到TRACE包，其向源节点回复当前位置和到目的地的跳数。接着发送方可以使用接收到的位置估计每个节点上跳数的增加。如果一个节点与前一跳相比跳数的增加不是1，那么该节点和它的前一跳被认为是蠕虫。综上所述，借助该方法，移动Ad Hoc网络可以有效地探测蠕虫节点并防止蠕虫节点的攻击，且运算的时间复杂度较低。但是，该技术仅仅针对蠕虫攻击，适用范围较为狭窄，并且对于移动Ad Hoc网络的动态性支持不够。

3 安全路由协议技术

由于传统的因特网路由协议无法适应移动Ad Hoc网络动态性的要求，因此对于移动Ad Hoc网络的基本路由协议的研究如火如荼。目前，对于移动Ad Hoc网络安全路由协议的研究主要分为两种：一种是提出一种全新的安全路由协议，该协议支持网络安全管理；另一种是对于现有的移动Ad Hoc网络路由协议进行优化，使之支持网络安全管理。对于第二种情况，本文称之为现有路由协议的安全化改进。

3.1 全新的安全路由协议技术

该类方法提出支持网络安全管理的路由协议，从而保障网络安全。该方法的关键是同时实现快速路由和安全管理。学者提出了多路径TCP安全路由协议、适应性模糊逻辑路由协议、安全邻居路由协议、基于信誉度的安全路由协议、Ariadne协议、以及信任识别路由协议等等。

多路径TCP安全路由(MTS)协议。为了解决安全路由问题，文献[13]提出的多路径路由方法主要针对意图窃取信息的被动攻击进行防范。MTS算法的工作原理是：首先源节点生成路由请求(RREQ)包；接着源节点向传送范围内的所有节点广播RREQ；然后邻居节点接着把RREQ转送其他节点，中间节点通过检测广播ID判断重复的RREQ并将其丢弃；最后目的节点在第一次接收到RREQ的时候生成路由回复(RREP)包，并沿着相逆路径将RREP单播传送回源路由；并且当目的节点接收RREQ的其他副本的时候，检测其是否是不通的路径并且存储不同路径的信息。该算法的特点是：源节点适应性地选择可用路由，而不是一个接一个测试在路由表中存储的路由，主动TCP会话不是固定不变的，而是随时间动态改变的；目的节点定期传送检测包以确保该路径仍然有效，当发现在数据安全方面有更好的路径的时候，源节点适应性地选择该路径代替原路径。该协议提供较好的安全性能，但是目的节点需要定期传送检测包，增加了网络负担。

上述协议网络负担较高，有学者提出网络负担较低的安全路由协议：安全邻居路由协议(SNRP)。同样为了解决安全路由问题，文献[14]提出的安全邻居路由协议在较低加密负载的前提下对移动Ad Hoc网络路由进行加密并且探测节点的不正常行为。主要包括两个阶段：首先端对端进行安全路由识别，其次在邻居节点之间建立本地信任。在新加入的节点与其邻居相互信任之后，公钥证书被用于将新加入的节点"介绍给"它的新邻居。一旦节点和其邻居建立一定级别的信任，路由协议可以简单地将加密信息验证码(HMAC)加以应用，以对路由控制包进行端对端的加密。该加密路由协议使用可信任的第三方发行的加密证书，所有节点必须在进入网络之前获得该证书，该证书将IP地址、MAC地址和公钥绑定，期望进行通信的节点对必须共享对称密钥。邻居识别验证是一个本地实现的全网范围的验证过程，当节点进入另一个节点的邻居范围内的时候，节点间相互进行验证，并且该验证定期重复以确保仅有当前邻居节点获得访问验证。采用广

告过程将节点的存在进行广告，从而获得网络访问。在一跳邻居节点之间建立对称会话密钥从而实现相互的验证。该协议的路由识别过程与 AODV 协议相类似，另外对 RREQ 和 RREP 包增加了标签和消息散列鉴别码以确保端对端的安全。综上所述，该协议使用 IP 地址、MAC 地址和公钥确定的证书，有效地实现了安全邻居路由的确定，但是其增加了节点存储的负担。

上述协议网络负担或者节点存储负担较高，有学者提出不加重网络负担和节点存储负担的安全路由协议，该类协议主要根据节点的行为进行安全化路由。该类协议主要包括基于信誉度的安全路由协议（COSR），信任识别路由协议（TARP）和基于安全级别的适应性模糊逻辑路由协议（FLSL）。文献[15]提出的基于信誉度的安全路由协议（COSR）包括信誉度模型和路由协议两部分。COSR 协议使用信誉度模型测量节点的贡献以探测恶意节点，其定义了两种类型的信誉度：节点信誉度和路由信誉度。节点信誉度（NR）是特定节点的贡献和转发能力的量度。节点信誉度不仅仅包含信誉度请求者的观察，还包含邻居的调查和推举，其计算公式为：$NR_{ij}=C(i,j)\alpha+cof(j)\beta+rec(j)\gamma$，其中，$NR_{ij}$ 代表由 N_i 计算的节点 N_j 的信誉度值；$C(i,j)$ 用于描述节点 N_j 的贡献，也就是说由节点 N_j 转发的节点 N_i 及其邻居的路由包和数据包的数量；$cof(j)$ 标明特定节点的转发能力，该转发能力使用能量和带宽资源加以描述；$rec(j)$ 代表根据节点的行为以及合作性等的其他客观标准；α,β 以及 γ 是影响 NR 信誉度的各种因素的权重，并且 $\alpha,\beta,\gamma\in[0,1]$，$\alpha+\beta+\gamma=1$。对于新节点而言，COSR 给予其一个默认的信誉度直到其完成足够的行为。路由信誉度（RR）用以估算和选择最优路由。$\{N_i\rightarrow N_{k1}\rightarrow N_{k2}\rightarrow\cdots\rightarrow N_{km}\rightarrow N_{km+1}\rightarrow N_j\}$ 被定义为：当每个 $NR\geqslant 0$ 的时候，$RR_{ij}=NR_{ikj}$；其他情况下 $RR_{ij}=-1$。综上所述，COSR 协议使用信誉度模型探测恶意节点，并使得所有节点更好地协同工作，但是其计算的时间复杂度较高，并且信誉度具有一定程度上的滞后性。文献[16]提出的信任识别路由协议（TARP）基于最短路径和节点的安全特性选择路由。只有满足发送者要求的节点才能够转发数据包。在该协议中，计算节点的信任级别的安全参数包括：软件配置、硬件配置、电源电能、信用历史、有无防护和组织结构。每个节点基于上述参数计算邻居的信任级别，并且将其使用在下一跳节点的判断中。总而言之，上述协议基于信任级别识别安全路由，但是上述信任级别计算的时间复杂度较高。在文献[17]提出的基于安全级别的适应性模糊逻辑路由协议（FLSL）中，首先，确定 MANET 的各个移动节点的安全级别；然后，确定最佳安全级别的路由路径。确定移动节点安全级别 s 的公式如下，其中 l 代表密钥长度，f 代表密钥改变频率，n 代表活动邻居节点的数量：$S\propto l*f*\frac{1}{n}$。最佳安全级别的路由路径是基于模糊逻辑运算进行比较和确定的。综上所述，该协议将模糊逻辑引入路由协议中，实现了最佳安全级别的路由路径的确定，但是其具有较高的时间复杂度。

有学者将密钥技术引入移动 Ad Hoc 网络安全路由协议中，并且提出了 Ariadne 协议。为了解决安全路由问题，文献[18]提出的基于请求的安全移动 Ad Hoc 网络路由协议基于高效的对称密钥技术加以设计。在该协议中，具有以下 3 个特征：该协议使得目标节点能够验证路由请求，该协议能够验证路由请求和路由回复中的验证数据，该协议采用高效的逐跳哈希技术确保所有节点记录在路由请求的节点表中。就目标节点对于路由请求的验证而言，初始程序在路由请求中增加消息验证码，该消息验证码是由基于特定数据（例如时间戳）的密钥计算得出的，目标节点可以使用公钥验证该路由请求。对于路由数据的验证而言，具有 3 种可以采用的技术：TESLA 协议、数字签名和标准消息验证码。TESLA 协议将单独的消息验证码增加到用于广播验证的报文中，用于验证路由报文。当 Ariadne 协议和 TESLA 协议一起使用的时候，每跳都验证请求中的新信息，直到中间节点释放相应的 TESLA 密钥的时候目标节点才发送回复。当 Ariadne 协议和数字签名一起使用的时候，使用路由请求中的签名列表计算签名。使用消息验证码的 Ariadne 协议是 3 种技术中最为高效的验证机制，但是其需要所有节点之间具有成对的共享密钥。使用目标节点和当前节点之间共享的密钥计算路由请求中的消息验证码列表。对于逐跳哈希技术而言，使用单行道哈希技术确保所有的跳都没有被忽略。因此，攻击者为了改变或者移除前一跳，必须监听没有列出的节点的路由请求，或者能够插入单行道哈希函数。对不能够将包转送到下一跳的发送者而言，沿安全路由将包转发到下一跳的节点向包的发送者发出路由错误消息。为了防止未授权的节点发送路由错误消息，该错误消息必须得到发送者的验证。返回源节点的路径上的每个节点都转发该错误消息。基于此，每个节点能够验证错误消息。综上所述，Ariadne 协议基于对称密钥操作对攻击者进行防范，但对于移动 Ad Hoc 网络的动态性支持不够。

3.2 现有路由协议的安全化改进技术

该类方法的关键在于安全化策略与现有路由协议之间的协调支持。学者对于常见的移动 Ad Hoc 网络的路由协议进行改进，提出了下述安全化的方案：AODV 协议的安全化、DYMO 协议的安全化、OLSR，MPR 协议的安全化，DSR 协议的安全化等等。

AODV 协议的安全化。AODV 协议是移动 Ad Hoc 网络常用的路由协议，但是其设计之初没有考虑安全问题，学者对 AODV 协议的安全化问题做了很多研究。第一，SAODV 协议。为了使得 AODV 协议安全化，文献[19]所提出的 SAODV 协议使用电子签名验证路由请求 RREQ 和路由回复 RREP，并且使用哈希链对跳数信息进行加密。第二，AODV-SEC 协议。为了使得 AODV 协议安全化，文献[20]提出的基于 AODV 协议的安全路由协议 AODV-SEC 使用安全控制器代替 AODV 协议中的控制器。该安全控制器探测安全性并且运行相应的机制验证包或者对包加密。每个加密包也使用加密包回复。如果接收到未加密包，控制器需要确定对其处理还是将其丢弃。该协议使用公钥基础设施（PKI）在节点级别上进行验证，并且使用 PKI 提供的证书进行验证。该技术具有较高的时间复杂度和空间复杂度。第三，基于信任机制的增强 AODV 路由协议。为了使得 AODV 协议安全化，文献[21]提出的带有攻击探测的 AODV 协议为网络建立了信任机制。当恶意节点被该信任机制确定为攻击者的时候，该协议实现了路由重建以将攻击者从网络中排除。同时，为了提供安全和可靠的数据转送服务，在对包进行路由的时候，节点

应当首先使用高信任度的路由。其中信任度的计算采用下述公式，其中 R_r 代表路由可信度的值；R_n 代表成功转发的包的数量；R_{rf} 代表未能成功转发的包的数量：当转送包成功的时候，$R_r=1-\frac{2*R_f}{R_n+R_{rf}}$（$R_n+R_{rf}\neq 0$，否则 $R_r=0$）；当转送包失败的时候，$R_r=\frac{2*R_s}{R_n+R_{rf}}-1$（$R_n+R_{rf}\neq 0$，否则 $R_r=0$）；路由信任度为 $R_r=\frac{R_n-R_{rf}}{R_n+R_{rf}}$（$R_n+R_{rf}\neq 0$，否则 $R_r=0$）。当节点具有下述相应行为的时候，其信任度得以改变。当节点具有合法行为的时候，$R_{m+1}=R_m+\Delta R$；节点具有非法行为并且 $R_m>0$ 的时候，$R_{m+1}=R_m/2-\Delta R$；节点具有非法行为并且 $R_m<0$ 的时候，$R_{m+1}=R_m-2*\Delta R$。基于上述信任度计算，在网络中建立信任机制，从而为 AODV 协议提供安全支持。该技术具有较高的时间复杂度。第四，令牌路由协议（TRP）。为了使得 AODV 协议安全化，基于 SAODV 协议高能耗的缺点，文献[22]提出的令牌路由协议使用低成本的哈希链算法计算代替 SAODV 协议的高成本的不对称算法计算。在 AODV 协议中，路由报文有两部分：易变部分和非易变部分。为了使得 AODV 协议安全化，TRP 协议使用两条单向的哈希链，其中一条哈希链用于验证报文的非易变部分，另外一条用于验证跳数信息（跳数信息是报文中唯一的易变部分）。TRP 使用与 SAODV 协议类似的方式保护 RREQ 和 RREP 包的跳数，即使用哈希链验证。对于报文的非易变部分的验证，TRP 的基本思想在于：源节点和目的节点知道共享密钥，它们可以相互验证；中间节点不知道密钥，但是它们将每个数据包绑定到前一个 RREQ 和 RREP 包的路由，从而来自可信的源节点和目的节点的数据包只会沿原有的 RREQ 和 RREP 包之间的路径传送，该路径来自可信的源节点和目的节点，因此该路径是可信路由。该技术降低了能耗，但是具有较高的空间复杂度。综上所述，AODV 协议的安全化使用各种安全技术，使得 AODV 协议具备安全的功能。但是，上述协议多数具有较高的时间复杂度和能耗。

DYMO 协议的安全化。为了保证完整性和真实性，文献[23]提出的 DYMO 路由协议的安全扩展 SEDYMO 基于数字签名和哈希链，并且设立两条规则：第一，中间节点必须对其转发的路由报文添加路由信息；第二，即使其是稳定的或者不重要的，转发的路由报文和来自先前路由的数据不能被移除。SEDYMO 协议使用路由请求报文中的哈希链迫使每个节点提出其与原始节点之间的真实跳距，以确保两个节点之间的最短路径得以选出。SEDYMO 协议使用数字签名机制，当中间节点接受到路由方面的信息的时候，其必须验证该信息包含的所有签名。综上所述，DYMO 协议的安全化使用哈希链和数字签名保证了安全，但是其需要较大的空间存储哈希链和数字签名。

OLSR，MPR 协议的安全化。为了实现路由安全，文献[24]为 OLSR，MPR 协议提供侵入探测系统。其基于语义特征检测技术，利用一系列与协议相关的用于特定化正确 OLSR，MPR 行为的特性实现安全通信。OLSR，MPR 协议易受攻击的方面表现在：首先，生成过程中的控制 MPR 攻击，表现为 HELLO 报文的识别欺骗，HELLO 报文的连接欺骗，MPR 报文的识别欺骗，MPR 报文的连接欺骗；其次，转发过程中的控制消息攻击，转发节点通过插入或者删除 MPR 选择器篡改 TC 报文等。针对上述 OLSR，MPR 协议易受攻击的方面，该文献提出，首先，源自 MANET 节点的 HELLO 消息包含该节点的所有一跳邻居；其次，如果 MANET 节点接收将其列为 MPR 选择器的 TC 消息，TC 消息的生成则必须是该 MANET 节点的邻居；再次，如果 MANET 节点接收其邻居生成的 TC 消息，并注意到 TC 消息将其列为 MPR 选择器，该 MANET 节点必须将该 TC 生成器作为 HELLO 消息的 MPR；还有，TC 消息的发送者接听由所有 MPR 转发的相同的 TC 消息。综上所述，该文献提出一种在 OLSR 和 MPR 协议下探测非法路由控制消息的方法。综上所述，该方法可以高效地防止 OLSR 和 MPR 协议下的非法侵入，但是增加了消息的长度以及整个网络的传送负担。

DSR 协议的安全化。为了保障移动 Ad Hoc 网络的安全性，文献[25]提出的安全路由识别协议（SRDP）是对于 DSR 协议的安全优化。SRDP 协议采用加密信息验证码或者电子签名进行验证。该协议根据下述情况判断使用加密信息验证码或者电子签名：如果成对密钥的预先分配是可能的，则采用加密信息验证码，除非下述两个问题的回答也为肯定；如果中间节点需要验证路由完整性，则必须采用签名；如果禁止拒绝是重要的，则必须采用签名；如果不存在公钥架构，则加密信息验证码或者公钥签名都可以使用；如果计算成本是主要的问题，则加密信息验证码更为优越。该方法简便易行，并且计算的时间复杂度和空间复杂度不高，但是需要预知一些信息，如成对密钥的预先分配是否可能、禁止拒绝以及计算成本是否重要等等。

4 密钥技术

密钥技术是传统的网络安全技术。基于移动 Ad Hoc 网络的特点，对于现有密钥技术进行改造，也是一种保障移动 Ad Hoc 网络安全的重要技术。

文献[26]将移动 Ad Hoc 网络的密钥管理技术分为部分分布式证书验证、完全分布式证书验证、基于身份的密钥管理、基于证书链的密钥管理、基于簇的密钥管理、基于预部署的密钥管理、基于动态性的密钥管理和并行密钥管理。该文献并将上述 8 类技术分别进行了介绍和比较。第一，部分分布式证书验证。文献[27]提出的分布式公钥管理服务通过让节点共享系统密钥，使得在一系列节点中建立信任关系。若干分布式证书验证（DCA）通过提供阈值群签名签发证书。文献[28]是对于文献[27]所提出的方案的进一步优化，其中采用移动证书验证（MOCA）进行验证。MOCA 证书协议使得一个需要证书服务的节点广播证书请求包，任何接收到上述包的 MOCA 节点将包含证书签名的证书回复包回复给上述节点，如果在一定时间内节点成功收到所有的包，则重建证书。如果证书验证正确，则证书请求成功。如果获得的证书回复包数量不足，节点初始化另一个请求。第二，完全分布式证书验证。文献[29,30]指出，DCA 的私钥 SK 由网络中的所有节点共享，需要 DCA 服务的节点联系任意的一跳邻居节点即可。第三，基于身份的密钥管理。文献[31-33]基于降低传统公钥系统的存储成本和降低获得公钥的负担的需要，建立基于身份的密钥管理。在该方案下，公钥就是唯一标识用户的用户身份标识。第四，基于证书链的密钥管理。文献[34]基于证书链进行密钥管理，其不需要信任的第三方，每个节点

向其他节点发行自己的证书。每个节点保存由其邻居发行的证书构成的"证书库"。第五，基于簇的密钥管理。文献[35]使用区域算法构建基于簇的网络模型。该区域算法用以将移动 Ad Hoc 网络的节点聚簇到不同的子集中，从而发现最小生成树。第六，基于预部署的密钥管理。文献[36]基于预部署进行密钥管理。在部署之前，离线验证为每个节点加载密钥池。因为移动 Ad Hoc 网络具备动态性，因此基于预部署的密钥管理仅仅适用于大规模网络中。第七，基于动态性的密钥管理。文献[37,38]基于动态性进行密钥管理，其是基于节点动态性的点对点的密钥建立方法。该方法使得节点在不依赖安全路由架构的情况下，相互交换密钥；从而打破了路由安全中的相互依赖造成的循环。第八，并行密钥管理。文献[39]提出的并行密钥管理的方法结合使用分布式证书验证和证书链。

另外，为了进一步保障移动 Ad Hoc 网络的网络安全，有学者提出将密钥技术与架构模型技术加以结合。在文献[40]提出的移动 Ad Hoc 网络的高效验证方案中，委任一些安全性高的节点，由它们共享密钥管理的责任。也就是说，由一些安全性高的节点共同构成认证中心(CA)，进行密钥管理。从而避免了一个节点侵入导致网络安全瘫痪的情况，并且降低了将私钥暴露于外部的风险。

还有，为了有效地利用密钥，有学者将其应用于特定的数据结构中。文献[41]提出安全通信树以及基于安全通信树的密钥技术以提高移动 Ad Hoc 网络的安全。在该方案下，在预处理阶段，基站确定系统参数和每个节点的保密数据；在初始化阶段，节点确定相互之间以及与基站之间通信用的密钥对；在第三个阶段，用户使用密钥执行网络组织并且建立路由路径。

综上所述，密钥技术采用密钥进行网络安全验证，高效地保障了网络安全，并且具有较低的空间复杂度，但是其对于移动 Ad Hoc 网络的动态性支持不够，并且有些方案需要进行预先配置。

5 其他技术

除了上述几种常见的移动 Ad Hoc 网络安全技术之外，有学者提出了其他几种网络安全技术：信任启动程序和针对资源耗尽攻击的技术等。

信任启动程序。Jaydip 等学者提出的分布式信任建立方案中[42]，移动 Ad Hoc 网络系统中设置信任启动程序。在系统的自引导阶段启动信任启动程序，该程序用以初始化信任建立的过程。该信任启动程序使得充分信任的关系得以建立，从而网络中的节点对可以借助信任链相互验证。在自引导阶段，节点从信任启动程序接收密钥列表的副本并且将其存储在本地；在自引导的第二阶段，成员节点发行与密钥列表中接收到的绑定相对应的 m 个证书；从而信任关系得以建立。当节点加入的时候，证书发行过程与自引导过程相同，成员节点发行绑定目标节点 ID 和公钥的证书，当新的节点能够收集到足够的证书，其成为网络成员。当节点删除的时候，意图离开网络的节点通过广播数字签名消息的方式表达该意图，该广播的消息被每个节点独立验证，并且如果被认为是真实的，那么在合理的延迟之后发行给该节点的证书被撤销。该方案可以作为移动 Ad Hoc 网络高层安全技术的底层模块，并且其适应于移动 Ad Hoc 网络的动态性，但是其要求在自引导阶段对于信任启动程序完全信任，存在一定的安全隐患。

针对资源耗尽攻击的技术。Masao 等学者提出的针对资源耗尽攻击的 3 种方法包括时隙方法、令牌方法、密钥方法[43]。在时隙方法中，移动 Ad Hoc 网络的每个节点在预定的时隙发送包。所有节点知道针对所有节点的所有时隙。攻击节点没有自己的时隙，因此合法节点能够识别并且丢弃来自攻击节点的非法包。在令牌方法中，仅仅当移动 Ad Hoc 网络的节点接收到令牌的时候，其才能发送包。因为攻击节点没有令牌，因此其不能发送包。在密钥方法中，移动 Ad Hoc 网络中的每个节点所传送的包具有密钥，节点加入到移动 Ad Hoc 网络的时候获得该密钥。攻击节点不属于移动 Ad Hoc 网络，无法得到密钥，因此其传送的包会被其他节点丢弃。该方案实现简便，但是仅适用于防止资源耗尽的攻击。

6 已有研究的比较

移动 Ad Hoc 网络的网络安全技术可以采用如下技术指标进行衡量：第一，时间复杂度；第二，空间复杂度；第三，能量消耗；第四，高效性；第五，准确性。基于上述技术指标，表 1 对上述各种移动 Ad Hoc 网络安全技术进行了比较。

表 1 安全技术的比较

Literature	Time complexity is low?	Space consumption is low?	Energy consumption is low?	Efficiency	Accuracy
[7]	No	No	No	Yes	No
[8]	No	No	No	Yes	No
[9]	No	No	Yes	No	No
[10]	No	No	No	Yes	Yes
[11]	Yes	No	No	Yes	Yes
[12]	Yes	No	No	No	Yes
[13]	Yes	Yes	Yes	No	Yes
[14]	No	No	No	Yes	No
[15]	No	No	No	Yes	No
[16]	No	No	No	Yes	Yes
[17]	No	No	No	Yes	Yes
[18]	No	Yes	No	Yes	No
[19]	No	No	No	Yes	Yes
[23]	No	No	No	Yes	No
[24]	No	No	No	Yes	No
[25]	Yes	Yes	No	No	No
[27]	No	Yes	No	Yes	Yes
[29]	No	No	No	No	Yes
[31]	No	Yes	No	Yes	No
[34]	No	Yes	Yes	Yes	No
[35]	No	No	No	Yes	Yes
[36]	No	Yes	No	No	No
[37]	No	No	No	Yes	No
[39]	No	No	No	No	No
[42]	No	No	No	Yes	No
[43]	Yes	No	No	No	Yes
[44]	No	No	No	No	Yes

结束语 随着移动 Ad Hoc 网络的广泛应用，移动 Ad Hoc 网络的网络安全技术的研究如火如荼。本文对入侵检测与防范、安全路由协议技术、密钥技术、架构模型技术和其他技术分别进行了介绍和分析。其中入侵检测与防范包括节点级的入侵检测与防范和系统级的入侵检测与防范，安全路由协议技术包括全新的安全路由协议技术和现有路由协议的安全化改进技术。

基于对上述网络安全技术的分析，可以得出如下结论：首先，大多数技术都将节点动态性作为安全技术设计考虑的首要因素。节点动态性是移动 Ad Hoc 网络的主要特点之一，因此大多数网络安全技术将其作为重要指标加以考虑。入侵检测与防范根据节点的动态性针对节点行为或者系统行为进行分析，以防范非法入侵；安全路由协议技术在节点的动态性的基础上对现有路由协议进行改造或者设计新的路由协议；大多数密钥技术基于网络的动态性设立或者对网络的动态性加以支持。架构模型技术对于网络的动态性也加以考虑，并且在架构或者模型的设计上加以支持。其次，大多数技术保障了移动 Ad Hoc 网络的节点对等性。节点对等性是移动 Ad Hoc 网络的主要特点之一，因此大多数网络安全技术对节点对等性加以支持。入侵检测与防范在节点对等性的基础上建立检测模型，对节点行为或者系统行为进行分析；安全路由技术所设计或者改造的路由协议对节点的对等性加以支持；大多数密钥技术建立在节点对等性的基础上，并没有对移动 Ad Hoc 网络的基础结构加以改变；但是，为了提高移动 Ad Hoc 网络的安全性，架构模型技术在节点上建立一定的架构或者模型，使得节点之间不完全对等。

基于对上述网络安全技术的分析，还可以得出如下结论：首先，全新的安全路由协议技术基于移动 Ad Hoc 网络自身特有的网络特点建立，使得移动 Ad Hoc 网络快速路由与安全管理得以实现，对于 Ad Hoc 网络的离散性以及能量有限性支持较好，以及实现高效的安全路由协议具有较好的研究前景。其次，入侵检测与防范和密钥技术多是对现有的网络安全技术进行改造，使之适应移动 Ad Hoc 网络的网络特点。然而，该类方法是否能够完全支持移动 Ad Hoc 网络无稳定拓扑结构、节点离散、无线通信、能量有限的特点；以及如何更好地支持上述特点值得研究。还有，现有路由协议的安全化改进技术是对于移动 Ad Hoc 网络的网络路由技术进行改造，使之保障移动 Ad Hoc 网络的网络安全。然而，该类方法在保障网络安全的同时是否能够保障快速路由值得研究。另外，架构模型技术通过改变移动 Ad Hoc 网络离散性的网络特点实现网络安全，虽然其保障了移动 Ad Hoc 网络的完全，但是其改变了移动 Ad hoc 网络的网络结构。做出这种改变是否会影响移动 Ad Hoc 网络其他功能的实现，以及是否会影响移动 Ad Hoc 网络的性能值得研究。

综上所述，如何将安全性问题体现在路由协议中，在高效路由的同时保障通信安全，是非常值得研究的领域。首先，如何对移动 Ad Hoc 网络中的安全路由问题良好地建模非常值得研究。针对可能存在的攻击建立全面的模型，可以使得协议设计者有效地评估路由协议的安全性。至今，尚未有学者提出有效评估移动 Ad Hoc 网络中的路由协议的模型。另外，具有较高安全性并且具有较高网络性能的高效路由协议非常值得研究。在安全和性能上加以平衡，使得路由协议高效安全，可以有效地促进移动 Ad Hoc 网络的广泛应用。

参 考 文 献

[1] Murphy A L, Roman G-C, Varghese G. An exercise in formal reasoning about mobile communications[C]// IEEE Ninth International Workshop on Software Specification and Design. 1998: 25-33

[2] Ramanatan R, Redi J. A brief overview of ad hoc networks: challenges and directions[J]. IEEE Communications Magazine, 50th Anniversary Commemorative Issue, 2002, 5: 20-22

[3] Garbinato B, Rupp P. From ad hoc networks to ad hoc applications[C]// IEEE Proceedings of the 7th International Conference on Telecommunications(ConTEL 2003). 2003, 1: 145-149

[4] Marin G A. Network security basics[J]. IEEE Security & Privaty Magazine, 2005, 3(6): 68-72

[5] Graft D, Pabrai M, Pabrai U. Methodology for network security design[J]. IEEE Communications Magazine, 1990, 28(11): 52-58

[6] Hubaux J-P, Buttyan L, Capkun S. The quest for security in mobile ad hoc networks[J]. IEEE MobiHoc, 2001: 146-155

[7] Yu Wei, Liu K J R. Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks[J]. IEEE Transactions on Moblie Computing, 2007, 6(5): 459-473

[8] Khanna R, Liu Huaping. System approach to intrusion detection using hidden Markov model[C]// Proceeding of the 2006 international conference on Communications and mobile computing (IWCMC'06). 2006: 349-354

[9] Karygiannis A, Antonakakis E, Apostolopoulos A. Detecting critical nodes for MANET intrusion detection systems[C]// Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2006(SecPerU 2006). 2006: 9

[10] Karim A H M R, Rajatheva R M A P, Ahmed K M. An efficient collaborative intrusion detection system for MANET using Bayesian Approach[C]// Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems(MSWiM'06). 2006: 187-190

[11] Zheng H, Wang S, Nichols R A. Policy-based security management for ad hoc wireless systems[C]// Military Communications Conference. 2005, 4: 2531-2537

[12] Wang Xia. Intrusion detection techniques in wireless ad hoc networks[C]// Computer Software and Applications Conference, (COMPSAC'06). 2006: 347-349

[13] Li Zhi, Kwok Y-K. A new multipath routing approach to enhancing TCP security in ad hoc wireless Networks[C]// Proceedings of the 2005 International Conference on Parallel Processing Workshops(ICPPW'05). 2005: 372-379

[14] Jadhav A, Johnson E E. Secure Neighborhood Routing Protocol. Military Communications Conference, (MILCOM 2006). 2006, 10: 1-7

[15] Wang Fei, Mo Yijun, Huang Benxiong. COSR: Cooperative On-Demand Secure Route Protocol in MANET[C]// International Symposium on Communications and Information Technologies, (ISCIT '06). 2006: 890-893

[16] Abusalah L, Khokhar A, BenBrahim G, et al. TARP: trust-aware routing protocol[C]// Proceeding of the 2006 international conference on communications and mobile computing. 2006: 135-140

[17] Jin Lu, Zhang Zhongwei, Lai D, et al. Implementing and evaluating an adaptive secure routing protocol for mobile ad hoc network[C]// IEEE Wireless Telecommunications Symposium, (WTS '06). 2006: 1-10

[18] Hu Yih-Chun, Perrig A, Johnson D B. Ariadne: a secure on-demand routing protocol for ad hoc networks[J]. Wireless Networks, 2005, 11(1/2): 21-38

（下转第 14 页）

model for static analysis of programs by construction or approximation of fixpoints[C]// Proceedings of the 4th ACM SIGACT-SIGPLAN symposium on Principles of programming languages. 1977:238-252

[34] Nielson F, Nielson H R, Hankin C. Principles of Program Analysis[M]. Springer, 1999

[35] Aho A V, Sethi R, Ullman J D. Compilers: principles, techniques, and tools[M]. Inc. Boston, MA, USA: Addison-Wesley Longman Publishing Co., 1986

[36] Balakrishnan G, Reps T. DIVINE: DIscovering Variables IN Executables. VMCAI, 2007: 1-28

[37] Brumley D, Newsome J. Alias analysis for assembly[R]. CMU-CS-06-180. Carnegie Mellon University School of Computer Scie-nce, 2006

[38] Prasad M, Chiueh T. A binary rewriting defense against stack based buffer overflow attacks[C]// Proceedings of the USENIX Annual Technical Conference. 2003: 211-224

[39] Haugh E, Bishop M. Testing C Programs for Buffer Overflow Vulnerabilities[C]// Proceedings of the Network and Distributed System Security Symposium. 2003

[40] Aggarwal A, Jalote P. Integrating Static and Dynamic Analysis for Detecting Vulnerabilities[C]// Proceedings of the 30th Annual International Computer Software and Applications Conference(COMPSAC'06). Volume 01, 2006: 343-350

[41] Harris L C, Miller B P. Practical analysis of stripped binary code [J]. ACM SIGARCH Computer Architecture News, 2005, 33 (5): 63-68

[42] Nethercote N. Dynamic Binary Analysis and Instrumentation [D]. University of Cambridge, UK, 2004

[43] Luk C K, et al. Pin: building customized program analysis tools with dynamic instrumentation [C] // Proceedings of the 2005 ACM SIGPLAN conference on Programming language design and implementation. 2005: 190-200

[44] Dynamorio[OL]. http://www.cag.lcs.mit.edu/dynamorio

(上接第 7 页)

[19] Zapata M G. Secure ad hoc on-demand distance vector routing [J]. Mobile Computing and Communications Review, 2006, 6 (3): 106-107

[20] Eichler S, Roman C. Challenges of secure Routing in MANETs: A Simulative Approach using AODV-SEC[C]// IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS2006). 2006: 481-484

[21] Liu Jun, Li Zhe, Lin Dan, et al, A Security Enhanced AODV Routing Protocol Based On the Credence Mechanism[C]// International Conference on Wireless Communications, Networking and Mobile Computing 2005. 2005, 2: 719-722

[22] Li Leiyuan, Chigan C. Token Routing: A Power Efficient Method for Securing AODV Routing Protocol[C]// Proceedings of the 2006 IEEE International Conference on Networking, Sensing and Control, (ICNSC '06). 2006: 29-34

[23] Rifa-Pous H, Herrera-Joancomarti J. Secure Dynamic MANET On-demand(SEDYMO) Routing Protocol[C]// Fifth Annual Conference on Communication Networks and Services Research, (CNSR '07). 2007: 372-380

[24] Wang M, Lamont L, Mason P, et al. An Effective Intrusion Detection Approach for OLSR MANET Protocol[C]// 1st IEEE ICNP Workshop on Secure Network Protocols, (NPSec). 2005: 55-60

[25] Kim PJihye, Tsudik PGene. SRDP, securing route discovery in DSR[C]// Proceedings of the The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services2005. 2005: 247-260

[26] Van Der Merwe J, Dawoud D, Mcdonald S. A survey on peer-to-peer key management for mobile ad hoc networks [J]. ACM Computing Surveys, 2007, 39(1): 1-45

[27] Zhou R, Haas Z J. Securing ad hoc networks[J]. IEEE networks (Special Issue on Network Security), 1999, 13(6): 24-30

[28] Yi S, Kravets R. MOCA: Mobile certificate authority for wireless ad hoc networks[C]// Proceedings of the 2nd Annual PKI Research Workshop(PKI 2003)

[29] Kong J, Zerfos P, Luo H, et al. Providing robust and ubiquitous security support for mobile ad-hoc networks[C]// Proceedings of the Ninth International Conference on Network Protocols 2001(ICNP'01)

[30] Luo H, Zerfos P, Kong J, et al. Self-securing ad hoc wireless networks[C]// Proceedings of the Seventh International Symposium on Computers and Communications 2002(ISCC'02)

[31] Joye M, Yen S M. ID-based secret-key cryptography[J]. ACM Operat. Syst. Rev., 1998, 32(4): 33-39

[32] Boneh D, Franklin M. Identity-based encryption from weil pairing[C]// Proceedings of the Conference on Advances in Cryptology 2001(CRYPTO'01)

[33] Cha J C, Cheon J H. An identity-based signature from gap diffie-hellman groups[C]// Proceedings of the Conference on Public Key Cryptography 2003(PKI'03)

[34] Capkun S, Buttyan L, Hubaux J. Self-organized public-key management for mobile ad hoc networks[J]. IEEE Transactions on Moblie Computing, 2003, 2(1): 52-64

[35] Ngai E C H, Lyu M R, Chin R T. An authentication service against dishonest users in mobile ad hoc networks[C]// Proceedings of the IEEE Aerospace Conference. 2004

[36] Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks[C]// Proceedings of the 9th ACM Conference on Computer and Communication Security 2002 (CCS'02)

[37] Capkun S, Buttyan L, Hubaux J. Mobility helps security in ad hoc networks[C]// Proceedings of MobiHoc 2003

[38] Capkun S, Hubaux J, Buttyan L. Mobility helps peer-to-peer security[J]. IEEE Transactions on Moblie Computing, 2006, 5 (1): 43-51

[39] Yi S, Kravets R. Composite key management for ad hoc networks[C]// Proceedings of the First Annual International Conference on Mobile and Ubiquitous Systems: Network and Services(MobiQuitous'04)

[40] Shin K, Kim Yoonho, Kim Yanggon. An Effective Authentication Scheme in Mobile Ad Hoc Network[C]// Proceedings of the Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing(SNPD'06). 2006: 249-252

[41] Nikodem J, Nikodem M. Secure Communication Trees in Ad Hoc Networks[C]// Proceedings of the 14th Annual IEEE International Conference and Workshops on Engineering of Computer-Based Systems 2007(ECBS'07)

[42] Sen J, Chowdhury P R, Sengupta I. A Distributed Trust Establishment Scheme for Mobile Ad Hoc Networks[C]// International Conference on Computing: Theory and Applications, (ICCTA '07). 2007: 51-58

[43] Tanabe M, Aida M. Preventing Resource Exhaustion Attacks in Ad Hoc Networks[C]// Eighth International Symposium on Autonomous Decentralized Systems(ISADS'07). 2007: 543-548