移动自组网的访问控制技术研究

熊庭刚[1,2] 卢正鼎[1] 张家宏[2]
(华中科技大学计算机科学与技术学院 武汉 430074)[1] (武汉数字工程研究所 武汉 430074)[2]

摘 要 网络资源的共享与保护是移动自组网需要解决的关键问题之一。运用Voronoi图模型和quorum系统的思想,提出了一种移动自组网的动态路径quorum系统,设计了动态路径quorum的生成算法。基于移动自组网的动态路径quorum系统,提出了基于quorum系统的移动自组网的分布式访问控制机制,详细描述了节点的身份认证、网络资源的访问控制和权限管理协议。与传统的基于单个节点自身的访问控制机制相比,该访问控制机制具有较强的抗攻击能力和较高的可靠性,能够有效地提高移动自组网的资源共享与保护水平。

关键词 移动自组网,Voronoi图,动态quorum系统,分布式访问控制
中图法分类号 TP393 **文献标识码** A

Research on Access Control Technology on Mobile Ad-hoc Networks

XIONG Ting-gang[1,2] LU Zheng-ding[1] ZHANG Jia-hong[2]
(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)[1]
(Wuhan Digital and Engineering Institute, Wuhan 430074, China)[2]

Abstract Resources share and protection are one of key problems needed to solve on mobile ad-hoc networks (MANET). A dynamic paths quorum system on MANET was proposed by making use of the model of voronoi diagram and the idea of quorum system. The construction algorithm of dynamic paths quorum was designed. Based on the dynamic paths quorum system on MANET, a distributed access control mechanism was given and the protocols, such as node authentication, network resources authorization and rights management, were described in detail. Compared with traditional access control mechanism grounded on single node in MANET, the distributed access control mechanism grounded on more nodes, i. e. a quorum nodes, has higher availability and greater capability to withstand attack. It can improve the level of resources share and protection on MANET observably.

Keywords Mobile ad-hoc networks, Voronoi diagram, Dynamic quorum system, Distributed access control

1 引言

无线移动自组网(MANET)是一组带有无线通信装置的移动终端组成的无中心的网络,可以在任何时刻、任何地点不需要现有信息基础网络设施的支持,快速构建起一个移动通信网络。MANET由于具有灵活机动、组网迅速和适应环境能力强的特点,已经广泛应用于突发事件处理、野外联络、传感器组网、移动作战指挥、单兵系统等民用和军用领域。

由于MANET在结构和通信方式上的开放性,使得它所面临的安全威胁和可靠性问题比其它形式的网络系统更加严重。目前,MANET的安全研究还不很成熟,现有的大多数安全方面的研究主要是在密钥的分配管理、安全路由、数据传输的机密性和完整性等方面,而针对MANET的访问控制研究还不多[1]。访问控制是保障MANET安全的重要组成部分,无论是单节点内的还是全网络的资源和服务都需要实施访问控制,以确保非授权的节点和用户无法得到相应的网络资源和提供的相关服务。但是,MANET没有始终在线的集中式节点和明确的网络防护边界,也不存在网络基础设施(譬如路由器、交换机、网关等,每个节点既是资源拥有者、路由功能的提供者,也可能是资源的请求者)。现有的访问控制都只依赖于单个节点,一旦节点被控制、被破坏或者发生故障,将给网络的安全和可靠性带来很大的威胁[2]。因此,如何建立高效的访问控制机制,实现全网范围的网络资源和服务的访问控制,是急需解决的问题。

2 基本概念和相关工作

quorum系统是一种在分布式系统中用来协调处理器行为、保持数据一致性的工具。它是一种集合系统,定义如下:

定义1 设U是n个节点的集合,$S=\{Q_1,Q_2,\cdots,Q_m\}$是U的非空子集的集合,若$\forall iQ_i\subseteq U$和$\forall i,jQ_i\cap Q_j\neq\emptyset$,称$S$为一个quorum系统,$Q_i$是一个quorum。

在每个quorum内部,节点之间通过相互通信保持信息或者操作的一致;多个quorum之间通过交叉特性,保持相互之间的信息或者操作的一致性。当某些节点失效时,存活节

到稿日期:2010-05-18 返修日期:2010-08-29 本文受国家自然科学基金(70771043,60873225,60773191)资助。
熊庭刚 男,博士生,研究员,主要研究方向为信息安全和容错计算,E-mail:xtg_hb@yahoo.com.cn;卢正鼎 男,教授,博士生导师,主要研究方向为分布式计算、数据库系统和信息安全;张家宏(1980—),男,博士,主要研究方向为信息安全和密码算法理论等。

点构成的 quorum 能够保持整个系统的信息或者操作的一致性和完整性。分布式系统、quorum 系统已经被广泛用来实现数据复制[3]、操作互斥等[4]。利用 quorum 系统的特性，熊庭刚等人[5,6]提出了基于 quorum 系统的分布式访问控制结构和访问控制授权系统的构造方案与算法，把分布式系统中的授权服务器按 quorum 系统进行组织，通过授权 quorum 而非单个服务器对访问控制申请进行授权，使得分布式系统的访问控制服务的可用性水平得到较大的提高。

MANET 是一种典型的分布式网络。本文把 quorum 系统的思想和方法与 MANET 的访问控制需求结合起来，针对 MANET 的特殊性提出一种访问控制机制，以实现全网范围的网络资源访问控制。

3 移动自组网的动态 quorum 系统

3.1 MANET 的 Voronoi 图模型

Voronoi 图把平面分割成若干个凸多边形，以至于每个凸多边形内只有一个点，而且凸多边形内的任何位置到该点的距离最短。

定义 2 设 P 是一离散点集合 $P_1,P_2,\cdots,P_n$，定义 P_i 的 Voronoi 区域 $V(P_i)$ 为所有到 P_i 距离最小点的集合：$V(P_i)=\{P/d(P,P_i)\leqslant d(P,P_j),j\neq i,j=1,2,\cdots,n\}$，称节点 P_i 是 Voronoi 图的生成元。

Voronoi 图非常适用于描述移动自组网的结构与状态。设 MANET 由 n 个节点组成，MANET 的每一个节点随机均匀地分布在 $Z=[0,l)\times[0,w)$ 大小的平面上（其中 l 和 w 为平面的长和宽）。每个节点 P_i 的 Voronoi 区域 $V(P_i)$ 是该节点的任务区域。随着节点的移动，$V(P_i)$ 会发生变化。所有节点的 Voronoi 区域合起来覆盖 Z 平面，即 $V_{manet}=\bigcup_1^n V(P_i)\geqslant Z$。每个节点都能够与其相邻区域的生成元节点通信。每个节点通过卫星定位系统能够确定自己是否处于 Z 平面的边界。

3.2 MANET 的动态路径 quorum 系统

文献[6]构造了一种自适应的路径 quorum 系统，它具有良好的负载特性、较快的 quorum 构造速度和可扩展性能，如图 1 所示。其中每个顶点能够与相邻顶点通信。一条路径是一个从左到右，或者从上到下相邻顶点形成的一条通信链路。这已经与 Voronoi 图在形式上非常接近，可以直接转化为 Voronoi 图，如图 1(b)所示。图 1(a)中的粗虚线和图 1(b)中的粗边框围成的 $V(P_i)$ 区域分别表示一条路径，只是这种 Voronoi 图的路径比较规整。

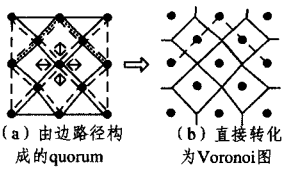

图 1 规整拓扑的 Voronoi 图路径 quorum 系统

下面提出并设计一种 MANET 的动态路径 quorum 系统。

定义 3 根据定义 2，设有一个 MANET 的任务空间 $V_{manet}=\bigcup_1^n V(P_i)$，覆盖区域 $Z=[0,l)\times[0,w)$，MANET 任务空间中的一条动态路径是从左到右横穿（或者从上到下纵穿）区域 Z 的由相邻的 Voronoi 区连接的一条链路，相邻的生成元节点能够相互通信，满足条件 $\sum_i len(V(P_i))\geqslant l$（或者 $\sum_i wid(V(P_i))\geqslant w$），$P_i\in LP$，且 $\exists V(P_{l\text{-most}})$ 和 $\exists V(P_{r\text{-most}})$，分别覆盖 Z 的最左和最右边界（或者 $\exists V(P_{u\text{-most}})$ 和 $\exists V(P_{d\text{-most}})$ 覆盖最上和最下边界），u-most，d-most，l-most，r-most $\in\{1,2,\cdots,n\}$，函数 len 和 wid 分别表示取 Voronoi 区的长度和宽度。MANET 的动态路径 quorum 系统由一条横向路径加一条纵向路径组成。图 2 中 quorum A 和 quorum B 分别用长划虚线和短划虚线表示。

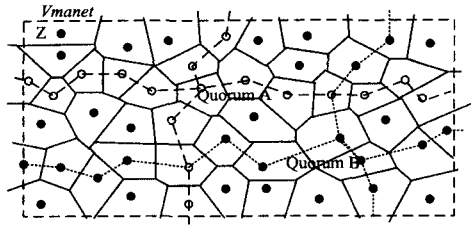

图 2 MANET 的动态路径 quorum 系统

显然，任意两个 quorum 之间都至少有两个生成元节点的 Voronoi 区域相交。

3.3 MANET 动态路径 quorum 的生成算法

在 MANET 中生成动态路径 quorum 的前提条件是生成 MANET 的 Voronoi 图，其关键是每个节点构建自己的 Voronoi 区。每个节点探测相邻节点的位置并确定与它们的相对位置关系，从而建立自己的 Voronoi 区域。每个节点只与 Voronoi 区域相邻的节点通信，即使它的通信能力能够到达 Voronoi 区不相邻的位置较远的节点，如图 3(a)所示。

设节点 S 以图 3(b)所示的位置为基点开始构造路径 quorum。它分别向上、下、左、右 4 个方向（对应区域 Z 的正北、正南、正西、正东方向）发出路径搜索请求 $Su(g)$，$Sd(g)$，$Sl(g)$，$Sr(g)$，g 初值为 0，用于保持搜索尽量沿着 S 的水平和垂直方向进行。根据穿过节点 S 的 45 度和 135 度（逆时针方向为正）两条相位平分线（如图 3(b)中的虚线所示），判别节点 S 的相邻节点在上、下、左、右方向所处的确切位置。

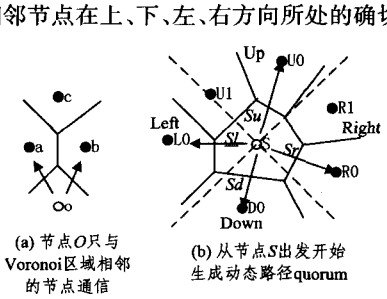

图 3 构造动态路径 quorum

对每个方向，具体如下：

1）若没有相邻点，则把请求转发给有相邻节点的下一个节点。对于 $Su(g)$，$Sd(g)$，如果向右转发一次，$g=g+1$，反之 $g=g-1$。对 $Sl(g)$，$Sr(g)$，如果向上转发一次，$g=g+1$，反之 $g=g-1$。如果同时存在两个可转发的节点，则根据 g 的值选择转发节点，如果 $g<0$，向 g 加 1 方向转发；否则，向 g 减 1 方向转发。

2）若只有一个相邻点，则把请求转发给它，如图 3(b)中的 Sl 和 Sd。

3）若有多个相邻点，则按照接近任务空间边沿的程度

approach 选择转发请求的下一个节点。

4)如果当前节点 S 已经覆盖 Z 的边沿,则停止。

approach 的计算方法有两种:

a)计算当前节点 S 至下一个候选节点的连线与水平或者垂直方向线之间的夹角,approach 等于最小夹角值;

b)计算下一个候选节点与任务空间的边沿距离,approach 等于最小距离值。

该算法在每一个方向上与经典的地理路由算法类似[7-9]。如果 approach 按照 a)取值,则类似于 compass 和 most-forwarding 路由算法;如果 approach 按照 b)取值,则类似于 greedy 路由算法。文献[7-9]证明了如果底层是 Delaunay 三角(Voronoi 图的对偶图),这几种路由算法都可以保证抵达目的地。

本文按照文献[5]提出的访问控制结构和协议,采用基于动态路径的 quorum 系统实现 MANET 全网范围的节点身份认证与资源访问控制。

4 基于 quorum 系统的 MANET 分布式访问控制

由任意节点组成的 quorum 都能够承担身份认证。由资源的拥有者进行权限认证并实施访问控制,因此全局资源须由全体节点控制,而 quorum 能够作为全体节点的代表行使职责。

4.1 预备工作

节点身份的识别:采用公钥密码体制。首先设定存在一个全局可信的身份证书中心 CA,CA 为每个主体签发由它签名的、与主体惟一身份代码绑定的身份公钥证书。CA 的公钥分发给每一个节点。

节点权限/角色的识别:同样采用公钥密码体制。每个任务空间都有一个与之对应的权限证书中心 AA,AA 代表所管理的任务空间为节点签发角色证书。一个节点在访问 MANET 的某个任务空间之前,必须从管理该空间的 AA 获得用户-角色分配。得到 AA 为其签发的角色证书,才能够申请对任务空间的访问。

访问控制规则:等价于"角色-权限"分配关系。访问控制规则由属性证书中心 AA 制定并签名,发布给每个参与任务的节点。在同一任务空间中的节点必须遵循统一的全局资源和服务访问控制规则。

MANET 网络的节点在部署前后都需要做一些预备工作:

1)进入任务空间之前,每个节点得到 CA 公钥、CA 颁发的身份证书、AA 的公钥、AA 颁发的角色证书、在所参与任务中的编号、私钥和分配给节点的访问控制规则。

2)进入任务空间后,节点通过 GPS 得到自己所在的空间信息,寻找周围的相邻节点,以自己为生成元节点构建局部 Voronoi 区图,并向邻接节点发布自己的公钥证书。

4.2 分布式身份认证

认证是实现访问控制的前提。在 MANET 中,由于节点的行为可能被其它某些节点指控[10],或者身份信息过期,或者身份被管理节点取消,因此对一个节点合法性的认证信息分布在整个网络中,而不是集中保存在某个中心节点上。因此好的身份认证方法应该不仅仅依赖于某个或某几个节点,而是应该得到全体任务空间中节点或者大多数节点的认可,从而排除持有已经失效、被取缔或者伪造身份证书的节点。下面分两种情况进行讨论,相关节点如图 4 所示。

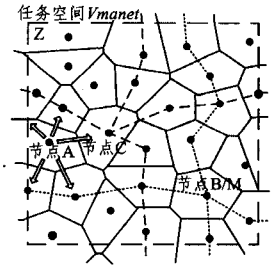

图 4 MANET 任务空间中的节点申请身份认证和访问网络资源

1)认证节点 A 身份

(1)节点 A 向任务空间发出身份认证请求{A 的身份证书,节点 A 编号 Id,A 的签名},显然只有部分节点(通常为相邻点,称为源节点,可能有多个)能够收到 A 的请求。

(2)收到请求的源节点首先用 CA 的公钥验证 A 的身份证书,确认是 CA 颁发的有效证书,然后用 A 的身份证书中 A 的公钥验证 A 的签名,确认 A 是证书的持有者。如果均为真,并且本节点没有记录 A 的任何非法身份信息,则以源节点(譬如节点 C)所在的位置为基点,构造动态路径 quorum,把 A 的认证请求进一步转发给 quorum 中的每一个成员,寻求进一步的验证。

(3)路径中的每个成员均对 A 的认证请求进行验证,并把验证结果按路径回传给源节点。

(4)源节点对收到的所有验证结果进行综合,如果至少有两个验证结果不为真,则节点 A 的身份被否认。

上述过程能够防止一个被指控、被删除或者被暂时取消身份的节点在网络中继续活动。通过 A 的签名包含时间信息和随机信息,则能够防止重放攻击。如果节点 A 是新加入的节点(Id 编号不在现有节点编号中),则源节点与 A 建立邻居关系并重构邻接 Voronoi 区域。

根据 3.2 节,在基于路径的 MANET 动态路径 quorum 系统中,每两个 quorum 之间至少有两个相交节点,所以在步骤(4)中如果至少有两个节点的验证结果不为真,则说明节点 A 的身份已经被任务空间中的某个 quorum 否认,因此拒绝节点 A 的身份认证请求。

2)节点撤离/退出任务空间

若某个节点 B 希望退出任务空间 V_{MANET},它只需要通过一个 quorum 即可向整个任务空间发布退出请求。

(1)节点 B 以自身所在的位置为基点开始构造动态的 quorum,向 quorum 中的每一个成员发送退出请求{节点 B 的身份证书,节点 B 编号 Id,B 的签名}。

(2)收到 B 请求的每一个节点对请求进行验证。如果证实该请求确实由 B 所发,则将 B 的编号从任务空间节点表中删除。

过程的优化:

(1)利用多源节点动态路径 quorum 的交叉特性减少网络的通信开销。根据 3.2 节,路径 quorum 系统的每对 quorum 之间至少有两个节点交叉。当 m 个源节点同时搜索网络,构造 quorum 时,至少有 $2m$ 个交叉节点将收到至少两个构造 quorum 的请求。但是,任意一个 quorum 都可以代表整个网络做出判断,所以可以选择一种方案使交叉节点只传递

某一源节点的构造请求，譬如选择节点 Id 号较大或者时间上先到达的源节点。

(2)多个源节点首先选举搜索 quorum 的权利，由胜出者构造认证 quorum。

4.3 分布式访问控制和权限管理

参与任务的每一个节点拥有自己的私有资源，也拥有全局资源的某一部分，节点在任务空间部署前均获得一个基本规则表，这个规则表规定了不同角色访问任务空间中资源的初始权限。在任务执行过程中，这个规则表的内容可以动态改变，以便及时更新访问控制政策。相关节点如图 4 所示。

1)资源访问控制：分两种情形讨论：其一是节点 A 访问指定节点 B 的资源 R_B，其二是节点 A 访问任务空间的全局资源 R_Z。

情形 1　节点 A 请求访问指定节点 B 的资源 R_B

(1)节点 A 向节点 B 提出访问资源 R_B 的请求{节点 A 身份证书，节点 A 角色证书，资源名 R_B，访问操作，A 签名}；

(2)节点 B 首先用 A 的(在 A 的身份证书中)公钥验证 A 的签名，确认资源访问请求确实由节点 A 发出，然后检查 A 的角色证书，确认 A 拥有任务空间管理中心 AA 签发的角色，最后根据自己的规则表确定是否把资源发送给节点 A；

(3)如果上述检查均未通过，则拒绝 A 的申请。

情形 2　节点 A 访问任务空间的全局资源 R_Z

(1)节点 A 向所有邻接点广播全局资源访问请求{节点 A 身份证书，节点 A 角色证书，资源名 R_Z，访问操作，A 签名}；

(2)相邻的节点选举一个源节点为基点构造访问控制 quorum，并向其中的每个节点转发 A 的访问请求；

(3)quorum 中的每个节点首先(用 A 的身份证书中的公钥)对 A 的签名进行验证，确认访问请求确实由节点 A 所发，然后检查 A 的角色证书，确定角色证书的有效性，最后检查自己的规则表，确认是否把资源发送给节点 A，每个节点把验证和检查的结果反馈给源节点；

(4)如果 quorum 中有两个以上节点的检查未通过，源节点就生成一个拒绝 A 访问请求的应答，并且停止把 A 的访问请求继续向其它节点转发；

(5)如果 quorum 中至多 1 个检查未通过，源节点生成一个允许 A 的访问请求的应答，附上自己的签名(包括时间)连同 A 的访问请求向其它节点转发；

(6)收到 A 请求的节点把节点 A 所需要的资源发送给 A。

对于步骤(4)和(5)，同样根据 3.2 节的描述，若有两个以上节点的检查未通过，则说明至少存在一个 quorum 对 A 的角色或者访问权限不认可；若至多 1 个检查未通过(这个节点可能故障，也可能被攻击而叛变)，则说明全体节点同意 A 的请求。

2)权限管理：权限的管理包括规则分发、撤销、暂停等命令。设某节点 M 需要发布或者修改其拥有的或者与其相关的全局资源的访问权限。

(1)M 以自身所在的位置为基点开始构造动态的权限管理 quorum，并向 quorum 中的每个节点发出权限管理请求：{M 的身份证书，M 角色证书，规则项，M 签名})；

(2)quorum 中收到请求的每个节点首先用 M 的公钥验证 M 的签名，确认权限请求确实由节点 M 发出；

(3)然后检查 M 的角色证书，确认 M 拥有发布或者修改全局资源访问权限的角色；

(4)如果检查通过，更新本地的规则表，否则丢弃请求。

5 安全性、可靠性和实时性分析

5.1 安全性分析

(1)抗共谋攻击。一个新节点加入网络、一个节点更新访问规则或者申请对全局资源的访问，都必须得到一个代表了整个网络的 quorum 中成员的一致认可，即使敌人能够俘获地理上靠近的源节点(尤其是网络边沿上的孤立节点)。但是由于 quorum 是一种即时构建的动态路径，因此敌人不可能预先知道并且不可能攻破一个 quorum 上的所有成员节点，所以它具有很强的抗共谋攻击能力。

(2)抗篡改。每个节点的身份认证请求、加入撤离请求、访问请求以及权限管理请求的信息都用该节点的私钥进行了数字签名。对这些信息的任何微小改动，都会使后续的验证失败，因此提出的身份认证及权限管理具有抗篡改能力。

(3)抗重放攻击。选用的签名算法中有一个关键步骤，即产生随机数。这样，每次签名的值都会随着随机数的变化而变化，不可能存在两次完全一样的签名值，因此系统能够抵抗重放攻击。

(4)防身份假冒。每次请求身份或是管理权限都会以某一节点的私钥进行签名加以验证。私钥由每个实体秘密保管，因此非法实体不可能假冒合法节点。

(5)防拒绝服务攻击。每次认证请求都是一次完整的过程，不会因为某一步被拒绝而出现双方信息不一致的情况，从而导致下次认证失败。拒绝服务攻击只会使当前传输受阻，下次重新发起的请求又是一次完整的请求，可以被正常执行，因此系统能防止拒绝服务攻击。

(6)能够充分利用 quorum 之间相交的特点。通过一个 quorum 内部的操作，能够在全体任务空间上实现节点的身份和角色的认证和撤销，在一定程度上解决了证书撤销难的问题[11]。

5.2 可靠性分析

quorum 系统的基本出发点就是为了提高系统的可靠性，网络中的任一节点都可能因为硬件或者软件故障而失效。但是，由于 quorum 是动态构造的，个别节点的失效不影响整个网络的正常运行，也不会影响 quorum 的构造。如果节点的可靠性 $p \geqslant 1/2$，则系统的可用性(具有最大的可能)为 $1-2e^{-\varphi(\sqrt{N})}$，其中 $\varphi(\sqrt{N})$ 是一个正比例于 N 的正数[12]。因此，系统的可靠性随着节点数的增加而增大。

5.3 实时性分析

对于身份认证，花费的总时间＝动态 quorum 的构造时间 × quorum 中的每个节点用 CA 的公钥和 A 的公钥验证节点 A 的证书合法性所花费的时间。其中前一因子为 $O(\sqrt{N})$[12]，N 是任务空间中所有的节点数，而在密钥长度和算法确定后，后一因子是常数，记为 C_t。

对于访问控制(不包含节点访问请求通过检查后获取资源的时间)，花费的总时间＝动态 quorum 的构造时间 × quorum 中的每个节点验证节点 A 身份证书合法性、角色和

(下转第 110 页)

在外围区域再布置若干参考标签，定位精度仍有进一步提升的潜力。

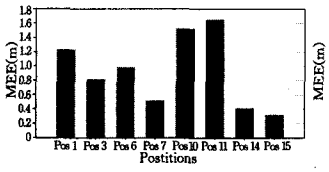

图 4　中心区域定位误差分析

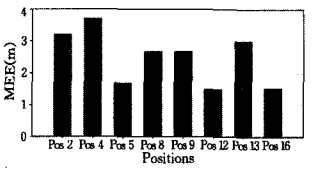

图 5　外围区域定位误差分析

结束语　本文通过对典型 RFID 定位方法的研究与分析，针对为了提高定位精度而部署大量 RFID 设备引起的信息信号干扰问题，提出了一种基于虚拟参考标签的 RFID 定位系统构建方法。实际测试表明，本文方法具有较好的抗干扰能力和较高的定位精度。未来的工作将集中在结合多种位置感知信息，进一步提高定位精度。

参 考 文 献

[1] Yan Sun, La Porta T F, Kermani P. A Flexible Privacy-enhanced Location-based Services System Framework and Practice[J]. IEEE Transaction on Mobile Computing, 2009, 9(3): 304-321

[2] Alsindi N, Xinrong L, Pahlavan K. Analysis of Time of Arrival Estimation Using Wideband Measurements of Indoor Radio Propagations[J]. IEEE Transaction, Instrumentation and Measurement, 2007(5): 1537-1545

[3] 王扬，付永庆，司顺奇. 基于 DOA 和 TOA 的机载单站无源定位[J]. 测绘工程，2008(3)：13-15

[4] Hao N, Guangliang R, Yilin C. A TDOA location scheme in OFDM based WMANs[J]. IEEE Transaction, Consumer Electronics, 2008(3): 1017-1021

[5] 李兴鹤，胡咏梅，宋吉波，等. 基于 landmarc 系统的室内定位仿真研究[J]. 计算机工程与应用，2008(27)：209-212

[6] Paul A S, Wan E A. Wi-Fi based indoor localization and tracking using sigma-point Kalman filtering methods[C]// Position, Location and Navigation Symposium. 2008: 646-659

[7] Ni L M, Yunhao L, Yiu Cho L, et al. LANDMARC: Indoor location sensing using active RFID[C]// Pervasive Computing and Communications. 2003: 407-415

[8] McNeff J G. The global positioning system [J]. IEEE Transactions on Microwave Theory and Techniques, 2002, 50(3): 645-652

[9] Hossain M M, Prybutok V R. Consumer Acceptance of RFID Technology: An Exploratory Study[J]. IEEE Transaction, Engineering Management, 2008(2): 316-328

[10] Jeffrey W R, Borriello G. SpotON: An Indoor 3 D Location Sensing Technology Based on RF Signal Strength[R]. Department of Computer Science and Engineering, University of Washington, 2000

[11] Hightower J, Vakili C, Borriello G, et al. Design and Calibration of the SpotON Ad-Hoc Location Sensing System[R]. 2001

[12] Zhao J, Zhang Y, Ye M. Research on the Received Signal Strength Indication Location Algorithm for RFID System[C]// International Symposium on Communications and Information Technologies, 2006 (ISCIT 2006). 2006: 881-885

[13] Yiyang Z, Yunhao L, Ni L M. VIRE: Active RFID-based Localization Using Virtual Reference Elimination[C]// the 2007 International Conference on Parallel Processing (ICPC 2007). 2007: 56-56

(上接第 75 页)

权限合法性所花费的时间。其中第一因子为 $O\sqrt{N}$，同样地，第二因子是一个常数，记为 C_r。

因此无论是身份认证还是访问控制，所花费的时间均为 $O(C\sqrt{N})=O(\sqrt{N})$，其中 $(C=C_i/C_r)$，可见实时性比较好。

结束语　MANET 的访问控制一直是一个较难解决的问题。本文采用 quorum 技术，结合 Voronoi 图模型，充分利用 quorum 系统的抗攻击、抗毁能力强的特点，所设计的 MANET 访问控制机制不仅能够抵抗共谋、篡改、假冒、重放和拒绝服务等多种攻击行为，而且具有较高的可靠性和较好的实时性，实现了安全技术与可靠性技术的融合。此外，基于该访问控制机制能够方便地实现节点身份和角色的撤销，易于实现全局资源的访问控制权限的维护与更新，解决了 MANET 中节点证书和权限撤销难的问题。

本文的研究结果适用于野外指挥系统、突发事件处理系统、传感器网络(如移动雷达网、声纳网)等军民应用领域。但是在节点频繁移动的 MANET 应用系统中还存在保持角色和权限更新 quorum 结构的稳定性问题，这是今后研究的重点方向。

参 考 文 献

[1] 林闯，蒋屹新，伊浩. 网络安全控制机制 [M]. 北京：清华大学出版社，2008

[2] 林闯，封富君，李俊山. 新型网络环境下的访问控制技术 [J]. 软件学报，2007，18(4)：955-965

[3] Theel O. A general framework for modeling data replication schemes[C]// Proc of the Int'l Workshop on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS'93). San Diego, CA: SCS and IEEE, 1993: 347-250

[4] Agrawal D, El-Abbadi A. An efficient solution to the mutual exclusion problem [J]. Proc of the ACM Trans. Comp. Sys., 1991, 9(1): 1-20

[5] 熊庭刚，卢正鼎，张家宏，等. 基于 Quorum 系统的分布式访问控制框架研究 [J]. 计算机科学，2010，37(5)：120-125

[6] Xiong Ting-gang, Lu Zheng-ding, Zhang Jia-hong, et al. Construction of High Dependable Distributed Access Control Architecture Based on Quorum System [J]. Wuhan University Journal of Natural Sciences, Springer-Verlag, 2010, 15(3): 210-216

[7] Bose P, Morin P. Online routing in triangulations [C] // Aggarwal A, Rangan C P, eds. Proc. of the 10th Int'l Symp. on Algorithms and Computation (ISAAC). Chennai: Springer-Verlag, 1999: 113-122

[8] Bose P, Morin P, Stojmenovic I, et al. Routing with guaranteed delivery in ad hoc wireless networks [J]. ACM/Kluwer Wireless Networks, 2001, 7(6): 609-616

[9] Kranakis E, Singh H, Urrutia J. Compass routing on geometric networks [C]// Proc. of the 11th Canadian Conf. on Computational Geometry. Vancouver, 1999: 52-54

[10] Claude C, Carlton D R. A certificate revocation scheme for wireless ad hoc networks [C]// Proc of the 1st ACM Workshop Security of Ad Hoe and Sensor Networks. Fairfax, Virginia, 2003: 54-61

[11] National Institute of Standard and Technology. Public key infrastructure, Final Report [R]. MITRE Corporation, 1994

[12] Naor M, Wieder U. Scalable and dynamic quorum systems [J]. Distributed Computing, 2005, 17: 311-322