MANET 中基于 HIP 的访问控制模型研究与设计

何智勇[1],朱纯仁[1],方立刚[2]
(1. 南京工业职业技术学院 能源与电气工程学院,江苏 南京 210046;
2. 苏州职业大学 计算机工程系,江苏 苏州 215104)

摘 要:在 MANET 环境下,由于结点的随机移动性和缺乏中心管理控制,每个结点承担路由器和结点双重角色。为了确保网络资源安全,确定新结点的身份和把恶意结点排除在网络之外应该是目前要重点研究的工作。文中在深入研究主机身份协议(HIP,Host Identity Protocol)的基础上,结合主机身份协议基本交换机制,提出一种新的 MANET 访问控制模型,对新加入网络内结点进行身份验证和资源访问权限控制。最后,从 MANET 域内认证和跨 MANET 域间认证两方面,详细分析了基于 HIP 的访问控制模型认证过程,并对模型的安全性能进行分析。

关键词:MANET;主机身份协议;访问控制
中图分类号:TP31 **文献标识码**:A **文章编号**:1673-629X(2013)02-0145-04
doi:10.3969/j.jssn.1673-2013.02.037

Research and Design of Access Control Model Based on HIP in MANET

HE Zhi-yong[1],ZHU Chun-ren[1],FANG Li-gang[2]
(1. College of Energy and Electrical Engineering,Nanjing Institute of Industry Technology,Nanjing 210046,China;
2. Department of Computer Engineering,Suzhou Vocational University,Suzhou 215104,China)

Abstract:It is an important research task to identify the new host identity and reject illegal host to ensure the safety of network resources, because of the host mobility and no central control,every terminal has two roles as node and router in MANET. Based on the deeply research of host identity protocol and HIP exchange mechanism,propose an MANET access control model,which identify the new host identity and resource access control. Finally,analyzed the authentication process of access control model based on HIP from MANET domain and span MANET domain in detail and security of the model.

Key words:MANET;host identity protocol;access control

0 引 言

移动自组织网络[1](MANET,Mobile Ad hoc Network)是由若干无线移动结点在不依赖任何固定基础设施的条件下构建的一种多跳自组织临时性自治系统。网络中的每个移动结点具有终端和路由器的双重功能,作为一种不需要基础设施支持的自组织分布式网络,具有组网方式灵活、抗毁性强、移动通信等优势,在军事应用、抢险救灾等临时通信领域得到了广泛的应用。移动自组织互联网[2](MAINET,Mobile Ad hoc Internet)是由 MANET 通过互联网互连的网络,移动自组织互联网的提出,把 MANET 引入到了民用和商用领域,通过与 Internet 互联,有效地延伸了 Internet 服务覆盖范围, 网络运营商可以提供具有服务质量保证的增值业务,开发新的业务增长点。

访问控制作为保护信息资源的机密性和完整性的重要手段,它的主要任务是保证信息资源不被非法使用和访问,其规定了主体对客体访问的限制,并在身份识别的基础上,根据客体身份对提出信息资源访问的请求加以控制。

基本交换机制是 HIP 核心[3],也是应用的关键部分,文中是在参考文献[2]提出的 MAINET 网络架构基础上进行进一步研究,利用主机身份协议[3]在安全通信、身份验证高效支持的特性,提出一种新的基于 HIP 的 MANET 访问控制模型,该访问控制模型为实现 MANET 移动主机安全接入、用户访问权限控制和

收稿日期:2012-06-04;**修回日期**:2012-09-08
基金项目:苏州市科技计划项目(SYN201105);江苏省现代企业信息化应用支撑软件工程技术研发中心开放基金项目(SX201201);南工院青年科研基金项目(QK12-04-02)
作者简介:何智勇(1984-),男,硕士研究生,主要研究方向为计算机网络与分布计算系统、物联网技术;朱纯仁,硕士,副教授,主要研究方向为过程自动化、楼宇自动化。

保护网络资源提供了一种新的思路。

1 问题提出

在 MANET 环境下,由于结点的随机移动性、网络的临时性、缺乏中央管理控制、无线链路带宽有限等因素的影响,对网络内资源访问权限的控制,例如:网络内 IP 地址资源,接入网络内结点身份验证等,如果在通信之前无法验证接入 MANET 管理域移动主机合法身份和用户合法身份,其它的安全措施也就失去了意义。

近年来 MANET 工作组在 DSR[4]、地址配置[5,6]等方面的研究花费了很大的精力,但是对 MANET 的访问控制很少涉及。随着 MANET 技术的不断发展和移动自组织互联网的提出,怎样保证移动主机的安全接入和访问控制是一个值得研究的内容。

2 HIP 相关研究工作

主机身份协议(HIP)引进一个新的加密命名空间--主机标识符(HI, Host Identity),用主机标识符来全球唯一标识一台主机[7],从根本上解决了主机移动和多宿主问题。主机身份协议的核心思想是:将传送层与网络层分开,网络套接字与拓扑位置独立的主机标识符绑定,IP 地址只用于路由。主机标识符和 IP 地址之间动态绑定,当移动主机动态改变它的 IP 地址时,不会导致正在进行的通信中断,可以很好地解决主机移动性问题[8]。Nováczki Szabolcs[9]等人提出的 HIP-NEMO,是基于 HIP 的扩展,应用于移动网络环境,在 HIP 层提供安全、高效的移动性支持。

近年来,国内的各个研究机构也对该领域做了比较深入的研究。文献[10]提出了下一代互联网实名访问控制模型,并给出了下一代可信网络实名身份验证、访问控制工作框架,该模型把 HI 验证、地址注册、地址更新都在 DNS 上进行,增加了 DNS 负担,导致解析效率很低。陈俊霞[11]提出的基于 HIP 的访问控制模型,通过主机身份协议的基本报文交换把用户身份验证和访问控制有机地结合在一起。但是没有对访问控制模型的部署和可行性进行探讨。

3 基于 HIP 访问控制模型

3.1 用户标识管理

在任何网络系统中,每个实体必然拥有一个唯一确定的符号,用来向系统中的其它的实体表明身份。用户标识赋予网络用户唯一确定的名字,用来标明使用者的身份。用户标识用来唯一标明用户的身份。移动主机接入到 MANET 网络中,通过注册协议申请获得唯一的主机标识符。用户的标识可以通过带外方式注册。在 MANET 域的 RVS 上,记录用户注册的标识信息。用户标识格式可以 username@ gatewayHI 形式来定义。可以从用户的标识看出他所注册的 MANET 域的标识。在主机移动时,可以在不同的 MANET 域之间进行用户身份认证。

3.2 访问控制机制

在 MAINET 网络中,实现用户身份认证和访问控制,需要一套全局访问控制机制。访问控制是保护资源安全的重要途径,可以限制对关键资源的访问,防止非法用户的入侵或者不合法用户的不慎操作所造成的破坏。文献[10]提出访问控制模型,它定义了访问控制系统设计时所需要的一些基本访问控制功能(access control functions)组件,并且描述了各功能组件之间不同的通信状态。访问控制功能组件包括 initiator、访问控制执行功能(Access Enforcement Function, AEF)、访问控制决策功能(Access Decision Function, ADF)、目标(target)资源几个部分[8,12]。其访问控制过程为:首先是由主体(用户)提出对于客体(各类资源)的访问请求,当执行模块(AEF)收到这个请求后,则将其发送给决策模块(ADF)。由决策模块对该请求进行分析,并根据访问控制策略及其访问控制规则来判断是否允许这个请求,然后将判断结果回送给执行模块。再由执行模块根据判断结果,更新相应的控制信息,执行允许或拒绝用户对资源的访问。

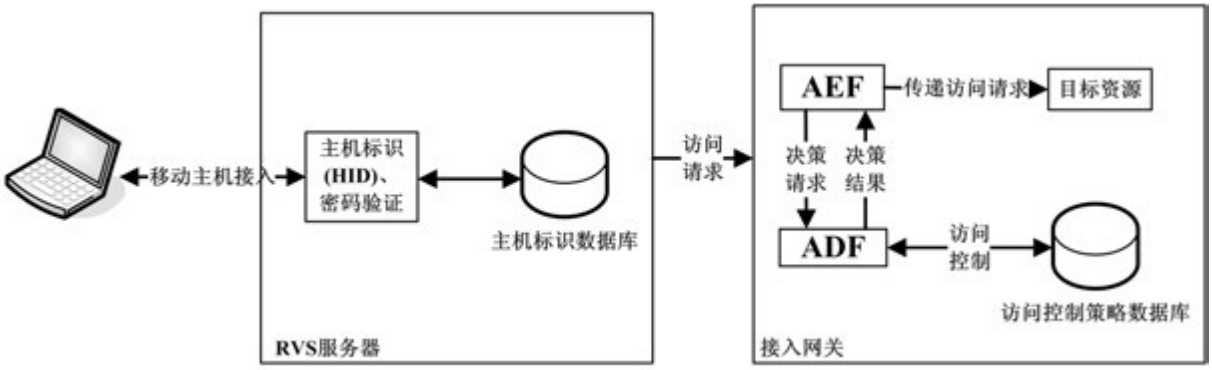

图 1 基于 HIP 的访问控制模型

文中,如图 1 所示,利用 HIP 提供的基本报文交互,通过基本报文交互提供身份验证功能,HIP 的 RVS 服务器负责验证主机身份,在 RVS 服务器认证没有通过的用户,将不进行 AEF 和 ADF 处理,直接拒绝他接入到 MANET 网络中。AEF 模块和 ADF 模块部署在 MANET 域接入 Internet 的网关上面,控制用户和移动主机的访问权限。

3.3　MANET 中基于 HIP 访问控制模型设计

在图 2 所示的 MAINET 网络拓扑结构中,接入到 MANET 域内的移动主机身份验证正确,通过注册协议在 RVS 上获得主机标识,主机标识的唯一性由 RVS 来确定,RVS 记录下分配的记录,移动主机在本地保存自己申请获得的 HI。

从实现的角度看,本访问控制模型大致分为 4 个部分:移动主机(MN)、HIP RVS(Rendezvous Server)、MANET 网关、DNS。移动主机(MN)向 HIP RVS 发送资源访问请求,在 HIP RVS 上对用户登录绑定的服务器的 HI 进行验证,再进行用户身份验证,并把响应的结果显示给用户。HIP RVS 接收来自移动主机的请求,并验证移动主机和用户的身份,把验证的结果发送给 MANET 网关上的访问控制模块。MANET 网关负责用户权限的分配。DNS 维护各 MANET 域的 HIP RVS 的主机标识与 IP 地址的映射关系。

对 MANET 域中用户的访问权限控制,可以通过如下步骤完成。

1. 移动主机 MN 接入 MANET 域,通过注册协议,申请获得一个全球唯一的 HI,HI 与 IP 地址的映射关系保存在 RVS 的记录表中。

2. 用户从移动主机访问 MANET 网络资源的时候,把用户标识(UI, User Identity)与本地移动主机的 HI 绑定。在 RVS 上进行移动主机的身份验证,移动主机身份验证失败,直接拒绝用户的访问请求; 验证成功,RVS 向网关发出资源访问请求。

3. 网关启用基于角色的访问控制体系,根据用户标识,分配用户操作权限,确定提供何种级别的服务。

4. 移动主机 MN 移动到一个新 MANET 域之中,发送位置更新信息,申请地址等。并通知正在通信的 CN 它位置改变信息。用户向初始注册的 MANET 域进行身份验证。

4　访问控制认证过程

一个移动主机接入到一个 MANET 域之中,用户标识和主机标识绑定。通过 HIP 基本交换[3],验证通过之后,用户获得访问控制权限。

图 3 所示的 MANET 域内认证过程,其中的具体流程说明如下:

(1) ~ (2)移动主机通过注册协议,申请获得唯一的主机标识,并把申请获得的 HI 传送给移动主机。

(3)HIP 的 I1 报文,用户通过<User-identity, Password>,在 RVS 上进行身份验证,若成功,RVS 在 I1 中添加成功标志,并转发给 MANET 网关。身份验证失败,RVS直接丢弃I1报文,不进行转发,这样,没有注

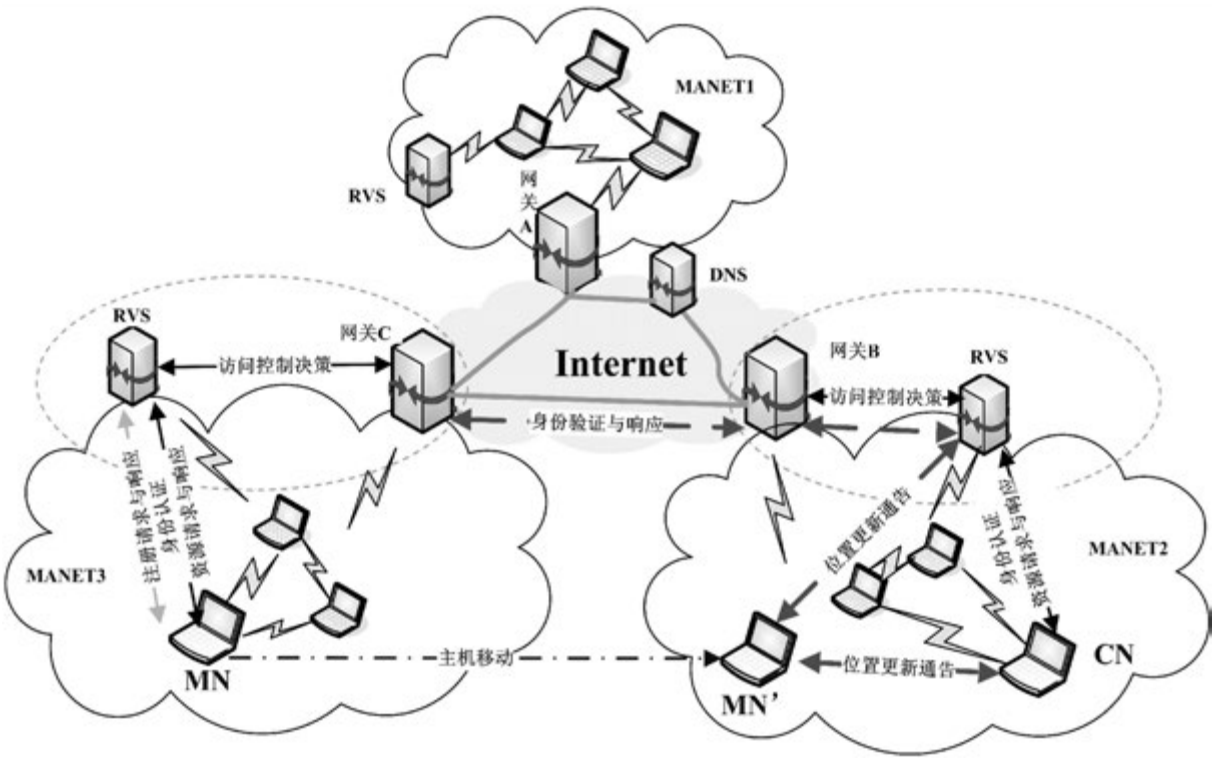

图 2　基于 HIP 的 MAINET 网络拓扑结构

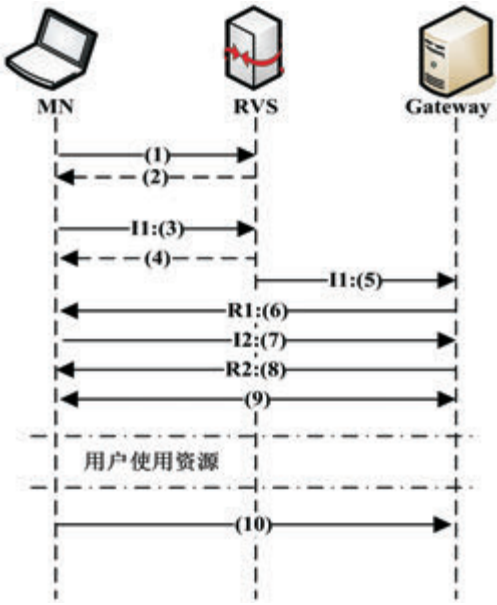

图 3 MANET 域内认证过程

册的用户就不能直接接入 MANET 网络之中,不用进行访问控制处理和用户权限分配。

(6) ~ (8)HIP 基本交互过程,R1, I2, R2。

(9)用户取得访问权限。

(10)用户注销。

用户首次注册的 MANET 域称为家乡域(Home),如图 2,从一个 MANET 域移动到另一个管理域(Foreign)中访问资源时,RVS_Foreign 并不掌握该用户的注册信息,需要到 RVS_Home 去验证用户的身份。由于移动主机的移动,接入到新的管理域后,主机的地址发生改变。要在 RVS_Home 更新 HI 与 IP 地址的映射关系。

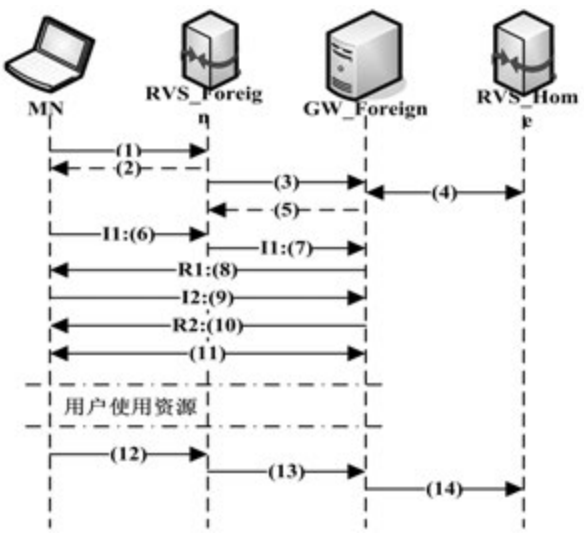

图 4 跨 MANET 域认证过程

图 4 所示为跨 MANET 域内认证过程,其中的具体流程说明如下:

(1) ~ (5)移动主机位置更新以及到用户注册域中去进行身份验证。

(6) ~ (10)HIP 基本交互过程,I1,R1, I2, R2。

(11)用户取得访问权限。

(12) ~ (14)用户注销。

5 安全性分析

文中提出基于 HIP 访问控制模型的安全性来自以下几个方面:

①在 HIP 基本交换过程中创建主机之间的安全关联,四次握手基本交换过程是加密的,可以抵抗 DoS 攻击,在基本交换时进行主机身份验证。

②主机在申请资源之前,通过 HIP 基本报文交换进行主机身份验证,对网络内资源进行有效的保护。

③当主机移动到一个新的 MANET 域,在 RVS 服务器上进行身份验证,从而可以确定外来主机身份的合法性。

6 结束语

MAINET 网络,延伸了传统网络的覆盖范围,由于 MANET 网络的特殊性,对用户访问权限的控制要求非常严格,文中将 HIP 机制应用到移动自组织网络访问控制模型的设计中,可以有效解决 MANET 网络中结点身份验证。

参考文献:

[1] Corson S, Macker J. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations[S]. IETF, RFC2501, 1999.

[2] 欧阳志友,沈苏彬. 基于 P2P 的移动自组织互联网应用平台设计[J]. 北京邮电大学学报,2009,32(4):59-61.

[3] 唐 科,汪文勇,周明天. HIP 基本交换机制的研究与应用[J]. 电子科技大学学报,2007,36(6):1470-1472.

[4] 李光成,张连芳,舒炎泰,等. 动态源路由协议(DSR)在 Linux 下的实现[J]. 计算机工程与应用,2003(22):174-178.

[5] 张 治,戴冠中,赵玉亭. 移动自组网的动态编址问题[J]. 计算机应用,2005,25(7):1503-1508.

[6] 黎俊伟,徐 丹,高传善. Ad Hoc 网络 IP 地址自动配置技术研究[J]. 计算机工程,2005,31(17):111-112.

[7] Moskowitz R, Nikander P, Henderson T, et al. Host Identity Protocol[S]. IETF, RFC5201, 2008.

[8] Yang Xin, Ji Xinsheng. Host identity protocol-realizing the separation of the location and host identity[C]//Proceedings of the 2008 IEEE International Conference on Information and Automation. [s. l.]: [s. n.], 2008: 749-752.

[9] Szabolcs N, László B, Sándor I. A HIP based network mobility protocol[C]//International Symposium on Applications and the Internet-Workshops. [s. l.]: [s. n.], 2007.

(下转第 152 页)

的 CVCSIMM 算法跟踪精度要明显高于一般 CVCAIMM 算法,而改进后的自适应 CVCSIMM 算法虽然增加了部分计算量,在切换时速度较一般 CVCAIMM 算法稍慢,跟踪精度短时间下降,但整体精度得到了提高,对机动目标的跟踪效果更好。

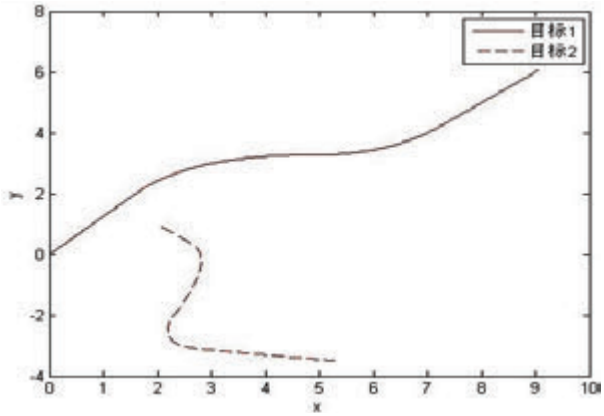

图 1 目标运行轨迹

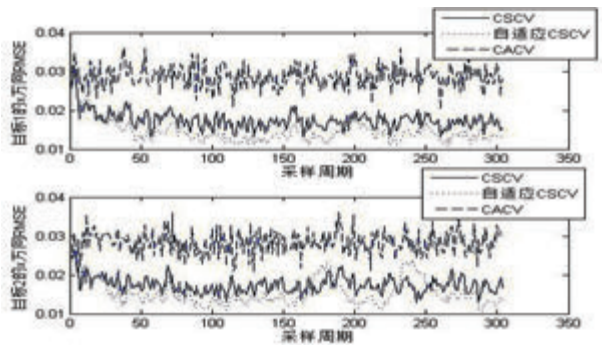

图 2 目标 x 方向 RMSE 曲线

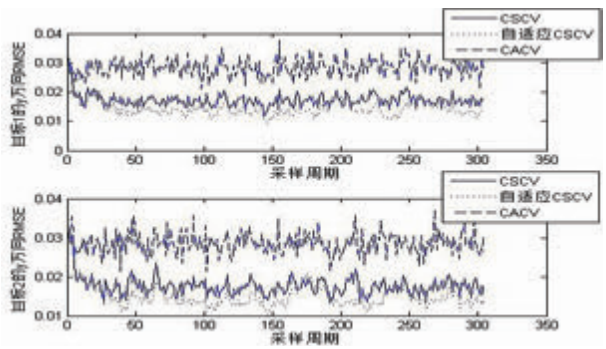

图 3 目标 y 方向 RMSE 曲线

5 结束语

文中将改进基于当前模型的 IMM 算法用于机器人对机动目标的跟踪,并进行了仿真比较。结果表明改进后的算法性能更好,能够更精确地估计机动目标的状态,具有很好的稳定性,为机器人在动态环境中的路径规划打下了基础。

参考文献:

[1] 刘卫光,李广鑫. 一种通用的视频目标跟踪系统设计[J]. 计算机技术与发展,2009,19(10):110-112.

[2] 闵华清,黄欣欣,罗荣华. 基于激光和视觉信息的机器人目标跟踪方法[J]. 计算机技术与发展,2010,20(4):113-116.

[3] 雷 云,王夏黎,孙 华. 基于视频的交通目标跟踪方法研究[J]. 计算机技术与发展,2010,20(7):44-47.

[4] Singer R A. Estimating optimal tracking filter performance for manned maneuvering targets[J]. IEEE Transactions on Aerospace and Electronic Systems,1970,AES-6(4):473-483.

[5] ITU-T Draft H. 263. Video Coding for Low Bit Rate Communication[S]. 1999.

[6] Zhang J S,Yang W Q,Hu S Q. Target tracking using the interactive multiple model method[J]. Journal of Beijing Institute of Technology,1998,7(3):299-304.

[7] Rong L X,Vesselin P J. A survey of maneuvering target tracking:dynamic models[C]//Proceedings of SPIE. [s. l.]:SPIE Press,2000.

[8] van der Merwe R. Sigma-point Kalman filters for probabilistic inference in filters for probabilistic inference in dynamic state-space models[D]. Portland:OGI School of Science & Engineering at Oregon Health & Science University,2004.

[9] 周宏仁,敬忠良,王培德. 机动目标跟踪[M]. 北京:国防工业出版社,1991.

[10] 夏忠婷,汪圣利,武 洋. 基于 UKF 的马尔科夫参数自适应 IFIMM 算法[J]. 现代雷达,2009,31(5):43-47.

[11] 减荣春,崔平远. 马尔可夫参数自适应 IFIMM 算法研究[J]. 电子学报,2006(3):522-523.

[12] 陈东炎,张 玘,王艳玲,等. 图像跟踪系统中机动目标预测的实现[J]. 应用光学,2007(1):33-37.

(上接第 148 页)

[10] 汪文勇,苏鹏声. 下一代互联网实名访问机制研究[J]. 电子科技大学学报,2006,35(1):82-84.

[11] 陈俊霞. 基于 HIP 的移动管理关键技术的研究[D]. 成都:电子科技大学,2008.

[12] Trent J,Frederique G,Nayeem I,et al. Role-based access control model for protection domain derivation and management[C]//Proceedings of the ACM Workshop on Role-based Access Control. [s. l.]:[s. n.],1997:95-106.

MANET中基于HIP的访问控制模型研究与设计

作者： 何智勇， 朱纯仁， 方立刚
作者单位： 何智勇,朱纯仁(南京工业职业技术学院 能源与电气工程学院,江苏 南京 210046)， 方立刚(苏州职业大学 计算机工程系,江苏 苏州 215104)

刊名： 计算机技术与发展
英文刊名： Computer Technology and Development
年，卷(期)： 2013(2)