轻量级可移交CA的MANET网络认证体系

郭 萍[1] 傅德胜[1] 朱节中[2] 成亚萍[1]
(南京信息工程大学计算机与软件学院江苏省网络监控中心 南京 210044)[1]
(南京信息工程大学滨江学院 南京 210044)[2]

摘 要 为解决移动自组网(Mobile Ad Hoc Network,MANET)网络信道开放、节点灵活多变且资源受限以及难以部署复杂认证机制的问题,结合轻量级CA思想,构造出一种适用于生存周期短、拓扑结构高度动态变化的MANET的认证体系结构即轻量级可移交认证中心(Lightweight and Shifted Certification Authority,LSCA)。LSCA结构简化了传统基于证书CA机制的公钥产生及验证的复杂性,无需证书管理;同时以移交CA角色的方式工作,不需预先配置节点及预知网络拓扑结构,使系统在不采用门限机制的情况下具备一定的容侵能力。性能分析及仿真实验表明:LSCA对DoS攻击表现出较强的健壮性,在通信、计算及存储代价方面均优于分布式CA及门限机制CA,适用于动态多变、生存周期较短的MANET网络应用。

关键词 无线网络安全,移动自组网(MANET),轻量级移交CA(LSCA),认证体系
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.03.032

Lightweight and Shifted CA Architecture for MANET

GUO Ping[1] FU De-sheng[1] ZHU Jie-zhong[2] CHENG Ya-ping[1]
(Network Monitoring Center of Jiangsu Province,College of Computer and Software,Nanjing University of Information Science and Technology,Nanjing 210044,China)[1]
(Bingjiang College,Nanjing University of Information Science and Technology,Nanjing 210044,China)[2]

Abstract In order to solve the problem that it is difficult to adopt more security and complex authentication mechanisms in mobile Ad hoc network (MANET) because of the opening communication channels, highly dynamic moving and sources-constrained nodes, a lightweight and shifted certificate authority (LSCA) authentication architecture for MANET was put forward, which is combined with an idea of lightweight CA, and it's designed for MANET with short lifetime and highly dynamic topology. LSCA is equipped with the advantage of lightweight CA through simplifying the traditional certificate-based CA, which needs no certificates. Moreover, LSCA, through the transfer of the overall CA among a number of alternative CA nodes in a regular rotation, is not needed to preset nodes and know the topology of MANET, and the system is attained a certain degree of tolerance. Analysis and simulation results show that LSCA has robust resistance for DoS attacks, balances the tradeoff between communication, computation and storage, which is better than distributed CA and CA with threshold mechanism, and is especially suitable for the topology of very dynamic MANET networks.

Keywords Wireless network security, Mobile Ad hoc network(MANET), Lightweight and shifted certificate authority (LSCA), Authentication architecture

1 引言

移动自组网MANET具有自组性、移动性、易部署及无基础设施要求等特点,可广泛应用于军事指挥、政府管理、医疗卫生、紧急灾后营救等众多领域,具有重大的军事价值和广阔的商业应用前景。安全是MANET网络实际部署中的焦点问题,在军事、商业等应用中尤为重要,而认证体系是安全的第一道防线,也是MANET网络安全路由、密钥管理、身份认证、数据安全的基础。大型MANET网络需要数量众多的密钥,这些密钥的安全生成、更新和撤销是非常复杂和困难的。MANET节点资源的有限性、控制的分布性和网络的动态性大大增加了密钥管理的困难程度。因此,设计安全、完善和高效的MANET认证体系具有重要的研究价值。

鉴于基于对称密码体制的密钥在管理及分发上的困难

到稿日期:2015-11-06 返修日期:2016-02-17 本文受国家自然科学青年基金项目(61070133),江苏省大学生实践创新训练计划省级重点项目(201410300049Z),江苏省产学研联合基金创新项目(201400703)资助。

郭 萍(1973—),女,博士,副教授,主要研究方向为信息安全、无线网络安全,E-mail:guoping@nuist.edu.cn;傅德胜(1951—),男,教授,主要研究方向为信息安全、图像处理;朱节中(1974—),男,硕士,副教授,主要研究方向为信息安全、网络安全;成亚萍(1968—),女,硕士,副教授,主要研究方向为信息安全、数字水印。

性，本文只探讨基于非对称(公钥)密码体制的认证机制。经过总结，已有研究成果主要包括以下几种 MANET 网络的公钥认证机制。

(1)集中式 CA 认证机制

这种认证机制是将有线网络中的 PKI(Public Key Infrastructure)[1]体系移植到 MANET 网络中，有两种实现方式：1)有线网络中服务器充当 CA(Certification Authority)为 MANET 网络提供认证及密钥管理服务，这需要 MANET 网络持续访问有线网络，显然不可行；2)MANET 网络中有一个节点充当 CA 角色，承担为其他节点颁发证书(将公钥与证书绑定)、管理证书、撤销证书等工作[2]。由于节点资源受到电能、存储、计算能力等的限制，在 MANET 网络中很难找到这样一个节点来承担 CA 的任务，且这个节点是整个网络的单失效点，容易受到 DoS(Denial of Services)的攻击，很难保障安全性。

(2)分布式 CA 认证机制

文献[3]提出一种局部分布式 CA，假设一个跨域的单 CA 将证书复制到多个充当服务器的节点上，这本质上还是一个单 CA 结构，但只适用于小规模的 MANET 网络，且缺乏对整个协议的详细描述，也没有说明多个服务器间的维护和控制。文献[4]发展了文献[3]的思想，构建了一种全局分布式 CA，将 CA 私钥份额分给网络中的所有节点，增强了分布式服务的可用性，但所有节点都拥有 CA 私钥的份额，增加了 CA 私钥暴露的风险及系统的复杂性，降低了整个系统的安全性。文献[5-6]采用另一种方法，假设每一个节点都是自己域内的 CA，并为相邻其他节点提供信任服务，类似于 PGP(Pretty Good Privacy)[7]思想，但这种传递式的信任机制很难被验证，且这种假设对 MANET 网络来说要求过高。

(3)门限分布式 CA 认证机制

为了增强节点的抗攻击能力，消除系统的单失效点，随着无线设备存储、计算及通信能力的日益增强，原来认为由于资源限制而不适用于无线环境的门限方案得到广泛研究。文献[8]提出一个分布式的信任机制，只有超过门限值的认证服务器一起合作才能颁发证书。文献[9]提出一种基于(t,n)门限机制的认证方案，其允许节点动态变化，重组共享认证服务器私钥。文献[10]提出一种有效的抵御口令猜测攻击的门限认证方案。以上的认证方案虽然都采用了(t,n)门限方案，使得 CA 具有一定的容侵性，但这些方案都基于传统的公钥证书机制 CA，这种 CA 体系任务繁重，承担对证书的管理、维护、撤销及更新工作，在资源相对丰富的有线网络中也容易成为系统瓶颈，加上门限方案的计算复杂性较高，各个认证服务器间需要更多的协同工作，这无疑使得系统负载及复杂性进一步增加，在 MANET 中利用门限机制来共享密钥很难取得理想效果。

(4)自组式 CA 认证机制

在完全没有外部 TTP(Trusted Third Party)支持的情况下，在 MANET 的初始化及运行阶段全部由内部节点承担初始化、密钥分发、管理、维护及撤销等工作。这种 CA 认证机制主要有以下两个问题：1)选择哪些节点承担 CA 工作；2)如何协调一致地维护 CA 功能。文献[11]提出基于簇的自组式 CA 认证机制，将 MANET 网络节点以簇为单位，每个簇的簇头担任 CA 角色，但存在如何选择簇头节点及如何在簇头间平衡负荷的问题。文献[12]利用蚁群优化算法在 MANET 网络簇头间平衡任务，虽然极大地提高了簇头协同工作的能力，但同样面临如何选择簇头节点的问题。文献[13]提出一种采用“隐式认证”思想构建的自组式认证公钥体制密钥协商协议，隐式认证即无证书认证，这种机制中公钥被分为两部分，其中一部分公钥没有经过 CA 签名的绑定，使得替换公钥攻击成为可能，因此其顽健性较差。

本文在前人工作的基础上，结合轻量级 CA 思想，构建一种适用于高度动态变化的 MANET 网络、可切换 CA 角色且具有一定容侵能力的认证体系结构 LSCA (Lightweight and Shifted CA)。LSCA 是建立节点间信任关系，提供认证及密钥管理服务，包括恶意节点撤销的认证架构平台。本文主要在以下几方面不同于前人工作：1)轻量化，以轻量级 CA 代替传统基于证书的 CA，轻量化使移交 CA 角色成为可能；2)对 MANET 节点进行分类，引入活跃 CA 节点和空闲 CA 节点，移交时 CA 角色只能由空闲 CA 节点即潜在活跃 CA 节点担当；3)引入激活机制，当前活跃 CA(Active CA)激活下次业务簇中的某个空闲 CA 节点(Idle CA)，并以该空闲 CA 节点为簇头形成临时簇完成业务，激活机制保证了 CA 的可移交性。在以上 3 点的基础上提出适用于动态 MANET 网络的轻量可移交 CA 的认证架构(LSCA)及基于 LSCA 的节点双向认证协议。

本文第 2 节针对拓扑结构动态多变且应用于紧急任务场景、生命周期较短的这类 MANET 网络提出一种轻量级可移交 CA 角色且具有一定容侵性的认证体系结构；第 3 节讨论所提方案的特点及安全性，并通过仿真实验分析计算通信代价等性能；最后总结全文。

2 轻量级可移交 CA(LSCA)方案描述

本节对 LSCA 的初始化、工作原理(即签名、验证及移交角色的各个阶段)进行详细描述。

2.1 LSCA 初始化

MANET 网络运行的拓扑结构如图 1 所示。

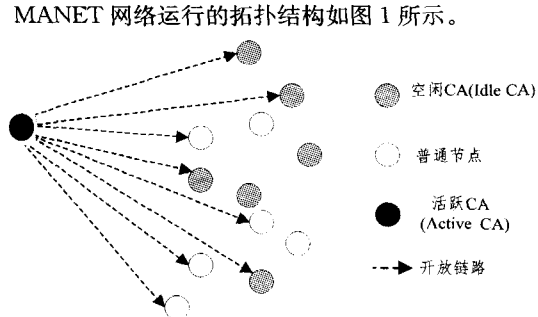

图 1 MANET 网络运行拓扑结构图

系统进行初始化，结果为输出 LSCA 的公/私钥对(PK_{LSCA},SK_{LSCA})；输出节点的主公钥/私钥对$(PK_{N_i}^{Master},SK_{N_i})$，其中$PK_{N_i}^{Master}$是节点的主公钥(篇幅所限，具体初始化过程参见文献[14])。

2.2 LSCA 的工作机制

2.2.1 LSCA 中的节点构成

初始化后，MANET 网络由 3 种不同节点构成。

(1)活跃 CA(Active-CA)节点：这类节点由存储能力较强、计算资源较丰富的节点构成，一个时刻只有一个节点真正

执行 CA 角色的功能。

(2)空闲 CA(Idle-CA)节点:资源相对丰富的节点,这类节点根据其信任度值[15]及所持资源情况在下一次业务中可能被选中成为 Active CA,并以 Active CA 作为簇头构成临时簇执行一次业务。其因曾承担 CA 角色为普通节点提供认证及密钥管理工作,所以即使移交 CA 权限也不能视作普通节点。空闲 CA 的个数决定了在整个 MANET 网络生存期间可移交的 CA 个数,它与 MANET 网络的规模和对安全的要求有关。

(3)非 CA(Non-CA)节点:通常是资源受限的普通节点。

2.2.2　LSCA 的工作过程

(1)LSCA 通告当前 Active-CA 节点

当前具有 CA 权限的节点广播 Active-CA 消息,如式(1)所示。

MESSAGE1:BROADCAST_ACTIVE_CA

$$CA_i \rightarrow N_{(j\cdots n)}, CA_{(j\cdots n)}, IDLE\_CA_{(j\cdots n)}$$

$$[ID_{CA_i}, ID_{CA_{i-1}}, PK_{CA_i}, T_{stamp1}, BCAST\_COUNT, H(ID_{CA_i} | ID_{CA_{i-1}} | PK_{CA_i} | T_{stamp1} | BCAST\_COUNT)] \quad (1)$$

其中,T_{stamp1} 是时间戳,哈希函数 $H(ID_{CA_i} | ID_{CA_{i-1}} | PK_{CA_i} | T_{stamp1} | BCAST\_COUNT)$ 用来进行完整性较验,ID_{CA_i} 是当前 Active-CA 的身份标识,且当前 Active-CA 是由之前的 $ID_{CA_{i-1}}$ 转交 CA 权限而对当前的交易形成的新的簇,PK_{CA_i} 是当前 Active-CA 的公钥。Idle-CA 和非 CA 节点可以从 ACTIVE-CA 消息中识别当前 Active-CA。*BCAST_COUNT* 参数累计由其他中间 Idle-CA 节点重新广播该消息直到达到最大值(这个值通常在初始化时根据网络规模及安全要求设定)从而限制重复广播的次数。

(2)LSCA 为节点生成辅公钥

初始化结束后,节点的公钥由自己保存,如果需要与其他节点通信,必须先由 LSCA 辅助其生成辅公钥并向 LSCA 申请与之通信节点的公钥信息。因此,有通信需求的节点必须向当前 Active-CA 申请辅公钥,如式(2)所示。

MESSAGE2:SLAVERY_PUBLIC_KEY_REQUEST

$$N_j \rightarrow CA_i: E_{PK_{CA_i}}[ID_{N_j}, PK_{N_j}^{Master}, T_{stamp2}, H(ID_{N_j} | PK_{N_j}^{Master} | T_{stamp2})] \quad (2)$$

Active-CA 收到消息(2)后,用自己的私钥解密得到节点 N_j 的身份标识 ID_{N_j} 及公钥 $PK_{N_j}^{Master}$,根据节点身份标识,查询节点状态列表 NSL(Node State lists),如果节点状态处于可信,则计算 $H'(ID_{N_j} | PK_{N_j}^{Master} | T_{stamp2})$ 并将其与收到的 $H(ID_{N_j} | PK_{N_j}^{Master} | T_{stamp2})$ 比较,若相等则说明节点 N_j 在发送消息(2)的过程中没有被篡改,Active-CA 发送响应报文,如式(3)所示。

MESSAGE3:SLAVERY_PUBLIC_KEY_REPLY

$$CA_i \rightarrow N_j: E_{PK_{N_j}^{Master}}[PK_{N_j}^{Slavery} = Sign_{SK_{CA_i}}(ID_{N_j} | PK_{N_j}^{Master}), T_{stamp3}] \quad (3)$$

Active-CA 为节点 N_j 生成辅公钥 $PK_{N_j}^{Slavery} = Sign_{SK_{CA_i}}(ID_{N_j} | PK_{N_j}^{Master})$,即 Active-CA 用自己的私钥对节点 N_j 的身份标识 ID_{N_j} 及其主公钥 $PK_{N_j}^{Master}$ 签名。

(3)节点间的双向认证

初始化结束后,任何需要通信的非 CA 节点向当前 Active-CA 请求目的节点公钥并验证其身份的合法性。协议假设至少一个非 CA 节点处于当前 Active-CA 节点的范围内,以致 Active-CA 可以为请求节点与目的节点间初始化一条安全信道。如果节点 N_j 想与节点 N_{j+1} 通信,双方必须先验证身份并交换主公钥,如式(4)、式(5)所示。

MESSAGE4−5:BILATERAL_AUTHENTICATION

$$N_j \rightarrow N_{j+1}: [PK_{N_j}^{Slavery}, T_{stamp4}, H(PK_{N_j}^{Slavery} | T_{stamp4})] \quad (4)$$

$$N_{j+1} \rightarrow N_j: [PK_{N_{j+1}}^{Slavery}, T_{stamp5}, H(PK_{N_{j+1}}^{Slavery} | T_{stamp5})] \quad (5)$$

节点 N_j 及节点 N_{j+1} 交换辅公钥,用 Active-CA 公钥验证后,分别得到对方的主公钥,同时验证了对方确实是由 Active-CA 签名的合法节点。双方可以协商会话密码,进而通过安全通道发送消息。

(4)LSCA 系统 CA 权限的移交

在成功结束一次通信后,当前 Active-CA 根据业务需求选择可用的 Idle-CA,通过消息 TRANSFER_CA_OWNERSHIP 转交 CA 角色,如式(6)所示。

MESSAGE 6:TRANSFER_CA_OWNERSHIP

$$CA_{i-1} \rightarrow CA_i: [ID_{CA_{i-1}}, ID_{CA_i}, T_{stamp6}, E_{PK_{CA_i}}(CA_{i-1}, CA_i, T_{stamp6}), BCAST\_COUNT, H(ID_{CA_{i-1}} | ID_{CA_i} | T_{stamp6} | E_{PK_{CA_i}}(CA_{i-1}, CA_i, T_{stamp6}) | BCAST\_COUNT)] \quad (6)$$

如果信道中没有节点通信,当前 Active-CA 等待一段时间后(通常是介质访问层 MAC 帧传输时延的 2 倍[15])仍然要转交 CA 权限以提高安全性。新的 Active-CA 广播消息 BROADCAST_ACTIVE_CA(见式(1))来宣布自己的 CA 角色,这将形成以当前 Active-CA 节点为簇头的临时簇,其存活时间等于当前一次通信的时间。广播消息的特性及在消息中出现的之前的 Active-CA 身份标识(即 $ID_{CA_{i-1}}$)及新选出的 Active-CA 的身份标识(即 ID_{CA_i})有助于识别任何恶意 Active-CA。式(1)中 *BCAST_COUNT* 所统计的值用于限制重复广播的次数,这个值只能在 CA 节点(包含 Active-CA 及 Idle-CA)发送的消息中找到。Active-CA 发送的消息被中间 Idle-CA 重复广播,同时消息中 *BCAST_COUNT* 值每重复广播一次就自增一次,直到消息到达目的节点;如果 *BCAST_COUNT* 达到最大值时消息仍未到达目的节点,将放弃此次通信。合理设置 *BCAST_COUNT* 值可有效控制簇规模及通信负载。

3　LSCA 的性能及安全性分析

本节对 LSCA 的性能及安全性进行分析。首先总结 LSCA 的结构特点,通过一系列仿真实验讨论 LSCA 在存储、通信、计算等方面的代价;然后针对无线环境下易实施的攻击,分析 LSCA 的抵抗能力。

3.1　LSCA 的结构特点

1)对网络拓扑结构变化的容忍性,甚至是较频繁的网络分化,LSCA 具有较好的自适应性。2)简单的预配置。只需要对初始承担 CA 角色的节点进行配置,随着网络的运行,形成 LSCA,其他节点信任关系的建立由 LSCA 负责,这极大减少了初始化时的配置工作,因此 LSCA 适合于生存周期短、需快速配置、执行特殊任务的 MANET 网络的应用场景。3)LSCA对节点信任关系的快速建立。LSCA 不是集中式 CA,不是分布式 CA,也不同于基于证书链的自组式 CA,它是一种漫游着的集中式 CA,或者是一种不可预知的、临时的、动态的且生存周期极短的、由某个节点承担的集中式

CA，因此继承了集中式 CA 能够方便快捷地建立节点间信任关系的优点。4）健壮性。LSCA 在一次业务完成后将当前 CA（称为 Active-CA）角色移交给下一次业务所涉及节点中可信的空闲节点（称为 Idle-CA），在不需要任何预配置的情况下形成以 Idle-CA（一旦激活即是 Active-CA）为簇头的临时簇，其生存周期仅限于当前业务或一次交互。这与长久簇的概念完全不同，系统健壮性的提高使得针对无线环境的各种攻击难以取得较好的效果。

3.2 LSCA 的计算代价分析及实现

本方案中节点的计算主要是加密/解密数据（如消息 2、消息 4 和消息 5）以及在交互过程中对数据进行完整性校验的哈希运算，CA 节点及非 CA 节点计算类型的统计具体如表 1 所列。

表 1 CA 节点及非 CA 节点计算类型统计

消息	Active-CA 节点	Idle-CA 节点	非 CA 节点
1	Hash	Hash	Hash
2	Hash	—	加密、Hash
3	加密、签名	—	解密、验证
4	—	—	Hash
5	—	—	Hash
6	加密、Hash	解密、Hash	—
总计	加密 2/4 次、签名 1 次、Hash 运算 3/5 次	解密 1/3 次、Hash 运算 2/4 次	加密 1 次、解密 1/3 次、验证 1 次、Hash 运算 4/6 次

表中统计数据不计节点在初始化过程中产生的公/私钥计算代价，只计算交互过程中各类型节点的最大计算量。“/”前的数字表示无需撤销节点时节点的计算次数；“/”后的数字表示包含所有消息时节点的计算次数。计算量的评估通过原型实现。只考虑理想情况，假设有 6 个节点，其中包含 2 个 CA 节点（1 个 Active-CA 节点和 1 个 Idle-CA 节点），剩余的为非 CA 普通节点，形成两个簇，场景如图 2 所示，其中 M 代表 Message（各消息意义详见 2.2.2 节），图中标识了各种类型节点发送及接收消息的情况。

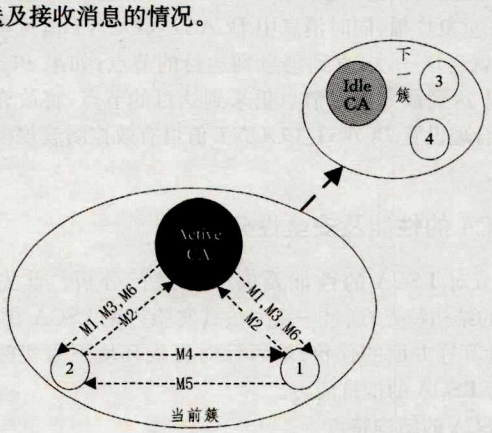

图 2 LSCA 原型实现通信模型

两个 CA 节点计算机配置相同（CPU Intel DuoDore 1.99 GHz，RAM 2GB），4 个普通节点笔记本配置相同（HP6520s，CPU 1GHz，RAM 1GB）。本方案与门限及基于身份的认证机制不同，门限认证机制初始化及通信的负载均较高，基于身份的认证机制的节点计算较复杂（如初始化、加密、提取及执行等），各种机制的设计目的、实现算法、执行过程完全不同。鉴于此，本方案 LSCA 不与其他类型的认证机制在计算量上进行比较，但是用不同算法来实现本方案设计，以定量分析计算复杂性。加密/解密算法分别采用 ECC（Elliptic Curve Cryptograph，160bits）/RSA（Rivest-Shamirh-Adleman，1024bits）实现，完整性校验分别用 SHA-1（Secure Hash Algorithm，128bits）/MD5（Message Digest，128bits）实现。

各种类型节点的计算耗时如图 3 所示。由图可知，对于加密和验证，RSA 比 ECC 快了大约 6 倍，但是对于解密和验证，ECC 比 RSA 快了大约 7 倍。SHA-1（128bits）CA 节点签名时间约为 0.28E−7ms，MD5（128bits）CA 节点签名时间约为 0.71E−3ms，前者比后者快了大约 25000 倍。这些不同的加密或签名算法，实现技术不同，密钥长度不同，应用环境不同，可能达到的安全强度也不同，通常作为安全措施中重要的一环，和其他安全协议结合使用。图 3 通过简单比较旨在为 LSCA 选择更合适的加密算法（ECC）和签名算法（SHA-1），因为计算时间越短，计算延迟和计算耗能就越低。

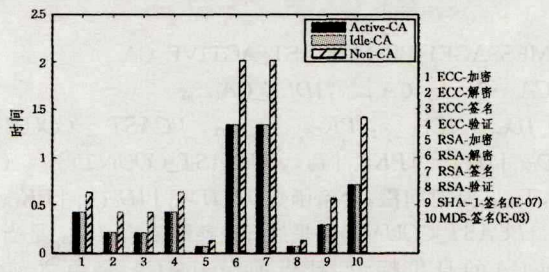

图 3 不同类型的节点执行不同算法所需时间

3.3 LSCA 通信代价的分析及仿真

用仿真工具 OPNET[16] 验证如图 2 所示通信模型 LSCA 的通信代价，仿真参数配置如表 2 所列。

表 2 仿真参数设置

参数	值	参数	值
仿真环境	OPNET10.0	MAC 协议	MAC-802.11b
分组大小	512Bytes	数据传输率	11Mbps
节点移动速度	5m/s	RSA 密钥长度	1024bits
节点分布范围	100 * 100 网格	ECC 密钥长度	160bits
节点规模	[10,50]	SHA-1	128bits
仿真时间	600s	MD5	128bits

仿真结果如图 4 所示。

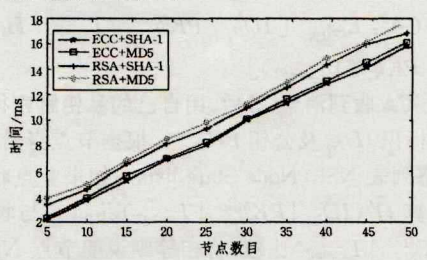

图 4 不同算法组合的情况下 LSCA 通信时间的对比

考虑消息 1−消息 6 这 3 种节点的总通信量，加/解密算法及签名算法分为 4 种情况（即 ECC+SHA-1，ECC+MD5，RSA+SHA-1 和 RSA+MD5）进行测试。在节点数目相同的情况下，4 种组合的通信量差别并不大，ECC+SHA-1 的通信量占用时间最少，其他从小到大依次为 ECC+MD5，RSA+SHA-1，RSA+MD5。这主要是由于在节点处采用不同的加/解密算法及签名算法引起的总通信时间不同。

图 5 是对不同类型节点通信量的分析。仿真参数如表 2 所列，加密、解密及签名算法为 ECC，哈希运算为 SHA-1 算法。5 个节点形成一个临时簇，Active-CA 首先广播自己的 CA 角色（即消息 1），然后为簇内 4 个节点签名发送辅公钥

(即消息 3)，最后移交 CA 给 Idle-CA 节点(即消息 6)；节点向 Active-CA 申请辅公钥(即消息 2)，然后两两节点间进行一次双向认证(即消息 4、消息 5)。Idle-CA 节点是由 Active-CA 节点转交 CA 角色后形成的，因此其通信量即是 Active-CA 的通信量，此处不单列 Idle-CA。由图 5 可见，Active-CA 的通信量远远小于 Non-CA 节点的通信量，因为 Non-CA 节点除了向 Active-CA 申请辅公钥外，还需两两节点间双向认证，而不需 Active-CA 参与。本方案中的 Active-CA 负责向临时簇内的节点签名并发送辅公钥，移交 CA 角色，撤销非法节点。图 5 没有考虑撤销节点的操作，可以看出，Active-CA 的通信量随着节点的增多呈缓慢上升的走势，即使节点数目达到 50，在本仿真场景下，Active-CA 发送的数据包大约为 2000 字节左右，这非常有利于 Active-CA 的切换移交。

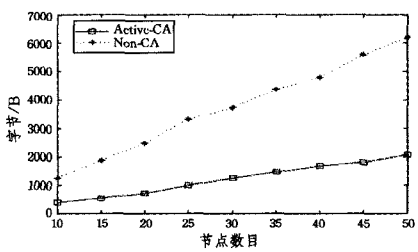

图 5　不同类型节点的通信量对比

图 6 示出了 Active-CA 的切换频率对通信负载的影响。仿真场景：以 30 个节点为例，Active-CA 分别移交 2 次、5 次、10 次、15 次，即临时簇的节点个数分别为 10，3，2。Active-CA 只发送消息 1、消息 3 和消息 6，结果如图 6 所示。

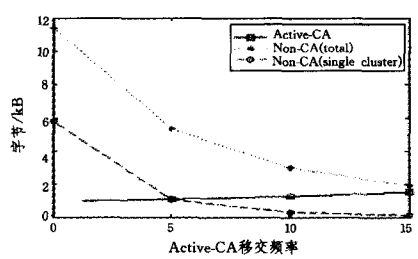

图 6　Active-CA 移交频率与发送数据量的关系

由图 6 可知，移交频率越高，Active-CA 发送的数据量越大，因为需要额外多次广播消息 1(Message1：Broadcast Active_CA)和消息 6(Message 6：Transfer CA Ownership)，移交 15 次时的通信量比移交 2 次时的增长了 57%。但是对于 Non-CA 节点，通信量却随着 Active-CA 移交频率的增加而下降，因为移交次数越多，意味着形成的临时簇越小，簇内节点与 Active-CA 的交互次数及节点间的双向认证次数也大幅下降，移交 2 次时 Non-CA 节点的通信量是移交 15 次时的 45 倍，即使对于所有簇的 Non-CA 节点总通信量也呈下降趋势，移交 2 次时所有簇 Non-CA 节点的通信量是移交 15 次时的 5.9 倍。可见，适当选取 Active-CA 移交次数及簇内节点数量可以很好地平衡网络负载与能耗之间的矛盾。

3.4　LSCA 安全性分析

本节分析 LSCA 对无线环境中易施攻击的抵抗性。

3.4.1　重放攻击

严格的同步要求及每次传输消息都嵌入的时间戳保证了恶意攻击者很难进行重放攻击，而且 Active-CA 广播宣布自己的 CA 角色及广播消息传输跳数的限制，可进一步预防重放攻击。即使攻击者截获部分有用信息或之前的数据包，接收者根据时间戳及同步关系也能很容易判断是否为伪造数据包。

3.4.2　中间人攻击

攻击者如果想截获通信双方数据包而冒充成合法用户，必须拥有 LSCA 颁发的辅公钥，即使假造一个 $PK_{attacker}^{Slavery}$，声称自己是合法用户，但是攻击者的 $PK_{attacker}^{Slavery}$ 没有经过 LSCA 签名，即用 LSCA 的公钥解密 $PK_{attacker}^{Slavery}$ 无法得到($ID_{attacker}$ | $PK_{attacker}^{Master}$)，因此很容易判定攻击者不是经 LSCA 认证的合法用户。由于辅公钥的使用类似于传统 CA 系统中的证书，在不知道 LSCA 私钥的情况下，攻击者不能伪造虚假身份，因此类似伪造攻击很容易被识别。如果截获合法 CA 节点的 ID 和公钥，但是攻击者并不拥有所冒用合法 CA 节点的私钥，因此在通信过程中并不能解密由 CA 公钥加密的消息 1、消息 2 和消息 6。

3.4.3　DoS 攻击

DoS 攻击在无线环境下通常是致命的。无线信道的开放性以及无线设备资源的受限性使得 DoS 攻击特别有效，因为很容易耗尽关键节点的资源而导致网络不可用。门限机制虽然能较好地预防 DoS 攻击，但承担服务器的节点是固定的，门限值过低，很容易被攻陷；而门限值过高，通信负荷对无线设备会造成巨大压力。本方案的 LSCA 是以移交 CA 权限的方式工作的，即以 Active-CA 为簇头形成临时簇来为参与本次交互的节点提供认证及密钥管理服务。换言之，CA 角色在不确定的节点间轮转，移交给哪个节点事先不能决定，而是取决于下一次业务的需求。轮转的时间取决于业务所持续的时间。这些都极大地增强了系统的健壮性及攻击的不可预见性，使得本系统对 DoS 攻击有较好的抵抗性及容忍性。

结束语　针对移动自组网 MANET 拓扑结构多变的问题，基于节点资源受限且移动性更强的特性，结合轻量级 CA 思想，提出在簇头节点集合移交 CA 的动态 MANET 网络认证体系 LSCA。分析及仿真实验表明：LSCA 不仅能消除集中式 CA 的单点失效，而且比分布式 CA 更加简洁高效，特别适合节点拓扑结构多变的应用场景，如战争、自然灾害等生存周期较短的 MANET 网络。在没有显著增加 MANET 网络复杂性的条件下，LSCA 具有一定容侵性，可承担节点密钥的分发、管理及节点的身份认证等工作，同时其在计算量、存储、带宽等方面的性能负载比分布式 CA 及门限机制 CA 更优。

参 考 文 献

[1] PKIX Working Group. Public key infrastructure (X.509)[EB/OL]. The Internet Engineering Task Force (IETF). [2011-8-16]. http://www.ietf.org/html.charters/pkix-charter.html.

[2] ANITA E A M, VASUDEVAN V, ASHWINI A. A certificate-based scheme to defend against worm hole attacks in multicast routing protocols for MANETs[C]// Proc of 2011 IEEE International Conference on Communication Control and Computing Technologies. Ramanathapuram: IEEE, 2011: 407-412.

[3] LUO H, KONG J, ZERFOS P, et al. URSA: ubiquitous and robust access control for mobile Ad hoc networks[J]. ACM Transactions on Networking, 2004, 12(6): 1049-1063.

[4] CHAN A C. Distributed private key generation for identity based cryptosystems in Ad hoc networks [J]. Wireless Communication Letters, 2012, 1(1): 46-48.

(下转第 157 页)

[7] LIU J M, FENG X L, OH C H. Remote preparation of arbitrary two-and three-qubit states [J]. Epl, 2009, 87(3): 30006.

[8] XIA Y, SONG J, SONG H S. Multiparty remote state preparation [J]. J. Phys. B-At. Mol. Opt. Phys., 2007, 40(18): 3719-3724.

[9] AN N B, KIM J. Collective remote state preparation [J]. Int. J. Quantum Inf., 2008, 6(5): 1051-1066.

[10] LIU W J, CHEN Z F, LIU C, et al. Improved deterministic N-to-one joint remote preparation of an arbitrary qubit via EPR pairs [J]. Int. J. Theor. Phys., 2015, 54(2): 472-483.

[11] NGURYEN B A. Joint remote preparation of a general two-qubit state [J]. J. Phys. B-At. Mol. Opt. Phys., 2009, 42 (12): 125501.

[12] WANG D, ZHA X W, LAN Q. Joint remote state preparation of arbitrary two-qubit state with six-qubit state [J]. Opt. Commun., 2011, 284(24): 5853-5855.

[13] HOU K, LI Y B, LIU G H, et al. Joint remote preparation of an arbitrary two-qubit state via GHZ-type states [J]. J. Phys. A-Math. Theor., 2011, 44(25): 255304.

[14] HOU K, WANG J, LU Y L, et al. Joint Remote Preparation of a Multipartite GHZ-class State [J]. Int. J. Theor. Phys., 2009, 48 (7): 2005-2015.

[15] XIAO X Q, LIU J M, ZENG G H. Joint remote state preparation of arbitrary two-and three-qubit states [J]. J. Phys. B-At. Mol. Opt. Phys., 2011, 44(7): 075501.

[16] CHEN Q Q, XIA Y, SONG J, et al. Joint remote state preparation of a W-type state via W-type states [J]. Phys. Lett. A, 2010, 374(44): 4483-4487.

[17] LUO M X, CHEN X B, MA S Y, et al. Deterministic remote preparation of an arbitrary W-class state with multiparty [J]. J. Phys. B-At. Mol. Opt. Phys., 2010, 43(6): 065501.

[18] ZHAN Y B, HU B L, MA P C. Joint remote preparation of four-qubit cluster-type states [J]. J. Phys. B-At. Mol. Opt. Phys., 2011, 44(9): 095501.

[19] AN B, BICH T, DON N V. Joint remote preparation of four-qubit cluster-type states revisited [J]. J. Phys. B-At. Mol. Opt. Phys., 2011, 44(13): 135506.

[20] HOU K. Joint remote preparation of four-qubit cluster-type states with multiparty [J]. Quantum Inf. Process., 2013, 12 (12): 3821-3833.

[21] ZHAN Y B, FU H, LI X W, et al. Deterministic Remote Preparation of a Four-Qubit Cluster-Type Entangled State [J]. Int. J. Theor. Phys., 2013, 52 (8): 2615-2622.

[22] CHEN Z F, CHEN Y F, LIU W J. Scheme for joint remote preparation of four-qubit Cluster-like states with unit sucess probability[J]. Appl. Res. Comput., 2015, 32(9): 2794-2797. (in Chinese)
陈正飞，陈云峰，刘文杰. 一种全概率联合远程制备四粒子 Cluster 类态的方案[J]. 计算机应用研究，2015，32(9)：2794-2797.

[23] DENG F G, LONG G L, LIU X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block[J]. Phys. Rev. A., 2003, 68(4): 042317.

[24] LIU W J, CHEN H W, MA T H, et al. An efficient deterministic secure quantum communication scheme based on cluster states and identity authentication[J]. Chinese Phys B, 2009, 18(10): 4105-4109.

[25] EKERT A, MACCHIAVELLO C. Quantum error correction for communication [J]. Phys. Rev. Lett., 1996, 77(12): 2585-2588.

(上接第 149 页)

[5] CCAPKUN S, BUTTYAN L, HUBAUX J P. Self-organized public key management for mobile Ad hoc networks [J]. IEEE Transaction on Mobile Computing, 2003, 2(1): 52-64.

[6] HAMOUID K. Self-certified based trust establishment scheme in Ad hoc networks [C]// Proc of the 5th International Conference on New Technologies, Mobility and Security. Istanbul: IEEE, 2012: 1-7.

[7] ZIMMERMANN P. The Official PGP User's Guide [M]. MA: MIT Press Cambridge, 1995: 191-198.

[8] EISSA T, RAZAK S A, NGADI M D A. Towards providing a new lightweight authentication and encryption scheme for MANET[J]. Wireless Network, 2011, 17: 833-842.

[9] YANG K, JIA X H, ZHANG B, et al. Threshold Key Redistribution for dynamic change of authentication group in wireless mesh networks[C]// Proc of IEEE Global Telecommunications. Miami: IEEE, 2010: 1151-1156.

[10] SHIN Y C, DONG M K, HUN J L, et al. Mechanism for regenerating CGA using threshold secret sharing in MANET[C]// Proc of the 13th International Conference on Advanced Communication Technology. Seoul: IEEE, 2012: 891-895.

[11] LI X, JING Z. A Trust cluster based key management protocol for Ad hoc networks[C]// Proc of IEEE International Workshop on Anti-counterfeiting, Security, Identification. Xiamen: IEEE, 2007: 371-376.

[12] YANG Y, XUE S Q, LUO M M, et al. A self-adaptive method of task allocation in clustering-based MANETs[C]// Proc of 2010 IEEE International Conference on Network Operations and Management Symposium. Osaka: IEEE, 2010: 440-447.

[13] QIN N Y, FU A M, CHEN S G. Blind Signature-based Handover Authentication Protocol with Conditional Privacy Preserving in LTE/LTE-A Networks[J]. Computer Science, 2015, 42 (8): 145-151. (in Chinese)
秦宁元，付安民，陈守国. LTE/LTE-A 网络中基于盲签名的具有条件隐私保护的切换认证协议[J]. 计算机科学，2015，42(8)：145-151.

[14] GUO P, ZHANG H, FU D S, et al. Hybrid and Lightweight Cryptography for Wireless Sensor Network[J]. Computer Science, 2012, 39(1): 14-19. (in Chinese)
郭萍，张宏，傅德胜，等. 一种混合轻量型无线传感器网络公钥密码方案[J]. 计算机科学，2012，39(1)：14-19.

[15] FENG D G, QIN Y, WANG D, et al. Research on Trust Computing Technology [J]. Computer Research and Development, 2011, 48(8): 1332-1349. (in Chinese)
冯登国，秦宇，汪丹，等. 可信计算技术研究[J]. 计算机研究与发展，2011，48(8)：1332-1349.

[16] LU Z. Research on OPNET Application in Wireless Network Simulation[D]. Shanghai: Fudan University, 2010. (in Chinese)
陆智. OPNET 在无线网络仿真中的应用研究[D]. 上海：复旦大学，2010.