基于可信计算的 Ad Hoc 网络直接匿名证明

张 弢[1],任 帅[2],张德刚[3]
(1. 长安大学 电子与控制工程学院,陕西 西安 710064;
2. 长安大学 信息工程学院,陕西 西安 710064;
3. 云南电力试验研究院(集团)有限公司 电力研究院,云南 昆明 650217)

摘 要:现有的 Ad Hoc 网络完整性认证存在固有的缺陷,且用于传统固定网络的安全认证策略不能适用于 Ad Hoc 网络完整性认证。因此,文中在研究 Ad Hoc 网络特点的基础上,将可信计算和直接匿名证明理论引入 Ad Hoc 网络认证环节中。Ad Hoc 网络安全认证的关键在于对其中各个节点的安全认证,文中在对各个节点认证之前先进行优化。首先在应用硬件层面上建立可信计算平台模块,其次在软件层面上建立直接匿名证明模块,从而实现 Ad Hoc 网络节点认证环节的优化。实际应用表明,文中提出的方案有效解决了 Ad Hoc 节点的安全性问题,降低了 Ad Hoc 网络受攻击的可能性。

关键词:可信计算;Ad Hoc 网络;直接匿名证明;零知识证明
中图分类号:TP391 **文献标识码**:A **文章编号**:1673-629X(2014)04-0147-04
doi:10.3969/j.issn.1673-629X.2014.04.037

Direct Anonymous Attestation to Ad Hoc Networks Based on Trusted Computing

ZHANG Tao[1], REN Shuai[2], ZHANG De-gang[3]
(1. School of Electronic and Control Engineering, Chang'an University, Xi'an 710064, China;
2. School of Information Engineering, Chang'an University, Xi'an 710064, China;
3. Electric Power Research Institute, Yunnan Electric Power Test and Research Institute (Group) Co., Ltd., Kunming 650217, China)

Abstract: The integrity authentication of the existing Ad Hoc networks has inherent defects, and the traditional fixed network security strategy is not appropriate for the integrity authentication of Ad Hoc networks. Therefore, based on the study about the features of Ad Hoc networks, introduce trusted computing and direct anonymous attestation theory into authentication of Ad Hoc networks. The crux of the security authentication for Ad Hoc networks is the security authentication for every node. Optimize the nodes before the authentication. Firstly, constitute trusted computing module on hardware level, and direct anonymous attestation module on software level. The application shows that this scheme can effectively solve security issues of the Ad Hoc nodes, thus declining the attacked possibility of the Ad Hoc networks.

Key words: trusted computing; Ad Hoc networks; direct anonymous attestation; zero-knowledge proof

0 引 言

Ad Hoc 网络为移动设备提供无线通信网络。在 Ad Hoc 网络中,没有固定的基础设施,如基站和移动交换中心。移动节点范围内的通信可以直接通过无线连接,对于那些相聚较远的节点将依靠其中间节点上的路由消息进行路由。

Ad Hoc 网络中的节点不断移动,肯定会导致网络拓扑结构不断变化,这样会使节点的安全性不能被认证,很容易使 Ad Hoc 网络受到非法节点的入侵和攻击[1]。因此,文中将充分发挥可信计算的理论优势,引入可信计算理论[2]对 Ad Hoc 网络节点进行认证,使用直接匿名证明理论[3]增加节点安全认证环节,提高 Ad Hoc 网络整体的安全性能。

收稿日期:2013-06-25 **修回日期**:2013-09-28 **网络出版时间**:2014-01-28
基金项目:中央高校基础研究项目(2013G1240118);国家"863"高技术发展计划项目(2012AA112312);交通运输部项目(2012-364-208-600,2012-364-208-200,201231849A70);吉林省外国专家局项目(2012-7-102-2)
作者简介:张 弢(1984-),女,山西吕梁人,讲师,博士,研究方向为网络与信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20140208.1655.001.html

1 Ad Hoc 网络安全性分析

移动 Ad Hoc 网络是一组带有无线收发装置的移动节点组成的一个多跳的临时性自组织系统,它具有动态拓扑、自组织、多跳性、无中心等特点,因此带来了无线接入的灵活与便利,同时它也具有生存时间短、安全有限性等缺点,所以其安全性也具有如下漏洞:

1)节点的脆弱性:Ad Hoc 网络中的节点通常由各种便携式移动设备充当,所有节点地位平等,理论上不存在中心节点。虽然 Ad Hoc 网络的分布式特性相对于集中式的网络具有一定的抗毁性,但是通常比固定网络更容易受到物理安全攻击,易于遭受窃听、欺骗和拒绝服务等攻击[4-5]。同时,移动节点不能或很难做出复杂的公共密钥加密计算,所以一些恶意攻击者会通过强制节点重组等操作让移动节点设备进行恶意耗电,或者发出一种特殊类型的拒绝服务攻击[6]。

2)基础设施缺乏:基础设施缺乏统一的认证机构,传统的电子商务安全解决方案已经不再适用于移动 Ad Hoc 网络[7]。

3)路由机制威胁:Ad Hoc 网络路由机制设计是去保护无障碍路由信息、路由信息的完整性以及消息的路由可靠[8]。

作为一个无中心和自组织的网络,寻找 Ad Hoc 网络的路由以及维护路由需要节点之间的相互合作。另一方面,节点的移动性让 Ad Hoc 网络自身的资源和能力有限,缺乏有效的网络物理保护。凡此种种,都令 Ad Hoc 网络路由机制面临着各种安全威胁,主要类别如下[9]:

(1)路由篡改:攻击者篡改路由信息,并利用伪造身份节点作出虚假的路由信息。

(2)路由隐藏:攻击者通过特殊的方式隐藏在可靠的路由节点中(仅由内部合法的路由节点),控制路由协议并进行路由攻击,控制通信网络流量等。

综上所述,移动 Ad Hoc 网络如此脆弱和不安全,无线节点认证的问题需要根本的解决。文中将介绍可信计算理论,可信计算可以利用较低成本实现移动 Ad Hoc 网络的高安全性身份验证的目的。

2 基于可信计算的节点可信安全解决方案

2.1 可信计算与直接匿名证明

可信计算开发出了硬件级的可信平台模块(TPM)的概念[10]。TPM 可借助物理方式为网络节点到可信环境的连接提供硬件基础。TPM 安全芯片能有效地保护 PC、防止非法用户访问。目前提供了两个版本的 TPM 解决方案,一个是隐私 CA,另一种是直接匿名证明(DAA)。基于 TPM 的"信任根"的功能是利用直接匿名认证实现访问网络的安全认证,并在特设的网络环境,使网络节点的安全性值得信赖。

直接匿名证明可以实现远程认证授权,且在进行身份认证时不暴露移动节点的真实身份,从而保护节点用户隐私。其原理是认证(TPM)产生 DAA 的组签名密钥,并从 DAA 密钥得到签名(证书)[11-12]。之后,利用 DAA 键 AKIi,验证者,以及时间生成签名 DAA PKI,并发送给 DAA 验证者,如图 1 所示。

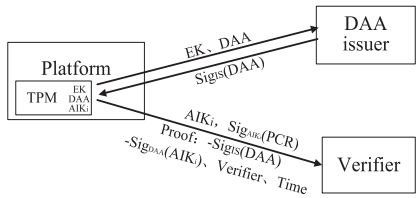

图 1 直接匿名证明策略

DAA 要实现匿名机制,必须采取合理的签名方案。而 DAA 采用了 Camenisch-Lysyanskaya 签名机制,TPM 安全芯片生成的成员公钥签发证书时利用的是基于离散对数的知识证明[13]。上述签名方案的步骤如下:

(1)确认来自 DAA 发行者的公钥 n,a,b,d。其中 n 是 RSA 算法的模,$c^e = a^x b^s d \bmod n$ 中的 x 为验证消息的签名;

(2)签署 TPM 公钥,即 DAA = $a^x \bmod n$,其中 x 是 TPM 的密钥;

(3)随机选取数值 s' ,计算 $c' = cb^{s'} \bmod n$,并把结果发送给验证者;

(4)验证者通过公式 $s + es' = s''$,将所得结果代入 $d \equiv c'^e a^{-x} b^{-s'} \bmod n$ 中。看等式成立与否,若成立,则可知 TPM 已经掌握了 c,e,s''。

作为直接匿名证明的数学基础,零知识证明[14]指的是证明者能够在不向验证者提供任何有用的信息的情况下,使验证者相信某个论断是正确的。零知识证明的具体实现有多种方法,下面介绍两种方案,即 Schnorr 验证方案和 Fiat-Shamir 协议。

2.1.1 Schnorr 身份验证

Schnorr 身份验证是一种困难性问题的知识证明[15],且以离散对数为基础。设系统中用于身份认证的参数为 p 和 q(均为素数,q 是 $p-1$ 素数因子),$g \neq 1$,且 $g^p \equiv 1 \bmod q$。证明者取 x_p ,计算 $y_p \equiv g^{x_p} \bmod p$。证明者 P 已知 x_p, y_p, p, q, g ,验证者 V 已知 p, q, g ,Schnorr 身份验证步骤如下:

(1)P 产生一个随机数 $r_1 \in GF(p)$,$r_1 \neq 0$,计算 $S \equiv g^{r_1} \bmod p$,P 将 (y_p, S) 送给 V;

(2)V 产生一随机数 r_2 ,并将 r_2 寄给 P;

(3)P 计算 $v = r_1 + r_2 x_p \bmod p$ 并将 v 寄给 V;

(4)V 校验 $g^v = S (y_p)^{r_2}$,如果相等则接受 P,否则予以拒绝。因为 $g^v \equiv g^{(r_1 + r_2 x_p)} \bmod p \equiv g^{r_1} \cdot (g^{x_p})^{r_2} \bmod p$

$\equiv g^{r_1} \cdot (y_p)^{r_2} \bmod p \equiv S \cdot (y_p)^{r_2}$。

2.1.2　Fiat-Shamir 协议

假定 P 身份有 k 个秘密的数 $x_{p1}, x_{p2}, \cdots, x_{pk}$。令 $n = pq$,作 $y_{pi} \equiv x_{pi}^2 \bmod n$。公开文件中 P 的身份记录为 ID: $y_{p1}, y_{p2}, \cdots, y_{pk}$,具体步骤如下:

(1)选取一随机数 $r \in Z_n$,并计算 $r^2 \bmod n$,P 给 V 送去 (P, r^2);

(2)V 给 P 送去 $b = (b_1, b_2, \cdots, b_k)$,$b_i$ 是随机产生的 0 或 1,即 $b_i \in \{0,1\}$,$i = 1,2,\cdots,k$;

(3)P 计算 $y = rc_1c_2\cdots c_k$,并将 y 送给 V,其中 $c_i = \begin{cases} 1, b_i = 0 \\ 0, b_i = 1 \end{cases}$;

(4)V 检验,若 $y^2 = r^2 \prod_{i=1}^{k} y_{pi}^{bi} \bmod m$ 则接受,否则拒绝。

2.2　特设节点基于可信计算的安全解决方案

由于缺乏在原来的 Ad Hoc 网络的受信任的身份验证链接,使得 Ad Hoc 网络的安全存在隐患。基于可信计算理论,改造原有的认证系统,网络可信验证方面,从而解决了 Ad Hoc 网络节点信任问题。

2.2.1　基于可信计算的 Ad Hoc 网络改造

第一点改造是互联网用户的节点连接 TPM。可信设置的实现是基于 TPM 引入到用户节点这一技术的。使用 TPM 的终端、一个单一的安全模块及其签名密钥(EK),可以生成唯一的独立组 DAA 签名密钥。这是在 Ad Hoc 网络中,基于可信计算的受信任证书颁发的第一步。

第二点改造是添加 DAA 第三方发布机制。DAA 第三方出版商的网络节点(TPM),负责验证的发送效率以及向网络节点发送 DAA 密钥签名。

第三是新增特殊认证服务器:由于有可能 DAA 私钥 x 可以从 TPM 获得,所以为了有效地监控和检测假冒 TPM,整个系统应包括 Ad Hoc 网络中节点的认证服务器。

2.2.2　基于可信计算的 Ad Hoc 网络的身份验证机制

基于可信计算的 Ad Hoc 网络的身份验证机制共有以下 3 个步骤:

(1)待认证者须计算 $NV = \zeta^x \bmod \Gamma$;

(2)抽取 x 并公开,则验证者将无效的 x 代入 $NV = \zeta^x \bmod \Gamma$,并将计算得出的 NV 与被认证者的 NV 对比,若相同,即为假 TPM;

(3)若连续收到很多类似的 NV 认证请求,则根据具体情况处理该认证。

在上述基于可信计算的检验机制中,验证者被允许检测欺骗性的 TPM,而每个被验证者在使用以一定频率改变的同时,也享有了基于 NV 的分析机会,所以许可证服务器应分为两个,授权检查验证和访问验证。根据上述三方面的变化,基于可信计算的 Ad Hoc 网络的结构如图 2 所示。

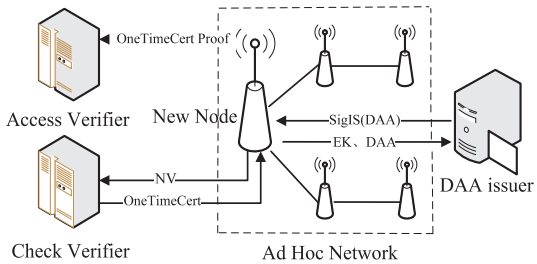

图 2　基于可信计算的 Ad Hoc 网络结构图

2.2.3　基于可信计算的 Ad Hoc 网络认证系统

基于可信计算的 Ad Hoc 网络认证系统同样也有三个步骤:

首先是在向许可证服务器申请之前,使用者首先用 TPM 唯一的 EK 产生一对 DAA 组签名密钥并向 DAA 发布者申请 DAA 公钥证明;

其次,DAA 发行者验证后向用户发送 DAA 密钥的签名;

最后,用户再向许可证服务器提出申请,这时的申请就是自身通过 DAA 密钥算法创造一个有关 AIKi、验证者和时间的签名,并且证明持有一个 DAA 发行者有关 DAA 密钥的签名。

3　安全性分析及实验结论

3.1　节点安全性分析

在基于可信计算的 Ad Hoc 网络中,首先要保证数据的可用性,即在网络节点受到恶意攻击或操控时仍然能够提供必要的服务。其次,要保证信息的机密性,即涉及到重大事件、敏感事件的信息要通过秘密方式传输。第三要保证完整性,包括信息传输途中的连续不间断和信息在用户设备存储时的完整性,也需要依赖于加密或信息隐藏手段,保证信息不被篡改或在遭到篡改时可以还原。此外,还需要保证路由的安全性。其中包括源路由、距离矢量路由、链路状态路由等的安全性。最后,还需对授权检查和访问节点认证所用的服务器分别进行验证,验证步骤如下:

(1)TPM 选取随机数,然后与核查校验模块进行交互,并通过加密算法计算后,将结果发送给核查校验模块进行身份识别和安全性分析,识别和分析通过后,签发通过 DAA 与 TPM 绑定的一次性证书、频率证书;

(2)TPM 与访问校验模块进行交互。访问校验模块使用一组随机数,将零知识证明转换为知识签名,并可以根据频率证书决定是否允许 TPM 访问服务。

3.2　验证结论

根据以上分析,Ad Hoc 网络中基于可信计算可以

成为一种有效的机制,以满足网络节点信任。其优势在于:

(1)没有人可以使用 DAA 公共密钥去确定节点的身份,从而保证 Ad Hoc 节点是可靠的;

(2)仿真实验证明:由于签发的 DAA 与 TPM 绑定的为一次性有效证书,所以有且仅有一次发行机会,因此不会给系统造成瓶颈;

(3)DAA 证书可以颁发给制造商,也可以发给购买的平台。很容易促进基于可信计算的 Ad Hoc 网络的安全性。

4 结束语

如果 Ad Hoc 技术被滥用,会导致大量的网络犯罪,所以文中提出基于可信计算的 Ad Hoc 网络。在节点访问网络之前,使用可信计算理论去验证和监控网络,可以确保网络节点可信,使 Ad Hoc 网络更安全。未来的工作将集中在 Ad Hoc 网络认证评估、TPM 和其他平台研究。随着可信计算的发展,Ad Hoc 将达到一个新的水平。

参考文献:

[1] Abraham J. A survey of intrusion detection for ad-hoc network [J]. Journal of global research in computer science, 2013, 4(4): 182-185.

[2] Noorman J, Agten P, Daniels W, et al. Sancus: Low-cost trustworthy extensible networked devices with a zero-software trusted computing base[C]//Proc of 22nd USENIX security symposium. [s. l.]: [s. n.], 2013.

[3] Brickell E F F, Li J. Apparatus and method for direct anonymous attestation from bilinear maps: U. S., 20, 130, 080, 771 [P]. 2013-03-28.

[4] Deodi P, Shrivastava S, Bhatele M. Security issues in monitoring medical disease through vehicular Ad Hoc network[C]// Proceedings of all India seminar on biomedical engineering 2012 (AISOBE 2012). India: Springer, 2013: 147-152.

[5] 金 伟,刘方爱,王晓洁. 基于 NS 的 Ad hoc 网络路由协议仿真研究[J]. 计算机技术与发展,2010,20(1):63-66.

[6] 沈 奔,秦 军,万 丽. 无线 Ad Hoc 网络中 AODV 路由算法的研究与改进[J]. 计算机技术与发展,2011,21(3):150-153.

[7] Kale M R A, Gupta S R, Prmit R B. An overview of Manet Ad Hoc network [J]. International journal of computer science and applications, 2013, 6(2): 223-227.

[8] Barton M, Kwon T J. Security method for mobile Ad Hoc networks with efficient flooding mechanism using layer independent passive clustering (LIPC): U. S., 20, 130, 145, 461[P]. 2013-06-06.

[9] 李奕男,钱志鸿,刘 影,等. 基于博弈论的移动 Ad hoc 网络入侵检测模型[J]. 电子与信息学报,2010,32(9):2245-2248.

[10] 刘孜文,冯登国. 基于可信计算的动态完整性度量架构[J]. 电子与信息学报,2010,32(4):875-879.

[11] 宋 成,孙宇琼,彭维平,等. 改进的直接匿名认证方案[J]. 北京邮电大学学报,2011,34(3):62-65.

[12] 陈小峰,冯登国. 一种基于双线性映射的直接匿名证明方案[J]. 软件学报,2010,21(8):2070-2078.

[13] 刘雪艳. 基于 ID 可证安全的带权限身份认证方案[J]. 计算机工程,2011,37(4):151-153.

[14] 李 睿,徐秋亮. 一种构造并发不可延展零知识的新方法[J]. 计算机学报,2012,35(4):682-692.

[15] 刘景美,王新梅. Schnorr 签名方案的一种攻击[J]. 计算机科学,2006,33(7):141-142.

(上接第 146 页)

参考文献:

[1] Hua N, Song H, Lakshman T. Variable-stride multi-pattern matching for scalable deep packet inspection[C]//Proc of INFOCOM 2009. [s. l.]: IEEE, 2009: 415-423.

[2] 杨 玲,孟传良. 基于启发式分析的木马检测技术研究[J]. 现代机械,2006(4):61-63.

[3] 唐彰国,李焕洲,钟明全,等. 基于网络通信指纹的启发式木马识别系统[J]. 计算机工程,2011,37(17):119-121.

[4] 孙玉星,黄松华,黄 皓,等. 自治网络中信任信誉模型的安全现状研究[J]. 计算机科学,2009,36(4):5-11.

[5] Martignoni L, Stinson E, Fredrikson M, et al. A layered architecture for detecting malicious behaviors[C]//Proc of RAID'08. Cambridge, USA: [s. n.], 2008: 78-97.

[6] 杨卫平. 面向虚拟机的网络入侵检测系统[D]. 武汉:华中科技大学,2008.

[7] Acharya S, Mills B N, Abliz M, et al. Optwall: A hierarchical traffic-aware firewall[C]//Proc of NDSS. [s. l.]: [s. n.], 2007: 528-533.

[8] 王倍昌. 走进计算机病毒[M]. 北京:人民邮电出版社,2010.

[9] 张仁斌,李 钢,侯整风. 计算机病毒与反病毒技术[M]. 北京:清华大学出版社,2010.

[10] 辛 毅,方滨兴,贺龙涛,等. 基于通信特征分析的蠕虫检测和特征提取方法的研究[J]. 通信学报,2007,28(12):1-7.

[11] 钟明全,李焕洲,唐彰国,等. 基于网络驱动技术的木马通信检测系统[J]. 计算机工程,2010,36(9):150-152.

[12] 单长虹,张焕国,孟庆树,等. 一种启发式木马查杀模型的设计与分析[J]. 计算机工程与应用,2004(20):130-132.

[13] 刘晓石,陈鸿建,何腊梅. 概率论与数理统计[M]. 北京:科学出版社,2006.

基于可信计算的Ad Hoc网络直接匿名证明

作者： 张弢， 任帅， 张德刚， ZHANG Tao， REN Shuai， ZHANG De-gang

作者单位： 张弢,ZHANG Tao(长安大学 电子与控制工程学院,陕西 西安,710064)， 任帅,REN Shuai(长安大学 信息工程学院,陕西 西安,710064)， 张德刚,ZHANG De-gang(云南电力试验研究院 集团 有限公司 电力研究院,云南 昆明,650217)

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2014(4)