一种基于TPM增强的ARAN安全路由协议

王 博 黄传河 杨文忠 王 桐
(武汉大学计算机学院 武汉 430072)

摘 要 安全路由协议设计是Ad hoc网络安全研究的重要组成部分。当前研究主要集中在采用经典密码学中的方法来保证路由安全。结合可信计算中的TPM和典型的安全路由协议ARAN,提出了一种新的安全路由协议TEARAN,该协议不再采用集中式的公钥证书分发中心PKI,而是采用TPM中的DAA(Directed Anonymous Attestation)方式来进行节点的身份认证,以及软安全中可信阈值来监测邻居节点的行为,从而进行公钥可信分发,同时确保了无恶意节点加入网络,另外,也采用公钥签名、会话密钥加密来保证端到端通信的保密性、完整性和不可否认性。理论证明了提出的TEARAN协议能够实现网络的匿名安全,防范当前常见的攻击方式,达到了很好的安全保证效果。

关键词 TPM,安全路由,可信,匿名,Ad hoc网络

Enhanced Secure Routing Protocol Based on TPM

WANG Bo HUANG Chuan-he YANG Wen-zhong WANG Tong
(School of Computer, Wuhan University, Wuhan 430072, China)

Abstract The design of secure routing protocol is one of an important part of research on network security for Ad hoc networks. At present, the research mainly focuses on means of classic cryptograph to guarantee security of routing. Integrating TPM of trusted computing and typical secure routing protocol - ARAN, this paper proposed a new secure protocol called TEARAN, this protocol doesn't adopt the way of the centralized public key certificate issued center - PKI, but utilizes the technique of DAA in TPM to authenticate the identity of each node, and employs the trust threshold of soft security to monitor the behavior of neighbor nodes, so that attaining the purpose of the trust-distributed public key, in addition, avoiding malicious nodes joining in the network. This paper also assured the end to end confidentiality, integrity and non-repudiation. By theoretical analysis on the proposed TEARAN was presented to satisfy the demand of anonymous security, resist conventional malicious attacks and possess better security in effect.

Keywords TPM, Secure routing, Trust, Anonymity, Ad hoc networks

1 引言

由于Ad hoc网络自身具有开放性的特点使得在设计路由协议时,必须加入安全因素进行考虑,并且传统有线网络安全路由协议的研究不再适合Ad hoc网络,因此该网络路由安全问题也成为当前学术研究的热点之一[1,2]。

目前对Ad hoc网络路由的攻击主要集中在被动攻击和主动攻击两类[2]。

被动攻击指恶意节点并不破坏路由协议的正常运行过程,而仅仅通过监听路由的建立过程来捕获有用的路由信息。

主动攻击指恶意节点通过阻止路由的建立、更改以及利用虚假路由信息来获得网络的认证和授权等恶意行为,从而破坏网络的正常运行。主动式攻击又可进一步分为外部攻击和内部攻击两种。外部攻击是指位于网络外部的攻击者对网络发起的攻击,而内部攻击是指网络内部节点被俘获之后被入侵者用来在网络内部发起攻击。

为了防范这两类攻击,当前存在的安全路由协议主要有:基于DSR协议的Ariadne[3]、SRP[7]和ARAN[5]、基于AODV协议的SAODV[6]以及基于表驱动路由协议的SEAD[4]等。这些协议基本上都是采用经典密码学中的Hash函数、对称加密算法、公开密钥算法、数字签名和密钥管理等成熟技术来设计安全路由协议,大部分协议都只能监测和避免网络中的部分攻击,但总体来说,ARAN协议的安全性是最好的。

基于以上的研究基础,把当前研究热点可信计算应用到Ad hoc网路中进行安全路由协议的设计是本文的创新。本文结合可信计算中的可信平台模块[10](TPM, Trusted Platform Module),以及数据安全存储、密钥安全生成、加解密算法引擎模块,来加快网络路由协议的身份认证和加解密的计算过程,同时对ARAN协议进一步改进,不再采用集中式的公钥管理中心PKI,而是采用TPM中的DAA[12]方式来实现平台的身份认证和鉴别,也基于软安全中可信的思想,建立了节点的可信阈值监测,剔除了恶意节点进入网络,实现了节点之间的公钥的可信分发,从而保证了路由建立过程中的不可否认性、保密性和完整性,增强了网络的防御能力。

到稿日期:2009-12-30 返修日期:2010-03-15 本文受国家自然科学基金重点项目(60633020)资助。

王 博(1982—),男,博士生,主要研究方向为无线网络、网络安全和QoS,E-mail:wbxyz@163.com;黄传河 男,博士,教授,博士生导师,CCF高级会员,主要研究方向为计算机网络和网络安全,分布并行处理、量子计算等。

2 可信计算介绍

可信计算技术[9]的主要思路是以密码学技术为基础，在现有计算平台上嵌入一个可信平台模块 TPM 作为可信根，通过可信度量的方式建立起一个从可信根[10]开始的信任链，这样一级度量一级，一级认证一级，从而将这种信任关系从底层硬件扩展到操作系统，再扩展到上层应用，最终建立起一个可信的应用环境。TCG[11]所提出的可信计算平台的通用结构如图 1 所示。

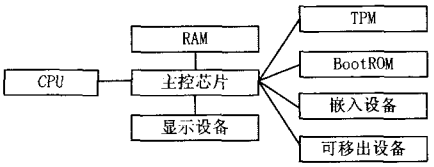

图 1 可信计算平台的通用结构

TPM 是可信计算平台的信任根源，一个签名密钥绑定到一个 TPM 上，一个 TPM 绑定到一个平台上，从而使得一个签名密钥对应唯一的一个平台，数据是否可信由该签名密钥去保证。TPM 功能结构图如图 2 所示，其中非对称密钥算法引擎能够有效加速 RSA，ECC 和 DSA 等各种常用公钥算法的运算，对称密钥算法引擎能有效加速 3DES 和 AES 等对称密钥密码算法的运算，散列算法引擎和签名加解密模块可以进行数字摘要、签名与认证等操作。

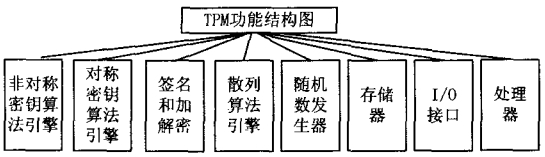

图 2 TPM 功能结构图

可信计算平台可以实现如下功能：①确保用户唯一身份、权限、工作空间的完整性、一致性；② 确保存储、处理、传输过程的机密性、完整性；③ 确保硬件环境配置、操作系统内核、服务及应用程序的完整性；④ 确保密钥操作和存储的安全；⑤ 确保系统具有免疫能力，从根本上阻止病毒和恶意代码。并且可信计算平台提供了确保和验证系统可信的机制，从而有利于建立一个真实可信的计算环境。

3 ARAN 协议

ARAN 协议利用经典密码学中的节点身份认证和数字签名技术来确保端到端节点之间的认证、消息的完整性和不可否认性，从而增强协议的安全性。

ARAN 协议采用公钥密码技术为路由正常运行提供安全保证，主要包括证书的申请、路由查找、路由维护和证书撤销等几个方面。在 ARAN 协议中，引入一个集中式认证服务器(PKI)，所有节点都已知其公钥，在加入这个网络之前，所有的节点都必须通过身份认证后从这个可信的认证服务器得到其颁发的证书，证书中的内容包括：

$T \rightarrow A: cert_A = [IP_A, K_{A+}, t, e]K_{T-}$

如果节点 A 需要与目的节点 X 进行正常通信，而其路由表中不存在到目的节点的路由，则发起路由请求，广播一个路由发现包 RDP 给邻居节点：

$A \rightarrow brdcast: [RDP, IP_X, cert_A, N_A, t]K_{A-}$

当邻居节点 B 收到了路由发现包后，建立一条到源节点的反向路径，然后利用证书中节点 A 的公钥来检查节点 A 签名的有效性和证书的时效性，同时它采用 (N_A, IP_A) 来检查是否已经处理过此路由发现包，如果没有处理，则节点 B 将对 RDP 包进行签名并将自己的证书附在 RDP 包之后，然后继续广播出去：

$B \rightarrow brdcast: [[RDP, IP_X, cert_A, N_A, t]K_{A-}]K_{B-}, cert_B$

节点 B 的邻居节点 C 收到广播包后，首先检查 B 的签名是否正确和此广播包是否已经处理过，然后节点 C 将节点 B 的签名和证书清除，利用自身的私钥对 RDP 包进行签名，并相应地附上自身的证书后，再次广播给下一跳邻居节点：

$C \rightarrow brdcast: [[RDP, IP_A, cert_A, N_A, t]K_{A-}]K_{C-}, cert_C$

最终 RDP 包到达目的节点 X，X 只回复接收到的第一个 RDP 包，并沿着反向路径向源节点 A 发送 REP 包(节点 X 的邻居节点为 D)：

$X \rightarrow D: [REP, IP_A, cert_X, N_A, t]K_{X-}$

假设节点 D 的下一跳是 C：

$D \rightarrow C: [[REP, IP_A, cert_X, N_A, t]K_{X-}]K_{D-}, cert_D$

然后节点 C 与上面的过程类似，核对 REP 包的正确性后，替换为节点 D 的签名和证书，利用自身的私钥签名并附加证书后按照发送 RDP 包时缓存的反向路由转发给其邻居节点。

从以上的路由建立过程中可以发现：网络节点通过端到端的认证，使具有有效证书和公钥的节点才能转发数据包，并且源节点对路由发现包进行签名，保证了路由包在传送过程中的不可否认性，而且只有目的节点才能响应路由发现，从而阻止恶意节点参与路由发现和路由响应过程。通过对协议进行深入分析：采用公钥密码技术，可以有效地阻止伪造、篡改、欺骗等攻击方式。与其他安全协议比较，ARAN 协议是当前安全性能最好的协议，但是该协议是以较高的计算量和网络负荷为开销来保证网络安全的。

4 TEARAN 协议

4.1 问题的描述

根据第 3 节对 ARAN 协议的分析，得出该协议有以下不足：

1)由于 ARAN 协议采用了证书认证鉴别的方式，节点用自己的私钥对路由发现包进行签名，从而有效地保证了参与路由的所有节点都必须以获得有效的证书为前提，使得不安全以及无证书的节点无法参与路由的建立过程。这种方式虽然为路由建立过程提供了基本的安全保证，但是在路由建立过程中，每一个节点为了验证上一跳节点的身份和向下一跳节点证实自己的身份，都要进行验证签名和加上签名的操作，因此在路由建立上效率很低。

2)ARAN 协议设计的前提：各个节点通过可信第三方 PKI 来进行注册、认证、授权和发布证书，因此，一旦 PKI 被恶意节点攻击，就可能产生单点失效的问题。

3)从保护网络的拓扑不被泄漏的角度考虑，ARAN 协议采用的策略是路由建立过程中不记录整个路径的路由信息和总跳数，每个节点只记录其前趋节点和后继节点的 IP 地址。这种策略就导致任何一对节点需要建立安全的路由时，都要重复保证路由请求建立过程中的消息的不可否认性、完整性

和保密性，因此网络开销过大。

4)攻击者可能通过多次网络中正常的数据通信的内容，获取网络传输过程中源节点或目的节点的隐私信息(IP 地址)，因此保证网络路由建立过程中的完全匿名通信是很有必要的。

4.2 协议设计思想

根据 ARAN 协议的不足之处，对该协议进行改进，即新协议为 TEARAN 协议。现列举假设条件如下：

1)网络中的每条链路是对称的，可以保证双向通信；

2)对网络中的各个节点安装 TPM 模块，由于 TPM 的可信根和可信链的逐级认证和度量，因此能够确保网络中各个节点自身是安全的，即自身的平台不会被篡改，不受病毒、木马程序的影响；

3)为了保证网络中正常通信的进行，各个节点都分配有唯一的 IP 地址，IP 地址能够作为被其他节点鉴别的身份信息；

4)不再考虑使用第三方可信的 CA 来进行颁发证书，而采用 TPM 中的远程证明来对网络中各个节点进行认证，保证各个节点在参与网络的数据包转发过程中是非恶意节点，对恶意节点不予授权访问；

5)采用 TPM 中的随机数产生器 RNG 生成会话密钥，以及采用 RSA 密钥生成器产生公钥/私钥对，保证所产生的密钥都安全存储在 TPM 中的安全存储芯片中，同时 TPM 也提供了数字签名、非对称密钥和对称密钥算法的引擎，从而加快节点之间签名、认证、加解密的处理过程。

TEARAN 协议的运行过程主要分为公钥可信分发、安全路由发现过程、安全路由回复过程、正常的数据传输过程 4 个阶段。协议中所使用的符号意义与 ARAN 协议中的相同，具体如图 3 所示。

K_{A+}	节点 A 的公钥	N_A	源节点 A 发送路由的序列号
K_{A-}	节点 A 的私钥	IP_A	节点 A 的 IP 地址
$\{d\}K_{A+}$	用节点 A 的公钥对数据 d 进行加密	RDP	路由发现数据包的标识
$[d]K_{A-}$	用节点 A 的私钥对数据 d 进行签名	REP	路由发回复数据包的标识
t	路由建立的时间戳		

图 3 本文用到符号及表示意义

4.3 公钥的可信分发

由于各个节点中的 TPM 模块对应生成了公钥/私钥对，随即在安全存储芯片中进行密封，并且私钥只能在内部的 TPM 中使用，外界无法读取篡改私钥，因此保证了节点私钥的安全保密性。但是节点与节点之间的路由建立过程中需要采用公钥进行签名、认证和加密等操作，因此公钥的安全分发就显得尤为必要。

本文结合可信思想[13,14]来考虑各个节点之间的公钥分发问题。根据相邻节点之间观察和直接/间接交往的历史情况，估计各个节点的可信值，预先给整个网路设置一个可信阈值，任何节点的可信值只要大于或等于该可信阈值，就认为该节点是善意节点，从而可以从自身的 TPM 模块中取出各自的公钥以及对应的 IP 地址，通过 Hello 数据包发送给可信的邻居节点，这就保证了公钥发送的过程在善意节点之间进行。同时，当节点加入网络时，我们通过 TPM 中的 DAA(直接匿名证明)[11]方式可以确保该节点的可信平台是可信的，然后对该节点设置一个初始的可信值即为可信阈值，并把自身的公钥和 IP 地址发送给邻居节点；当节点离开网络时，各个邻居节点要对该节点的有效信息给予清除。整个公钥分发的过程都是周期性进行的，各个节点结合最新的交互情况去更新对应的可信值，可信值过低的节点则被剔除网络，不再参与网络正常数据包的转发过程。每个节点在公钥分发过程中，在本地缓存中保存一张邻居节点可信公钥列表，格式如表 1 所列。

表 1 邻居节点可信公钥列表

IP 地址	对应的公钥	进入时间	退出时间	当前状态

IP 地址为公钥分发的节点身份信息，对应的公钥项保存由 IP 地址所发送的公钥信息，进入时间和退出时间项表示该节点在网络中的生存时间，当前状态项表示节点对应的状态，包含可信状态、不可信状态、退出状态、加入状态 4 个状态选项。各个节点根据可信值的情况，把各个节点保存的可信公钥列表的内容结合 Hello 控制消息来周期性地进行交换，从而达到网络中各个节点都可以直接从可信公钥列表中得到其他节点公钥信息和身份信息。

4.4 安全路由发现过程

ARAN 协议由于采用了节点身份认证和数字签名技术，从而导致计算开销过大。因此本文在进行路由建立的过程中，尽量使用 TPM 中的密钥算法引擎，减少节点的计算开销和数据包传输的时延要求。

若节点 A 要与目的节点 X 进行通信，但其路由表中不存在到目的节点的路由，则开始路由发现过程：首先根据本地邻居节点可信公钥列表，选择当前状态为可信状态的可信邻居节点作为下一跳的转发节点，并向其广播路由发现包 RDP，不再向列表中不可信的节点广播 RDP 路由发现包：

$$A \rightarrow brdcast: [\{RDP, IP_X, K_{AX}\}K_{X+}, \{IP_A, N_A, t\}K_{AX}, N_A]K_{A-}$$

假设节点 A 的邻居节点为 B，它收到了 RDP 包后，进行如下处理：

1)由于我们已经通过公钥可信分发过程确保各个善意节点都获得了网络中公钥和身份的有效信息，恶意节点不会加入网络。因此各个节点查找本地邻居节点可信公钥列表，通过遍历表中的公钥，对收到的 RDP 包中的数字签名部分进行鉴别认证，如果验证成功，则判断该 RDP 包是从节点 A 发来的，保证了消息来源的不可否认性；

2)同时判断节点 A 的可信当前状态是否为可信，若是则进入 3)步骤，反之，则丢弃该包，等待其他 RDP 包的到来；

3)判断该 RDP 包是否已经接收过，若重复接收过，则丢弃该包，若是第一次接收到该包，则进入步骤 4)处理；

4)节点 B 继续向其下一跳邻居节点 C 广播路由发现包 RDP：

$$B \rightarrow brdcast: [\{[\{RDP, IP_X, K_{AX}\}K_{X+}, \{IP_A, N_A, t\}K_{AX}, N_A]K_{A-}, IP_B\}K_{X+}]K_{B-}$$

5)节点 C 收到 RDP 包后，则按序执行步骤 1)—步骤 3)；

6)经过了节点 B 签名认证和下一跳节点可信情况的判断以后，节点 C 用目的节点的公钥 K_{X+} 对收到 RDP 包中的有效信息进行加密，并用节点 C 的私钥进行签名，节点 C 向其邻居节点 C 广播 RDP 包：

$C \rightarrow brdcast$:[{{[{$RDP, IP_X, K_{AX}\}K_{X+}$,{$IP_A, N_A, t\}K_{AX}, N_A]K_{A-}, IP_B\}K_{X+}, IP_C\}K_{X+}]K_{C-}$

7)重复以上6个步骤,直至RDP包发送给目的节点X。

4.5 安全路由回复过程

当第一个RDP包到达目的节点X时,目的节点做如下处理:

1)仍然根据本地的可信公钥列表判断上一跳邻居节点的当前状态,若为可信状态,则对上一跳到邻居节点进行签名认证,判断RDP包的来源是否可靠,若来源可靠,则进入2)处理;若为不可信状态,同时RDP包的来源不可靠,则丢弃RDP包,等待其他邻居节点发送的RDP包;

2)利用节点X中安全存储的私钥K_{X-},对RDP包进行层层解包,判断整条路由经过中间节点的可信情况,看其是否存在不可信的节点,包中的有效信息是否被篡改,若判断无误,则在本地缓存中保存所有中间节点信息;

3)当解包到最后一层时,得出发送RDP包的起始源头来自节点A,源节点A和目的节点X的会话密钥为K_{AX},以及路由开始建立的时间戳t,从而节点X安全存储会话密钥,为反向发送路由回复包REP作准备;

4)结合步骤2)、3)保存的中间节点信息,分别根据REP包记录节点的顺序,节点X利用对应节点的公钥对有效信息层层加密,开始进行反向路由回复过程,向RDP包中记录的上一跳邻居节点M发送REP包:

$X \rightarrow M$:{{{{$REP, IP_A, IP_X, N_A, t\}K_{AX}, IP_B\}K_{B+}, \cdots, IP_N\}K_{N+}, IP_M\}K_{M+}$

中间节点M接收到REP包时,作如下处理:

1)节点M用私钥对REP包进行解密,判断得到的IP地址是否属实:若确实属实,则转为步骤2),若不属实,REP包在发送过程中可能出现被修改截获的现象,则丢弃该包;

2)仍然结合本地的可信公钥列表判断周围邻居节点的可信状态,判断节点N是否可信,若可信,则对节点N转发该REP数据包:

$M \rightarrow N$:[[{{{$REP, IP_A, IP_X, N_A, t\}K_{AX}, IP_B\}K_{B+}, \cdots, IP_N\}K_{N+}$

若节点N不可信,则等待下一个REP包的到来;

3)处理过程类同以上步骤,直至源节点A收到REP包。

当节点A收到REP包后,利用会话密钥K_{AX}进行解密,得到包中的IP_X地址并进行验证:如果比较相同,则节点A认为REP包来自目的节点X,并且该路由回复过程中所经历的中间节点都是可信的;如果比较不相同,则节点A丢弃该包,等待下一个REP包的到来。

4.6 数据包的传输过程

经过了前两个阶段路由建立过程的实施,节点A和X之间的一条安全路由已经成功建立。正常的数据包传输过程采用K_{AX}对称密码技术来对所需转发的数据包进行加密,确保传输过程中的保密性和完整性,并且保证了数据包传输的时延要求。

5 协议安全分析与证明

在本节中,我们对TEARAN协议提供有效性的证明和分析。

定理1 TEARAN协议保证源节点和目的节点的匿名性。

证明:1)在安全路由发现过程中,源节点A在向下一跳可信节点广播RDP数据包时,为了保证目的节点X可以鉴别RDP包来源是可靠的可信节点,我们采用节点的公钥X对IP_X以及节点A和X的会话密钥K_{AX}进行加密,同时采用K_{AX}对源节点A的IP_A进行加密实现了匿名性[15,16],从而保证中间的可信节点在透明地转发RDP包时,无法获取源节点和目的节点身份信息。

2)在安全路由回复过程中,目的节点X采用会话密钥K_{AX}来对节点A和X的身份信息IP_A和IP_X进行加密,因而只有源节点A才能对身份信息进行解密,从而保证了节点A和X的匿名转发。

定理2 TEARAN协议能够抵挡网络中的被动和主动攻击,但是不能提供对DoS的攻击的保证。

证明:1)TEARAN协议确保网络不受被动攻击的影响。结合定理1,我们保证了源节点和目的节点在路由建立过程中的匿名性,中间任何节点都不可能获得源、目的节点的身份信息,从而根据源节点的序列号N_A,以及上一跳的身份信息等有效的信息,保证安全路由发现过程中对上一跳节点进行身份的鉴别和不可否认性的验证,因而免除了被动攻击的产生。安全路由回复过程证明也类同。

2)该协议也能保证网络免除主动攻击的影响。主动攻击主要表现在篡改、伪造、路由重放攻击等方面。由于源、目的节点匿名性的保证使得任何中间节点都不可能截获有用的信息来进行主动攻击,同时在路由发现过程中,节点都向可信的邻居节点转发RDP包,以及进行相邻节点的认证和鉴别双重安全检查,保证了路由不受篡改、伪造攻击,另外,源节点的序列号N_A和时间戳t的及时更新和比较保证了路由不可能产生重放攻击。路由回复过程证明也类似。

4)协议不能免除DoS的攻击。TEARAN协议没有提供一个合适的安全机制来抵制该攻击的影响。在路由发现过程中,中间节点持续对下一跳可信的邻居节点洪泛广播RDP包,而对于本身受能量和计算能力限制的中间节点来说,将受到资源浪费严重的DoS攻击。DoS攻击在当前Ad hoc网络的安全路由协议设计中是一个难点问题。

定理3 TEARAN协议能够避开网络中的恶意节点来建立路由。

证明:由于Ad hoc网络本身的开放性,以及节点对之间链路的双向通信等特点,节点可以监听邻居节点的转发数据包的情况。一旦任何中间节点表现出恶意行为,邻居节点都能实时监测判断,并及时地更新恶意节点的可信值以及本地邻居节点的可信公钥列表,从而在安全路由建立过程中,动态地选择可信的节点发送数据包,避开恶意节点参与路由的建立过程,保证网络的安全性。

定理4 TEARAN协议保证所建立的路由是一定无环的。

证明:在路由发现过程中,向除了它的源节点以外的所有满足可信阈值的邻居节点广播RDP包,同时本地缓存的节点序列号可以及时发现重复节点并删除该RDP包,另外,当中间节点接收到RDP包时,都会从RDP包中取出源节点的序

(下转第74页)

[4] Hankerson D, Menezes A, Vanstone S. 椭圆曲线密码学导论[M]. 张焕国,等译. 北京:电子工业出版社,2005

[5] Dimitrov V S, Jullien G A. A new nymber representation with application[J]. IEEE Circuits and Systems Magazine, 2003, 3(2):6-23

[6] Avanzi R, Dimitrov V S, et al. Extending scalar multiplication using double bases[C]// Proceedings of Advances in Cryptology-ASIACRYPT2006. Springer Berlin: Heidelberg Press, 2006

[7] Joye M, Quisquater J J. Hessian elliptic curves and side-channel attack[C] // Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems-CHES 2001. LNCS2162. Berlin: Springer, 2001: 402-410

[8] Edwards H M. A normal form for elliptic curves[J]. Bulletin of the American Mathematical Society, 2007, 44(3): 393-422

[9] Bernstein D J, Lange T. Faster addition and doubling on elliptic curves[C] // Kurosawa K, ed. Advances in cryptology-ASIACRYPT2007. volume 4833 of Lecture Notes in Computer Science. Berlin Heidelberg: Springer-Verlag, 2007: 29-50

[10] Hellman M E. The mathematics of public-key cryptography[J]. Scientific American, 1979, 16(7): 32-39

[11] 丁勇. 椭圆曲线密码体系中标量乘的快速算法研究[D]. 西安:西安电子科技大学,2005

[12] Fong K, Hankerson D, López J, et al. Field inversion and point halving revisited [J]. IEEE Transactions on Computers, 2004, 53(8): 1047-1059

[13] Knuth D E. The Art of Computer Programming: Seminumerical Algorithms(Third edition)[M]. Vol. 2, Addtion- Wesley, 1998

[14] Messerges T S, Dabbish E A, Sloan R H. Power analysis attacks of modular exponentiation in smartcards[A] // Proceedings of the Workshop on Cryptographic Hardware and Embedded System(CHES1999)[C]. Berlin: Springer, 2000: 144-157

[15] 张宝华,殷新春,张海灵. Edwards 曲线安全快速标量乘法运算算法—EDSM[J]. 通信学报,2008,29(10):76-81

(上接第 58 页)

列号 N_A 进行比较判断,从而保证了 TEARAN 协议一定是无环的。

结束语 本文结合目前信息安全中的研究热点即可信计算,以及当前 Ad hoc 网络中典型安全路由协议 ARAN 协议。提出了一种新的安全路由协议 TEARAN 协议。该协议采用了 TPM 中密钥对产生、密钥安全存储以及数字签名、非对称密钥和对称密钥算法的引擎,从而加快了端到端认证、鉴别和加解密的过程,同时,结合邻居节点可信阈值软安全的保证,避开网络中的恶意节点加入到网络中,实现了路由建立过程中双安全的保证,最后对该协议的有效性进行了理论的分析和证明。在未来的工作中,我们将进一步通过仿真实验与其他经典的安全路由协议进行性能对比,来评估该协议的有效性,以及与 QoS 要求进行结合考虑,实现一种满足 QoS 的安全路由协议。

参 考 文 献

[1] Li dong Z, Haas Z J. Securing ad hoc networks [J]. IEEE Network Magazine, 1999, 13(6): 24-30

[2] Zhang C, Zhou M C, Yu M. Ad hoc network security: a review [J]. Int. J. Commun. Syst., 2007, 20(8): 909-925

[3] Hu Y C, Perring A, Johnson D B. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks[S]. IEEE WMCSA, 2002: 23-28

[4] Hu Y C, Johnson D, Perring A. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks[C]// Fourth IEEE Workshop on Mobile Computing Systems and Applications. June 2002: 3-13

[5] Sanzgiri K, Dahill B, Levine B N, et al. Authenticated routing for ad hoc networks[J]. IEEE J. Select. Areas Commun., 2005, 2(1)

[6] Zapata M G. Secure Ad hoc on-demand distance vector(SAODV) routing[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2002, 8(3): 106-107

[7] Papadimitratos P, Haas Z J. Secure routing for mobile ad hoc networks[C] // Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS2002)

[8] Hu Yih-chun, Perrig A. A survey of secure wireless ad hoc routing[J]. IEEE Security& Privacy, 2004, 2(3): 28-39

[9] 张焕国,罗捷,金刚,等. 可信计算研究进展[J]. 武汉大学学报:理学版,2006,5(52):513-518

[10] TCG. Trusted Platform Module(TPM) Summary[EB/OL]. https://www.trusted computing group.org/. 2008,5

[11] TCG 1.2 Architecture Overview. Trusted Computing Group. 2004

[12] Brickell E, Camenisch J, Chen L. Direct anonymous attestation [C]// Proceedings of the 11th ACM Conference on Computer and Communications Security. Washington, DC, USA, 2004: 132-145

[13] Theodorakopoulos G, Baras J S. Trust evaluation in ad-hoc networks[C] // Proc. 2004 ACM Workshop on Wirel. Security, Philadelphia, U.S., 2004: 1-10

[14] Ren K, Li T, Wan Z, et al. Highly reliable trust establishment scheme in ad hoc networks[J]. Comput. Netw., Apr. 2004: 687-699

[15] Reed M G, Syverson P F, Goldschlag D M. Anonymous Connections and Onion Routing[J]. IEEE Journal on Selected Areas in Communications, 1998, 16(4)

[16] Zhang Y, Liu W, Lou W. Anonymous Communications in Mobile Ad Hoc Networks[C]// IEEE INFOCOM. 2005

[17] Zhu B, Wan Z, Kankanhalli M S, et al. Anonymous Secure Routing in Mobile Ad-Hoc Networks[C]// 29th IEEE International Conference on Local Computer Networks (LCN'04). 2004: 102-108

[18] Pfitzmann A, Kohntopp M. Anonymity, Unobservability, and Pseudonymity-A Proposal for Terminology[C] // H. Federrath, ed. DIAU'00, Lecture Notes in Computer Science 2009. 2000: 1-9