软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(9):2815−2829 [doi: 10.13328/j.cnki.jos.005588]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

群组密码的对等 VPN 系统及多播密钥分发协议*

朱 岩[1], 尹 昊[1], 王秋艳[2]

[1](北京科技大学 计算机与通信工程学院,北京 100083)

[2](中国计量科学研究院,北京 100013)

通讯作者: 朱岩, E-mail: zhuyan@ustb.edu.cn

摘 要: 互联网经济的发展,使得企业在大范围内建立连接各种分支机构网络的需求日益强烈,原有采用集中式网关模式的 VPN 逐渐转向采用对等技术的 VPN 系统.现有采用两方密钥交换方法的对等 VPN 技术更适用于两两通信,而在多节点通信中,由于隧道密钥相互独立,不同隧道加密的累计延迟将增加消息同步接收的困难.针对这一问题,提出一种被称为 GroupVPN 的对等 VPN 框架,通过设计具有非中心化、高扩展性的多播密钥分发协议,提高对等 VPN 中的多播通信效率.该框架在安全隧道层的基础上新增了便于动态群组管理、高效密钥分发的群组管理层,结合公钥群组密码下的广播加密方案,实现具有选择和排除模式的高效密钥分发,保证协议在 SDH 假设下满足数据私密性、数据完整性、身份真实性这 3 方面安全性要求.实验分析结果表明:该协议的通信耗时和密钥存储开销与群组规模无关,可将通信延迟限制在会话密钥共享阶段,提高系统性能.

关键词: 虚拟专用网;安全多播;密钥分发;群组密码;广播加密

中图法分类号: TP311

中文引用格式: 朱岩,尹昊,王秋艳.群组密码的对等 VPN 系统及多播密钥分发协议.软件学报,2019,30(9):2815−2829. http://www.jos.org.cn/1000-9825/5588.htm

英文引用格式: Zhu Y, Yin H, Wang QY. Group VPN system and multicast key distribution protocol based on group-oriented cryptography. Ruan Jian Xue Bao/Journal of Software, 2019,30(9):2815−2829 (in Chinese). http://www.jos.org.cn/1000-9825/5588.htm

Group VPN System and Multicast Key Distribution Protocol Based on Group-oriented Cryptography

ZHU Yan[1], YIN Hao[1], WANG Qiu-Yan[2]

[1](School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China)

[2](National Institute of Metrology China, Beijing 100013, China)

Abstract: The rapid growth of the Internet economy has already led to increasing demand for enterprises in establishing network connections with multiple branches in large scale, even global scale. The original VPNs constructed on centralized gateway mode are gradually turning to the VPN system using peer-to-peer technology. The existing peer-to-peer VPN technology built on the two-party key exchange method is more suitable for pairwise communication. However, considering that the tunnel keys are mutually independent in a multi-node communication, the cumulative computation delays of encryption under different tunnels will raise the difficulty in synchronous message-passing. Aiming at this problem, in this study, a peer-to-peer VPN framework called GroupVPN is proposed, which improves the efficiency of multicast communication by designing a non-centralized and highly scalable multicast key distribution protocol.

* 基金项目: 国家重点研发计划(2018YFB1402702); 国家自然科学基金(61972032); NSFC-通用技术基础研究联合基金(U1636104); NFSC 海外及港澳学者合作研究基金(61628201)

Foundation item: National Key Technologies R&D Programs of China (2018YFB1402702); National Natural Science Foundation of China (61972032); NSFC-Genertec Joint Fund For Basic Research(U1636104); NFSC-Joint Research Fund for Overseas Chinese Scholars and Scholars in Hong Kong and Macao(61628201)

收稿时间: 2018-01-05; 修改时间: 2018-03-26; 采用时间: 2018-04-17

The proposed framework adds a group management layer over the security tunnel layer in order to facilitate dynamic group management and efficient key distribution. This new protocol is applicable for realizing the efficient key distribution for arbitrary group in two mechanisms: designation and revocation by combining broadcast encryption (BE) under public-key group-oriented cryptography infrastructure. In addition, security analysis indicates that this protocol could meet the security requirements of data privacy, data integrity, and identities' authenticity under the strong Deffie-Hellman (SDH) assumption. Experimental analysis also shows that the communication and key-storage overheads of this protocol are actually independent of group size, and the communication delay is more limited by the phase of session key distribution for improving the performance.

Key words: virtual private network; secure multicast; key distribution; group-oriented cryptography; broadcast encryption

虚拟专用网(virtual private network,简称 VPN)是指在不可信公网上建立的一个临时的、安全的专有数据通信网络,为企业和个人提供高质量的网络服务,实现对企业内部网络的扩展.它可以使用不安全网络(如互联网)来发送可靠、安全的消息,核心是利用加密的隧道协议保证敏感信息的私密性、发送端认证、消息完整性等安全性质.

伴随全球经济的快速发展,越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司、研究所等,各分支机构的网络连接随着机构的增多使得网络结构趋于复杂,部署维护费用昂贵.利用 VPN 提供的隧道[1]、加密等特性可以构建满足要求的内联网(Intranet),保证信息在整个内联网上安全传输.然而,现有大部分 VPN 方案在分支机构增多时传输效率显著下降,难以满足大规模企业组网的现实需求.其原因在于:现有 VPN 方案多使用集中式网关模式,由 VPN 网关代理与客户端实现隧道通信,这种集中式结构难以支撑复杂的网络拓扑变化.

针对上述内联网 VPN 方案的缺陷,已有 VPN 采用了对等技术(P2P),充分利用网络中参与者的计算能力和带宽而不依赖于集中式网关,从而带来在可扩展性、健壮性等方面的优势.例如,该网络能够以自组织方式建立,并允许分支机构自由地加入和退出当前内联网,部分节点或网络遭到破坏对其他部分的影响很小,具有耐攻击、容错性的优点.鉴于上述优点,基于 P2P 的 VPN 已成为目前研究热点之一,并被应用于协同计算、群组聊天、在线会议等领域.

采用对等技术的 VPN 也称为对等 VPN 系统,尽管这种系统融合了 P2P 的非中心化、可扩展性等特性,但由于其依然延续了 VPN 中的常规两方密钥交换方法(如 Deffie-Hellman 密钥交换协议)建立加密隧道和实现密钥管理,因此,系统在实现动态多播(即一点对多点间通信)时的性能和安全性并没有较大的提升.解决这一问题的难点在于如何建立具有非中心化、高扩展性、且与对等 VPN 相适应的安全多播协议,保证在一个主机用该多播协议向多个主机发送相同数据时,只需加密和发送一次,其数据由网络中的路由器和交换机逐级进行复制并发送给各个授权接收方,这样既节省服务器资源,也节省网络主干的带宽资源.

本文致力于解决对等 VPN 系统中安全多播问题,通过实现具有非中心化、高扩展性的多播协议,提高对等 VPN 中多播通信效率和安全性.本文所提出的方案是在现有的 Overlay 虚拟专用网基础上,针对其两方密钥交换方式在群组通信中的不足,利用基于身份的群组加密与签名方案改造对等 VPN 中的密钥共享方法.所做创新工作如下.

(1) 提出一种支持安全多播的对等 VPN 框架,被称为 GroupVPN,该框架引入公钥群组密码系统改进了安全隧道层,并设计了便于动态群组管理、高效密钥分发的群组管理层,能够支持安全点播、多播、广播等多种通信模式;

(2) 设计一种多播密钥分发协议,通过将公钥群组密码下的广播加密与群签名方案相结合,实现具有选择和排除模式的高效密钥分发.分析表明:在 SDH 假设下,该协议满足数据私密性、数据完整性、身份真实性等 3 方面安全性要求.

与基于对称密码的密钥分发和基于公钥密码的密钥交换协议相比较,本文所提多播密钥分发协议实现的多播通信和密钥存储开销与群组规模无关.实验分析表明:多播组通信分为会话密钥共享和加密通信两个阶段,会话密钥共享阶段交互耗时与群组规模成正比,但加密通信阶段多播耗时基本保持不变,从而使得由群组规模

增长产生的通信延迟仅被限制在会话密钥共享阶段,提高了系统性能.

本文第 1 节介绍 VPN 和群组加密的相关工作.第 2 节和第 3 节详细描述系统模型及多播密钥分发的具体步骤.第 4 节和第 5 节描述密钥管理方案及其实验分析.最后,第 6 节总结全文.

1 相关工作

1.1 虚拟专用网发展现状

虚拟专用网是一种构架在已有网络技术之上的具有灵活性、安全性、高效性的通信网络.与普通网络不同之处在于它所涉及的两个核心技术点——虚拟和专用,其意义分别为:

(1) 虚拟是指该网络能够通过路由技术、协议转换等方式动态地接入网络并保证数据可靠传输;

(2) 专用是指该网络能够通过加密技术、隧道协议等方式有效地保护用户数据的隐私不泄露.

因VPN所拥有的这些优点和现实生活中业务的需要,近年来,有关VPN技术的研究以及工程应用都在不断更新.从网络组织形式上,VPN 大体被分为两类:点对点 VPN(SSL,GRE,IPSec)、远程接入 VPN(PPTP,L2TP,MPLS);Knight 和 Lewis 则在文献[1]中按 OSI 网络模型将 VPN 分为 2 层和 3 层 VPN,并分析了两者的架构和解决方案;Berger[2]分析了当前流行的几种 VPN 技术,通过交互测试比较协议的优劣;Jaha 等人[3]则试图在已有的公共 VPN 协议上,使用多种模型构建一个新的 VPN 协议;Hafiz 等人[4]比较了不同加密算法(如 AES256,3DES,SAH-1,MD5)应用于 IPSec VPN 中的性能差异;Jahan 等人[5]则是站在应用的角度对不同 VPN 的特点以及应用场景做了分析和推荐.然而,目前的方案仍仅限于用传统密码实现点对点安全隧道,尚无方案采用群组密码体制开展安全多播领域的研究.

随着软硬件技术的发展,计算和网络带宽已不再是VPN实现的瓶颈,近年来新开发的VPN技术都构架在应用层,以便能够更加灵活地满足不同业务的需求.例如:基于集中式架构的 OpenVPN,通过设立特殊的网关来支持异构设备,已广泛应用于教育、公司等机构;基于分布式架构与 P2P 技术的 N2N[6],采用两层结构,使用节点间的消息路由取代网关;采用相同结构的 PeerVPN,则直接构建平铺的网络,自动发现并连接其他的节点.鉴于 P2P 网络在网络动态自组织方面的优势,本研究也将参考上述分布式构架实现系统设计.

1.2 群组密码技术

群组加密技术是一种面向大规模群组的安全通信方式[2].与传统的具有 1:1 公/私钥对的加密系统不同,群组加密系统的密钥结构是 1:n,也就是 1 个公钥对应于 n 个不同的私钥,已知的广播加密(broadcast encryption)、身份基加密(identity-based encryption)、属性基加密(attribute-based encryption)、角色基加密(role-based encryption)等都属于群组加密的范畴.其中,广播加密是最基本的群组加密.目前,面向群组的通信研究分为两个方面:一方面是指定机制,即指定一个接受者集合,使得只有在指定集合内的用户才能解密;另一方面是撤销机制,即指定一个撤销者集合,使得只有在指定集合外的合法用户才能解密.

关于指定机制的研究,最重要的工作是 2005 年 Boneh 等人[7]提出的方案,该方案利用双线性映射以及连乘实现集合成员属于关系的判定,能够抵抗任意数目共谋者的攻击,且密文和私钥都是常数大小;随后,Delerablée 等人[8]提出了基于身份的广播加密方案,该方案不仅保证了密文和私钥是常数大小,并且公钥大小与接受者集合的最大数目呈线性关系;近年来,该方向的研究还包括文献[9−11].此外,撤销机制也得到了学者们的广泛研究[12−14].

可证明安全(provable security)是当前群组密码系统的基本要求[15].群组密码方案的可证明安全性通常是指密文的语义安全性(semantic security),即已知密文不会泄露任何明文信息,也等价于密文不可区分性(indistinguishability)[16].但与传统的加密方案不同,群组下的语义安全性需要考虑攻击者与群组内叛逆者(具有一定数量的解密密钥,但对挑战密文无效)共谋下的语义安全,用于模拟敌手具有一定先验密钥知识情况下的攻击.由于可证明安全性的引入,使得群组密码体制用于 VPN 更加高效、灵活与安全[17].

2 系统模型

2.1 系统目标

针对 VPN 在安全、高效、动态性等方面的现实需要,本文以构建一种采用公钥群组密码(public-key group-oriented cryptography,简称 PGC)技术的密钥管理框架为目标,并将该框架应用于由对等节点组成的基于覆盖网络的安全群组通信系统,提供密钥分发、更新、销毁等服务.该框架可支持消息的安全点播、多播和广播,被称为群组虚拟专用网络(简称群组 VPN,或 GroupVPN).

GroupVPN 中群组加密采用 1:n 结构的公钥密码体制,即 1 个群组公钥与 n 个用户私钥进行关联,且用户私钥与其身份 ID(标识身份的唯一字符串)进行绑定.在该密码体制下,系统能够对群组内的任意一组用户通过群组公钥对消息进行加密,而只有组内的成员能够解密信息.利用该特点,本文设计一种密钥管理框架,为群组中的多个用户创建共享密钥,从而实现用户组内的消息安全共享.因此,本文所设计的系统需拥有如下特性.

(1) 动态性:支持成员动态加入和退出,并在成员之间构成通信间群组(多播组);

(2) 高效性:保证身份认证、密钥交换、数据加密与解密的高效性;

(3) 高安全性:保证虚拟网络提供的安全功能是密码学可证明安全的.

2.2 系统模型

针对研究目标,GroupVPN 被建立在由 N 名成员{P_1,…,P_N}构成的 P2P 网络上,利用虚拟化技术建立功能虚拟化的覆盖网络,实现支持动态用户群下的安全群组通信.图 1 显示了 GroupVPN 的系统模型图,该系统由两层网络构成.

(1) 内层(下层)是运行在互联网中的物理网络,节点(交换机、路由器)之间直接互连组成核心的通信网络;

(2) 外层(或上层)是各子网路由器(VPN 接入节点)组成的覆盖网络,该网络中节点可以看做通过虚拟或逻辑链路连接起来的一个虚拟全连通网络.

GroupVPN 所形成的虚拟网络采用了全连通的完全网格拓扑(full mesh topology),使得用户之间可以通过虚拟 IP 地址相互访问,与下层的实际网络拓扑无关,对用户也是透明的.因此,在这种虚拟网络进行节点间的直接通信是十分便捷的.

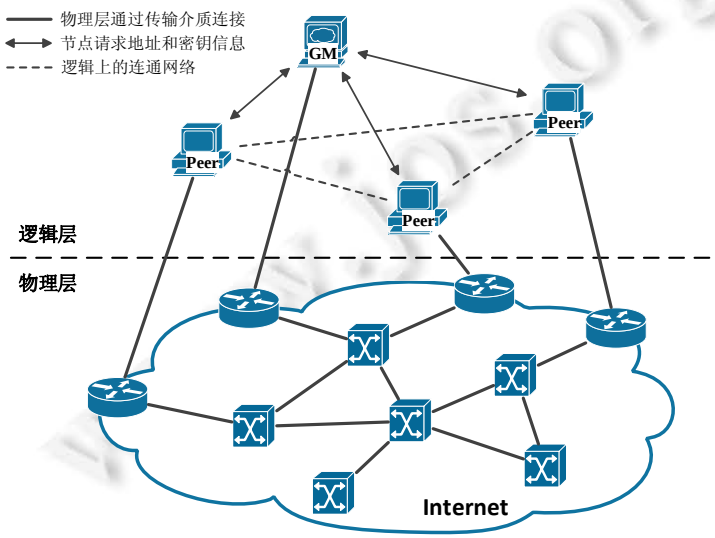

Fig.1 Group VPN system model diagram

图 1 群组 VPN 系统模型图

鉴于防火墙或 NAT 等技术对 VPN 的现实约束,上述系统模型参考了 N2N 系统中节点的功能划分,将上层节点分成两种角色——超级节点和边界节点.超级节点处于公有网段,运行守护进程并监听绑定端口,等待边界节点连接,并为其注册必要的网络地址和端口信息;对处于私有网段的边界节点,则利用 NAT 打洞、防火墙绕过等技术,解决其他边界节点与它的链路连通问题.据此,所提系统模型将实体和其功能划分如下.

(1) 对等节点(peer):是指参与群组间通信的实体,被看做 GroupVPN 群组中的成员,类似于边界节点,获取必要的密钥参数加入群组网络,维持与其他节点间的安全通信隧道;

(2) 群组管理者(GM):建立和维护群组网络的密码系统和参数,为新节点分配用户密钥并引导节点连接组成群组网络,但不参与群组通信.

GroupVPN 中的每个对等节点都相当于分支机构的 VPN 网关,通过对用户数据的封装加密以及虚拟目标地址的转换实现远程访问.有别于远程接入 VPN 的网关代理(需要对所有报文进行转发),GM 不处理任何 VPN 数据报文,其仅限于群组的密钥管理以及网络连接两项功能:前者可为各节点产生和分发有效的群组密钥,后者解决节点间地址发现和连接障碍问题.

2.3 协议架构

GroupVPN 系统被构架在参考模型协议栈中的传输层之上,属于一种传输层协议.该架构为应用层提供一种透明的群组访问接口,应用程序遵循该访问接口可实现安全群组内通信.GroupVPN 系统架构图(如图 2 所示)在协议栈基础上增加了两个新的结构,包括:

(1) 群组管理层:用于构建和维护 GroupVPN 所使用的公钥群组密码 PGC 系统,负责管理和响应对安全参数索引(security parameter index)的查询;

(2) 安全隧道层:用于构造 GroupVPN 的主体,它包括 3 个主要功能模块:载荷封装协议模块、虚拟地址映射模块、共享密钥分发模块,在与多个用户成功共享加密密钥后,对应用层发来的数据报文进行载荷封装,地址映射,并通过隧道广播加密报文实现安全群组多播.

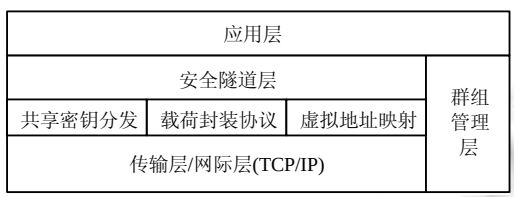

Fig.2 Group VPN system architecture diagram

图 2 群组 VPN 系统架构图

在群组管理层中,某个对等节点作为群组创建者向 GM 申请注册一个群组,GM 初始化有关该群组网络所需要的系统参数,节点获得对应自己身份的私钥信息,并等待其他节点以同样的方式向 GM 通过身份验证后与自己相连.群组管理者并不参与群组间的消息通信,只作为管理中心维护和监管相关安全参数,在群组建立和撤销时,相应地创建和回收密钥信息.

安全隧道层是 GroupVPN 系统的重要功能,用于在群组 $U=\{P_1,P_2,\ldots,P_n\}$ 中建立临时的多播组 S 进行组内安全数据传输.该部分所包含的 3 个模块分别具有以下功能.

(1) 共享密钥分发模块:采用公钥群组加密实现对多播组内成员的认证以及临时会话密钥的分发,该会话密钥在载荷封装协议模块中用于报文加密;

(2) 载荷封装协议模块:采用隧道技术对数据报文进行封装加密,提供机密性和抗重播服务,可参考 IPSec 中的封装安全载荷(ESP)协议对原始报文进行加密和隧道封装;

(3) 虚拟地址映射模块:实现对多播组内成员地址与真实 IP 地址之间的转换.

共享密钥分发模块提供与 IPSec 中密钥管理协议(ISAKMP)类似的密钥协商功能和安全参数定义,但是具

有以下不同:(1) 使用公钥证书(certificate)取代安全关联(SA),通过对 GM 的查询,实现群组信息的获取;(2) 采用 PGC 实现动态多播组的建立和会话密钥分发,避免 IPSec 所采用的手动预置参数的密钥管理;(3) 在某个多播组中建立所有成员共享的会话密钥,而不是单独两个对等体之间的协商.

这些不同得益于系统构架在网际层隧道技术而非链路层的 IP 隧道(L2TP),使它可支持 TCP/IP 协议栈下异构网络间的边界互联.同时,PGC 的使用简化了多播组的密钥管理过程,在宏观层面上降低了系统的空间和时间复杂性.总之,GroupVPN 的系统架构具有以下几点优势.

(1) 支持多种通信模式.目前的对等 VPN 技术通常是在两个对等节点间建立共享密钥用于加密通信,而本文提出的 GroupVPN 能够在多个节点的用户组中建立共享通信隧道,并且对用户成员集合的大小不予限制,实现单点发送多点接收的安全多播;

(2) 密钥管理简单.减少通信量,无需预先定义端对端安全关联和相关协议,采用基于身份的公钥群组密码系统实现多播组成员身份认证和密钥分发.相较于 TLS/SSL 的 PKI 公钥证书认证和预定义共享密钥的 IPSec 更加简单有效,适用于多播下的群组通信;

(3) 便于动态化的群组管理和网络接入服务.群组管理者 GM 能够提供公开可信的用户身份和地址信息引导节点连接,并且通过虚拟地址映射模块解决私有地址之间的连接障碍.

2.4 安全模型

GroupVPN 的安全目标旨在通过公开不可信网络环境实现端对端的安全互联与融合,保证动态群组成员之间的互认证、通信中数据报文的机密性及密钥在群组成员之间的一致性.为实现上述目标,群组管理者提供类似于密钥中心的服务,为节点的安全通信提供密码学基础环境.从层次关系上看,对等节点之间自组织形成网络,而不过度依赖上层管理中心,从而发挥对等网络的优势.因此,所提架构仅对 GM 做出如下假设.

假设(半忠诚假设). 群组管理者是可信的,并忠诚地为节点提供注册和唯一性群组私钥分发服务;同时,管理者不被接受成为群组中的成员,即,不与下层通信节点建立端对端的虚拟通信隧道.

系统模型所采用的是一种基于身份的群组密码系统,它要求用户的身份和密钥是一一对应的,而身份标识对应的群组私钥又是由管理者验证其身份而颁发的,因此在无法通过伪造身份骗取管理者的前提下,敌手因其没有密钥而无法冒充用户身份.在此基础上,鉴于 VPN 安全性主要体现在密钥交换和隧道安全两方面,GroupVPN 模型针对这两方面需满足如下安全性要求.

(1) 数据私密性:保护用于加密通信数据的会话密钥不被非授权用户获取.由于群组加密中该会话密钥由发起者单方面随机生成,若它不被发起者泄露,那么会话密钥的私密性则确保了加密数据的私密性;

(2) 数据完整性:保护群组中的多播通信数据无法被篡改,并能够迅速被接收者检测到异常.通常是在传输报文中添加密码学校验,如哈希函数或是校验码等,用来保护数据的完整性;

(3) 身份真实性:保证发送方与接收方身份的真实性.在基于身份的 PGC 系统中,接收方身份直接映射到密码系统中的用户标识 ID,由发送者加入到可解密用户集合生成密文,PGC 保证只有该集合内的接收者可解密;发送者的身份真实性则可由接收者验证发送者附带的消息签名来确定.

3 多播密钥分发

3.1 设计目标

本文利用群组加密的广播特性来设计并实现多播组生成和组内密钥分发,具体定义如下.

定义 1(多播密钥分发). 多播密钥分发是指在群组内多个用户之间共享同一个会话密钥以形成多播组的过程,该会话密钥能够安全地被多播组内成员共享,保证除此之外的其他用户无法得知.

多播密钥分发是 GroupVPN 中节点之间进行通信的基础,为群组内的多播组产生一个共享的安全会话密钥,数据传输则使用传统的 VPN 隧道技术处理完成.因此,该管理框架可构架于现有的 VPN 系统之上,耦合性低,易用性好.

该过程采用群组密码技术取代已有 VPN 系统中具有认证功能的密钥交换协议(如基于口令授权的密钥交换协议 PAKE 或其三方版本 3PAKE),后者是使通信双方在认证服务器的帮助下相互进行认证并建立一个会话密钥的过程.我们所提方案的不同之处在于,将两方或三方认证和密钥交换扩展为多播组下的多方认证和密钥分发.

为方便阅读,本节所使用符号见表 1.

Table 1 Description of notations

表 1 符号说明

符号	描述
$\mathbb{S}$	双线性映射系统,例 $e(g,h)$
msk	群组管理者的系统主私钥
mpk	群组管理者的主公钥,作为公开参数
ID_k	第 k 个用户的身份标识,任意字符串
sk_k	第 k 个用户的群组私钥
pp_k	第 k 个用户存储在群组中的公开标识
U	群组集合,包含所有的成员
S	群组成员的子集,用于构建多播组
G_S	集合 S 的零点聚合值
H_S	集合 S 的极点聚合值
ek	随机选取的临时会话密钥
$mode$	加解密模式,选择或排除
C	隐藏会话密钥 ek 的密文

3.2 系统初始化

本文采用文献[18]中的标识集广播加密方案(ISBE)作为多播密钥分发协议构建的基础,该方案由 4 个算法构成:*Setup*,*KeyGen*,*Encrypt*,*Decrypt*.但与通常加密方案不同的是,它可支持两种加密模式:选择模式和排除模式,即,给定集合 $S\subseteq U=\{P_1,P_2,\ldots,P_n\}$,两种模式功能如下.

- 选择模式:只有集合 S 内的指定成员能解密信息;
- 排除模式:除集合 S 外的合法成员均能解密信息.

方案的核心算法是两类聚合函数:零点聚合函数 *ZerosAggr* 和极点聚合函数 *PolesAggr*,用于实现标识集 S 的密码学表示.以 ISBE 为基础,GroupVPN 系统初始化分为两个部分:管理者 GM 初始化和新成员初始化.两个初始化的具体操作如下.

(1) 管理者初始化

本阶段用于生成系统所需要的主私钥 msk 和主公钥 mpk,它可通过采用 ISBE 方案中的 $Setup(\mathbb{S})\rightarrow(msk,mpk)$ 函数加以实现:给定素数阶双线性群系统 $\mathbb{S}=\{p,G_1,G_2,G_T,e\}$,在 G_1 和 G_2 群上分别选择两个随机元素 g 和 h 作为生成元,在整数域 $\mathbb{Z}_p^*$ 中选取两个随机指数 γ,ε,得到主密钥 $msk=(\gamma,\varepsilon,g,g^{\varepsilon})$;令 $R=e(g,h)^{\varepsilon}$并设定最大聚合数目 m,对 $\forall k\in[1,m]$依次计算 $g_k=g^{\gamma^k}\in G_1$,得到主公钥 $mpk=\{\mathbb{S},h,R,\{g_k\}_{k\in[1,m]},pp=\varnothing\}$,其中,$pp$ 作为用户记录表可由用户在任意时刻查询获取.

(2) 用户初始化

在 GM 完成初始化后,用户可向 GM 注册申请加入系统,在提供身份信息 $Info_k$(由系统自行设定)并通过管理者的验证后,GM 使用身份标识 ID_k 调用 $KeyGen(msk,ID_k)\rightarrow sk_k$ 函数获取相应的用户私钥 sk_k 成为群组成员.具体过程如下:令 $x_k=hash(ID_k)$,生成用户私钥 $sk_k=g^{x_k\varepsilon/(\gamma+x_k)}\in G_1$,并计算 $H_k=h^{\varepsilon/(\gamma+x_k)}$,得到该用户的公开记录 $pp_k=(ID_k,H_k,Info_k)$,并且将 pp_k 添加到公开参数 mpk 的集合中,即 $pp=pp\cup\{pp_k\}$,以公示新成员加入到了当前群组.

以上两个初始化过程分别对应系统框架中的管理和通信模块:管理者初始化仅针对 GM,在整个系统中只运行一次,关系到群组内所有用户的密钥有效性,因此参数更新也将影响用户的密钥;用户初始化过程也就是用户注册和申请群组私钥的过程,它为多播组建立和密钥分发做准备.本系统没有用户数目的限制,新用户可以随

时、动态地进行注册和添加到系统;同时,系统内节点通过向 GM 发起基于成员标识 ID_k 的用户信息 pp_k 查询与其他节点连接成网络.

3.3 多播密钥分发协议

公钥群组加密方案是实现安全多播密钥分发的合理选择,其 1:n 的密钥结构和聚合特性能够做到只需一次加密,被选择用户集合 $S\subseteq U$ 内的所有用户都可以解密获取会话密钥.因此,本文将 ISBE 加解密过程应用于密钥分发,由多播发起者构建一个可解密用户集合 S 作为通信对象,选取一个随机的临时会话密钥 ek 作为明文,经加密输出密文并发送,多播组内的用户解密恢复出临时会话密钥,则完成了多播组的密钥分发过程.多播密钥分发协议具体步骤分为如下 4 步.

1. 多播组构建

假设群组 U 内的用户子集 $T=\{P_1,P_2,\ldots,P_m\}$需要发起多播组通信,其中,P_i 拥有标识 ID_i.群组内的任何用户 $P_k\in T$ 能够发起多播组构建过程:该用户(称为发起者)将该子集 T 发送给 GM 并请求多播组构建;GM 做出响应进行模式判定:

(1) 如果子群用户数目 $m=|T|$小于总人数 $n=|U|$的一半,即 $m<n/2$,那么设定模式为选择模式,即 $mode=Select$ 且令 $S=T$;

(2) 如果子群用户数目 $m=|T|$大于等于总人数 $n=|U|$的一半,即 $m\geqslant n/2$,那么设定模式为排除模式,即 $mode=Cut$ 且令 $S=U\backslash T$.

注意,上述模式也可由发起者指定.根据不同的加密模式,令选择模式对应的集合为 T,排除模式对应的集合为 $U\backslash T$,再根据其模式分别计算零点聚合值 G_S 和极点聚合值 H_S 作为用户集合的表示:

$$\begin{cases} H_S = PolesAggr(mpk,S) = h^{\varepsilon\cdot\prod_{e_i\in S}\frac{1}{\gamma+x_i}}, & \text{for } Select\ mode \\ G_S = ZerosAggr(mpk,S) = g^{\gamma\cdot\prod_{e_i\in S}(\gamma+x_i)}, & \text{for } Cut\ mode \end{cases}.$$

最后,GM 将$\{mode,G_S,H_S\}$发送给发起者用于多播组会话密钥分发.上述函数也可由发起者采用公开参数 mpk 自行计算,但是考虑到系统运行效率和易用性,本文选择由 GM 加以实现.具体聚合算法见文献[21]中的函数 $Aggrs(S,mode)\rightarrow\{G_S,H_S\}$.

2. 会话密钥分发

本阶段由多播组通信的发起者完成会话密钥选择和对应密文的生成,具体如下:随机选取元素 $t\in\mathbb{Z}_p^*$ 并计算 $ek=R^t$ 作为临时的会话密钥,根据上一步得到的集合的聚合表示和相应的加密模式$\{mode,G_S,H_S\}$,发起者计算得到密文 $C=(S,mode,C_1,C_2)$,其中,

$$(C_1,C_2)=\begin{cases}(h^t,(H_S)^t), & \text{for } Select\ mode\\ (h^t,(G_S)^t), & \text{for } Cut\ mode\end{cases}.$$

3. 会话密钥恢复

多播组 T 内授权用户 P_k 接收到多播密文 C 后,根据密文中的用户集合 S 得知多播组的成员构成,并判断其加密模式恢复出隐藏的会话密钥:

(1) 选择模式:若满足当前用户 $ID_k\in S$,令 $S_-=S\backslash\{ID_k\}$,用户将其与模式一同发送给 GM,请求用该集合计算零点聚合函数 $G_{S_-}=ZerosAggr(mpk,S_-)$,并在获得返回值后使用私钥 sk_k 恢复出会话密钥:

$$ek=e(sk_k,C_1)\cdot e(G_{S_-},C_2);$$

(2) 排除模式:若满足当前用户 $ID_k\notin S$,令 $S_+=S\cup\{ID_k\}$,用户将其与模式一同发送给 GM,请求用该集合计算极点聚合函数 $H_{S_+}=PolesAggr(mpk,S_+)$,并使用私钥 sk_k 恢复出会话密钥:

$$ek=e(sk_k,C_1)\cdot e(C_2,H_{S_+}).$$

完成以上两个初始化阶段之后,就可在群组内组建一个共享同一会话密钥 ek 的多播组.会话密钥分发阶段时序图如图 3 所示.

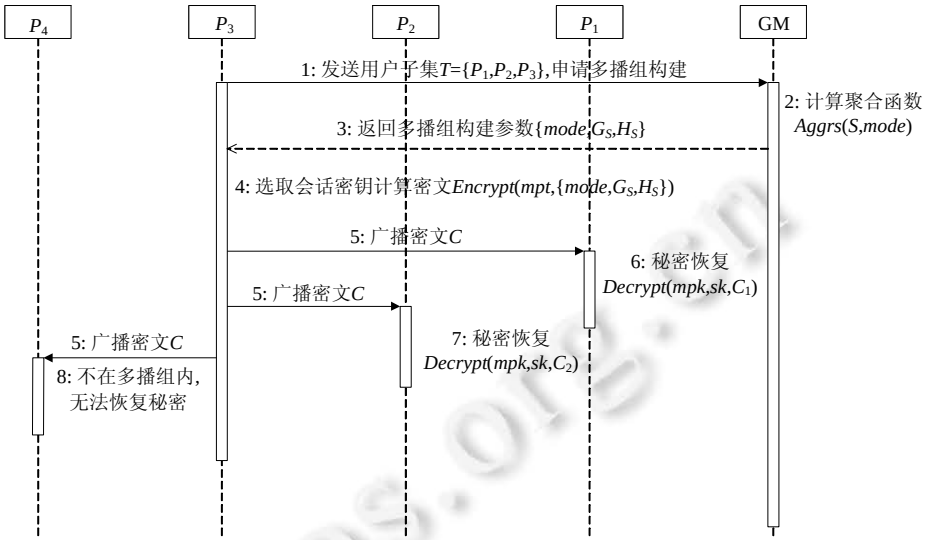

Fig.3 Multicast key distribution sequence diagram

图 3 多播密钥分发时序图

在上述协议运行过程中,多播组构建是算法中比较耗时的操作,且聚合函数的特点决定了计算时长随着多播组规模的增长而增加.但在具体应用中,可以优化这一过程:1) 拥有选择和排除两种模式,在多播组规模超过群组大小的一半时可用其补集的排除模式减少聚合计算的时长;2) 多播组构建操作可作为独立的模块预加载或者缓存,其计算结果可被多次使用,从而不会影响网络延迟.

4. 发送者身份认证

多播发起者 P_k(其标识为 ID_k)能够采用数字签名方式来验证发起者的身份.适用于本系统的数字签名方案包括基于身份的签名(IBS)或群签名(GS)等,下面以文献[19]中的短群签名 SGS 方案为例加以说明:该 SGS 方案由 4 个算法构成:*KeyGen*,*Sign*,…,*Open*,但与通常的签名方案不同之处在于,群签名中隐藏了签名者的身份,需要 *Open* 函数才能找出真实签名者.此外,由于 SGS 方案采用了与 ISBE 方案相同的用户私钥结构,因此用户可使用已分发的用户私钥 $sk_k = g^{x_k\varepsilon/(\gamma+x_k)}$ 变换为 $sk_k^{1/x_k} = (g^{\varepsilon})^{1/(\gamma+x_k)}$ 用于 SGS 方案,其中,g^{ε}可看做新的生成元.

基于上述签名方案的构造,可在第 2)步中的会话密钥分发结束后,由发起者生成群管理私钥 *gmsk*,使用用户私钥 sk_k 完成对发起者标识 ID_k 和密文 C 的签名δ=*Sign*(*gpk*,sk_k,(ID_k,*gmsk*,*C*,*M*));再用通常的加密算法对签名进行加密:C'=*Enc*(*ek*,(ID_k,*gmsk*,δ,*M*)),最终将(*C*,C')进行多播传送给组内成员.

与此对应,在第 3)步中的会话密钥恢复完成后,授权接收者首先用恢复后的会话密钥 *ek* 解密获得发起者标识 ID_k 和密文 *C*,即(ID_k,*gmsk*,δ,*M*)=*Dec*(*ek*,C');然后,验证签名 *Verify*(*gpk*,(ID_k,*gmsk*,*C*,*M*),δ)=True 且找出签名者 *Open*(*gpk*,*gmsk*,(ID_k,*gmsk*,*C*,*M*),δ)=ID_k.如果上述判定成立,则表明发起者与宣称的一致.

3.4 安全性分析

如安全模型所述,GroupVPN 系统构造采用了加密与签名相结合的方式,可满足数据私密性、数据完整性、身份真实性这 3 方面的要求.在上述结构中,分别采用了 ISBE 群加密和 SGS 群签名方案,两方案都以双线性映射群为数学基础,不仅具有相同的用户私钥结构,而且都以强 Diffie-Hellman(SDH)问题为安全基础:

定义 2(SDH 问题). 给定$\mathbb{G}$中元素 (G,G^{α},...,G^{α^t}),找到一对值(c,$G^{1/(\alpha+c)}$),其中,$c\neq 0 (\mathrm{mod}\ p)$.

下面分别对这 3 个方面进行分析.

1. 在数据私密性方面

系统通过数据加密实现数据私密性,这里的加密算法 *Enc* 是现有的标准常规加密算法(如 AES、国标 SM1

等).在加密密钥(即会话密钥)不可猜测情况下,其安全性能够满足数据语义安全的要求,因此,数据私密性取决于 ISBE 加密方案保护用于加密通信数据的会话密钥不被非授权用户集合获取.下面的定理证明了 ISBE 方案中会话密钥的语义安全性(不可区分性).

定理 1(ISBE 语义安全). 对于 $0\leqslant t\leqslant n$,假设任何(n,t)-GDHE$_1$和(n,t)-GDHE$_2$问题是困难的,那么基于标识集的加密方案在选择(select-mode)和排除(cut-mode)模式下对选择明文共谋攻击下具有语义安全.

上述语义安全性等价于会话密钥与随机字符串两者所生成密文的不可区分性,它意味着非授权集合中的用户即便共谋(collusion)也无法获取会话密钥,从而解密多播信息获得其内容.这里的共谋是指非授权集合中用户即便具有合法的密钥,也无法对授权集合下的密文进行解密.上述定理的证明通过设计一个敌手与挑战者之间的交互博弈过程,从而模拟敌手针对该方案在选择明文以及共谋条件下的优势.

- 首先,由挑战者初始化密钥参数,指定加密模式 *mode* 和挑战的授权用户集合 S^*,敌手获得主公钥 *mpk*;
- 然后,为模拟共谋条件,敌手可重复 n 次查询用户 ID_i 的私钥,当且仅当被查询用户不在授权集合内,即满足 $mode(ID_i,S^*)\neq 0$,则挑战者返回该查询用户的私钥;否则返回该用户的公开参数,其中,t 为共谋密钥的数量且$|S^*|=n-t$;
- 接着,挑战者完成加密操作 $Encrypt(mpk,S^*,mode)=(C,ek)$得到密文 C 和秘密 ek,随机掷币 $b=\{0,1\}$,令 $ek_b=ek$ 且 ek_{1-b} 为另一随机元素,将消息(C,ek_0,ek_1)发送给敌手;
- 最后,敌手输出对 b 的猜测 b'.

在上述博弈中,敌手的优势被定义为 $Adv^{IND}_{SBE,\mathcal{A}}(n,t)=|\Pr[b'=b]-1/2|$.假设敌手能够攻击该方案,则挑战者能够将敌手对方案的攻击优势转换为对困难问题的求解优势,因此,敌手拥有不可忽略的优势,能够在多项式时间内解决定理中的困难性问题.这与已知任何多项式时间算法求解上述困难问题的成功概率是可忽略的事实相矛盾.通过反证法可知,敌手能够攻击该方案的假设不成立,因此方案针对选择明文共谋攻击具有语义安全.

2. 在数据完整性方面

GroupVPN 系统通过 SGS 数字签名(及其使用的密码学 Hash 函数)实现保护群组中的多播通信数据无法被篡改.

(1) 针对多播组外敌手的攻击,ISBE 的组内授权会话密钥分发可阻止敌手对数字签名δ的获取;

(2) 针对多播组内敌手的攻击,即便敌手获取到数字签名δ,根据群签名的抗伪造性,敌手伪造其他用户的签名也是计算困难的,并可通过签名验证算法 Verify 迅速被接收者检测到异常.

3. 在身份真实性方面

GroupVPN 系统可保证发送方与接收方两方身份的真实性,即双向认证功能,具体安全保证如下.

(1) 采用 SGS 签名中的 *Open* 函数实现签名者身份确认.

由于群签名方案中群组内成员具有相同的签名权,因此签名验证算法 Verify 具有匿名性(anonymity),这一特性可满足可信多播组内的公平性协议要求,如选举协议、竞拍协议等;当需要对发送方进行身份确认,可采用 *Open* 协议去匿名化找出原始签名者,其安全性服从如下定理:

定理 2(SGS 完全可跟踪性[19]). 如果 SDH 问题在$(\mathbb{G}_1,\mathbb{G}_2)$群上是$(q,t',\varepsilon')$-困难的,那么上述群签名方案是$(t,q_H,q_S,n,\varepsilon)$-完全可跟踪的,其中,$n=q-1$, $\varepsilon=4n\sqrt{2\varepsilon' q_H}+n/p$ 和 $t=\Theta(1)\cdot t'$.这里,q_H 是哈希函数查询次数,q_S 是签名查询次数,且 n 是群内成员数目.

定理表明,敌手伪造签名避免被追踪或者假冒原始签名者的概率是可忽略的,从而保证报文发送者或群组发起者的身份安全.类似于定理 1 的证明过程,定理 2 的证明依然采用敌手与挑战者之间的交互博弈,模拟敌手能够成功伪造不可被追踪来源签名的优势:首先,由挑战者指定被挑战的签名者,将其公钥发送给敌手;然后,敌手可以查询到除被挑战者之外的其他私钥以及任意指定的签名者对消息的有效签名;接着,敌手伪造指定被挑战者的签名并返回给挑战者;最后,若伪造的签名不在查询过程中出现过,且跟踪算法错误地追踪到指定被挑战者,则敌手伪造成功.

同样地,假设敌手能够攻击上述方案,即伪造出不可被追踪来源的签名,挑战者能够将敌手对方案的攻击优势转换为对困难问题的求解优势,这表明敌手拥有不可忽略的优势,能够在多项式时间内解决定理中的 SDH 问题.这与已知任何多项式时间算法求解上述困难问题的成功概率是可忽略的事实相矛盾.通过反证法可知,敌手能够攻击方案的假设不成立,即敌手无法伪造正确的签名或该伪造签名能够被追踪其来源.

(2) 采用 ISBE 方案中的授权解密功能实现了多播组的接收方身份确认.

即,只有属于多播组 S 的授权成员能够解密 ISBE 密文获得会话密钥.同样地,定理 1 中 ISBE 针对抗共谋攻击的安全性保证了非授权用户无法恢复会话密钥:假设任何非授权用户(包括非系统内攻击者和系统内的非授权用户)能够共谋获取会话密钥,那么也就意味着他们破坏了 ISBE 方案的语义安全性,与定理矛盾,因此保证了只有多播组内的接收者是合法会话密钥持有者,间接实现了接收方身份确认.

4 报文协议设计

4.1 数据封装格式

本文提出的多播密钥分发协议构架于网络协议栈的传输层之上,参考已有的 VPN 封装协议,我们设计了如表 2 所示的数据封装格式.

Table 2 Data encapsulation message format

表 2 数据封装报文格式

字段名	意义(位长)	用途
Next	下一首部(8)	下一数据段类型
Size	字段长度(16)	报文载荷长度
Op	操作类型(4)	标记该报文是分发、更新或撤销
Mode	加密模式(4)	定义可解密集合是当前集合还是补集
SPI	密码参数(32)	安全参数索引
Seq	序列号(32)	单调递增计数器,防止重发攻击
Exp	使用期限(32)	定义该共享密钥何时到期失效
C_1	密文 1(256)	群组密文的第一部分
C_2	密文 2(256)	群组密文的第二部分
Data	有效载荷(变长)	包括用户集合 S 和签名验证数据

鉴于在多播组的构建中群组密码一对多的优势,即可以实现对于同一密文有多个被授权的私钥能够成功解密,本文建议采用 UDP 协议装载所述数据报文.这种传输层协议格式简单、无连接,可支持在网络中高效传输和广播扩散所载荷的数据报文.相比于面向连接的 TCP 协议需要与每个节点执行 3 次握手 4 次挥手完成通信,UDP 协议结构简单,支持消息广播,传输速率快,更适合于视频直播、群组聊天等需要消息即时同步应用场景.因此,本文所设计的这种多播密钥分发协议正是有这种消息即时同步的需求.同时,为了弥补 UDP 协议不可靠传输的缺陷,我们在数据封装格式中加入序列号以及在工程实现中采取心跳机制,完成对该协议的程序设计.

在所述协议报文格式中,字段{C_1,C_2,*Mode*}结合字段 *Data* 中的用户集合 S 实现多播组的构建.根据 ISBE 方案的特点,群组密文的两部分 C_1 和 C_2 为常量大小,与当前多播组的规模无关,由密钥空间定义的位长(如 256 bits)决定其密文的长度.字段{*Next*,*Size*,*SPI*,*Seq*}保持与 IPSec VPN 一致.此外,字段{*Op*,*Exp*}用于管理多播组,其中,*Op* 标记多播组会话密钥的分发、更新和撤销,*Exp* 标记该多播组会话密钥的有效时间.字段 *Data* 是可变长的有效数据载荷,它包括了当前所构建的多播组中用户集合的身份标识信息,以及如之前方案所述的签名验证数据用以核实发起者的身份.

4.2 会话密钥管理

为方便多播组协议实现,本系统定义 3 种操作类型来表示如何组装功能性的报文,并分别用于发起者分发(distribute)、更新(update)和撤销(revoke)多播组.令 S 为当前要建立的多播组成员集合,忽略密文生成具体采用何种加密模式的细节,使用期限 *Exp* 为系统默认配置,3 种操作定义如下.

(1) *Distribute*(*S*,*Exp*):用于生成多播报文,输入多播组成员集合 S 和密钥共享的有效时长 *Exp*,它将操作类

型 *Op* 标记为分发,随机产生初始序列号 *Seq*,定义密钥的有效期,根据多播组成员集合确定采取的加密模式填充密文部分,最后对该分发标记的报文签名;

(2) *Update*(*S*,*Exp*):用于更新多播会话密钥,输入多播组成员集合 *S* 和密钥共享的有效时长 *Exp*,将操作类型标记为更新,在上一个报文的序列号 *Seq* 基础上加 1 填入,重置密钥的有效时长,生成一个隐藏了新的会话密钥的密文,并为该更新标记的报文签名;

(3) *Revoke*(·):用于撤销多播组,输入为空,它设置操作类型为撤销标记,序列号 *Seq* 继续在已有基础上加 1,使用期限为空,不用填充密文,最后加上发送者签名.

多播组生存周期从发起者初始化构建并分发密钥,而后多次更新当前多播组的会话密钥,直到最后撤销密钥删除当前多播组.对于多播组成员的添加和删除,则都可以通过调用 *Update* 函数来为新的成员集合重新分配密钥,旧的密钥则被废弃.例如,对于用户 Alice 的加入和用户 Bob 的退出,将分别对应于集合的并和除,即调用函数 *Update*(*S*∪{Alice},*Exp*)更新密钥添加用户,调用函数 *Update*(*S*\{Bob},*Exp*)更新密钥删除用户.

多播组构建过程中的聚合值计算是群组算法中的主要耗时部分,取决于多播组的规模.在本文中,我们将这一过程交由 GM 实现,用户可随时查询并继续使用聚合值进行会话密钥分发操作,从而降低成员的计算负载和网络延迟.因此,GM 和用户都可以通过缓存计算结果并多次使用达到提高性能的目的.

5 性能评估

为评估系统性能,本文在一种开源的对等 VPN 软件上进行二次开发,分别比较原有软件与采用本文方案后开发成型的软件在密钥分发和加密通信上的性能差异.我们选取采用对等技术构建虚拟专用网络的 PeerVPN 软件,它使用 C 语言编程实现并运行于 Linux 系统上,在 OpenSSL 开发包的支持下,使用 DH 密钥交换生成节点之间的会话密钥,以及采用 256 位的 AES 算法加密通信数据,通过节点之间消息路由构建完全的平铺网络,是一种比较典型的对等 VPN.

在 PeerVPN 的基础上,我们嵌入本文所提出的多播密钥分发方案,采用斯坦福大学的 C 语言版本 PBC 库编写 ISBE 密码算法,替换原有对等 VPN 中的密钥交换方法,而分发的会话密钥则采用与该软件相同的加密方式,目前已有程序代码上万行,部署在 10 个节点上用于性能测试.测试环境使用三层交换机配置私有网段,并在物理服务器上安装 VMware 或 VirtualBox 等软件创建 10 台虚拟机,为其配置 1GB 内存、1 个 CPU 单核、20GB 硬盘存储以及一块虚拟网卡用于桥接至三层交换机上,每台虚拟机安装 Ubuntu 16.04 操作系统作为程序的开发运行环境.

下面将分别通过理论对比和实验分析对群组 VPN 中密钥分发方法的性能进行分析.

5.1 密钥分发方法比较

为了在两方之间产生共享的会话密钥,已有的会话密钥分发技术可分为下面两类.

(1) 基于对称密码的密钥分发协议,如 NS,Kerberos 等,它由用户发出请求并与密钥分发中心 KDC 进行多步交互最终产生两方(或多方)共享密钥;

(2) 基于公钥密码的密钥交换协议,如 Diffie-Hellman 密钥交换技术,不依赖第三方,而由两方共同生成一个随机的会话密钥.

表 3 给出了群组分发方法与已有的两种密钥分发方法之间的简单对比.在这两种方法中:方法(1)简称对称密钥分发方法,可支持从两方到多方的扩展,但等效于多次协议执行,通信代价也随着参与方规模线性增长;方法(2)简称密钥交换方法,只支持两方共同生成会话密钥,由于该会话密钥的计算取决于两方各自选取的随机数,任意一方无法猜测该随机会话密钥的计算结果,因此不能直接从两方扩展到多方,只能通过协议的多次执行满足在多播组内共享相同的会话密钥.

上述两种方法与本文所提基于群组密码的密钥分发方法(简称多播密钥分发方法)相比较,在分发方式、密码基础、通信开销等方面都有较大差异.通过表 3 的对比不难发现:群组分发方法不需要中心机构颁发会话密钥,且能够同时与多方共享相同的会话密钥,其通信开销和计算效率都有很大的提升;基于身份标识的认证方式

能够便捷用户注册过程,减少系统内密钥管理工作,提高针对身份伪造攻击的安全防护.

Table 3 Comparison of session key distribution methods

表 3 会话密钥分发方法对比表

属性	对称密钥分发	密钥交换	多播密钥分发
分发方式	基于 KDC	基于 CA 证书	基于群组公钥
类型	两方或多方	两方	两方或多方
密码基础	对称加密	DH 协议	群组密码
认证方式	KDC 认证	公钥证书	身份标签
安全性	密文语义安全	计算 DH 问题	扩展 SDH 问题
通信开销	$O(n)$	$O(1)$	$O(1)$

5.2 密钥分发实验分析

为使群组 VPN 与对等 VPN 之间性能对比结果更为显著,上述实验环境在设计上将 VPN 程序运行时产生的网络流量通过单台交换机转发,从而忽略数据报文在公网中的传输时延.在此基础上,本文分别对两种 VPN 在密钥分发和加密通信前后两个阶段进行实验分析.密钥分发阶段用于生成隧道通信的会话密钥,在工程实现上对等 VPN 需要至少 3 次交互以完成会话密钥的生成,包括:1) 产生一个会话;2) 交换随机数;3) 确认会话密钥.在此之后,两方交互初始化隧道参数.而群组 VPN 将一方产生的随机会话密钥隐藏在群组加密密文中,广播该密文而无需交互,即可完成对可选用户集合的会话密钥分发.

如图 4 所示,实验分析结果显示了随着群组规模增大,两种 VPN 在为群组成员分发会话密钥的交互耗时.实验中,接收方群组规模从 1~9 变化,交互耗时单位为毫秒.对等 VPN 中密钥交换协议需要与每个用户单独进行交互,所以实验结果(三角)显示,其密钥交换耗时随群组规模成线性增长.与之相比较,群组 VPN(圆点)中多播分发在群组规模较小时,耗时相对较大;当超过 5 个节点时,其交互耗时逐渐优于对等 VPN 中密钥交换.该实验结果的原因在于:多播分发使用的群组密码技术中的主要计算开销是聚合值计算与椭圆曲线下的双线性映射运算,当群组规模较小时,由于基于双线性映射的初始化过程耗时较多,导致群组 VPN 性能弱于对等 VPN.但该过程耗时并不随群组规模增长而变化,而更多耗时被用于聚合值计算,但从图中的拟合曲线可知,聚合值计算的耗时速率要小于密钥交换的耗时速率,因而群组 VPN 的交互耗时随规模增长要小于对等 VPN.因此,群组 VPN 更适用于更大规模的网络环境.

在相同实验环境下,图 5 表明了在密钥分发阶段完成之后,群组内成员通过加密隧道向群组内其他成员进行多播通信的耗时.

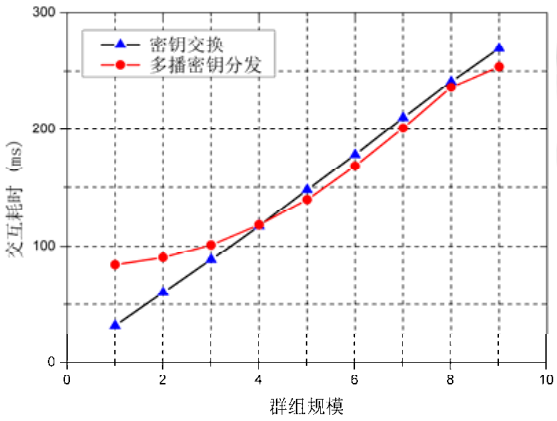

Fig.4 Interaction time-overheads in key distribution

图 4 密钥分发阶段交互耗时

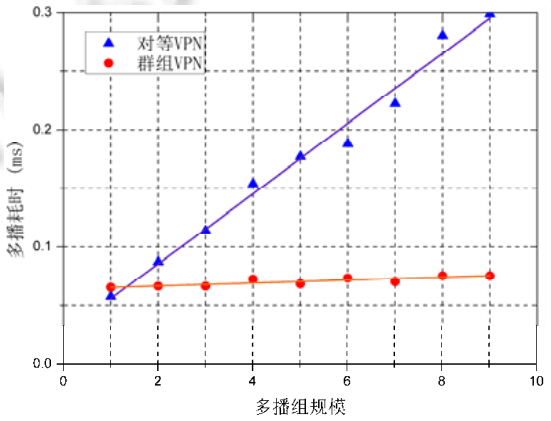

Fig.5 Multicast time-overheads in encrypted communication

图 5 加密通信阶段多播耗时

由于群组 VPN 中多播组内共享同一会话密钥,因此消息只需加密一次,多播耗时随群组规模的增长没有太大的变化,这可通过图中圆点及拟合直线予以验证.而对等 VPN 下的多播耗时则随着群组规模增长呈较明显的线性增长,其增长是由于不同会话密钥对同一消息进行隧道加密计算造成的.因此,群组 VPN 对消息的接收延迟较小,更适用于大规模群组内多播消息的同步接收.

6 总 结

本文提出一种被称为 GroupVPN 的对等 VPN 框架,该框架结合公钥群组密码下的广播加密和群签名方案,实现一种多播密钥分发协议,保证在 SDH 假设下满足数据私密性、数据完整性、身份真实性这 3 方面安全性要求.实验分析表明,该协议可将通信延迟限制在会话密钥分发阶段,从而降低了加密通信阶段的通信耗时.

References:

[1] Knight P, Lewis C. Layer 2 and 3 virtual private networks: Taxonomy, technology, and standardization efforts. Communications Magazine, IEEE, 2004,42(6):124−131.

[2] Berger T. Analysis of current VPN technologies. In: Proc. of the Int'l Conf. on Availability, Reliability and Security. IEEE, 2006. 8−115.

[3] Jaha AA, Shatwan FB, Ashibani M. Proper virtual private network (VPN) solution. In: Proc. of the 2nd Int'l Conf. on IEEE Next Generation Mobile Applications, Services and Technologies. IEEE Computer Society, 2008. 309−314.

[4] Zaharuddin MHM, Ab Rahman R, Kassim M. Technical comparison analysis of encryption algorithm on site-to-site IPSec VPN. In: Proc. of the Int'l Conf. on Computer Applications and Industrial Electronics (ICCAIE). IEEE, 2010. 641−645.

[5] Jahan S, Rahman MS, Saha S. Application specific tunneling protocol selection for virtual private networks. In: Proc. of the Int'l Conf. on Networking, Systems and Security (NSysS). IEEE, 2017. 39−44.

[6] Deri L, Andrews R. N2n: A layer two peer-to-peer VPN. In: Proc. of the Int'l Conf. on Autonomous Infrastructure, Management and Security: Resilient Networks and Services. Springer-Verlag, 2008. 53−64.

[7] Boneh D, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Proc. of the Int'l Conf. on Advances in Cryptology, Vol.3621. Springer-Verlag, 2005. 258−275.

[8] Delerablée C. Identity-Based broadcast encryption with constant size ciphertexts and private keys. In: Proc. of the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Springer-Verlag, 2007. 200−215.

[9] Libert B, Paterson KG, Quaglia EA. Anonymous broadcast encryption: Adaptive security and efficient constructions in the standard model. In: Proc. of the Int'l Workshop on Public Key Cryptography. Springer-Verlag, 2012. 206−224.

[10] Phan DH, Pointcheval D, Shahandashti SF, *et al*. Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts. Int'l Journal of Information Security, 2013,12(4):251−265.

[11] Wesolowski B, Junod P. Ciphertext-Policy attribute-based broadcast encryption with small keys. In: Proc. of the Int'l Conf. on Information Security and Cryptology. Cham: Springer-Verlag, 2015. 53−68.

[12] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers. In: Proc. of the Int'l Cryptology Conf. Berlin, Heidelberg: Springer-Verlag, 2001. 41−62.

[13] Lewko A, Sahai A, Waters B. Revocation systems with very small private keys. In: Proc. of the IEEE Symp. on Security and Privacy (SP). IEEE Computer Society, 2010. 273−285.

[14] Lai J, Mu Y, Guo F, *et al*. Anonymous identity-based broadcast encryption with revocation for file sharing. In: Proc. of the Australasian Conf. on Information Security and Privacy. Springer-Verlag, 2016. 223−239.

[15] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer and System Sciences, 1984,28(2):270−299.

[16] Barbosa M, Farshim P. On the semantic security of functional encryption schemes. In: Proc. of the Public Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 2013. 143−161.

[17] Krishnan AG, Wilson V. Improving security in a virtual network by using attribute based encryption algorithm. In: Proc. of the Int'l Conf. on Circuit, Power and Computing Technologies (ICCPCT). IEEE, 2016. 1−6.

[18] Zhu Y, Wang X, Ma D, *et al*. Identity-Set-Based broadcast encryption supporting cut-or-select with short ciphertext. In: Proc. of the ACM Symp. on Information, Computer and Communications Security. ACM Press, 2015. 191−202.

[19] Boneh D, Boyen X, Shacham H. Short group signatures. LNCS, 2004,22(6):41−55.

[20] Zhao AQ, Ji Y, Gu GQ. Research on tunneling techniques supporting VPN. Journal of Communication, 2000,21(6):85−91 (in Chinese with English abstract).

[21] Zhang QK, Wang RF, Tan YA. Identity-based authenticated asymmetric group key agreement. Journal of Computer Research and Development, 2014,51(8):1727−1738 (in Chinese with English abstract).

附中文参考文献:

[20] 赵阿群,吉逸,顾冠群.支持 VPN 的隧道技术研究.通信学报,2000,21(6):85−91.

[21] 张启坤,王锐芳,谭毓安.基于身份的可认证非对称群组密钥协商协议.计算机研究与发展,2014,51(8):1727−1738.

朱岩(1974－),男,博士,教授,博士生导师,CCF 专业会员,主要研究领域为信息安全,密码学.

尹昊(1993－),男,硕士,主要研究领域为信息安全,密码学.

王秋艳,女,主要研究领域为信息化技术,区块链与互联网.