一种安全有效的无线网络消息传输方案①

A Secure and Efficient Message Transmission Scheme in Wireless Networks

周 权 (广州大学信息安全研究所 广东广州 510006)
周 敏 肖德琴 (华南农业大学信息学院 广东广州 510642)
唐 屹 (广州大学信息安全研究所 广东广州 510006)

摘 要: 远程移动用户访问组织内部网络除了需要高数据传输率,还需要保证传输消息的安全。VPN 是一种较好解决组织员工、合作伙伴安全访问组织内部网络的技术,将 VPN 技术扩展到移动无线网络通信中构成 MVPN(Mobile VPN),可以通过公网基础设施利用无线通信设备如 GMS、GPRS、WLAN、UMTS 等建立同组织内部网络的安全隧道,进行安全消息传输;但这将促使传输数据的膨胀,通过采用 IPComp、IP 头压缩和优化的 IPSec 数据处理可以有效地减少 IPSec ESP 隧道模式下的数据膨胀,提高数据传输效率。

关键词: 无线网络 MVPN IPSec 数据压缩

1 引言

随着计算机技术和网络技术的发展,计算机网络已经进入到人们的日常生活中,网络技术集成了有线通讯和无线通讯技术,以致访问信息的手段也多样化。人们可以借助无线移动设备,如 PAD、移动笔记本电脑、手机等对组织内部网络信息资源进行访问,实现远程移动办公。使用无线设备访问信息资源,可以消除访问受地点和时间的限制,从而为工作和生活带来便捷,但是同时也带来了访问信息的安全问题。当人们进行无线办公时,可能泄漏组织内部的敏感信息,同时攻击者也可能冒充组织内部员工进行非法访问,破坏组织的业务连续性。因而,对于移动设备访问组织信息资源的安全一致是困扰组织的问题。为此许多组织限制使用移动无线设备访问组织的资源,从而导致组织的运行成本的增加。为了解决这个问题,本文设计了一种安全有效的无线网络信息传输方案,该方案借助于 MVPN(Mobile Virtual Private Network)技术,实现了无线设备访问组织信息资源的保密性,完整性和可控性;由于 MVPN 采用 IPSec ESP 来建立安全隧道,这将导致传输消息的膨胀,从而降低无线数据传输效率,为此我们采用 IP 头部压缩与 IP 数据压缩相结合,减少传输数据量来提高 UMTS(Universal Mobile Telecommunications System)中无线通信的效率;最后分析了方案的效率和安全性。

2 IPSec 和 VPN 技术

IPSec[1]协议是 IETF 制定在网络层保护 IP 数据报文安全的安全协议,能够提供传输消息的机密性、消息源的认证、无连接消息的完整性、抗重放攻击以及有限业务流机密性等安全服务。为了给 IP 数据报文提供高质量的、互操作的、基于密码学的安全性,IPSec 协议支持认证头(AH, Authentication Header[2])和封装安全载荷(ESP, Encapsulating Security Payload[3])以及 Internet 密钥交换(IKE, Internet Key Exchange[4])协议来达到目标。IPSec 协议为支持不同安全需求提供传输模式和隧道操作,两种操作模式均通过对原 IP 数据报文进行相应的修改,达到实现 IP 数据报文安全传输的目的。

VPN(Virtual Private Network[5])技术是一种利用公共网络基础设施来实现消息安全传输的方法,是实

① 基金项目:国家自然科学基金重点项目(90104005);广东省教育厅自然科学研究项目(Z03001)

现组织与其分支机构以及合作伙伴之间的信息安全交换的有效策略。VPN 技术在公共网络基础设施基础上建立安全隧道实现一种安全专用网络，能够防止信息被劫持、嗅探、假冒等攻击，同时能够降低组织的安全运行成本。安全隧道技术是构建安全 VPN 的关键技术，安全隧道协议可以在 OSI 网络模型的不同层上建立实现，主要有三种：采用口令应答机制实现拨号连接的认证的数据链路层 L2TP 协议和 PPTP 协议；实现对传输消息的认证和加密的网络层 IPSec 协议；基于 WEB 客户/服务应用的传输层 TLS/SSL 协议。IPSec 协议克服了 L2TP、PPTP 以及 SSL 的一些安全局限，同时，在设计安全 VPN 时，主要采用 IPSec 的隧道模式，因为传输模式仅仅保护被上层协议封装的负载，不能提供 IP 头部的保护；而隧道模式提供了整个 IP 数据报文的保护。MVPN 技术是对 VPN 技术在移动网络中的扩展，在移动设备（便携式电脑、PDA、智能手机等）上采用 IPSec 协议来建立安全隧道，实现移动设备主机与安全 IPSec 网关之间的消息安全传输。图 1 是 IPSec 隧道模式实现的 MVPN 体系结构框架。移动设备借助于 GSM、GPRS、WLAN、UMTS 等与 IPSec 安全网关通过安全隧道进行消息的安全传输。从而，MVPN 可以使分支机构以及合作伙伴和移动用户均可以与组织总部建立安全隧道，进行消息安全传输。

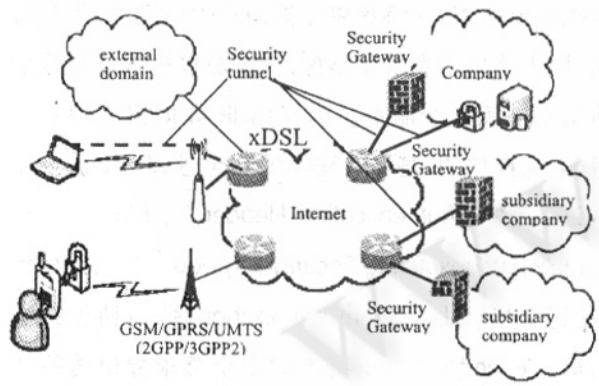

图 1　MVPN 体系结构框架

3　MVPN 中 IP 数据压缩与膨胀

IPSec ESP 隧道模式设计的 MVPN，能够保护 IP 数据报文的安全，但是需要增加一些额外的开销，即需要对原始的 IP 数据报文进行修改增加一些新的额外信息，也就是，数据报文附带其他安全信息，从而传输的消息膨胀。在 AH 隧道模式中膨胀的数据有：新 IP 头部（20 字节）、AH 头部（采用 MD5 认证方法为 40 字节，采用 SHA－1 认证方法为 44 字节）。在 ESP 隧道模式中膨胀的数据有：新 IP 头部（20 字节）、ESP 头部（8 字节）、ESP 尾部（2 字节再加上可变的填充部分 0－255 字节）、ESP 认证数据（采用 MD5 认证方法为 16 字节，采用 SHA－1 认证方法为 20 字节）。以致在 IPSec ESP 隧道模式下，整个传输数据膨胀了 46—305 字节。对于 IPv4 数据报的隧道模式 ESP 头部数据报平均可能增加 300 字节[6]。在 UMTS 无线通信中，通过使用 CRTP（Enhanced Compressed RTP）[7] 协议能实现对 TCP/IP 头进行较大的压缩，可以将 40 字节的 TCP/IP 头部压缩到 2－5 字节，但是对 IPSec ESP 隧道模式的 ESP 头部和尾部没有进行压缩处理。

在无线通信信道中，通信的可靠性、数据传输率、位错误率等是其关键的指标。为了提高无线通信服务质量，希望有尽可能高的数据传输率，低的位错误率。在位错误率一定的情况下，数据报的丢失率与传输的数据报的大小有关，传输的数据报越小，则丢包率就越小，从而无线网络服务质量就高，无线通信的吞吐量就高，通信开销就低。所以有必要在无线通信过程中采用较小数据报传输，这就必须对数据报进行相应压缩。为了解决无线通信中数据膨胀对 IPSec VPN 效率和无线通信质量的影响，我们采用 IPComp（IP Payload Compressor Proocol[8]）的压缩算法来减少 IP 数据报文的长度，如 DEFLAT 算法、LZS 算法。IPComp 协议对数据压缩是一种无损压缩，其压缩算法使用特殊的编码技术对数据进行编码消除冗余或重复部分数据，这将导致数据更加随机，因而，对随机数据的压缩是最无效的，实际上对随机数据的压缩可能导致数据量增加。所以，在使用 IPComp 协议对 IPSec 隧道模式的数据压缩可能无效，因为 IPSec 隧道模式加密后数据将更加随机。以致不能随便使用 IPConp 协议，我们采用先压缩，再加密，从而避免数据压缩的无效性。同时，IPComp 应用过程中，要求每个数据报独立压缩和解压，且数据报之间无任何关系。并且该协议没有对 IP 头或 IPSec ESP、IPSEC AH 头部压缩，仅仅对负载数据部分压缩处理。为此，我们采用 IP 头部压缩技术（IP Head-

er Compression[9])，来实现对 IP 头部的压缩，降低数据传输量。使用 IP 头部压缩技术可以将 40 字节的 TCP/IP 头部压缩到 2－5 字节，减少至少 35 字节的传输量。在 MVPN 中采用该技术能够实现 IPSec ESP 和 IPSec AH 载荷附带信息（ESP 和 AH 头部、密码算法、填充信息等）的压缩，从而提高无线通信的传输率。

4　MVPN 中数据处理流程

从上面分析可以发现无论采用 IPComp 协议还是采用 CRTP 协议对 UMTS 中传输的信息均要产生信息膨胀，这对无线通信是不利的，这也是为保证无线通信的安全所必须付出的代价。但是，将上述的压缩协议与 IPSec 数据处理的方式进行优化可以大大降低传输的信息量，从而提高无线通信的数据传输率。图 2 描述了优化的 IP 数据报文处理流程。

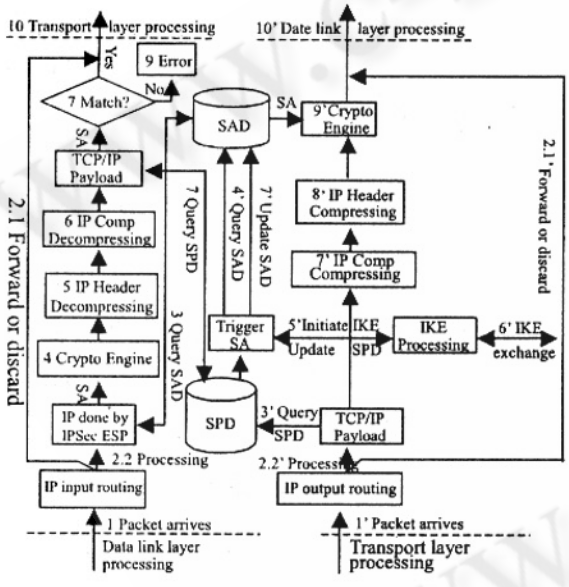

图 2　数据报文处理流程

对于发送方（图 2 的右部分）进行 4 步：

（1）原始 IP 数据报文利用 IPComp 协议对 IP 载荷数据部分压缩得到 IPComp 数据报，同时根据 IP 头部信息查询 SAD，找到相应的 SA；

（2）利用 IP 头部压缩协议进行 IPComp 数据报头部压缩，得到 IHC 数据报；

（3）对 IHC 数据报根据相应的 SA 进行 IPSec ESP 处理（加密，认证），得到 IPSec ESP 数据报；

（4）将 IPSec ESP 数据报转发到数据链路层进行 CRTP 处理，得到 L2 PPDCP 数据帧发送。

对于接收方（图 2 的左部分）进行 4 步：

（1）对收到的 IP 数据报文（IPSec ESP 数据报）进行认证、完整性验证以及解密，并去掉 ESP 头部和尾部，得到 IHC 数据报；

（2）对 IHC 数据报进行 IHC 头部解压得到 IPComp 数据报；

（3）对 IPComp 数据报的数据部分负载解压得到 IP 数据报；

（4）通过 IP 数据报文进行 SA 查询，再次验证 SA 是否与解密加压前得到的 SA 一致，如一致则传到上层处理，否则出错处理。

5 效率和安全性分析

原始的 IP 数据报文，经过 IPComp、IP 头部压缩和 IPSec ESP 处理的变化过程如图 3。

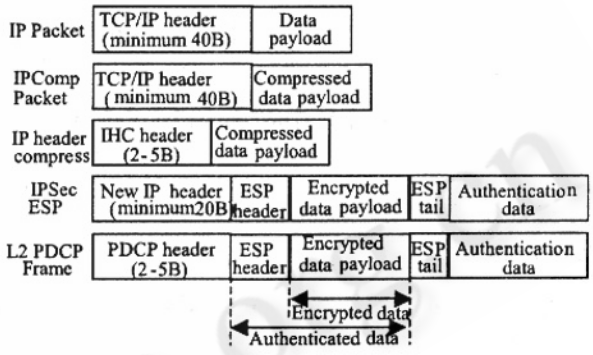

图 3　IPSec ESP 隧道模式 IP 数据报文结构变化

采用 IPComp 协议对 IP 数据报进行压缩，由于 IPComp 应用中可能出现 IP 载荷变大的可能，这个过程在进行 IPSec ESP 处理前进行，避免压缩数据的无效性，因为 ESP 加密将使数据更加随机，IPComp 对随机数据其压缩效率更低，甚至数据可能反而膨胀。在应用 IPComp 我们采用自适应算法，设置了一个门限值 96 字节，对于小于 96 字节 IP 载荷（去掉 IP 头的数据报）不进行压缩，直接进行 IP 头部压缩处理，从而来避免压缩处理可能占用大量的 CPU 时间，以便提高效率。在应用 IP 头部压缩过程中，由于只对 IP 头部处理，可以将原来 40 字节的 TCP/IP 头部减少 35—38 字节，减少了传输信息量。经过 IPComp 和 IP 头部压缩，原来 IP 数据报文长度减少了，至少减少 35 字节，在进行 IPSec ESP 处理时，加密的明文数据量减少了，如采

用 128 位的 AES(Advanced Encryption Standard[10])加密算法来说,可以至少减少 2 个分组和 2 个密钥流的扩展。同时在计算 MAC 过程中,由于数据量减少,也提高了认证处理能力。然而,由于应用了 IPComp 协议和 IP 头部压缩,以致在进行 IKE 交换生成安全策略和相应得 SA 时,增加了交换的信息,即 IKE 交换的数据报增大了,这也加大了 SPD 和 SAD 的管理。整个方案的安全性是建立在 IPSec ESP 的安全性上,具有 ESP 的所有安全功能,能够提供机密性、完整性、抗重放攻击等安全功能,并且处理上效率更高了。

参考文献

1 Kent S. ,Atkinson R. ,Security Architecture for the Internet Protocol[S],IETF RFC2401, Sep. 1998.

2 Kent S, Atkinson R1 IP Authentication Heard [S] IETF RFC2402 Nov. 1998.

3 Kent S. ,Atkinson R. ,Security IP Encapsulating Security Payloady (ESP)[S],IETF RFC2406, Sep. 1998.

4 Kent S, Atkinson R1 The Internet Key Exchange (IKE)[S] IETF RFC2409,Nov. 1998.

5 周权,肖德琴,唐屹. 基于 Linux 和 IPSec 的 VPN 安全网关设计与实现[J]. 计算机应用与研究,2005(9):229 - 234.

6 Carlton R. Davis, IPSec Securing VPNs, RSA Press, Mc Graw Hill.

7 T. Koren, S. Casner, J . Geevarghese, B. Thompson, and P. Ruddy, Enhanced Compressed RTP (CRTP) for links with high delay, loss and recording [S], IETF RFC 3545 Jul. 2003.

8 A. Shacham, B. Monsour, R. Pereira, and M. Thomas, IP Payload Compression Protocol (IPComp)[S], IETF RFC 3173. Sep. 2001.

9 M. Degermark, B. Nordgren, and S. Pink, IP Header Compression[S], IETF RFC 2507. Feb. 1999.

10 Advanced Encryption Standard (AES)[S]. Federal Information Processing Standards Publication 197, Nov. 26, 2001. http// csrc. nist. Gov/publications/fips/fips197/fips2197. pdf