一个采用分段验证签密隐蔽路由的设计与实现

赵福祥[1,2], 赵红云[2], 王育民[1], 杨世平[2]
(1. 西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071; 2. 西安通信学院, 陕西西安 710106)

摘 要: 在公开的计算机网络中采用隐蔽路由网络连接, 任何隐蔽网络的用户只能获得与其直接连接的前序和后继节点的地址, 使得攻击者既不能窃听到机密, 也不能实施流量分析. 现有的隐蔽路由方案或采用原子签名和加密, 或采用嵌套加密和签名, 即洋葱路由, 本文应用分段验证签密的方法提出了一个新的隐蔽路由实现方案, 该方案用签密代替现有方案中先签名再加密两步常规密码方法, 减少协议的计算和通信量, 提高了执行效率, 并包容了两种方法各自具有的优点. 最后分析了方案的安全性.

关键词: 网络安全; 信息隐藏; 隐蔽路由; 签密; 分段验证签密
中图分类号: TN915.08; TP393.08 文献标识码: A 文章编号: 0372-2112 (2002) 07-0995-04

An Anonymous Routing Based on Domain-Verifiable Signcryption

ZHAO Fu-xiang[1,2], ZHAO Hong-yun[2], WANG Yu-min[1], YANG Shi-ping[2]
(1. *The National Key Lab on ISN, Xidian University, Xi'an, Shaanxi 710071, China;*
2. *The Xi'an School of Communication, Xi'an, Shaanxi 710106, China*)

Abstract: Anonymous routing connections on open computer networks are strongly resistant to both eavesdropping and traffic analysis, as any user of the anonymous networks can only obtain the addresses of its predecessor and successor sites. The anonymous routing schemes available are constructed either by using atomic signature and encryption or by nested signature and encryption, or onion routing. A new scheme that hides information and prevents from disturbing data packages is presented with Domain-Verifiable Signcryption technique. In this context, it appears to be efficient that the system is built by using efficient digital signcryption techniques instead of traditional paradigm of generating a digital signature of a message and then encrypting the signature together with the message and reducing computation and overhead costs in the protocol. At the same time, the merit of two kinds of schemes above is obtained. Finally, an analysis of security is given.

Key words: networks security; information hiding; anonymous routing; signcryption; domain-verifiable signcryption

1 引言

在公开的计算机网络中, 每个 IP 包的地址等包头信息必须是公开的. 因此通过加密数据虽可抵御窃听, 但攻击者仍能由其公开的地址等信息进行流量分析从而得出安全网络的结构信息. 为此, Chaum 在文献[1]中提出了无条件不可跟踪消息交换和计算性不可跟踪消息交换两种方法, 其中计算性不可跟踪消息交换定义了一个经过多个中间节点转发数据的多级目标路径, 称为混淆(Mixes). 即假定发送者选定 N 个连续目标, 其中之一为真正接收者, 窃听者在一段路径上获取真正接收者的概率为 1/N, 并且中间节点在传送消息时可采取重新排序、延迟和填充手段使获取真正目标的概率更低, 增加攻击者流量分析的难度[1~3]. 其实现上采用洋葱路由方案作为一个特殊的混淆结构, 动态地构造一条隐蔽路径, 满足对所传数据和网络结构都给予隐蔽的要求, 它是运用加密技术分层隐藏 IP 包地址的方法来构造一条混淆路径的[4,5]. 但是现有的隐蔽路由方案大都采用了常规密码方法, 即采用先对消息签名然后再把消息和签名一起加密, 采用这一方法的结果, 由于签名和加密的大量重叠计算, 使得系统的运行效率不高, 因此要取得实用, 就必须采用新的高效的密码算法和灵活的协议.

本文首先分析了现有隐蔽路由方案, 针对其密码算法效率低和路由分配不灵活的不足, 结合文献[6~10]中高效的分段验证数字签密算法, 对现有隐蔽路由方法加以改进, 提出了新的分段验证签密隐蔽路由方案, 最后给出了安全分析.

2 隐蔽路由方案

2.1 隐蔽路由的定义

采用确定路由地址的源路由协议, 选定由若干中间目标组成的多段路径, 并把后段路径的 IP 包的数据和地址一起加密作为前段路径 IP 包的载体传送, 就隐蔽掉了目标节点地

收稿日期: 2001-05-08; 修回日期: 2002-01-05
基金项目: 国家自然科学基金重点资助项目(No. 19931010)

址, 从而得到多级混淆的隐蔽路径. 其 IP 包可分别采用原子签名和加密或采用从后向前逐层的嵌套签名和加密, 即格式就如同多层的洋葱. 由网络节点分别采用不同的加密密钥加密, 使收到这个包的目标节点只能解密与本节点对应的信息, 而不能读取其它节点的任何信息. 对于任意中间节点只能获取与其相关前序和后继两相邻节点的路由信息, 不能从 IP 包获取整个路径更多的其它信息, 隐蔽路由(Anonymous Routing)就是对这一路径的分配过程. 图 1 说明了一个具有五个洋葱路由器的洋葱路由分配包的结构. 通常在安全网络的首节点上运行有代理服务器负责隐蔽路由的分配. 中间目标执行 IP 包解密, 从中取得下一目标地址以完成隐蔽网络的传递, 因而称为隐蔽路由器. 整个安全网络可由多个隐蔽路由器和代理组成, 可同时构成多条隐蔽路径. 隐蔽路径可以构造成实时和双向的[11~14]. 隐蔽路径屏蔽掉了路由信息, 使得攻击者从任何一点截取此 IP 包也不能得到整个路径的信息[4, 5, 11~13]. 分配双向加密密钥和加密函数的信息包如下所示.

$$\{exp\_time, next\_hop, F_f, K_f, F_b, K_b, payload\}_{PK} \quad (1)$$

其中 exp_time 为包的生命周期, $next\_hop$ 为下一个节点地址, (F_f, K_f) 为前向函数/密钥对, (F_b, K_b) 为后向函数/密钥对, $payload$ 或为下一个相同结构的信息包或为一个 $PADDING$, PK 为所接收洋葱路由器的公钥.

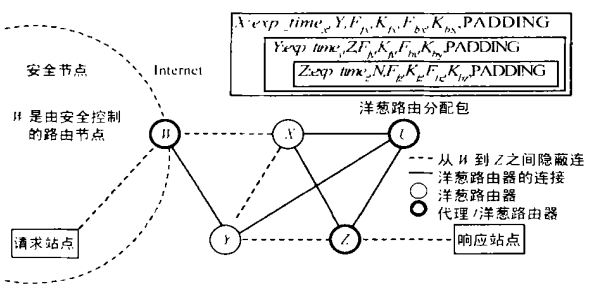

图 1 隐蔽网络拓扑结构及路分配

2.2 现有方案分析

Goldschlag 的隐蔽路由方案采用了实时双向洋葱路由的方法. 洋葱路由是首节点上的代理服务器确定的. 其数据流经过若干中间洋葱路由器后抵达目的节点而形成一条隐蔽路径. 现有方案中, 建立隐蔽路径的核心问题是隐蔽路由的分配. 当把函数/密钥及后继节点地址等信息简化为路由 ip, 则隐蔽网络所使用的嵌套式洋葱路由如下式所示:

$$r = E_{e_1}[ip(c_2), t_2, S_{h_2}(ip(c_1), ip(c_2), t_2), E_{e_2}[ip(c_3), \cdots, E_{e_{n-1}}[ip(c_n), t_n, S_{h_n}(ip(c_{n-1}), ip(c_n), t_n)]\cdots]] \quad (2)$$

其中 $ip(c_i)$ 代表下一节点的路由分配信息, $S_{h_i}(\cdot)$ 代表用私钥 h_i 实现的签名, t_i 代表生命周期(其中 $i = 2, \cdots, n$). 除采用嵌套式洋葱路由, Westhoff 在文献[14]中还提出原子签名加密路由结构, 如下式所示:

$$r = E_{e_1}[ip(c_2), t_2, S_{h_2}(ip(c_1), ip(c_2), t_2)] \parallel E_{e_2}[ip(c_3), t_3, S_{h_3}(ip(c_2), ip(c_3), t_3)] \parallel \cdots \parallel E_{e_{n-1}}[ip(c_n), t_n, S_{h_n}(ip(c_{n-1}), ip(c_n), t_n)] \parallel \quad (3)$$

另外, 现有方案采用动态实时的双向加密函数和密钥分配, 这样的分配使各洋葱路由器节点安全独立性增强, 动态实时的分配使得攻击者没有机会对加密的信息进行分析; 加密的函数和密钥同时分配使得信息传输的安全与隐蔽路由器无关; 独立的双向分配使得任意的路由器节点与两个相邻的路由器使用加密方法不同, 同时使隐蔽路径在正反两个方向独立. 这些方法都加大了攻击者进行流量分析的难度, 使路径隐蔽性进一步增强. 并且, 中间隐蔽路由器不知道安全网络的结构, 因此不允许路径重排.

现有的方案虽然加大了攻击的难度, 但由于构造隐蔽路径耗费大, 采用常规密码实现方法因效率很低, 实际实现中必然存在下列问题:

(1)隐蔽路径进行路由分配和信息传输时都用加密来隐蔽, 要使得其信息是保密且是可靠的, 常规密码方法采用的是先签名再加密两步实现的, 计算量和通信量都很大, 并且随着隐蔽路径长度增加, 其实现上越困难, 因而不适合构造大的隐蔽路径.

(2)虽然采用签密方法可以用一个逻辑步骤代替常规密码的两步计算, 大大提高签名和加密的执行效率, 但一般的签密方法或不能在解密前验证签名, 或只能完成单步解密前验证签名, 应用于隐蔽路由, 其结果仍会由每个节点的单独使用而形成简单的多层嵌套 IP 包结构或原子 IP 包结构.

(3)当采用多层嵌套 IP 包结构使得中间节点不能随意删除其它信息, 易于保证其信息的完整性, 但其签名和加密的重复程度要远远高于原子 IP 包结构, 并且不易扩展; 而当采用原子 IP 包结构时, 任意一个节点信息都可被删除, 从而可发生不诚实节点间的串通攻击, 而不留证据.

(4)若采用常规密码方法管理隐蔽路由, 其密钥证书机构非常复杂, 动态分配隐蔽路径困难, 安全网络由于运行复杂而难于实现.

基于上述原因, 新的隐蔽方案采用了分段验证签密方法来构造隐蔽路径.

2.3 分段验证签密算法

使用签密除了可一次同时完成两个步骤而使其效率比先签名然后加密的方法好外, 改进的签密方案还实现了让第三方在不取得原文的情况下验证签名. 分段验证签密则适合让多个参与者共同完成, 即一个完整的签密信息被分成若干段, 在每个参与者段内, 参与者能获得其明文信息而使得其他参与者不能得到它; 但所有的参与者可以验证整个信息的正确性. 假定 p 是大素数, q 是 $p-1$ 的大素因子, g 是 Z_p^* 中一个 q 阶元素, $E_k(m)$ 和 $D_k(c)$ 分别表示如 DES 一类的加密和解密算法, $hash(m)$ 为一单向 hash 函数, $KH_k(m)$ 表示一个 hash 函数, 即 $KH_k(m) = hash(k, m)$. $Alice$ 从 $[1, \cdots, q-1]$ 选取私钥 $x_a \in Z_q^*$, 公开相应公钥 $y_a \in Z_p^*$ 且 $y_a = g^{x_a} \bmod p$; B_i 为第 i 个接收者, 同样具有密钥对, 即私钥 $x_{b_i} \in Z_q^*$ 和公钥 $y_{b_i} \in Z_p^*$ 且 $y_{b_i} = g^{x_{b_i}} \bmod p$(其中 $i \in \{1, \cdots, n\}$). 图 2 给出了其签密的实现说明.

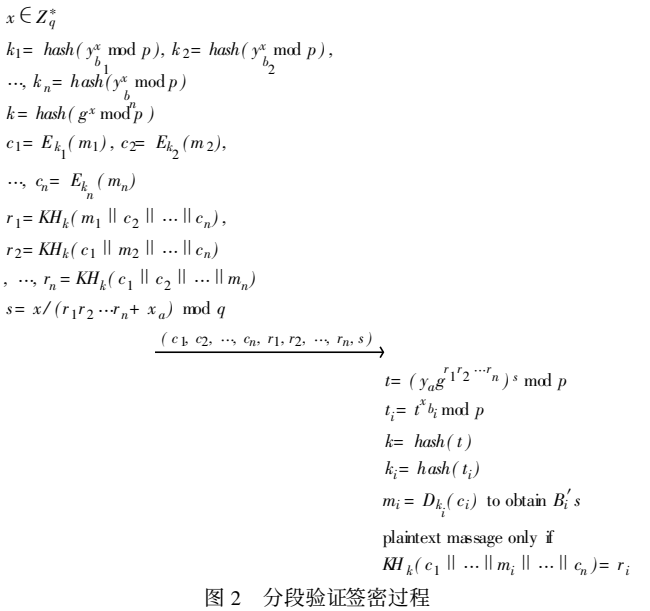

图 2　分段验证签密过程

2.4　新的隐蔽路由方案

通过以上对现有隐蔽路由方案的分析可以看出,路径安全性不但依赖于该路径的隐蔽性,还要保证所传 IP 数据的可信赖程度,所传输的 IP 数据包除加密外还要经过签字. 另外,在保证不被相互串通的攻击者任意窜改 IP 路由信息的同时,IP 数据包要从多层嵌套结构向原子结构方向扩展. 因此,采用 2.3 节分段验证签密算法可高效地实现这样需求的数据传输. 为了最好地保持隐蔽路由方案中好的特性,即在各隐蔽路由器之间要签字,但除相邻节点外又不能暴露彼此的身份,因此新的隐蔽路由方案采用了可信标识(TrustMark)和群签密方法来增加 IP 数据包的可信赖度,其密钥可采用集中管理方式管理(也可分散管理),并增加时戳信息以保证实时性. 本文以集中管理方式为例说明具体协议实现方法.

首先假设群密钥管理中心就为安全网络管理体中心 SMC, $R_i(i = 1, \ldots, N)$ 属于向管理中心注册的隐蔽路由器/代理,并假定 R_i 与 SMC 已通过安全通道取得对方签密公钥,但除隐蔽路径中采用分段验证签密外,其它过程的实现仍采用一般签密方法.

(1)初始化: R_i 在注册时生成自己的密钥对 $(s_i, g^{s_i} \pmod p)$,并把 g^{s_i} 交给 SMC. SMC 记录下所有 R_i 真实身份 ID_i(隐蔽路由器地址或名称等)和公钥 g^{s_i},并为 R_i 生成一个安全隐蔽路由器/代理可信的标识 TM_i, TM_i 包含属于该群的身份标识和用户 ID_i 生成的随机数. SMC 把 TM_i 返还给 R_i. 每隔一段时间 SMC 随机选取一组数 $d_{it}(t = 1 \cdots T$ 的小时段)并公布所有盲签名的公钥 $(g^{s_i})^{d_{it}}$,把 d_{it} 返还给 R_i, R_i 用 s_i 和 d_{it} 生成签名私钥 $s_i d_{it} \pmod p$. 初始化协议如图 3 所示.

(2)请求分配隐蔽路由:当 R_i 需建立到 R_j 隐蔽路径时,经安全通道向 SMC 发出一个隐蔽路由分配请求,该请求包括隐蔽路径所经隐蔽路由器节点地址及其相应的公钥证书,SMC 在验证了 R_i 真实身份后,按 R_i 到 R_j 路径顺序分配隐蔽路由器 R_x 的节点地址(可选)和相应的群签密公钥 $(g^{s_x})^{r_{xt}}$ 证书返回 R_i;请求分配隐蔽路由协议如图 4 所示.

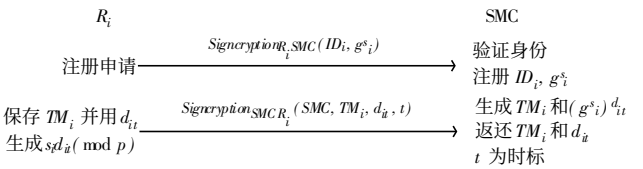

图 3　初始化协议

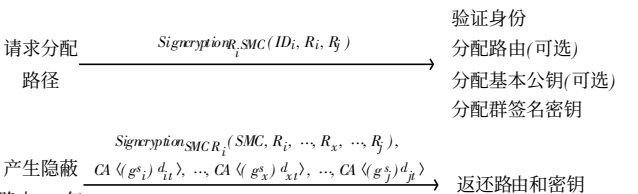

图 4　隐蔽路由分配协议

(3)建立隐蔽路径: R_i 按 R_i 到 R_j 的顺序选取一 R_x,用 2.3 节分段验证签密方法,把 TM_i 和 R_x 后继隐蔽路由器节点地址构成请求 IP 包加密后就得 R_x 分段签密包,然后再把所有的分段签密包连接成一个完整的隐蔽路分配包,把 R_i 的签密公钥证书作为该隐蔽路分配包的公用部分. 当 R_x 接收到隐蔽路分配包后,用自己的群密钥解密其中属于自己的那一段信息,当验证 R_i 的 TM_i 整个隐蔽路分配包有效后,继续把该隐蔽路分配包发送给后续隐蔽路由器 R_{x+1},重复上述过程直至最后的路由器 R_j 就完成了隐蔽路径建立. 建立的洋葱隐蔽路径协议如图 5 所示.

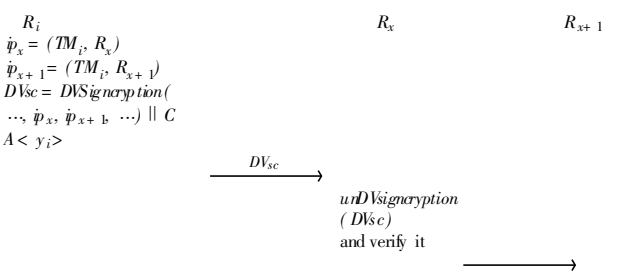

图 5　建立隐蔽路径协议

在上面各协议的实现中,都有一个公开的可识别的标识,并经签密加密认证,使得接收到的 IP 数据包是可识别的又可信赖的. 隐蔽路径建立后,群签密可继续作为 IP 数据包可靠性的加密认证工具,直至数据全部传输完毕. 每个群签密密钥只在一次数据传送中使用,以保证其唯一.

2.5　安全性分析

提出新的隐蔽路由方案的目的在于用完整的分段签密来提高隐蔽路径效率,并同时增强 IP 数据包传输的可靠性,以增强安全网络的抗攻击性. 为此采用了群分段验证签密来提高 IP 数据包传输效率和可信赖度. 签密算法加密函数和 Hash 函数是安全的,并且从签密者的公钥 y_a 得出签密者密钥 x_a 和从签密文 $(c_1, c_2, \ldots, c_n, r_1, r_2, \ldots, r_n, s)$ 中得出解签密文者的私钥 x_{b_i} 等价于求离散对数的难度. 在隐蔽数据传送中,每对隐蔽路由器都能依靠其群签密验证 IP 数据包的可靠性,又不暴露真实身份. 当验证不正确时可以拒绝继续向下传送,而接收数据的目标节点当解密其所收到的信息包后发现仍有问

题时, 还可以通过 SMC 执行公开协议确定出产生问题路段. 由于一次性分配隐蔽路由, 更适合较大的安全网, 可更灵活地动态管理密钥和分配路由.

群签名认证时, SMC 只拥有各路由的公钥, 无法伪造洋葱路由器的签名; 洋葱路由器之间采用群签名的身份认证只证实了它们是一个组织内"群"的成员, 不暴露真实身份, 保持了原路径的隐蔽性; 但新方案的传输却是可靠的. 其抗攻击能力和运行效率都会增高.

3 结论

在公开的计算机网络中隐蔽一个网络结构是困难的. 计算机网中的攻击者所利用的资源会更多, 破解秘密的能力更强, 因此攻击更难防御. 除防范窃听这样的被动攻击外, 同时也要防范攻击者的主动攻击. 本文中所提出的方案包含了高效的认证和加密密封, 并完整地从密码角度解决路由分配包的递送问题, 更符合下一代 IPv6 包的结构, 因为 IPv6 增加了认证和密封功能. IPv4 也可通过扩展功能实现. 因此实现是现实的.

参考文献:

[1] Chaum D. The dining cryptographers problem: unconditional sender and recipient untraceability [J]. Journal of Crptology, 1988, (1): 65- 75.

[2] Brands S. Untraceable off line cash in wallet with observers [A]. Proc. of 13th Annual Inter. Cryptology Conf. (Crypto' 93) [C]. Berlin: Springer-Verlag, 1993. 302- 318.

[3] Reed M, Syverson P, Goldschlag D. Protocols using anonymous connections: mobile applications [A]. Security Protocols, Proc. LNCS Vol 1361 [C]. Berlin: Springer-Verlag, 1998. 13- 23.

[4] Goldschlag D, Reed M, Syverson. Hiding routing information [A]. Arrderson R, ed. Information Hiding, First Inter. Informatina Hiding Workshop Proceedings LNCS Vol 1174 [C]. Berlin: Springer-Verlag, 1996. 137- 150.

[5] Goldschlag D, Reed M, Syverson. Onion routing for anonymous and private Internet conections [J]. Communication of the ACM, 1999, 42 (2): 39- 41.

[6] Seo M, Kim K. Electronic funds transfer protocol using domair-verifrable signcryption scheme [A]. JooSeok Song ed. Information Secunity and Cryptology-ICISC' 99, Proc. LNCS Vol 1787 [C]. Berlin: Springer-Verlag, 2000. 269- 277.

[7] Bao F, Deng R H. A signcryption scheme with signature directly verifrable by public key [A]. Hideki Imai, Yuliang Zheng eds. 1st Inter. Workshop on Practice and Theory in Public Key Cryptography (PKC' 98), Proc. LNCS Vol 1431 [C]. Berlin: Springer-Verlag, 1998. 55- 59.

[8] Gamage C, Leiwo J, Zheng Y. Encrypted message authentication by firewalls [A]. 2nd Inter. Workshop on Practice and Theory in Public Key Cryptography (PKC' 99) Proc. LNCS Vol1560 [C]. Berlin: Springer-Verlag, 1999. 69- 81.

[9] Zheng Y. Digital signcryption or how to achieve cost (signature and encryption) < < cost (signature) + cost (encrytion) [A]. Advances in Cryptology-CRYPTO' 97, Proc. LNCS Vol 1294 [C]. Berllin: Sringer-Verlag, 1997. 165- 179.

[10] Zheng Y. signcryption and its application in efficient public key solutions [A]. Information Security Workshop (ISW' 97), Proc. LNCS Vol 1396 [C]. Berlin: Springer-Verlag, 1998. 291- 312.

[11] von Solms S H, Sgeldenhuys J H. Managing multilevel security in a military intranet environment [J]. Computer&Security, 1999, 18(3): 237 - 270.

[12] von Solms S H Sgeldenhuys J H. Collecting securit baggage on the internet [J]. Computer&Security, 1998, 17(4): 337- 345.

[13] Boshoff W H, von Solms S H. A path context model for addressing security in potentially norr secure environments [J]. Computer&Security, 1989, 8(8): 417- 425.

[14] Westhoff D, Schneider M, Unger C, Kaderali F. Methods for protecting a mobile agent' s route [A]. Mambo M, Zheng Y, eds. Second Inter. Workshop ISW' 99, Proc. LNCS Vol 1729 [C], Berlin: Springer-Verlag 1999. 57- 71.

作者简介:

赵福祥 男, 1964 年 10 月出生于河北省, 西安通信学院讲师, 总参西安创新工作站进站专家, 西安电子科技大学博士研究生, 研究方向: 电子商务和网络安全.

赵红云 女, 1965 年 6 月出生于陕西省西安市, 西安通信学院讲师 西安电子科技大学毕业硕士, 研究方向: 网络管理和管理信息系统.

王育民 男, 1936 年 2 月出生于北京市, 西安电子科技大学教授, 博士生导师, 研究方向: 通信理论, 信息论, 编码和密码学.

杨世平 男, 1953 年 5 月生于湖南, 现为西安通信学院教授, 研究方向: 通信理论, 网络管理和网络安全.