doi:10.11887/j.cn.201806018 http://journal.nudt.edu.cn

携带诱骗信息的多层网络隐写方法*

薛鹏飞,胡劲松,胡荣贵,王友瑞
(国防科技大学 电子对抗学院,安徽 合肥 230037)

摘 要:为了提升网络隐写方法中秘密信息隐蔽传输的安全性,研究了携带诱骗信息的多层网络隐写方法。方法分为两层,高层方法用于携带诱骗信息欺骗检测者,低层方法利用网络协议栈纵向多协议之间的关系编码秘密信息,实现隐蔽通信。实验结果表明,该方法能够在保证隐写带宽的同时,确保了秘密信息传输的安全性。

关键词:信息隐藏;网络隐写;多层隐写;多协议协同
中图分类号:TP399 **文献标志码**:A **文章编号**:1001-2486(2018)06-129-05

Multi-level network steganography carrying decoy message

XUE Pengfei, HU Jingsong, HU Ronggui, WANG Yourui
(College of Electronic Countermeasures, National University of Defense Technology, Hefei 230037, China)

Abstract: In order to improve the security of covert information transmission in network steganography, a decoy method of multi-level steganography based on vertical multi-protocol collaboration was proposed. The proposed method consisted of 2 levels. The upper level was used to carry the decoy message to deceive the detector. The lower level used the vertical relationship of multi-protocol to encode steganogram. Experimental results show that the proposed method is more undetectable than others due to the usage of decoy message and multi-level steganography.

Key words: information hiding; network steganography; multi-level steganography; multi-protocol collaboration

网络隐写是信息隐藏领域新的研究方向[1],它利用公开的网络通信流量作为秘密信息的载体,将秘密信息嵌入通信过程中,并确保对正常通信的影响最小,从而隐藏秘密信息和通信过程。Wendzel等按照隐写模式将网络隐写分为两大类[2]:空域方法和时域方法。空域方法主要通过修改数据包中的特定字段来实现[3-12]。时域方法主要是通过更改数据包之间的相互关系编码秘密信息[13-20]。相比于传统的数字媒体隐写,网络隐写的优势在于难以检测。

Seo认为目前没有一种明确的方法能检测所有的隐蔽信道[21]。但是已经有研究者指出基于单一协议的网络隐写无法提供较强的抗检测性。Zander等[22]和Petitcolas等[23]分别提出了多种网络隐写检测方法。2012年,Mazurczyk等提出了利用流量可视化分析来进行隐写检测的方法steg-tomography[24]。

网络隐写的主要目的是实现秘密信息在网络隐信道中的隐蔽传输,使得除了隐蔽通信的各方知晓隐蔽信道的存在性之外,隐写检测者难以发现或者提取秘密信息。这是设计经典隐写方法的一般性思路。但是在某些特定的应用场景中,隐写方法反而需要有意的暴露。例如,隐蔽通信的双方在明确知道信道中存在隐写检测者的前提下,依然进行隐蔽通信,通过有意地构建并传递虚假的诱骗信息,欺骗检测者,使其误以为所截获的就是秘密信息,从而掩盖真正秘密信息的隐蔽传输,确保秘密信息传输的安全性。

为了提升网络隐写方法中秘密信息隐蔽传输的安全性,本文基于Frączek所提出的多层隐写(Multi-Level Steganography, MLS)[25]的基本思想,提出一种携带诱骗信息的基于纵向多协议协同的MLS方法,其中高层方法携带诱骗信息,用于欺骗检测者;低层方法传输秘密信息,实现隐蔽通信。

* **收稿日期**:2017-10-31
基金项目:国家自然科学基金资助项目(61602491)
作者简介:薛鹏飞(1989—),男,安徽合肥人,博士研究生,E-mail:leorick092182@163.com;
胡荣贵(通信作者),男,教授,博士,博士生导师,E-mail:rghu2000@126.com

1 多层隐写

MLS 最早由 Al-Najjar[26] 提出，应用在图像隐写领域。秘密信息首先被隐藏在一幅诱饵图片的最低有效位（Least Significant Bit，LSB）中，然后再将诱饵图片嵌入载体图片的 LSB，实现了图像的两层隐写，提升了图像隐写的抗检测性。

Sikarwar[27] 提出了基于 MLS 和动态加密技术结合的隐写方法。该方法中，秘密信息被划分为多段，第一段秘密信息经过加密后嵌入载体 1 中。然后载体 1 和第二段秘密信息一起经过加密后嵌入载体 2 中，以此类推，直至所有的秘密信息均被隐藏。假设秘密信息被划分为 N 段，那么载体也需要有 N 个，整个隐写过程经过 N 层加密。

Mazurczyk[28] 指出层次过多的隐写方法存在两点弊端。一是隐写层次的增多会导致算法复杂度的上升；二是过多的隐写层会造成大量的隐写开销，破坏载体的完整性，增加隐蔽通信过程暴露的风险。因此通常的 MLS 均是指两层隐写。

Frączek[25] 在 2011 年首次将 MLS 应用在网络隐写中（如非特别指出，后文的 MLS 均指网络隐写中的 MLS 方法），并将 MLS 归类于深度隐写技术（Deep Hiding Techniques，DHTs）。DHTs[29] 定义了可以用于提高各种网络隐写方法抗检测性的五种一般性的技术。MLS 属于其中的一种，同时采用了至少两种隐写方法，其中一种方法（高层方法）作为另一种方法（低层方法）的载体。2012 年，Frączek 等[30] 进一步提出了两种实用的 MLS 方法，并以音频丢包隐写[31]（Lost Audio paCKets steganography，LACK）为例进行说明。

通过分析可知，MLS 确实能够提升隐写方法的抗检测性，但由于出现得较晚，很多具体的实现技术有待探索和研究。

2 方法描述

MLS 的核心思想是通过增加隐写的层次，提升隐蔽通信的复杂性，从而给试图破坏隐蔽通信的第三方制造困难，设置障碍，提升隐蔽通信的安全性。本文基于 MLS 的思想，受 Al-Najjar 所提出的诱饵图片的启发[26]，提出一种携带诱骗信息的基于纵向多协议协同的 MLS 方法，如图 1 所示。其中高层方法用于携带诱骗信息，低层方法用于传输秘密信息。高层方法以公开流量作为载体，隐写带宽表示为 B_{SU}，影响公开流量所产生的隐写开销表示为 C_{SU}。低层方法以高层方法作为载体，隐写带宽表示为 B_{SL}，影响高层方法所产生的

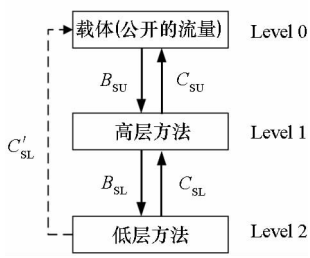

图 1 两层隐写方法

Fig. 1 Two level MLS

隐写开销表示为 C_{SL}，间接地对公开流量产生的隐写开销为 C'_{SL}，通常 $C'_{SL}\approx 0$。那么 MLS 方法的总隐写带宽 B_S 为：

$$B_S = B_{SU} + B_{SL} \tag{1}$$

总隐写开销 C_S 为：

$$C_S = C_{SU} + C_{SL} + C'_{SL}, C'_{SL}\approx 0 \tag{2}$$

隐写带宽用来衡量秘密信息的传输速率，隐写带宽越高，秘密信息传递得越快。隐写开销用来衡量由于采用隐写方法所导致的载体退化或者变形的程度，隐写开销越大，隐写带宽越高，但同时载体退化得越明显，被检测出的风险也越高。下面分别从高层方法和低层方法两个层次对该方法进行具体描述。

2.1 高层方法

在正常的网络公开信道中，位于传输层的 TCP/UDP 协议和位于网络层的 IP 协议都是常见的通信协议。选择这几种协议作为载体，不会引起网络流量类型异常，也不会引起检测者的怀疑，且能够在一定程度上降低隐蔽信道暴露的可能性。

高层方法利用这几种协议隐藏诱骗信息。假设单个 TCP 或 UDP 数据包可以隐藏的数据容量为 V_T，单个 IP 数据包首部可以隐藏的数据容量为 V_I。在一般的网络隐写方法中，为避免引起检测者的怀疑，V_T 和 V_I 不应过大。在本文中，虽然 V_T 和 V_I 被用于隐藏诱骗信息，但是为了保证隐蔽通信的安全性，设定 $V_T = 2$ bit，$V_I = 1$ bit。假设诱骗信息的大小为 V_D，一般的 $V_D > V_T + V_I$，需要将诱骗信息分成 n 段（$D_1, D_2, D_3, \cdots, D_n$），如图 2 所示。

分段数目 n 按照式（3）进行计算。

$$n = \begin{cases} 2\times\lfloor V_D/(V_T+V_I)\rfloor + 1, 0 \leqslant V_D \bmod (V_T+V_I) \leqslant V_T \\ 2\times\lfloor V_D/(V_T+V_I)\rfloor + 2, V_T < V_D \bmod (V_T+V_I) \leqslant V_T+V_I \end{cases} \tag{3}$$

对于每一个诱骗信息分段 D_i（$i = 1, 2, 3, \cdots, n$），当 i 为奇数时，将 D_i 隐藏在 TCP 或者 UDP 数

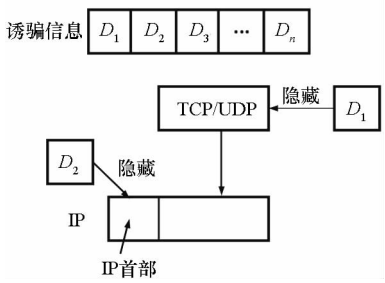

图 2　高层方法隐藏诱骗信息

Fig. 2　Decoy embedding of the upper level method

据包中(选择何种传输层数据包隐藏 D_i 需要根据秘密信息确定,选择方法在下一节算法 1 中具体描述),将 D_{i+1} 隐藏在 IP 数据包的首部。由于篇幅有限,关于数据如何嵌入某种协议类型的数据包不是本文研究的重点,详细了解请参考文献[3 - 12]中描述的网络隐写空域方法。

2.2　低层方法

网络协议栈中的上层协议数据包作为下层协议的数据单元。例如,TCP/UDP 协议数据包作为 IP 协议的数据单元。这种协议之间纵向的相互关系是由开放系统互联网(Open System Interconnection, OSI)参考模型所定义的。利用协议栈不同层协议之间的纵向关系,实现 MLS 的低层方法。假设以 UDP 数据包为数据单元的 IP 数据包表示 0,以 TCP 数据包为数据单元的 IP 数据包表示 1(如图 3 所示)。这种方法可以用来编码需要隐蔽传输的秘密信息。

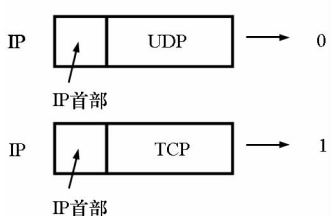

图 3　编码秘密信息

Fig. 3　Encoding real steganogram

假设有两台主机进行隐蔽通信,CS 表示隐蔽发送方,CR 表示隐蔽接收方。通信过程如图 4 所示。

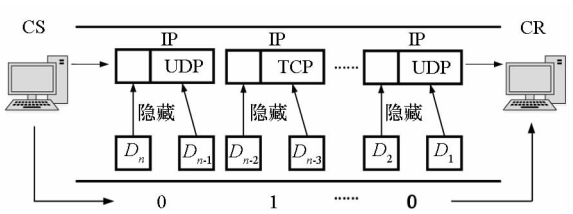

图 4　隐蔽传输

Fig. 4　Covert transmission

利用 MLS 的思想实现其隐蔽传输的过程如算法 1 所示。

算法 1　携带诱骗信息的多层网络隐写方法

Alg. 1　Multi-level network steganograpy carrying decoy message (MLS-DM)

输入:诱骗信息 D, 秘密信息 S
输出:提取的秘密信息 S'

1. 将 S 转换为二进制表示
2. **if** 第 k 个二进制位是 0
3. 　将诱骗信息分段 D_{2k-1} 隐藏在 UDP 数据包
4. 　将诱骗信息分段 D_{2k} 隐藏在 IP 数据包首部
5. **else if** 第 k 个二进制位如果是 1
6. 　将诱骗信息分段 D_{2k-1} 隐藏在 TCP 数据包
7. 　将诱骗信息分段 D_{2k} 隐藏 IP 数据包首部
8. **end if**
9. 发送方 CS 依次将 IP 数据包发送至接收方 CR
10. **if** IP 包内封装的是 UDP 数据包
11. 　提取秘密信息位 0
12. **else if** IP 包内封装的是 UDP 数据包
13. 　提取秘密信息位 1
14. **end if**
15. 将秘密信息位按序重组得到秘密信息 S'

3　实验结果与分析

由于 B_{SU} 用于传递诱骗信息,对于秘密信息而言 $B_{SU}=0$,因此隐写带宽 $B_S=B_{SL}$。由于低层方法只是利用高层方法协议之间的关系编码秘密信息,并未改变协议的结构,因此 $C_{SL}=0$,总隐写开销 $C_S=C_{SU}$。C_{SU} 按照式(4)计算。

$$C_S=C_{SU}=\frac{V_T+V_I}{\overline{size_P}}\times 100\% \tag{4}$$

其中,V_T 是每个 TCP 或者 UDP 数据包中隐藏的诱骗信息大小,V_I 是每个 IP 数据包中隐藏的诱骗信息大小。$\overline{size_P}$ 表示已发送的 IP 数据包大小的平均值。在 $\overline{size_P}$ 一定的情况下,随着 V_T 和 V_I 的增长,C_S 会逐渐增大。如图 5 所示,每种方法的隐写开销有一个阈值 TC_S。当 $C_S<TC_S$ 时,隐写方法具有一定的抗检测性;当 $C_S>TC_S$ 直至 $C_S=100\%$ 时,隐写方法被检测出的可能性为 100%。

另外,由于 $C_{SL}=0$,而 $B_S=B_{SL}$,因此 C_S 的增大并不会导致 B_S 的提高。所以增加 V_T 和 V_I 并不能够提升隐写带宽,反而会提升隐蔽信道被检测的风险。

在理想的网络环境下(网络无拥塞,无丢

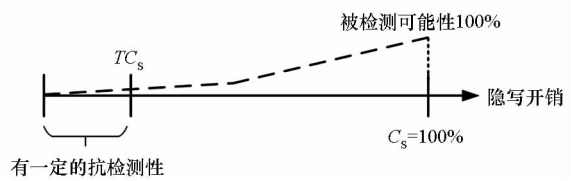

图5 隐写开销和抗检测性的关系[28]

Fig. 5 Relationship between steganographic cost and undetectability[28]

包),设定 $V_T = 2$ bit 和 $V_I = 1$ bit。通过多次实验,$\overline{Size}_P$ 为 1000 Byte,则 $C_S = 0.037\,5\%$,B_S 达到 1 bit/包。隐写带宽结果和 Kundur、EI-Atawy 等的方法比较如图 6 所示。Kundur 提出了基于数据包重排序编码秘密信息的隐写方法[32],是网络隐写领域的经典方法,其隐写带宽为 1 bit/包。EI-Atawy 提出了基于数据包排序的另外一种隐蔽信道[33],利用乱序的数据包表示某种信息,这种表示方式不依赖于数据包负载,对于包间延时抖动也不敏感,其隐写带宽为0.5 bit/包。这两种方法均是网络隐写方法中典型的时域方法。和空域方法相比,时域方法的优势在于具有较强的抗检测性。本文提出的 MLS-DM 方法中用于传递秘密信息的低层方法利用了协议之间的关系编码秘密信息,也属于时域方法。

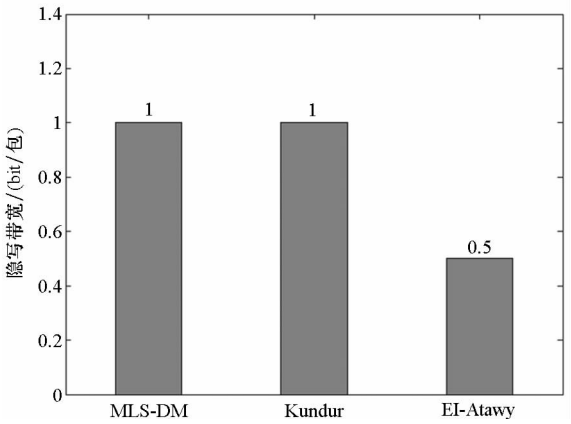

图6 隐写带宽比较

Fig. 6 Bandwidth comparison

从图 6 中可以看出,MLS-DM 的隐写带宽高于 EI-Atawy 的方法,但与 Kundur 的方法基本一样。但是由于 Kundur 的方法只是利用数据包的重排序产生不同的排列来编码秘密信息,一旦隐蔽信道被发现,秘密信息就会泄露。而 MLS-DM 采用了多层隐写方法,即使高层方法被发现,检测者也只会获得诱骗信息,难以发现低层方法所隐藏的秘密信息,不会导致秘密信息泄露,能够在一定程度上保证秘密信息隐蔽传输的安全性。

Kundur 和 EI-Atawy 的方法并未对隐写开销进行计算和说明。研究者们一般认为一旦隐写开销超过 50%,隐蔽信道将面临被检测出的较大风险。而本文 MLS-DM 方法的隐写开销为 0.037 5%,远低于 50%,这说明其抗检测性较强。

4 结论

MLS 是网络隐写新的发展方向,本文利用 MLS 的思想,设计了基于两层隐写的网络隐写方法。其中高层方法利用公开的网络流量中的 TCP、UDP 以及 IP 数据包作为载体隐藏诱骗信息,用于欺骗可能存在的检测者,并掩盖低层方法所传递的秘密信息的存在性。低层方法利用高层方法中协议之间的纵向关系隐藏并传输秘密信息,实现隐蔽通信。实验结果表明,本文所提方法能够保证较高的隐写带宽,能够提升秘密信息隐蔽传输的安全性。

参考文献(References)

[1] Szczypiorski K. Steganography in TCP/IP networks[C]// Proceedings of State of the Art and a Proposal of a New System-HICCUPS, Institute of Telecommunications' Seminar, 2003.

[2] Wendzel S, Zander S, Fechner B, et al. Pattern-based survey and categorization of network covert channel techniques[J]. ACM Computing Surveys, 2015, 47(3): 50.

[3] Girling C G. Covert channels in LAN's[J]. IEEE Transactions on Software Engineering, 1987, SE-13(2): 292-296.

[4] Murdoch S J, Lewis S. Embedding covert channels into TCP/IP[C]//Proceedings of the Information Hiding Conference, 2005.

[5] Trabelsi Z, Jawhar I. Covert file transfer protocol based on the IP record route option[J]. Journal of Information Assurance and Security, 2010, 5(1): 64-73.

[6] Graf T. Messaging over IPv6 destination options[EB/OL]. [2017-07-25]. http://net.suug.ch/articles/2003/07/06/ip6msg.html.

[7] Wendzel S, Kahler B, Rist T. Covert channels and their prevention in building automation protocols: a prototype exemplified using BACnet[C]//Proceedings of the 2nd Workshop on Security of Systems and Software Resiliency, 2012.

[8] Lucena N, Lewandowski G, Chapin S. Covert channels in IPv6[C]//Proceedings of the 5th International Workshop on Privacy Enhancing Technologies, 2006.

[9] Zander S, Armitage G, Branch P. Covert channels in the IP time to live field[C]//Proceedings of Australian Telecommunication Networks and Applications Conference, 2006.

[10] Giffin J, Greenstadt R, Litwack P, et al. Covert messaging through TCP timestamps[C]//Proceedings of the 2nd International Conference on Privacy Enhancing Technologies, 2003.

[11] Handel T G, Sandford M. Hiding data in the OSI network model[C]//Proceedings of the First International Workshop

on Information Hiding, 1996.

[12] Wendzel S. Protocol channels as a new design alternative of covert channels[EB/OL]. [2017 - 07 - 25]. CoRR, arXiv: 0809.1949, http://cds.cern.ch/record/1126596.

[13] Yao L H, Zi X C, Pan L, et al. A study of on/off timing channel based on packet delay distribution[J]. Computers & Security, 2009, 28(8): 785 - 794.

[14] Cabuk S, Brodley C E, Shields C. IP covert timing channels: design and detection [C]//Proceedings of the 11th ACM Conference on Computer and Communications Security, 2004.

[15] Padlipsky M A, Snow D W, Karger P A. Limitations of end-to-end encryption in secure computer networks: MTR - 3592 - VOL - 1[R]. MITRE Corporation, 1978.

[16] Li W Q, He G L. Towards a protocol for autonomic covert communication [C]//Proceedings of the 8th International Conference on Autonomic and Trusted Computing, 2011.

[17] Sellke S H, Wang C C, Bagchi S, et al. Covert TCP/IP timing channels: theory to implementation[C]//Proceedings of the 28th Conference on Computer Communications, 2009.

[18] Gianvecchio S, Wang H N. Detecting covert timing channels: an entropy-based approach [C]//Proceedings of the 14th ACM Conference on Computer and Communication Security, 2007.

[19] Berk V, Giani A, Cybenko G. Detection of covert channel encoding in network packet delays: TR536 [R]. USA: Department of Computer Science, Dartmouth College, 2005.

[20] Gianvecchio S, Wang H N, Wijesekera D, et al. Model-based covert timing channels: automated modeling and evasion [C]//Proceedings of International Workshop on Recent Advances in Intrusion Detection, 2008.

[21] Seo J O, Manoharan S, Mahanti A. A discussion and review of network steganography [C]//Proceedings of 14th Intl. Conf. on Pervasive Intelligence and Computing, 2nd Intl. Conf. on Big Data Intelligence and Computing and Cyber Science and Technology Congress, 2016.

[22] Zander S, Armitage G, Branch P. A survey of covert channels and countermeasures in computer network protocols[J]. IEEE Communications Surveys & Tutorials, 2007, 9(3): 44 - 57.

[23] Petitcolas F A, Anderson R, Kuhn M. Information hiding—a survey[J]. Proceedings of the IEEE, 1999, 87(7): 1062 - 1078.

[24] Mazurczyk W, Szczypiorski K, Jankowski B. Towards steganography detection through network traffic visualisation[C]// Proceedings of 4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, 2012: 947 - 954.

[25] Frączek W, Mazurczyk W, Szczypiorski K. Multi-level steganography applied to networks[C]//Proceedings of Third International Workshop on Network Steganography, the International Conference on Telecommunication Systems, Modeling and Analysis, 2011: 27 - 28.

[26] Al-Najjar A J. The decoy: multi-level digital multimedia steganography model [C]//Proceedings of 12th WSEAS International Conference on Communications, 2008.

[27] Sikarwar N S. An integrated synchronized protocol for secure information transmission derived from multilevel steganography and dynamic cryptography [J]. International Journal of Computer Science and Telecommunication, 2012, 3(4): 31 - 36.

[28] Mazurczyk W, Wendzel S, Villares I A, et al. On importance of steganographic cost for network steganography [J]. International Journal of Security and Communication Networks, 2016, 9: 781 - 790.

[29] Frączek W, Mazurczyk W, Szczypiorski K. How hidden can be even more hidden? [C]//Proceedings of 3rd International Conference on Multimedia Information Networking and Security, 2011: 581 - 585.

[30] Frączek W, Mazurczyk W, Szczypiorski K. Multi-level steganography: improving hidden communication in networks[J]. Journal of Universal Computer Science, 2012, 18(14): 1967 - 1986.

[31] Mazurczyk W, Lubacz J. LACK: a VoIP steganographic method[J]. Telecommunication Systems, 2010, 45(2/3): 153 - 163.

[32] Ahsan K, Kundur D. Practical data hiding in TCP/IP[C]// Proceedings of the ACM Workshop on Multimedia Security, 2002.

[33] El-Atawy A, Al-Shaer E. Building covert channels over the packet reordering phenomenon[C]//Proceedings of the 28th Annual IEEE Conference on Computer Communications, 2009.