

基于移动切换认证的分层异构网络中的用户敏感信息隐藏方法

张建安

(解放军信息工程大学三院昆明大队 昆明 650231)

摘 要 为了保证用户敏感信息的安全性,需要对用户敏感信息进行隐藏传输。采用已有方法对分层异构网络中的用户敏感信息进行隐藏时,所得信息的完整性和安全性较低。鉴于此,提出一种基于移动切换认证的分层异构网络中的用户敏感信息隐藏方法。该方法采用嵌入单元置乱算法对用户的敏感信息进行置乱,打乱用户敏感信息在分层异构网络中的正常排序序列;根据字符亮度编码机制并结合 HSI 模型,在打乱的用户敏感信息排序序列内得到最优的用户敏感信息嵌入位置;采用载体操纵法对分层异构网络中用户敏感信息的嵌入单元集合进行分析,根据分析结果将用户的敏感信息嵌入到最优嵌入位置中,完成分层异构网络中用户敏感信息的隐藏。实验结果表明,所提方法得到的信息的完整性和安全性均较高。

关键词 移动切换认证,分层异构网络,用户信息,敏感信息隐藏

中图法分类号 TP309 文献标识码 A DOI 10.11896/j.issn.1002-137X.2019.03.032

Users' Sensitive Information Hiding Method in Hierarchical Heterogeneous Network Based on Mobile Switching Authentication

ZHANG Jian-an

(Kunming Branch, No. 3 College, PLA Information Engineering University, Kunming 650231, China)

Abstract In order to ensure the security of users' sensitive information, it's essential to transmit the users' sensitive information in a covert manner. When the current method is used to hide the users' sensitive information in the hierarchical heterogeneous network, the obtained information has low integrity and low information security. This paper proposed a users' sensitive information hiding method in hierarchical heterogeneous networks based on mobile switching authentication. It uses the embedded unit scrambling algorithm to scramble the sensitive information of users and disrupts the normal ordering of users' sensitive information in hierarchical heterogeneous networks. Then, combined with the HSI model, the optimal users' sensitive information embedding position is obtained within the scrambled users' sensitive information sorting sequence according to the character brightness encoding mechanism. And the vector-based manipulation method is used to set the embedding unit of users' sensitive information in the hierarchical heterogeneous network. According to the analysis results, users' sensitive information is embedded in the optimal embedding position, and the users' sensitive information hiding in the hierarchical heterogeneous network is completed. The experimental results show that the information obtained by the proposed method has high integrity and security.

Keywords Mobile switching authentication, Layered heterogeneous network, User information, Sensitive information hiding

1 引言

移动互联网行业的不断推动和发展促进了移动终端市场数量和种类的增长。当今社会已有多种不同的网络,在未来的发展中也会出现更加优秀的终端产品,因此需要不同接入技术的通信支撑终端产品的发展^[1]。在目前的无线通信领域中,有全球通用微波接入系统、全球移动通信系统、无线局域网、通用移动通信系统和码分多址接入系统等^[2]。未来网络发展的重要领域之一是不同类型的网络通信制式之间的切换技术。为了保证网络传输的安全性,通常需要对传输的数

据进行加密,但随着计算机运算能力和加密算法破解技术的不断提升,加密技术被破解的概率不断增大^[3]。

信息隐藏技术是指在正常的文件数据中加入需要隐藏的信息,尽可能地不起引起监控者和观察者的注意,从而完成隐蔽传输^[4]。网络中存在大量的数据和协议,在这些数据和协议中,很容易找出供数据隐藏传输的隐蔽信道,也可以利用设备和终端通过隐蔽信道进行隐秘信息的传输。采用当前的信息隐藏方法进行敏感信息的隐蔽传输时,存在信息完整性和安全性低的问题,因此需要对敏感信息隐藏方法进行深入的分析和研究^[5]。

李松斌等^[6]提出了一种基于运动矢量空间编码的敏感信息隐藏方法,该方法通过信息运动矢量空间的编码及构建方法描述了空间中点与信息运动矢量集合的映射关系,通过信息运动矢量结合的映射值完成敏感信息的隐藏。该方法得到的用户敏感信息的完整性较低。Lin 等^[7]提出了一种基于差值直方图的敏感信息隐藏方法,该方法对原始信息进行扫描、分块,通过计算得到原始信息差值的直方图,并对其进行分块处理,从图中选取两个峰值,根据峰值得到嵌入信息的空缺,完成敏感信息的隐藏。该方法对信息隐藏的安全性较低。高斌等^[8]提出了一种基于 BitTorrent 协议的敏感信息隐藏方法,该方法通过设置容量分析模块,对敏感信息的嵌入量是否高于隐藏容量的上限进行判断;在正常信息的排序中通过映射信息编码的方法嵌入需要隐藏的信息,完成敏感信息的隐藏。该方法得到的信息的完整性较低。

为解决上述方法中存在的问题,本文提出一种基于移动切换认证的分层异构网络中的用户敏感信息隐藏方法,对用户敏感信息进行置乱处理,寻找敏感信息的嵌入位置,在最优嵌入位置完成敏感信息的隐藏。

2 基于移动切换认证的分层异构网络

移动分层异构网络切换是移动通信系统中较为重要的关键特征,是移动性的管理功能,在个人通信业务中具有巨大作用,对整个移动系统的性能有很大影响^[9]。切换发起阶段、判决阶段和执行阶段是分层异构网络中的主要切换步骤。

分层异构网络的内部切换技术是在一个范围内完成的,网络的选择根据站点观测到的网络参数完成^[10]。完成网络的选择后,接入网站进行切换。分层异构网络移动切换的具体过程如下:

- 1) 分层异构网络的终端探测到新的移动切换目标接入点,对当前接入的点进行切换连接,将重连接请求信号传送到目标的接入点中;
- 2) 在终端与目标接入点之间进行连接,将进行切换的通知发送到当前连接的接入点,并对二层路由进行更新;
- 3) 分层异构网络中的移动切换接入点接收到切换信号后,将移动终端的认证信息传送到目标接入点中,同时删除本机上的信息;
- 4) 接收到终端相关信息的目标接入点对相关信息进行存储,完成与终端用户的连接。

分层异构网络的移动切换构架如图 1 所示。

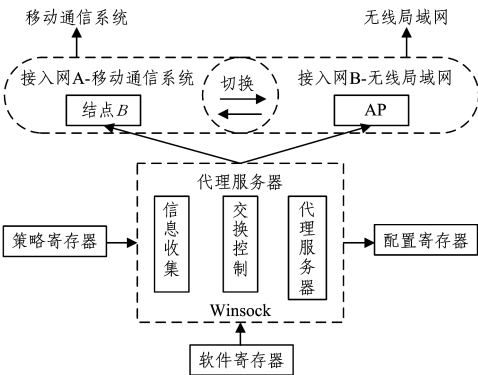


图 1 分层异构网络的移动切换构架

Fig. 1 Mobile switching architecture of layered heterogeneous network

在分层异构网络移动切换构架中,代理服务器统计吞吐量和网络负载情况^[11]。每隔一段时间无线局域网和移动通信系统基站都会上报资源使用率和网络负载情况等参数^[12]。移动网络终端的接入设备从代理服务器中获取网络情况。在执行分层异构网络中的移动切换时,终端先将含有当前接入点信息的请求数据、需要速率和业务种类发送到代理服务器中,代理服务器接收到请求信息后,将接收到的请求信息发送到新接入点^[13]。接入点将确认字符的响应包传送给服务器,在终端中留下准备接收连接的资源,并向终端传送一个确认字符包。终端接收确认字符包后,向新接入点发起切换连接。新的连接建立完成后,断开终端与旧接入点的连接,完成分层异构网络中的移动切换^[14-16]。

3 敏感信息隐藏方法

采用基于移动切换认证的分层异构网络中的用户敏感信息隐藏方法对用户的敏感信息进行隐藏时,首先通过嵌入单元置乱算法将用户敏感信息的排序序列打乱,然后根据字符亮度的编码机制找到用户敏感信息的最优嵌入位置,最后通过载体操纵法完成用户敏感信息的嵌入。

3.1 嵌入单元置乱算法

设 S 代表分层异构网络中用户敏感信息的抽象嵌入单元集合。 S_i 代表嵌入单元, seq 代表嵌入单元 S_i 的位置信息, sn 代表嵌入单元经置乱处理后的顺序。每个 S_i 中都会储存用户敏感信息在 S_i 中的 seq 和 sn 。 X 代表第 i 个用户敏感信息嵌入单元 S_i 的同义集合,该集合的密钥记作 K 。

hash 函数根据密钥 K 在同义集合中选择代表元素,以保证嵌入单元经过同义替换后仍然可以正确排列。设 $r = Random(K)$ 代表伪随机数,根据密钥 K 决定随机函数的种子。在集合 X 中,下标为 r 的代表元素记作 $w = X_r$ 。 $res[]$ 代表字节数组,用来储存代表元素的哈希值。

分层异构网络中用户敏感信息的排序序号通过代表元素的哈希值数组 $res[]$ 得到。 $y[n]$ 代表分层异构网络中的数组,用来存储生成的用户敏感信息排序序号。通过式(1)和式(2)计算用户敏感信息的代表元素的排序序号:

f(j)=res[j]⋅pow(255,j) (1)

y[i]=∑j=03f(j)+Si,seq⋅pow(255,4)+∑j=57f(j) (2)

其中, $pow(x, y)$ 为函数对 x 的 y 次幂进行计算, $f(j)$ 代表分层异构网络中用户敏感信息的代表元素排序序号。

$z[]$ 代表排序后的用户敏感信息数组,通过式(3)对用户敏感信息的数组 $y[]$ 进行排序得到。 $z[]$ 的计算公式为:

z[]=sort y[] (3)

其中, $sort$ 代表排序命令。

3.2 基于字符亮度的编码机制

通过 HSI 模型对分层异构网络中用户敏感信息的色彩进行描述,其中, H 代表用户敏感信息的色调, S 代表用户敏感信息的饱和度, I 代表用户敏感信息的亮度。 H, S, I 的表达式为:

H=⎧⎩θ360−θ (4)

$$S=1-3/(R+G+B)\min(R,G,B)$$
 (5)

$$I=1/3(R+G+B)$$
 (6)

其中, R,G,B 代表三原色, θ 代表色调参数。通过式(6)对分层异构网络中用户敏感信息中的字符亮度进行计算,并对字符的亮度进行调整,调整的字符亮度记为 d ,其计算公式为:

$$d=1/3(\Delta R+\Delta G+\Delta B)$$
 (7)

设 I' 代表调整后的用户敏感信息字符的亮度, $[I-d,I+d]$ 为字符亮度的区间, W 代表嵌入隐藏用户敏感信息的位置, W 的计算公式为:

$$W=\begin{cases} 0, & I'\in[I-d,I] \\ 1, & I'\in[I,I+d] \end{cases}$$
 (8)

3.3 用户敏感信息嵌入算法

设 M' 代表二进制比特串,将需要隐藏的用户敏感信息转换为 M' 。通过载体操纵法对原始用户敏感信息文本 C 中的信息嵌入单元集合 S 进行分析:

$$S=\{S_0,S_1,\cdots,S_{n-1}\}$$
 (9)

设 T_i 代表嵌入单元集合 S 的同义集合。 T_i 通过载体操纵算法对分析得到的嵌入单元 S 进行变换,得到:

$$Transform(S)\rightarrow T_i$$
 (10)

其中, $Transform()$ 代表预变换操作。分层异构网络中嵌入单元 S_i 对应的嵌入敏感信息比特串 M' 中的第 P_i 位,通过密钥 K 计算得到:

$$P_i=Mapping(S_i,K)$$
 (11)

其中, $Mapping$ 为计算比特串的函数。将用户敏感信息嵌入到由 3.2 节计算得到的隐藏用户敏感信息的最优位置,得到含有密文的用户信息 T' ,完成分层异构网络中用户敏感信息的隐藏。

$$T'=Output(S_i)\cdot WP_i$$
 (12)

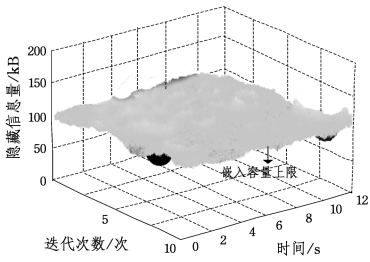
其中, $Output(S_i)$ 代表用户敏感信息的嵌入。

4 实验证明

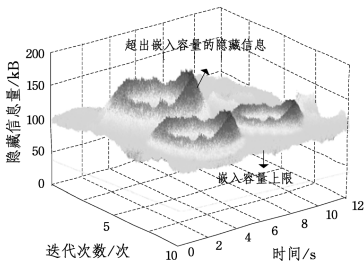
为了验证基于移动切换认证的分层异构网络中的用户敏感信息隐藏方法的有效性,本节进行实验分析。本次实验的操作系统为 Windows,实验环境为 Visual Studio。在用户信息隐藏中,嵌入容量是决定用户信息的完整性的基础。当隐藏的信息大于嵌入容量时,得到的用户信息的完整性较低;当隐藏的信息小于嵌入容量时,得到的用户信息完整性较高。分别采用基于移动切换认证的分层异构网络中的用户敏感信息隐藏方法(方法 1)、基于运动矢量空间编码的敏感信息隐藏方法(方法 2)、基于差值直方图的敏感信息隐藏方法(方法 3)进行测试,对比 3 种不同方法得到的隐藏信息的完整性,测试结果如图 2 所示。

图 2(a)为基于移动切换认证的分层异构网络中的用户敏感信息隐藏方法的测试结果。分析图 2(a)可知,采用本文方法对用户敏感信息进行隐藏时,隐藏的信息量没有超过嵌入容量的上限。图 2(b)为基于运动矢量空间编码的敏感信息隐藏方法的测试结果,图 2(c)为基于差值直方图的敏感信息隐藏方法的测试结果。分析图 2(b)和图 2(c)可知,采用这两种方法对用户敏感信息进行隐藏时,隐藏的信息量超过了嵌入容量的上限。当隐藏的信息大于嵌入容量时,得到的用

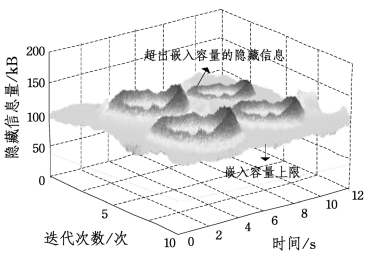
户信息的完整性较低;当隐藏的信息小于嵌入容量时,得到的用户信息的完整性较高。因此,基于移动切换认证的分层异构网络中用户敏感信息隐藏方法得到的信息的完整性较高。



(a) 方法 1 的测试结果



(b) 方法 2 的测试结果



(c) 方法 3 的测试结果

图 2 3 种不同方法隐藏信息量的测试结果

Fig. 2 Test results of hidden information of three different methods

利用 P_i 表示嵌入敏感信息比特串 M' 中的具体位置。当 P_i 排在前三位时,隐藏的用户敏感信息的安全性较高。分别采用方法 1、方法 2、方法 3 进行测试,对比 3 种不同方法的信息安全性,测试结果如表 1 所列。

表 1 3 种不同方法信息安全性的测试结果

Table 1 Test results of information security of three different methods

迭代次数	参数 P_i 的位置		
	方法 1	方法 2	方法 3
1	第 1 位	第 3 位	第 4 位
2	第 2 位	第 4 位	第 4 位
3	第 2 位	第 4 位	第 3 位
4	第 3 位	第 5 位	第 5 位
5	第 2 位	第 2 位	第 4 位

分析表 1 中的数据可知,采用方法 1 进行测试时,得到的参数 P_i 的位置分别为第 1 位、第 2 位、第 2 位、第 3 位、第 2 位,参数 P_i 在前 3 位的概率为 100%;采用方法 2 进行测试时,得到的参数 P_i 的位置分别为第 3 位、第 4 位、第 4 位、第 5 位、第 2 位,参数 P_i 在前 3 位的概率为 40%;采用方法 3 进行测试时,得到的参数 P_i 的位置分别为第 4 位、第 4 位、第 3 位、第 5 位、第 4 位,参数 P_i 在前 3 位的概率为 20%。已知当 P_i 在前 3 位时,隐藏的用户敏感信息的安全性较高,因此基

于移动切换认证的分层异构网络中用户敏感信息隐藏方法的安全性较高。

结束语 信息隐藏方法是用户完成信息隐蔽传送的基础,当前用户敏感信息隐藏方法存在信息完整性和安全性低的问题。本文提出了一种基于移动切换认证的分层异构网络中的用户敏感信息隐藏方法,该方法解决了当前方法中存在的问题。未来将从以下几个方面对信息隐藏方法进行进一步研究。

- 1)总结和研 究语法变换的方式,以及句式变换方法。
- 2)设计相应的句法变换载体操作方法和同义词载体操作方法。
- 3)对嵌入位置的确定方法进行深入研究。

参 考 文 献

[1] WU M T,ZHAN J,LIN C W. Ant Colony System Sanitization Approach to Hiding Sensitive Itemsets[J]. IEEE Access,2017, PP(99):1

[2] XIANG L,PENG J X,ZHANG L. Network Clustering Algorithm Based on Energy Time Competition Mechanism in Heterogeneous Network Environment[J]. Bulletin of Science and Technology,2017,33(8):185-188. (in Chinese)

向岚,彭进香,张莉. 异构网络环境中基于能量时间竞争机制的网络分簇算法研究[J]. 科技通报,2017,33(8):185-188.

[3] LUO C,FYLA KIS A,PARTALA J,et al. A data hiding approach for sensitive smartphone data[C]// ACM International Joint Conference on Pervasive and Ubiquitous Computing. ACM,2016:557-568.

[4] ZHANG X,ZHANG Y,JIN C F,et al. A Dynamic Almost Blank Subframes Allocation for Interference Coordination in Heterogeneous Networks[J]. Computer Measurement & Control,2016,24(7):215-218. (in Chinese)

张新,张艳,金春风,等. 异构网络动态配置空白子帧干扰协调算法[J]. 计算机测量与控制,2016,24(7):215-218.

[5] SHARMA S,TOSHNIWAL D. Scalable two-phase co-occurring sensitive pattern hiding using MapReduce[J]. Journal of Big Data,2017,4(1):4-14.

[6] LI S B,WANG L R,LIU P,et al. A HEVC Information Hiding Approach Based on Motion Vection Space Encoding[J]. Chinese Journal of Computers,2016,39(7):1450-1463. (in Chinese)

李松斌,王凌睿,刘鹏,等. 一种基于运动矢量空间编码的 HEVC 信息隐藏方法[J]. 计算机学报,2016,39(7):1450-1463.

[7] LIN C W,LIU Q,FOURNIER-VIGER P,et al. A sanitization approach for hiding sensitive itemsets based on particle swarm optimization[J]. Engineering Applications of Artificial Intelligence,2016,53(C):1-18.

[8] GAO B,ZHAI J T,DAI Y W. Information hiding method based

on Have messages in BitTorrent protocol[J]. Journal of Computer Applications,2017,37(1):200-205. (in Chinese)

高斌,翟江涛,戴跃伟. 基于 BitTorrent 协议 Have 消息的信息隐藏方法[J]. 计算机应用,2017,37(1):200-205.

[9] KHEDEKAR L S. Security:An effective technique to protecting sensitive information using quick response code[C]// International Conference on Communication and Signal Processing. IEEE,2016:1185-1188.

[10] PENG Y B,XIE X T. The adaptive Web information extraction based on single DOM tree characteristics and classification[J]. Electronic Design Engineering,2017,25(19):56-59. (in Chinese)

彭艳兵,谢馨庭. 基于单 DOM 树特征预分类的自适应 Web 信息抽取方法[J]. 电子设计工程,2017,25(19):56-59.

[11] YANG M J,SHAO D,LIU K Y. Vertical handoff for heterogeneous wireless network based on mobile terminal priority[J]. Journal of Dalian Polytechnic University,2018,20(1):73-78. (in Chinese)

杨明极,邵丹,刘恺悌. 移动终端在异构无线网络中的接入方法[J]. 大连工业大学学报,2018,20(1):73-78.

[12] FEI H H. Research on Optimal Detection Method of User Information Resources In Network[J]. Computer Simulation,2017(12):318-320. (in Chinese)

费宏慧. 导构网络中用户信息资源优化检测方法研究[J]. 计算机仿真,2017(12):318-320.

[13] Innowireless Co. L. Method of switching connection to femtocell and wifi ap in sdn[J]. New Patents & Technology,2016,21(3):12.

[14] MA B,DENG H,XIE X Z. Two-sided Matching Model Based Vertical Handover Algorithm in Heterogeneous Wireless Networks[J]. Journal of Electronics & Information Technology,2018,40(2):421-429. (in Chinese)

马彬,邓红,谢显中. 基于双向匹配模型的异构网络垂直切换算法[J]. 电子与信息学报,2018,40(2):421-429.

[15] LI X W,WANG X J,TIAN F X,et al. Analysis and Implementation of Handover Process of Dual Connectivity Technology based on Heterogeneous Networks[J]. Study on Optical Communications,2017,43(2):68-70. (in Chinese)

李小文,王晓娟,田凤仙,等. 基于异构网双连接技术切换流程的分析与实现[J]. 光通信研究,2017,43(2):68-70.

[16] WU W G,ZHANG Z W,WANG Q S. A Information Security Risk Assesment Model Based on AHP and Fuzzy Comprehensive Evaluation[J]. Journal of Chongqing University of Technology(Natural Science),2017,31(7):162-167. (in Chinese)

吴文刚,张志文,王庆生. 基于模糊综合评判和 AHP 信息安全风险评估模型[J]. 重庆理工大学学报(自然科学),2017,31(7):162-167.