基于空域技术的无线通信物理层信息安全技术研究

吴伊蒙[1] 石志东[1] 房卫东[1,2*] 邓 斌[1] 单联海[2,3]

[1](上海大学通信与信息工程学院 上海 201800)

[2](中科院上海微系统与信息技术研究所 上海 200050)

[3](上海物联网有限公司 上海 201899)

摘 要 无线网络通信非常容易受到窃听、拥塞和干扰等攻击,而从物理层层面上来抵御这些攻击能够有效减轻上层网络的压力。从无线通信网络的隐患开始,调研无线通信网络的常见攻击及基于空域的相应安全技术的技术要点,并对这些方法进行比较总结和技术分类,同时对其安全性能进行分析,为后续的研究与应用提供帮助。

关键词 无线通信 物理层安全 空域技术 拥塞干扰 窃听

中图分类号 TP309 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2016.12.067

RESEARCH ON PHYSICAL LAYER INFORMATION SECURITY TECHNOLOGY BASED ON SPATIAL TECHNOLOGY IN WIRELESS COMMUNICATION

Wu Yimeng[1] Shi Zhidong[1] Fang Weidong[1,2*] Deng Bin[1] Shan Lianhai[2,3]

[1](*School of Communication and Information Engineering, Shanghai University, Shanghai 201800, China*)

[2](*Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*)

[3](*Shanghai Internet of Things Co., Ltd., Shanghai 201899, China*)

Abstract Since wireless networks communication is vulnerable to the attacks of eavesdrop, jamming and interference, but to resist these attacks from physical layer can effectively mitigate the pressure on upper layers. Therefore in this paper, proceeding from the hidden troubles in wireless communication networks, we investigate the common attacks in wireless communication networks and the technical points of corresponding spatial technology-based countermeasures, and compare and summarise these methods, as well as make technical classification on them. At the same time, we also analyse their safety performances so as to provide helps for the subsequent researches and applications.

Keywords Wireless communication Physical layer security Spatial technology Jamming interference Eavesdrop

0 引 言

无线通信的发展起源于 19 世纪莫尔斯电报和贝尔电话的发明。一百多年来,无线通信行业得到了迅猛发展,给我们的工作和生活方式带来了巨大改变。无线网络也由最初的单一网络发展成为了现在的多模、多制式网络(如 3G、4G 等),无线传感器网络(WSNs)、无线自组网(Ad Hoc)的出现也极大地方便了我们的生活。

不容否认的是,随着无线网络的飞速发展,信息安全问题也成为了无线网络发展的一个重大挑战。由于无线网络的信道开放性、网络的移动性、拓扑结构的动态变化等特点[1],无线网络面临着各种安全威胁和攻击(如 DoS、假冒、干扰、篡改、泄露、网络泛洪、窃听等)。攻击者利用各种攻击手段对传输网络或是数据进行破坏,不但影响了通信的质量,而且严重危害了网络与信息的安全。因此,保障无线网络的信息安全是促进无线通信技术更加广泛应用的重要基础。

针对无线网络信息安全的威胁和攻击,应用最多的技术就是加密。但随着新技术的发展及计算能力的提高,加密技术并不能完全确保网络的信息安全,无法从根本上消除窃听和干扰等物理层攻击的影响。目前,新兴的不依赖计算能力的物理层安全技术可以克服上述缺点。一方面,它无需复杂度很高的算法,充分利用无线信道的特性进行信息传输;另一方面,可通过各种物理层安全技术来降低或消除这些有意或无意的网络安全攻击和干扰的影响。而我们通常把物理层安全技术划分为频域、时域和空域三个方面,其中基于空域的安全技术主要为一些天线技术,能够从空间上有效避免干扰和拥塞等物理层攻击的影响。而且作为信号传输的媒介,天线的使用也是无线通信中所必不可少的,因而采用空域技术来确保无线通信安全具有广阔的发展前景。相对于已经在无线通信中应用较为成熟的加密与安全攻击检测技术而言,基于空域的物理层的信息安全技术还是较新的研究方向。

本文采用了对比分析的方法,从物理层安全攻击的研究入手,对基于空域的物理层信息安全技术进行了对比研究。

收稿日期:2015-08-31。国家自然科学基金青年基金项目(61302113);上海市自然科学基金项目(13ZR1440800);上海市青年科技启明星计划项目(14QB1404400)。**吴伊蒙**,硕士生,主研领域:信息安全。**石志东**,研究员。**房卫东**,高级工程师。**邓斌**,硕士生。**单联海**,副研究员。

1 物理层攻击

无线通信的物理层位于网络的最底层,主要负责接收来自上层的数据流,并将其调制到无线信道进行传输;同时,从空口接收无线信号,将解调后的数据流发送给上层。由于物理层自身的传输特性,其面对的攻击主要是干扰、拥塞、窃听和流量分析。通常,将这些攻击分为主动攻击和被动攻击。

1.1 主动攻击

主动攻击主要是干扰和拥塞,其攻击原理基本相同,都是在某一频带上广播一个干扰信号,区别在于其作用对象不同。拥塞攻击主要针对发送方,攻击者通过长期占用信道,使发送者无法正常发送信号;而干扰则针对接收方,通过破坏合法信号,使接收者其无法接收到正确信号。拥塞攻击多为恶意攻击,而干扰除了来自有目的的攻击者外,还可能来自于周围同一信道的其他用户信号的干扰或是环境的影响。比如 WSNs 中,传感器节点大量随机分布于网络中,且通过多跳传输于同一信道中进行通信,彼此间信号的传输非常容易干扰到其他节点。

根据拥塞攻击技术的不同,常见的拥塞可以分为:定点拥塞、扫频拥塞、全波段拥塞和欺骗拥塞[2]。

1) 定点拥塞:主要针对某个单一频率进行拥塞,用足够的功率覆盖掉原始信号,实现简单,应用范围较广。

2) 扫频拥塞:干扰攻击者在拥塞过程中,拥塞频率快速地从一个频率跳变到另一个频率,优点是频率覆盖范围广,但无法同时覆盖多个频率;可对跳频技术造成有效攻击。

3) 全波段拥塞:干扰攻击者可以一次性拥塞一个大范围的频率,对覆盖范围内的用户通信造成巨大影响。但是由于发射功率的限制,频率范围越广则相应的拥塞能力也越弱。

4) 欺骗性拥塞:干扰攻击者向网络中发射伪造的正常数据,混淆用户的视听,将其当作正常数据包进行接收。而且此种拥塞方式不易于检测,极具破坏性。

攻击者也有多重的干扰方式,比如主动干扰和应对干扰[3]。主动干扰又可分为持续干扰、欺骗性干扰和按需干扰[4]。

1) 持续干扰指攻击者不间断地持续发射干扰信号,从而影响用户的正常通信。其目的是长期占用用户信道使信道保持繁忙状态,同时能够对正在进行的数据传输造成干扰,破坏其传输报文[2]。

2) 随机干扰是指攻击者随机对用户进行干扰,干扰时间和周期均不确定,相较于持续干扰可以有效节约攻击者的能耗,能够对 WSNs 这样的多跳网络造成较大影响。

3) 应对干扰是指干扰者在其信道空闲时内没有通信时保持闲置空闲状态,而只有在感知到信号传输时才会发送干扰信号来打断正在进行的传输。针对此类攻击,也可采取一些信息隐蔽技术,如 DSSS,传输信号功率谱密度小,且信号频谱类似于噪声信号,可有效增强信息隐蔽性。

干扰和拥塞攻击的信号带宽也有窄带和宽带之分。早期的攻击类型多为窄带攻击,其干扰带宽通常较小;而宽带干扰和拥塞则是在近年 3G、4G 技术出现以来,无线网络带宽迅猛增长后才发展起来的,其干扰带宽可达数十到数百兆赫兹不等。

1.2 被动攻击

被动攻击主要是窃听和流量分析。这两种攻击主要由无线通信的广播特性造成,致使位于其信号传播范围内的任何合法或非法用户都能拦截到无线广播信号,并对其进行分析和利用。

窃听是指网络通信的第三方有意或无意窃听到其他用户的通信信息而导致的信息泄露问题。由于无线信道的广播特性,通常情况下这一行为的实现非常容易。流量分析是指攻击者根据网络中信息流量的变化,得到一些有用信息,从而发动一些其他攻击。比如在无线传感网络中,攻击者可以通过对网络流量的监测变化判断出基站的位置,并对其基站进行干扰或捕获,从而导致整个 WSN 网络通信的瘫痪。

2 空域物理层安全技术

物理层安全传输最早可追溯到香农于 1949 年首次提出的信息理论加密[5],之后由 Wyner[6]、Csiszar 等人[7]对其进行了扩展。Shannon 主要研究了信息加密,证明了若要保证信息安全则需使秘钥长度大于或等于传输信息;而 Wyner 则证明了当合法用户的信道状况优于窃听者时,源节点和目的节点间能够安全可靠地传输信息;Csiszar 等人将其推广到了更为一般的应用场景。他们的研究为物理层信息安全提供了理论依据,使得我们能够从物理层的角度来解决信息的传输安全问题,从而减少上层网络的压力。

物理层安全技术大体上可以分为频域、时域和空域[9]三个方面。频域技术主要是扩频,利用载波频率的广阔和多变性,从频域上降低或避免攻击者对载波频段的干扰;时域技术主要为信道编码,通过在传输信息中加入一些监督码元来检查信息传输过程中的错误,并进行纠正。而空域技术主要是一些天线技术,包括定向天线、波束成形及基于波束成形技术的一些改进技术。它们通过采用适宜的天线技术从空间上躲避攻击者的信号干扰或是实现信道等参数的随机化,以达到抗干扰、抗拥塞和抵御窃听的目的。

近年来,由于各种新兴技术的兴起,也涌现了大量针对 SIMO、MIMO 和中继信道等的空域物理层安全技术的研究。因为 MIMO 等技术的采用在一定程度上可以增大网络的信道容量,那么就具备了增大保密容量和增强物理层安全的潜能[8]。利用空域多天线技术提供的空间冗余,便能达到增强物理层安全的目的,有效保证信息的传输安全。是以本文将主要从空域技术的角度来综述物理层的常见安全技术,并对其各自的性能优势及不足之处进行比较。

1) 定向天线技术

定向天线是指在某一个或多个特定方向上具有很高的传输功率的天线,具有信号传输距离远和地理覆盖范围广的特点。定向天线在接收信号时,能够将其主波束对准有用信息方向,零陷对准干扰信号,从而避免或降低干扰信号的接收,达到抗干扰和拥塞的目的[9]。相比于应用颇广的全向天线,定向天线能够显著提高网络的抗拥塞干扰性能[10],并具有更小的功耗。而且在发射功率较低且接收者方向的等效全向辐射功率相等的情况下,定向天线可以有效减小被检测的概率,使其在敌对环境中具有更好的匿名性[11]。

随着定向天线的小型化及增益性能的不断提升,它也被广泛用于各种无线 Mesh、Ad hoc 等多跳网络中来提升网络性能[12],解决网络干扰和连接问题,使其具有更大空间复用和传输距离。但是定向天线造价相对高昂,需合理配置使用。而且,复杂的无线通信环境总是存在各种干扰,给无线网络通信造成诸多困难。因而定向天线技术也不断在天线极化和增益方面寻

求突破,以获取更好的通信性能。

2) 波束成形技术

波束成形也是一种特别的方向可变的定向天线,又称智能天线,由一个多天线阵列组成。通过对其天线数量、元素间隔和几何结构等的配置[13],可实现天线波束方向的转变,令其天线辐射方向朝向合法接收者,方向图零点指向干扰者,从而避免干扰影响。波束成形技术的发射信号强烈且集中,有着比定向天线更高的信号增益和更大的传输距离,受干扰影响也同样较低,能够很好地抵御窃听[14]和拥塞攻击;而且集中的发射波束使其有效避免了多用户间的串扰问题。但是由于其采用多个天线,数据处理和功率消耗都要远大于定向天线,对硬件配置要求也较高,因而仍旧不能适用于一些能源有限和成本相对低廉的网络环境;而且功耗和成本控制也是波束成形技术所需要面临的难题。

目前,这一技术在 3G、4G 通信中得到了广泛应用,在有效解决多用户间通信干扰问题的同时,还使得网络的通信速率得到了提升,给用户带来了更好的网络体验。而且,波束成形技术还可采用中继协同的方式来形成波束成形系统,从而增强物理层安全,通常适用于一些多节点的中继协同网络。此外,除了依靠'零空间'波束成形外,文献[15]还在不依靠零空间时取得了较好的安全性能,而且窃听者数量大于中继数量时仍能适用。

3) 随机参数技术和随机天线技术

随机参数法是在波束成形的基础上发展来的。通过随机化发射天线权重造成窃听者接收信号的随机化,而经过预先信道估计和训练的合法用户却不受影响,其信道参数与预设的随机加权系数的乘积为定值,信号解调不会受到影响[16]。然而此方法虽达到了低拦截率(LPI)的目的,却是以牺牲发射功率为代价的,具有较高的发射功耗。

随机天线类似于随机参数,区别在于前者通过随机化加权系数来实现,而后者则是通过随机化发射天线实现窃听者接收信号的随机化的。该方法多用于一些多输入输出信道进行研究。在信号传输过程中发射方通过不断地随机变换发射天线,从而实现发射机与合法或非法用户间信道的随机化,相当于其加权系数也在不断变换[17]。类似于随机参数,经过信道训练的合法接收用户可以顺利解调出发射信号,而窃听者的接收信号却会发生错乱叠加。而且合理配置天线数量[8]或是选择信道质量好的天线也可带来天线性能的提升。然而,由于其随机选用多个发射天线,造成了阵列天线的冗余,信号利用率低也是此类技术不可忽略的一个弱点。而且随机天线技术的安全保密主要建立在窃听者的天线数量低于发送者的情况下,如若窃听者数量高于发送者,现有的多天线技术并不能完全保证发送者的信息安全。

4) 人工噪声技术

人工噪声的出发点就是使合法信道的保密容量高于窃听信道,那么便需要合法信道的信道状况(CSI)相对优于窃听信道[6],或者说需要恶化窃听信道或优化合法信道的 CSI。人工噪声法便是通过添加人工噪声来实现窃听信道恶化,令其只对窃听者有影响而对合法接收者没有影响。现今使用较为普遍的方法是人工噪声辅助波束成形。

人工噪声辅助波束成形法最早由 Goel 等人[18],采用多天线阵列创建出一个"零空间",将引入的噪声信号置于合法信道的零空间内,使知晓该信息的合法接收者能够将噪声滤除,而非法用户却会受到该噪声的影响。近年来,研究人员又对该方法进行了许多的后续研究和优化,比如:在确保网络服务质量的基础上,使用 SINR 作为限制指标辅助以人工噪声,达到能源节约和保密容量增强的目的[19]。而文献[20]更是将位于零空间的人工噪声推广到了更为一般的人工噪声,使其不再仅局限于零空间内,也可注入到信号空间,并取得了更好的成效。但是该技术实现复杂度仍旧较高,实际得到应用仍旧有较多问题要解决。图 1 从空域安全防御技术的角度给出了物理层的攻击分类及应对方式。

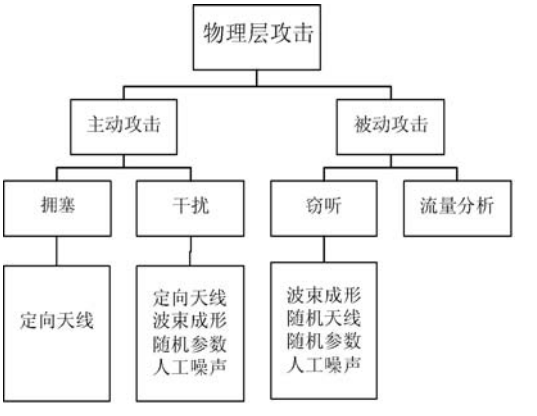

图 1　物理层攻击及应对措施

3　物理层安全技术分析

作为上层安全技术的一个补充,物理层安全技术的主要目的是减小信号传输过程中所遭受的安全攻击的影响,使其在复杂无线环境中仍能安全可靠地进行数据传输。空域物理层安全技术主要从空域的角度出发,利用一些天线技术从空间上避免了外界干扰的影响,从而保证了信息传输安全。本节将从各种空域技术应对攻击的类型和能力、技术特点、实现复杂度等方面做一个比较(如表 1 所示),从而清晰直观地展现各种空域技术的优势和不足之处,以及在整个领域里的研究现状(表中"–"表示应对能力较弱或不(少有)从该角度进行研究)。

由表 1 中可以看出,空域物理层安全技术对窃听攻击大都具有一定的抵御能力。可以根据其技术特点将其分为三类:一类是波束成形和定向天线这样的信息定向传输技术,只能在一定程度增强对窃听的抵御能力,却不能够有效消除来自窃听攻击的威胁,但是随着天线技术的发展,性能也在逐步得到提升。另一类便是随机参数、随机天线,通过对其加权系数、信道参数的随机化,使非法窃听者不能有效解调出正确信息,提高了其接收信息的误码率,从而具有较高的抵御窃听的能力,但是该类方法主要建立在发射天线数量多于窃听者的情况下。第三类是人工噪声技术,依靠在信道中添加人工噪声增加信道差异,使窃听信道的信道质量远差于合法信道,影响窃听者对信息的解调。后两类技术总的来说还是依赖于窃听者对合法信道 CSI 信息的未知,从而不能正确解调信号信息。但是由于它们实现起来较为复杂,因此目前多还处于理论研究阶段,尚不能用于实际应用中。

表 1 无线通信物理层安全技术分析

安全技术	技术特点	应对窃听的能力	应对拥塞的能力	应对干扰的能力	实现复杂度	实际应用情况
定向天线	在空间上加强某方向的接收增益	低	较高	中	低	广泛应用
波束成形	多天线信号叠加	低	较高	高	高	大量应用于3G、4G 通信
随机参数	增加信号随机性	较高	—	高	高	理论研究
随机天线	增加信道随机性	较高	—	—	高	少量应用
人工噪声	增加信道差异	高	—	高	高	理论研究

针对拥塞攻击的防御技术主要是定向天线和波束成形,它们通过在空间上实现拥塞避免,可躲避来自攻击者的攻击,同时具有较大的传输距离。对于干扰攻击,定向天线和波束成形主要依靠其信号的定向传输来减少对其他方向的干扰接收;而且定向天线和波束成形的天线增益较大,发射信号强烈集中,因而对干扰具有一定的抵御能力。而人工噪声和随机参数技术中也采用了波束成形,所以也具有抵御干扰攻击的能力。

与此同时,也可以从表 1 中看出,空域技术大多针对窃听攻击,对窃听具有较好的应对能力,而对拥塞和干扰的应对能力相对较弱。因为拥塞和干扰攻击主要针对发送和接收方,我们通常从时域和频域技术的角度来对其进行抵御,而空域安全技术则主要针对窃听攻击。

4 物理层空域安全技术展望及研究方向

无线通信技术,尤其是个人手持设备的快速发展,极大地促进了天线技术的研究进程,也给空域物理层安全技术带来了广阔的发展空间。但是随着我们对信号传输速率和信息安全性的不断追求,也不断呈现一些新的问题需要去解决。

1) 由于定向天线具有较高的天线增益,因而更适合较远距离的信号传输,且能起到外界干扰的作用,是以高增益宽频带的定向天线是当前的一个发展需求。

2) 人工噪声和随机参数都是在波束成形的基础上发展而来的。当前的波束成形技术可实现在多个方向上对用户进行追踪,因而精准地追踪定位用户并选取最佳传输信道是当前波束成形技术的一个重要研究方向。同时,智能天线技术的大规模应用又要求其具有较低的生产成本和复杂度,因而新的更为便捷的波束合成技术的研发也是当前波束成形的另一个努力方向。而随机参数和人工噪声法的应用实现也是其研究的一个难点。

3) 随机天线技术依靠阵列天线冗余实现其对窃听者的数据保密,但是也造成了信号利用率低的问题,且在窃听者天线数目多于自身时,并不能完全保证信息的安全性,是以提高信号利用率和增加信号的保密性可使其具有更广阔的应用前景。

5 结 语

本文主要调研了无线通信物理层的常见攻击类型,并从空域技术的角度展开综述了当前无线通信领域的常见安全技术及发展应用,对其技术要点和安全性能进行了分析,并对该领域面临的问题及发展趋势进行了总结论述。然而,由于空域技术的实现复杂度及能耗问题,应对窃听较为有效的随机参数和人工噪声技术大都还处于理论研究阶段。能够在实际中得到应用的空域安全技术主要还是针对干扰和拥塞攻击,针对窃听主要还是依赖于上层的数据加密技术。如何将其从理论研究应用到实际应用中仍旧是空域技术未来研究的一个重点和难点。

参 考 文 献

[1] Jiang T, Li T, Ren J. Toward secure cognitive communication in wireless networks[J]. IEEE Wireless Communications, 2012, 19(4): 82-88.

[2] Mpitziopoulos A, Gavalas D, Konstantopoulos C, et al. A survey on jamming attacks and countermeasures in WSNs[J]. IEEE Communications Surveys and Tutorials, 2009, 11(4): 42-56.

[3] Shiu Y S, Chang S Y, Wu H C, et al. Physical layer security in wireless networks: a tutorial[J]. IEEE Wireless Communications, 2011, 18(2): 66-74.

[4] Xu W, Trappe W, Zhang Y, et al. The feasibility of launching and detecting jamming attacks in wireless networks[C]//Proceeding of the 6th ACM international symposium on Mobile ad hoc networking and computing, 2005: 46-57.

[5] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[6] Wyner A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.

[7] Csiszar I, Korner J. Broadcast channels with confidential messages[J]. IEEE Transactions on Information Theory, 1978, 24(3): 339-348.

[8] Zou Y, Zhu J, Zheng B. Defending against eavesdropping attack leveraging multiple antennas in wireless networks[C]//Communications and Networking in China (CHINACOM), 2013 8th International Conference on, 2013: 699-703.

[9] 杨潘宏. 基于 OPNET 的战术通信网节点天线抗干扰研究[D]. 西安:西安电子科技大学, 2011.

[10] Noubir G. On connectivity in ad hoc networks under jamming using directional antennas and mobility[M]//Wired/Wireless Internet Communications. Springer Berlin Heidelberg, 2004: 186-200.

[11] Lu X, Wicker F D, Towsley D, et al. Detection Probability Estimation of Directional Antennas and Omni-Directional Antennas[J]. Wireless Personal Communications: An International Journal, 2010, 55(1): 51-63.

[12] Li Y, Pioro M, Landfeldt B G. Fair flow rate optimization by effective placement of directional antennas in wireless mesh networks[J]. Performance Evaluation, 2015, 87: 92-106.

[13] Bazan O, Jaseemuddin M. A survey on MAC protocols for wireless Adhoc networks with beamforming antennas[J]. IEEE Communications Surveys and Tutorials, 2012, 14(2): 216-239.

[14] Walsh C, Hakkarinen D, Camp T. Distributed decode and forward beamforming[C]//LCN'12 Proceedings of the 2012 IEEE 37th Conference on Local Computer Networks (LCN 2012), 2012: 436-444.

[15] Liu Z, Chen C, Bai L, et al. Transmit power minimization beamforming via amplify-and-forward relays in wireless networks with multiple eavesdroppers[C]//2014 IEEE International Conference on Communications (ICC), 2014: 4698-4703.

[16] Li X, Hwu J, Ratazzi E P. Using antenna array redundancy and channel diversity for secure wireless transmissions[J]. Journal of Communications, 2007, 2(3): 24-32.

(下转第 317 页)

SaM: A Split and Merge Algorithm for Fuzzy Frequent Item Set Mining	2016-06-03 17:02:29
谷歌浏览器历史记录插件	2016-06-03 16:37:22
URLviewer	2016-06-03 16:32:12
Browser History spy	2016-06-03 16:18:51
Browser history spy	2016-06-03 16:14:01
Briton Googled 'how to kill' days before murders: court	2016-06-03 11:00:36
blank faced	2016-06-03 10:07:10
Briton Googled 'how to kill' days before murders: court	2016-06-03 9:58:25
sqlite3	2016-06-03 9:40:59

图 11　按时间筛选检索关键词

4　结　语

本文针对目前的浏览器历史记录提取工具在展示结果时生成的报表数据冗长,缺乏直观性这一问题,提出基于域名聚合与频繁项集挖掘的 Chrome 浏览器历史记录提取与分析方法,为调查人员提供更直观的展示结果。该方法能够从 SQLite 数据库中提取 Chrome 浏览器 Web 访问记录,并根据调查人员的需要对记录按时间段进行筛选展示;再通过分析历史记录挖掘 TOP-K 频繁访问网站,能够实现把检索关键词与搜索引擎相关联或按时间段展示。真实的 Chrome 浏览器历史记录数据上的实验评估证明了方法的有效性。此外,本文提出的方法同样可应用于 Safari、Firefox 等使用 SQLite 数据库存储并管理历史记录数据的浏览器。

参　考　文　献

[1] Fei B K L. Data visualization in digital forensics[D]. Pretoria, South Africa: University of Pretoria, 2007.

[2] Marcella A J, Menendez J D. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes [M]. 2nd ed. New York, NY, USA: Auerbach PublicationsCRC Press, 2007.

[3] Agence France-Presse. Briton Googled 'how to kill' days before murders: US court[N/OL]. (2008-06-18). [2016-06-01]. http://news.asiaone.com/News/AsiaOne%2BNews/World/Story/A1Story20080618-71463.html.

[4] 搜狐新闻. 警方"预感"马加爵会逃亡海南[N/OL]. (2004-03-17). [2016-06-29]. http://news.sohu.com/2004/03/17/72/news219467286.shtml.

[5] Net Applications. Desktop Browser Market Share[EB/R/OL]. (2016-05-01). [2016-06-29]. http://www.netmarketshare.com/browser-market-share.aspx?qprid=0&qpcustomd=0.

[6] Jones K J. Pasco v1.0: An Internet Explorer aActivity fForensic aAnalysis tTool[EB/OL]. [2016-06-29]. http://www.mcafee.com/us/downloads/free-tools/pasco.aspx#.

[7] SecurityXploded. Browser History Spy (version4.6)[EB/OL]. (2015-07-18). [2016-05-29]. http://securityxploded.com/browser-history-spy.php.

[8] Wang Z, Lin F X, Zhong L, et al. How far can client-only solutions go for mobile browser speed? [C]//Proceedings of the 21st International Conference on World Wide Web, Lyon, France, 2012: 31-40.

[9] Catledge L D, Pitkow J E. Characterizing browsing strategies in the World Wide Web[J]. Computer Networks and ISDN Systems, 1995, 27(6): 1065-1073.

[10] Hannak A, Sapiezynski P, Kakhki A M, et al. Measuring personalization of web search[C]//Proceedings of the 22nd International Conference on World Wide Web, Rio de Janeiro, Brazil, 2013: 527-538.

[11] Jerath K, Ma L, Park Y H. Consumer click behavior at a search engine: the role of keyword popularity[R]. Reports-Marketing Science Institute, 2013.

[12] Ho C L, Lin M H, Chen H M. Web users' behavioural patterns of tourism information search: from online to offline[J]. Tourism Management, 2012, 33(6): 1468-1482.

[13] 朱小龙,孙国梓. 浏览器历史痕迹提取技术[J]. 信息网络安全, 2013(1): 19-21.

[14] 王宇阳. 智能手机平台浏览器上网记录的提取与分析[D]. 长春: 吉林大学软件学院, 2015.

[15] UrlViewer[DB/OL]. (2014-09-15). [2016-05-20]. http://www.pc0359.cn/downinfo/14976.html.

[16] Better History for Chrome 3.9.13[EB/OL]. [2016-05-30]. http://better-history.com.

[17] Borgelt C, Wang X M. SaM: A split and merge algorithm for fuzzy frequent item set mining[C]//Proceedings of the 13th International Fuzzy Systems Association World Congress and 6th Conference of the European Society for Fuzzy Logic and Technology Conference, Lisbon, Portugal, 2009: 968-973.

[18] Jeon S, Bang J, Byun K, et al. A recovery method of deleted record for SQLite database[J]. Personal and Ubiquitous Computing, 2012, 16(6): 707-715.

[19] Aouad L M, Kechadi T M, Russo R D. ANTS ROAD: A new tool for SQLite data recovery on aAndroid devices[C]//Proceedings of the 4th International ICST Conference on Digital Forensics and Cyber Crime, Lafayette, IndianaN, USA, 2012: 253-263.

[20] Pereira M T. Forensic analysis of the fFirefox 3 Internet history and recovery of deleted SQLite records[J]. Digital Investigation, 2009, 5(3-4): 93-103.

[21] Public suffix list[EB/OL]. [2016-05-24]. https://publicsuffix.org.

(上接第 223 页)

[8] Bouhana A, Fekih A, Abed M, et al. An integrated case-based reasoning approach for personalized itinerary search in multimodal transportation systems[J]. Transportation Research Part C Emerging Technologies, 2013, 31(2): 30-50.

[9] Roy B, Slowinski R. Criterion of distance between technical programming and socio-economic priority[J]. Recherche opérationnelle, 1993, 27(1): 45-60.

[10] Khelifa S B, Martel J M. A distance-based collective weak ordering [J]. Group Decision and Negotiation, 2001, 10(4): 319-329.

[11] Fan Z P, Li Y H, Wang X H, et al. Hybrid similarity measure for case retrieval in CBR and its application to emergency response towards gas explosion[J]. Expert Systems with Applications, 2014, 41(5): 2526-2534.

[12] 张本生,于永利. CBR 系统案例搜索中的混合相似性度量方法[J]. 系统工程理论与实践, 2002, 22(3): 131-136.

(上接第 290 页)

[17] 赵根银. 随机天线阵列的物理层安全传输在无线通信中的应用[J]. 信息系统工程, 2013(5): 96.

[18] Goel S, Negi R. Guaranteeing Secrecy using Artificial Noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.

[19] Liao W C, Chang T H, Ma W K, et al. QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach[J]. IEEE Transactions on Signal Processing, 2011, 59(3): 1202-1216.

[20] Lin P H, Lai S H, Lin S C, et al. On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels[J]. IEEE Journal on Selected Areas in Communications, 2013, 31(9): 1728-1740.