一种解决认知无线电网络模仿主用户攻击问题的方案

薛 楠 周贤伟 辛晓瑜 李 丹 杨 桢
(北京科技大学信息工程学院通信系 北京 100083)

摘 要 针对认知无线电网络中出现的模仿主用户攻击问题,提出一种基于HASH匹配技术的解决方案。当主用户网络工作时,主用户基站在要传输的数据上附加用于HASH计算的原始数据,然后将它们发送出去,认知用户先对接收到的那些原始数据做HASH计算,然后将计算结果同预先保留的HASH值相比较。如果匹配成功,则证明有主用户出现。方案充分利用HASH函数计算速度快的特点,保证认知用户及时切换频谱,避免干扰主用户正常工作,利用HASH函数单向不可逆的特点保证了方案的安全性。给出了具体的设计方案。通过与相关方案比较,该方案具有安全、高效、可行的特点,能有效解决认知用户网络中出现的模仿主用户攻击问题。

关键词 认知无线电,模仿主用户攻击,网络安全,HASH
中图法分类号 TP309.2 **文献标识码** A

Scheme for Primary User Emulation in Cognitive Radio Networks

XUE Nan ZHOU Xian-wei XIN Xiao-yu LI Dan YANG Zhen
(Department of Communication Engineering, College of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)

Abstract To solving the threat to the primary user emulation (PUE) in cognitive radio networks, this paper presented a security scheme based on HASH matching technique. In this scheme, when primary user network was working, we added the HASH original data to the data sent by primary user base station, firstly secondary users used HASH function to calculate those received original data, and then compared results with predistribution HASH values. Successful matching proved that the message of primary user emergency was true. This scheme made the best of the HASH characteristic of quickly calculating, which guaranteed timely spectrum handoff of secondary users and avoided interfering with primary user. The security of this scheme was guaranteed by the irreversible of one-way HASH function. The detail of the scheme was presented in this paper. Comparing with relevant schemes, it provides safety, efficiency and feasibility, and can effectively solve primary user emulation problem in cognitive radio networks.

Keywords Cognitive radio, Primary user emulation (PUE), Network security, HASH

认知无线电技术是为了防止无线频谱资源日益紧张而提出的。它通过检测那些处于空闲状态的频谱,在不影响授权用户工作的前提下智能地选择和利用这些空闲频谱[1]。从1999年瑞典皇家工学院的Mitola J.博士首先提出认知无线电概念[2]以来,这种技术受到人们广泛关注,取得了长足的发展。

在认知无线电技术发展过程中产生了许多特有的安全问题,其中影响较大的一种是模仿主用户攻击问题。通常规定使用认知无线电技术的用户叫认知用户,使用授权频段的授权用户叫主用户。认知用户工作时的一个特点是,认知用户在空闲授权频段工作时,如感知到主用户存在,则必须立即退出该授权频段或降低发射功率以避免干扰主用户。攻击者利用这个特点发起模仿主用户攻击。攻击具体表现为当攻击者检测到空闲授权频段时,它在该频段发送与主用户信号具有相似特征的信号,以此来阻止其它认知用户竞争此频段。这种攻击不但严重干扰认知用户的频谱感知过程,而且显著减少认知用户的可用频谱[3]。

为了区分主用户信号和认知用户信号,现有的频谱感知方法主要为能量检测[4,5]技术、滤波器匹配技术和静态循环特征检测技术[6]等几种。

能量检测技术主要是通过在一定频带范围内作能量积累,如果积累的能量高于一定的门限,则说明有主用户信号存在。这种检测方法不够精确,容易受噪声功率影响。

滤波器匹配技术利用滤波器的输出端能够获得最大信噪比的特点,来准确判断主用户是否出现。这种技术实现复杂,认知用户对每个主用户都需要一个单独的匹配滤波器。

到稿日期:2008-10-31 返修日期:2009-01-05 本文得到国家自然科学基金项目(No. 60773074 认知无线电安全关键技术研究)资助。
薛 楠(1978—),男,博士研究生,主要研究方向为信息安全、认知无线电网络安全、组播安全、传感器网络安全,E-mail:xuenanhello@163.com;周贤伟(1963—),男,博士后,教授,博士生导师,主要研究方向为通信网安全、宽带移动通信和组播安全等;辛晓瑜(1981—),女,硕士研究生,主要研究方向为认知无线电网络安全;李 丹(1983—),女,硕士研究生,主要研究方向为认知无线电网络安全;杨 桢(1983—),男,硕士研究生,主要研究方向为认知无线电网络安全。

静态循环特征检测技术利用调制信号的均值和自相关函数都具有周期性的特点。通过分析频谱自相关函数能够把噪声能量和已调信号的能量区分开，从而判断主用户信号的存在，但这种技术实现复杂，测量时间较长。

Chen R. 和 Park J. 在文献[3]中提出应用距离比校验和距离差校验方法来解决模仿主用户攻击的问题。通过位置确认可判断主用户的真实性，但这种方法测量误差较大。

鉴于以上方案的不足，我们提出基于 HASH 匹配技术的解决方案。当主用户网络工作时，主用户基站将用于计算 HASH 值的原始数据添加到要发送的数据上。认知用户接收到这些原始数据后，对其做 HASH 计算。如果计算结果同预先保留的 HASH 值相同，则证明主用户网络正在工作。该方案具有安全、高效、可行的特点。

本文第 1 节描述采用的认知无线电网络模型；第 2 节介绍基于 HASH 匹配技术解决模仿主用户攻击问题的具体方案；第 3 节是性能分析；最后总结全文。

1 认知无线电网络工作模型

如图 1 所示，认知无线电网络工作模型包括两部分，主用户网络和认知用户网络。

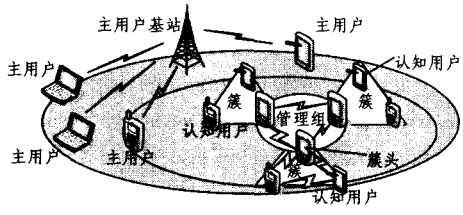

图 1 认知无线电网络工作模型

主用户网络是一个已存在的网络，有自己的授权频段。它可以是现有的广播电视网络。它由主用户基站和主用户组成。主用户基站是一个固定的基础设施，有频段使用授权书，负责在授权频段向主用户提供服务，类似广播电视塔。主用户是接收装置，它们可以在授权频段接收数据，类似无线接收机，主用户不必为与认知用户网络共存而作任何功能上的改变。

通常主用户网络工作有如下两种方式：一种方式，由主用户向主用户基站发送请求信息，主用户基站接收到请求信息后在其授权频段发送数据。当主用户不需要提供服务时，就向主用户基站发送停止信息，主用户基站接收到停止信息后，立即停止发送数据。另一种情况，主用户基站不受主用户控制，自主决定是否在授权频段发送数据。

认知用户网络由认知用户组成。相邻的认知用户组成一簇，每簇选出一个簇头，簇头可在控制信道转发簇间数据，簇头共同组成管理组。认知用户不停地感知周围的频谱使用情况，将检测结果汇报给由簇头组成的管理组，然后由管理组决定频谱分配策略，经簇头下发给各个认知用户。认知用户网络使用固定的控制信道发送频谱感知信息和控制信息，使用空闲授权频段发送数据信息。认知用户网络处于主用户基站发射信号的覆盖范围内。

这个模型中主用户仅发送控制信号，主用户网络中出现的信号大都是主用户基站发出的，主用户在多数情况下只作为一个接收装置。所以这里可将模仿主用户攻击概念具体化为模仿主用户基站发送信号攻击。它具体表现为当攻击者检测到一个空闲频段时，攻击者发送模仿主用户基站信号特征的信号，以此来阻止其它认知用户竞争此频段。

为便于表述，作如下记号：

B 表示主用户基站。C_i 表示认知用户网络的簇 i。CH 表示全体簇头组成的管理组。PU 表示全体主用户。$SU_{i,j}$ 表示认知用户网络中簇 C_i 的第 j 个认知用户，SU 表示全体认知用户。D_T 表示主用户基站 T 时刻发送的数据，T 为主用户基站开始发送数据 D_T 的时间。f_{D_T} 表示主用户基站发送数据 D_T 时占用的授权频段，发送不同数据时主用户网络占用的授权频段可能不同。M_x 表示第 x 个用于计算 HASH 的原始数据。H_x 表示与 M_x 相匹配的、经 HASH 计算的结果。K_i 表示簇 C_i 的簇密钥，簇成员拥有，当簇内有成员加入、离开时需及时更新。K 表示由簇头组成的管理组组密钥，同样管理组有成员需要加入、离开时也需及时更新。

2 基于 HASH 匹配技术解决模仿主用户攻击问题的方案

(1)认证中心将大量不同的 HASH 值$\{H_1, H_2, H_3, \cdots, H_n\}$作为一个整体分配给认知用户网络中的所有认知用户，再将计算这些 HASH 值的原始数据$\{M_1, M_2, M_3, \cdots, M_n\}$分配给主用户基站 B。主用户基站每次使用的 M_x 各不相同。这两部分数据是一一对应的。

(2)主用户基站 B 在授权频段 f_{D_T} 发送数据 D_T 时，将用于计算 HASH 值的原始数据 M_x 和开始发送数据时间 T 附加在数据 D_T 上，将它们一起发送出去。

$$B->(SU,PU):\{M_x,T,D_T\}$$

(3)认知用户 $SU_{i,j}$ 在 f_{D_T} 频段感知到$\{M_x, T, D_T\}$数据包后，它先对其中的 M_x 做 HASH 计算，然后将计算结果 HASH(M_x)同预先分配的$\{H_1, H_2, H_3, \cdots, H_n\}$作比较，如有 H_x=HASH(M_x)，则说明主用户基站正在使用 f_{D_T} 频段。

$SU_{i,j}$ 及时通过控制信道向本簇 C_i 中的其他认知节点广播 H_x 及 $MAC_{K_i}(H_x)$，

$$SU_{i,j}->C_i:\{MAC_{K_i}(H_x),H_x\}$$

$SU_{i,j}$ 同时通过控制信道向簇头 CH_i 发送主用户出现消息，

$$SU_{i,j}->CH_i:\{MAC_{K_i}(f_{D_T},H_x,T),f_{D_T},H_x,T\}$$

(4)簇 C_i 中的其他簇成员接收到 $SU_{i,j}$ 发送过来的消息后，验证消息的正确性。通过验证后，它们就不向簇头 CH_i 发送由 M_x 得到的主用户出现消息。

(5)簇头 CH_i 接收到 $SU_{i,j}$ 发送的主用户出现消息$\{MAC_{K_i}(f_{D_T},H_x,T),f_{D_T},H_x,T\}$后，首先验证消息的正确性。如果其中包含的时间 T 是簇头 CH_i 接收到的所有数据包中距当前时间最近的一个，而且 H_x 以前没有被重复接收过，CH_i 就及时通过控制信道向管理组转发$\{MAC_K(f_{D_T},H_x,T),f_{D_T},H_x,T\}$。

$$CH_i->CH:\{MAC_K(f_{D_T},H_x,T),f_{D_T},H_x,T\}$$

管理组 CH 判断$\{MAC_K(f_{D_T},H_x,T),f_{D_T},H_x,T\}$的正确性。如果其中包含的时间 T 是管理组 CH 接收到的所有数据包中距当前时间最近的一个，而且 H_x 以前没有被接收过，CH 就迅速根据 f_{D_T}，决定频谱切换策略。随后各个簇头使用各自的簇密钥将频谱切换策略和 H_x 加密，通过控制信道下发给各簇内认知用户。簇成员及时根据接收到的策略进

行频谱切换并将其中的 H_x 从$\{H_1, H_2, H_3, \cdots, H_n\}$中删除。

(6)当 CH 经过一段时间 σ 后,没接收到某频段被占用的消息,就认为该频段是空闲的。

(7)当预先分配的 HASH 值和原始数据用完后,认证中心及时加以补充。

如果认知用户在授权频段检测到的信号中,没有用于计算 HASH 值的原始数据或原始数据经过 HASH 计算以后不能正确匹配,则说明这个信号不是主用户基站发出的。即使有攻击者发送的模仿主用户基站信号非常接近真实的基站信号,也不能达到冒充主用户基站占用授权频段的目的。上面的设计方案仅仅检测出了这种安全问题,随后可采取某种方法(比如定位技术)找到攻击者,限制其活动或将其破坏,从而彻底消除干扰。

3 性能分析

(1)主用户基站每次发送用于计算 HASH 值的原始数据各不相同,这样可防止攻击者利用截获的原始数据发送虚假主用户出现消息。

$SU_{i,j}$ 向本簇中其他认知用户广播$\{MAC_{K_i}(H_x), H_x\}$,可避免簇 C_i 中的其他认知用户再次向 CH_i 发送由 M_x 判断出的主用户出现消息,节省通信资源,减轻 CH_i 数据处理负担。其中 $MAC_{K_i}(H_x)$可保证 H_x 是由簇内认知用户发出的,避免某些已退出认知用户网络,但仍拥有 HASH 值的认知用户发送错误信息,妨碍认知用户发送由 M_x 判断出的主用户出现消息。CH_i 接收到$\{MAC_{K_i}(f_{D_T}, H_x, T), f_{D_T}, H_x, T\}$后,判断 H_x 是否重复,可避免其再次向管理组发送相同的频谱变化信息,保证对于由同一个 H_x 检测出的频谱变化情况,每簇至多有一个消息发送到管理组。CH_i 对 T 做比较可及时转发最新的频谱变化情况。

CH_i 向管理组 CH 发送 $MAC_K(f_{D_T}, H_x, T)$,这样 CH 可验证 f_{D_T}, H_x, T 的真实性,避免某些已退出管理组但仍拥有 HASH 值的簇头向管理组发送虚假主用户出现消息。CH 判断 H_x 是否重复,可避免对由同一 H_x 得出的频谱变化情况做重复处理。CH 仅对最先到达的$\{MAC_K(f_{D_T}, H_x, T), f_{D_T}, H_x, T\}$做处理。这样可避免恶意节点截获同样的数据包,发起重放攻击。并且如果数据包中的 T 不是接收到的数据包中距当前时间最近的一个,那么就放弃该数据包。这样可保证对当前最新的环境变化做出频谱切换策略。

认知用户要及时删除匹配过的 H_x。因为网络中部分认知用户可能没有接收到主用户基站发送过来的用于计算 H_x 的 M_x,这样攻击者就可以在其他时间利用截获的 M_x 向这部分认知用户发送虚假主用户出现消息,使这部分认知用户误以为主用户出现而向网络发送主用户出现消息。及时删除匹配过的 H_x 以后,就消除了这个安全隐患。

簇头加密频谱切换策略可避免恶意节点得到切换策略,发起有针对性的攻击。

(2)HASH 计算实现简单是一种较成熟的密码学技术,其拥有的单向性,保证任何认知用户都不能通过预先得到的 H_x 确定 M_x,从而利用算出的原始数据发起模仿主用户攻击。

(3)主用户基站保留用来计算 HASH 值的原始数据$\{M_1, M_2, M_3, \cdots, M_n\}$,其易遭到攻击。但由于主用户基站是主用户网络的一部分,其安全性可由主用户网络保证。

(4)HASH 计算相对以公钥为基础的数字签名来说计算量小,计算速度快,缩短了判断授权频段主用户出现的时间,进而加快了认知用户频谱切换速度。

(5)利用主用户基站发送$\{M_1, M_2, M_3, \cdots, M_n\}$是可行性的。主用户基站是运营商集中管理的设备,易于为达到某种目的而改变其部分功能。而主用户往往是大量分散到各地的设备,为了适应认知用户网络而对主用户重新加以改造是不现实的。方案充分利用了网络已有的基础设施,避免主用户与认知用户间的直接交互,并没有改变认知用户任何功能。

表 1 是本方案同其他方案的一个比较,通过比较可知,本方案除了在适用性方面略显欠缺以外,在其他性能上均有优势,是一种比较优秀的解决模仿主用户攻击问题的方案。

表 1 HASH 匹配技术解决方案同其他方案比较

解决方案	优点	缺点
HASH 匹配技术	实现简单、测量精度高、计算量小、时间快	适用范围有限,仅局限于有主用户基站的网络
能量检测技术	简单易实现、适用性广	受噪声影响大、测量精度低
静态循环特征检测技术	测量精度高、适用性广	实现复杂、计算量大
滤波器匹配技术	测量精度高、时间快	实现复杂、对每个主用户,接收机都需要一个单独的匹配滤波器
距离比,距离差校验技术	实现简单	测量精度低

结束语 模仿主用户攻击是认知无线电网络特有的安全威胁,它严重减少了认知用户网络的可用频谱,降低了网络的通讯能力。文中利用 HASH 计算的高效性和不可逆性,提出了一种基于 HASH 匹配技术的解决方案。该方案安全、高效、可行,可以较好地解决认知用户网络中出现的模仿主用户攻击问题。如果有攻击者发起攻击,即使它发送的模仿主用户基站信号非常接近主用户基站信号,那么只要不能成功进行 HASH 匹配,就认为该信号不是主用户基站发出的。这样它就不能达到冒充主用户基站占用授权频段的目的。但该方案仅可应用于有主用户基站的网络中,方案的适用范围受到限制。因此在将来的研究中应充分考虑安全方案的适用性,设计出适用性更强的安全解决方案。

参 考 文 献

[1] Prasad R. Special issue on " cognitive radio technologies "[J]. Wireless Personal Communications, 2008, 45(3): 277-279

[2] Mitola J, Maquire G J. Cognitive radios: making software radios more personal[J]. IEEE Personal Communications, 1999, 6(4): 13-18

[3] Chen R, Park J M. Ensuring trustworthy spectrum sensing in cognitive radio networks[C]// IEEE Workshop on Networking Technologies for Software Defined Radio Networks. Reston, VA, USA, 2006: 110-119

[4] Challapali K, Mangold S, Zhong Z. Spectrum agile radio: Detecting spectrum opportunities[C]// 6th Annual International Symposium on Advanced Radio Technologies. Colorado. USA, 2004: 23-27

[5] Olivieri M P, Barnett G A, Lackpour A, et al. A scalable dynamic spectrum allocation system with interference mitigation for teams of spectrally agile software defined radios[C]// First IEEE International Symposium on New Frontiers in Dynamic

Spectrum Access Networks. Piscataway, NJ, USA, 2005: 170-179

[6] Cabric D, Mishra S M, Brodersen R W. Implementation issues in spectrum sensing for cognitive radios[C]// Thirty-Eighth Asilomar Conference on Signals, Systems and Computers. Piscataway, NJ, USA, 2004: 772-776

(上接第 7 页)

(1)设计一个简洁的符号表示方案表示时间,从而达到有效建模的目的;(2)在时间建模的基础上,研究一套更有效的符号化验证方法对时间敏感协议进行验证,例如上节提出的在验证中加入约束条件等;(3)对存在攻击的协议构造相应的反例;(4)根据反例生成的约束条件,给出避免反例产生时的约束,从而能通过控制有效期等因素有效地避免攻击的产生;(5) 对时间同步协议的认证性进行验证;(6)设计自动验证工具自动完成验证和反例构造工作;(7) 自动验证带时间特性的大规模复杂安全协议。

参 考 文 献

[1] 薛锐,冯登国. 安全协议的形式化分析技术与方法[J]. 计算机学报,2006:1-20

[2] 冯登国. 国内外安全协议研究现状及发展趋势[C]// 信息安全国家重点实验室安全协议研讨会文集. 2004,10

[3] Sangiorgi D, Walker D. The π-calculus: a Theory of Mobile Processe[M]. Cambridge University Press, 2001

[4] Abadi M, Gordon A D. A calculus for cryptographic protocols: The spi calculus[J]. Information and Computatiuon, Academic Press, 1999: 148(1): 1-70

[5] Bella G. Inductive Verification of Cryptographic Protocols[D]. University of Cambridge, 2000

[6] Berezin S. Model Checking and Theorem Proving : a Unified Framework[D]. Carnegie Mellon University, 2002

[7] Bozga L, Lakhnech Y, Périn M. Pattern-based Abstraction for Verifying Secrecy in Protocols[C]// TACAS 2003. 2003: 299-314

[8] Butler F, Cervesato I, Jaggard A, et al. A Formal Analysis of Some Properties of Kerberos 5 Using MSR[C]//Proceedings of the 15th IEEE Computer Security Foundations Workshop(CSFW'02). 2002

[9] Cervesato I, Durgin N A, Lincoln P D, et al. A Meta-notation for Protocol Analysis[C]// Proc. of the Twelfth IEEE Computer Security Foundations Workshop. 1999: 55-69

[10] Corin R, Etalle S, Hartel P H, et al. Timed Model Checking of Security Protocols[C]// Proceedings of the 2004 ACM workshop on formal methods in security engineering. ACM Press, 2004: 23-32

[11] Delzanno G, Ganty P. Automatic Verification of Time Sensitive Cryptographic Protocols[C]// TACAS 2004, Held as Part of the Joint European Conferences on Theory and Practice of Software. ETAPS 2004. Barcelona, Spain, March 2004: 342-356

[12] Dolev D, Yao A. On the security of public-key protocols[J]. IEEE Transaction on Information Theory, 1983, 2(29): 198-208

[13] Denning, Sacco. Timestamps in Key Distribution Protocols[J]. Communications of the ACM, 1981, 24(8): 533-536

[14] Evans N, Schneider S. Analysing Time Dependent Security Properties in CSP using PVS[C]// Frédéric Cuppens, Yves Deswarte, Dieter Gollmann, Michael Waidner, eds. ESORICS, volume 1895 of LNCS. Springer, 2000: 222-237

[15] Lee J, Žic J. On Modeling Real-time Mobile Processes[C]//25th Australasian Computer Science Conference(ACSC2002). 2002

[16] Lowe G. A Hierarchy of Authentication Specifications [C]// Proc. 10th IEEE Computer Security Foundations Workshop. 1997: 31-43

[17] Lowe G. Casper: A Compiler for the Analysis of Security Protocols[C]//Proceedings of 10th IEEE Computer Security Foundations Workshop. 1997

[18] Lowe G, Ouäknine J. On timed models and full abstraction[C]// Proceedings of the Twenty-first Conference on the Mathematical Foundations of Programming Semantics(MFPS '05). ENTCS, 2005

[19] Gorrieri R, Locatelli E, Martinelli F. A Simple Language for Real-Time Cryptographic Protocol Analysis[C]// Pierpaolo Degano, ed. 12th European Symposium on Programming. ESOP 2003, volume 2618 of LNCS. Heidelberg, Springer-Verlag, 2003: 114-128

[20] Schneider S A. Concurrent and Real-time Systems[M]. Wiley, 1999

[21] Syverson P F. Adding Time to a Logic of Authentication[C]// CCS '93. 1993: 97-101

[22] Syverson P, Meadows C, Cervesato I. Dolev-Yao is no better than Machiavelli[C]// WITS'00. Workshop on Issues in the Theory of Security. 2000

[23] Tripakis S, Yovine S. Analysis of Timed Systems Using Time-Abstracting Bisimulations[C]// Formal Methods in System Design. Springer Science+Business Media B. V., Formerly Kluwer Academic Publishers B. V, 2001

[24] Abadi M, Blanchet B. Analyzing security protocols with secrecy types and logic programs[C]//29th ACM Symposium on Principles of Programming Languages(POPL'02). ACM Press, 2002: 33-44

[25] Blanchet B. An efficient cryptographic protocol verifier based on prolog rules[C]//Proc. of the 14th Computer Security Foundation Workshop(CSFW14). IEEE Computer Society Press, 2001: 82-96

[26] Blanchet B. From Secrecy to Authenticity in Security Protocols [C]// 9th International Static Analysis Symposium(SAS'02). Vol 2477 of LNCS. Springer-Verlag, September 2002: 242-259

[27] Bozga L, Ene C, Lakhnech Y. A Symbolic Decision Procedure for Cryptographic Protocols with Time Stamps (Extended Abstract)[C]//CONCUR 2004. LNCS 3170. 2004: 177-192