无线跳频技术在局域网的安全应用分析

栗 勇　卿斯汉　（湖南大学软件学院 ）

摘要：在网络技术快速发展的今天，无线网络已经成为新一代的网络基础，但是由于安全问题一直得不到很好的解决，制约了无线网络的发展。通过跳频技术建立一个优于现在使用的无线局域网，分析跳频技术在无线网中的应用所带来的影响和实现的可行性。

关键词：无线局域网络 无线网安全 跳频通信

1 引言

无线局域网络由于其摆脱了通信线缆的束缚，其发展已经成为今后网络的主要的连结形式。但是在无线网络发展的同时，一个突出的问题显现出来，这就是无线网的安全问题。下面将通过采用跳频技术来加强无线网的链路的手段，在现有条件下，完善网络的安全性能。

2 跳频通信特性

跳调频通信系统（FH－SS）是一个用户的载波频率按某种跳频图案（伪随机调频序列）在很宽的频带范围内跳变的通信系统。

跳频技术的优点：

（1）抗干扰能力强，特别是抗窄带干扰能力。

（2）可检性低，（LPI－－－Low Probability of Intercept），不容易被侦破。

（3）具有多址能力，易于实现码分多址（CDMA）技术。

（4）可抗多径干扰。

（5）可抗频率选择性衰落。

（6）频谱利用率高，容量大（可有效利用纠错技术、正交波形编码技术、话音激活技术等）。

（7）具有测距能力。

主要缺点：技术复杂，但是随着数字处理技术的发展，集成工艺进步，使扩频系统的实现变的简单，只需对扩展技术有一般的了解就可以从事扩频系统的设计工作。因此，扩频技术在这些年发展非常迅速，由军用到民用，商用，范围很广。

3 跳频技术的安全性分析

跳频的安全性主要体现在其载波频率跳变的随机性，首先跳频通信的原理是通过硬件生成一个伪随机序列，其次，再通过伪随机性序列生成通信所需要的跳频图案，最后，再由硬件实现通信的同步，使通信双方按照跳频图案同时跳变调制解调的频率，完成跳频信号的收发。

跳频图案是实现跳频安全性的关键，下面简述一下跳频图案在安全防护上的作用。

3.1 跳频图案

为了不让攻击者知道我们通信使用的频率，需要经常改变载波频率，即“打一枪换一个地方”似地对载波频率进行跳变，跳频通信中载波频率改变的规律，叫作跳频图案。

通常我们希望频率跳变的规律不被攻击者所识破，所以需要随机地改变以至无规律可循才好。但是若真的无规律可循的话，通信的双方（或友军）也将失去联系而不能建立通信。因此，常采用伪随机改变的跳频图案。

只有通信的双方才知道此跳频图案，而对攻击者则是绝对的机密。所谓“伪随机”，就是“假”的随机，其实是有规律性可循的，但当攻击者不知跳频图案时，就很难猜出其跳频的规律来。

图1所示为一个跳频图案。图中横轴为时间，纵轴为频率。这个时间与频率的平面叫作时频域。也可将这个时频域看作一个棋盘，横轴上的时间段与纵轴上的频率段构成了棋盘格子。阴影线代表所布棋子的方案，就是跳频图案；它表明什么时间采用什么频率进行通信，时间不同频率也不同。

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

图1(a)中所示为一快跳频图案,它是在一个时间段内传送一个码位(比特)的信息。通常称此时间段叫跳频的驻留时间,称频率段为信道带宽。

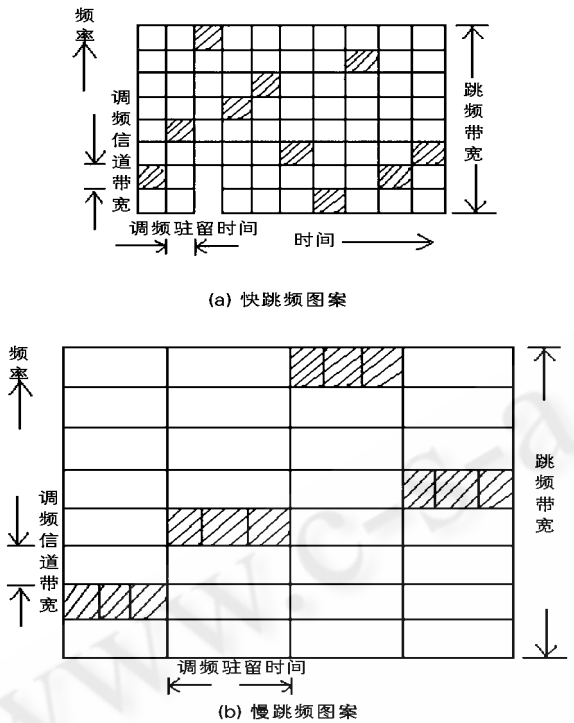


图 1　跳频图案

图1(b)所示则是一慢跳频图案,它是在一个跳频驻留时间内传送多个(此处3个)码位(比特)的信息。在时频域这个"模盘"上的一种布子方案就是一个跳频图案。当通信收发双方的跳频图案完全一致时,就可以建立跳频通信了。图2所示就是建立跳频通信的示意图。

其中t表示时间,s表示空间,f表示频率。当收、发双方在空间上相距一定距离时,只要时频域上的跳额图案完全相重合,就表示收、发双方同步跳频地进行通信。

3.2 跳频通信的抗干扰性能

通信收、发双方的跳频图案是事先约定好的,或者是由发方通知收方的。这个跳频图案是攻击者所不知道的。攻击者若想干扰跳频通信,有几种策略可供选择:

干扰方式1,在某一个频率上施放长时间的大功率的干扰,即单频干扰。

干扰方式2,在某几个频率上施放长时间大功率的干扰,即多频干扰。

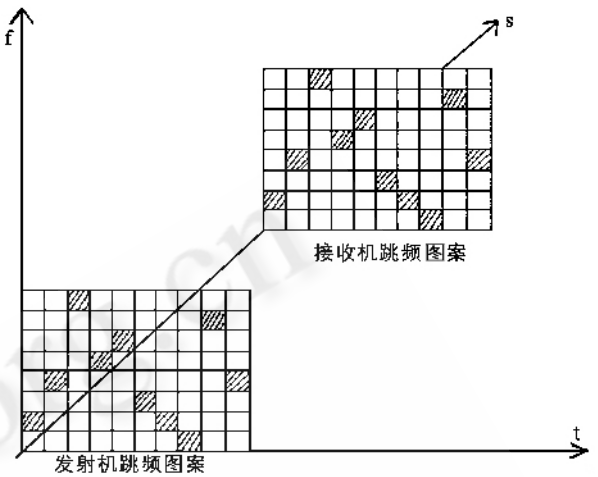


图 2　跳频发射与接收图案

干扰方式3;在连续的几个频带上施放长时间大功率的干扰,称作部分频带来扰。

干扰方式4,在不同时间内在不同的频率上施放大功率的干扰。

干扰方式5,依照跳频图案的规律跟踪施放大功率的干扰。

这些干扰方式和跳频通信的关系正像二人对奕时相互"出子"一样,当双方的"布子"落在时一频域棋盘内的同一小格时,则干扰有效。因此,跟踪跳频图案施放的干扰策略就是最佳的干扰跳频通信的策略了。

图3给出了方式1和方式4的干扰策略与跳频图案的关系。

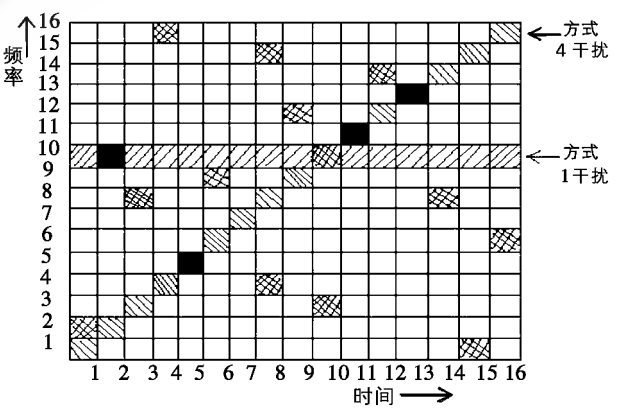


图 3　跳频干扰

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

图中示出一种跳频图案,方式 1 干扰策略是在时间上连续的施放一个窄带干扰,即第 10 个频率段以斜线表示的干扰带;方式 4 干扰策略是在第一个时间段用第一个频率段进行干扰,第二个时间段用第二个频率段进行干扰,依次下去,就形成了沿时频域模盘对角线上的干扰带。跳频图案中受到这两种干扰时就用全黑色方块来表示。由图中可以看出,干扰方式 1 只干扰了一个跳频驻留时间的通信,而干扰方式 4 则干扰了三个跳频驻留时间的通信。

跳频图案的不同,其干扰的效果也不尽相同。当跳频图案的随机性越大时,跳频抗干扰的能力就越强;"棋盘"越大时,即频率和时间的乘积越大时,可容纳的随机图案也越多,跳频图案本身的随机性也越大,从而抗干扰能力也越强。所谓抗干扰能力强,实际上是指碰到干扰的概率小。

4　无线局域网扩频技术对比

现行的无线局域网在抑制干扰的方面主要采用直接序列扩频技术(DS－SS),对于局域网采用跳频技术通过一下比较会发现在哪些方面可以改善系统安全性能和通信质量。

4.1　直序扩频和跳频扩频比较

扩频技术的最大优点在于较强的抗干扰能力,以及保密、多址、组网、抗多径等,但由于各种扩频方式的抗干扰等机理不同,因而各有其长处与不足,很难笼统断言某一种扩频方式比其他的扩频方式更优。对扩频方式的比较只能是在一定条件下对各种扩频方式综合考虑,从而得出某种结论,以便人们在扩频方式的选择上作一参考。

直扩和跳频技术的抗干扰机理不同,直扩系统靠伪随机码的相关处理,降低进入解调器的干扰功率来达到抗干扰的目的;而跳频系统是靠载频的随机跳变,躲避干扰,将干扰排斥在接收通道以外来达到抗干扰的目的。因此,这两者都具有很强的抗干扰的能力,也各有自己的特点,也存在自身的不足,现将直扩和跳频技术的性能作一比较。

(1) 抗强的定频干扰。由直扩抗干扰的机理可知,直扩抗干扰是通过相关解扩取得处理增益来达到抗干扰目的的,但超过了干扰容限的定频干扰将会导致直扩系统的通信中断或性能急剧恶化。而跳频系统是采用躲避的方法抗干扰,强的定频干扰只能干扰跳频系统的一个或几个频率,若跳频系统的频道数很大,则对系统性能的影响是不严重的。因此,在抗强的定频干扰上,跳频系统比直扩系统优越。

(2) 抗衰落。由于直扩系统的射频带宽很宽,小部分频谱衰落不会使信号频谱产生严重的畸变,而对跳频系统而言,频率选择性衰落将导致若干个频率受到影响,导致系统性能的恶化。

(3) 抗多径干扰。多径问题是在移动通信、室内通信等系统中必须考虑的问题。多径干扰是由于电波传播过程中遇到的各种反射体(如高山、建筑物、墙壁、天花板等)引起的反射或散射。由于直扩系统采用伪随机码的相关解扩,只要多径时延大于一个伪随机码的切普宽度,这种多径就不能对直扩系统形成干扰,直扩系统甚至可以利用这些干扰能量来提高系统的性能。而跳频系统则不然,跳频系统要抗多径干扰,则要求每一跳的驻留时间很短,即要求快跳频,在多径信号没有到来之前接收机已开始接收下一跳信号。

(4) "远－近"效应。"远－近"效应如图 4 右图所示。有两对收发信机,正常工作时,接收机 1 接收发射机 1 发射的信号,接收机 2 接收发射机 2 的信号。现接收机 1 移动到 A 点,受到附近发射机 2 的干扰,而接收机 1 距发射机 1 很远,这样接收机 1 收到的干扰信号电平远远大于有用信号的电平,这就是"远－近"效应。"远－近"效应对直扩系统的影响很大,而对跳频系统的影响就小得多。这是因为虽然直扩系统有一定的处理增益,但是由于有用信号的路径衰减很大,因而构成的威胁就小得多。

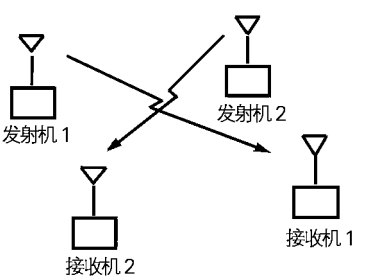


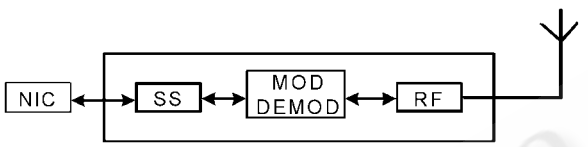
图 4　远近效应

(5) 组网能力。扩频技术本身就具有一种多址能力－SSMA,属于 CDMA,直扩系统和跳频系统都具有很强的组网能力。从频谱利用率上来看,直扩系统和

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

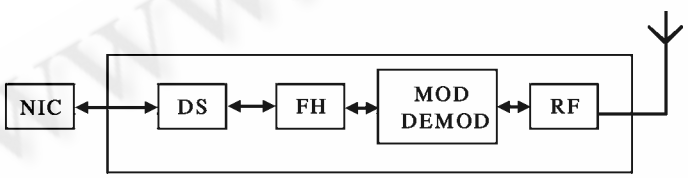
跳频系统的频谱利用率比单频单信道系统还要高。就直扩和跳频系统而言,跳频系统的组网能力和频谱利用率略高于直扩系统。

(6) 与窄带系统的兼容性。直扩系统是一个宽带系统,虽然可与窄带系统电磁兼容,但不能与其建立通信。另外,对模拟信源(如话音)需作预先处理(如语声编码后),才可接入直扩系统。而对跳频系统而言,由于它是瞬时窄带系统,它易于与目前的窄带通信系统兼容。



NIC　网络接口单元　　SS　扩频/解扩单元
MOD/DEMOD 中频调制解调器　　RF　射频单元

图 5　无线网卡



NIC 网络接口单元　　DS 直接序列扩频 FH　跳频模块
MOD/DEMOD 中频调制解调器　　RF 射频单元

图 6　无线跳频网卡

5　跳频通信在局域网中可行性分析

在考虑在无线网中实施跳频通信首先考虑的就是无线局域网中是否存在跳频通信实现的条件,换句话说就是频率资源是否够用;其次就是实现跳频通信会对现有系统的影响。

5.1　频率资源

无线局域网通信所采用的频带为 5.15 – 5.35GHz 和 5.725 – 5.875GHz 的频带和 2.4GHz 频带。采用跳频通信,在频率间隔不重叠的情况下,可同时采用的跳频数 802.11a——58333;802.11b——166666,,如采用频率重叠,频率储备将翻一番,并且为减小干扰对信号的影响,采用增加冗余度的办法来判定信息的真实性,每个终端采用五选三的判决(即每一帧信息有五个频率分别传送,其中三次接受的内容相同,则此相同内容为正确信息)。而且,在无线局域网的标准制定时考虑电磁污染,其有效半径最大为 100m,在如此空间里,跳频通信的容量已经超过千个,因此系统拥有储存了足够的频率资源可供使用。

5.2　系统影响

采用跳频通信对现有系统的影响主要是在系统耗时和硬件开销。一块无线网卡的结构如图 5。

针对现有网卡的硬件加上跳频改造其结构改变如图 6。

从电路改造上看,系统开销并不大,在系统设计中增加一个跳频模块即可实现。与此同时,由于模块的加入使得系统不能够与现有的网卡兼容,这一变化对于现有无线局域网络来讲,正好可以满足非公开的局域网需求,例如:政府的内部网、国家机关的局域网。而且各网络之间也可以通过共享广播跳频图案的方式实现广播通信。

6　小结

通过以上的阐述,可以得到一个结论,在无线局域网内采用跳频通信可以有效的分割网络,并且在现有条件下,并不需要改造网络结构就可以加强网络的安全性能,网络的跳频改造通过更换网卡就可以实现,因此这一方法是可行的,也是有效的。

参考文献

1 《无线网络安全防护》,Christian Barnes,刘□译,机械工业出版社,2003。

2 《扩频通信》,查光明,西安电子科技大学出版社,1990。

3 http://www.bnc.com.cn/jszc/jszc – wxbjzs15.htm,直序扩频和跳频扩频比较,2004.1。

4 《通信网的安全》,王育民、刘建伟,西安电子科技大学出版社,1999。

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn