TKIP 的实现及其改进算法

Implement and Improved Algorithm of TKIP

邓　光　（中国科学院研究生院 北京 100039）
鲁士文　（中国科学院计算技术研究所 北京 100080）

摘　要: 安全问题已经成为无线局域网推广应用的一个关键问题。本文致力于实现无线局域网安全的关键协议并提高相关安全强度。首先详述了在 IEEE 802.11 无线局域网中使用的临时密钥完整性协议(TKIP)的过程;实现了 TKIP 协议算法的关键技术,同时我们分析指出:虽然使用 TKIP 可以代替有线对等保密协议(WEP),不必替换现有的硬件产品,但是它并没有足够的安全强度去完全解决无线局域网中所有的数据加密问题;最后我们给出了 TKIP 的一个改进算法,该改进算法可以提高 TKIP 的安全强度。能够在理论上指导用户如何构造满足所需安全性能的 WLAN 数据加密增强机制。

关键词: 无线局域网　加密　临时密钥完整性协议　IEEE 802.11i

1　引言

Wi－Fi Protected Access(WPA,Wi－Fi 保护访问)是 Wi－Fi 产业联盟提出的一种新的 WLAN 的安全方式,以取代安全性不足的 WEP。WPA 采用了基于动态密钥的生成方法及多级密钥管理机制,方便了 WLAN 的管理和维护。WPA 由认证、加密和数据完整性校验三个部分组成。目前 Wi－Fi 推荐的安全解决方案 WPA 以及 802.11i 标准均采用 TKIP 作为一种过渡安全解决方案。TKIP 与 WEP 一样基于 RC4 加密算法,但相比 WEP 算法,将 WEP 密钥的长度由 40 位加长到 128 位,初始化向量 IV 的长度由 24 位加长到 48 位,并对现有的 WEP 进行了改进,追加了四种算法:每包一密钥(Per－Packet Key)、消息完整性检查(MIC)、具有序列功能的初始向量和密钥生成和定期更新功能,这极大地提高了 WEP 加密的安全强度。虽然其所能提供的安全措施有限,不过它能使各种攻击变得比较困难。本文详细讨论 TKIP 数据加密协议,并给出一个改进的算法,能够提高 TKIP 的数个等级的安全强度。

2　TKIP 加解密机制

2.1　TKIP 加密机制

图 2.1 为 TKIP 的加密过程。从图可以看出 TKIP 的加密过程主要包括以下几个步骤:

2.1.1　MPDU 的生成:包括了消息完整性编码(Message Integrity Code,MIC)的产生和 MSDU 的分段两个部分。首先发送方在 MSDU 基础上计算 MIC,这是一个基于 MSDU 明文数据(Plaintext MSDU Data)的 HASH 值,将此 MIC 加到 MSDU 后面,作为 WEP 算法的输入 MPDU,如果有必要的话可以将其分成一个或多个明文 MPDU。

2.1.2 WEP 种子(WEP seeds)生成:这一步是为了弥补 WEP 静态共享密钥的缺陷。对于每个 MPDU,TKIP 都将计算出相应的 WEP seeds。WEP seeds 的生成主要包括两个密钥混合过程:第一阶段的密钥混合基于临时密钥(TemporaryKey,TK)生成一个临时的混合密钥(TTAK),TKIP 给每个新生成的 MPDU 分配一个递增加的 TKIP 序列计数器(TKIP sequence counter,TSC)值。值得注意的是,所有的来自同一个 MSDU 的 MPDU 使用的 TSC 值来自相同的计数空间。利用 TTAK,TK 和 TSC 做为第二阶段混合的输入即可得到用于 WEP 加密的 WEPseeds。

2.1.3　WEP 封装:TKIP 把从经过两次混合产生的种子密钥 WEP seed 分解成 WEP IV 和 RC4 密钥,然后把它和 MPDU 一起传给 WEP 进行加密。

总的来看,加密时的输入的有 TK,MIC Key,Plaintext MSDU Data,TSC,TA。TK,TSC 的和 TA 参与第一阶

段的混合,生成 TTAK ;TTAK 和 TSC,TK 经过第二阶段的混合生成 WEP seed,供 RC4 调用生成密钥流 ;同时,数据和 MIC Key 经过 Michael 函数 Hash 得到 Hash 值(MIC),然后与明文的 MSDU 和 MIC 串联行分段,每一个分段后的(MPDU)都对应着一个特定的 TSC,分段后的 MPDU 作为 WEP 协议的明文输入 RC4,与密钥流异或后生成密文。

2.2 TKIP 解密机制

图 2.2 为 TKIP 的解密过程。从图可以看出 TKIP 的解密过程与加密过程相反。在利用 WEP 解密 MPDU

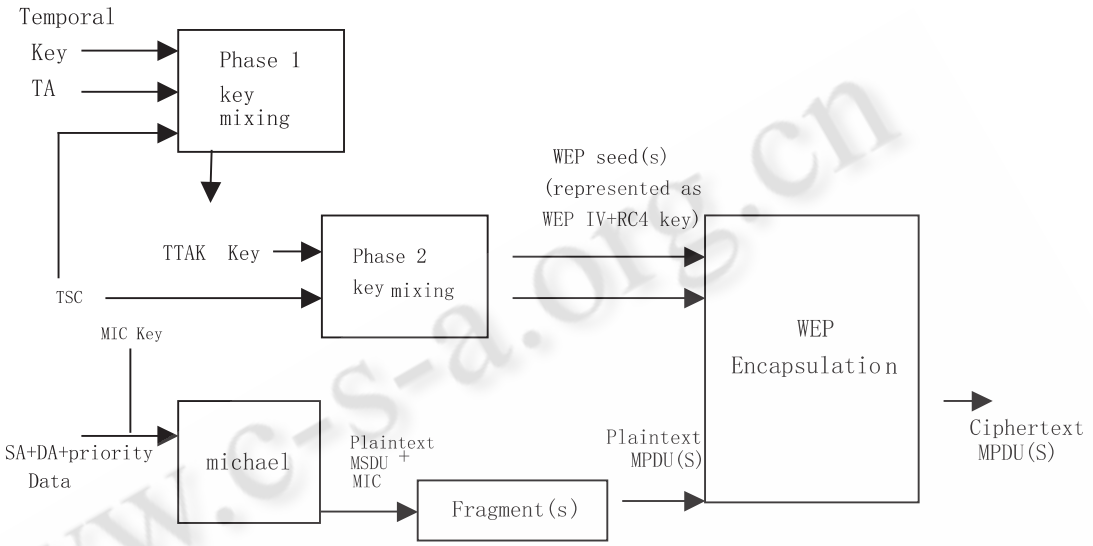

图 2.1　TKIP 的加密过程

之前,需要先从 WEP IV 和扩展的 IV 中提取出 TSC 序列号和密钥 ID。如果 TSC 不符合一定的排序规则,则该 MPDU 将被丢弃,否则根据 Key ID 定位 TK,然后通过两个阶段的混合函数来创建 WEP 种子。WEP 解密种子的生成方式和加密过程中的完全相同,这里不再赘述;接着,TKIP 把 WEP seed 分解成 WEP IV 和 RC4 Base Key 的形式,把他们和 MPDU 一起送入 WEP 解密器进行解密 如果 WEP ICV 检查正确,该 MPDU 被组装入 MSDU。MSDU 重组完后重新计算 MIC 值,然后将其和收到的 MIC 值逐位相比较。如果接收到和本地计算的 MIC 值相同,校验就成功,TKIP 就把 MSDU 传递给上层协议。如果 MIC 出错,将会认为校验失败,该数据包将被丢弃,并转入对策机制,执行规定的策略(countermeasure)。

2.3 TKIP MIC 函数

IEEE 802.11 WEP 设计中的缺点导致了它没能达到其保护数据传输不被窃听的目标。在最突出的 WEP 缺点中有一个就是缺少一种机制来防止消息伪造和遭受其它的主动攻击。为了防护主动攻击,TKIP 包括了 MIC 函数,即 Michael 函数。Michael 函数只提供了较弱的对伪造消息的保护,但是它制定了在多数遗留下来的硬件上可以获得的最好的性能。

Michael 函数产生一个 64 比特的 MIC。Michael 密钥由 64 比特组成,描绘成一个 8 字节序列 $k_0 \ldots k_7$。这个序列被转换成为两个 32 比特的字 K_0 和 K_1。在整个 Michael 函数设计中,所有字节和字之间的转换将使用 little – Endian 算法。

Michael 对每个 MSDU 进行操作,包括优先级,3 个保留字节,源地址和目的地址。一个 MSDU 由如下字节组成 m0...mn –1,其中 n 是 MSDU 的字节数,包括源地址,目的地址,优先级和数据区域。这个消息在末尾做了铺垫,即一个单独字节后面跟着 4 到 7 个 0 字节。零字节数可以选择以使得总的 MSDU 长度可以被 4 整除。末尾的铺垫没有随 MSDU 一起传送 ;只是用于方便最后的计算。MSDU 被转换成一个有序的 32 比特字 M0...Mn –1,其中 N = [(n +5)/4],其中[a]表示对 a 取整,M(N –1) =0,M(N –2) ≠0。

Michael 实现见参考文献[6],MIC 的值从密钥值开始,对每个消息字反复应用分组函数 b。算法循环 N 次,结果产生两个字(l,r)。Michael 中的分组函数 b

是一个 Feistel 型结构,具有交互的加和 XOR 运算,其中要用到 XSWAP 交换函数,用来交换两个最不重要的字节和最重要的字节。

2.4 TKIP 混合函数

混合函数有两个阶段:第一阶段混合相应的临时密钥 TK(对成的或者成组的)和发送者地址(TA)和 TSC,消除了各通讯方使用相同密钥的隐患。第二阶段混合第一个状态的输出和 TSC 以及 TK 来产生 WEP 种子,这也叫做针对每帧的密钥,把已知的弱密钥从 Per – Packet Key 中剔除。两阶段的过程可以总结如下:

TTAK←Phase1(TK,TA,TSC)

WEP seed←Phase2(TTAK,TK,TSC)

2.4.1 S – box

两个阶段都使用 S 盒子,S – BOX 是一个长为 2256 的二维数组。它替换一个 16 比特值成另外一个 16 比特值。

2.4.2 混合函数第一阶段密钥混合函数的第一阶段

Phase1 流程见参考文献[7]。Phase1 的输入为 48 比特 TA、128 比特 TK 和 32 比特的 TSC[2] ~ T SC[5],这些值均表示为 8 比特数组 输出为 80 比特的 TTAK[0] ~ TTAK[5] 的 16 比特数组。Phase1 使用 MK16 函数将两个 8 比特字节以 Little Endian 格式合并为 16 比特字,其中 S 为上述的 S – box。PHASE1 分为 STEP1 和 STEP2,STEP1 用 TSC[2] ~ TSC[5] 和 TA 对 TTAK 进行初始填充,STEP2 中采用一个 PHASE1 LOOP COUNT(通常取 8)轮的不平衡 Feistel 结构,使得 TTAK 与 TK 充分混合。

在第一阶段,通过引入本地 MIC 地址,使具有相同 TK 的 STA,AP 产生不同的密钥。

2.4.3 混合函数第二阶段 密钥混合函数的第二阶段

Phase2 流程见参考文献[7],主要操作分为 STEP1,STEP2 和 STEP3。STEP1 用 TTAK 和 TSC0,TSC1 初始填充

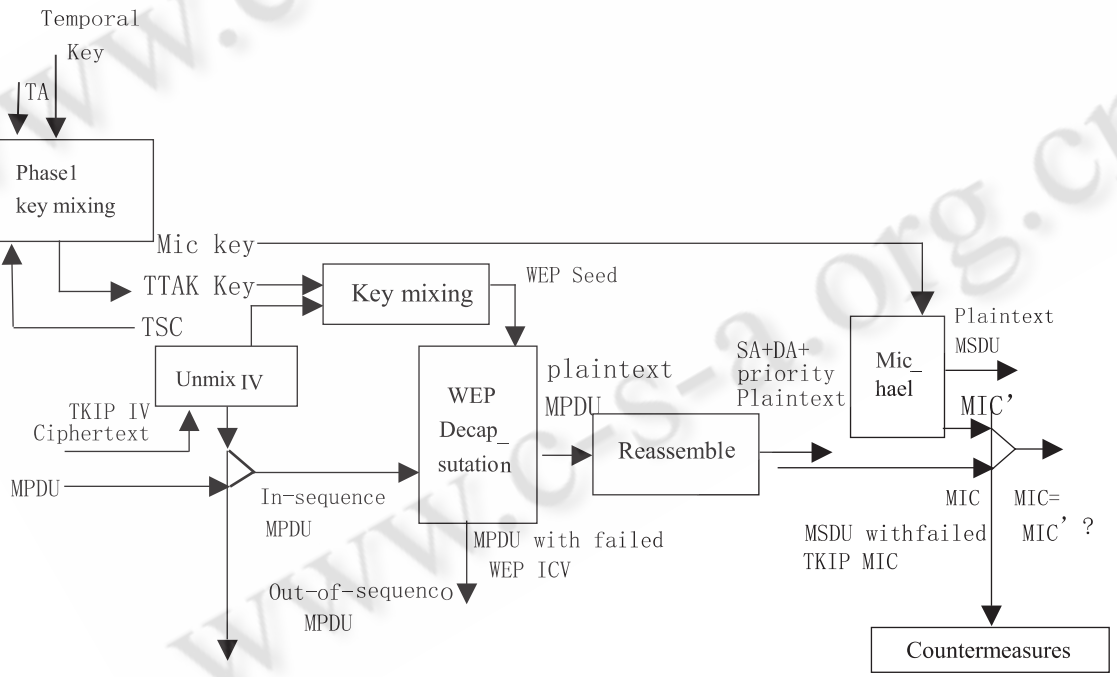

图 2.2 TKIP 的解密过程

PPK。STEP2 中首先将 TK 和 PPK 混合,然后使用右循环一位函数 RotR1 以消除最低位比特之间的简单关系。至此当 TTAK 一定时,96 比特输入(TA,TSC[0]... TSC[5])唯一确定一个 96 比特输出 PPK,PPK 可以看作(TA,TSC[0]... TSC[5])在 TTAK 控制下的置换。在 STEP3 中按 WEP 的密钥格式将 TSC[0],TSC[1] 和 PPK 填入 K 中。

通过两个阶段的运算,生成了 128 位的 Per – Packet Key(RC4,Key),Per – Packet Key(RC4,Key)的前三个字节对应于 WEP IV,后 13 个字节对应于 WEP Base Key,现存的 WEP 硬件将它们级联成为 Per – Packet Key(RC4,Key)。

3 TKIP 改进算法

根据文献[8]给出的结果,我们知道 WEP 加密机制安全性最差,在输出 4000 多个数据包时,其被攻破的可能性接近 1,TKIP 协议的安全强度比 WEP 提高约 4 个等量级,当输出数据包为 107 时,被攻破的可能性为 0.6。这意味着其密钥的生命周期约为 2.4×10^4 小时,在实际环境中基本上满足需求的。但是,TKIP 协议的安全强度并不是太高,事实上在相同密钥长度下,TKIP 协议的安全强度要比 RC4 算法低。这主要有两个原因,加密机制跟密钥更新模块的安全强度有关。若密钥更新模块的安全性能远远低于 RC4 算法,则最终的安全强度与密钥更新模块的安全强度近似相等,而 TSC 只有 48 位。另外,为了提高 TKIP 协议的运算性能,密钥混合函数又分成两个阶段,第一阶段每发送 2^{16} 个数据包才会执行一次,这对安全性能也产生了一定影响。

为了提高 TKIP 的安全性能,我们在这里提出一个改进算法,用以克服 TKIP 协议的二阶段结构造成的安全强度低的问题。其主要思路是保持 TKIP 二阶段密钥混合结构不变,通过扩大 TKIP 序列计数器(TSC)的计数空间的方式来提高 TKIP 算法的安全强度:我们将 TSC 由 48 比特扩展为 128 比特。

其混合函数设计如下:第一阶段混合相应的临时密钥 TK(对成的或者成组的)和发送者地址(TA)和 TSC。第二阶段混合第一个状态的输出和 TSC 以及 TK 来产生 WEP 种子。

3.1 密钥混合函数的第一阶段流程

改进后的 Phase1 的流程与改进前的 Phase1 流程基本相同,不过输入为 48 比特 TA、128 比特 TK 和 112 比特的 TSC[2] ~ TSC[15],这些值均表示为 8 比特数组;输出为 128 比特的 TTAK[0] ~ TTAK[7] 的 16 比特数组。MK16 函数将两个 8 比特字节以 Little Endian 格式合并为 16 比特字。在 PHASE1 STEP1 中用 TSC[2] ~ TSC[15] 和 TA 对 TTAK 进行初始填充,在 PHASE1 STEP2 中采用一个 PHASE1 LOOP COUNT(通常取 8)轮的不平衡 Feistel 结构,使得 TTAK 与 TK 充分混合。

3.2 密钥混合函数的第二阶段流程

改进后的 Phase2 的流程与改进前的 Phase2 流程基本相同,密钥混合函数以 128 比特的 TTAK、128 比特的 TK 以及 TSC[0],TSC[1] 为输入,128 比特的 WEP-Seed 为输出(表示为 8 比特 ×16 的数组),中间过程用到 128 比特的 PPK(表示为 16 比特 ×8 的数组)。STEP1 用 TTAK 和 TSC0,T SC1 初始填充 PPK。STEP2 用于将 TK 和 PPK 混合,然后向右移一位以消除最低位比特之间的简单关系。至此当 TTAK 一定时,(TA,TSC[0]... TSC[15])唯一确定一个 128 比特输出 PPK,PPK 可以看作(TA,TSC[0]... TSC[15])在 TTAK 控制下的置换。在 STEP3 中按 WEP 的密钥格式将 TSC[0],TSC[1] 和 PPK 填入 K 中。

4 结束语

可以证明,TKIP 协议的安全强度比 WEP 提高约 4 个等量级,而改进的 TKIP 协议的算法由于将 TSC 由 48 比特扩展为 128 比特,安全性能要比同样密钥长度的 RC4 算法本身提高 3 个等量级。无线局域网的数据加密技术是安全技术的关键,是基于密码学算法基础的,三个著名的数学难题(整数分解、离散对数和椭圆曲线上的离散对数)的研究成果建立了现代公钥密码学的基础,发展出了各种加密技术。从安全协议的设计与实现角度看,无线局域网安全体系的设计与架构不仅需要考虑安全性,还需要考虑很多其他因素,比如无线环境的不稳定性对安全协议执行的影响,用户漫游和快速切换是认证延时的限制以及协议执行的效率问题,漫游时的用户管理和认证,对网络质量服务的支持等。无线局域网安全是一个需要深入研究的课题、要由多方进行共同探讨,而它的发展也必将推动无线局域网的广泛应用。

参考文献

1 Canetti R and Krawczyk H. Security analysis of ike's signature – based key – exchange protocol. In Advances in Cryptology – Proceedings of CRYPTO '02, Lecture Notes in Computer Science 2442. Spinger Verlag, 2002. 143 – 161.

2 Arup A, Chatschik B, Archan M, et al. ts – pwlan: a value – add system for providingtiered wireless services in public hot – spots. In. IEEE International Conference on Communications(ICC '03). 2003(1): 193 – 197.(下转第 19 页)

(上接第 39 页)

3 Anton B, Bullock B, and Short J. Best. current practices for wireless internet service provider(wisp) roaming. Technical report, WiFi Alliance, February 2003.

4 曹秀英,耿嘉,沈平等编著. 无线局域网安全系统. 北京:电子工业出版社,2004.

5 Wi - Fi Alliance Introduces Next Generation of Wi - Fi Security. Wi - Fi Alliance (2004 - 09 - 01).

6 马建峰,朱建明等编著. 无线局域网安全 - 方法与技术. 北京:机械工业出版社. 2005. 169 - 172.

7 Retrieved from " http://en. wikipedia. org/wiki/Temporal_Key_Integrity_Protocol" IEEE P802. 11i D3. 0, Specification for Enhanced Security. http://www. cs. und. edu/mhshin/doc/802. 11/802. 11i - D3. 0. pdf, November 2002.

8 J. R. Walker. Unsafe at any key size; an analysis of the wep encapsulation. IEEE Document 802. 11 - 00/362, October 2000.