ETC中加密算法的软件实现及一些问题

郑州大学信息工程学院　张　元　王香丽

一、ETC及其安全机制

ETC(电子不停车收费系统)是一种用于公路、大桥和隧道的电子自动收费系统。它通过路侧天线与车载电子标签之间的专用短程通讯,在不需要司机停车和其它收费人员采取任何操作的情况下,自动完成收费处理全过程。在ETC不停车收费系统中,路侧天线与车载电子标签之间的信息交互是通过国际上专门开发的适用于ITS(智能交通系统)领域的道路与车辆之间的通信协议,即专用短程通信(DSRC)协议。

在现有的DSRC标准中,采用了简单的加密方式。为了保证在短程通信中的信息安全,在电子标签与路边设备进行通信前要进行身份认证。在ETC中采用的是双向认证机制。当路边设备向车载设备读写数据时,首先必须提供一个有效的访问身份码(Access Cretential);同时在路边设备接受数据前,车载设备必须提供一个有效的信息鉴别码(Attribute Authentication)。在双向认证的过程中,电子标签的许可访问码(Access Cretential)以及信息鉴别码(Attribute Authentication)是基于单个的DES运算产生的,其加密密钥是对主密钥基于TDES加密产生的。

二、认证码的产生过程

访问身份码(Access Cretential)是一个4字节长的串,是用数据元访问密钥(Element Access Key,简称EAcK)进行DES加密产生的。为了提高安全性,EAcK是由一个数据元访问主密钥(Master Element Access Key)对2个字节的OBEGroupID进行TDES加密产生的。主密钥只存在于RSE中。EAcK被计算出并连同OBEGroupID一起被储存在OBE中。Access Cretential则是由EAcK对一个随机数RndOBE进行DES加密所得,计算如下所示:

EAcK=TDES(MEAcK,OBEGroupID||OBEGroupID||OBEGroupID||OBEGroupID)

OUTput=DES(EAcK,RndOBE||00 00 00 00$_{16}$)

访问身份码则取OUTput的最左边4个字节。

信息鉴别码(Attribute Authenticator)也是一个4字节长的串,是用数据元鉴别密钥(Element Authentication Keys,简称EAuK)进行DES加密产生的,同样为了提高安全性,EAuK是由一个数据元鉴别主

之,如果解码失败,则需要增加编码冗余量,直到解码正确为止。显然,编码冗余度的增加必将导致有效数据速率的降低和延时的增加。

EDGE技术的核心就是链路自适应,不仅编码方案可以选择,调制方式也不再是固定的一种GMSK方式,而是引入了另一种调制方式,即八进制移相键控(8-PSK)。这种调制方式能提供更高的比特率和频谱效率,且实现复杂度属于中等。GMSK和8-PSK的符号速率都是271kbit/s,但由于8-PSK将GMSK的信号空间从2扩展到8,因此每个符号可以包括的信息是GMSK的4倍。为了保证链路的健壮性,EDGE对两种调制方案和几种编码方案进行组合,形成了9种不同的传输模式。EDGE标准支持的链路自适应算法包括周期性的对下行链路质量的测量和报告以及为下一个要传输的内容选择新的调制和编码方法等。

对于链路自适应技术来讲,传输模式的选择策略是核心算法,准确高效的选择算法是该技术得以成功运用的关键。

三、递增冗余传输方式 IR

EDGE中另外一种对付链路质量变化的方式是逐步增加冗余度。在这种方式中,信息刚开始传输时,采用纠错能力较低的编码方式,如果接收端解码正确,则能得到比较高的信息码率。反之,如果解码失败,则需要增加编码冗余量,直到解码正确为止。显然,编码冗余度的增加将导致有效数据速率的降低和延时的增加。EDGE系统的最高数据传输率可达473.6kbit/s。结合以上特点,EDGE可以被视为一个提供高比特率、并且因此促进蜂窝移动系统向第三代功能演进的、有效的通用无线接口技术。EDGE的运用必能弥补3G到来前的空缺,为目前还未成熟的3G进一步完善争取时间,并且为3G市场培养用户习惯,让我们期待EDGE的到来吧。

密钥 MEAuK（Master Authentication Keys）对 ContractSerialNumber 和 EFC-ContextMark 的头三个字节 ContractProvider 进行 TDES 加密产生的。这个密钥对于 OBE 来说是唯一的。RSE 发出的 GET-STAMPED 请求，附带一个随机数（RndRSE）和一个 OBE 的密钥（key ref），OBE 将会产生一个经过加密的校验数作为认证数(authenticator)，此数是 EAuK 对随机数 RndRSE 和设备号 EquipmentStatus 进行 DES 加密产生的，计算如下所示：

EAuK =TDES （MEAuK，ContrackSerialNumber ‖ ContractProvider‖00）。另外，OBE 使用了 CBC（密码分组连接）加密模式的 DES 加密。

数据将被分成每 8 个字节的块 D1，D2…D（n-1）。剩下的位左置，右边补 0，产生最后一个 8 字节块。具体如下：

第一个块 D1 被 EAuK 加密，输出 C1；

C1 与 D2 异或，然后由 EAuK 加密，输出 C2；

C2 与 D3 异或，然后由 EAuK 加密，输出 C3；

…

n 最后 C（n-1）与 D（n）异或，由 EAuK 加密；n+1 输出 MAC_{init}。如图 1 所示：

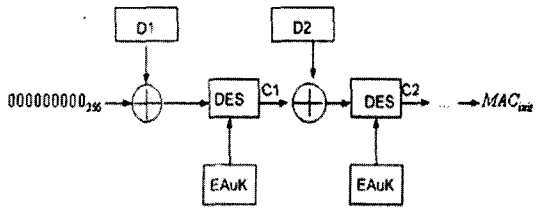

图 1

Attribute Authenticator 取 MAC_{init} 左边的四个字节。

三、DES 加密算法及其软件的实现

数据加密标准（DES）是一种用 56 位密钥来加密 64 位数据的方法，它被应用于很多需要安全加密的场合。DES 密码体制的安全性不依赖于算法的保密，其安全性仅以加密密钥的保密为基础实现经济，运行有效，并且适用于多种完全不同的应用。

DES 对 64_ 位的明文分组进行操作。通过一个初始置换，将明文分组分成左半部分和右半部分，各 32 位长。然后进行 16 轮完全相同的运算，包括左移，异或，扩展以及 SP 盒置换等等，在运算过程中数据与密钥相结合。最后进行一个末置换就完成了算法。

我使用的是编程语言 C 来实现基于 CBC 加密模式的 DES 加解密程序。该程序的特点是在此程序中设置了加解密模式，可同时完成加解密工作。在 CBC 加密模式中加入了初始向量 ip，它可以唯一化向量。通常我们可以使用时间和随机串来作为初始向量。将 DES 加密算法中的 S 盒置换和 P 盒替代合成一个 SP 盒，这样优化了 DES 算法，节约了 CPU 的计算时间，提高了 DES 算法的实现速度。经查有关资料，一般的 DES 加密在计算机上的速度如果是 0.04MB/S 的话，使用了 SP 盒置换的 DES 加密在相同的计算机上加密速度约为 3.3MB/S，提高了 80 倍之多。

四、ETC 保密通信中的一些问题

简单加密方式是 DSRC 标准专用的、最低限度的抗无线干扰措施，也从一定程度上提高了可靠性。但是在安全保密问题上，不同应用对于安全性要求不尽相同，虽然 DSRC 协议采用了简单的加密和检错功能，但无法满足对安全性有特殊要求的应用场合。在这里我们考虑以下几个方面：

实时性：对于嵌入式系统，由于应用系统中软件运行的时间耗费，常常不能满足限定的时间响应要求，所以实时性的问题也是很重要的。在这里采用了 DES 和 TDES 加密，其安全性得到很大的增强。但是它是静态加密方法，不利于信息的实时处理。所以我们可以考虑采用混沌加密等动态加密方法，应用在实时性要求较高的场合。

效率特性：一般地情况下，要求模式的效率不能明显的低于基础的密码。在这里使用的是 CBC 加密模式。它对于加密算法安全性的增加很有意义。其速度与分组密码相同，解密是并行的且有随机存储的特性。对于基于软件的加密，CBC 是最好的选择。

容错性：对于密码，在一些应用时需要并行加解密的，而在其它一些应用时则需要能够尽可能多的进行一些预处理。对于解密，能够从位错误中恢复这一点也是很重要的。对于 CBC 这种加密模式，对于位错误，它可以很快的自恢复。但是对于同步错误（即：位的丢失或增加），它却不能恢复。这样就直接影响到效率的问题。所以我们也可以考虑别的加密模式来替代 CBC 这种加密模式。

主要参考文献

[1]吴世忠，祝世雄等译。应用密码学协议、算法与 C 源程序（M）。北京：机械工业出版社。2000

[2]李海泉，李健。计算机网络安全与加密技术[M]。北京：科学出版社。2001

[3]陈良。《一种优化的 DES 算法》[J]。计算机工程与应用。2004.6

[4]Alcatel，Combitech，Kapsch。Telematics Applications Programme TR 4001 A1（S）。CSSI。1999