基于混沌和 WEP 的无线传感器网络加密研究

卢政桥

(中国航发控制系统研究所软件部 江苏 无锡 214063)

摘 要 无线传感器网络是一个易受监听和干扰的开放系统,传感器节点的 CPU 计算速度、字长和存储空间有限,无法像 pc 级那样执行运行成本较大的加密算法,而运行成本较低的 WEP、THIP 等无线网加密算法已被证实存在密钥强度等问题。文中提出了一种基于 WEP 和混沌序列结合的加密协议,通过混沌序列作为子密钥的生成算法,可以在不增加时间复杂度和空间复杂度的情况下,同时利用混沌序列映射提高密钥随机性,回避 WEP 协议的密钥重复问题,增加破译的难度。

关键词 混沌序列,嵌入式,加密

中图法分类号 TP393.1 **文献标识码** A

Encryption of Wireless Sensor Networks Based on Chaos and WEP

LU Zheng-qiao

(Aero Engine Control System Institute of China, Wuxi, Jiangsu 214063, China)

Abstract Wireless sensor network is an open system which is easy to be monitored and disturbed. The CPU of sensor nodes has limited computing speed, word length and storage space. It is impossible to execute the encryption algorithm with high running cost like PC level. The encryption algorithm of wireless network such as WEP and THIP with low running cost has been proved to have the problem of key strength and so on. This paper proposes an encryption protocol based on the combination of WEP and chaotic sequence. By using chaotic sequence as a sub-key generation algorithm, the key randomness can be improved by using chaotic sequence mapping without increasing the time complexity and space complexity, avoiding the key duplication problem of WEP protocol and increasing the difficulty of deciphering.

Keywords Chaotic queues, Embedded, Encryption

1 引言

近年来,随着网络技术的飞速发展,无线传感器网络(WSN)已被广泛地应用于工业控制领域。无线传感器网络由一组传感器和基站(BS)组成。传感器从它工作的环境获取数据,并将该数据发送到 BS,BS 记录和分析数据并形成系统的目标数据。

作为工作在无线网络中的机制,WSNs 可能会从不安全的来源收到信息。攻击者可以用回放攻击造成网络信息堵塞、窃听并尝试破解信息、蛮力破解 WSN 的保护密码、使用拒绝服务(DoS)的形式使合法用户得不到资源。

本文讨论利用嵌入式控制器搭建能够抵抗攻击的无线传感器网络。

2 传感器网络保护措施的难点

为了保护数据转换,研究人员已经尝试了许多技术来确保无线传感器网络的安全性,例如扩频方法,其中初始传输带宽是"展开"或扩展的,以便为传输消息的部分或分组使用部分扩展带宽。该方法可用于对抗物理层上的 DoS 攻击,缺点是需要较为复杂的硬件支持。

消息传输容易受到攻击,如干扰信号或重放攻击。目前研究人员已经提出了许多广播认证技术来确保传输。对于传输的干扰,一种称为跳频扩频的技术,可以让传输"跳过"多个频率信道来消除被堵塞的频率。这种技术及其改进的技术在消除信号干扰方面是有效的,但是它不适用大规模网络。目前可以通过时间戳消息和私钥/公钥基础措施来有效地应对重放攻击。

许多嵌入式系统受限于它所操作的环境和拥有的资源,面临以下一些挑战,因此不能直接照搬桌面系统的安全实现方式。首先是计算处理能力的差距,与桌面计算机的处理能力相比,嵌入式系统可用的计算能力是非常有限的,例如,使用 2.6GHzPentium 4 处理器的桌面计算机与使用 Intel StrongARM 1100 处理器的嵌入式控制器相比,前者可以处理 2890MI/s 条指令(注:MI/S 是每秒百万条指令数),而后者在最快的频率 206 MHz 下仅仅处理 235 MI/S 条指令。对于现在已有的一些通过密钥算法(公钥、Hash 函数、私钥)实现的加密算法,它们要求比较高的计算能力,例如,3DEs(三重数据加密标准)加密/解密,它的计算速度要求为 651.3 MI/S。因此,在嵌入式系统中出现了常用加密算法的要求与嵌入式控制器可用的处理能力不匹配的问题,而且随着数据传输速率的提高和更复杂密钥算法的使用,这种不匹配将更加明显[1]。其次是字长的问题,受限于成本和工作环境等,很多嵌入式的控制器处理器,采用了字长有限的型号,难以保存和计算字长较多的密钥算法[2]。

卢政桥 硕士生,主要研究方向为数字控制、软件实现,E-mail:448207632@qq.com(通信作者)。

3　现有保护机制

3.1　无线网保护机制

现有无线网络机制为 802.11,多使用基于 RC4 加密算法为核心的 WEP 加密机制,用出厂时设置的密钥矩阵作为密钥发生器供 RC4 算法使用。

RC4 算法是一种轻量级加密算法。其主要流程是通过密钥生成伪随机的队列,再通过 xor 算法用伪随机的队列将明文处理成没有随机性的密文,加解密效率高,实现简单。当 RC4 的密钥长度达到 128 比特时,用暴力法搜索密钥是不可行的,也没有其他有效的攻击方法可以针对 128 比特密钥的 RC4 加密算法,可以保障较高的安全性[3]。

RC4 加密算法的缺点主要是对密钥空间的需求较高。RC4 加密算法采用 xor 作为加密的核心步骤,采用使用这种方式的加密算法时,一旦密钥出现了重复,密文就有被破解的可能。

WEP 主要靠 24 位初始化向量 IV(下文简称 IV)和 40 位密钥产生伪随机位流,24 位 IV 的密钥空间有限,在高频通讯中很容易就用尽。对 RC4 的研究发现,存在特殊格式的 IV,生成的位流中初始字节和密钥的几个字节存在很强的相关性,导致密钥信息被泄露[4]。

针对这一问题,新机制 TKIP 在 WEP 密码外扩展动态密码,外加 48 位序列号就可以解决密钥碰撞的问题,也可以防范重放攻击,但目前以 RC4 为核心的 WEP 和 TKIP 等协议因为密钥空间不足正在被下一代标准 IEEE 802.11i 淘汰[3]。IEEE 802.11i 采用了以 AES 为核心的加密算法,这种加密算法的加密成本更高,需要更高性能的硬件支持。

3.2　WEP 加密协议

WEP 协议采用 RC4 加密算法,在协议中没有对密钥的生成和更新做出规定,在使用过程中很多厂商都采用静态密钥的方式开始直接通讯。对静态密钥的更新需要对所有的 AP 和客户端进行手动设定,因此很多应用中静态密钥很少甚至没有更新过。伪随机位流的变化主要依赖于通过 IV 的变化,IV 又要通过明文附加在密文头部一起传输,可以被直接监听,从而被分析或攻破。2001 年,ATST 实验室通过手机弱密钥的 IV 样本成功破译出静态密钥。

3.3　混沌序列

混沌序列是数学领域的一个现象,它具有对初始条件的敏感性和系统变化的不可预测性,混沌序列的特性具有非周期和类似随机的过程[5]。由于这个特性,混沌序列被应用于通信保密领域[6-8],目前混沌序列已经在 DES 加密中尝试作为初始密钥,有较好的保密性[9-10]。

在混沌序列中,最常用的是移位逻辑斯蒂映射(Logistic 映射),它的映射关系式为:

$$X_{n+1}=uX_n(1-X_n),u\in(0,4),X_n\in[0,1]$$

要使 Logistic 映射出现随机性,u 的取值范围主要有:(3.570～3.582),(3.584～3.605),(3.607～3.626),(3.635～3.655),(3.657～3.672),(3.674～3.701),(3.703～3.738),(3.744～3.828),(3.850～3.854),(3.857～3.905),(3.907～3.960),(3.962,4.000)[11]。

经实验验证,初始值相差 10^{-16} 时,生成的随机序列在迭代 60 次左右时出现了明显的差异,因此 start 应从 60 次以上取值[12]。

4　协议设计

WEP 的问题主要在于密钥空间有限、握手时明文专递密钥等。在 WEP 基础上对协议进行改进,设计满足无线传感器网络的加密协议。

4.1　加密设计

在加密传输过程中,WEP 存在密钥向量不足的情况。WEP 通过有限位数的初始化向量和密钥产生伪随机位流,该方式容易出现密钥空间用尽的情况,而单纯地增加密钥长度会增加加密成本。因此选择混沌序列随机算法替代 RC4 密钥发生器,使用更短长度的密钥生成相关性更低的伪随机队列。混沌序列的参数由 X_0(Logistic 的迭代起始值)、u(Logistic 的控制参数)、start(Logistic 的起始位置)组成。其中,u 以固定值写入终端和 AP 中,X_0,start 在每次起动时由终端生成并通过握手发送给 AP。

加密和解密过程中,软件加载 X_0,u 和 start 生成混沌序列,由于 Logistic 队列的成员值位于 0～1 之间,需要对其进行放大,放大公式如下:

$$Y=round(255*X)$$

在获得的密钥中,截取 128bit 的种子密钥 key 后,产生最终用于数据加密的密钥流。加密时用密钥流的第 N 的元素和明文的第 N 的元素异或,获得密文。解密时采用同样的密钥流进行异或,从而恢复出明文。

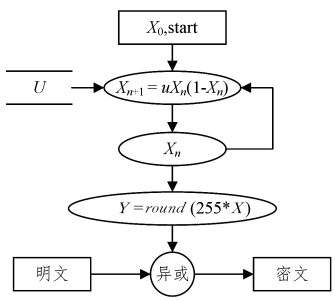


图 1　加密数据流图

4.2　握手实现

握手采用二次握手,其中 AP 为固定地址,所有终端都向该固定地址握手。第一次握手帧终端将 X_0,start 以默认的固定密钥 X_{01},start1,u 加密,加上终端的标识发给 AP。为防止 AP 因未启动等原因遗漏握手信息,第一次握手帧按固定时间无次数限制地重发,直到收到 AP 的反馈帧为止。第二次握手帧表示 AP 接收到密钥 X_0 和 start 并安装密钥开始通讯。为防止伪造节点冒认 AP 破坏握手,第二次握手帧的正文填充固定的文本并按照 X_0 和 start 加密。由于 X_0 和 start 每次握手各不相同,加密后的握手帧可以抵抗重放攻击。依靠混沌序列的不相关性,即使通过已知明文攻击解出握手帧的加密数,也无法还原出种子密钥和完整的伪随机流。

DOS 攻击用于破坏握手的资源和流程,从而达到干扰网络正常运行的目的。DOS 的攻击原理在于 IEEE 802.11 的握手协议中第一帧的非加密性,通过伪造第一帧的方式给 AP 制造抵赖或者错误的握手信息。本协议对握手的所有握手帧进行加密和校验,防止抵赖和伪造握手信息,可以有效地解决 DOS 攻击。

4.3 协议帧设计

通讯时软件在密文的基础上在前端封装数据头、帧 ID，在后端封装校验和。

针对回放攻击，协议帧 ID 为累加，由于帧 ID 具备明显的连续性，它不被加密成密文，但参与校验和计算。攻击者如果只修改帧 ID 进行篡改攻击，等同篡改正文效果，将被校验和检查逻辑发现。

为了防止篡改攻击，明文加密末尾加上校验和，AP 解密后检查原文与校验和是否一致。由于 Xor 异或算法具有组合性，攻击者对明文和校验和的某一位同步使用 Xor 篡改，可以让累加校验和无法被识别。针对这一攻击，校验和采用累加后取反加一的计算方式，并随明文一起加密，篡改者匹配校验和的难度较大。

表 1 协议帧格式

数据顺序	数据长度/kB	数据帧含义
1	2	数据头
2	2	帧类型
3	2	帧长
4	2	帧 ID
5	4	本机 IP
6	4	目标 IP
7	变长	正文(加密)
8	2	校验和(加密)

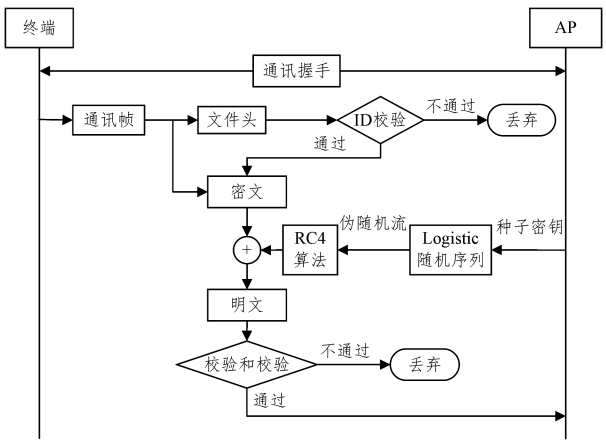


图 2 加密通讯流程

5 加密测试

将基于 486 芯片某无线传感器的某次通讯作为明文开展加密测试，数据文件总长度超过 20 MB。选用 $X_0=0.4$，$u=3.9$，$start=100$ 作为密钥，对原文进行加密，对密文统计各数字的出现概率，统计结果如图 3 所示。

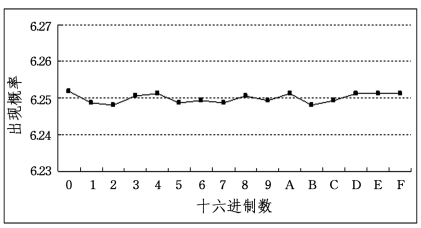


图 3 密文中数字的出现概率

对原文中每个数据的出现概率进行统计，统计结果如图 4 所示。

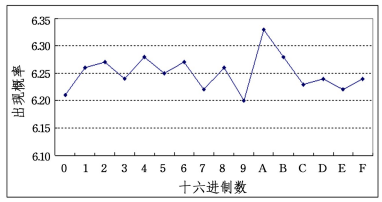


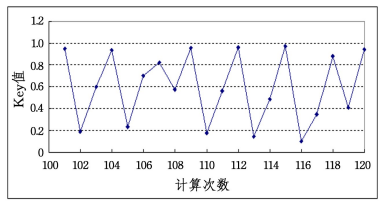
图 4 明文中数字的出现概率

经加密，字符出现概率显得平均，说明算法的扩散和混淆特性较好，具有抵抗统计攻击的能力。

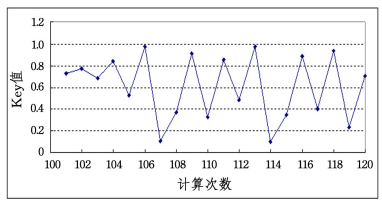
6 加密性能分析

(1)密钥的随机性

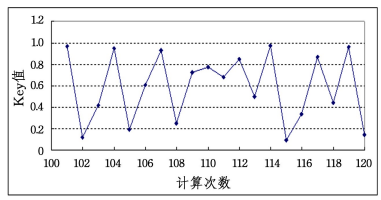
用混沌序列生成的秘钥的随机性很好，图 5 是密钥队列的分布图。



(a)$X_0=0.4$，$u=3.9$，$start=100$ 时的计算效果



(b)$X_0=0.4$，$u=3.900001$，$start=100$ 时的计算效果



(c)$X_0=0.4000001$，$u=3.9$，$start=100$ 时的计算效果

图 5 Logistic 混沌序列密钥效果

由此可见，微小的差异使得产生的成员密钥毫不相关，参数对密钥的敏感性可达到 10^{-16}，从队列中截取的子密钥之间呈现随机性，这些特性使得破译难度增加。

(2)安全性

传感器握手的操作频率不高，攻击者获取的样本规模在 300 以下，难以进行差异比较。加密软件中 X_0 和 start 随机生成，握手帧无相关性供攻击者分析。整个通讯和握手中，不会出现明文，密钥 U 也不参与通讯，攻击者只能监听到密文，即使使用了伪装的节点，因为没有密钥 U，所以无法实现解密。密钥空间大，硬破解的难度较大，即使攻击者破解了一段密钥，因为密钥的无关性，所以无法破译其他部分的数据。

(3)复杂度分析

每轮加密的密钥计算为 2 次浮点数计算和 1 次浮点数保存，时间复杂度为 O(1)，每轮加密后只需保存最新的 X 参数，需要临时开辟空间存放密钥流 Y，空间复杂度为 O(1)。

对比原 RC4 加密算法，新算法没有增加时间复杂度和空间复杂度，可以验证具备 RC4 算法的轻量级优势。

(下转第 391 页)