doi:10.11959/j.issn.1000-436x.2017292

基于动态子密钥的 WSN 混沌分组加密方案

王亚华[1]，凌玉华[1]，廖力清[1]，孙克辉[2]，刘文浩[2]
（1. 中南大学信息科学与工程学院，湖南 长沙 410083；2. 中南大学物理与电子学院，湖南 长沙 410083）

摘 要：鉴于无线传感器网络（WSN）对加密算法高效性和安全性的要求，设计一种轻量级的混沌分组加密算法，并提出了安全性更高的动态子密钥扩展方案。该方案依托 WSN 云服务器的强大数据运算和处理能力，利用新的加解密机制，将子密钥同步任务转移到云服务器进行处理，大幅降低节点的运算负担。实验结果和性能分析表明，该方案具有较好的扩散混乱特性和统计平衡性，且密钥安全性强、算法效率高，在 WSN 通信加密领域具有良好的应用前景。

关键词：WSN；动态子密钥；分组加密；整数型混沌系统
中图分类号：TP 309.7 **文献标识码**：A

Novel chaotic block encryption scheme for WSN based on dynamic sub key

WANG Ya-hua[1], LING Yu-hua[1], LIAO Li-qing[1], SUN Ke-hui[2], LIU Wen-hao[2]
(1. School of Information Science and Engineering, Central South University, Changsha 410083, China;
2. School of Physics and Electronics, Central South University, Changsha 410083, China)

Abstract: In view of high efficiency and security requirements in WSN encryption algorithm, a lightweight chaotic block encryption algorithm was designed and a novel scheme of dynamic sub keys extension was proposed. To greatly reduce the computing burden of WSN nodes, this scheme made full use of WSN cloud servers monitoring platform, which was powerful in data computing and processing, and transfered the sub keys synchronization task from nodes to cloud servers. Experimental results and performance analysis show that the scheme has good characteristics of diffusion, confusion and statistical balance, strong key security and high algorithm efficiency. It has a good application prospect in the field of WSN communication encryption.

Key words: WSN, dynamic sub key, block encryption, integer-type chaotic system

1 引言

无线传感器网络（WSN, wireless sensor network）是由一组传感器以 ad hoc 方式构成的无线网络，其目的是协作地感知、采集和处理网络覆盖的地理区域中感知对象的信息，并发布给观察者[1]。通过使用无线射频技术，传感器节点不仅能够彼此通信，而且可以与基站连接，这使它们能够将传感器数据传输到远程的处理、可视化、分析和存储系统[2]。图 1 为无线传感器网络的系统架构，传感器节点通过多跳路由，周期性地将采集的数据发布给基站（或通过网关协调器转发给基站），并通过基站连接到互联网端的云服务器，实现远程对不同地理区域的物理环境或设备运行状态的监测。

随着“万物互联”时代的到来，无线传感器网络（WSN）必将迎来大规模的发展和应用。但 WSN 分布式的特点及其固有的脆弱性，使之很容易成为黑客入侵的对象，导致整个网络受到威胁。因此，WSN 的安全问题就显得尤为重要。但是鉴于 WSN 节点运算能力较低、存储空间有限、能量需求紧张的特殊性，在设计加密算法时，一方面需要考虑减少算法的复杂度和运算量，另一方面又要均衡考虑

收稿日期：2017-02-06；**修回日期**：2017-06-30
基金项目：国家自然科学基金资助项目（No.61161006, No.61073187）
Foundation Item: The National Natural Science Foundation of China (No.61161006, No.61073187)

算法的安全性和可靠性，这也是 WSN 加密算法设计的难点所在。

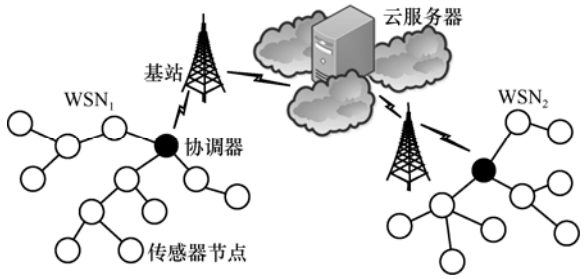

图 1　无线传感器网络的系统架构

混沌系统具有对系统参数与初始值极端敏感的特性，相同的混沌系统无论初始值相差多么微小，经过一段时间演化以后，都会使系统彻底偏离原来的演化方向，有着非常好的密码学特性[3]，因此，将混沌理论应用于 WSN 通信加密成为近年来的研究热点[4~9]。文献[8]考虑到 WSN 节点运算能力有限，在 Feistel 网络结构下设计出以 8 bit 为运算单元的混合混沌加密系统，非常适合字长为 8 bit 的 WSN 节点处理器，但密钥扩展算法借鉴于 RC5 算法，属于固定子密钥加密，且子密钥初始化被简化处理，存在一定的安全风险。文献[9]发现使用相同子密钥进行多轮加密存在安全问题，并提出了一种基于混沌映射的动态子密钥生成方法，该方法将密文作为混沌映射初始值，通过混沌迭代来生成新的子密钥。但这违背了柯克霍夫原则，一旦密码攻击者熟悉该密码系统的设计和工作原理，便可根据截获的密文来生成子密钥，进而实现对密文的完全破解。

鉴于以上情况，本文提出了一种全新的适用于 WSN 的动态子密钥（DSK, dynamic sub key）混沌加密方案，该方案依托混沌系统优良的伪随机特性和 WSN 云服务器监控平台强大的数据运算和处理能力，并利用新的加解密机制，将子密钥同步任务从节点转移到云服务器，使安全性更高的动态子密钥混沌加密算法在 WSN 中的应用成为可能，同时，不增加节点的运算处理量。

2　基于动态子密钥的 WSN 混沌分组加密方案设计

本文方案的加密算法采用了 RC6 加密体系结构[10]，加密算法的分组长度为 32 bit，使用了密码分组连接模式（CBC 模式，初始向量也为 32 bit），主密钥长度为 64 bit，加密轮数为 5 轮。

2.1　加密算法

RC6 算法继承了 RC5 算法设计简单、使用循环移位的思想，同时，增强了抵抗攻击的能力，改进了 RC5 算法循环移位不依赖寄存器中所有位的不足。因此，本文方案的加密算法采用 RC6 的加密体系结构。但鉴于一般情况下，WSN 节点 CPU 的机器字长为 8 bit，为了便于 8 bit CPU 更好更快地进行数据运算和处理，将 RC6 算法的 4 个 32 bit 寄存器改为 4 个 8 bit 寄存器，这样单次加密的分组长度为 32 bit。

新的加密算法保留了 RC6 中的循环移位非线性运算，同时，还在加密体系中融入了整数型 Arnold 混沌映射。关于 Arnold 混沌系统的优良特性及其整型数值化研究，文献[11]给出了详细的说明和推导，这里不再赘述。加密算法中使用了典型的 Arnold 混沌映射整数化方程，如式(1)所示。

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 2^{\omega} \tag{1}$$

其中，ω为节点 CPU 的机器字长，取模运算使 $x_n, y_n \in [0, 2^{\omega}-1]$，这个区间恰好为$\omega$ bit CPU 字长所能表示的无符号整数范围，这里$\omega = 8$。Arnold 混沌映射整数化方程只涉及加和乘 2 种操作（可以使用左移 1 位替代），取模运算也可以利用 CPU 字长固有的限制来替代，因此，加密算法的混沌迭代部分是非常适合 WSN 节点 CPU 运算处理的。

图 2 给出了加密算法的整体加密流程，轮加密过程的伪代码如下。

for $i = 0$ to $r-1$ do

$(F_1, F_2) = f(B, S_i[0], B^*)$;

$(F_3, F_4) = f(D, S_i[1], D^*)$;

$A = (A + F_1) <<< F_4^*$;

$C = (C + F_3) <<< F_2^*$;

$(F_1, F_2) = f(A, S_i[2], A^*)$;

$(F_3, F_4) = f(C, S_i[3], C^*)$;

$B = (B <<< F_4^*) \oplus F_1$;

$D = (D <<< F_2^*) \oplus F_3$;

$(A, B, C, D) = (B, C, D, A)$;

其中，r 表示轮加密的轮数；计算 $(f_1, f_2) = f(a, b, a^*)$ 中的 $f()$ 函数表示 Arnold 映射整数化方

程的迭代运算过程，a、b 为方程的初始输入值，迭代运算执行 a^* 次后，输出迭代结果 f_1、f_2；a^* 表示 a 的低 lbω 位的值，由于 $\omega=8$，故 a^* 表示 a 的低 3 位的值；‘+’表示模 2^ω 加法运算；$a<<<b$ 或 $a>>>b$ 分别表示将 a 循环左移或右移 b 位；⊕ 表示按位异或运算。

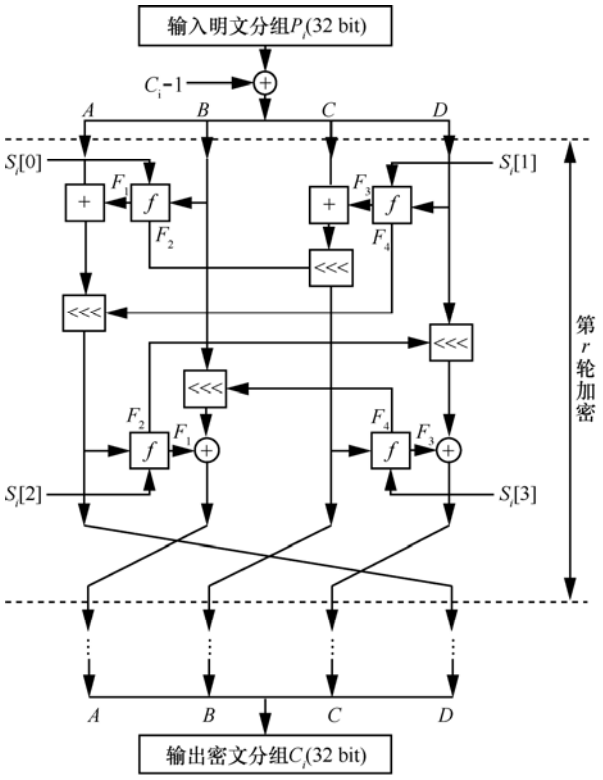

图 2　基于 RC6 加密体系结构的混沌加密模型

该算法一次可以处理 32 bit 数据，首先按 CBC 模式将输入的明文分组与上一次的密文进行异或操作（首次输入明文分组时，以初始向量替代密文），以增强算法的扩散和混乱特性，然后将结果从高字节到低字节依次放入 4 个 8 bit 寄存器 A、B、C、D 中，这 4 个寄存器会按照上述伪代码的顺序参与运算。在这个过程中，Arnold 混沌映射的迭代次数由初始输入值而动态决定，同时，混沌映射的迭代结果又会与循环移位运算相互交错关联，并决定循环移位的次数，以进一步增强算法的扩散和混乱特性。当执行所有运算之后，4 个寄存器会按照 A、B、C、D 的顺序组合成 32 bit 的密文并输出。从上述过程可以看出，所有的数据处理都是以 8 bit 为单位进行存储和运算的，而且算法中只涉及加法、异或、移位等 CPU 基本运算指令，这就使加密算法在确保安全性的同时具备了运行快、耗时少、能耗低的优势。

考虑到节点 CPU 的加密执行速度、时间、存储空间以及算法的安全性等因素，整个加密算法的加密轮数最终确定为 5 轮（本文 5.1 节会有详细的实验数据论证）。每轮加密使用 1 个 32 bit 子密钥 S_i，每个子密钥可以分成 4 个 8 bit 子密钥分量，分别为 $S_i[0]$、$S_i[1]$、$S_i[2]$、$S_i[3]$，参与以 8 bit 为单位的加密运算。因此，5 轮加密过程，需要 5 个 32 bit 子密钥 $S_i\ (i=0,1,2,3,4)$，这些子密钥都是主密钥通过密钥扩展算法产生的。

2.2　密钥扩展算法

目前，比较有代表性的是 RC5[10]和 AES[12]密钥扩展算法，这 2 种算法都是通过不同手段复杂化加密子密钥与主密钥之间的关系，从而使密码攻击者即使在知道加密子密钥的情况下依然很难分析出主密钥，它们都属于基于固定子密钥的密钥扩展算法。

本文中的动态子密钥扩展算法基于加密计数器和整数型 Logistic 混沌映射系统。加密计数器是一个 32 bit 寄存器，因为在扩展算法中每加密一帧数据，该寄存器自动加 1，故称之为加密计数器。关于 Logistic 混沌系统的优良特性及其整型数值化研究，文献[9]给出了详细的说明和推导，这里也不再赘述。密钥扩展算法中使用的 Logistic 混沌映射整数化方程，如式(2)所示，该方程在文献[9]基础上做了补充和调整。

$$z_{n+1}=\begin{cases}2 & ,z_n=0\\ 4z_n-\dfrac{z_n^{\,2}}{2^{\omega-2}}-1, & z_n\in[1,2^\omega-1]\end{cases}\tag{2}$$

其中，ω为节点 CPU 的机器字长，为了获取超长周期混沌序列和便于 32 bit 子密钥组的生成，这里取ω = 32。根据序列的单调性可以证明，当 $z_n\in[1,2^\omega-1]$ 时，迭代结果将始终位于 $[3,2^\omega-1]$。对于 $z_{n+1}=4z_n-\dfrac{z_n^{\,2}}{2^{\omega-2}}-1$ 的计算，可以简化为

$$z_{n+1}=(z_n<<2)-(z_n^{\,2}>>(\omega-2))-1\tag{3}$$

以加快节点 CPU 的运算速度，下面具体介绍密钥扩展算法。

鉴于 WSN 节点特殊性以及加密安全性的综合考虑，主密钥长度选为 64 bit，为便于密钥管理，将主密钥划分为 8 B，表示为 K[0L 7]。

密钥扩展流程如图 3 所示，具体内容如下。

1) 将主密钥 $K[0\text{L }7]$ 进行一次置换操作，置换规则为

$$K[0]\leftrightarrow K[6]$$
$$K[1]\leftrightarrow K[3]$$
$$K[2]\leftrightarrow K[5]$$
$$K[4]\leftrightarrow K[7]$$

2) 取高 32 bit 作为加密计数器的输入初始值，取低 32 bit 作为整数型 Logistic 混沌映射的输入初始值。

3) 进行一次迭代操作。其中，加密计数器每次迭代自动加 1，整数型 Logistic 混沌映射则按照式(2)迭代。

4) 将加密计数器和整数型 Logistic 混沌映射的迭代结果按位进行异或运算，输出 32 bit 子密钥 S_0。

5) 重复步骤 3）和步骤 4）4 次，输出余下子密钥 $S_i\ (i=1,2,3,4)$。

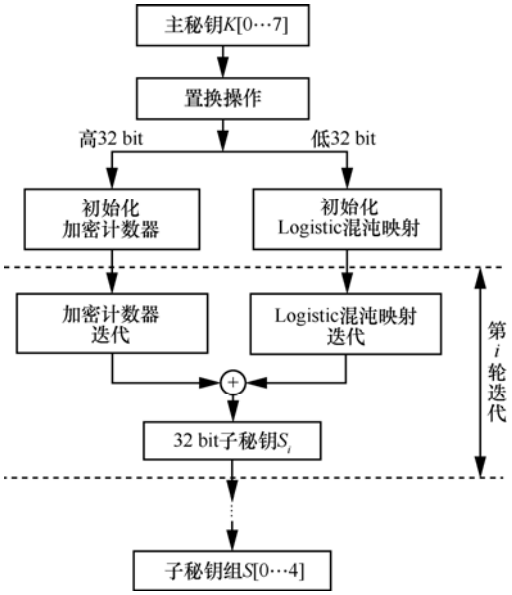

图 3　基于动态子密钥的密钥扩展模型

至此，完成一次动态子密钥扩展，生成的子密钥组将用于数据帧的加密，当一帧数据完成加密后，又会重新执行上述步骤 3）~步骤 5），来将生成新的子密钥组用于后续数据帧的加密，这里称之为“一帧一密”。这种动态子密钥扩展方案实现了类似“一次一密”的加密特性，Shannon 曾经证明一次一密是无法破解的，而且加密计数器与 Logistic 混沌映射产生的超长周期伪随机序列，使前后每帧数据分组的加密子密钥相对独立，每个数据分组都有相同的破解强度，最大程度上确保了通信的安全性。

2.3　解密算法

使用 RC6 加密体系结构进行加密算法设计时，只需要确保 4 条主干路上（垂直方向）运算的具备可逆性即可，对于支路上（水平方向）的运算没有可逆性要求。从图 2 中可以看出，位于 4 条主干路上的运算包括取模加法、按位异或和循环移位，这 3 种运算都是可逆的；位于支路上的运算为 Arnold 混沌映射迭代，虽然该映射也具备可逆性，但在此处已无关紧要。因此，本文方案中的加密算法设计符合 RC6 加密体系算法设计原则，可以正确实现加密和解密过程。

轮解密过程的伪代码如下。

for $i=r-1$ to 0 do

$$(A,B,C,D)=(D,A,B,C);$$
$$(F_1,F_2)=f\left(A,S_i[2],A^*\right);$$
$$(F_3,F_4)=f\left(C,S_i[3],C^*\right);$$
$$B=\left(B\oplus F_1\right)>>>F_4^*;$$
$$D=\left(D\oplus F_3\right)>>>F_2^*;$$
$$(F_1,F_2)=f\left(B,S_i[0],B^*\right);$$
$$(F_3,F_4)=f\left(D,S_i[1],D^*\right);$$
$$A=\left(A>>>F_4^*\right)-F_1;$$
$$C=\left(C>>>F_2^*\right)-F_3$$

3　动态子密钥同步的实现原理

基于动态子密钥的密钥扩展算法难以在 WSN 中获得广泛应用，一方面是由于动态子密钥的生成并非像固定子密钥那样“一劳永逸”，而是“一次一密”的，节点加密每帧数据时既要进行加密运算，又要进行子密钥更新，这样就加重了 WSN 节点的运算负担；另一方面是由于实现 WSN 中每个节点间的子密钥同步很困难，在一个 WSN 中所有节点要想正常地进行加解密通信，必须确保全网所有节点的动态子密钥时刻保持同步，这对于运算能力有限的 WSN 节点是相当困难的，因此，这也是制约动态子密钥扩展算法在 WSN 中应用的关键因素。

为实现安全性更高的动态子密钥加密算法在 WSN 中的应用，本文从 WSN 的系统角度，提出了将子密钥同步任务转移到云服务器处理的解决方

案。该方案的实施主要依托密钥扩展算法中的一个 32 bit 寄存器——加密计数器。加密计数器，一方面结合 Logistic 混沌映射，用于生成超长周期伪随机序列，另一方面是作为当前加密的状态指示。对于一个 WSN 云服务器监控平台而言，它具备从被监控 WSN 的主密钥中获取加密计数器输入初始值的权限，如果它还能知晓被监控节点当前的加密计数器状态值，那么两者的差值就是该节点曾经加密过的帧数据分组个数，以及该节点生成子密钥组时 Logistic 混沌映射的历史迭代次数，这意味着在监控平台上可以复现节点密钥扩展过程，从而计算出节点当前所使用的子密钥组，这对于云服务器解密节点密文至关重要。反之，如果帧数据分组从监控平台发往某一个 WSN 节点，那么监控平台需要事先在该节点当前加密计数器状态值的基础上进行一次密钥扩展，生成新一轮的子密钥组 $S_{\text{server}}[0\text{L}\ 4]$，并用该子密钥组加密帧数据分组，该节点收到加密后的帧数据分组后，直接进行一次密钥扩展，生成新一轮的子密钥组 $S_{\text{endpoint}}[0\text{L}\ 4]$，并用该子密钥组解密帧数据分组。如果节点与监控平台间的子密钥同步正常，则 $S_{\text{server}}[0\text{L}\ 4]=S_{\text{endpoint}}[0\text{L}\ 4]$，此时节点可以正确解密来自监控平台的帧数据分组。

从安全性角度来看，上述子密钥同步过程中加密计数器状态值有可能被密码攻击者截获，但仅获取加密计数器状态值，而不知晓加密系统的主密钥，密码攻击者无法计算出加密系统的历史迭代次数，就无法复现节点的密钥扩展过程，更无法计算出子密钥组来破解密文了，而破解主密钥也是相当困难的，详见 5.2 节的密钥和密钥空间分析。

从上述过程可以看出，对于 WSN 节点而言，只需在发送或接收帧数据分组时进行一次密钥扩展操作，并用生成的子密钥组加解密帧数据分组；对于监控平台而言，则需要在数据库中创建一张表记录每个节点最新的加密计数器状态值，这个状态值会被封装在帧数据分组中，监控平台每接收到一个节点帧数据分组，就会从中提取加密计数器状态值，一方面用于更新数据库中加密计数器状态值表，另一方面用于解密帧数据分组。显然，监控平台管理和维护的这张加密计数器状态值表实现了每个节点与监控平台之间的子密钥同步。因此，即使节点之间的子密钥不同步，监控平台可以充当“翻译官”，辅助完成两者间的正常通信。这样，需要庞大数据运算和数据处理的子密钥同步工作都交由云服务器监控平台来完成，节点只需按部就班地完成加解密算法操作，从而灵巧地实现了子密钥同步运算量的转移，大大减轻了节点的运算负担。

4 WSN 应用层通信协议的制定

整个 WSN 加密系统的稳定可靠运行需要建立在统一完善的应用层通信协议之上，无论是节点还是监控平台，在收发数据分组时都应严格按照协议格式进行相应数据的存取。

ZigBee 是基于 IEEE 802.15.4 标准的低功耗局域网协议，在 WSN 领域有着广泛的应用。因此，本文在 TI 公司半开源的 ZStack-CC2530-2.5.1a 协议栈（后面简称 Z-Stack 协议栈）基础上讲述 WSN 应用层通信协议的制定。Z-Stack 协议栈采用分层体系结构，从底层到顶层依次分为：物理层、MAC 层、网络层和应用层[13]。这里主要讨论应用层数据的加密，并设计了一种简洁的应用层数据帧协议，帧格式如图 4 所示。

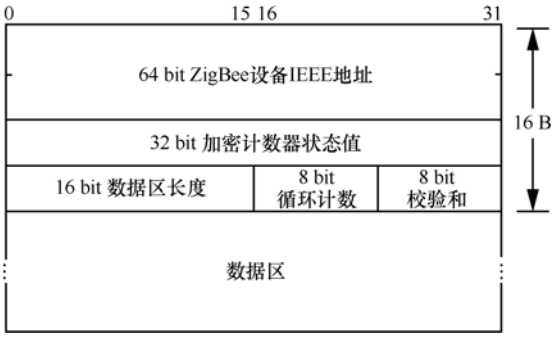

图 4 WSN 应用层数据帧格式

考虑到加密算法一次可处理 32 bit 数据，因此，帧格式采用 4 B 对齐方式，下面详细介绍数据帧格式的含义。

ZigBee 设备 IEEE 地址。占据 64 bit 空间，该地址为全球唯一地址，通常由 ZigBee 芯片制造商固化在芯片内部，用于每个 ZigBee 设备的身份识别。

加密计数器状态值。占据 32 bit 空间，应该在密钥扩展算法执行前，向该寄存器中写入加密计数器的状态值。

数据区长度。占据 16 bit 空间，用于记录数据区的字节数。

循环计数。占据 8 bit 空间，用于记录加密计数器循环计数时回到初始值的次数，以便正确区分同一个节点的 2 个相同加密计数器状态值的加密

状态。

校验和。占据 8 bit 空间，主要用于确保数据在无线传输过程中的完整性和准确性。在发送方将应用层的帧格式数据分组中除校验和之外的其他所有数据按字节方式求和，并取其低 8 bit 作为校验和，在接收方用相同方式进行重新计算，并将计算结果与校验和比对，若相同则校验通过。

数据区。占据空间视具体情况而定，但必须按 4 B 对齐，不足 4 B 的加 0 补齐。

当节点接收到一个帧格式数据分组时，首先计算校验和，校验通过后，读取数据分组中的加密计数器状态值，并将其与本地的加密计数器状态值比对。若相同则说明节点与监控平台间的子密钥同步正确，则按密钥扩展算法和解密算法对数据分组进行解密；若不相同则说明两者间同步有误，为增强加密系统的顽健性，此时节点不进行解密操作，而是主动向监控平台发送同步数据分组。同步数据分组与帧格式数据分组的格式相同，只是数据区长度为 0，数据区为空，因此，同步数据分组很简短，监控平台收到同步数据分组后，在数据库中更新对应 IEEE 地址节点的加密计数器状态值，使节点与监控平台间重新达到子密钥同步。

5　实验结果与性能分析

5.1　扩散和混乱特性分析

在分组密码算法体制中，算法的扩散和混乱程度可以通过非线性扩散特性的统计检测给出，加密算法的非线性扩散程度分析通常包括算法的完全性、雪崩效应和严格雪崩准则，这里也将用这 3 个指标对算法的扩散和混乱特性进行分析。

完全性是指加密算法输出的每一比特都和输入的所有比特有关，其数学表达式为

$$d_1 = 1 - \frac{1}{nm}\#\{(i,j)\,|\,a_{ij}=0\},(i=0,1,\mathrm{L}\ n-1; j=0,1,\mathrm{L}\ m-1) \tag{4}$$

雪崩效应是指输入的任一比特变化都应该导致平均半数输出比特的变化，其数学表达式为

$$d_2 = 1 - \frac{2}{\#T \times nm}\sum_{i=0}^{n-1}\left|\sum_{j=0}^{m-1} jb_{ij} - \frac{m}{2}\#T\right| \tag{5}$$

严格雪崩准则是指输入的任一比特变化都应该导致输出数据的每一比特以 $\frac{1}{2}$ 的概率发生改变，其数学表达式为

$$d_3 = 1 - \frac{2}{\#T \times nm}\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\left|a_{ij} - \frac{1}{2}\#T\right| \tag{6}$$

式(6)中，设加密算法的输入长度为 n bit，输出长度为 m bit，输入的样本空间的大小为 T，a_{ij} 表示 T 中只改变输入第 i bit 导致输出的第 j bit 变化的个数，b_{ij} 表示 T 中改变输入第 i bit 的输出与原输出之间的差分汉明重量为 j 的个数，$\#X$ 表示集合 X 中元素的个数[14]。

本文选取 $T = 20\,000$ 的样本空间进行测试，若 $d_1 = 1$，$d_2 \approx 1$，$d_3 \approx 1$，则说明加密算法的非线性扩散特性满足要求。表 1 为本文加密算法（以下简称 DSK 加密算法）的扩散混乱特性与加密轮数间的比较，可以看出进行 3 轮加密之后就已经满足扩散和扰乱特性指标，这得益于 CBC 加密模式以及加密算法中的混淆机制，考虑到安全性和加密速度等问题，本文方案的加密轮数最终定为 5 轮；表 2 将 5 轮 DSK 加密算法与目前已经广泛应用于 WSN 安全加密的 AES-128 算法进行扩散和混乱特性比较，两者均满足非线性扩散的要求，但 AES-128 加密算法的扩散和混乱特性更加出色。

表 1　DSK 算法的扩散混乱特性与加密轮数间的关系

加密轮数	d_1	d_2	d_3
1	1.000 000	0.997 252	0.979 819
2	1.000 000	0.997 710	0.982 651
3	1.000 000	0.997 921	0.990 694
4	1.000 000	0.998 006	0.993 787
5	1.000 000	0.998 272	0.996 844
6	1.000 000	0.997 996	0.996 246
7	1.000 000	0.998 299	0.997 062
8	1.000 000	0.998 601	0.997 774

表 2　扩散和混乱特性的比较

加密算法	d_1	d_2	d_3
DSK	1.000 000	0.998 272	0.996 844
AES-128	1.000 000	0.999 781	0.999 781

5.2　密钥及密钥空间分析

本文设计的加密算法主密钥长度为 64 bit，同时，算法采用了 CBC 加密模式，32 bit 的初始向量可以作为辅助密钥，因此，总密钥长度为 96 bit，

密钥组合有 $2^{96} \approx 7.922\,816 \times 10^{28}$ 种可能，即使使用每秒超过 10 亿亿次运算速度的超级计算机进行密钥穷举，也要连续运算 25 123 年，因此，使用暴力破解本文方案是不现实的。

本文设计的动态子密钥扩展算法，使用加密计数器与 Logistic 混沌映射产生的超长周期伪随机序列作为子密钥来源，其中，32 bit 加密计数器周期为 $2^{32}-1$，32 bit 整数型 Logistic 混沌映射受初始值影响周期不定[15]，平均长度为 4.2×10^3，则根据周期复合定理——2 个独立的离散非负周期序列进行复合运算，所得新序列的周期为原序列周期的最小公倍数，因此，可以计算出子密钥的周期长度为 $1.202\,591 \times 10^{12}$。按照“一帧一密”的动态子密钥扩展规则，假设 WSN 节点上传加密帧格式数据分组的周期为 1 s（考虑到网络容量和节点能量限制等因素，实际周期没有这么短），则本文设计的密钥扩展算法，依然可以确保子密钥不重复使用 7 626 年，这个时间已经远远超过 WSN 节点的使用寿命。

综上所述，本文设计的加密方案符合柯克霍夫原则、子密钥在节点寿命期间为动态非周期序列，密钥安全性极高。

5.3 密文统计性分析

安全性高的密文，应该具备很强的随机性，能够抵抗任何手段的统计性分析，使密码攻击者无法直接从密文下手寻找密文中的统计学规律。密文的统计性分析，主要包括“0-1”平衡性测试、字符平衡性测试和信息熵测试。

5.3.1 “0-1”平衡性测试

“0-1”平衡性测试指将密文转化为二进制表示，并对密文中的二进制“0”和“1”的个数进行统计。若密文是随机性的，理论上“0”和“1”的个数应该相等。这里给出“0-1”平衡性测试的计算式为

$$\varepsilon = \frac{|n_0 - n_1|}{n} \tag{7}$$

其中，n_0 和 n_1 分别表示密文中二进制“0”和“1”的个数，n 表示“0”和“1”的总数。式(7)中 ε 越趋近于 0，则密文的“0-1”平衡性越好。表 3 将 DSK 加密算法与 AES-128 加密算法在不同密文长度时的“0-1”平衡性进行比较，从表 3 中可以看出，DSK 算法在处理长数据分组加密时，“0-1”平衡性与 AES-128 算法相当，处理短数据分组加密时优势显著，适合于低流量的 WSN 通信。

表 3 “0-1”平衡性的数据比较

加密算法	平衡性	
	1 000 bit	1 000 000 bit
DSK	0.007 481	0.000 923
AES-128	0.012 067	0.000 776

5.3.2 字符平衡性测试

安全性高的密文要能够很好地掩盖明文的语言信息，这里给出字符平衡性测试的定义：对密文中各字符的 ASCII 值（0~255）出现的次数进行概率学统计，理论情况下每个 ASCII 值出现的概率均等，大小为 $\frac{1}{256}$，即 0.003 906 25。图 5 所示为明文中各字符 ASCII 值的概率统计情况，图 6 所示为 DSK 加密算法和 AES-128 加密算法的密文字符平衡性对比，可以看出加密后二者的明文字符的统计规律均消失，各字符出现的概率基本都集中在 0.003 9 附近，具有较好的字符平衡特性。

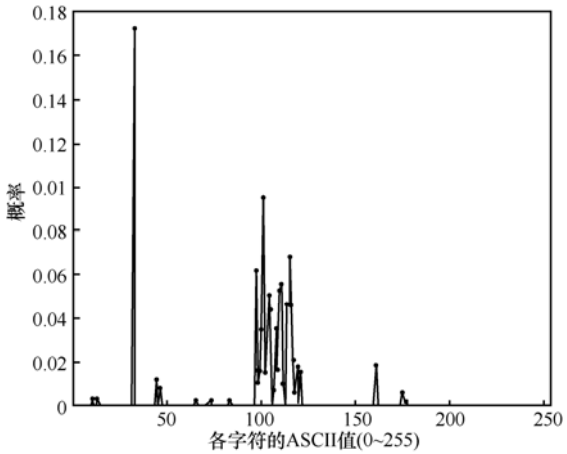

图 5 明文各字符 ASCII 值的概率统计情况

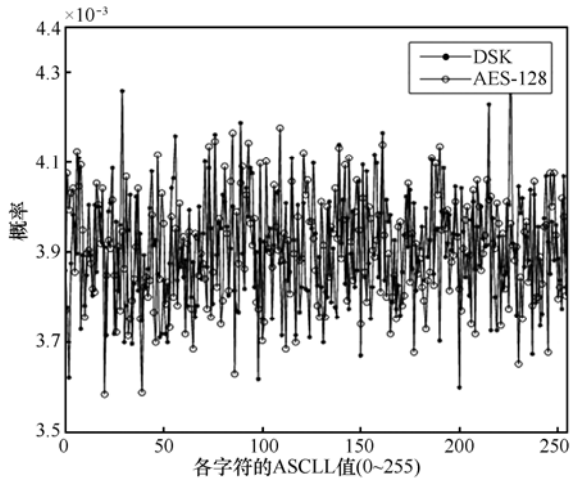

图 6　字符平衡性的比较

5.3.3　信息熵测试

信息熵的计算式为

$$H(S)=\sum_{S}P(s_i)\mathrm{lb}\frac{1}{P(s_i)} \tag{8}$$

其中，$P(s_i)$代表在被测信息源 S 中每个字符 s_i 出现的频率，每个字符占 8 bit，如果信息源符合均匀分布，则理论上每个字符出现的概率为 $\frac{1}{2^8}$，所以根据式(8)计算所得的信息熵值应该为 8。表 4 给出了分别用 DSK 加密算法和 AES-128 加密算法生成密文的信息熵测试对比，可以看出 2 种算法的信息熵测试都非常接近理论值，说明 2 种加密算法生成的密文信息复杂度都很高。

表 4　　信息熵测试的比较

信息熵值	DSK	AS-128
$H(S)$	7.999 306	7.999 319

5.4　算法效率分析

为了测试加密方案的实际算法效率，采用了 TI 公司的 2.4 GHz 射频片上系统 CC2530F256 作为测试平台，搭建了基于 ZigBee 设备的 WSN 和与之配套的服务器监控平台，并在 Z-Stack 协议栈上实现了本文方案加密算法。CC2530F256 芯片拥有一个性能优良、具备代码预取功能的低功耗增强型 8051 微控制器内核，配备有 256 KB 可编程 Flash 和 8 KB RAM，系统外部高频晶振为 32 MHz。表 5 为 2 种算法的效率各项指标的对比，从表 5 中可以看出，DSK 加密算法无论是在加密速度方面，还是在存储空间占用方面，都要明显优于 AES-128 加密算法，上述实验也直接验证了“一帧一密”的动态子密钥加密方案在 WSN 分组加密应用的优越性与可行性。

表 5　　算法效率的比较

加密算法	每字节时间/μs	速度/(KB·s^{-1})	全局变量空间/B	局部变量空间/B
DSK	298	3.356	36	16~25
AES-128	390	2.564	528	262~300

6　结束语

本文提出了一种适用于 WSN 的动态子密钥混沌分组加密方案，其核心是借助混沌系统优良的伪随机特性，并充分利用 WSN 监控平台的强大数据和运算处理能力，巧妙地将子密钥同步任务从节点转移到云服务器。这种全新的设计思路不仅使基于“一帧一密”的动态子密钥混沌加密算法成功应用于 WSN，而且使 WSN 的通信加密兼顾高安全性与低复杂度。实验结果和性能分析表明，该方案具有较好的扩散混乱特性、统计平衡性和密钥安全性，且在算法效率方面要优于目前商用的 AES-128 加密算法，为 WSN 通信加密领域的研究提供了一种新的思路。尽管如此，该方案在基于密钥扩展算法的扩散性和安全性等方面缺乏长期的验证与考验，还有待进一步研究与完善。

2017292-8

参考文献：

[1] TILAK S. A taxonomy of wireless micro-sensor network models[J]. ACM SIGMOBILE Mobile Computing and Communications Review, 2002, 6(2): 28-36.

[2] WALTENEGUS D, CHRISTIAN P. 无线传感器网络基础：理论和实践[M].北京：清华大学出版社，2014:6-7.
WALTENEGUS D, CHRISTIAN P. Fundamentals of wireless sensor networks: theory and practice[M]. Beijing: Tsinghua University Press, 2014:6-7.

[3] 孙克辉. 混沌保密通信原理与技术[M]. 北京：清华大学出版社，2015:2.
SUN K H. Principle and technology of chaotic secure communication[M]. Beijing: Tsinghua University Press, 2015:2.

[4] TONG X J, WANG Z, LIU Y. A novel compound chaotic block cipher for wireless sensor networks[J]. Communications in Nonlinear Science and Numerical Simulation, 2015, 22(1): 120-133.

[5] BISWAS K, SINGH K. An encryption scheme using chaotic map and genetic operations for wireless sensor networks[J]. IEEE Sensors Journal, 2015, 15(5): 2801-2809.

[6] AL-MASHHADI H M, HASSAN R F. Data security protocol for wireless sensor network using chaotic map[J]. International Journal of

Computer Science and Information Security, 2015, 13(8): 80.

[7] 陈铁明,葛亮. 面向无线传感器网络的混沌加密与消息鉴别算法[J]. 通信学报,2013,(05):113-120.
CHEN T M, GE L. Chaotic encryption and message authentication algorithm for WSN[J]. Journal on Communications, 2013, (05): 113-120.

[8] 佟晓筠,左科,王翥. 基于无线传感器网络的混合混沌新分组加密算法[J]. 物理学报,2012,03:52-63.
TONG X Y, ZUO K, WANG Z. A new mixed chaotic encryption algorithm based on WSNs[J]. Journal of Physics, 2012, 03:52-63.

[9] 蔡科,左宪章. 基于混沌 RC5 的传感器网络分组加密算法[J]. 计算机测量与控制,2009,11:2249-2252.
CAI K, ZUO X Z. Block encryption algorithm based on chaotic RC5 for WSN[J]. Computer Measurement and Control, 2009, 11: 2249-2252.

[10] OTHMAN S B, TRAD A, YOUSSEF H. Performance evaluation of encryption algorithm for wireless sensor networks[C]//2012 International Conference on Information Technology and e-Services (ICITeS). 2012: 1-8.

[11] 吴成茂. 离散 Arnold 变换改进及其在图像置乱加密中的应用[J]. 物理学报,2014,09:91-110.
WU C M. Improvement of discrete Arnold transform and its application in image scrambling encryption[J]. Journal of Physics, 2014, 09: 91-110.

[12] LEE H, LEE K, SHIN Y. Implementation and performance analysis of AES-128 CBC algorithm in WSNs[C]//The 12th International Conference on Advanced Communication Technology (ICACT). 2010, 1: 243-248.

[13] QST 青软实训. ZigBee 技术开发: Z-Stack 协议栈原理及应用[M]. 北京: 清华大学出版社，2016:2-18.
QST Soft Training. ZigBee technology development: Z-Stack protocol stack principle and application[M]. Beijing: Tsinghua University Press, 2016:2-18.

[14] 邢长岩. 基于 WSN 的多混沌加密算法的研究与应用[D]. 哈尔滨: 哈尔滨工业大学,2014:59-60.
XING C Y. Research and application of multi chaotic encryption algorithm based on WSN[D]. Harbin: Harbin Industrial University, 2014: 59-60.

[15] 李涛护,高保生. 基于 Logistic-map 的长周期混沌序列发生器[J]. 无线电工程,2014,02:77-80.
LI T H, GAO B S. Long period chaotic sequence generator based on logistic-map[J]. Radio Engineering, 2014, 02:77-80.

作者简介：

王亚华（1990-），男，河南信阳人，中南大学硕士生，主要研究方向为无线传感器网络、网络与信息安全技术。

凌玉华（1965-），女，湖南衡阳人，博士，中南大学教授、硕士生导师，主要研究方向为现代测控技术与智能仪器、软测量技术。

廖力清（1965-），男，湖南武冈人，博士，中南大学教授、硕士生导师，主要研究方向为电力电子与电力传动、分布式系统、信息安全。

孙克辉（1968-），男，湖南益阳人，博士，中南大学教授、博士生导师，主要研究方向为混沌理论与应用、信息安全。

刘文浩（1992-），男，湖南湘潭人，中南大学硕士生，主要研究方向为混沌密码设计与分析。