基于增强型检索机制 Baptista 混沌的物联网加密技术研究*

田 涛
(广西民族大学 商学院, 南宁 530006)

摘 要: 研究了一种适用于物联网的基于增强型检索机制密码方案的 Baptista 混沌加密技术。针对物联网对无线射频识别及其数据传输高可靠性和高安全性的要求,在深入分析了基于检索机制的 Baptista 混沌密码方案的特点及其局限性基础上,建立了一种基于快速收敛、具有自适应调整安全优先级的 Baptista 混沌加密技术。该技术首先根据基于 S 盒的混沌掩码技术增强了 Baptista 混沌密码方案;然后设计了适用于物联网的实时加密系统,并能够根据应用需求预置数据传输安全级别。数学分析表明,该加密技术可以为物联网应用中的智能识别和数据传输提供有效的安全性和实时性。

关键词: 物联网; Baptista 混沌; 检索机制; 加密技术; 智能识别
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)04-1424-03
doi:10.3969/j.issn.1001-3695.2012.04.062

Research of encryption technology based on enhanced Baptista chaotic cipher for Internet of things

TIAN Tao
(*School of Business*, *Guangxi University for Nationalities*, *Nanning* 530006, *China*)

Abstract: Researched a enhanced Baptista chaotic cipher technology based on retrieval algorithm for Internet of things. The networking of radio frequency identification and data transmission with high reliability and high safety requirements, an in depth analysis based on retrieval mechanism of Baptista chaotic encryption scheme based on the characteristics and its limitation, which was based on fast convergence, adaptive adjusting safety priority Baptista chaotic encryption technology. The technology based on S box, according to the chaotic mask technology had enhanced the Baptista chaotic encryption scheme, and then applied to design the content of network real-time encryption system and according to the application requirements of preset data transmission security level. Mathematical analysis shows that, the encryption technology can provide Internet application in the intelligent recognition and data transmission to provide effective security and real-time.

Key words: Internet of things; Baptista chaotic cipher; retrieval mechanism; encryption technology; intelligent recognition

0 引言

随着物联网通信[1]、传感技术和加密技术[2,3]的快速发展,如何为物联网应用过程中的智能识别和无线数据通信提供高效率、高可靠性和具有自适应调节能力的加密技术得到国内外相关专业人士的广泛关注[4,5]。

文献[6]基于加密引擎设计了一种低成本的超高频射频识别标签。文献[7]综述了适用于物联网的可信安全体系结构。HUGUES-SALAS 等人[8]基于扩展的 Kalman 滤波方法提出了一种应用于混沌保密通信的非线性时滞系统。文献[9]分析了混沌人工神经网络在物联网大规模数据融合处理过程中的反积限制算法。但是文献[6,7]忽略了基于检索机制方案的 Baptista 混沌密码方案的缺陷,文献[8,9]对加密算法在物联网具体应用中的快速收敛和实时性等特点未作深入研究。

因此,在已有研究成果的基础上,本文提出了一种适用于物联网应用系统的基于增强型 Baptista 混沌密码方案的加密技术。该技术根据 S 盒的优秀混乱作用,应用多组密码算法结合混沌掩码技术增强了 Baptista 混沌加密机制,然后设计了能够改善智能识别精度,提高无线数据传输可靠性、实时性和安全性的物联网加/解密系统。

1 增强型 Baptista 混沌密码系统

1.1 基于检索机制 Baptista 混沌密码方案

假设一维混沌映射 P: $Y \to Y$。将混沌区间$[y_{\min}, y_{\max})$根据检索需要分割为 n 个子区间,表示为 $Y_1 \sim Y_n$,其中 Y_j 如式(1)所示。

$$Y_j = [y_{\min} + (i-1)\varphi, y_{\min} + j\varphi) \tag{1}$$

其中:$\varphi = (y_{\max} - y_{\min})/n$。

针对物联网应用中传输的大规模数据量的明文消息分给为 m 个长度为 p 的子消息序列记为 Cp_i,且每个子消息字符组成为$\partial_1, \partial_2, \cdots, \partial_p$,则基于检索机制的 Baptista 混沌密码方案工作步骤如下:

a)混沌系统初始化。对一维混沌建立 Logistic 映射。

b)生成密钥过程。根据一维混沌的 Logistic 映射生成初

收稿日期: 2011-09-24; **修回日期**: 2011-10-27 **基金项目**: 广西壮族自治区自然科学基金资助项目(2010GXNSFB013053)
作者简介: 田涛(1979-),男,陕西渭南人,讲师,硕士,主要研究方向为海量存储、对等网、数据库(tiantaols@163.com).

始密钥对,其中包括初始条件 y_0 和控制参数 r。

c)对大规模明文分簇加密。从 Cp_1 开始分别对子明文消息根据 y_0 和 r 经过多次迭代后进行加密,加密后的密文序列为 $y_j^{(i)} = P^{Cp(i)}(\varphi y_j)$。

d)对大规模明文逐列解密。对每个 Cp_i 的 Baptista 混沌密文根据已有混沌状态标记 $y_{j-n}^{(i-n)} = P^{Cp(i-n)+Cp(i)+Cp(i-1)}(\varphi y_{-n})$ 经多次迭代轮询后的 Cp_i 限制,解密得到明文 p_i 和混沌系统映射关系 P_n。

e)更新 Cp_i 限制条件和混沌控制参数。在区间[0,$y_{\min}$)和[$y_{\min}$,$y_{\max}$)上根据检索机制得到多个待选的 Cp_i 值,然后结合附加参数 $\eta \in [0, 1]$ 经多次迭代和混沌后选择当前区间内最佳解。具体分解过程为:若 $\eta = 0$,则 Cp_i 选择经最小迭代次数得到的值;若 $\eta = 1$,则 Cp_i 选择使得 $y_{j-n}^{(i-n)} = P^{Cp(i-n)+Cp(i)+Cp(i-1)}(\varphi y_{-n})$ 收敛的最小迭代次数时的解,其他情况有唯一解对应。

1.2　基于 S 盒的混沌掩码技术密码系统

由文献[10]可知,基于检索机制的 Baptista 混沌密码方案存在以下缺陷:a)对大规模明文加密后的密文处于集中状态,不具备分布式特点,Cp_i 限制条件值在区间[0,$y_{\min}$)和[$y_{\min}$,$y_{\max}$)呈指数衰减,加密效率低下,容易受到噪声干扰;b)加密收敛速度相对较慢,基于检索机制的混沌迭代次数较多。

因此,本节采用 S 盒的混沌掩码技术对 Baptista 混沌密码方案进行改进,主要是对步骤 c)~e)进行增强,改进后工作流程如下:

步骤 a)和 b)与 1.1 节所述相同。

c)基于 S 盒采用非线性双映射对大规模明文数据进行加密。具体操作如式(2)和(3)所示。

$$rt\left(\sum_{k=1}^{p}\partial_k P_k\right) = Cp_k 2^{n-1} \tag{2}$$

$$N_p 2^{n-1}\left(1 - 2^{-n}\max_{w \triangleright HU(2\partial)} |M_{\langle p\rangle}|\right) \tag{3}$$

其中:p 的 walsh 谱如式(4)所示。

$$M_{\langle p\rangle} = \sum_{x \cong HU(2^n)} (-1)^{p(x)\otimes R} \tag{4}$$

d)采用混沌掩码技术对大规模 S 盒密文进行高效、实时解密。混沌掩码技术对于非线性双映射加密的大规模密文解密的精确度概率密度函数如式(5)所示。

$$DM_{\langle p\rangle} = \max_{y \cong \beta}\left\{\sum_{y}^{\Omega}\iint_{x \cong HU(2n)} p(x)\otimes \mathscr{R}\right\} \tag{5}$$

e)因为加密和解密过程中使用了 S 盒和混沌掩码技术,为了保证系统输出比特间独立性,在 1.1 节步骤 e)的基础上加入一个解密后明文输出处理操作,如式(6)所示。

$$\Gamma(s,t) = \frac{\lambda(s,t)}{\Phi(s,t)} \tag{6}$$

其中:s 和 t 是密文输入矩阵,可由步骤 c)得到。

2　支持安全级别区分的物联网密码系统

针对如图 1 所示的采用物联网技术实现智能城市管理的网络拓扑结构规划架构,基于 S 盒的混沌掩码技术的增强型 Baptista 混沌密码技术的支持实时安全优先级预置的物联网密码系统设计如图 2 所示。

根据物联网控制中心以及应用需求,结合式(7)可预置物联网密码系统中各类应用业务的安全优先级 op 的等级值为

$$op = \left[\frac{1}{MN_i}\sum_{i=1}^{M}\oint_N (F(i,N) \to S(M,N))^2\right]^{\delta} \tag{7}$$

其中:M 表示应用业务需求的安全级别,N 表示增强型 Baptista 混沌密码技术的收敛速度。

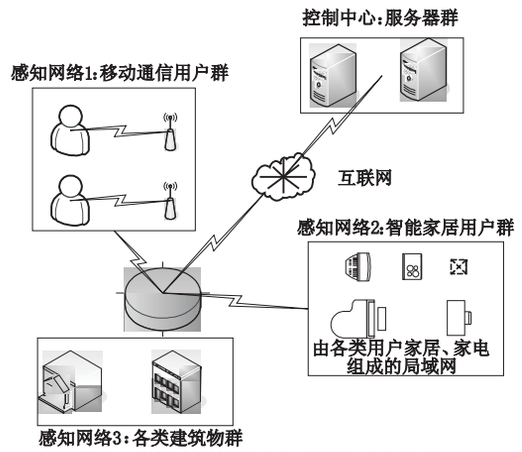

图1　基于物联网技术智能城市规划架构

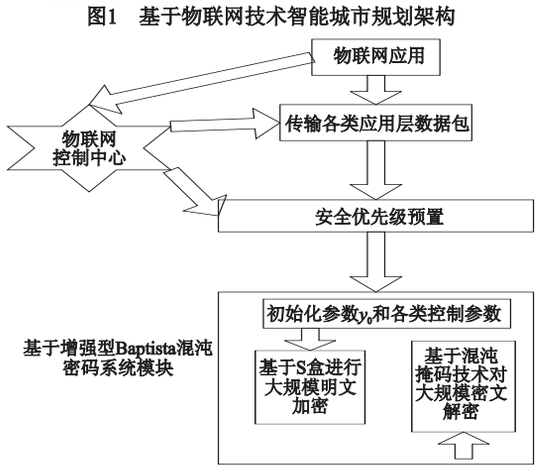

图2　基于增强型Baptista混沌方案的物联网系统

此外,在物联网应用层数据包经过安全级别预置,封装完发送到发送功能模块过程中设计了一个传输器,该传输器在 Baptista 混沌系统中加入加密算法。封装后的物联网应用层数据包序列记为 $BmP(t)$,针对式(1)所示的混沌系统,设计密钥池由式(8)构建:

$$K\_BmP(i) = K\_BmP(x(i)) + c(i) + b(BmP(i)Y_i)lc_{en} \tag{8}$$

其中:lc_{en} 是根据安全级别设置的系统反馈和等级效应系数。

为了便于性能分析,在此给出发射端功能模块和接收端功能模块,如式(9)和(10)所示:

$$\overset{<}{Y}(i) = BmP(i) * bY_i(x) + \min BmP(i)aY_{i+j}(x) \tag{9}$$

$$\overset{>}{Y}(i) = BmP(i) * bY_i(x) * rt\left(\sum_{k=1}^{p}\partial_k P_k\right) + \min BmP(i)aY_{i+j}(x)^{op} + DM_{\langle p\rangle} \tag{10}$$

其中:a、b 是 Baptista 混沌方案自适应参数。

3　加密技术性能分析

假设物联网感知区域的传感器网络中,传感器节点采集到大规模数据经增强型 Baptista 混沌方案加密后向控制中心发送,数据传输经过若干个局域网和感知分簇转发,控制中心接收到大规模密文后启动增强型 Baptista 混沌方案中的解密模块得到明文。加密和解密操作性能分析可由式(2)~(6)得到,其中对于安全优先级别的预置根据式(7)完成。采用 MATLAB 对本文所提出的物联网加密技术与基于 Baptista 混沌方案的加密技术在收敛速度、端到端平均时延、误差等性能

上进行对比。

两种 Baptista 混沌密码方案在物联网应用中的收敛速度和混沌迭代性能对比如图3 所示。可以看出,基于增强型 Baptista 混沌方案的加密技术对于大规模明文数据加密时采用 S 盒技术增强了对于感知数据信息的汇聚融合操作,有效降低了混沌轮询迭代次数,从而显著地减少了产生密钥对和计算加密后密文的收敛次数;同时,在中继转发节点和控制中心采用混沌掩码技术对大规模密文进行解码。因为加密和解密的收敛速度和迭代次数明显降低,所以基于增强型 Baptista 混沌方案的加密技术的数据发送方与接收方之间端到端平均时延明显低于原 Baptista 混沌方案的加密技术;而且随着网络规模的增大,两种加密技术的平均时延相差越来越大,如图 4 所示。从图 4 中可以看出,基于增强型 Baptista 混沌方案的加密技术避免了数据传输时延抖动,使得数据传输趋于平稳。

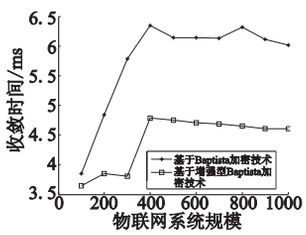

图3 收敛速度

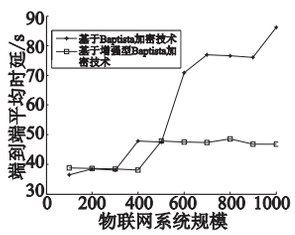

图4 端到端平均时延

图 5 给出了两种 Baptista 混沌密码方案在物联网应用中接收端的解码与原文误差对比结果。基于增强型 Baptista 混沌方案的加密技术的解码误差明显低于原基于 Baptista 混沌方案的加密技术,特别是对于大规模感知节点的物联网应用仍然保持较好的性能。

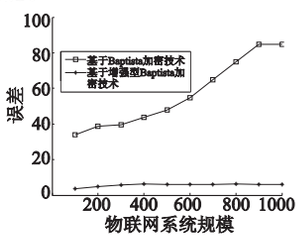

图5 误差对比结果

4 结束语

针对物联网系统应用中感知信息数据的采集、传输与控制等处理过程对物联网安全的要求,首先建立基于检索机制的 Baptista 混沌密码算法模型及其工作流程,在修正其局限性的基础上,提出了一种收敛速度快、轮询混沌迭代次数少的 Baptista混沌加密技术;然后设计了一种物联网智能应用实时加密系统,该系统预置安全优先级别的功能。数学分析表明,该物联网加密技术在智能实时识别和数据传输安全性等物联网应用方面均具有良好性能。

参考文献:

[1] YANG Zhi-hong, YUE Ying-zhao, YANG Yu, *et al*. Study and application on the architecture and key technologies for IOT[C]//Proc of International Conference on Multimedia Technology. [S. l.]: IEEE Press,2011: 747-751.

[2] LI Shu-jun, CHEN Guan-rong, MOU Xuan-qin. On the security of the Yi-Tan-Siew chaotic cipher[J]. IEEE Trans on Circuits and Systems II: Express Briefs,2004,51(12):665-669.

[3] GE Xin, LIU Fen-lin, LU Bin, *et al*. Analysis of Baptista-type chaotic cryptosystem[C]//Proc of IEEE International Conference on Multimedia and Expo. [S. l.]: IEEE Press,2007: 891-894.

[4] WONG K W, YUEN C H. Embedding compression in chaos-based cryptography[J]. IEEE Trans on Circuits and Systems II: Express Briefs,2008,55(11):1193-1197.

[5] WANG Xiao-yu, ZHANG Han, LI Zhao-hui. An improved Baptista encryption algorithm based on conservative chaotic system[C]//Proc of the 5th International Conference on Natural Computation. Washington DC: IEEE Computer Society,2009: 442-446.

[6] SHEN Xiang, LIU Dan, YANG Yu-qing, *et al*. A low-cost UHF RFID tag baseband with an IDEA cryptography engine[C]//Proc of Internet of Things. [S. l.]: IEEE Press,2010: 1-5.

[7] XIONG Li, ZHOU Xuan, LIU Wen. Research on the architecture of trusted security system based on the Internet of things[C]//Proc of International Conference on Intelligent Computation Technology and Automation. Washington DC: IEEE Computer Society,2011:1172-1175.

[8] HUGUES-SALAS O, SHORE K A. An extended Kalman filtering approach to nonlinear time-delay systems: application to chaotic secure communications[J]. IEEE Trans on Circuits and Systems I: Regular Papers,2010,57(9):2520-2530.

[9] LIN Wei, CHEN Guan-rong. Large memory capacity in chaotic artificial neural networks: a view of the anti-integrable limit[J]. IEEE Trans on Neural Networks,2009,20(8):1340-1351.

[10] HUI Yue-chao, WANG Yi-ming. Secure RFID system based on lightweight block cipher algorithm of optimized S-box[C]//Proc of IEEE International Conference on RFID-Technology and Applications. [S. l.]: IEEE Press,2010: 11-15.

[11] DAVID M, RANASINGHE D C, LARSEN T. A2U2: a stream cipher for printed electronics RFID tags[C]//Proc of IEEE International Conference on RFID. [S. l.]: IEEE Press,2011:176-183.

(上接第 1419 页)率、误检率尽量小的前提下,在很大程度上提高了入侵检测的效率,对构建轻量级入侵检测系统具有重要意义。下一步的研究重点将放在设计一种能使 GSA 算法达到最高效用的入侵检测算法及系统上。

参考文献:

[1] JELONEK J, KRAWIEC K, SLOWINSKI R. Rough set reduction of attributes and their domains for neural net works[J]. International Journal of Computational Intelligence,1995,11(2): 339-347.

[2] 蒋玉娇,王晓丹,王文军,等. 一种基于 PCA 和 ReliefF 的特征选择方法[J]. 计算机工程与应用, 2010,46(26):170-172.

[3] 邰淑彩,孙韫玉,何娟娟. 应用数理统计[M]. 2 版. 武汉:武汉大学出版社,2005:266-279.

[4] 郭文忠,陈国龙,陈庆良,等. 基于粒子群优化算法和相关性分析的特征子集选择[J]. 计算机科学,2008,35(2):144-146.

[5] 陈仕涛,陈国龙,郭文忠,等. 基于粒子群优化和邻域约简的入侵检测日志数据特征选择[J]. 计算机研究与发展,2010,47(7):1261-1267.

[6] FRANK E, HALL M, TRIGG L. Weka data mining software[J]. ACM SIGKDD Explorations NewsLetter,2009,11(1):10-18.

[7] 崔自峰,吉小华. 基于线性判别分析的特征选择[J]. 计算机应用,2009,9(10):2781-2785.

[8] 杨恢先,杨心力,曾金芳,等. 在线特征选择的目标跟踪[J]. 计算机应用研究,2010,27(3):1180-1182.