基于大数据混沌耦合优化方式的 WSN 网络数据自递归加密机制

杜宗福
(陕西广播电视大学宝鸡市分校 宝鸡 721001)

摘　要:为解决当前 WSN 网络数据自递归加密机制难以实现混沌递归集有效收敛、元数据性能较差、致使出现加密性能下降、算法收敛程度较低等瓶颈现象,提出了一种基于大数据混沌耦合优化方式的 WSN 网络数据自递归加密机制。首先通过信息交互方式,基于瀑布流生成的思想对网络中混沌度较低的数据进行耦合优化,提高了混沌自归集的自适应收敛性能,降低了数据加密过程中的资源成本;随后基于元数据的阶数,采取微分方式对收敛过程进行二次整合,改善了加密过程中难以降低收敛复杂度的难题,极大的提高了本机制的弹性,降低了加密复杂度。仿真实验表明,与传统的宽带数据融合优化加密机制(optimal encryption scheme for ultra wideband data fusion,OEUW 机制)、线性终端数据误差时延优化推断加密机制(linear terminal data error delay optimal inference encryption mechanism,LTED 机制)相比,本算法能够有效的降低加密复杂度,减少加密时间,提升传输带宽质量,具有显著的实际部署价值。

关键词:无线传感器网络;数据加密;信息交互;瀑布流;元数据
中图分类号: TP393　TN91　　**文献标识码**:A　　**国家标准学科分类代码**: 520.3040

Self recursive encryption mechanism of WSN network data based on chaotic coupling optimization of large data

Du Zongfu
(Shaanxi Radio and TV University, Baoji 721001, China)

Abstract: in order to solve the current WSN network data encryption mechanism to realize chaotic self recursive set effective convergence, metadata poor performance, resulting in the emergence of encryption algorithm convergence performance decrease, the low degree of bottleneck phenomenon, proposes a self recursive encryption mechanism of big data chaotic optimization method based on WSN data network; first by information exchange. The waterfall flow generated by coupling optimization of network ideological chaos low based on data can greatly improve the convergence performance of adaptive chaotic self collection, reduce the data encryption in the process of resource cost; then based on the order of metadata, take differential form two integration of the convergence process, greatly improved to reduce the problem of convergence complexity of the encryption process, greatly improves the system flexibility, reduces the complexity of encryption. Simulation results show that the fusion and broadband data encryption mechanism, optimize the traditional linear terminal data error delay optimization inference (Linear terminal data error encryption mechanism delay optimal inference encryption mechanism LTED mechanism) compared to the algorithm in this paper can effectively reduce the complexity of encryption, reduce the encryption time, enhance the quality of transmission bandwidth, has significant practical deployment value.

Keywords: wireless sensor networks; data encryption; information interaction; waterfall flow; metadata

1　引　言

随着信息化 3.0 的不断演进,无线传感网技术在国民经济中的地位呈现出日益提高的趋势,带动了以无线传感网加密技术为核心的安全技术的飞速发展;由于无线传感网加密机制为 WSN 中处于制高点的技术之一,当前广泛

收稿日期:2017-02

应用于无线传感网数据追踪、节点定位、数据融合、云平台分析等领域，成为主要的发展热点[1]。由于无线传感网均采用传统一次性成型方式组网，一旦若干节点失效将失去应有的加密方式，因此采取一定的解决机制，通过有效优化系统的安全特性，提高网络的生存能力，成为当前无线传感网的应用方向[2]。

为此，研究具有一定前瞻性的解决机制，一定程度上改善了 WSN 网络的加密性能。如 Jiang 等人[3]提出了一种基于混沌度精度校验机制的 WSN 网络数据自递归加密机制，能够实现在复杂电磁频谱环境下的 WSN 网络实时加密；不过该算法对于信号间自适应性能考虑不足，容易导致在频谱相似条件下的网络发生严重的泄密，降低了网络的安全系数；Zeng 等人[4]提出了一种基于传感耦合优化算法的 WSN 网络数据自递归加密机制，在 WSN 节点数据传输带宽较高的情况下实现对网络加密过程的传感耦合优化，然而由于该算法对信预发射过程中的信号成型现象考虑较差，易导致产生较严重的信号加密鲁棒性难题；Ahmed 等人[5]提出了一种超限度一体化成型算法的 WSN 网络数据自递归加密机制，通过巴基球的映射机制将 WSN 中处于自相似状态的网络数据进行一体化成型，能够在任意可控的安全系数范围内实现对 WSN 的高效混沌加密；不过由于巴基球映射过程需要进行超限度成型，因此该算法存在严重的收敛性不足的缺陷。

鉴于当前算法中存在的一些不足，提出了一种基于大数据混沌耦合优化方式的 WSN 网络数据自递归加密机制，首先通过大数据混沌耦合的方式，对 WSN 数据实行瀑布流加密；随后采用线性度微分提升加密的方式，对网络中的 WSN 数据实行二次加密。最后采取 NS2 仿真实验环境对算法进行了仿真实验，证明了机制的有效性。

2 WSN 网络数据加密机制

结合当前研究过程中存在的一些优势，且对存在的不足之处进行进一步的考虑，提出了一种基于大数据混沌耦合优化方式的 WSN 网络数据自递归加密机制(self recursive encryption mechanism of WSN data based on chaotic coupling optimization of large data，SRE_CLD)，该机制主要由大数据混沌耦合优化及线性度微分提升等两个部分构成，如图 1 所示。

2.1 大数据混沌耦合优化

由于无线传感网数据获取过程中存在一定的同质化现象，因此通过不同终端获取的 WSN 数据具有量化级别较低、混沌度高、耦合系数较差等特性[6-8]；对于任意处于正常工作的 WSN 数据终端而言，在同质化现象较高的情况下，其加密过程将会出现严重的收敛程度下降等现象，致使算法整体的加密性能呈现递归程度逐渐降低的现象[9-11]。该现象的发生主要是由于不同 WSN 数据在进行

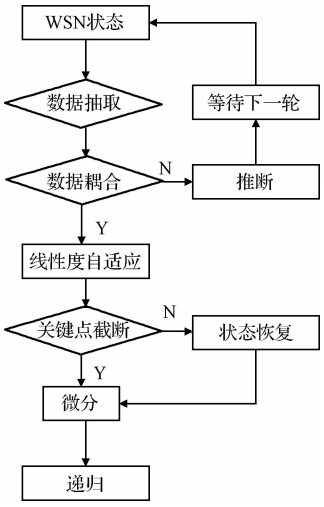

图 1 本文 WSN 网络数据自递归加密算法过程

独立加密过程中存在互相扰动的因素，因此数据加密过程需要考虑该过程的大数据特性及耦合程度较低的特性，通过一定的混沌耦合方式，改善相似数据间的混沌扰动，从而提升数据的加密性能。

不妨设 i 为需要进行数据加密的某一时刻 WSN 混沌云中的元数据，具有相似混沌度且能够实现独立加密的元数据数量为 λ_i，则 λ_i 满足：

$$\lambda_i = \sum_{j\in i} v_{ij} \tag{1}$$

式(1)中 v 为与 i 具有相似耦合程度的元数据 j 的混沌递归集。

令 i 的初始加密系数扰动度为 D_{ij}，则 D_{ij} 满足：

$$D_{ij} = \lambda_i \oiint \frac{kP_s + R^3 P_n}{R^3 P_n} \mathrm{d}s \tag{2}$$

由式(2)可知，若处于相似耦合程度的元数据位于相同的混沌递归集中，则能够采取式(2)的方式对相似耦合度的元数据实行初步的结构耦合；不过采取该方式仅能在数据量较低时实现对 WSN 数据的高效加密，一旦网络数据的混沌度及数据量呈现飞速增加时将降低算法的适用性能，因此采取大数据方式实现对加密过程的混沌耦合优化，通过构建混沌耦合优化指数对式(2)所示的混沌递归过程进行优化，提高了算法的耦合性能与加密强度。

首先采用递归方式对整个混沌递归集中处于相似耦合程度的元数据进行统计，筛选出混沌度较低的若干元数据作为基准元数据。一旦 WSN 网络进行加密过程时，首先通过这些基准元数据进行混沌度判断，且将相似耦合程度的混沌递归集进行有限收敛扩充，然后依据混沌排序方式进行二次收敛，其中排序指数 $index(r)$ 的获取方式如下：

$$index(r) = \oint \frac{(1 - T/r)PC - P_r}{P_r} P_C D_{ij} \tag{3}$$

式中：T 为基准元数据收敛周期，r 为混沌递归集的耦合系数

更新强度，P_C 为基准元数据在混沌递归集中的出现概率，P_r 为当前加密过程中元数据的映射概率，D_{ij} 定义同式(2)。

混沌集中元数据进行更新后，初始加密系数扰动度的形式将变为：

$$D_{ij}=\lambda_i\oint\frac{(1-T/r)P_C-P_r}{P_r}P_C\iint\frac{kP_s+R^3P_n}{R^3P_n}\mathrm{d}s \quad (4)$$

考虑到基准元数据通过式(3)进行二次收敛，D_{ij} 也将依托混沌排序进行收敛。

$$D_{ij}=index(k)\lambda_i\frac{kP_s+R^3P_n}{R^3P_n} \quad (5)$$

综合式(4)、(5)可得最大耦合强度 ω_i 为：

$$\omega_i=\frac{\oint\frac{(1-T/r)P_C-P_r}{P_r}P_C}{index(k)\lambda_i\frac{kP_s+R^3P_n}{R^3P_n}} \quad (6)$$

显然，耦合过程具有很强的平稳随机特性[8-9]，且可以由式(3)所示的指数进行混沌收敛。其优化流程如图2所示。

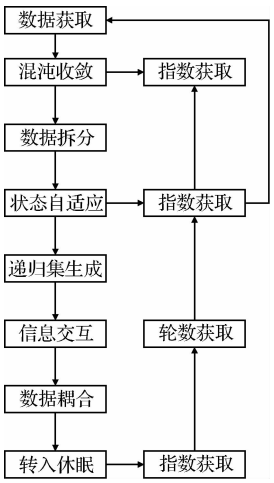

图2 大数据混沌耦合优化流程

2.2 线性度微分提升机制

虽然通过式(6)所示的过程能够有效的提高耦合过程的平稳随机特性，进一步的增强加密过程中的混沌收敛程度，且可以有效的对加密过程中的混沌递归集进行扩充，且采取式(5)可精确降低混沌集合扩充过程中存在的混沌系数提高的现象，因此可通过线性度微分方式对式(5)、(6)所示的过程进行线性度微分提升，提高机制的收敛性能。如图3所示。

对式(6)进行偏微分后，求取第 $n+1$ 阶微分可得：

$$\omega_i=\frac{r-T}{(r-2)^{n+1}} \quad (7)$$

其极限为2，考虑到式(6)存在平稳随机特性可得：

$$\omega_i=0 \quad (8)$$

由式(8)可知，经过 $n+1$ 次线性度微分提升，则混沌递归集的收敛时间能够迅速提高到0。

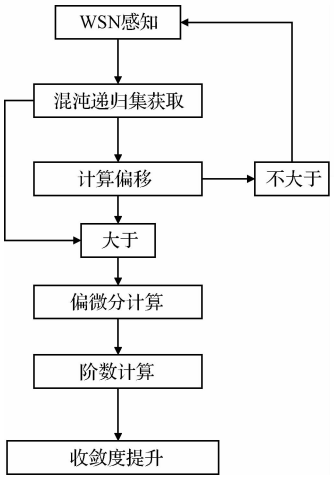

图3 线性寻错机制

3 仿真实验

为验证本机制的优越性，采用当前WSN仿真技术中常用的NS2仿真实验环境[12-13]，与当前广泛得到应用的超宽带数据融合优化加密机制(optimal encryption scheme for ultra wideband data fusion，OEUW)[14]、线性终端数据误差时延优化推断加密机制(linear terminal data error delay optimal inference encryption mechanism，LTED)[15]视为对照组，采取加密时间误差、数据收敛相对误差、加密时延、加密带宽/传输带宽占比等多个指标进行仿真实验，仿真参数如表1所示。

表1 仿真参数表

参 数	数 值
混沌节点分布面积	12 400 m×21 600 m
元数据数据生存周期/min	3 600
元数据分布点	<1 024
数据生成方式	随机抛洒分布
元数据占比/个/百 m^2	不高于10
数据通信能力/m	20
粒度缓存/KB	512
加密周期/s	60
超带宽能量密度/J	4～16

1)加密时间误差

图4所示为本机制与OEUW机制及LTED机制在加密时间误差上的仿真对比情况，由图4可知，随着元数据总量的不断增加，本算法的加密时间误差始终处于较低的水平，而两种对照组机制的加密时间误差均要高于本算法。这是由于本算法采取大数据混沌耦合方式，能够改善混沌递归集的混沌性能，从而在加密过程中可有效的提高加密效率，从而降低了加密时间误差；OEUW机制的混沌递归集仅采用简单现象收敛方式进行一次性生成，需要对

全部的元数据进行线性维度排序后采取冒泡机制进行收敛，因此加密过程中存在严重的不稳定性，导致加密时间误差较高；LTED机制使用超线性一体化成型的方式，需要将元数据进行粒度分割后方可进行混沌递归集的收敛过程，因此导致加密的鲁棒性较差，因而加密时间误差也要高于本算法。

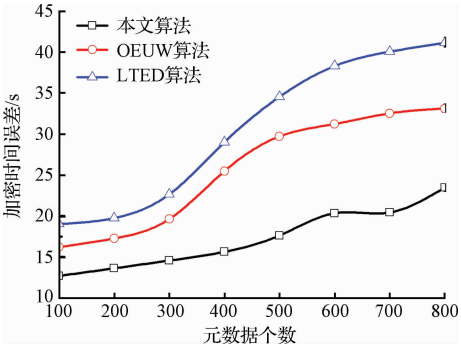

图4　3种算法加密时间测试

2)数据收敛相对误差

图5所示为本机制与OEUW机制及LTED机制在数据收敛相对误差上的仿真对比情况；由图5可知，随着元数据数量的不断增加，本机制与两种对照组机制均出现数据收敛相对误差下降的现象，且本文机制的数据收敛相对误差幅度下降的更为距离，显示了良好的收敛性能；这是由于本算法采取的大数据混沌耦合方式能够有效的提高混沌递归集的收敛强度，且采取的线性度微分方式可提高收敛过程中数据对环境波动的适应性能；OEUW机制由于需要采取推断方式对任意时刻的混沌递归集进行数据分割，且需要进行混沌度判断后方可将分割过后的混沌递归集进行二次整合，因此数据收敛过程中收敛性能要低于本算法；LTED机制虽然不需要将混沌递归集进行数据分割，然而由于该机制需要通过复杂的校验机制进行数据整合，因此导致了数据收敛性能出现严重的下降现象，造成数据收敛相对误差要高于本机制。

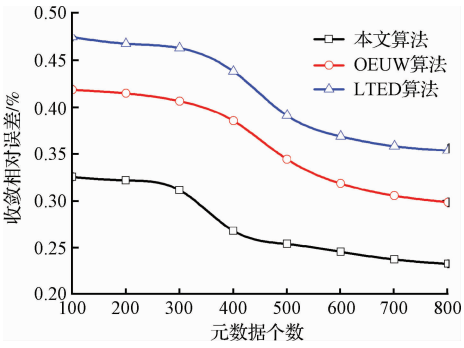

图5　3种算法数据收敛相对误差测试

3)加密时延

图6所示为本机制与OEUW机制及LTED机制在加密时延性能上的仿真对比情况；由图6可知，本机制与对照组机制均随着元数据的不断增加而出现加密时延上升的现象，然而本机制的加密时延要始终低于对照组机制，且波动也较为平缓，具有良好的加密时延性能；这是由于本机制采用微分方式，能够在元数据阶数的范围内实现加密过程的迅速收敛；OEUW机制及LTED机制均为超线性阶数的方式进行时延控制，最佳收敛阶数也远远高于元数据阶数，且两种对照组算法加密过程中需要对混沌递归集进行复杂的处理，该过程也将显著增加加密过程中出现时延的可能性，因此两种对照组算法的加密时延性能均要低于本文算法。

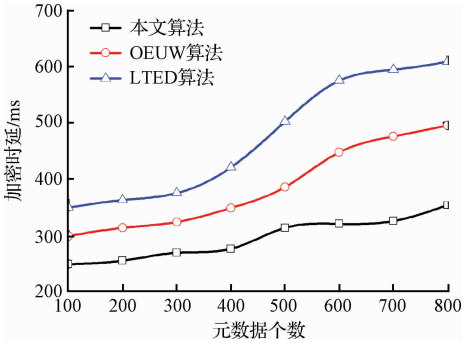

图6　3种算法定位时延测试

4)加密带宽/传输带宽占比

图7所示为本机制与OEUW机制及LTED机制在加密带宽/传输带宽性能上的仿真对比情况；由图7可知，本机制的加密带宽/传输带宽占比始终要低于两种对照组机制，这是由于本机制在加密过程中不需要对混沌递归集进行任何处理，该混沌递归集均通过自然方式收敛生成，因此带来的加密带宽数量有限；OEUW机制需要采用冒泡方式进行混沌递归集的收敛过程，因此随着冒泡数量的不断增加极易导致出现收敛失败的现象，因而需要更多的加密带宽进行数据保障；LTED机制虽采取一体化成型的方式，然而由于该算法需要采用校验方式对成型质量进行裁决，每次的校验均将产生一定数量的加密带宽，因此导致LTED机制的加密带宽/传输带宽性能要差于本算法。

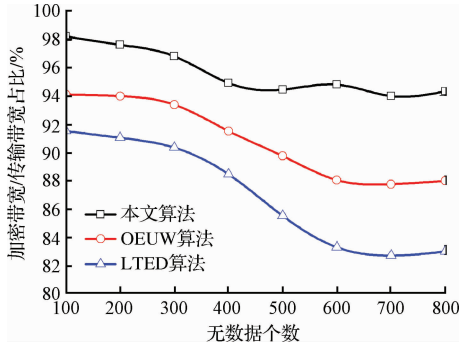

图7　3种算法加密带宽/传输带宽占比测试

4 结 论

为解决当前 WSN 网络数据自递归加密机制难以实现较高的收敛程度、元数据性能不高、混沌递归集生成过程复杂等不足，提出了一种基于大数据混沌耦合优化方式的 WSN 网络数据自递归加密机制；该机制采用元数据交互的方式直接生产混沌递归集，且进行资源整合过程中采取微分方式，改善算法的收敛性能，极大的增强了本机制的适用性能。仿真实验表明，本算法具有加密时间误差低，数据收敛容易等优势，具有显著的实际使用价值。

下一步，将针对本机制收敛过程中对累积误差时延的适应性较低等不足，采用超混沌移动二次成型一体化映射机制，进一步改善本算法的混沌递归集的收敛性能，促进本文算法在实际领域中的使用。

参 考 文 献

[1] 章韵，巨德文.基于可预测移动汇聚节点的无线传感网分簇算法研究[J].计算机科学，2012，6(9)：89-92.

[2] LI J，LI J，CHEN H，et al. Data transmission scheduling algorithm for rapid-response earth-observing operations[J]. Chinese Journal of Aeronautics，2014，2(7)：349-364.

[3] JIANG H，JIN S，WANG C. Prediction or not? An energy-efficient framework for clustering based data collection in WSN[J]. Parallel and Distributed Systems，IEEE Transactions，2010，22(6)：1064-1071.

[4] ZENG L，LI X，JI H，et al. Cross-layer adaptive resource allocation algorithm with diverse QoS requirements for single-cell OFDMA systems[J]. Journal of Harbin institute of Technology，2015，22(1)：15-22.

[5] AHMED A，BAKAR K A，CHANNA M I，et al. A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks[J]. Frontiers of Computer Science，2015，9(2)：280-296.

[6] 朱舟，余绍俊，于勃. WSN 节点中能量管理方案设计[J].电子测量与仪器学报，2015，29(12)：1798-1805.

[7] 余小华.一种基于蚁群优化的 WSN 拥塞控制算法[J].计算机应用研究，2012，29(4)：1525-1528.

[8] 何敏，官铮，保利勇. 无线传感器网轮询接入控制平均查询周期分析[J]. 仪器仪表学报，2016，37(11)：2637-2644.

[9] SICHITIU M L. Cross-layer scheduling for power efficiency in WSN[C]. 23rd Annual Joint Conference of the IEEE Computer and Communications Societies，2004.

[10] 肖欣招，魏峰. 无线传感器网络能量改进路由算法研究[J].电子测量技术，2016，39(10)：183-187.

[11] 孙昊，马列. 基于 IPv6 的无线传感器网络协议一致性测试方法研究[J]. 国外电子测量技术，2013，32(2)：29-31.

[12] LIN Q M，WANG R CH，GUO J，et al. Novel congestion control approach in wireless multimedia sensor networks [J]. The Journal of China Universities of Posts，2011，18(2)：1-8.

[13] 刘军. 基于 NS2 的无线传感器网络 LEACH 协议的改进与仿真[J]. 电子技术应用，2013，38(2)：21-23.

[14] SHAH S A，NAZIR B，KHAN I A. Congestion control algorithms in wireless sensor networks：Trends and opportunities [J]. Journal of King Saud University Computer and Information Sciences，2015，4(1)：108-114.

[15] LIN Q M，WANG R CH，GUO J，et al. Novel congestion control approach in wireless multimedia sensor networks [J]. Journal of China Universities of Posts and Telecommunications，2011，18(2)：1-8.

作 者 简 介

杜宗福，1975 年出生，硕士，讲师，主要研究方向为计算机网络、信息安全、计算机应用。

E-mail：DuzongF1975bjd@163.com