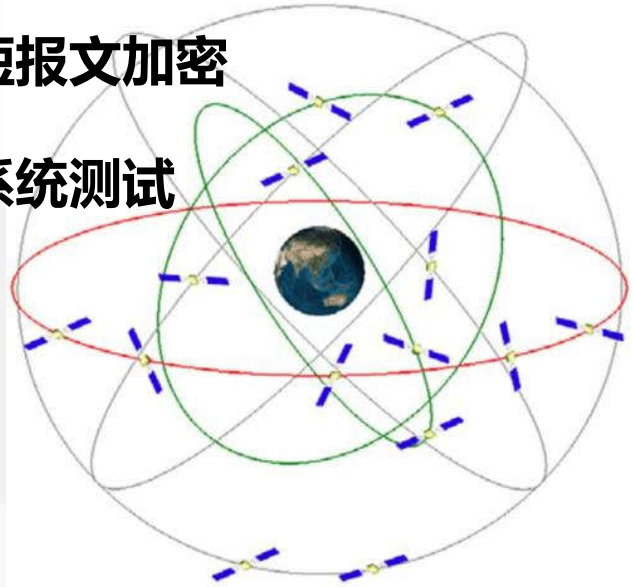
北斗导航系统短报文加密技术研究

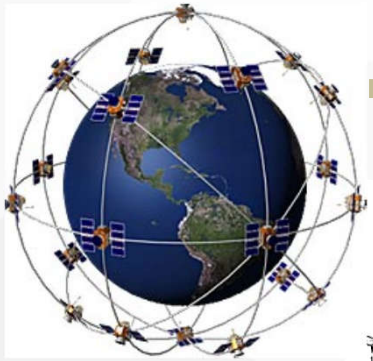
周一廷

目 录
Contens

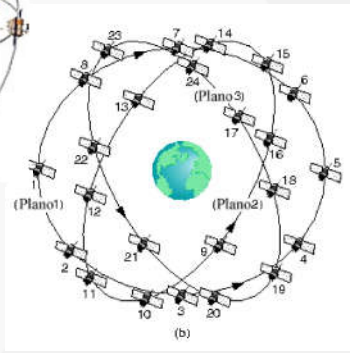


课题研究意义

课题研究意义-四个全球定位导航系统

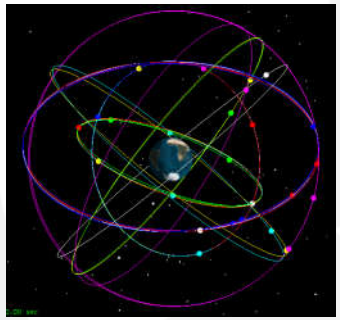


美国 GPS导航系统



俄罗斯 GLONASS系统

高精度定位导航、
高可靠授时



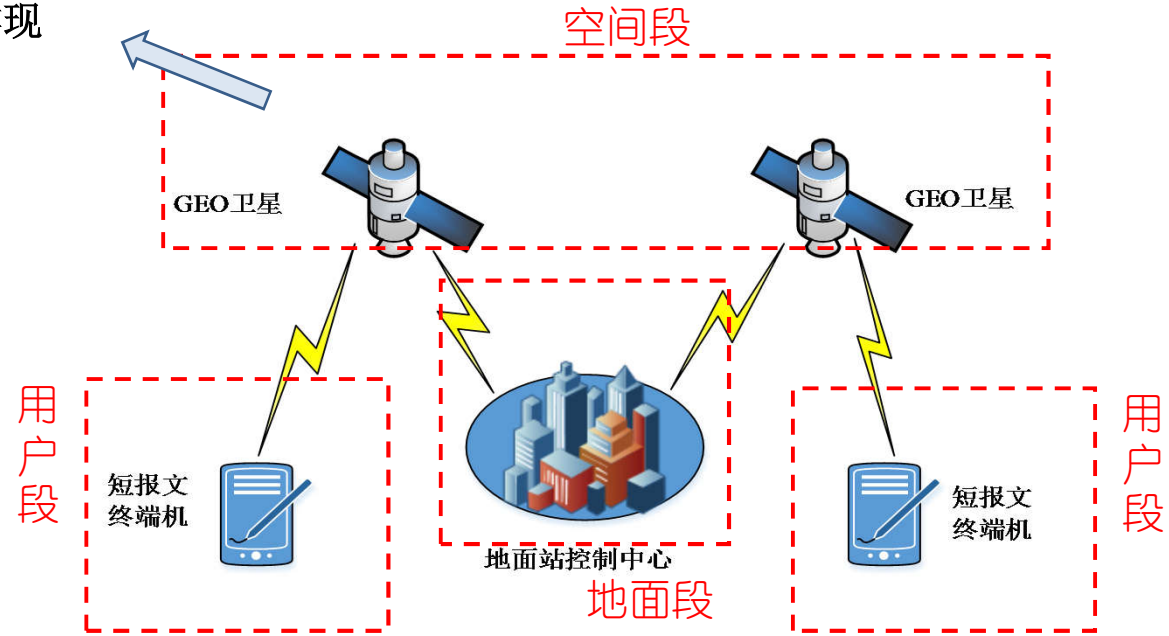
中国 北斗导航系统

欧盟 GALILEO导航系统

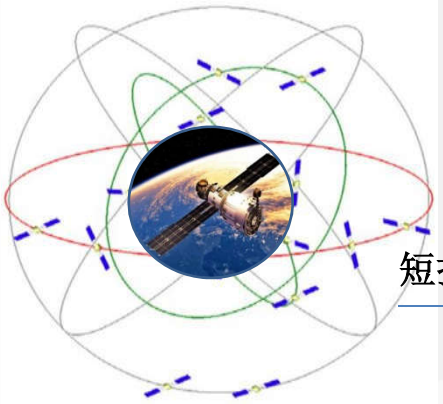
短报文通信功能
北斗独有
应用广泛：
海事、交通、航天

北斗短报文系统架构图

5颗GEO卫星实现



课题研究意义与主要工作-短报文通信优点及存在的问题



短报文通信优点：

1. 覆盖区域广，无通信盲区
2. 具备远距离通信能力
3. 应用广泛
4. 实现简单

短报文通信存在的问题：

1. 传输过程数据采用明文形式
2. 信息的载波频率、调制方式、传输格式等基本信息均公开
3. 传输过程未采用任何加密措施

解决办法 → 对短报文传输数据采取安全措施

课题研究意义与主要工作-研究现状

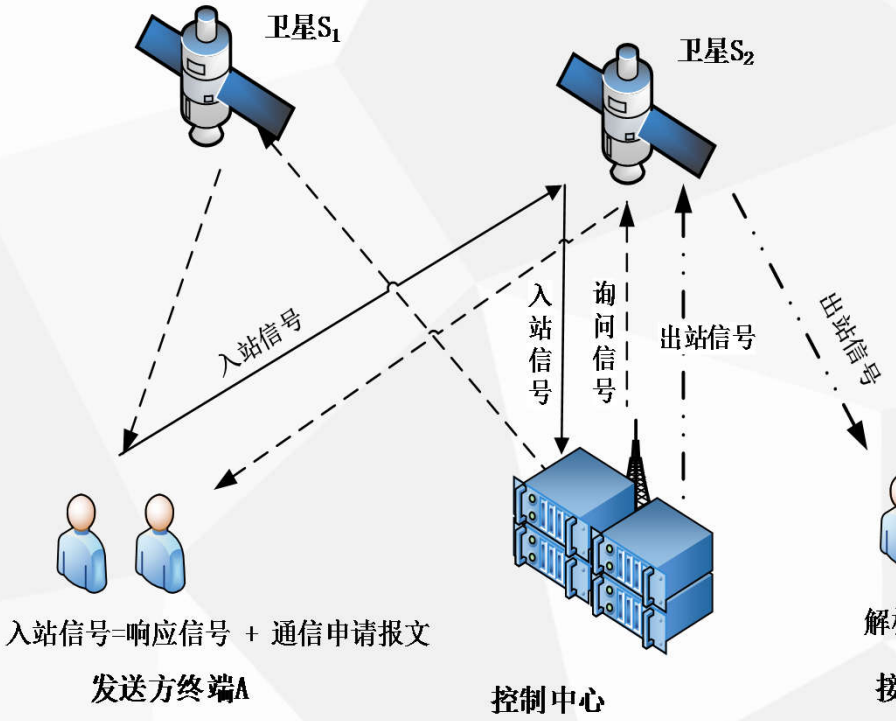
采用密码学加密方法解决短报文传输安全性问题

1. 非对称算法实现信息来源认证、授权访问
2. 国密SM1加密 SM2身份认证
3. 增加加密模块

混沌加密技术和对称加密技术对短报文传输数据进行安全加密

短报文通信加密方案

短报文通信加密方案-加密对象



加密对象

通信申请协议

指令	长度	用户地址	信息内容					校验和
通信申请 $TXSQ	16bit	24bit	信息类别 8bit	用户地址24bit	电文长度 16bit	是否应答 8bit	电文内容	8bit

短报文通信加密方案-短报文常见传输内容

02
聊天交流信息

04
救援信息

01
监测数据

03
定位信息

短报文通信加密方案-定位传输协议

指令	长度	用户地址	定位信息						校验和
$BDM	38	249449	序号	时间	纬度	N/S	经度	E/W	04
5	1	3	2	6	9	1	10	1	1

定位信息传输协议显示示例如下：

$BDM,78,1,091937,3414.0447,N,10854.8080,E,374.4,7

$BDM,78,8,092108,3414.0428,N,10854.8083,E,376.2,2

ASCII码形式：

24 42 44 4D 2C 37 38 2C 31 2C 30 39 31 39 33 37 2C 33 34 31 34 2E 30 34 34
37 2C 4E 2C 31 30 38 35 34 2E 38 30 38 30 2C 45 2C 33 37 34 2E 34 2C 37

24 42 44 4D 2C 37 38 2C 38 2 C 30 39 32 31 30 38 2C 33 34 31 34 2E 30 34 32
38 2C 4E 2C 31 30 38 35 34 2E 38 30 38 33 2C 45 2C 33 37 36 2E 32 2C 32

短报文通信加密方案-短报文数据特征

1. 数据传输格式固定
2. 数据以明文形式进行传输
3. 传输数据值相对集中
4. 单条报文数据量有限
5. 短报文服务频度有限

短报文通信等级分类

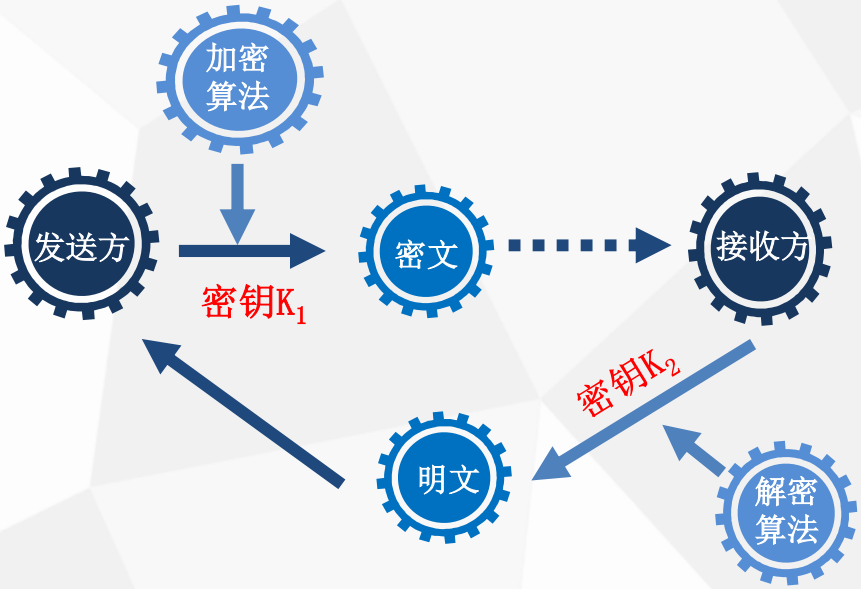
通信等级	电文长度	备注
1	110bit	7个汉字/27个BCD
2	408bit	29个汉字/102个BCD
3	628bit	44个汉字/157个BCD
4	848bit	60个汉字/210个BCD

北斗卡服务频度

用户类别	服务频度	默认值
一类	300-600秒/次	600秒/次
二类	10-60秒/次	60秒/次
三类	1-5秒/次	5秒/次

短报文通信加密方案-短报文加密密码系统

密码系统结构



当$K_1=K_2$时，为对称密钥加密算法

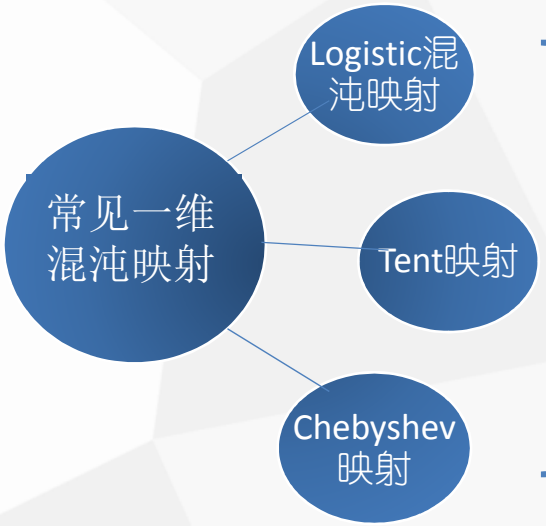
当$K_1\neq K_2$时，为非对称密钥加密算法（公钥算法）

混沌理论和传统密码学的对应关系

混沌系统		密码算法
对初值和参数的敏感性	⟷	扩散
迭代	⟷	循环
参数或初值	⟷	密钥
相空间；实数集	⟷	相空间；有限集

基于混沌映射的短报文加密方法

基于混沌映射的短报文加密方法-混沌加密算法



1. logistic组成最为简单
2.NIST随机性检测，logistic随机性通过率为93.75%

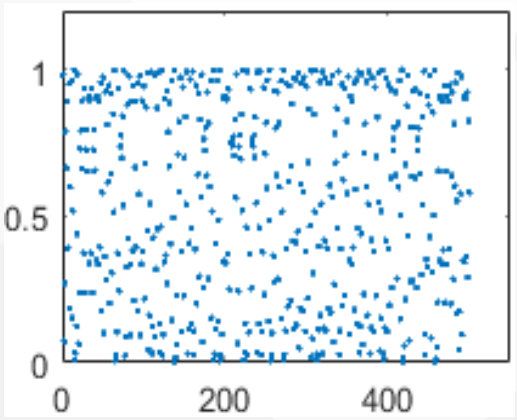
Logistic混沌映射：

$$X_{n+1} = \mu \bullet X_n \bullet (1 - X_n) \quad n \geq 0$$

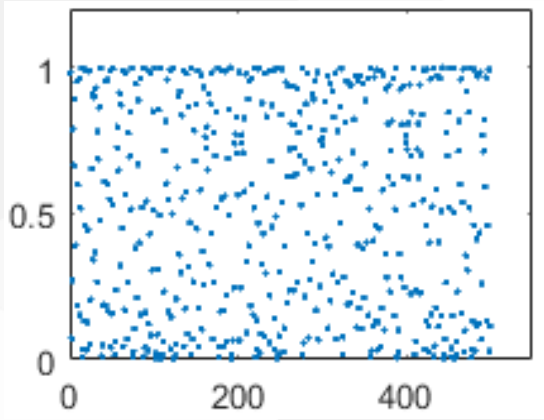
关键参数	X_n 上一轮映射结果值
	μ 控制参数

$$\mu \in [3.56994, 4.0] \qquad x_0 \in [0,1]$$

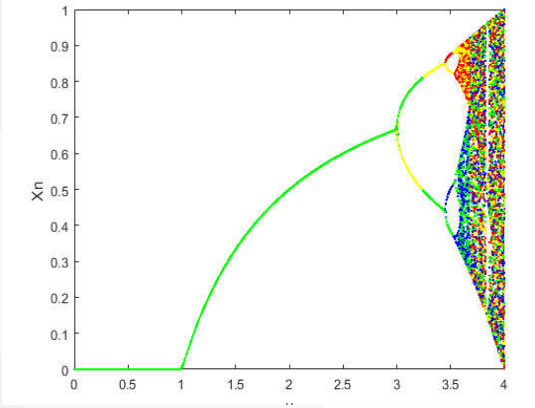
基于混沌映射的短报文加密方法-Logistic混沌映射特性



$X_0 = 0.566\ 6779$ 时的混沌序列

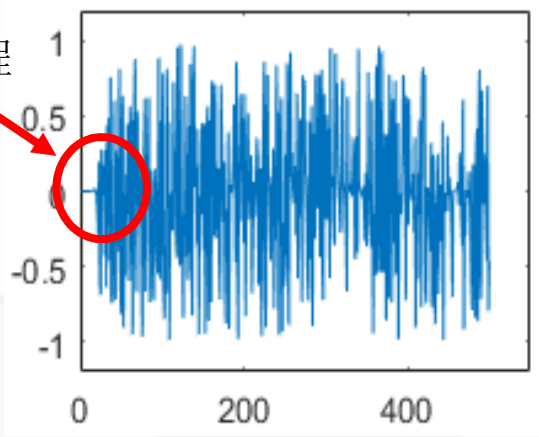


$X_0 = 0.566\ 6778$ 时的混沌序列



Logistic映射分岔图

过渡过程



迭代500次差值序列图

Logistic算法的穷举攻击

以混沌初值 $x_0 \in (0,1)$ 和关键参数 $\mu \in [3.56994, 4.0]$ 作为算法密钥进行密钥空间计算，一般计算机所能支持小数的最大精确度为14位小数值，因此密钥空间大小为：

$$K = 0.5\times10^{14}\times1\times10^{14} = 0.5\times10^{28}$$

根据Alvarez G , Li S提出的第15条安全性规则，依靠目前计算机软硬件资源条件，密钥空间能有效抵抗穷举攻击的大小应不小于 $2^{100} = 1.27\times10^{30}$

基于混沌映射的短报文加密方法-改进Logistic算法实现

Tent映射作为局部映射的一维耦合映像格子迭代公式：

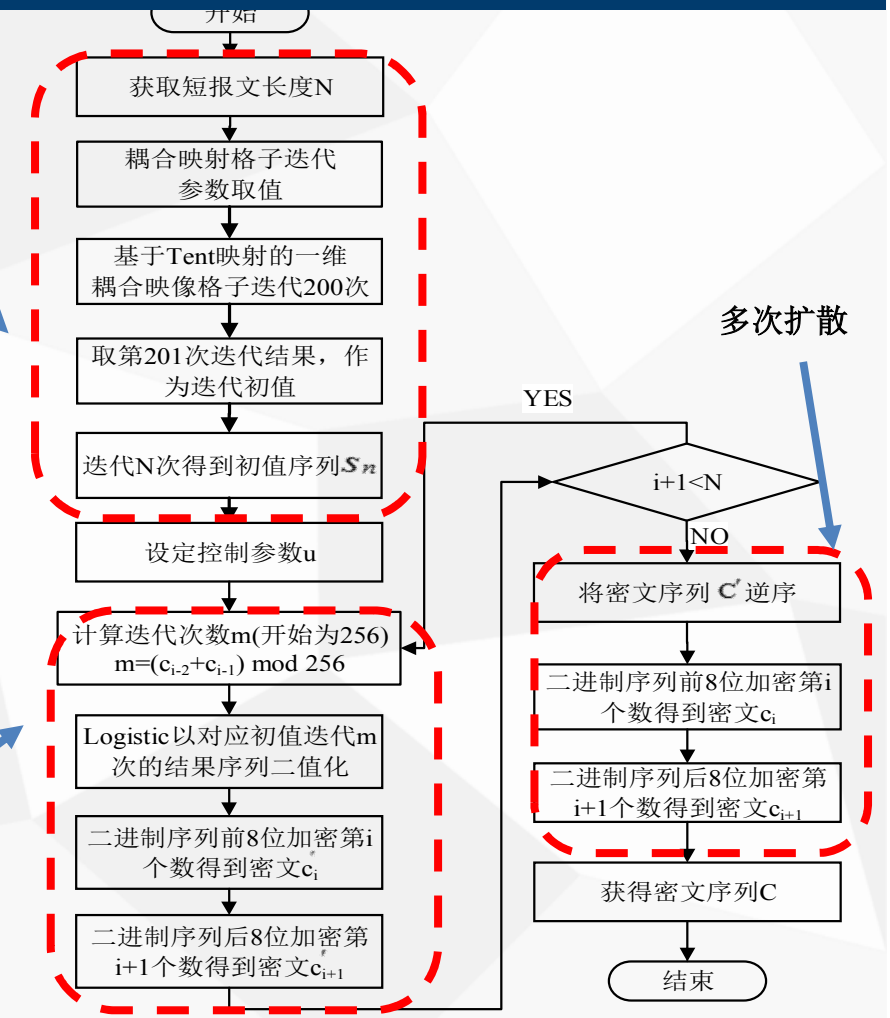
$$x_{n+1}^{i}=\begin{cases}(1-\varepsilon)\left(\dfrac{x_n^i}{q^i}\right)+\dfrac{\varepsilon}{2}\times\left(\left(\dfrac{x_n^{i+1}}{q^{i+1}}\right)+\left(\dfrac{x_n^{i-1}}{q^{i-1}}\right)\right) & x_n^i\in\left(0,q^i\right] \\ (1-\varepsilon)\left(\dfrac{1-x_n^i}{1-q^i}\right)+\dfrac{\varepsilon}{2}\times\left(\left(\dfrac{1-x_n^{i+1}}{1-q^{i+1}}\right)+\left(\dfrac{1-x_n^{i-1}}{1-q^{i-1}}\right)\right) & x_n^i\in\left(q^i,1\right)\end{cases}$$

$$(i=1,2,3)$$

关键参数为：$\left(x_0^1,x_0^2,x_0^3,q^1,q^2,q^3\right)$

耦合混沌系统生成迭代初值

- 迭代次数由前面的密文数据生成
- 一次加密两个明文数值



序列随机性分析

根据混沌序列的概率分布函数，则混沌序列的均值能够表示为：

$$\overline{X}=\lim_{N\to\infty}\frac{\sum_{i=0}^{N-1}X_i}{N}=\int_0^1 X\rho(X)dX=0$$

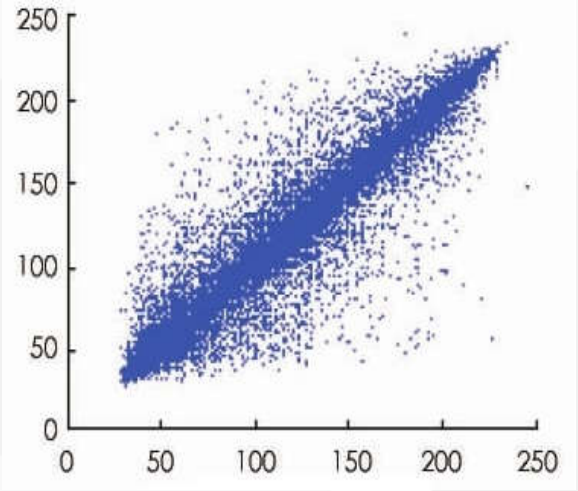
混沌序列的关联函数为：

$$c=\lim_{N\to\infty}\frac{\sum_{i=0}^{N-1}\left(X_i-\overline{X}\right)\left(Y_i-\overline{Y}\right)}{N}=\int_0^1\int_0^1\left(X_i-\overline{X}\right)\left(\tau^{(t)}(Y)-\overline{Y}\right)=0$$

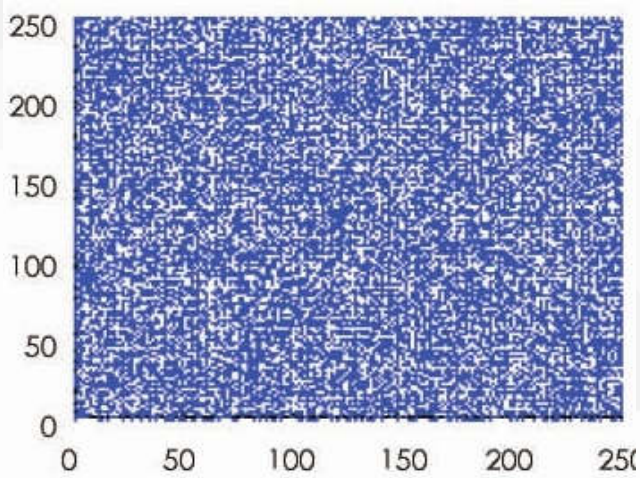
可以看出其混沌序列均值和关联函数值均为0，说明耦合混沌加密映射产生的混沌序列统计学特性与白噪声相似，其混沌序列是具有足够随机性的。

基于混沌映射的短报文加密方法-相关性分析

1000条短报文的通信申请协议电文部分加密前后明文序列和密码序中的相关分布



短报文明文序列相关分布



短报文加密密文序列相关分布

计算其相关系数分别为0.9814和0.0085,改进的算法加密后其数据间的相性变得很小，密文数据具有较高的混沌特性，满足随机分布。

基于混沌映射的短报文加密方法-改进算法穷举攻击

改进加密算法中用于生成Logistic加密密钥的关键参数分别有 $\left(x_0^1, x_0^2, x_0^3, q^1, q^2, q^3\right)$ 等6个关键参数，关键参数可看作整个算法的密钥参数，则其密钥空间最大为：

$$K = \left(1\times10^{14}\right)^6 = 1\times10^{84} > 2^{100}$$

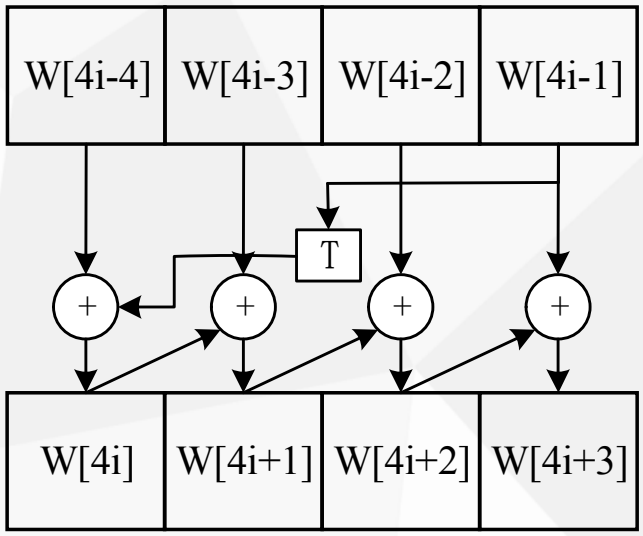
算法	密钥空间大小	穷举攻击
Logistic算法	0.5 x 10^{28}	不能抵抗
改进加密算法	1.0 x 10^{84}	能抵抗

基于对称体制的短报文加密方法

基于对称体制的短报文加密方法-对称加密算法加解密速率分析

算法	工作模式	执行时间
DES 算法	ECB	10.65MB/S
	CBC	10.67MB/S
3DES算法	ECB	4.59MB/S
	CBC	4.59MB/S
AES算法	ECB	12.73MB/S
	CBC	12.74MB/S
SM1算法	ECB	3.38MB/S
	CBC	3.38MB/S
SM2-192算法	点乘	0.73s/次以上
	生成秘钥	0.73s/次
	公钥运算	2.10s/次
	私钥运算	0.73s/次
	签名	1.05s/次
	验证	2.11s/次

基于对称体制的短报文加密方法-AES对称加密算法存在的问题



AES密钥数组扩展

AES密钥生成过程中当前轮密钥仅与上一轮密钥有关，不能有效抵抗Square攻击

解决方案

基于二维离散混沌映射系统TD-ERCS（切延迟椭圆反射腔映射系统）生成AES加密密钥

- 每一轮加密由混沌映射迭代获取新的轮密钥
- 每个轮

基于对称体制的短报文加密方法-TD-ERCS混沌映射公式

迭代次数满足n>m+1

TD-ERCS混沌映射公式：

$$\begin{cases} x_n = -\dfrac{2k_{n-1}y_{n-1} + x_{n-1}\left(\mu^2 - k_{n-1}^2\right)}{\mu^2 + k_{n-1}^2} \\ k_n = -\dfrac{2k'_{n-m} - k_{n-1} + k_{n-1}k'^2_{n-m}}{1+2k_{n-1}2k'_{n-m} - k'^2_{n-m}} \end{cases} \quad n > m+1$$

$$y_n = k_{n-1}\left(x_n - x_{n-1}\right) + y_{n-1}$$

初始值及切斜率：

$$y_0 = \mu\sqrt{1-x_0^2}$$

$$k'_0 = -\frac{x_0}{y_0}\mu^2$$

发生模型切延迟**m**后椭圆切线的斜率：

$$k'_{n-m} = \begin{cases} -\dfrac{x_{n-1}}{y_{n-1}}\mu^2 & n < m \\ -\dfrac{x_{n-m}}{y_{n-m}}\mu^2 & n \geq m \end{cases}$$

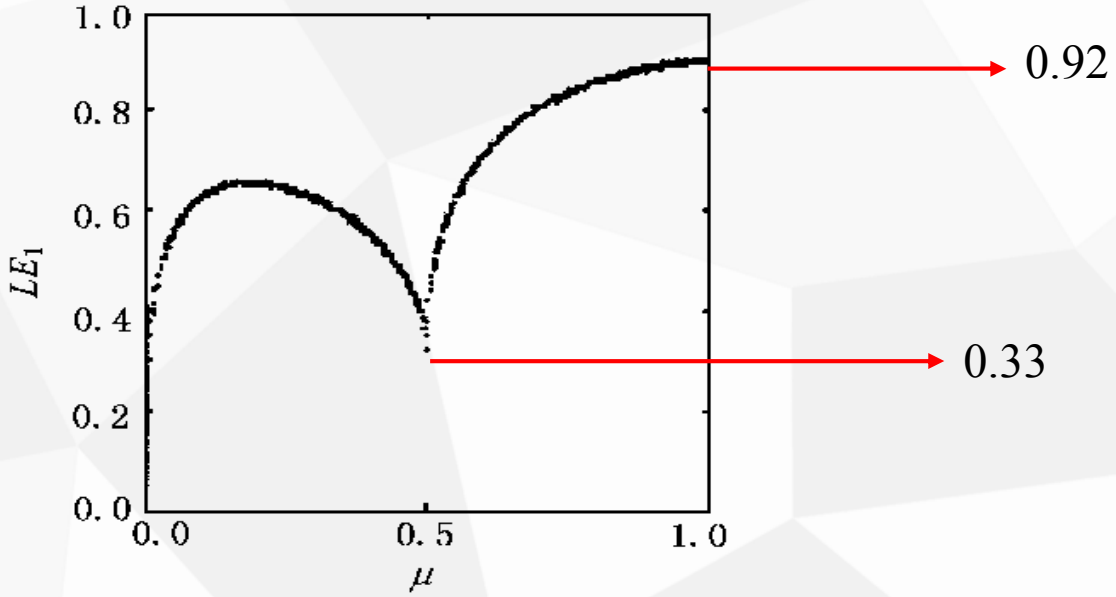
由系统入射角**α**的正切函数可得序列$\mathbf{k_n}$中的值$\mathbf{k_0}$：

$$k_0 = \frac{\tan\alpha + k'_0}{1 - k'_0\tan\alpha}$$

$\mu(0 \leq \mu \leq 1)$　　$x_0(-1 \leq x_0 \leq 1)$　　$\alpha(0 \leq \mu \leq \pi)$

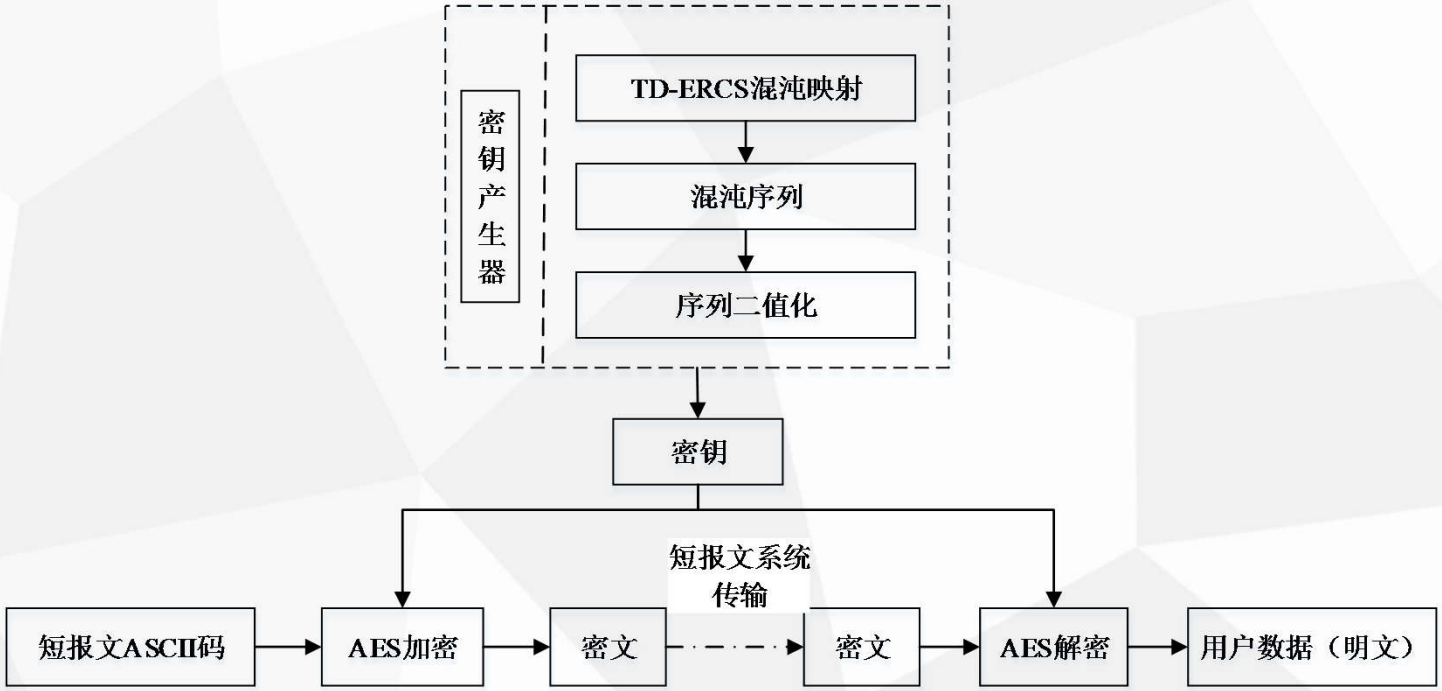
基于对称体制的短报文加密方法-李雅普诺夫（Lyapunov）指数

定义域内最大的Lyapunov指数随系统参数变化



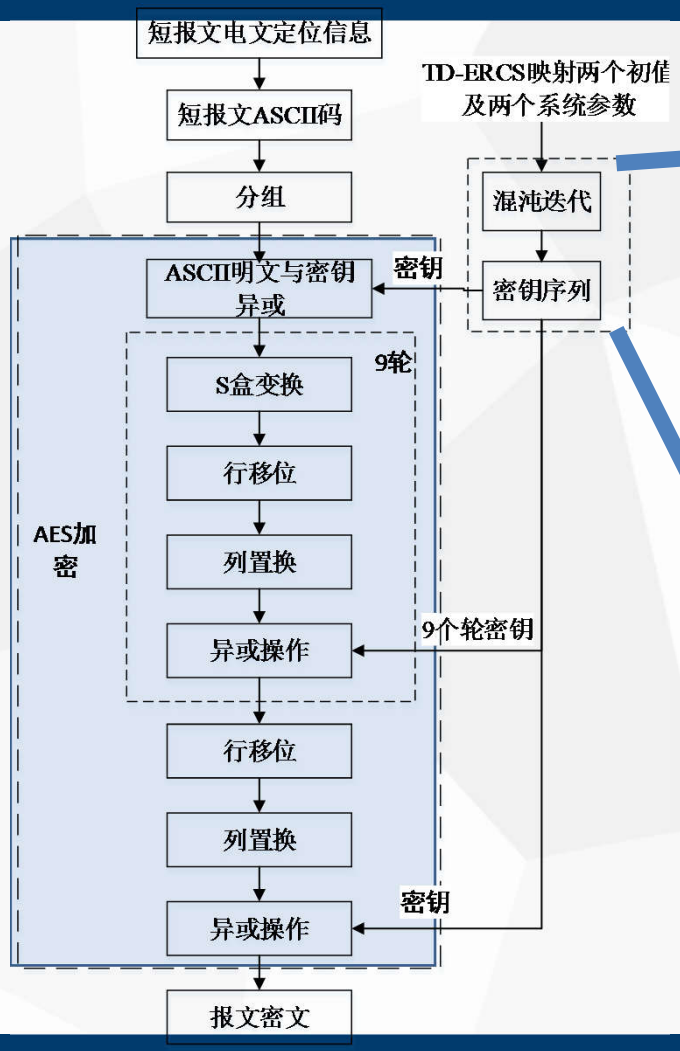
当指数为正时证明映射局部运行轨道存在不稳定性。正值越大，表示邻近的两个点之间的信息量丢失越严重，映射系统的混沌性能越好。

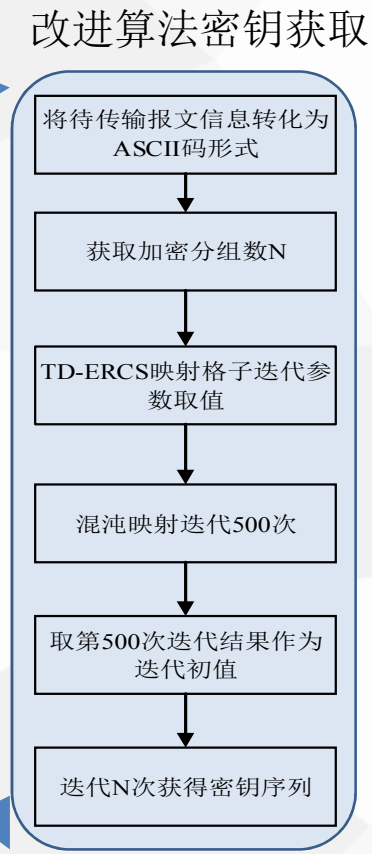
基于对称体制的短报文加密方法-改进算法加密原理图



基于TD-ERCS混沌改进算法加密短报文原理图

基于对称体制的短报文加密方法-改进算法密钥获取





基于对称体制的短报文加密方法-改进算法穷举攻击分析

改进算法密钥长度与传统AES加密算法长度一致均为128位，此时密钥空间为：

$$\frac{1}{2^{128}}\sum_{i=1}^{2^{128}} i \approx 1.70\times10^{38}=2^{127}>2^{100}$$

改进算法密钥空间主要考虑混沌映射中的两个初始参数X_0和a以及两个系统参数u和m，则其密钥空间大小为：

$$K = 1\times10^{14}\times2\times10^{14}\times3.14\times10^{14}=6.28\times10^{42}>2^{128}>2^{100}$$

算法	密钥空间大小	穷举攻击	Square攻击
AES算法	1.70×10^{38}	能抵抗	不能
改进加密算法	6.28×10^{42}	能抵抗	能

北斗短报文加密系统实现与测试

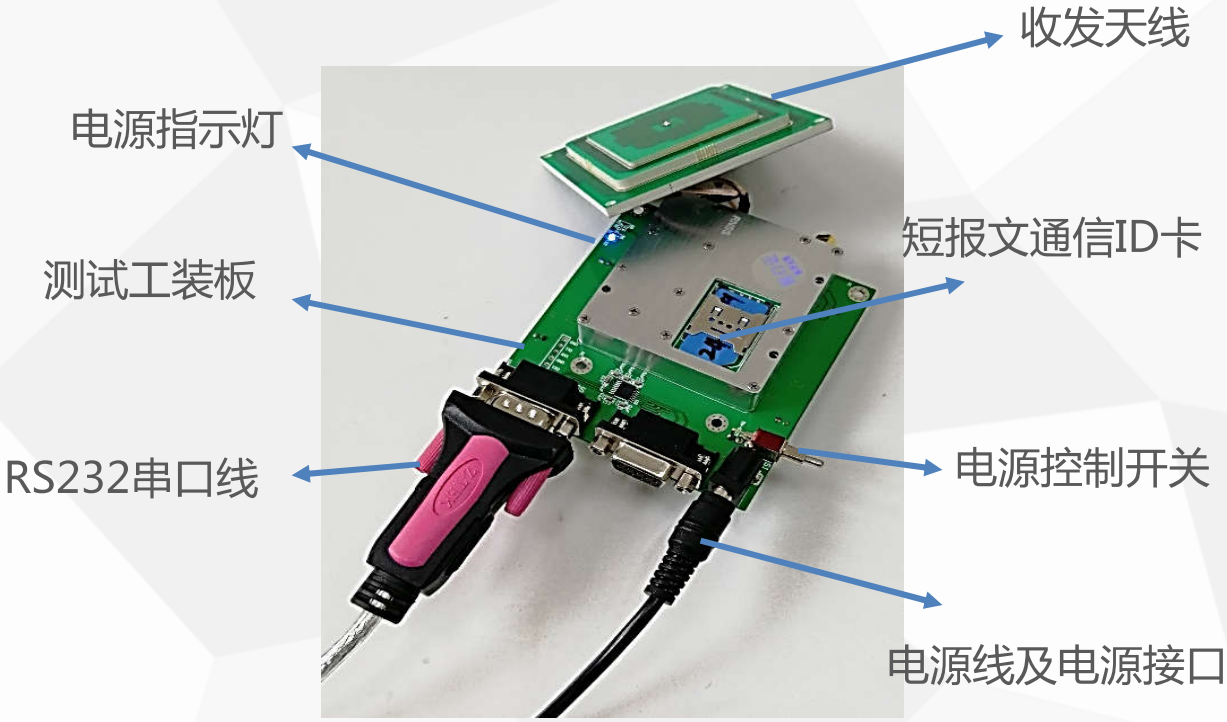
测试过程：

- 硬件平台搭建
- 软件平台搭建
- 传输数据统计
- 算法可行性验证

测试内容：

- 传输延时

硬件平台结构图

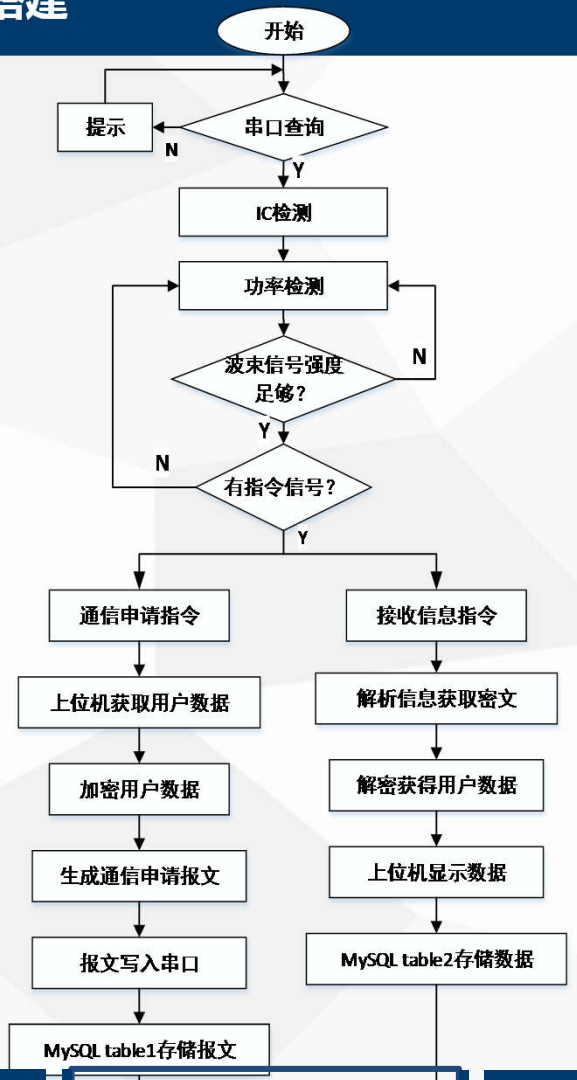


北斗短报文加密系统实现与测试-系统软件平台搭建

开发环境

系统参数项	说明
版本号	64位Windows7操作系统
处理器	Intel(R) Core(TM) i3-3220 CPU @ 3.3 0GHz
内存	4GB
编程平台	Visual Studio 2015
编程语言	C#

系统实现流程图



北斗短报文加密系统实现与测试-测试环境及数据

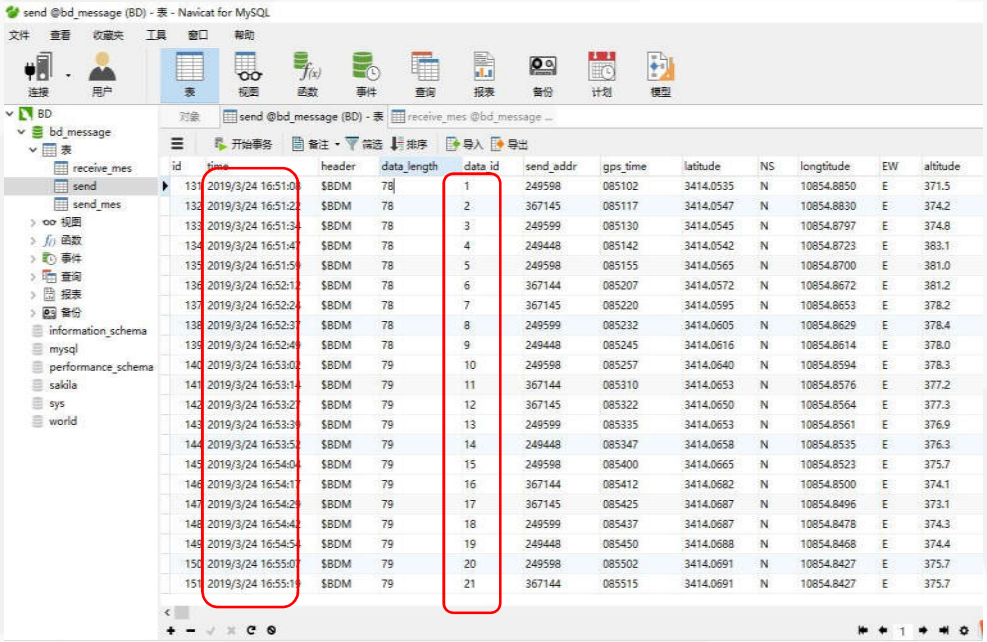
测试环境

- 传输用户由定位信息传输协议生成
- 包含当前报文序号

- 波束信号较好
- 进行6次报文集测试

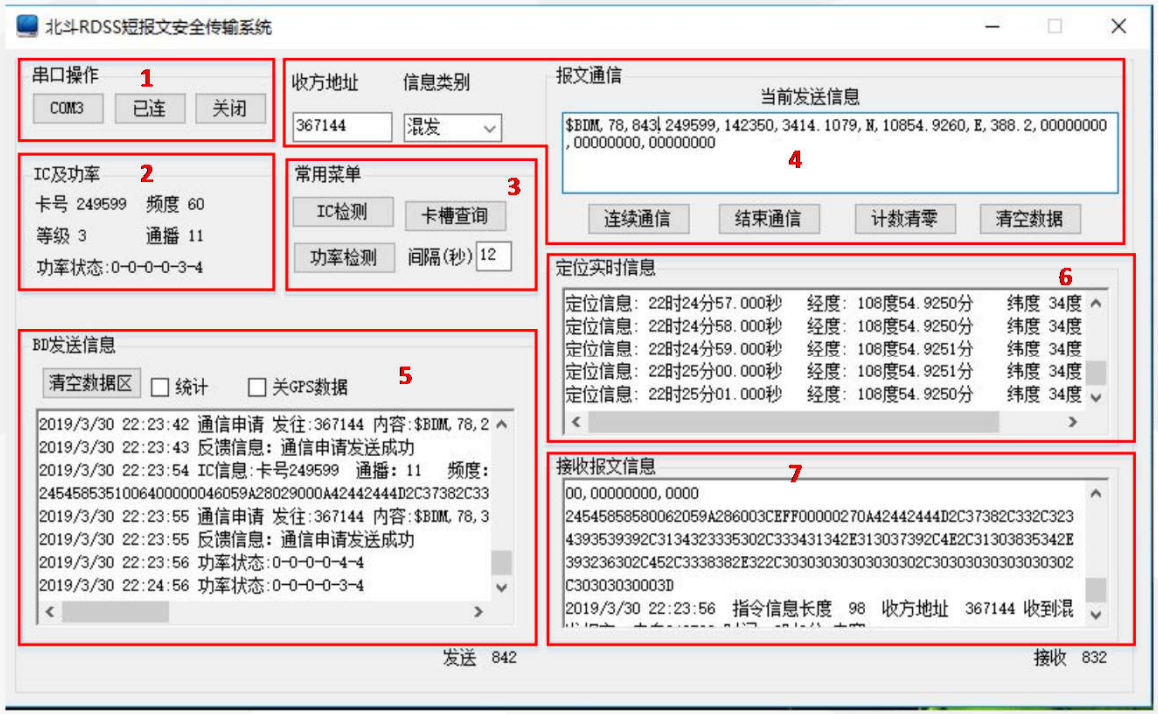
- 5张ID卡轮询机制
- 服务频度12s/次

发送报文数据界面



北斗短报文加密系统实现与测试-传输系统界面图

北斗RDSS短报文安全传输系统界面图



$\bar{\tau}$=1.47s

北斗短报文加密系统实现与测试-传输延时计算

统计数据集BDM-4中报文数据收发成功的830条数据收发时间的延时进行计算得到平均延时。

短报文数据为：

发送数据时间信息：

1 2019/3/30 18:43:00 $BDM,78,1,367145,104255,3414.1036,N,10854.9154,E,404.1,19

2 2019/3/30 18:43:15 $BDM,78,2,249599,104310,3414.1026,N,10854.9134,E,410.9,45

3 2019/3/30 18:43:27 $BDM,78,3,249448,104323,3414.1018,N,10854.9114,E,412.2,54

· · · · · ·

837 2019/3/30 21:37:18 $BDM,80,837,249599,133714,3414.1043,N,10854.9263,E,404.3,32

838 2019/3/30 21:37:30 $BDM,80,838,249448,133726,3414.1047,N,10854.9277,E,404.1,16

839 2019/3/30 21:37:43 $BDM,80,839,249598,133739,3414.1062,N,10854.9236,E,405.0,26

接收数据时间信息：

1 2019/3/30 18:43:02 104255 $BDM,78,1,367145,104255,3414.1036,N,10854.9154,E,404.1,12

2 2019/3/30 18:43:16 104310 $BDM,78,2,249599,104310,3414.1026,N,10854.9134,E,410.9,25

· · · · · ·

829 2019/3/30 21:37:32 133726 $BDM,80,838,249448,133726,3414.1047,N,10854.9277,E,404.1,41

830 2019/3/30 21:37:44 133739 $BDM,80,839,249598,133739,3414.1062,N,10854.9236,E,405.0,19

计算式为：

$$\bar{\tau} = \frac{1}{N}\sum_{i=1}^{N} T_1 - T_2$$

结果为：

计算平均延时为：$\bar{\tau} = 1.47s$

传统平均延时为：$\bar{\tau} = 1s$

工作总结

工作总结

主要工作

确定北斗短报文安全加密方案：

- 针对短报文申请协议电文内容进行数据加密
- 设计电文定位信息传输协议

基于耦合混沌系统的Logistic加密算法：

- logistic混沌加密算法加密短报文对应数据
- 耦合多个混沌加密算法改进Logistic算法
- 验证算法安全性与可行性

基于TD-ERCS的改进AES算法：

- 基于TD-ERCS混沌系统生成加密密钥
- 验证算法安全性

北斗短报文加密系统测试：

- 搭建北斗短报文加密系统（包含改进加密算法）
- 计算传输平均延时

感谢聆听！