基于 SRCSM 的装备无线分布式测试系统数据加密传输

李　超[1]，肖明清[1]，王　矗[2]，陈永龙[3]，张　磊[3]，唐希浪[1]
(1.空军工程大学航空工程学院，西安，710038；2.94106 部队，西安，710614；
3.国防大学联合勤务学院，北京，100858)

摘要　在非对称加密技术的基础上，提出了一种自定位随机编码签名机制(SRCSM)。该方法将 LR 签名算法与随机编码相结合，通过软件逻辑对移动接收端及接收端通信时所处物理区域划定接收权限，防止无关人员或相关人员在非规定地点接收到加密信息，防止造成无意识泄密。简要介绍了 SRCSM 的基本内容，并将其与非对称加密技术相结合，搭建了装备分布式测试系统数据加密无线传输框架，实验表明采用 SRCSM 进行加密传输时，相比于无加密传输，测试最长耗时增加 26.67%、测试总时增加 46.67%、CPU 使用率增加 50%，测试可平稳进行；当丢包率较小，同时监听个数较大时，算法可将通信被监听概率降低 5 个数量级。

关键词　分布式测试系统；无线通信；SRCSM；保密性
DOI　10.3969/j.issn.1009-3516.2018.02.013
中图分类号　TP274　　**文献标志码**　A　　**文章编号**　1009-3516(2018)02-0072-07

Research on Data Encryption Transmission of Wireless Distributed Test System Based on SRCSM

LI Chao[1], XIAO Mingqing[1], WANG Chu[2], CHEN Yonglong[3], ZHANG Lei[3], TANG Xilang[1]
(1. Aeronautics Engineering College, Air Force Engineering University, Xi'an 710614, China;
2. Unit 94106, Xi'an 710038, China; 3. Joint Service College, National Defense University, Beijing 100858, China)

Abstract: Aimed at the problem that wireless communication in the broadcast of the transmission has a threat against the military information on the safe transmission, this paper proposes a self-locating random coded signature mechanism (SRCSM) on the basis of asymmetric encryption technology. The method combines the LR signature algorithm with the random code through defining the receiving right of the physical area while the mobile receiver and the receiving end are communicating by the software logic to prevent the unrelated person or related person from receiving the encrypted information at the non-specified location and preventing cases of unconscious leakage of a state secret. The paper briefly introduces the basic content of SRCSM, and combines it with asymmetric encryption technology to build a distributed data system with distributed data encryption system, and analyzes its complexity and execution efficiency, and finally analyzes it with data analysis. The experiments show that using SRCSM encrypted transmission, compared to non encrypted transmission, the longest test time increased by 26.67%, total test period 46.67%, CPU utilization rate increased by 50%, the test goes smoothly; when the packet loss rate is low and number of

收稿日期：2017-06-05
作者简介：李　超(1993—)，男，黑龙江安达人，硕士生，主要从事武器系统与测试自动化研究. E-mail:924244414@qq.com

引用格式：*李超，肖明清，王矗，等. 基于 SRCSM 的装备无线分布式测试系统数据加密传输[J]. 空军工程大学学报(自然科学版)，2018，19(2)：72-78. LI Chao，XIAO Mingqing，WANG Chu，et al. Research on Data Encryption Transmission of Wireless Distributed Test System Based on SRCSM [J]. Journal of Air Force Engineering University (Natural Science Edition)，2018，19(2)：72-78.*

the monitored are large, the possibility of being monitored can be reduced by 5 orders of magnitude.
Key words: Distributed test system; Wireless communication; SRCSM; Confidentiality

随着无线传输技术的成熟，以无缆化思想为基础的装备无线分布测试系统成为测试系统发展的主要方向，可缩减电缆在运输及使用过程中所占用的体积，并可解除不同设备间因电缆连接所带来的分布限制，使更多种类的设备能够实现分时复用。无线传输的保密性、接收人员及接收地点的定向性可能阻碍了其在军用分布式测试领域的应用。

实现无线分布式测试的首要任务是实现严格的数据加密，民用领域在此方面的研究以相对成熟，为军用无线分布式测试系统突破自身的局限提供了一些参考。文献[1～3]将外部元器件引入到系统中，利用物理隔离的方式，将消息储存在接收端外部的存储介质中，防止了接收端泄密。文献[4～6]利用混沌特有的对初始参数值的敏感依赖性、拓扑传递性、正的李氏指数、混合性、周期点稠密性、拉伸折叠变换特性、遍历性、分数维和奇怪吸引子等典型特征，提出了具体的混沌密码算法，提高了传输内容的保密性。文献[7～10]提出了一系列加密传输方法，在传输过程中利用信道、消息排列顺序的不同来提高传输内容的保密性。文献[11～13]使用了数字签名来提高传输消息的指向性，防止了消息在传输过程中被删或伪造增加了消息的公开可验证性，提高了传输过程中消息的安全性，保证了消息的完整性。文献[14～17]依据加密原理，设计了不同的加密算法，从软件层面提高了消息安全传输的可靠性，以上方法虽在保密性能上都有一定的作用，但仍不能完全满足军用消息传输无缆化、定向性等方面的要求。

以可实现位置定向传输的 LR 签名[18]为基础，结合随机编码的思想，本文首先提出了自定位随机编码签名机制(Self-locating Random Coding Signature Mechanism，SRCSM)。只有被系统赋予相应权限的接收端才能够在经系统验证的位置接收无线传输的信息，并将其解析成消息。本文基于 SRCSM，在非对称加密的基础上，构造了一个测试数据安全传输的可靠方案，并对该方案的安全性进行了分析，知密范围缩小的同时保密性能有所提升。

1　SRCSM

SRCSM 将 LR 签名的原理，使窃听人员(Eve)与数据接收端存在物理隔离，将随机编码、定人接收的思想引入到数据传输中，增加了 Eve 窃取、解析信息的难度。SRCSM 整体结构图，见图 1：

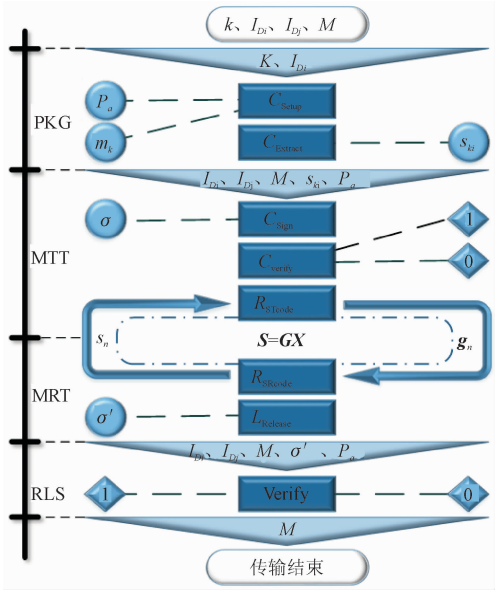

图 1　SRCSM 整体结构图

Fig. 1　The whole construction of SRCSM

SRCSM 在消息加密过程中，基本参数有：安全参数 k、发送者标识 I_{D_i}、接收者标识 I_{D_j}、消息 M 等，分别在私钥生成服务器 PKG、消息传输端 MTT、消息接收端 MRT、可信位置服务器 RLS 等 4 个终端，运行 8 个主要算法。结合 SRCSM 整体结构图，可对算法的参数与作用总结如下：

$C_{\mathrm{Setup}}(k)$：PKG 生成主密钥的基础算法。

$C_{\mathrm{Extract}}(P_a, m_k, I_{D_i})$：PKG 生成特定私钥的高阶算法。

$C_{\mathrm{Sign}}(I_{D_i}, I_{D_j}, s_{k_i}, M)$：MTT 生成消息签名的初级算法。

$C_{\mathrm{Verify}}(I_{D_i}, I_{D_j}, P_a, M, \sigma)$：MTT 生成消息签名的判定算法。判断 σ 是否为 I_{D_i} 相对于消息 M 的签名，若是，则输出 1，否，则输出 0。

$R_{\mathrm{STcode}}(\sigma, s_{k_i}, P_a)$：MTT 对传输数据随机编码、定向加密传输的算法。通过对需发送的签名 σ、私钥 s_{k_i}、公共参数 P_a 等信息进行编排，将其划分为 K 组行向量，通过与 R_{SRcode} 算法的配合，实现加密。

$R_{\mathrm{SRcode}}(\cdot)$：MRT 配合 MTT 加密传输的算法，也是定向传输的主要算法。承担对 R_{STcode} 加密后的数据解密工作，起安全传递的作用。

$L_{\mathrm{Release}}(\sigma, I_{D_j}, s_{k_i}, P_a)$：MRT 生成位置验证签名的算法。

$V(\sigma', M, I_{D_i}, I_{D_j}, P_a)$：RLS 生成消息签名的判定算法。通过综合计算，判断最终签名 σ' 是否有效。若有效，则输出 1，MRT 开始解密工作；若无效，则

输出 0,MTT 重新进行计算与传输。

通过以上 8 个算法,使消息在传输过程中,拥有了以下几个属性:

1)定向性。

当且仅当特定的 MRT 运行 R_{SRcode} 时,MTT 的 R_{STcode} 才被触发工作,故非指定工作人员无法接收到来自 MTT 的相关数据。且在 L_{Release}、V 的配合下,只有在经认证的指定位置时,签名才能有效的还原出原始的消息。

2)完整性。

信息在传输前会被分割加密为若干小部分,当且仅当 R_{SRcode} 将数据全部接收并确定无误后,系统才会释放其所占用的资源,并启动其它程序;否则,将回传命令至发送端,使其再次发送消息。

3)准确性。

在信息传输结束后,系统利用消息的身份特征对的准确度进行再次检验,确保信息在传输过程中没有被篡改、损坏。在本文中,对于消息 M 当且仅当满足下列关系式时,才能顺利完成传输:

$$\begin{cases} C_{\text{Sign}}(I_{D_i}, I_{D_j}, s_{k_i}, M) = \sigma \\ C_{\text{Verify}}(I_{D_i}, I_{D_j}, P_a, M, \sigma) = 1 \end{cases} \tag{1}$$

$$\begin{cases} L_{\text{Release}}(\sigma, I_{D_j}, s_{k_i}, P_a) = \sigma' \\ V(\sigma', M, I_{D_i}, I_{D_j}, P_a) = 1 \end{cases} \tag{2}$$

消息的定向性、完整性及准确性是 SRCSM 最显著的特质,是针对内部人员可能存在泄密风险的情况下,缩小内部人员知密范围的一种辅助方法。

2 装备分布式测试系统数据加密无线传输

本文所研究的系统是通过带有无线发射装置的采集卡,对分布于不同地点的装备同时测量、分析的测试系统。为实现无线传输,采集卡在信息采集完成后,在其内部便将模拟信号通过 A/D 转换为数字信号,并无线传输至服务器进一步处理,从而达到对武器装备情况基本掌握的效果。无线传输实现了营区内部资源乃至外围部分资源的统筹协作,但由于无线网络的开放性,也对我军的保密工作提出了巨大的挑战,现有的非对称加密技术只能降低外部窃取的概率,对内部泄密问题还没有过多涉及,故本节中,将基于本文提出的 SRCSM,结合非对称加密技术,通过对加密数据组提供不定长的 SRCSM 数据头,将此数据头与数据组进行不定长耦合,并按照 SRCSM 方法操作,从而实现整体数据的定向传输。

具体方案如下:

$C_{\text{Setup}}(k)$:设定安全参数 k,通过双线性生成概率算法[19],输出相应的双线性参数(q,G,G_T,e,P),其中,q 为大素数,且$|q|=k$,G,G_T 均是阶数为 q 的循环群,$e:G\times G\to G_T$ 为从 G 到 G_T 的有效双线映射,P 为 G 的生成元。在 PKG 内随机选择 $m_k\in Z_q^*$ 作为系统的主密钥,并计算出系统的公钥 $P_{\text{pub}}=sP$。取 H、H_1、H_2、H_3、H_4 等 5 个抗碰撞散列函数,其中,H、$H_3:\{0,1\}\times\to G$,H_1、$H_2:\{0,1\}\times\to Z_q^*$,$H_4:\{0,1\}\times\to G_T$。最终,PKG 产生公开参数 $P_a=(q,G,G_T,e,P,P_{\text{pub}},H,H_1,H_2,H_3,H_4)$。

$C_{\text{Extract}}(P_a,m_k,I_{D_i})$:为每个用户分配 I_D,通过 KGS 为 ID 添加特定的私钥:$s_{k_i}=xH(I_{D_i})$,并通过固定信道发送给用户并利用 $Q(s_{k_i},P)=Q(W,P_{\text{pub}})$ 判断用户私钥是否由 KGS 分配产生,其中,$W=H(I_{D_i})$。设 KGS 发送端生成私钥 $s_{k_i}=x\boldsymbol{Q}_i=xH(I_{D_i})$,为接收端生成私钥 $s_{k_j}=x\boldsymbol{Q}_j=xH(I_{D_j})$。

$C_{\text{Sign}}(I_{D_i},I_{D_j},s_{k_i},M)$:确定发送者标识 I_{D_i},接收者标识 I_{D_j},及其私钥 s_{k_i},消息 M,外加随机选择的数据$\delta\in Z_q^*$,$\omega=e(H(I_{D_j}),P_{\text{pub}})^r\in G_T$,$W=H_2(\omega,I_{D_i},I_{D_j})\in Z_q^*$。计算:

$$\begin{aligned} U &= rP \\ V &= s_{k_i}+\delta H_1(I_{D_i},I_{D_j},U,W) \end{aligned} \tag{3}$$

输出签名 $\sigma=(U,V,W)$。

$C_{\text{Verify}}(I_{D_i},I_{D_j},P_a,M,\sigma)$:输入发送者标识 I_{D_i},接收者标识 I_{D_j},与签名 σ,使任意第 3 方可确定签名是否为有效签名。计算:

$$\delta = H_3(I_{D_i},I_{D_j},U,W) \tag{4}$$

若下等式成立

$$Q(P,V)=Q(P_{\text{pub}},H_1(I_{D_i}))Q(U,\delta) \tag{5}$$

则输出 1,否则输出 0。

$R_{\text{STcode}}(\sigma,s_{k_i},P_a)$、$R_{\text{SRcode}}(\cdot)$随机编码配合算法,分别运行于 MTT 与 MRT,建立在接收者数据接收成功与窃听者数据窃取成功为相互独立事件的数学基础上,通过数据的分割、重组传输,来增加数据的破解难度。随机编码配合算法传输流程图如图 2:

数据传输过程中,MTT 将信息分割成 T 个信息 $X_1,X_2,\cdots,X_T$ 发送给 MRT,数据 $\boldsymbol{X}_i$,$i\in(1,T)$,是长度为 N 的二进制行向量,传输数据可表示为 $K\times N$ 矩阵:

$$\boldsymbol{X}=(\boldsymbol{X}_1^{\mathrm{T}},\boldsymbol{X}_2^{\mathrm{T}},\cdots,\boldsymbol{X}_n^{\mathrm{T}})^{\mathrm{T}} \tag{6}$$

由于无线信道的可靠性与安全性等问题,MTT 将数据信息 $\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_T$ 线性组合成 $s_1,s_2,\cdots,s_T$,后再进行发送。其中:

$$\boldsymbol{s}_n=\boldsymbol{g}_n\boldsymbol{X} \tag{7}$$

n 为传输中分割后子数据的编号,$\boldsymbol{g}_n$ 为 $\boldsymbol{X}$ 生成 $\boldsymbol{s}_n$ 的变换行向量,且由 MRT 选择,并通过无线通信

的方式与 MTT 传输。

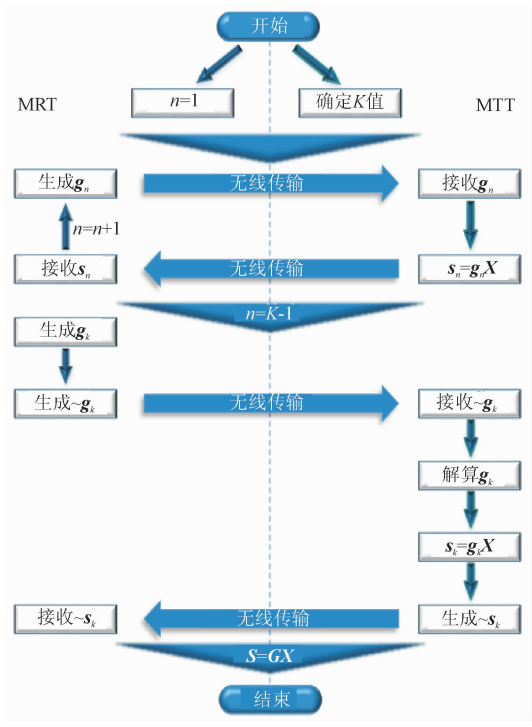

图 2　随机编码配合算法传输流程图

Fig. 2　The whole construction of SRCRSM transmissing flow of randan coding coupled algarithm

通信启动后，MRT 选择适当的 $\boldsymbol{g}_n$，将其与编号 n 一并发送至 MTT；接收到 $\boldsymbol{g}_n$ 后，MTT 通过 $\boldsymbol{s}_n=\boldsymbol{g}_n\boldsymbol{X}$ 计算后，将 $\boldsymbol{s}_n$ 发送回 MRT；若 MRT 接收到 $\boldsymbol{s}_n$，则将该对（$\boldsymbol{g}_n$，$\boldsymbol{s}_n$）储存，否则，MRT 将生成一个新 $\boldsymbol{g}_n$，并重复以上过程，直到 MRT 收到 $\boldsymbol{s}_n$。当传输至 $n=T$ 时，对于 $\forall n\in(1,T-1)$，（$\boldsymbol{g}_n$，$\boldsymbol{s}_n$）都是 MTT 和 MRT 所共享。

MRT 以 g_T 为基础，生成需发送的信息 $\tilde{g}_T$：

$$\tilde{g}_T = g_T + \sum_{n=1}^{K-1}\boldsymbol{g}_n \tag{8}$$

故 MTT 可从 $\tilde{g}_T$ 与历史数据中反推出 g_T，并生成最后的编码 $s_T=g_T\boldsymbol{X}$。与 MRT 类似，MTT 在 s_T 的基础上，生成发送信息 $\tilde{s}_T$：

$$\tilde{s}_T = s_T + \sum_{n=1}^{T-1}s_n \tag{9}$$

若 MRT 未收到 $\tilde{s}_T$，则 MRT 将重新生成一个 g_T，并将新的 $\tilde{g}_T$ 发送至 MTT，相应地，MTT 也将从新生成一个 s_T 并发送回 $\tilde{s}_T$ 至 MRT。在此过程中，若消息经反复传输仍无法实现全部的接收，则 MTT 需报告错误，由系统智能替换测试设备进行传输。若出现信息模块缺失的情况，则系统无法继续工作。保证了信息在传输过程中的完整性。

MRT 将收到 $\tilde{s}_T$ 恢复出 s_T，此时，依靠 K 对传输向量，可得线性方程：

$$\boldsymbol{S}=\boldsymbol{G}\boldsymbol{X} \tag{10}$$

式中：$\boldsymbol{G}=(\boldsymbol{g}_1^{\mathrm{T}},\cdots,\boldsymbol{g}_T^{\mathrm{T}})^{\mathrm{T}}$，$\boldsymbol{S}=(\boldsymbol{s}_1^{\mathrm{T}},\cdots,\boldsymbol{s}_{dT}^{\mathrm{T}})^{\mathrm{T}}$。在规则的限定下，$\boldsymbol{G}$ 定为满秩矩阵。因此，MRT 可以解析出 $\boldsymbol{X}$ 的具体数值。数据传输完成。

$L_{\mathrm{Release}}(\sigma,I_{D_j},s_{k_i},P_a)$：MRT 接收数据成功后，通过对签名 σ、接收者标识 I_{D_j}、私钥 s_{k_i} 及公开参数 P_a 进行如下计算：

$$\overline{w}=Q(s_{k_i},U) \tag{11}$$

则最终有效签名为：

$$\sigma'=(U,V,\overline{w}) \tag{12}$$

$V(\sigma',M,I_{D_i},I_{D_j},P_a)$：MRT 解密数据时，搜索是否有 RLS 存在，并验证 σ' 中所带有的接收方信息是否与 I_{D_j} 相同：

$$W=H_2(\overline{w},I_{D_i},I_{D_j}) \tag{13}$$

$$z=H_3(I_{D_i},I_{D_j},U,W) \tag{14}$$

若如下等式成立，

$$Q(P,V)=Q(P_{\mathrm{pub}},H(I_{D_i}))Q(U,z) \tag{15}$$

则数据可在此处，被 I_{D_j} 转换成明文。

若以上等式不成立，则说明消息在传输过程中可能被篡改或损坏，消息无法还原成原始信息。故 MTT 与 MRT 将重新启动通信模式，进行信息传输。保证了信息在传输过程中的准确性。

数据头部分传输结束后，开始数据主体部分加密传输，数据使用非对称加密技术加密。

3　性能分析

3.1　实用性分析

在某型导发架的测试项目中，测试项目几十余项，其中耗时最长的测试项目不超过 3 s（从开始测量至传输完成），最高频率不足 1 000 Hz，单项测试中，CPU 最高使用率不超过 30%；测试过程中，虽测试种类繁多，但数据总量不足 1 Mbit、测试总时长（不含等待与连接）不足 1 min，数据压力较小。

基于以上数据，本文分别对非对称性加密技术及 SRCSM 在导发架测试过程中进行对比分析。由于数据加密的原因，使得上文中提到的各项参数都有所改变，相对于无加密传输，性能均略有降低。SRCSM 系统中，C_{Setup}、C_{Extract} 运行于 PKG，C_{Sign}、C_{Verify}、P_{STcode} 运行于 MTT，R_{SRcode}、L_{Release} 运行于 MRT，C_{Verify}运行于 RLS，8 个算法分 4 部分运行于不同设备中。当 SRCSM 系统搭载在非对称性加密技术上时，系统的各项性能将进一步降低。其中，在单项测试耗时方面，使用非对称性加密技术时，最长耗时增加为 3.4 s，增加 13.33%，使用 SRCSM 时，最长耗时增加为 3.8 s，增加 26.67%；在测试总时长方面，使用非对称性加密技术时，时长为 79 s，增

加 31.67%，使用 SRCSM 时，时长为 88 s，增加 46.67%；在 CPU 使用方面，使用非对称性加密技术时，使用率为 37%，增加 23.33%，使用 SRCSM 时，使用率为 45%，增加 50%。

仅考虑导发架的测试问题时，各项参数指标都在合理范围内，测试可平稳进行，不会出现过多问题，在现有状态下，CPU 可以负担的起在非对称加密技术基础上的 SRCSM 方法的使用。

但从各项指标的增长来看，数据变化比率比较大，当原始系统过于复杂时，若强行加装 SRCSM，可能会引发系统崩溃等事故。此问题需深入研究，但不影响 SRCSM 在小系统中的使用。

3.2 保密性分析

保密性是军事信息的重要属性[20]，仅使用非对称加密的方式对数据进行加密，保密性能良好，但密钥泄露后，信息被窃听的概率急剧增加。在其基础上使用 SRCSM，在一定程度上降低了因密钥泄露所带来的风险，为补救工作留出时间。

假设在一次数据传输中存在 n_{MTT} 个 MTT，且有 n_{MRT} 个 MRT 可用，平均每发射一条消息需要 t_M，传输时间可忽略；无线便携监听设备可在同一时间监听 n_{Eve} 个信号，且每 t_E 更新一次搜索对象。故 MTT、MRT 均被 Eve 锁定的情况有 2 种：MTT、MRT 同时被锁定；MRT 被锁定后 t_M 内，MTT 被锁定。

监听锁定时序图如图 3。

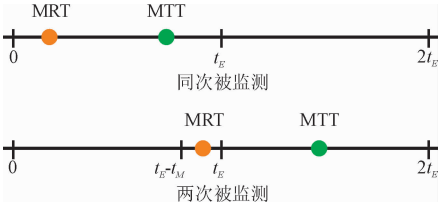

图 3 监听锁定时序图

Fig. 3 Lock time sequence of monitoring

MTT、MRT 同时被锁定的概率 P_1：

$$P_1 = \frac{t_E - t_M}{t_E} \frac{\sum_{i=1}^{n_{\mathrm{Eve}}} c_{n_{\mathrm{MRT}}}^{i} c_{n_{\mathrm{MTT}}}^{n_{\mathrm{Eve}}-i} \frac{i(n_{\mathrm{Eve}}-i)}{n_{\mathrm{MRT}} n_{\mathrm{MTT}}}}{c_{n_{\mathrm{MTT}}+n_{\mathrm{MRT}}}^{n_{\mathrm{Eve}}}} \tag{16}$$

MRT 被锁定后 t_M 内，MTT 被锁定的概率 P_2：

$$P_2 = \frac{t_M}{t_E} \frac{\left(\sum_{j=1}^{n_{\mathrm{Eve}}} c_{n_{\mathrm{MRT}}}^{j} c_{n_{\mathrm{MTT}}}^{n_{\mathrm{Eve}}-j} \frac{j}{n_{\mathrm{MRT}}}\right)\left(\sum_{k=1}^{n_{\mathrm{Eve}}} c_{n_{\mathrm{MTT}}}^{k} c_{n_{\mathrm{MRT}}}^{n_{\mathrm{Eve}}-k} \frac{n_{\mathrm{MTT}}-k}{n_{\mathrm{MTT}}}\right)}{\left(c_{n_{\mathrm{MTT}}+n_{\mathrm{MRT}}}^{n_{\mathrm{Eve}}}\right)^2} \tag{17}$$

MTT、MRT 均被锁定的概率 P_l：

$$P_l = P_1 + P_2 \tag{18}$$

假定某次传输过程中，$n_{\mathrm{MTT}}=200$，$n_{\mathrm{MRT}}=50$，$t_M=6$ ms，$t_E=30$ ms，通过 Matlab 编程计算，对 P_1、P_2、P_l 随 n_{Eve} 变化的趋势加以展示，直观表达出 P_1、P_2、P_l 与 n_{Eve} 之间关系，见图 4。

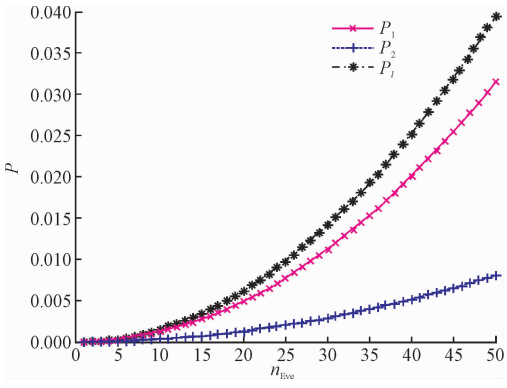

图 4 P_1、P_2、P_l 随 n_{Eve} 变化的曲线图

Fig. 4 Curve of P_1、P_2、P_l with n_{Eve}

通过图可以明显的看出，随着 n_{Eve} 的增加，P_1、P_2、P_l 的数值不断加大，信息被截获的概率越来越大。

Eve 已锁定 MTT、MRT 时，已获得的数据信息集合为 $(g_i, s_i) \in \varepsilon$。由 2.2 节中的方案构架可知，当且仅当 C_1：Eve 获取的通讯信息中包含全部有用信息，$\forall n \in (1, K-1), n \in R, (g_i, s_i) \in \varepsilon$；$C_2$：$\exists (\hat{g}_t, \hat{s}_t) \in \varepsilon, t = T$。

设 p_{XY}，X、$Y \in \{T, R, E\}$ 表示 $X \to Y$ 处的丢包率。假设 $0 \leqslant p_{XY} < 1$，且不同传输途径与不同传输方式的数据包丢失是随机独立事件。故 C_1 的概率 p_{C_1} 为：

$$p_{C_1} = (1-q)^{T-1} \tag{19}$$

式中：$q \triangleq 1-(1-p_{TE})(1-p_{RE})$。

C_2 的概率 p_{C_2} 为：

$$p_{C_2} = \sum_{t=1}^{\infty} (1-q^t)(1-p)p^{t-1} = \frac{1-q}{1-pq} \tag{20}$$

其中 $p \triangleq 1-(1-p_{TR})(1-p_{RT})$。因此，$X$ 被 Eve 窃取的概率为：

$$P_{\mathrm{crack}} = p_{C_1} p_{C_2} = \frac{(1-q)^T}{1-pq} \tag{21}$$

数据传输过程中，由于本文应用背景为近距离监听，信道环境差别不大，故认为 p_{XY} 为不因传输信道不同而改变。在实际应用中，信息量不大，MTT 将信息分割成 15 份便可满足发送要求，故本节选取 $T=15$，通过 Matlab 进行计算，对数据进行可视化处理，观察数据走向，对变化趋势加以分析，判断方法的合理性，p_{C_1}、p_{C_2}、P_{crack} 随 p_{XY} 变化的曲线图，见图 5。

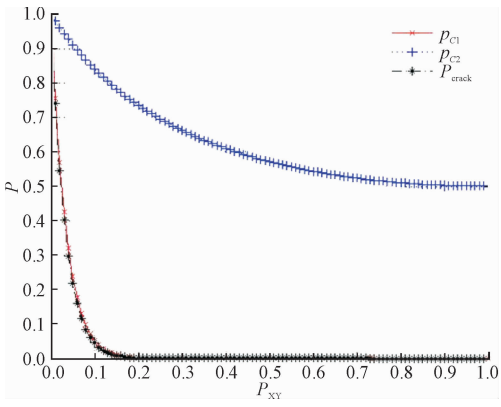

图 5　p_{C_1}、p_{C_2}、P_{crack}随 p_{XY}变化的曲线图

Fig. 5　Curve of p_{C_1}、p_{C_2}、P_{crack} by p_{XY}

通过图 5 可以看出，随着 p_{XY}的增加，p_{C_1}、p_{C_2}、P_{crack}的数值不断减小，信息安全传输的可能性不断增加。

Eve 监听成功的概率为 P：

$$P = P_l P_{crack} \tag{22}$$

当 $T=15$，$n_{MTT}=200$，$n_{MRT}=50$，$t_M=30$ ms，$t_E=6$ ms 时，控制 $p_{XY}=0.3$ 时，被监听的概率 P 的部分数据见表 1；控制 $n_{Eve}=20$ 时，被监听的概率 P 的部分数据见表 2。

由此可以看出，当丢包率较小，同时监听个数较大时，都能在算法的基础上将保密性能提升 5 个数量级，具有良好的保密功能。

表 1　$p_{XY}=0.3$ 时被监听概率 P 的部分数据

Tab. 1　Data of probability P when $p_{XY}=0.3$

n_{Eve}	5	10	15	20	25	30	35	40	45	50
P	9.1×10^{-9}	4.3×10^{-8}	1.0×10^{-7}	1.8×10^{-7}	3.0×10^{-7}	4.3×10^{-7}	5.8×10^{-7}	7.7×10^{-7}	9.8×10^{-7}	1.2×10^{-6}

表 2　$n_{Eve}=20$ 时被监听概率 P 的部分数据

Tab. 2　Data of probability P when $n_{Eve}=20$

p_{XY}	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
P	2.6×10^{-5}	8.4×10^{-6}	1.8×10^{-7}	2.2×10^{-9}	7.2×10^{-12}	2.3×10^{-14}	1.8×10^{-17}	8.2×10^{-22}	3×10^{-32}	0

4　结语

SRCSM 将车联网 LR 签名中定位接收的原理及随机编码定人接收的原理相融合，应用到装备无线分布式测试系统的消息加密传输中，仅有被系统验证过的人员与位置才能成功解析传输信息，使得监听人员即便在截获传输信息的前提下，也无法在授权地点之外激活数字签名、解析数据，提升了外部人员窃密的门限；同时，对消息接收人员权限进行管理，缩小了知密范围，降低了内部人员无意识泄密的概率。经数据计算分析 SRCSM 将保密性能在算法的基础上提升了 5 个数量级，保密性良好，且对现有装备不会产生过多计算负担。但在使用过程中，SRCSM 方法在对数据量要求较小的系统中可以流畅运行，不会对系统的计算能力产生过高压力，但在数据量大的系统中，若使用此方法，可能会导致 CPU 负载急剧增大，系统压力大。因此，本文认为，方法虽在保密性能上有所提升，但在简化运行方式上，仍具有进一步研究的价值。

参考文献(References)：

[1]　黎妹红，李论，张大伟，等. 基于 SDKEY 的安卓手机安全传输技术 [J]. 解放军理工大学学报(自然科学版)，2015(2)：114-119.
LI M，LI L，ZHANG D D W，et al. SDKEY-based Secure Data Transmission for Android Smartphones [J]. Journal of PLA University of Science and Technology(Natural Science Edition)，2015(2)：114-119. (in Chinese)

[2]　常国权，戴国强. 对无线 IC 卡传输数据实行 3DES 加密 [J]. 电子产品世界，2015，22(9)：35-38.
CHANG G Q，DAI G Q. Implementation of 3DES Encryption for Wireless IC Card Transmission Data [J]. Electronic Products World，2015，22 (9)：35-38. (in Chinese)

[3]　KLEINJUNG T，AOKI K，FRANKE J，et al. Factorization of a 768-Bit RSA Modulus [C] // Conference on Advances in Cryptology. Springer-Verlag，2010：333-350.

[4]　刘婷，梁平，柴建伟. 混沌序列在船舶网络数据传输中的加密研究 [J]. 舰船科学技术，2017(2)：88-90.
LIU T，LIANG P，CHAI J W. Research on Encryption of Chaotic Sequences in Ship Network Data Transmission [J]. Journal of Ship Science and Technology，2017(2)：88-90. (in Chinese)

[5]　ZHU C S，SUN K H. Chaotic Image Encry p tion Algorithm by Correlating Keys with Plaintext [J]. China Communications，2012，9(1)：73-79.

[6]　ZHU C. A Novel Image Encryption Scheme Based on Improved Hyperchaotic Sequences [J]. Optics Communications，2012，285(1)：29-37.

[7] MU P, YANG P, WANG B, et al. A New Scheme to Improve the Secrecy Throughput Under the Constraints of Secrecy Outage Probability and Average Transmit Power [C]// ICC-2014 IEEE International Conference on Communication Workshop IEEE, 2014: 777-782.

[8] XIONG J, WONG K K, MA D, et al. A Closed-Form Power Allocation for Minimizing Secrecy Outage Probability for MISO Wiretap Channels via Masked Beamforming [J]. IEEE Communications Letters, 2012, 16(9): 1496-1499.

[9] RUKHIN A L, SOTO J, NECHVATAL J R, et al. SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [M]. USA: Nist Special Publication, 2010.

[10] MIN L, HAO L, ZHANG L. Study on the Statistical Test for String Pseudorandom Number Generators [M]// Advances in Brain Inspired Cognitive Systems. Berlin Heidelberg: Springer, 2013: 3-17.

[11] 李旋, 吴其聪. 数字签名与加密在网络隔离中的应用研究 [J]. 信息网络安全, 2013(10): 178-180.
LI X, WU Q C. Application of Digital Signature and Encryption in Network Isolation [J]. Information Network Security, 2013(10): 178-180. (in Chinese)

[12] 俞惠芳, 杨波, 张文政. 混合签密综述 [J]. 西安邮电大学学报, 2015, 20(3): 1-10.
YU H F, YANG B, ZHANG W Z. A Survey of Hybrid Sign Cryption [J]. Journal of Xi'an University of Posts and Telecommunications, 2015, 20(3): 1-10. (in Chinese)

[13] 肖欧, 尹震宇. 中国科学院 SAMP 系统的加密通信 [J]. 计算机系统应用, 2016, 25(5): 19-27.
XIAO O, YIN Z Y. Communication Encryption of Axis2 in Apparatus and Equipment Sharing Management System of Chinese Academy of Sciences [J]. Journal of Computer Applications, 2016, 25(5): 19-27.

[14] 陈燕俐, 杨庚. 适合于无线传感器网络的混合式组密钥管理方案[J]. 通信学报, 2010, 31(11):56-64.
CHEN Y L, YANG G. Hybrid Group Key Management Scheme for Wireless Sensor Networks [J]. Journal of Communications, 2010, 31 (11): 56-64. (in Chinese)

[15] 姚丽莉, 袁操今, 强俊杰, 等. 基于 gyrator 变换和矢量分解的非对称图像加密方法[J]. 物理学报, 2016, 65(21):139-144.
YAO L L, YUAN C J, QIANG J J, et al. Asymmetric Image Encryption Method Based on Gyrator Transform and Vector Decomposition [J]. Acta Physica Sinica, 2016, 65 (21): 139-144. (in Chinese)

[16] 张猛, 杨可新, 鞠九滨. 改进加密算法实现的性能 [J]. 软件学报, 2001, 12(6):878-883.
ZHANG M, YANG K X, JU J B. Improved Performance of Improved Encryption Algorithm [J]. Journal of Software, 2001, 12 (6): 878-883. (in Chinese)

[17] 翁云翔. 基于 DES 和 RSA 的混合加密算法研究与设计[J]. 电子设计工程, 2016, 24(17):42-44.
WENG Y X. Research and Design of Hybrid Encryption Algorithm Based on DES and RSA [J]. Electronic Design Engineering, 2016, 24 (17): 42-44. (in Chinese)

[18] LIN X, LU R, SHEN X. Location-Release Signature for Vehicular Communications [C]// Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of, Internatonal Conference on IEEE, 2009: 1-7.

[19] GASSIAT P, MIJATOVI A, OBERHAUSER H. An Integral Equation for Root's Barrier and the Generation of Brownian Increments [J]. Annals of Applied Probability, 2015, 25(4): 481-90.

[20] RACHLIN Y, BARON D. The Secrecy of Compressed Sensing Measurements [C] // Communication, Control, and Computing, Allerton Conference on IEEE, 2014: 813-817.

(编辑: 徐敏)