重放攻击下雷达组网系统的目标跟踪性能

林　东，王布宏，王振昊
（空军工程大学信息与导航学院，西安，710077）

摘要　作为一种复杂的分布式系统，雷达组网系统受到各种攻击的威胁。为了研究赛博攻击对雷达组网系统性能的影响，提出一种针对雷达组网系统的重放攻击方式。首先建立目标运动模型和系统模型，其次分析了重放攻击对单站雷达位置估计误差的影响，基于此扩展到对雷达组网系统目标跟踪性能的影响，最后研究了攻击参数与位置估计误差的关系。通过仿真分别展示了单站雷达和雷达组网系统受到重放攻击时的状态估计误差，以及单站雷达和雷达网估计误差与攻击强度的关系。仿真结果表明：对于单站雷达，重放攻击可以造成巨大的跟踪误差，且攻击效果与攻击强度成正比关系。当攻击的对象是雷达组网系统时，需要合理地选择攻击参数才能产生明显的攻击效果。

关键词　雷达组网系统；目标跟踪；重放攻击；卡尔曼滤波；概率数据关联
DOI　10.3969/j.issn.1009-3516.2018.04.010
中图分类号　TN95　　**文献标志码**　A　　**文章编号**　1009-3516(2018)04-0054-05

Target Tracking Performance in Radar Network System under Replay Attack

LIN Dong, WANG Buhong, WANG Zhenhao
(Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)

Abstract: As a complicated distributed system, radar network system encounters various attacks. In order to study the impact of cyber attacks on the performance of radar network system, a kind of replay attack mode for radar network system is proposed. Firstly, a target motion model and a system model are established. Then, the influence of the replay attack on the position estimation error of the mono-static radar is analyzed. For the above-mentioned reasons, the influence on the tacking performance of the radar network system is extended. Finally, the relationship between the attack parameter and the position estimation error is studied. The state estimation error of mono-static radar and radar network system under replay attack, as well as the relationship between single-station radar and radar network estimation error and attack strength are obtained by simulation. The simulation results show that for mono-static radar, replay attacks can cause huge tracking errors, and the attack effect is directly proportional to the attack strength. When the target of replay attack is a radar network system, a reasonable selection of attack parameters is required to produce a significant attack effect.

Key words: radar network system; target tracking; replay attack; Kalman filtering; probabilistic data association

收稿日期：2017-10-23
基金项目：国家自然科学基金(61671465)
作者简介：林　东(1993—)，男，四川绵阳人，硕士生，主要从事雷达组网系统研究. E-mail:1121295777@qq.com

引用格式：林东，王布宏，王振昊. 重放攻击下雷达组网系统的目标跟踪性能[J]. 空军工程大学学报(自然科学版)，2018，19(4)：54-58.
LIN Dong, WANG Buhong, WANG Zhenhao. Target Tracking Performance in Radar Network System under Replay Attack[J]. Journal of Air Force Engineering University (Natural Science Edition), 2018, 19(4): 54-58.

近年来，雷达组网一直是国内外的研究热点。雷达组网系统包含一系列地域分离布置的雷达，通过收集和融合具有空间差异的雷达信号，在目标跟踪方面可以实现比单个雷达好的性能[1]，特别是针对隐身目标和低空突防目标。因此，雷达组网系统在民用和军事领域都有十分重要的应用[2]。

在带来性能提升的同时，雷达组网系统面临着严峻的安全挑战。与传统的单基或者多基雷达相比，雷达组网系统更加的复杂、实现更加困难[3]。由于这些雷达分布于广阔的地域，需要把收集的目标信息发送给数据融合中心，雷达组网系统的发送端、接收端、通信链路和数据融合中心都很容易受到攻击[4]。

传统的针对雷达的攻击手段主要有 2 种，分别是欺骗干扰和压制干扰[5]。欺骗干扰通过距离和角度欺骗产生虚假航迹或虚假目标[6]；压制干扰则是使用大功率干扰机对目标雷达进行功率压制[7]。随着科技的发展，雷达组网系统信息化和智能化的程度越来越高[8]。作为一种典型的多传感器系统，雷达组网系统也面临着来自赛博空间的安全挑战[9]75-83。研究人员已经从多个角度研究了雷达组网系统面临的安全问题。文献[10]参考无线传感器网络的攻击方法，提出了针对雷达组网系统的常量偏差虚假数据注入攻击，并分析了在该攻击下的雷达组网系统的目标跟踪性能。文献[11]提出了一种针对常量偏差虚假数据的安全数据融合算法，有效地提高了雷达组网系统的鲁棒性。为防止通信链路遭到攻击，文献[12]提出了一种通信加密机制，提高了雷达组网系统通信的安全性。文献[13]提出了针对 MIMO 雷达的赛博攻击，并分析了赛博攻击对检测性能的影响。文献[14]提出了一种针对雷达组网系统的协同攻击方式，使用 N 个无人机可以产生 $N\times N$ 个虚假目标。文献[15]使用传感器网络的方法对多基雷达网进行了建模分析，指出了多基雷达网面临的安全威胁和应对方法。

由于可以对雷达网的数据进行加密[16]，文献[10]的虚假数据构造方式在实际应用中难以实现。为解决这一问题，本文在上述研究的基础上提出一种针对雷达组网系统的赛博攻击——重放攻击。攻击者首先收集被攻击站点的一系列数据，用经过仔细选择的旧数据替代真实的数据重新发送给雷达组网系统。重放攻击不需要攻击者提前获得被攻击系统的情况，且重放的数据来源于真实的数据，很难被基于认证和加密的入侵检测算法检测出来，具有很强的隐身性。

1　问题定义

雷达组网系统包含若干独立的雷达和一个数据融合中心，每个雷达都要将探测到的目标信息发送给数据融合中心[17-18]。数据融合中心获得并处理这些探测的数据，最终得到探测目标的位置和速度信息。在本文中，假定数据融合中心采用概率数据关联算法算法进行数据融合，每个雷达采用卡尔曼滤波算法进行跟踪滤波。

1.1　目标运动和测量公式

在直角坐标系中，建立点目标的运动模型[19]

$$\boldsymbol{x}_{k+1}=\boldsymbol{F}\boldsymbol{x}_k+\boldsymbol{v}_k,\boldsymbol{x}_k\in R^{n_x} \tag{1}$$

式中：$\boldsymbol{x}_k$ 为 k 时刻目标的状态向量；$\boldsymbol{F}$ 为状态转移矩阵；$\boldsymbol{v}_k$ 为相互独立的零均值高斯白噪声，其协方差为 $\boldsymbol{Q}$。在直角坐标系中，状态向量 $\boldsymbol{x}_k$ 包含速度和位置信息。

假设该雷达组网系统给包含有 n 个雷达，则第 i 个雷达的测量值记为：

$$\boldsymbol{y}_{k+1}^i=\boldsymbol{H}\boldsymbol{x}_{k+1}+\boldsymbol{w}_{k+1}^i,i\in[1,n] \tag{2}$$

式中：$\boldsymbol{H}$ 为测量矩阵；$\boldsymbol{w}_k^i$ 为相互独立的零均值高斯白噪声，其协方差为 $\boldsymbol{R}^i$。

1.2　卡尔曼滤波

卡尔曼滤波被广泛用于目标跟踪领域，具体描述如下[20]：

$$\boldsymbol{x}_{k+1|k}=\boldsymbol{F}\boldsymbol{x}_{k|k} \tag{3}$$

$$\boldsymbol{P}_{k+1|k}=\boldsymbol{F}\boldsymbol{P}_{k|k}\boldsymbol{F}^{\mathrm{T}}+\boldsymbol{Q} \tag{4}$$

$$\boldsymbol{K}_k=\boldsymbol{P}_{k|k-1}\boldsymbol{H}^{\mathrm{T}}(\boldsymbol{H}\boldsymbol{P}_{k|k-1}\boldsymbol{H}^{\mathrm{T}}+\boldsymbol{R})^{-1} \tag{5}$$

$$\boldsymbol{x}_{k|k}=\boldsymbol{x}_{k|k-1}+\boldsymbol{K}_k(\boldsymbol{y}_k-\boldsymbol{H}\boldsymbol{x}_{k|k-1}) \tag{6}$$

$$\boldsymbol{P}_{k|k}=\boldsymbol{P}_{k|k-1}-\boldsymbol{K}_k\boldsymbol{H}\boldsymbol{P}_{k|k-1} \tag{7}$$

式中：$\boldsymbol{x}_{k|k}$ 代表状态向量的最小均方误差估计；$\boldsymbol{x}_{k+1|k}$ 代表一步预测状态估计；$\boldsymbol{P}_{k|k}$ 为估计误差协方差；$\boldsymbol{P}_{k+1|k}$ 代表一步预测状态估计协方差；$\boldsymbol{K}_k$ 是 k 时刻的增益参数；$\boldsymbol{F}^{\mathrm{T}}$ 为转移矩阵 $\boldsymbol{F}$ 的转置。虽然卡尔曼增益参数 $\boldsymbol{K}_k$ 是时变的，但因为系统是可测和稳定的，$\boldsymbol{K}_k$ 和 $\boldsymbol{P}_{k|k}$ 将会指数收敛[21]。因此，可以做如下定义：

$$\begin{aligned}\boldsymbol{P}&=\lim_{k\to\infty}\boldsymbol{P}_{k|k}\\ \boldsymbol{K}&=\lim_{k\to\infty}\boldsymbol{K}_{k|k}\end{aligned} \tag{8}$$

1.3　数据融合

概率数据关联算法是数据融合算法中最基础的算法之一，因此在本文中采用该算法进行研究。数据融合中心利用 $k-1$ 时刻的预测状态估计 $\boldsymbol{x}_{k|k-1}$ 作为验证区内的一步预测值。然后给 k 时刻每个雷达在验证区内的数据分配关联概率[22]。算法可被描

述如下[23]:

$$\boldsymbol{x}_{k|k}=\boldsymbol{x}_{k|k-1}+\boldsymbol{K}_k\sum_{i=1}^{n}\beta_k^i\boldsymbol{u}_k^i,\boldsymbol{u}_k^i=\boldsymbol{y}_k^i-\boldsymbol{H}_i\boldsymbol{F}\boldsymbol{x}_{k-1|k-1} \quad (9)$$

$$\beta_k^i=\frac{e_i(k)}{b+\sum_{j=1}^{n}e_j(k)},\beta_k^0=\frac{b}{b+\sum_{j=1}^{n}e_j(k)} \quad (10)$$

$$\boldsymbol{P}_{k|k}=\boldsymbol{P}_{k|k-1}\beta_k^0+(\boldsymbol{I}-\beta_k^0)(\boldsymbol{I}-\boldsymbol{K}_k\boldsymbol{H})\boldsymbol{P}_{k|k-1}+\tilde{\boldsymbol{P}}_k \quad (11)$$

$$\tilde{\boldsymbol{P}}_k=\boldsymbol{K}_k\Big[\sum_{j=1}^{n}\beta_k^i\boldsymbol{u}_k^i\boldsymbol{u}_k^{i\mathrm{T}}-(\sum_{j=1}^{n}\beta_k^i\boldsymbol{u}_k^i)(\sum_{j=1}^{n}\beta_k^i\boldsymbol{u}_k^i)\Big]\boldsymbol{K}_k^{\mathrm{T}} \quad (12)$$

式中:b 为一个常数;$e_i(k)=\exp\{-\frac{1}{2}[y_k-x_{k|k-1}]^{\mathrm{T}}\boldsymbol{S}_k^{-1}[\boldsymbol{y}_k-\boldsymbol{x}_{k|k-1}]\}$;$\boldsymbol{S}_k$ 为滤波残差协方差矩阵,β_k^i 是数据关联概率,代表着第 i 个雷达 k 时刻测量值的加权系数。$\boldsymbol{K}_k$ 和 $\boldsymbol{P}_{k|k-1}$ 的定义由式(4)和式(5)给出。

1.4 重放攻击

建立一个针对雷达组网系统的重放攻击模型。假设攻击者能够获得将一个雷达的测量值序列 $\boldsymbol{y}_k$ 并将其修改为 $\boldsymbol{y}'_k$。攻击者的攻击行为可以分为 2 个阶段:①攻击者在不攻击的情况下记录足够的测量值 $\boldsymbol{y}_k$;②攻击者将记录下的数据重放给雷达组网系统。

值得注意的是,在攻击的阶段中,为实现隐蔽攻击的效果,攻击者需要使虚假数据 $\boldsymbol{y}'_k$ 与真实数据 $\boldsymbol{y}_k$ 相似。为达到这一目的,直接将记录下的数据间隔一段时间重放给雷达组网系统是一个很好的选择。设定真实数据与重放数据的时间间隔为 t。实际上,被攻击系统是真实系统的一个时间变换,其关系如下:

$$\begin{cases}\boldsymbol{x}'_k=\boldsymbol{x}_{k-t}\\ \boldsymbol{x}'_{k|k}=\boldsymbol{x}_{k-t|k-t}\end{cases} \quad (13)$$

假设只有第 n 个雷达被攻击者劫持,因为估计误差很快地指数收敛,可以认为在攻击之前状态估计是稳定的。如果攻击发生在 k 时刻,可以得到:

$$\boldsymbol{y}_k^{i'}=\begin{cases}\boldsymbol{y}_k^i,i\in[1,n-1]\\ \boldsymbol{y}_k^{i'},i=n\end{cases},\boldsymbol{y}_k^{i'}=\boldsymbol{y}_{k-t}^i \quad (14)$$

2 重放攻击下目标跟踪性能分析

本节研究在重放攻击下雷达组网系统的目标跟踪性能。以单个雷达的性能研究为基础,扩展到整个雷达组网系统。在 l 时刻发动攻击攻击者,将雷达的测量值由 $\boldsymbol{y}_k$ 篡改为 $\boldsymbol{y}'_k(k\geqslant l)$。

2.1 单雷达站目标跟踪

首先研究 $\boldsymbol{K}_k$,根据式(5)可知,攻击并不改变 $\boldsymbol{K}_k$。毫无疑问的是系统已经与初始系统不同了,因为雷达数据处理部分没有察觉到攻击的存在会导致 $\boldsymbol{K}_k$ 不再是最佳[6]。根据式(4)和式(7),同理可知在攻击下 $\boldsymbol{P}_{k|k}$ 和 $\boldsymbol{P}_{k+1|k}$ 也不改变。综上可得到:$\boldsymbol{K}'_k=\boldsymbol{K}_k,\boldsymbol{P}'_{k|k}=\boldsymbol{P}_{k|k},\boldsymbol{P}'_{k+1|k}=\boldsymbol{P}_{k+1|k}$。

然后,探讨在攻击开始之后 $\boldsymbol{x}_{k+1|k+1}$ 的变化。令 $\Delta\boldsymbol{y}_k=\boldsymbol{y}_k-\boldsymbol{y}'_k$,表示攻击者在 k 时刻造成的测量值的偏差。由式(2)和式(13)可得:

$$\Delta\boldsymbol{y}_k=\boldsymbol{y}_k-\boldsymbol{y}_{k-t} \quad (15)$$

在 k 时刻,由式(3)和式(6)可得真实系统的目标状态估计值为:

$$\boldsymbol{x}_{k|k}=(\boldsymbol{I}-\boldsymbol{K}_k\boldsymbol{H})\boldsymbol{F}\boldsymbol{x}_{k-1|k-1}+\boldsymbol{K}_k\boldsymbol{y}_k \quad (16)$$

同时,被攻击系统的目标状态估计值为:

$$\boldsymbol{x}'_{k|k}=(\boldsymbol{I}-\boldsymbol{K}_k\boldsymbol{H})\boldsymbol{F}\boldsymbol{x}'_{k-1|k-1}+\boldsymbol{K}_k\boldsymbol{y}'_k \quad (17)$$

由式(16)和式(17)可得:

$$\boldsymbol{x}_{k|k}-\boldsymbol{x}'_{k|k}=(\boldsymbol{I}-\boldsymbol{K}_k\boldsymbol{H})\boldsymbol{F}(\boldsymbol{x}_{k-1|k-1}-\boldsymbol{x}'_{k-1|k-1})+\boldsymbol{K}_k(\boldsymbol{y}_k-\boldsymbol{y}'_k) \quad (18)$$

真实系统和被攻击系统在有限步之后都会收敛。$\Delta\boldsymbol{x}_k=\boldsymbol{x}_{k|k}-\boldsymbol{x}'_{k|k}$ 由式(8)和式(18)可得:

$$\Delta\boldsymbol{x}_k=(\boldsymbol{I}-\boldsymbol{K}\boldsymbol{H})\boldsymbol{F}\Delta\boldsymbol{x}_{k-1}+\boldsymbol{K}\Delta\boldsymbol{y}_k \quad (19)$$

不妨令 $\boldsymbol{M}=(\boldsymbol{I}-\boldsymbol{K}\boldsymbol{H})\boldsymbol{F}$,则上式可表示为:

$$\Delta\boldsymbol{x}_k=\boldsymbol{M}\Delta\boldsymbol{x}_{k-1}+\boldsymbol{K}\Delta\boldsymbol{y}_k \quad (20)$$

忽略噪声的影响,由式(1)、式(2)和式(15)可得:

$$\Delta\boldsymbol{y}_k=\boldsymbol{H}(\boldsymbol{x}_k-\boldsymbol{x}_{k-1})=\boldsymbol{H}(\boldsymbol{F}^t-I)\boldsymbol{x}_{x-1} \quad (21)$$

式中:$\boldsymbol{F}^t$ 表示 t 个 $\boldsymbol{F}$ 相乘;$\Delta\boldsymbol{y}_k$ 只与数据真实数据与攻击数据的时间差 t 有关,且与时间差 t 成线性正比关系。因此,可以令 $\Delta\boldsymbol{y}_k=\Delta\boldsymbol{y}(t)$,则式(20)可表示为 $\Delta\boldsymbol{x}_k=\boldsymbol{M}\Delta\boldsymbol{x}_{k-1}+\boldsymbol{K}\Delta\boldsymbol{y}(t)$,同理可得 $\Delta\boldsymbol{x}_{k-1}=\boldsymbol{M}\Delta\boldsymbol{x}_{k-2}+\boldsymbol{K}\Delta\boldsymbol{y}(t)$,反复利用该原理可得:

$$\Delta\boldsymbol{x}_k=\boldsymbol{M}^{k-l+1}\Delta\boldsymbol{x}_{l-1}+\boldsymbol{K}\sum_{j=0}^{l-1}\boldsymbol{M}^j\Delta\boldsymbol{y}(t) \quad (22)$$

因为攻击从 l 时刻开始,则 $\Delta\boldsymbol{x}_{l-1}=0$,则式(22)可以改写为:

$$\Delta\boldsymbol{x}_k=\boldsymbol{K}\sum_{j=0}^{l-1}\boldsymbol{M}^j\Delta\boldsymbol{y}(t) \quad (23)$$

由范数的相容性可知:$\Delta\boldsymbol{x}_k$ 是有界收敛的,且与测量偏差 $\Delta\boldsymbol{y}(t)$ 是近似线性正比关系。

2.2 雷达组网系统目标跟踪性能

接下来研究具有数据融合中心的雷达组网系统在重放攻击下的目标跟踪性能。由式(9)和式(10)可得:

$$\boldsymbol{x}_{k|k}=\boldsymbol{F}\boldsymbol{x}_{k-1|k-1}+\boldsymbol{K}_k\Big(\sum_{i=1}^{n}\beta_k^i\boldsymbol{y}_k^i-\sum_{i=1}^{n}\beta_k^i\boldsymbol{H}_i\boldsymbol{F}\boldsymbol{x}_{k-1|k-1}\Big) \quad (24)$$

假设所有的雷达测量值都在验证区域内,因此

式(10)和式(11)中的 $b=0$ 且 $\sum_{i=1}^{n}\beta_k^i=1$。不妨假设所有的雷达使用相同的测量矩阵即 $\boldsymbol{H}_i=\boldsymbol{H}$，$\forall i$，式(24)可表示为：

$$\boldsymbol{x}_{k|k}=(\boldsymbol{I}-\boldsymbol{K}_k\boldsymbol{H})\boldsymbol{F}\boldsymbol{x}_{k-1|k-1}\boldsymbol{F}\boldsymbol{x}_{k-1|k-1}+\boldsymbol{K}_k\sum_{i=1}^{n}\beta_k^i\boldsymbol{y}_k^i \quad (25)$$

讨论雷达组网系统的 $\boldsymbol{K}_k$，未受到攻击的系统，$\boldsymbol{K}_k$ 也会收敛于 $\boldsymbol{K}$。然而，由式(9)可知当第 n 个雷达受到攻击，$\boldsymbol{u}_k^n$ 会变为 $\boldsymbol{u}_k^{n'}$，这也会导致数据关联概率 β_k^i 和协方差 $\boldsymbol{P}_{k|k}$、$\boldsymbol{P}_{k+1|k}$ 和 $\boldsymbol{K}_k$ 的改变。此时，受到攻击的系统，$\boldsymbol{K}'_k$ 收敛于 $\boldsymbol{K}'$。k 时刻被攻击系统的状态估计表示为：

$$\boldsymbol{x}'_{k|k}=(\boldsymbol{I}-\boldsymbol{K}'\boldsymbol{H})\boldsymbol{x}'_{k-1|k-1}+\boldsymbol{K}'\Big(\sum_{i=1}^{n-1}\beta_k^i\boldsymbol{y}_k^i+\beta_k^{n'}\boldsymbol{y}_k^{n'}\Big) \quad (26)$$

定义 k 时刻的估计误差 $\Delta\boldsymbol{x}_k=\boldsymbol{x}_{k|k}-\boldsymbol{x}'_{k|k}$。随着攻击误差的增大，被攻击站点数据的关联概率就会降低，因此估计误差与攻击参数不是线性关系。通过代入不同的时间差值 t 迭代式(25)和式(26)，可以得到 $\Delta\boldsymbol{x}_k$ 与 t 的关系，结果将在第 3 节通过仿真展示。

3　仿真与分析

本节通过仿真分别展示单个雷达站受到攻击时目标跟踪性能的影响，雷达组网系统的 1 个雷达站受到攻击时目标跟踪性能的影响，以及 $\Delta\boldsymbol{x}_k$ 与 t 之间的关系。

设置 1 个包含 3 个雷达和 1 个数据融合中心的雷达组网系统，用以监视 1 个二维区域。目标的初始位置为[10 m，20 m]，初始速度为[2 m/s，2 m/s]。目标的运动模型与式(1)相同，状态转移矩阵、测量矩阵和测量误差协方差矩阵：

$$\boldsymbol{F}=\begin{bmatrix}1&0&T&0\\0&1&0&T\\0&0&1&0\\0&0&0&1\end{bmatrix},\boldsymbol{H}=\boldsymbol{H}_i=\begin{bmatrix}1&0&0&0\\0&0&1&0\end{bmatrix},$$

$\boldsymbol{R}=\begin{bmatrix}r&0\\0&r\end{bmatrix}$，$r=25$。其中 $T=1$ 是采样周期。四维状态向量 $\boldsymbol{x}_k$ 包含位置和速度信息。

图 1 和图 2 分别表示单个雷达和雷达组网系统在无攻击情况下的位置估计误差。在 $k=100$ 的时刻发起攻击，攻击参数 $t=2$，使用 $k-t$ 时刻的数据替换 k 时刻的数据。由图可知，随着时间的变换误差收敛于一个稳定值。同等条件下，雷达组网系统的估计误差小于单个雷达，具有一定的抗重放攻击能力。

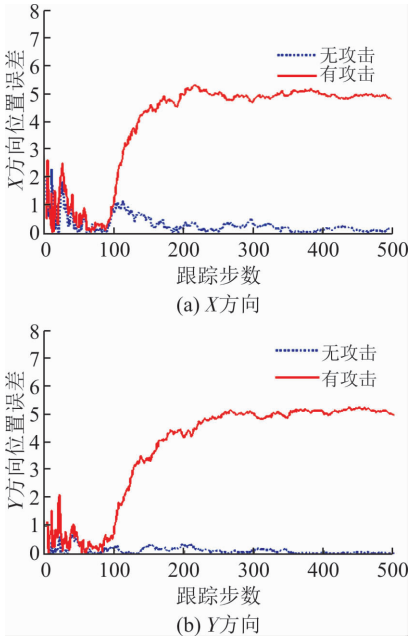

图 1　单站雷达位置误差

Fig. 1　The position error of monostatic radar

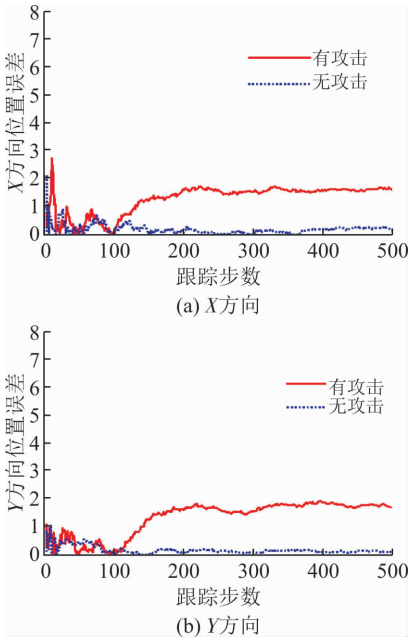

图 2　雷达组网系统位置误差

Fig. 2　The position error of radar network system

最后仿真展示攻击参数 t 和估计误差 $\Delta\boldsymbol{x}_k$ 的关系，由于 X 方向和 Y 方向误差变化相似，只展示了 X 方向的误差与 t 的关系。在图 3 中，估计误差 $\Delta\boldsymbol{x}_k$ 随着攻击参数 t 的增大而不断加大，可知单个雷达的估计误差 $\Delta\boldsymbol{x}_k$ 与攻击参数 t 是在该仿真条件下是线性关系，证明了式(23)的正确性。如图 4 所示，在雷达组网系统中，$\Delta\boldsymbol{x}_k$ 和 t 不是线性关系。由计算关联概率的式(10)可知，当第 i 个雷达被攻击，随着攻击参数变大，重放数据与真实数据的残差也会增大导致 $e_i(k)$ 变小，关联概率 β_k^i 也会变小。因

此,存在一个攻击参数阈值,当超过这个阈值攻击效果就会快速下降。但是,存在估计误差最大值,意味着合理选取攻击参数可以使得攻击效果最大化。可见,重放攻击可以有效的影响雷达组网系统目标跟踪的准确性。

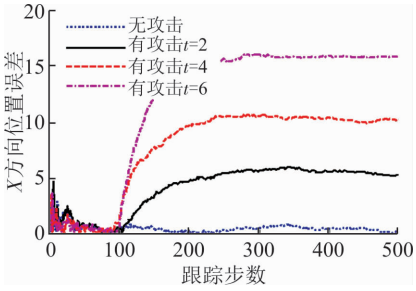

图 3 单站雷达 $\Delta \boldsymbol{x}_k$ 与 t 的关系

Fig. 3 Relationship between $\Delta \boldsymbol{x}_k$ and t of monostatic radar

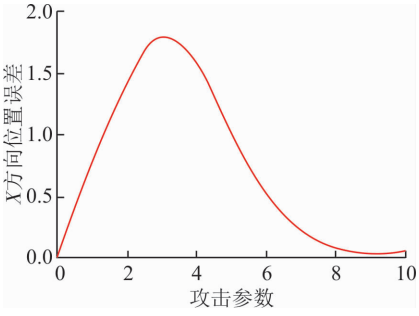

图 4 雷达组网系统 $\Delta \boldsymbol{x}_k$ 与 t 的关系

Fig. 4 Relationship between $\Delta \boldsymbol{x}_k$ and t of radar network system

4 结语

本文研究了雷达组网系统在重放攻击下的目标跟踪性能,在定义了问题之后,首先分析了单个雷达在重放攻击下的目标跟踪性能,基于此,扩展到研究雷达组网系统在重放攻击下的目标跟踪性能,其次分析了攻击参数和估计误差的关系。通过研究可得:单个雷达在重放攻击下出现了显著的估计误差,而雷达组网系统对于重放攻击具有一定的鲁棒性,但是适当的选择攻击参数也可以造成明显的估计误差。最后,通过仿真证明了其正确性。

参考文献(References):

[1] ZHENG G, ZHENG Y. Radar Netting Technology & Its Development[C]// IEEE CIE International Conference on Radar. Chengdu: IEEE, 2011:933-937.

[2] HONG S, WANG L, SHI Z G, et al. Simplified Particle Phd Filter for Multiple-Target Tracking: Algorithm and Architecture[J]. Progress in Electromagnetics Research, 2011, 120(7):481-498.

[3] WANG N, SUN J, WANG W, et al. Netted Radar Management Based on Anti-Jamming Capability[C]// International Conference on Information Fusion. IEEE, 2017:1-7.

[4] CHEN H, HIMED B. Analyzing and Improving MIMO Radar Detection Performance in the Presence of Cybersecurity Attacks[C]// IEEE Radar Conference. Philadelphia:IEEE, 2016:1-4.

[5] 吴玉清. 针对组网雷达的电子干扰技术研究[D]. 成都:电子科技大学, 2013.
WU Y Q. Research on Electronic Jamming Technology for Netted Radar[D]. Chengdu: University of Electronic Science and Technology of China, 2013. (in Chinese)

[6] 刘瀛,徐佳婧,苏伟,等. 基于有源/无源融合的雷达抗欺骗干扰方法研究[J]. 舰船电子对抗,2016,39(6):19-26.
LIU Y, XU J J, SU W, et al. Research into Radar Anti-Deception Jamming Method Based on Active and Passive Fusion[J]. Shipboard Electronic Countermeasure, 2016, 39(6): 19-26. (in Chinese)

[7] XU J, YU J, PENG Y N, et al. Radon-Fourier Transform for Radar Target Detection (II): Blind Speed Sidelobe Suppression[J]. IEEE Transactions on Aerospace & Electronic Systems, 2011, 47(4):2473-2489.

[8] GRIFFITHS H, BAKER C J. Towards the Intelligent Adaptive Radar Network[C]// IEEE Radar Conference. IEEE, 2013:1-5.

[9] KARIM M E, PHOHA V V. Cyber-Physical Systems Security[M]. New York: Springer, 2014.

[10] YANG C, ZHANG H, QU F, et al. Performance of Target Tracking in Radar Network System under Deception Attack[C]//International Conference on Wireless Algorithms, Systems, and Applications. Montréal: Springer International Publishing, 2015: 664-673.

[11] YANG C, ZHANG H, QU F, et al. Secured Measurement Fusion Scheme Against Deceptive ECM Attack in Radar Network[J]. Security and Communication Networks, 2016, 9(16):3911-3921.

[12] LESTRIANDOKO N H, JUHANA T, MUNIR R. Security System for Surveillance Radar Network Communication Using Chaos Algorithm[C]// International Conference on Telecommunication Systems Services and Applications. Bali: IEEE, 2015:1-6.

[13] CHEN H, HIMED B. Analyzing and Improving MIMO Radar Detection Performance in the Presence of Cybersecurity Attacks[C]// IEEE Radar Conference. Philadelphia: IEEE, 2016:1-4.

(下转第 92 页)

[9] 那丹彤.跳频通信干扰与抗干扰技术[M].北京:国防工业出版社,2013.
NA D T. Technology of Frequency-Hopping Communication Jamming and Anti-Jamming[M]. Beijing: National Defense Industry Press,2013. (in Chinese)

[10] 齐海兵.自适应滤波器算法设计及其 FPGA 实现的研究与应用[D].长沙:中南大学,2006.
QI H B. Design and Application of Adaptive Filter Algorithm and Its FPGA Implementation[D]. Changsha: Central South University,2006. (in Chinese)

[11] AZUBOGU A C O, NWALOZIE G C, IDIGO V E, et al. Simulation Evaluation of Least Mean Square (LMS) Adaptive Beamforming Algorithm tor Smart Antennas[J]. The IUP Journal of Telecommunications, 2012,IV(1):27-39.

[12] JEONG T T,KOO K,CHOI G T,et al. A Variable Step Sizefor Normalized Subband Adaptive Filters [J]. IEEE Signal Processing Letters,2012,19(12): 906-909.

[13] HUANG H, LEE T. A New Variable Step-Size NLMS Algorithmand Its Performance Analysis[J]. IEEE Transactions Signal Process, 2012, 60(4): 2055-2060.

[14] QIN J F. A Novel Variable Step Size LMS Adaptive Filtering Algorithm Based on Sigmoid Function[J]. Journal of Data Acquisition&Processing, 1997, 12(3):171-174.

[15] YANG Y, CAO X Y, YANG Q, et al. New Variable Step-Size LMS Algorithm Based on Exponential Function[J]. Computer Engineering, 2011, 38(10): 134-136.

[16] MAYYAS K, MOMANI F. An LMS Adaptive Algorithm with a New Step-Size Control Equation[J]. Journal of the Franklin Institute, 2011, 348(4): 589-605.

[17] YI Y, WOODS R, TING L K, et al, High Speed FPGA-Based Implementations of Delayed-LMS Filters[J]. Journal of VLSI Signal Processing Systems for Signal, Image and Video Technology, 2005(1):113-131.

[18] TINGL K, WOODS R, COWAN C F N. Virtex FPGA Implementation of a Pipelined Adaptive LMS Predictor for Electronic Support Measures Receivers[J]. IEEE Transactions on Very Large Scale Integration Systems, 2005,13(1):86-95.

[19] MAHFUZ E, WANG C, AHMAD M O, A High-Throughput DLMS Adaptive Algorithm[C]//IEEE International Symposium on Circuits and Systems. Kobe, Japan: IEEE, 2005:3753-3756.

[20] OBA H, KIM M, ARAI H, FPGA Implementation of LMS and N-LMS Processor for Adaptive Array Applications[C]//2006 International Symposium on Intelligent Signal Processing and Communications. Tottori, Japan: IEEE, 2006:485-488.

(编辑:徐楠楠)

(上接第 58 页)

[14] ZHAO Z C, WANG X S, XIAO S P. Cooperative Deception Jamming Against Radar Network Using a Team of UAVs[C]// Radar Conference, 2009 IET International. Guilin: IET, 2009:1-4.

[15] TAHMOUSH D. Securing Radars Using Secure Wireless Sensor Networking[C]// SPIE Defense + Security. Amsterdam: SPIE, 2014:90970B.

[16] CHAN H, PERRIG A, SONG D. Random Key Predistribution Schemes for Sensor Networks[C]// Proceedings 2003 Symposium on Security and Privacy. IEEE, 2003:197-213.

[17] 赵永刚.基于雷达/红外数据融合跟踪系统简述[J].电脑与信息技术,2017,25(2):20-22.
ZHAO Y G. Research on Tracking System Based on Radar/Infrared Data Fusion[J]. Computer & Information Technology, 2017, 25(2): 20-22. (in Chinese)

[18] 李翠芸,王精毅,姬红兵.模型参数未知时的 CPHD 多目标跟踪方法[J].西安电子科技大学学报,2017,44(2):37-41.
LI C Y, WANG J Y, JI H B. CPHD Multi-Target Tracking Algorithm with Unknown Model Parameters[J]. Journal of Xidian University, 2017, 44(2): 37-41. (in Chinese)

[19] 马丽丽,陈金广,胡西民,等.目标跟踪性能的评价准则[J].西安工程大学学报,2013,27(3): 364-368.
MA L L, CHEN J G, HU X M, et al. Evaluation Metrics for Filtering Performance in Target Tracking System[J]. Journal of Xi'an Polytechnic University, 2013,27(3): 364-368. (in Chinese)

[20] MO Y, SINOPOLI B. Secure Control Against Replay Attacks[C]// Allerton Conference on Communication, Control, and Computing. Illinois: IEEE, 2009:911-918.

[21] ZHANG H, CHENG P, SHI L, et al. Optimal DoS Attack Policy Against Remote State Estimation[C]// Decision and Control. Firenze: IEEE, 2013:5444-5449.

[22] GUO H D, ZHANG X H. Distributed Fusion of Multisensory Data Based on Probabilistic Data Fusion[J]. Control and Decision, 2004, 19(12): 1359-1363.

[23] HE Y, XIU J J, GUAN X. Radar Data Processing with Applications[M]. New York: John Wiley & Sons, 2016.

(编辑:徐楠楠)