ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, 25-27 June, 2017, pp. 574-578
doi: 10.18178/wcse.2017.06.099

Performance of Target Tracking in Radar Network Under Replay Attack

Dong Lin [+], Buhong Wang and Zhenhao Wang

Information and Navigation College, Air Force University, Xi’an, 710077, China

Abstract. As a complicated distributed system, radar network is vulnerable to various attacks. In this paper, a replay attack model for radar network is proposed based on the theory of cyberspace. Replay attack has the advantages of simple implementation and outstanding effect. Based on the influence of replay attack on the performance of single radar target tracking, the paper extends to the research on the influence of the radar network. The simulation results show that the replay attack has a significant effect on the target tracking performance of the radar network.

Keywords: Target tracking, Replay attack, Radar network.

1. Introduction

Since the proposed, the radar network has been a hot research at home and abroad. Radar network consists of multiple radars appropriately deployed in difference geographic positions, has shown the capability of achieving better detection and tracking performance compared conventional radars by utilizing spatial diversity and data fusion technique [1]. Radar network, as a typical multi-sensor target tracking system, which plays an important role in both civilian and military application[2].

While bringing performance to the same time, the radar network is facing a serious security challenge. Compared with the traditional single-base or multi-base radar, radar network is more complex, more difficult to achieve. Because these radars are distributed in a wide area and need to send the collected target information to the data fusion center, the transmitter, receiver, communication link and data fusion center of the radar network are vulnerable to attack [10].

The traditional means of attack for the radar there are two, namely, deception and suppression of interference [11]. In recent years, as a typical multi-sensor system, radar network is also facing new security challenges. The At present, there are two kinds of new attacks for radar network, denial of service attacks and deceptive attacks [3]. Denial of service attacks similar to the traditional Internet attacks, attack radar network communication system links to prevent the exchange of data. Deceptive attacks affect the performance of the radar by modifying the radar's real data or injecting false data. On the basis of the above research, this paper proposes a special deceptive attack - replay attack. The attacker first collects a series of data from the target, and the attacker can modify the data according to the needs of the attack, and finally re-send the modified data to the radar network at a certain time.

The rest of the paper is organized as follows: Sect. 2 describes the problem formulation. Section 3 analyzes the performance of target tracking when radar network is under replay attack. Section 4 presents the simulation result. Finally Sect. 5 concludes the whole paper.

2. Problem Formulation

[+] Corresponding author. Tel.: 15328228274
E-mail address: dongllss@163.com

This paper is based on a centralized radar network, which contains several independent radar and a data fusion center. Each radar sends the detected target information to the data fusion center. The data fusion center obtains and processes the data of these probes, and finally obtains the position and velocity information of the detection target. In this paper, it is assumed that the data fusion center uses PDA (probabilistic data association) algorithm for data fusion, and each radar uses Kalman filter algorithm for data filtering.

2.1. Target Dynamics and Measurement Equation

In Cartesian coordinate, we build the movement model of the target [4], as in Formula 1:

$$x_{k+1} = Fx_k + v_k \,, \qquad x_k \in R^{n_x} \tag{1}$$

x_k is the state vector of the moment k; F is the state transition matrix; v_k is zero-mean, white Gaussian noise with covariance Q. In Cartesian coordinates, the state vector contains velocity and position information.

Assuming that the radar network contains n radars, the measured value of the first radar is recorded as:

$$y_{k+1}^i = Hx_{k+1} + w_{k+1}^i \,, \qquad i \in [1, n] \tag{2}$$

H is the radar measurement matrix; w_k^i is zero-mean, white Gaussian noise with covariance R^i.

2.2. Kalman-filter-based data fusion scheme

Kalman filter provides an unbiased and optimal estimation of targets state-vector in the sense of minimum estimation covariance and can be described as follows [5]:

$$x_{k+1|k} = Fx_{k|k} \tag{3}$$

$$P_{k+1|k} = FP_{k|k}F^T + Q \tag{4}$$

$$K_k = P_{k|k-1}H^T \left(HP_{k|k-1}H^T + R\right)^{-1} \tag{5}$$

$$x_{k|k} = x_{k|k-1} + K_k \left(y_k - Hx_{k|k-1}\right) \tag{6}$$

$$P_{k|k} = P_{k|k-1} - K_k HP_{k|k-1} \tag{7}$$

where $x_{k|k}$ represents the state minimum mean squared error estimate, $x_{k+1|k}$ represents one step predicted state estimate, $P_{k|k}$ is the covariance of the estimate error, $P_{k+1|k}$ is the covariance of one step predicted state estimate, and K_k is the gain at each time k, F^T stands for the transposition of F .Although the Kalman filter uses a time varying gain K_k , it is known that this gain will converge if the system is detectable and steady[6]. Hence, we can define:

$$P = \lim_{k\to\infty} P_{k|k} \quad , \; K = \lim_{k\to\infty} K_{k|k} \tag{8}$$

Since PDA algorithm is one of the most fundamental fusion algorithms, we choose PDA algorithm to analyze in this paper. The data fusion center uses the predicted state estimate $x_{k|k-1}$ at time $k-1$ as a step prediction value within the validation region. Then it assigns a weighting factor to the data of each radar in the validation region at time k [7]. The PDA algorithm can be described as follows[8]:

$$x_{k|k} = x_{k|k-1} + K_k \sum_{i=1}^{n} \beta_k^i u_k^i \tag{9}$$

$$u_k^i = y_k^i - H_i F x_{k-1|k-1} \tag{10}$$

$$\beta_k^i = \frac{N\left\lfloor u_k^i; 0, S_k \right\rfloor}{b + \sum_{j=1}^{n} N\left[u_k^j; 0, S_k\right]} \tag{11}$$

$$\beta_k^0 = \frac{b}{b + \sum_{j=1}^{n} N[u_k^j; 0, S_k]} \tag{12}$$

$$P_{k|k} = P_{k|k-1}\beta^0 + (I - \beta^0)\left(I - K_k H\right)P_{k|k-1} + \tilde{P}_k \tag{13}$$

$$\tilde{P}_k = K_k \left\lfloor \sum_{j=1}^{n} \beta_k^i u_k^i u_k^{iT} - \left(\sum_{j=1}^{n} \beta_k^i u_k^i\right)\left(\sum_{j=1}^{n} \beta_k^i u_k^i\right)^T \right\rfloor K_k^T \tag{14}$$

In the above formulas, b is a constant number， $N\lfloor u_k^j;0,S_k \rfloor$ represents that the residues u_k^j is Gaussian distributed with zero mean and covariance S_k , β_k^i Is the data association probability, which represents the weighting factor of the measurement of the i -th radar at time k .

2.3. Replay attack

We suppose that an attacker can obtain a sequence of measurement y_k of a radar station and obtain attack data y_k' based on y_k . The attacker will implement the following attack strategy, which can be divided into two stages:

- The attacker records enough measurements y_k without interfering with the radar
- The attacker replays the attack data y_k' to the radar networking system

It is worth noticing that in the attacking stage, the goal of the attacker is to make the attack data y_k' look normal y_k . Replaying the previous y_k is just the easiest way to achieve this goal [8]. In order to provide a unified framework to analyze such kind of attack, we can think of y_k' as the output of the following virtual system:

$$x_{k+1}' = Fx_k' + v_k', \qquad x_k' \in R^{n_x} \tag{15}$$

$$y_{k+1}^i{}' = Hx_{k+1}' + w_{k+1}^i{}', \quad i \in [1,n] \tag{16}$$

$$x_{k+1|k}' = Fx_{k|k}' \quad x_{k+1|k+1}' = x_{k+1|k}' + K_k\left(y_{k+1}' - Hx_{k+1|k}'\right) \tag{17}$$

For a replay attack, the time interval from the start of recording the real data to the attack is set to t .Then the virtual sys tem is just a time shifted version of the real system:

$$x_k' = x_{k-t}, \quad x_{k|k}' = x_{k-t|k-t} \tag{18}$$

Without loss of generality, we assume that only the n -th radar is hijacked. Since the estimation error will converge exponentially, we also assume the state estimation is steady before attacker action implements. If the attack occurs at time k , we can obtain:

$$y_k^i{}' = \begin{cases} y_k^i, i \in [1,n-1] \\ y_k^i{}', i = n \end{cases} \tag{19}$$

3. Performance Analysis of Target Tracking Under Replay Attack

According to (5), it is obvious that the attack does not influence K_k . There is no doubt that the system has been different from the initial system, because the data fusion center did not notice the existence of the attack will lead to K_k is no longer the best state[9]. From (4) and (7), similarly, we can see that under attack $P_{k|k}$ and $P_{k+1|k}$ do not change. In summary, the following formulas can be obtained:

$$K_k' = K_k, \quad P_{k|k}' = P_{k|k}, \quad P_{k+1|k}' = P_{k+1|k} \tag{20}$$

Thirdly, we investigate $x_{k+1|k+1}$ after the attack. Let $\Delta y_k = y_k - y_k'$, indicates the deviation of the measurement caused by the attacker at time k . According to (16) and (18), $\Delta y_k = y_k - y_{k-t}$. Similarly, let $\Delta x_{k+1} = x_{k+1|k+1} - x_{k+1|k+1}'$, represents the attenuation of the state estimation performance at time $k+1$. According to (3) and (6), $x_{k|k} = (I - K_k H)Fx_{k-1|k-1} + K_k y_k$. In summary,

$$\Delta x_{k+1} = (I - KH)F\Delta x_k + K\Delta y_{k+1} \tag{21}$$

Ignoring the effects of noise, available from (1) and (2), $\Delta y_{k+1} = H(x_{k+1} - x_{k+1-t}) = H(F^t - I)x_{k+1-t}$. It can be seen that the deviation of the measurement produced by the replay attack is independent of the starting time in the uniform linear motion model, only with the time difference t between the data recording time and the attack start time. Therefore, make $\Delta y_{k+1} = \Delta y(t)$ and $M = (I - KH)F$, then (21) can be expressed as:

$$\Delta x_{k+1} = M\Delta x_k + K\Delta y(t) \tag{22}$$

Because the system is stable, it must converge to a stable value, so you can get:

$$\lim_{l\to\infty} \Delta x_l = -(M - I)^{-1} K\Delta y(t) \tag{23}$$

From (23), we can see that the stability of the state estimation error is approximately linear with the measurement deviation.

Assume that all radars' measurements are in validation region. Therefore, (12) and (13) where b is 0 and $\sum_{i=1}^{n} \beta_k^i = 1$. For easy to deduction, it is assumed that $H_i = H, \forall i$, From (9) and (10), we can obtain:

$$x_{k|k} = \left(I - K_k H\right) F x_{k-1|k-1} + K_k \sum_{i=1}^{n} \beta_k^i y_k^i \tag{24}$$

Similar to a single radar attack, the replay attack does not change the K_k at time k and K_k will converge to K . At the same time, the system will converge after limited steps. However, according to (9) and (10), because of the attack to n-th radar, u_k^n will change to $u_k^{n\prime}$, which will also cause changes of β_k^i 、 $P_{k|k}$ and $P_{k+1|k}$. The estimated error for the time $k+1$ is defined as $\Delta x_{k+1} = x_{k+1|k+1} - x_{k+1|k+1}{}'$, and measurement deviation of the n-th radar is defined as $\Delta y_{k+1}^n = y_{k+1}^n - y_{k+1}^n{}'$, State estimation error can be expressed as:

$$\Delta x_{k+1} = \left(I - KH\right) F \Delta x_k + K\left(\sum_{i=1}^{n} \beta_{k+1}^i y_{k+1}^i - \sum_{i=1}^{n-1} \beta_{k+1}^i{}' y_{k+1}^i - \beta_{k+1}^n{}' y_{k+1}^n{}'\right) \tag{25}$$

4. Simulation

Set up a radar network with 3 radars and a data fusion center to monitor a two-dimensional area. The initial position of the target is $\left[20m, 10m\right]$ and initial speed is $\left[2m/s, 1m/s\right]$. The dynamic model of the target is the same as the formula (1), the state transition matrix F, measurement matrix H and measurement error covariance matrix R:

$$F = \begin{bmatrix} 1\,0\,T\,0 \\ 0\,1\,0\,T \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{bmatrix}, \quad H = H_i = \begin{bmatrix} 1\,0\,0\,0 \\ 0\,0\,1\,0 \end{bmatrix}, \quad R = \begin{bmatrix} r\;0 \\ 0\;r \end{bmatrix} \tag{26}$$

where T =1 is the sample period, r = 25 m, the state x_k consists of position and velocity.

Figure 1 and Figure 2 show the estimated error of the single radar and radar network in the absence of attack . Attack at 100s, $t = 2$, as can be seen from the figures, the error over time converges to a stable value. Moreover, the same attack parameters, the error of radar network is less than a single radar, because the PDA data fusion algorithm can improve the accuracy of a certain extent.

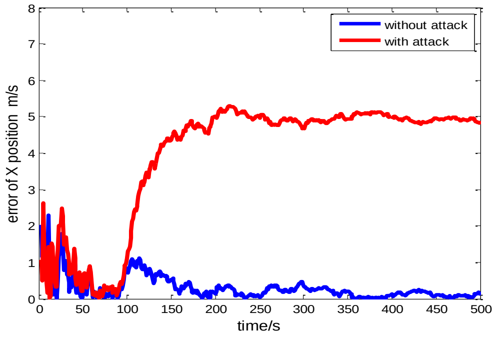

Fig. 1: Position error of one radar station

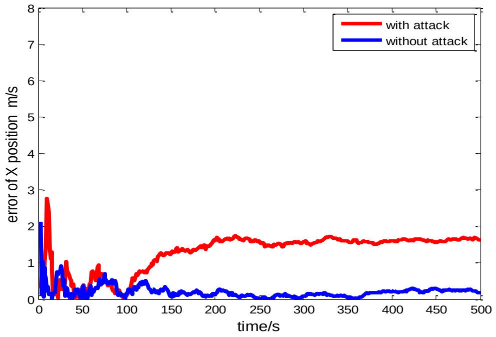

Fig. 2: Position error of one radar network

In Figure 3, it can be seen that the estimated error Δx_{k+1} of the single radar is linear with the attack parameter t under the simulation condition, and it is proved that the correctness of (34).As shown in Figure 4, in the radar network, Δx_{k+1} and t are not linear. From (12) and (38), we can see that the larger the attack parameters, the smaller the weight coefficient of the radar, so when the attack parameter exceed a certain threshold, attack effect will drop. However, there is a maximum estimate error, which means that a reasonable selection of attack parameter can maximize the attack effect. It can be seen that the radar network has a certain anti-interference ability.

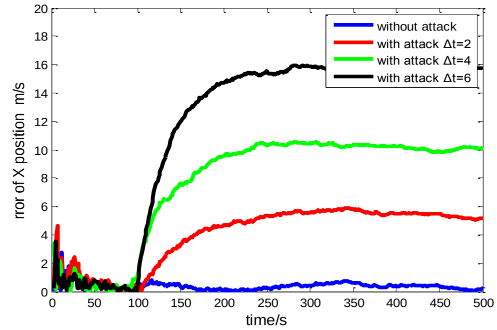

Fig. 3: single radar, relationship between Δ*x* and *t*

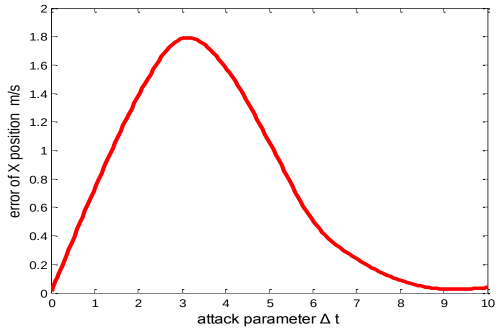

Fig. 4: radar network, relationship between Δ*x* and *t*

5. Conclusion

In this paper, the target tracking performance of the radar network system under the replay attack is studied. After problem formulation, the tracking performance of a single radar under the replay attack is studied. Based on this, it extends to the target tracking performance of the radar network system under the replay attack, and also analyzes the relationship between the attack parameter and the estimation error. Finally, the correctness of the research is proved by simulation

6. References

[1] Walters J P, Liang Z, Shi W, et al. Wireless sensor network security: A survey [J]. Security in distributed, grid, mobile, and pervasive computing, 2007, 1: 367.

[2] Dutta P K, Arora A K, Bibyk S B. Towards radar-enabled sensor networks[C]// International Conference on Information Processing in Sensor Networks. IEEE, 2006:467-474.

[3] Parno B, Perrig A, Gligor V. Distributed detection of node replication attacks in sensor networks[C]// Security and Privacy, 2005 IEEE Symposium on. DBLP, 2005:49-63.

[4] Mo Y, Sinopoli B. Secure control against replay attacks[C]//Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on. IEEE, 2009: 911-918.

[5] Yang C, Zhang H, Qu F, et al. Performance of target tracking in radar network under deception attack[C]//International Conference on Wireless Algorithms, Systems, and Applications. Springer International Publishing, 2015: 664-673.

[6] Zhang H, Cheng P, Shi L, et al. Optimal DoS attack policy against remote state estimation[C]//Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on. IEEE, 2013: 5444-5449.

[7] 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.

[8] You H, Jianjuan X, Xin G. Radar data processing with applications[M]. John Wiley & Sons, 2016.

[9] Lee E H, Musicki D, Song T L. Multi-sensor distributed fusion based on integrated probabilistic data association[C]//Information Fusion (FUSION), 2014 17th International Conference on. IEEE, 2014: 1-7.

[10] Chen, H, Himed, B. Analyzing and improving MIMO radar detection performance in the presence of cybersecurity attacks. IEEE Radar Conference. IEEE, 2016, pp.1-4.

[11] Wu Y. Research on Electronic Jamming Technology for Networked Radar. University of Electronic Science and Technology, 2013.