Unobservable Collaborative Byzantine Attacks in the Distributed Target Localization

Author 1 and Author 2

Abstract

In this letter, we investigate unobservable collaborative Byzantine attacks in distributed target localization from the perspective of the attacker. By sending the falsified data to the fusion center (FC), an unobservable collaborative data Byzantine attack misleads the FC to make incorrect location estimation, as well as hides the presence of Byzantine nodes. We present the equivalent condition and the minimum cost of launching an unobservable attack. Numerical results show that the optimal unobservable collaborative attacks are based on the topology of sensors within the transmission range of the attacked target.

Index Terms

Unobservable attack, collaborative Byzantine attacks, distributed target localization

I. Introduction

DISTRIBUTED target localization is a typical application in wireless sensor networks (WSNs) [1]. The framework of distributed target localization consists of a group of spatially deployed sensors that observe the target and send the processed data to the fusion center (FC). The FC then estimates the location of the target.

To achieve higher estimation accuracy, authors in [2] proposed a time-of-arrival based location estimation algorithm. However, this technique requires extra equipment for sensors in the network. Authors in [3] studied the range-free distributed target localization problem, and proposed the received signal strength based method. In addition, authors in [4] addressed the range-based distributed target localization problem. The proposed method offers high estimation accuracy. However, the attack problem is not considered in these methods.

Distributed target localization is used to estimate the location of a target in the region of interest (ROI). As such, security is an important issue. Byzantine attack is a typical attack technique in distributed target localization. In this letter, we focus on Byzantine data attacks, in which some compromised sensors send falsified local processed data to the FC to undermine the distributed estimation performance. Two types of Byzantine data attacks, independent attack and collaborative attack, are defined in [5]. Nadendla et al. [6] addressed the problem of distributed target localization with quantized data in the WSN under independent Byzantine data attack, and presented an optimal attack strategy to make the FC incapable of estimating the target location. A generalized Byzantine data attack model is defined for distributed estimation [7], and an enhanced expectation-maximization algorithm is proposed to estimate the desired parameters. Most extant research deals with independent Byzantine data attacks in distributed target localization, and does not address collaborative Byzantine data attacks. Our study is intended to remedy the lack of information on collaborative Byzantine data attacks in distributed target localization.

We study collaborative Byzantine data attacks in distributed target localization from the perspective of the attacker. At the FC, we adopt the range-based location estimation method proposed in [8] to estimate the target location. We propose an unobservable collaborative Byzantine data attack strategy, which causes the FC to make wrong location estimation. The proposed strategy also hides the presence of Byzantine node(s). In addition, we address the equivalent condition and the minimum cost of launching unobservable collaborative attacks.

II. System Model

A. Distributed Target Localization Framework

We consider a 2-dimensional Cartesian plane deployed with N sensors and G targets. Let $\boldsymbol{u}_g$ be the location of target g, $\boldsymbol{u}_g = [x_g, y_g]^T \in \mathbb{R}^{2\times 1}$, $\boldsymbol{z}_i = [x_i, y_i]^T \in \mathbb{R}^{2\times 1}$ is the location of sensor i. The locations of the targets and sensors can be expressed by $\mathbf{u} = [\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_G]^T \in \mathbb{R}^{G\times 2}$ and $\mathbf{z} = [\boldsymbol{z}_1, \boldsymbol{z}_2, \ldots, \boldsymbol{z}_N]^T \in \mathbb{R}^{N\times 2}$, respectively. The locations of all the targets and sensors can be represented as $\mathbf{x} = [\mathbf{u}^T, \mathbf{z}^T]^T \in \mathbb{R}^{(G+N)\times 2}$.

We assumed that sensors are sparsely deployed in the ROI. If the distance between sensor i and target g is too large, sensor i cannot sense the radiated signal from target g. As such, for a range-based location estimation method, only sensors within the transmission range of target g can obtain a local measurement (i.e., each target is partially observed by sensors in the network).

Define $\boldsymbol{e}_{g,i}$ be the vector in which the gth element is 1 and the $(G+i)$th element is -1, while the other elements are 0, $\boldsymbol{e}_{g,i} \in \mathbb{R}^{(G+N)\times 1}$, $g \in \{1, 2, \ldots, G\}$ and $i \in \{1, 2, \ldots, N\}$. Therefore, we have $\boldsymbol{e}_{g,i}^T \mathbf{x} = \boldsymbol{u}_g^T - \boldsymbol{z}_i^T = \boldsymbol{y}_{g,i}^T$, where $\boldsymbol{y}_{g,i} \in \mathbb{R}^{2\times 1}$

Manuscript received April 16, 2017.

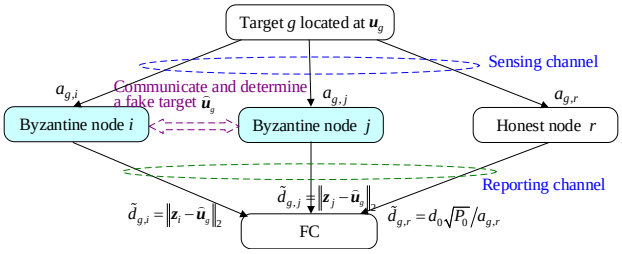

Fig. 1. An illustration of the collaborative Byzantine data attack model

is the location difference between target g and sensor i. $\bar{d}_{g,i}$ is the true distance between target g and sensor i. As such, $\bar{d}_{g,i} = |\boldsymbol{u}_g^T - \boldsymbol{z}_i^T| = |\boldsymbol{y}_{g,i}^T|$. $|\boldsymbol{c}|$ is defined as follows: if $\boldsymbol{c}$ is a vector, $|\boldsymbol{c}|$ is the 2-norm of vector $\boldsymbol{c}$; if $\boldsymbol{c}$ is a matrix, $|\boldsymbol{c}|$is a column vector consisting of 2-norm of each row vector in matrix $\boldsymbol{c}$. $\bar{\mathbf{d}} \in \mathbb{R}^{L\times 1}$ is the local distance vector, $\bar{\mathbf{d}} = [\bar{d}_1, \bar{d}_2, \ldots, \bar{d}_L]$, where L is the number of all the local measurements for the distributed target location estimation.

The signal radiated from the target is assumed to follow an isotropic power attenuation model as $\bar{a}_{g,i}^2 = P_0(d_0/\bar{d}_{g,i})^\kappa$, where $\bar{a}_{g,i}$ is the received signal amplitude at sensor i from target g, P_0 is the power measured at a reference distance d_0, and κ is the path-loss exponent. Without loss of generality, $d_0 = 1$ and $\kappa = 2$. In this study, we assumed that a target is not on a sensor, and $\bar{d}_{g,i} \neq 0$.

First, sensor i obtains a local measurement of the received signal amplitude from target g, $a_{g,i}$. Based on $a_{g,i}$ and the isotropic power attenuation model, sensor i calculates the local distance measurement of target g as $d_{g,i} = d_0\sqrt{P_0}/a_{g,i}$.

Let $\mathbf{d} \in \mathbb{R}^{L\times 1}$ be the vector consisting of all the distance measurements available in a network without compromised sensors. Therefore, we have $E(\mathbf{d}) = \bar{\mathbf{d}}$. We assumed that each element in $\mathbf{d} - \bar{\mathbf{d}}$ is dependent, identically distributed, and follows Gaussian distribution, $\mathcal{N}(0, \sigma^2)$.

B. Collaborative Byzantine Data Attack Model

Fig. 1 illustrates the collaborative Byzantine data attack model. There are 3 sensors, i, j, and r, in the transmission range of target g, where sensors i and j are Byzantine nodes and sensor r is an honest node. We assumed that the communication channels between sensors and the FC are error-free.

Let $\widetilde{d}_{g,r}$ be the received distance measurement of target g sent by sensor r at the FC. Therefore, $\widetilde{d}_{g,r} = d_{g,r}$. However, Byzantine nodes i and j send the falsified distance measurements to make the FC generate a wrong location estimation of target g instead of $\boldsymbol{u}_g$. We name the wrong locations of a target suspected of cooperating with Byzantine nodes "fake targets".$\widehat{\boldsymbol{u}}_g$ is the fake target of target g. Since fake targets are the ultimate goal of Byzantine nodes, the distances between $\widehat{\boldsymbol{u}}_g$ and the Byzantine nodes are sent in place of the correct distances. Specifically, Byzantine nodes i and j send $\widetilde{d}_{g,i}$ and $\widetilde{d}_{g,j}$ to the FC, $\widetilde{d}_{g,i} = \|\boldsymbol{z}_i - \widehat{\boldsymbol{u}}_g\|_2$ and $\widetilde{d}_{g,j} = \|\boldsymbol{z}_j - \widehat{\boldsymbol{u}}_g\|_2$.

Similarly, other targets can be attacked by Byzantine nodes within their transmission range. Let $\widetilde{\mathbf{d}} \in \mathbb{R}^{L\times 1}$ be the vector consisting of all the distance measurements received by the FC.

$\mathbf{E}$ is a matrix whose row vectors are $\boldsymbol{e}_{g,i}^T$ and $\mathbf{E} \in \mathbb{R}^{L\times(G+N)}$. Similarly, $\mathbf{y}$ is a matrix whose row vectors are $\boldsymbol{y}_{g,i}^T$, $\boldsymbol{y}_{g,i}^T \in \mathbb{R}^{1\times 2}$ and $\mathbf{y} \in \mathbb{R}^{L\times 2}$. Thus, $\mathbf{Ex} = \mathbf{y}$. $\mathbf{E}$ can be partitioned as $\mathbf{E} = [\mathbf{E}_1, \mathbf{E}_2]$, where $\mathbf{E}_1 \in \mathbb{R}^{L\times G}$ and $\mathbf{E}_2 \in \mathbb{R}^{L\times N}$. By defining $\mathbf{v} \triangleq \mathbf{E}_2\mathbf{z}$, we have

$$\mathbf{E}_1\mathbf{u} + \mathbf{v} = \mathbf{y}, |\mathbf{E}_1\mathbf{u} + \mathbf{v}| = \bar{\mathbf{d}} \tag{1}$$

At the FC, we adopt the ranged-based location estimation method proposed in [8]. Let $\hat{\mathbf{u}}$ be the estimate of the targets' locations. At the kth iteration, the estimation procedure is given as

$$\begin{aligned} &\text{(i)}\ \ \mathbf{y}^{(k)} = \mathbf{E}_1\hat{\mathbf{u}}^{(k-1)} + \mathbf{v}, \\ &\text{(ii)}\ \ \widetilde{\mathbf{y}}_l^{(k)} = (\widetilde{d}_l\mathbf{y}_l^{(k)})/|\mathbf{y}_l^{(k)}|, l = 1, 2, \ldots, L, \\ &\text{(iii)}\ \ \hat{\mathbf{u}}^{(k)} = (\mathbf{E}_1^T\mathbf{E}_1)^{-1}\mathbf{E}_1^T(\widetilde{\mathbf{y}}^{(k)} - \mathbf{v}), \end{aligned} \tag{2}$$

where $\mathbf{y}_l^{(k)}$ is the lth row vector of $\mathbf{y}$ at the kth iteration, $\mathbf{y}_l^{(k)} \in \mathbb{R}^{1\times 2}$, and $\widetilde{\mathbf{y}}^{(k)} \in \mathbb{R}^{L\times 2}$. It is proved that the iterative estimation procedure in Eq. (2) converges well because no Byzantine nodes exist in the network[8].

When Byzantine nodes exist in the network, the FC should determine whether Byzantine nodes exist by using a residual test as in [9]. Specifically, the FC calculates the residual as $\|\widetilde{\mathbf{y}} - \mathbf{v} - \mathbf{E}_1\hat{\mathbf{u}}\|_2$. The presence of Byzantine nodes is declared if $\|\widetilde{\mathbf{y}} - \mathbf{v} - \mathbf{E}_1\hat{\mathbf{u}}\|_2 > \tau$, where τ is a pre-defined threshold.

III. Unobservable Collaborative Byzantine Data Attack Strategy

For distributed target localization in the WSN under collaborative Byzantine data attacks, $\widetilde{\mathbf{d}}$ used in Eq. (2) contains the falsified distance measurements introduced by the Byzantine nodes. Therefore, the iterative estimation procedure in Eq. (2) has two potential consequences. One potential consequence is that the procedure fails to converge. Another potential consequence is that the procedure converges and provides a wrong result.

If the iterative estimation procedure fails to converge, the attack can be easily detected by the FC. However, if the procedure converges and provides a wrong result, the residual calculated by $\|\widetilde{\mathbf{y}}-\mathbf{v}-\mathbf{E}_1\hat{\mathbf{u}}\|_2$ still remains at a small value, making it appears that all of the sensors in the network are honest. Specifically, the distributed target localization is suffering an unobservable collaborative Byzantine data attack, which means that Byzantine nodes make the FC obtain a wrong estimation of the target location while bypassing the residual test.

By using the iterative estimation procedure in Eq. (2), it is evident that $\widehat{\mathbf{u}}$ should be specifically designed to launch an unobservable collaborative Byzantine data attack. The equivalent condition of launching an unobservable collaborative attack is given in Theorem 1.

Theorem 1: Assume that the Byzantine nodes have prior knowledge of the deployment of the honest nodes and targets, and the matrix $\mathbf{E}$. The equivalent condition of launching an unobservable collaborative Byzantine data attack is to construct $\widehat{\mathbf{u}}(\widehat{\mathbf{u}} \neq \mathbf{u})$ so that the distances between all of the honest nodes and the true targets are equal to those between all of the honest nodes and the fake targets.

Proof: It is assumed that the Byzantine nodes launch a successful unobservable collaborative data attack and the distributed target location estimation process converges after K iterations. That is, $\hat{\mathbf{u}}^{(K)} = \hat{\mathbf{u}}^{(K-1)} = \breve{\mathbf{u}}$, where $\breve{\mathbf{u}}$ is the wrong estimate of the targets' locations. By combining this with Eq. (2), we have

$$\mathbf{E}_1\breve{\mathbf{u}} = \mathbf{y} - \mathbf{v}, \breve{\mathbf{u}} = (\mathbf{E}_1^T\mathbf{E}_1)^{-1}\mathbf{E}_1^T(\widetilde{\mathbf{y}} - \mathbf{v}) \tag{3}$$

Then, we have

$$\mathbf{y} - \mathbf{v} = \mathbf{E}_1(\mathbf{E}_1^T\mathbf{E}_1)^{-1}\mathbf{E}_1^T(\widetilde{\mathbf{y}} - \mathbf{v}) \tag{4}$$

Since $\mathbf{E}_1\breve{\mathbf{u}} = \mathbf{y} - \mathbf{v}$, both columns of $\mathbf{y} - \mathbf{v}$ fall into the column space of $\mathbf{E}_1$. That is,

$$\mathbf{y} - \mathbf{v} = \mathbf{P}_{\mathbf{E}_1}(\mathbf{y} - \mathbf{v}) \tag{5}$$

where $\mathbf{P}_{\mathbf{E}_1}$ is the projection matrix on the column space of $\mathbf{E}_1$, and $\mathbf{P}_{\mathbf{E}_1} = \mathbf{E}_1(\mathbf{E}_1^T\mathbf{E}_1)^{-1}\mathbf{E}_1^T$.

By combining Eqs. (4) and (5), we have $\widetilde{\mathbf{y}} = \mathbf{y}$. Using $\mathbf{E}_1\breve{\mathbf{u}} = \mathbf{y} - \mathbf{v}$ and $\widetilde{\mathbf{y}} = \mathbf{y}$, we have $\widetilde{\mathbf{y}} - \mathbf{v} - \mathbf{E}_1\breve{\mathbf{u}} = 0$. As such, if $\widetilde{\mathbf{y}} = \mathbf{y}$, the residual test is passed. From Eq. (2), we conclude that the condition$|\widetilde{\mathbf{y}}| = \widetilde{\mathbf{d}}$ is always true. Therefore, $|\mathbf{y}| = \widetilde{\mathbf{d}}$.

By using $\mathbf{E}_1\breve{\mathbf{u}} = \mathbf{y} - \mathbf{v}$ and $|\mathbf{y}| = \widetilde{\mathbf{d}}$,we have

$$|\mathbf{E}_1\breve{\mathbf{u}} + \mathbf{v}| = \widetilde{\mathbf{d}} \tag{6}$$

As an unobservable collaborative data attack is launched successfully by the Byzantine nodes, $E(\breve{\mathbf{u}}) = \widehat{\mathbf{u}}$. Therefore, Eq. (6) can be written in a statistic point of view as

$$|\mathbf{E}_1\widehat{\mathbf{u}} + \mathbf{v}| = \mathrm{E}\left(\widetilde{\mathbf{d}}\right) \tag{7}$$

where $|\mathbf{E}_1\widehat{\mathbf{u}} + \mathbf{v}|$ denotes the distances between all the sensors and fake targets.

$E(\widetilde{\mathbf{d}})$ includes two types of data. First, $E(\widetilde{\mathbf{d}})$ contains falsified data introduced by the Byzantine nodes. According to the collaborative attack model defined in Section II.B, the expectations of the falsified data are equal to the distances between the fake targets and the Byzantine nodes. Second, apart from the falsified data, the rest of the elements in $E(\widetilde{\mathbf{d}})$ are realistic distance measurements reported by honest nodes. The expectations of realistic distance measurements are equal to the distances between the true targets and the honest nodes.

Therefore, the equivalent condition of Eq. (7) is to make the distances between the true targets and the honest nodes equal to the distances between fake targets and honest nodes. ■

We provide the minimum cost of launching an unobservable collaborative Byzantine data attack in Theorem 2.

Theorem 2: The minimum cost of launching a collaborative Byzantine data attack on an arbitrary target g in an unobservable manner is to compromise some sensors within the transmission range of target g so that only one straight line can be drawn among the honest nodes within the transmission range of target g. Moreover, $\widehat{\boldsymbol{u}}_g$ should be set at the symmetrical point of $\boldsymbol{u}_g$ on the line.

Proof: Let $\mathbf{E}_{1g}^H, \boldsymbol{u}_g, \mathbf{v}_g^H, \mathbf{y}_g^H, \widetilde{\mathbf{d}}^H$ be the part of $\mathbf{E}_1, \mathbf{u}, \mathbf{v}, \mathbf{y}, \widetilde{\mathbf{d}}$ related to target g and the honest nodes within the transmission range of target g. Theorem 2 is proven with the contradiction method.

If more than one line can be formed among the honest nodes within the transmission range of target g, then there should be at least 3 honest nodes within the transmission range of target g, and these nodes should not be on the same line. Therefore, $|\mathbf{E}_{1g}^H\boldsymbol{u}_g + \mathbf{v}_g^H| = \widetilde{\mathbf{d}}^H$ is an over-determined equation. The FC can estimate the location of target g correctly only using the distance measurements reported by honest nodes. Specifically, the attacker cannot find $\widehat{\boldsymbol{u}}_g(\widehat{\boldsymbol{u}}_g \neq \boldsymbol{u}_g)$, which makes the distances between the fake targets and the honest nodes equal to the distances between target g and the honest nodes. Thus, the condition in Theorem 1 is not satisfied and the attacker cannot launch an unobservable collaborative Byzantine data attack.

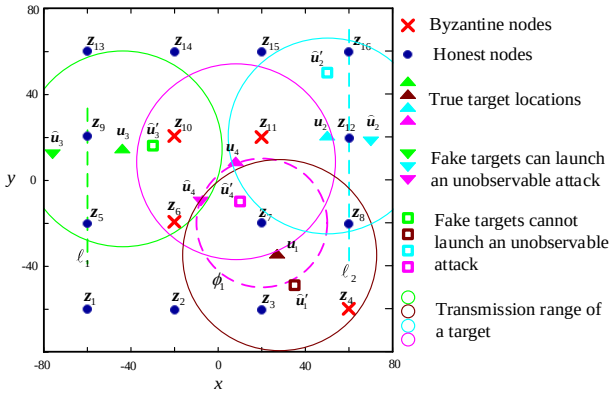

Fig. 2. An illustrative example with 16 sensors and 4 targets deployed in the ROI with $160m \times 160m$

Therefore, the minimum cost of launching an unobservable collaborative Byzantine data attack is to compromise some sensors within the transmission range of target g so that only one straight line can be drawn among the honest nodes within the transmission range of target g.

If point A and point B are symmetrical to a straight line, then the distance between any point on the line (such as point C) and point A is the same as that between point C and point B. Therefore, the attacker should set the fake target at the symmetrical point of $\boldsymbol{u}_g$ on the line to satisfy the condition in Theorem 1. ■

IV. Numerical Results

Fig. 2 is an illustrative example that includes 12 honest nodes, 4 Byzantine nodes, and 4 targets. As illustrated in Fig. 2, a circle in a solid line denotes the transmission range of the target located at the center. Only sensors deployed in a circle can obtain local observations of the corresponding target. Fig. 2 illustrates 4 typical topologies corresponding to 4 targets. Any topology of sensors within the transmission range of a target can be mapped to one of the 4 typical topologies.

Table I lists the effects of a collaborative Byzantine data attack under different topologies, where σ^2=10 and τ=2.63. The estimation performance is evaluated in terms of the root mean square error (RMSE). Attack cost is denoted by the percentage of Byzantine nodes among sensors in the corresponding topology.

For topology 1, the attacker cannot launch an unobservable collaborative attack because the attack cost is smaller than the minimum cost. For topologies 2 and 3, the attacker can launch an unobservable collaborative attack because only one straight line (ℓ_2 and ℓ_1) is formed among the compromised sensors. Moreover, the fake target ($\widehat{\boldsymbol{u}}_2$ and $\widehat{\boldsymbol{u}}_3$) should be chosen as the symmetrical point of the true target ($\boldsymbol{u}_2$ and $\boldsymbol{u}_3$) on the line (ℓ_2 and ℓ_1). From the comparison, it is evident that the minimum cost is determined by the deployment of sensors in the topology. For topology 4, the Byzantine nodes can launch an unobservable collaborative attack because the attack cost is larger than the minimum cost. Moreover, the fake target can be set as any point on ϕ_1 except $\boldsymbol{z}_7$, where ϕ_1 is a circle using $\boldsymbol{z}_7$ as the center and the distance between $\boldsymbol{z}_7$ and $\boldsymbol{u}_4$ is the radius.

From Table I, it is evident that when an unobservable collaborative attack is launched, the RMSE is high while the residual is small. That is, the estimated location is far from the actual location, while the presence of the Byzantine nodes remains hidden.

If the fake target is randomly set, the estimated location is still far from actual location, but the residual is much larger than τ. Hence, the attacker deteriorates the network at the price of exposing the presence of the Byzantine nodes.

V. Conclusion

In this letter, we studied unobservable collaborative Byzantine data attacks in the distributed target localization, where the ranged-based location estimation method is used at the FC. From the equivalent condition in Theorem 1 and the minimum cost in Theorem 2, it can be seen that an unobservable collaborative attack should be launched based on the topology of the sensors within the transmission range of the target to be attacked. Numerical results show that our proposed collaborative attack strategy can cause the FC to make an incorrect location estimation, while also hide the presence of Byzantine nodes. Moreover, if the number of compromised nodes in cooperation is larger than the minimum cost, more potential locations can be chosen as the fake target for launching an unobservable attack.

References

[1] J. Li, R. Zhao, J. Chen, C. Zhao, and Y. Zhu, "Target tracking algorithm based on adaptive strong tracking particle filter," *IET Sci. Measurement Tech.*, vol. 10, no. 7, pp. 704–710, Sep. 2016.

[2] T. Qiao and H. Liu, "An improved method of moments estimator for TOA based localization," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1321–1324, July 2013.

TABLE I
THE EFFECTS OF COLLABORATIVE BYZANTINE DATA ATTACK UNDER 4 TYPICAL TOPOLOGIES

	Without Byzantine attack	CAN launch an unobservable collaborative attack	CANNOT launch an unobservable attack
1# topology			
4 sensors	$\boldsymbol{z}_3$=(20,-60),$\boldsymbol{z}_4$=(60,-60) [1],$\boldsymbol{z}_7$=(20,-20),$\boldsymbol{z}_8$=(60,-20)		
True target	$\boldsymbol{u}_1$=(27,-37)		
Fake target	-	-	$\widehat{\boldsymbol{u}}'_1$=(35,-48)
Estimate target	(27.51,-35.26)	-	(33.17,-38.99)
RMSE	1.81	-	6.49
Residual	1.12	-	8.98
Attack cost	-	-	25%
2# topology			
4 sensors	$\boldsymbol{z}_8$=(60,-20),$\boldsymbol{z}_{11}$=(20,20),$\boldsymbol{z}_{12}$=(60,20),$\boldsymbol{z}_{16}$=(60,60)		
True target	$\boldsymbol{u}_2$=(50,20)		
Fake target	-	$\widehat{\boldsymbol{u}}_2$=(70,20)	$\widehat{\boldsymbol{u}}'_2$=(50,50)
Estimate target	(51.28, 21.62)	(69.31, 21.59)	(65.39, 22.10)
RMSE	2.07	19.38	15.53
Residual	0.03	0.92	4.43
Attack cost	-	25%	25%
3# topology			
4 sensors	$\boldsymbol{z}_5$=(-60,-20),$\boldsymbol{z}_6$=(-20,-20),$\boldsymbol{z}_9$=(-60,20),$\boldsymbol{z}_{10}$=(-20,20)		
True target	$\boldsymbol{u}_3$=(-44,14)		
Fake target	-	$\widehat{\boldsymbol{u}}_3$=(-76,14)	$\widehat{\boldsymbol{u}}'_3$=(-30,16)
Estimate target	(-43.62, 15.80)	(75.88, 15.42)	(-37.70, 14.88)
RMSE	1.84	31.61	6.37
Residual	1.58	0.77	10.78
Attack cost	-	50%	50%
4# topology			
4 sensors	$\boldsymbol{z}_6$=(-20,-20), $\boldsymbol{z}_7$=(20,-20),$\boldsymbol{z}_{10}$=(-20,20),$\boldsymbol{z}_{11}$=(20,20)		
True target	$\boldsymbol{u}_4$=(8,8)		
Fake target	-	$\widehat{\boldsymbol{u}}_4$=(-8,-8)	$\widehat{\boldsymbol{u}}'_4$=(10,-10)
Estimate target	(8.06, 9.92)	(-8.66, -7.66)	(4.16, -4.16)
RMSE	1.92	22.86	12.75
Residual	0.88	0.86	13.07
Attack cost	-	75%	75%

[1] *Note: Sensor in red color denote Byzantine node.*

[3] Y. Xu, J. Zhou, and P. Zhang, "RSS-based source localization when path-loss model parameters are unknown," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1055–1058, June 2014.

[4] J. Lee, Y. Kim, J. Lee, and S. Kim, "An efficient three-dimensional localization scheme using trilateration in Wireless Sensor Networks," *IEEE Commun. Lett.*, vol. 18, no. 9, pp. 1591–1594, Sep. 2014.

[5] K. Agrawal, A. Vempaty, H. Chen, and P. K. Varshney, "Target localization in Wireless Sensor Networks with quantized data in the Presence of Byzantine attacks," *The 45th Asilomar Conference on Signals, Systems and Computers,* 2011, pp. 1669–1673.

[6] V. S. S. Nadendla, Y. S. Han, and P. K. Varshney, "Distributed inference with M-ary quantized data in the presence of Byzantine attacks," *IEEE Trans. Signal Process.*, vol. 62, no. 10, pp. 2681–2695, Oct. 2014.

[7] J. Zhang, R. S. Blum, L. M. Kaplan, and X. Lu. "Functional forms of optimum spoofing attacks for vector parameter estimation in quantized Sensor Networks," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 705–720, Feb. 2017.

[8] A. J. Weiss and J. Picard, "Maximum likelihood positioning of network nodes using range measurements," *IET Signal Process.*, vol. 2, no. 4, pp. 394–404, Dec. 2008.

[9] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 13:1–13:33, May 2011.