Optimal Byzantine attack strategy for distributed localisation with *M*-ary quantised data

Huifang Chen✉, Lei Xie and Congqi Shen

The distributed localisation with *M*-ary quantised data at sensor nodes is investigated in the presence of Byzantines from the perspective of the attackers. The Byzantine nodes attack the network by transmitting falsified data to the fusion centre (FC) to deteriorate the performance of the distributed target location estimation, where the independent and probabilistic Byzantine attack model is considered. By making the determinant of Fisher information matrix be zero, the optimal Byzantine attack strategy, which makes the FC incapable of estimating target location, is found using the data at sensor nodes. Numerical results show that the security performance of the distributed localisation improves sharply as the number of quantisation bits increases. Moreover, the security performance also increases tremendously as the attack probability decreases. Hence, the Byzantine attacker faces a trade-off between the performance damage and the hazard to be identified.

Introduction: Distributed target localisation in sensor networks has been widely studied [1]. The distributed estimation framework consists of a number of spatially distributed sensor nodes which get observations about a target in the region of interest (ROI) and send processed data to a fusion centre (FC) where the target location is estimated.

The problem of the distributed target localisation in the presence of Byzantine attacks has gained attention in recent years [2, 3]. Here, we only focus on the data-falsification aspect of the Byzantine attack wherein the compromised sensor nodes of the network send false data to the FC in order to deteriorate the distributed estimation performance.

Vempaty *et al.* [2] addressed the distributed target localisation with binary quantised data in the presence of Byzantine attacks from both the Byzantine attack's and the network's perspectives. In [2], the optimal Byzantine attack, the Byzantine identification method and the attack mitigation scheme using non-identical quantisers at sensor nodes are presented. Nadendla *et al.* [3] extended the framework of Byzantine attack as the sensor nodes generate *M*-ary symbols, and when the Byzantine attack is ignorant about the quantisation thresholds used at sensor nodes. In [3], authors presented the optimal Byzantine attack, the distributed estimation scheme with resource-constrained Byzantine attacker and a reputation-tagging-based attack mitigation scheme. However, the distributed target localisation with *M*-ary quantised data in the presence of probabilistic Byzantine attacks is still not addressed.

In this Letter, we investigate the distributed target localisation with *M*-ary quantised data in the presence of probabilistic Byzantine attacks from the Byzantine attacker's perspective. We assume that the attacker does not have any knowledge about the quantisation thresholds at the sensor nodes. By making the determinant of Fisher information matrix be zero, we find the optimal Byzantine attack strategy for the distributed target location estimation with *M*-ary quantised data in the presence of Byzantines. This attack can make the FC incapable of estimating target location using the data transmitted by the sensor nodes. Finally, we analyse the impact of the number of quantisation bits and the attack probability on the security performance of the distributed target localisation.

System model: We consider a scenario where N sensor nodes are deployed in a wireless sensor network to estimate the location of a target at $\theta = [x_t, y_t]$, where x_t and y_t denote the coordinates of the target in the ROI within two-dimensional Cartesian plane.

It is assumed that the signal radiated from the target follows an isotropic power attenuation model [4]. That is, the signal amplitude at sensor i, a_i, is $(a_i)^2 = P_0(d_0/d_i)^n$, where P_0 is the power measured at a reference distance d_0, n is the path-loss exponent, d_i is the distance between the target and sensor i at (x_i, y_i) and $d_i = [(x_i - x_t)^2 + (y_i - y_t)^2]^{1/2}$. We assume that the target is not on a sensor, i.e. $d_i \neq 0$. Without loss of generality, $d_0 = 1$ and $n = 2$. The signal amplitude is corrupted by additive white Gaussian noise at each sensor. And the corrupted signal amplitude at sensor i is $s_i = a_i + n_i$, where n_i follows $N(0, \sigma_n^2)$.

The quantisation process is used to map the received signal at sensor i to one of the M symbols, $u_i \in \{0, 1, \ldots, M-1\}$, based on the maximum output entropy quantisation approach [5] and the set of quantisation thresholds $\boldsymbol{\eta}_i = [\eta_{i0} = -\infty,\ \eta_{i1}, \ldots,\ \eta_{iM} = +\infty]$ (In the following text, $\boldsymbol{\eta}_i^{\mathrm{H}}$ and $\boldsymbol{\eta}_i^{\mathrm{B}}$ denote the set of quantisation thresholds used by an honest node and a Byzantine node, respectively.). Owing to the Gaussian noise assumption, the probability that u_i takes a specific value m is $P(u_i = m|\theta) = Q(\eta_{im} - a_i/\sigma_n) - Q(\eta_{i(m+1)} - a_i/\sigma_n)$, where $Q(\cdot)$ is the complementary distribution function of the standard Gaussian distribution.

It is assumed that α fraction of the sensor nodes in the network are compromised. These compromised nodes transmit falsified data with a probability β to the FC in order to deteriorate the performance of the distributed target location estimation. The transmitted symbol by sensor i is v_i, and $v_i \in \{0, 1, \ldots, M-1\}$.

In this Letter, we assume that the communication channels between sensor nodes and the FC are perfect. Hence, FC receives the message, $\boldsymbol{v} = [v_1\ v_2\ \ldots\ v_N]$, and estimates the target location using $\boldsymbol{v}$. Note that the performance of the FC is determined by the mass function $P(\boldsymbol{v}|\theta)$.

Distributed target localisation with Byzantines: It is assumed that the Byzantine nodes attack the network independently. In other words, each Byzantine node attacks the network according to its own observation without any knowledge about other Byzantine nodes.

If sensor i is honest, $v_i = u_i$. Otherwise, Byzantine node i modifies $u_i = l\ (l \neq m)$ to $v_i = m$ with a probability βp_{lm}, and $v_i = u_i$ with a probability $(1 - \beta + \beta p_{mm})$. Since the FC is not aware of the type of the node, it is assumed that sensor i is compromised with a probability α. Therefore, the conditional distribution of v_i at the FC is

$$\begin{aligned} P(v_i = m|\theta) &= (1-\alpha)P(v_i = m|\theta,\ i = \text{Honest}) \\ &\quad + \alpha P(v_i = m|\theta,\ i = \text{Byzantine}) \\ &= \frac{\alpha\beta}{M-1} + (1-\alpha)\left[Q\left(\frac{\eta_{im}^{\mathrm{H}} - a_i}{\sigma_n}\right) - Q\left(\frac{\eta_{i(m+1)}^{\mathrm{H}} - a_i}{\sigma_n}\right)\right] \\ &\quad + \alpha\left(1 - \frac{M\beta}{M-1}\right)\left[Q\left(\frac{\eta_{im}^{\mathrm{B}} - a_i}{\sigma_n}\right) - Q\left(\frac{\eta_{i(m+1)}^{\mathrm{B}} - a_i}{\sigma_n}\right)\right] \end{aligned} \quad (1)$$

After collecting $\boldsymbol{v}$, the FC estimates the target location by using the maximum likelihood estimator as in [4]. That is

$$\hat{\theta} = \arg\max_{\theta} \ln P(\boldsymbol{v}|\theta) = \arg\max_{\theta} \sum_{i=1}^{N}\sum_{m=0}^{M-1} \delta(v_i - m)P(v_i = m|\theta) \quad (2)$$

where $\delta(\cdot)$ is the Kronecker delta function.

The posterior Cramer–Rao lower bound (PCRLB) and posterior Fisher information matrix (FIM) are two performance metrics to analyse the estimation performance. Let $\hat{\theta}(\boldsymbol{v})$ be an estimator of θ. The PCRLB can be given as the inverse of FIM, $E\left\{\left[\hat{\theta}(\boldsymbol{v}) - \theta\right]\left[\hat{\theta}(\boldsymbol{v}) - \theta\right]^{\mathrm{T}}\right\} \geq F^{-1}$, where $\boldsymbol{F}$ is the FIM. **Q1**

From the perspective of Byzantine attackers, they would want PCRLB to be large to have the maximum damage. If Byzantine nodes can make the CRLB approach infinity, the FC will be made incapable of estimating the target location. In this Letter, we focus on the Byzantine attack to 'blind' the FC completely.

Optimal attack strategy: The FIM and its elements are given as

$$\boldsymbol{F} = -E\left[\nabla_\theta \nabla_\theta^{\mathrm{T}} \ln P(\boldsymbol{v}|\theta)\right] = \begin{pmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{pmatrix} \quad (3)$$

$$F_{11} = \int p_0(\theta)\left(\sum_{i=1}^{N}\sum_{m=0}^{M-1} \frac{-1}{P(v_i = m|\theta)}\left[\frac{\partial P(v_i = m|\theta)}{\partial x_t}\right]^2\right) \mathrm{d}\theta \quad (4a)$$

$$F_{22} = \int p_0(\theta)\left(\sum_{i=1}^{N}\sum_{m=0}^{M-1} \frac{-1}{P(v_i = m|\theta)}\left[\frac{\partial P(v_i = m|\theta)}{\partial y_t}\right]^2\right) \mathrm{d}\theta \quad (4b)$$

$$\begin{aligned} F_{12} &= F_{21} \\ &= \int p_0(\theta)\left(\sum_{i=1}^{N}\sum_{m=0}^{M-1} \frac{-1}{P(v_i = m|\theta)} \frac{\partial P(v_i = m|\theta)}{\partial x_t} \frac{\partial P(v_i = m|\theta)}{\partial y_t}\right) \mathrm{d}\theta \end{aligned} \quad (4c)$$

$$\frac{\partial P(v_i=m|\theta)}{\partial x_t} = -\frac{(1-\alpha)a_i}{\sigma_n\sqrt{2\pi d_i^2}}(x_i-x_t) \times\left[\exp\left(-\frac{(\eta_{im}^{H}-a_i)^2}{2\sigma_n^2}\right)-\exp\left(-\frac{(\eta_{i(m+1)}^{H}-a_i)^2}{2\sigma_n^2}\right)\right] \times -\frac{\big(\alpha-(M\alpha\beta/M-1)\big)a_i}{\sigma_n\sqrt{2\pi d_i^2}}(x_i-x_t) \times\left[\exp\left(-\frac{(\eta_{im}^{B}-a_i)^2}{2\sigma_n^2}\right)-\exp\left(-\frac{(\eta_{i(m+1)}^{B}-a_i)^2}{2\sigma_n^2}\right)\right], \quad (4d)$$

$$\frac{\partial P(v_i=m|\theta)}{\partial y_t} = -\frac{(1-\alpha)a_i}{\sigma_n\sqrt{2\pi d_i^2}}(y_i-y_t) \times\left[\exp\left(-\frac{(\eta_{im}^{H}-a_i)^2}{2\sigma_n^2}\right)-\exp\left(-\frac{(\eta_{i(m+1)}^{H}-a_i)^2}{2\sigma_n^2}\right)\right] -\frac{\big(\alpha-(M\alpha\beta/M-1)\big)a_i}{\sigma_n\sqrt{2\pi d_i^2}}(y_i-y_t) \times\left[\exp\left(-\frac{(\eta_{im}^{B}-a_i)^2}{2\sigma_n^2}\right)-\exp\left(-\frac{(\eta_{i(m+1)}^{B}-a_i)^2}{2\sigma_n^2}\right)\right] \quad (4e)$$

where $p_0(\theta)$ is the prior distribution of the target location assumed by the FC.

Let α_{blind} denote the minimum fraction of Byzantine nodes which makes the FC incapable of estimating the target location using the data at sensor nodes. Since FIM is multi-dimensional, Byzantine nodes will try to make the determinant of FIM approach to zero. In other words, α_{blind} can be found by making $F_{11}F_{22}-F_{12}F_{21}=0$.

Substituting (4) into $F_{11}F_{22}-F_{12}F_{21}=0$, we can find $\alpha_{\text{blind}}=(M-1)/M\beta$.

As we know, designing the quantisation thresholds is an important challenge in the distributed target localisation with M-ary quantised data. It is reasonable that the same type of sensor nodes uses the same quantisation thresholds. That is, the honest nodes use $\boldsymbol{\eta}^{H}$, while the Byzantine nodes use $\boldsymbol{\eta}^{B}$. In [6], it was shown that the optimal strategy for the Byzantine and the honest nodes is to use $\boldsymbol{\eta}=\boldsymbol{\eta}^{H}=\boldsymbol{\eta}^{B}$ since the attacker has no knowledge about the quantisation thresholds.

Hence, the conditional distribution of v_i at the FC can also be presented as

$$P(v_i=m|\theta)=(1-\alpha\beta+\alpha\beta p_{mm}) + \sum_{l=0,l\neq m}^{M-1}\big[\alpha\beta p_{lm}-(1-\alpha\beta+\alpha\beta p_{mm})\big]P(v_i=l|\theta) \quad (5)$$

To completely blind the FC is equivalent to making $P(v_i=m|\theta)=1/M$ for all $m\in\{0,1,\ldots,M-1\}$. Substituting $\alpha_{\text{blind}}=(M-1)/M\beta$ into (5), we have $p_{mm}=0$ and $p_{lm}=1/(M-1)$ for all $m\in\{0,1,\ldots,M-1\}$ and $l\neq m$. The results are summarised as a theorem as follows.

Theorem 1: If the Byzantine attacker with the attack probability β has no knowledge of the quantisation thresholds used at each sensor node, the optimal Byzantine attack strategy for the distributed localisation with M-ary quantised data is given as

$$\alpha_{\text{blind}}=\min(1,(M-1/M\beta)), \quad p_{lm}=\begin{cases}1/(M-1) & \text{if } l\neq m\\ 0 & \text{if } l=m\end{cases} \quad (6)$$

Numerical results: Fig. 1 shows the impact of the number of bits needed to encode the M symbols, $\lceil\log_2 M\rceil$, and the attack probability, β, on the minimum fraction of Byzantine nodes, α_{blind}.

From Fig. 1, we observe that α_{blind} increases sharply as $\lceil\log_2 M\rceil$ increases. When $\beta=1$ and a 3 bit quantiser is used, the attacker needs to compromise at least 87.5% of the sensor nodes in the network to blind the FC. When $\beta=1$ and a 6 bit quantiser is used, the attacker needs to compromise at least 98.44% of the sensor nodes to blind the FC. Obviously, this security performance improvement is in the cost of the communication overhead. Hence, the network designer faces a trade-off between the security guarantee and the communication cost.

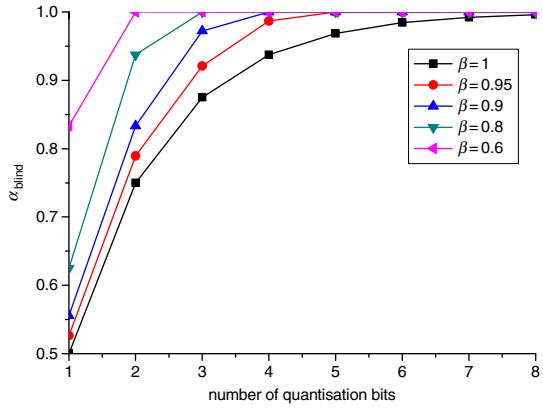

Fig. 1 *Impact of number of bits needed to encode M symbols and β on α_{blind}*

Moreover, we also observe that α_{blind} increases as β decreases. When a 2 bit quantiser is used and $\beta=1$, the attacker needs to compromise at least 75% of the sensor nodes to blind the FC. When a 2 bit quantiser is used and $\beta=0.8$, the attacker needs to compromise at least 93.75% of the sensor nodes to blind the FC. From the perspective of attackers, Byzantine nodes would attack the network with a large attack probability to cause the maximum damage. However, as β increases, the probability of the Byzantine attacker to be identified will increase. Hence, a trade-off between the performance damage and the risk to be identified should be settled by the Byzantine attacker.

Conclusion: In this Letter, under the assumption that the attacker has no knowledge about the quantisation thresholds at the sensor nodes, and using independent and probabilistic attack model, we find the optimal Byzantine attack strategy for the distributed target location estimation with M-ary quantised data in the presence of Byzantines. With this attack strategy, the FC is made incapable of estimating target location using the information sent by the sensor nodes. Numerical results show that the security performance of the distributed localisation improves sharply as the number of quantisation bits increases. Hence, the network designer faces a trade-off between the security guarantee and the communication cost. Moreover, as the attack probability increases, the security performance degrades tremendously. Hence, a trade-off between the performance damage and the hazard to be identified should be achieved by the Byzantine attacker.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (no. 61471318, 61071127), Science and Technology Department of Zhejiang Province (no. 2012C01036-1, no. 2011R10035).

Submitted: *21 June 2015*
doi: 10.1049/el.2015.2172
One or more of the Figures in this Letter are available in colour online.

Huifang Chen, Lei Xie and Congqi Shen (*Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, People's Republic of China*)

✉ E-mail: chenhf@zju.edu.cn

References

1 Brooks, R.R., Ramanathan, R., and Sayeed, A.M.: 'Distributed target classification and tracking in sensor networks', *Proc. IEEE*, 2003, **91**, (8), pp. 1163–1171, doi: 10.1109/JPROC.2003.814923

2 Vempaty, A., Ozdemir, O., Agrawal, K., *et al.*: 'Localization in wireless sensor networks: Byzantines and mitigation techniques', *IEEE Trans. Signal Process.*, 2013, **61**, (6), pp. 1495–1508, doi: 10.1109/TSP.2012.2236325

3 Nadendla, V., Han, Y.S., and Varshney, P.: 'Distributed inference with M-ary quantized data in the presence of Byzantine attacks', *IEEE Trans. Signal Process.*, 2014, **62**, (10), pp. 2681–2695, doi: 10.1109/TSP. 2014.2314072

4 Niu, R., and Varshney, P.: 'Target location estimation in sensor networks with quantized data', *IEEE Trans. Signal Process.*, 2006, **54**, (12), pp. 4519–4528, doi: 10.1109/TSP.2006.882082

5 Chaudhari, S., Lunden, J., Koivunen, V., *et al*.: 'Cooperative sensing with imperfect reporting channels: hard decisions or soft decisions?', *IEEE Trans. Signal Process.*, 2012, **60**, (1), pp. 18–28, doi: 10.1109/TSP.2011.2170978

6 Agrwal, K., Vempaty, A., Chen, H., *et al*.: 'Target localization in sensor network with quantized data in the presence of Byzantine attacks'. Asilomar Conf. Signals, Systems and Computers, Pacific Grove, CA, USA, November 2011, pp. 1669–1673, doi: 10.1109/ACSSC.2011.6190303

EL20152172

Author Queries

Huifang Chen, Lei Xie, Congqi Shen

Q1 IEE style for matrices and vectors is to use bold italics. Please check that we have identified all instances.