9

Decision-Making in Energy-Efficient Ordered Transmission-Based Networks Under Byzantine Attacks

Chen Quan[1] *and Pramod K. Varshney*[2]

[1] *Faculty of Electrical Engineering, Mathematics, and Computer Science, Delft University of Technology, Delft, Netherlands*
[2] *Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY, USA*

9.1 Introduction

Over the years, wireless communication systems have evolved into the most widely used framework for communication devices and networks. Many applications have benefited from wireless sensor networks (WSNs) such as military surveillance, autonomous driving systems and smart-homes. One important factor to consider when designing WSNs is the limited power supply. Reducing energy consumption due to radio communication is key to sustainability and longevity of WSNs since radio communication is the major component of WSNs that consumes large amounts of energy.

Radio communications' energy consumption is mainly determined by the amount of data transmitted throughout the entire network. Therefore, by reducing the amount of data transmitted and optimizing communication processes, energy-efficiency can be achieved. For example, it can be done through data compression, power-saving modes, and efficient routing algorithms. In the literature, some promising frameworks have been proposed for improving the energy efficiency of the WSNs such as censoring, ordered transmission and compressive sensing (e.g. [Baraniuk, 2007; Appadwedula et al., 2008; Blum and Sadler, 2008; Candès and Wakin, 2008]). Energy efficiency is achieved by either reducing the number of transmissions in the networks (e.g. censoring and ordered transmission) or compressing the data sent by the sensors (e.g. quantization and compressive sensing).

This chapter is concerned with the security aspects of one kind of promising energy-efficient framework mentioned earlier, namely ordered transmission. In ordered transmission-based (OT-based) schemes, energy efficiency is achieved

Wireless Sensor Networks in Smart Environments: Enabling Digitalization from Fundamentals to Advanced Solutions, First Edition. Edited by Domenico Ciuonzo and Pierluigi Salvo Rossi.

by omitting transmission of less informative data. The security threat we are particularly interested in is Byzantine attacks, which are one of the most significant security threats faced by WSNs. In Byzantine attacks, a fraction of the sensors within the network may be compromised and completely controlled by adversaries, while the fusion center (FC) is unaware of the behavioral identity of the malicious sensors. This can lead to the intentional transmission of corrupted data that degrades system performance. A number of studies have been conducted in the literature to design various defense mechanisms for mitigating the effect of Byzantine attacks on the overall system performance. However, energy-efficient OT-based frameworks make it more challenging to address security issues since only a portion of sensors' data is transmitted to the FC during each decision-making interval. Since FC does not receive data from all the sensors all the time, it cannot fully learn the behavior of all the sensors.

In this chapter, we conduct an investigation into the impact of Byzantine attacks on several energy-efficient OT-based schemes used in WSNs. The organization of this chapter is as follows. In Section 9.2, some existing threats from Byzantine attacks on conventional wireless sensor networks are briefly discussed, along with some possible defense mechanisms. Section 9.3 introduces the conventional OT-based (COT-based) scheme and investigates the impact of Byzantine attacks on this system. In Section 9.4, a communication-efficient ordered transmission-based (CEOT-based) scheme is presented, and an analysis of the effect of Byzantine attacks on the overall system is conducted. Section 9.5 compares the resilience of CEOT-based with COT-based systems. Finally, a summary of the chapter and some challenges related to the security of energy efficient OT-based schemes employed in WSNs are presented in Section 9.6.

9.2 Byzantine Attack Model

Byzantine attack is a type of attack that occurs at the physical layer. This type of attack can be traced back to the issue of Byzantine generals, first introduced by Pease et al. [1982], where traitors attempted to mislead other loyal generals by providing false information. In WSNs, this term specifically refers to the malicious behaviors that occur within WSNs when certain sensors are compromised and transmit false data within the network. There are different types of Byzantine attacks such as data modification attack, data omission attack, and delayed attack. Malicious nodes can selectively delay data (delayed attack), drop data (data omission attack), or alter data packets directly (data modification attack) to manipulate the network.

In the existing literature, there have been studies of distributed WSNs under Byzantine attacks (e.g. [Kailkhura et al., 2018; Vempaty et al., 2018; Quan et al., 2022b]). The interactions between Byzantines and the WSNs can be viewed as

games between attackers and the detection systems. Byzantines aim to undermine the integrity of data transmitted, thereby lowering the reliability of wireless sensor networks. Correspondingly, the FC can enhance the reliability of the network by identifying the Byzantines and making suitable use of information coming from Byzantines for mitigation purposes. Hence, strategic Byzantines attackers strive to maximize their attack gains while attempting to avoid detection by the defense system.

The level of effort required for an effective attack varies depending on the data fusion system architecture. In centralized fusion, the system can better evaluate the behavior of all the sensors so that the attacks can be mitigated, especially when the majority of nodes are honest and the FC is trustworthy. However, in decentralized fusion, each sensor can only communicate with its neighbors to gather additional information regarding the phenomenon of interest before making a decision. This decentralized approach makes the system more susceptible to attacks since false data can be stealthily incorporated into the decisions of neighboring nodes and diffused throughout the network.

9.2.1 Typical Attack Model in WSNs

There are several factors that can be used to classify Byzantine attacks in WSNs. One such factor is the availability of additional information besides the sensing results at the Byzantine nodes. If no extra information is available, the attacks are referred to as *independent attacks*, meaning that the Byzantine nodes can only rely on their own sensing capabilities. On the other hand, if the attacks involve the acquisition of extra information by the Byzantine nodes, such as the current sensing results of other malicious nodes, fusion rules, and defense strategies, they are referred to as *dependent attacks*. The exchange of information in dependent attacks allows malicious nodes to increase their accuracy in sensing and the success rate of their attacks, making their collusion more effective. One approach to defend against these types of attacks is to use statistical methods to detect and identify malicious nodes that are demonstrating anomalous behavior [Quan et al., 2022c]. Another factor is the manner in which the attacks are executed. If the attacks are launched with a certain probability, they are referred to as *probabilistic attacks*. Defense algorithms for these types of attacks usually identify attackers by analyzing the consistency of their attack behavior over time, such as reputation-based schemes (e.g. [Quan et al., 2022c]) and cluster-based schemes (e.g. [Chen and Wang, 2019]). Conversely, if the attacks are launched based on specific conditions, such as when their posterior probability of being a malicious node exceeds a certain threshold, they are referred to as *non-probabilistic attacks*. These attacks are much harder to model compared to probabilistic attacks and can be very difficult to defend against, as the Byzantine nodes are intentionally trying to appear normal while causing disruptions.

9.2.2 Existing Defense Schemes

There are a number of studies exploring various defense mechanisms in the literature aimed at mitigating the impact of Byzantine attacks on the overall system performance. They either directly identify and isolate Byzantine attackers or design the system parameters to mitigate the effects of attacks on the system. There are many promising methods for dealing with Byzantine attacks in networks, such as game-theoretic techniques [Liu et al., 2020], reputation-based methods [Nadendla et al., 2014; Quan et al., 2022c], and machine learning techniques [Yang et al., 2020]. Several consensus-based algorithms have been used in decentralized fusion to improve their robustness under attack. Efforts have been made to exclude nodes with significant deviations from consensus (e.g. [Liu et al., 2012]) and to design network parameters to mitigate the impact of data falsification attacks (e.g. [Kailkhura et al., 2017; Mustafa et al., 2021]).

The previously discussed works have made strides in improving the resilience of systems against Byzantine attacks, however, they still have limitations in detecting distributed attacks when a large number of sensor nodes are attacked. Some works, such as Hashlamoun et al. [2017, 2018] and Zhang et al. [2018], have successfully reduced the impact of Byzantine attacks on wireless sensor networks (WSNs) even when the majority of sensors are malicious. There are also some works that have used the idea of quickest change detection to detect the presence of anomalous measurements due to the malicious sensors in the networks. A model of quickest change detection problems was proposed to detect the presence of Byzantines. The malicious behavior of Byzantines is characterized by distributions before and after the change time (e.g. [Fellouris et al., 2017; Huang et al., 2021]). Aside from works that deal with performance analysis and robust design of networks with fixed sample sizes, there are also studies that deal with performance analysis and robust design of networks with unknown sample sizes, such as sequential hypothesis testing (e.g. [Wu et al., 2018; Li et al., 2021]).

In the literature, there appears to be a large body of literature on performance analysis and robust design of networks that utilize data from all the sensors to make final decisions under Byzantine attacks, while the literature on performance analysis and the robust design of energy-efficient networks with an unknown number of sensors still needs more effort on methods, such as censoring-based schemes, ordered transmission-based schemes, and sleep scheduling algorithms. The reduced number of sensors needed to reach a final decision appears to meet the increasing demand for low-energy consumption and long-lasting WSNs for a variety of applications. Compressed sensing is also an energy-efficient framework in which data sent by the sensors is compressed using quantization and compressed sensing. These energy-efficient frameworks are still under investigation in terms of their robustness and their robust design in the context of error-prone environments and under attacks. In the rest of this chapter, we will focus on one promising framework which is ordered transmission-based framework.

9.3 COT-Based System

The COT-based scheme was initially introduced by Blum and Sadler [2008]. In this scheme, the FC receives the log-likelihood ratios (LLRs) instead of raw data from only a subset of sensors. This approach has been utilized in a wide range of detection problems to enhance energy efficiency while preserving the detection performance of networks. For instance, Rawas et al. [2011] applied the OT-based framework to the detection of noncoherent signals. Hesham et al. [2012] applied the OT framework to sequential detection problems. Chen et al. [2020a, 2021] applied the OT framework to quickest change detection problem. Gupta et al. [2020] applied the OT framework to energy-harvesting systems. In addition, researchers have explored the use of the OT-based framework in various applications beyond detection tasks for transmission-saving purposes. For instance, Chen et al. [2020b] proposed a scheme that applies the idea of ordered transmission to the gradient descent approach. This new scheme guarantees the same order of convergence rate but with fewer transmissions. Yang et al. [2019] applied the concept of ordered transmission to the discretized estimation problem and demonstrated its ability to significantly decrease latency without deteriorating estimation accuracy. The above literature demonstrates the versatility and efficiency of the OT-based framework in various applications.

In this section, the COT-based system proposed by Blum and Sadler [2008] is discussed. An evaluation of such a system under Byzantine attacks, as well as a discussion of possible defense strategies, will be conducted.

9.3.1 System Model of COT-Based System

To elucidate the basic concepts of COT schemes, a binary hypothesis testing problem is considered. The observations at the N sensors in the system indicate either the presence ($\mathcal{H}_1$) or absence ($\mathcal{H}_0$) of a phenomenon of interest (PoI). In COT-based frameworks, only a subset of sensors needs to transmit their LLRs to the FC. Once the FC gathers sufficient observations for a final decision of desired quality, it broadcasts a stop signal to halt further sensor transmissions for the current decision interval. Sensors that have not yet transmitted reset their timers for the next decision interval upon receiving the stop signal.

For sensor $i \in \{1, 2, \dots, N\}$, its observation y_i is modeled as

$$y_i = \begin{cases} n_i, & \text{under } \mathcal{H}_0, \\ s + n_i, & \text{under } \mathcal{H}_1, \end{cases} \tag{9.1}$$

where n_i is the Gaussian noise with zero mean and variance σ^2 and s is the signal strength at each sensor. n_i and s are assumed to be independent, and all the observations are assumed to be independent and identically distributed (i.i.d) conditioned on the hypotheses. Each sensor $i \in \{1, 2, \dots, N\}$ computes its LLR,

which is given by $L_i = \log\left(\frac{f_{Y_i}(y_i|\mathcal{H}_1)}{f_{Y_i}(y_i|\mathcal{H}_0)}\right)$, and sends it to the FC. Here, $f_{Y_i}(y_i|\mathcal{H}_h)$ is the probability density function (PDF) of y_i given hypothesis $\mathcal{H}_h$, for $h = 0, 1$. The sensors send their LLRs to the FC according to the magnitude of their respective LLRs.[1] Based on this setup, the optimal decision rule is expressed as [Blum and Sadler, 2008]

$$\begin{cases} \sum_{i=1}^{k} L_{[i]} > \xi + (N-k)|L_{[k]}|, & \text{decide } \mathcal{H}_1, \\ \sum_{i=1}^{k} L_{[i]} < \xi - (N-k)|L_{[k]}|, & \text{decide } \mathcal{H}_0, \end{cases} \tag{9.2}$$

where $\xi = \log\left(\frac{\pi_0}{\pi_1}\right)$ is the threshold used by the FC. $L_{[i]}$ is the ith largest LLR and $\pi_h = P(\mathcal{H}_h)$ is the prior probabilities of hypothesis $\mathcal{H}_h$ for $h \in \{0, 1\}$.

9.3.1.1 Attack Model

One possible security threat for an OT-based framework in an error-prone environment is the order altering Byzantine attack (OA-Byzantine attack) [Quan et al., 2022a]. If attackers launch OA-Byzantine attacks, they can manipulate both the order and the data in the binary hypothesis testing problem. We assume that every sensor in the network has a probability α of being OA-Byzantine (B) and a probability $1 - \alpha$ of being honest (H). Additionally, OA-Byzantine sensors are assumed to possess perfect knowledge of the underlying true hypothesis.[2] If sensor $i \in \{1, 2, \ldots, N\}$ is OA-Byzantine, the falsified observation is expressed as

$$\tilde{y}_i = \begin{cases} s + n_i - D, & \text{under } \mathcal{H}_1, \\ n_i + D, & \text{under } \mathcal{H}_0, \end{cases} \tag{9.3}$$

where $D \in \mathbb{R}^+$ is the attack strength. The above attack strategy involves generating falsified observations from an altered distribution, achieved by shifting the mean of the original distribution, and it is commonly utilized and discussed in the literature [Zhang et al., 2014; Kailkhura et al., 2017]. If sensor i is honest, its observation y_i as given in Eq. (9.1).

9.3.2 Performance Analysis

The effect of OA-Byzantine sensors on the FC's performance can be evaluated from two perspectives: the system's detection performance and the average percentage of transmission savings.

---

1 Specifically, if $|L[1]| > |L[2]| > \cdots > |L_{[N]}|$, then the sensor with the largest absolute LLR value, $L_{[1]}$, transmits first, followed by $L_{[2]}$, and so forth.

2 Although difficult to achieve in practice, considering this scenario is still useful as it illustrates the worst-case impact of OA-Byzantines.

9.3.2.1 Detection Performance

The following lemma stated in Quan et al. [2022a] always holds for COT-based systems:

Lemma 9.1 Under the optimum Bayesian decision rule, the detection performance remains the same whether or not the system uses the COT-based scheme in the presence of OA-Byzantine sensors.

Lemma 9.1 establishes that the COT-based system can achieve equivalent detection performance compared to the unordered system, irrespective of the presence of OA-Byzantine sensors. Hence, to assess the detection performance of the COT-based system under OA-Byzantine attacks, we analyze the detection performance of the corresponding unordered distributed system. According to Quan et al. [2022a], the detection probability P_d^{FC} and false alarm probability P_f^{FC} at the FC of an OT-based system are given as

$$P_d^{FC} = \sum_{t=1}^{2^N} (1-\alpha)^{N-b_t} \alpha^{b_t} Q\left(\frac{\xi - (\mu_1)_{A_t}}{\sqrt{N\beta}}\right) \tag{9.4}$$

and

$$P_f^{FC} = \sum_{t=1}^{2^N} (1-\alpha)^{N-b_t} \alpha^{b_t} Q\left(\frac{\xi - (\mu_0)_{A_t}}{\sqrt{N\beta}}\right), \tag{9.5}$$

respectively, where $Q(.)$ is the tail distribution function of the standard normal distribution. Here, $\beta = \frac{s^2}{\sigma^2}$ and A_t is the tth subset of the set $\{1, \ldots, N\}$. The cardinality of set A_t is denoted by b_t, i.e. $b_t = |A_t|$, and $(\mu_h)_{A_t} = \mu_h|A_t| + \eta_h(N - |A_t|)$ for $h = 0, 1$, where $\mu_1 = -\mu_0 = \frac{s^2}{2\sigma^2}$, and $\eta_0 = -\eta_1 = \frac{s^2 - 2Ds}{2\sigma^2}$. The optimal attack strength D^* that attackers can adopt is given by [Quan et al., 2022a]

$$D^* = \frac{s}{2\alpha}, \tag{9.6}$$

which indicates the attack strategy to blind the FC, i.e. achieving a probability of error of 1/2 so that the FC does not derive any information from the observations.

9.3.2.2 Average Number of Transmissions Saved Under OA-Byzantine Attacks

In the COT-based system, the average number of transmissions (ANT) saved $\overline{N_t}$ under OA-Byzantine attacks can be calculated as

$$\overline{N_t} = \sum_{k=1}^{N} \pi_1 \Pr(\ell \geq k | \mathcal{H}_1) + \pi_0 \Pr(\ell \geq k | \mathcal{H}_0), \tag{9.7}$$

where ℓ is the minimum number of transmissions required to make a final decision without any loss of detection performance. Hence, to calculate $\overline{N_t}$, we need to

first calculate $\Pr(\ell \geq k|\mathcal{H}_h)$ for $h = 0, 1$. According to Quan et al. [2022a], we have

$$\Pr(\ell \geq k|\mathcal{H}_h) = E_{\mathbf{L}_{k-1}}\left[F_{|L_{k-1}|}(L_{k-1}|\mathcal{H}_h)^{N-k+1}\mathbf{1}_{\{\mathcal{R}\}}\frac{N!}{(N-k+1)!}\right], \tag{9.8}$$

where $F_{|L|}(l_i|\mathcal{H}_h) = \alpha\left(Q\left(\frac{-l_i-\eta_h}{\sqrt{\beta}}\right) - Q\left(\frac{l_i-\eta_h}{\sqrt{\beta}}\right)\right) + (1-\alpha)\left(Q\left(\frac{-l_i-\mu_h}{\sqrt{\beta}}\right) - Q\left(\frac{l_i-\mu_h}{\sqrt{\beta}}\right)\right)$ is the cumulative distribution function (CDF) of $|L_i|$ for $h = 0, 1$, and $\mathbf{1}_{\{\mathcal{R}\}}$ is an indicator function that is equal to 1 if $\mathbf{L}_{k-1} = \{L_1, L_2, \ldots, L_{k-1}\}$ lies in the region $\mathbf{1}_{\{\mathcal{R}\}}$ and equal to 0 otherwise. Here, $\mathcal{R}$ is a hyperplane with $k-1$ dimensions formed by the intersection of three hyperplanes, $\mathcal{R} = \mathcal{S} \cap \mathcal{L} \cap \mathcal{D}$, where $\mathcal{S} = \left\{\mathbf{L}_{k-1} : \sum_{i=1}^{k-1} L_i \leq \xi + (N-k+1)|L_{k-1}|\right\}$, $\mathcal{L} = \{\mathbf{L}_{k-1} : \sum_{i=1}^{k-1} L_i \geq \xi - (N-k+1)|L_{k-1}|\}$, and $\mathcal{D} = \left\{\mathbf{L}_{k-1} : |L_1| > |L_2| > \cdots > |L_{k-1}|\right\}$. The set $\mathcal{S}$ consists of $\mathbf{L}_{k-1}$ for which the FC is unable to determine hypothesis $\mathcal{H}_1$. Similarly, the set $\mathcal{L}$ consists of $\mathbf{L}_{k-1}$ for which the FC is unable to determine hypothesis $\mathcal{H}_0$. The set $\mathcal{D}$ consists of $\mathbf{L}_{k-1}$ such that $L_1, L_2, \ldots, L_{k-1}$ are ordered by magnitude.

For a given k, (9.8) can be numerically evaluated using the Monte Carlo approach. However, when the number of sensors N increases, the Monte Carlo approach requires a significant increase in the number of samples to accurately evaluate (9.8). It can become quite time-consuming to obtain the ANT saved under attack with a substantial number of sensors deployed in the network. While, for sufficiently large values of N, the upper bound (UB) (given in (9.9)) and lower bound (LB) (given in (9.10)) for the ANT saved can be obtained [Quan et al., 2022a].

$$\begin{aligned}\overline{N}_s^U = \sum_{k=1}^{N-1}\sum_{h=0}^{1}\pi_h\Bigg[&\Pr\left(|L_{[k]}| \leq \frac{q_U-\xi}{N-k}|\mathcal{H}_h\right) + \Pr\left(|L_{[k]}| \leq \frac{\xi-q_L}{N-k}|\mathcal{H}_h\right) \\ &- \Pr\left(|L_{[k]}| \leq \min\left(\frac{q_U-\xi}{N-k}, \frac{\xi-q_L}{N-k}\right)|\mathcal{H}_h\right)\Bigg]\end{aligned} \tag{9.9}$$

$$\overline{N}_s^L = \sum_{k=1}^{N-1}\sum_{h=0}^{1}\pi_h\left[\Pr\left(|L_{[k]}| < \frac{q_L-\xi}{(N-k)}|\mathcal{H}_h\right) + \Pr\left(|L_{[k]}| < \frac{\xi-q_U}{(N-k)}|\mathcal{H}_h\right)\right] \tag{9.10}$$

q_L and q_U in (9.9) and (9.10) are given as $q_L = -\left[\sum(a_i - k/N)^2 N\zeta_h^2\right]^{\frac{1}{2}} + k\delta_h$ and $q_U = \left[\sum(a_i - k/N)^2 N\zeta_h^2\right]^{\frac{1}{2}} + k\delta_h$, respectively. Here, the value of a_i for $i = 1, 2, \ldots, N$ changes with the value of k, that is $a_i = 1$ if $i \leq k$ and $a_i = 0$ if $i > k$. δ_h and ζ_h^2 are given as $\delta_h = \alpha\eta_h + (1-\alpha)\mu_h$ and $\zeta_h^2 = \beta + \alpha\eta_h^2 + (1-\alpha)\mu_h^2 - \delta_h^2$, respectively. Since the pdf of $f_{|L_{[k]}|}(l_{[k]}|\mathcal{H}_h)$ is

$$f_{|L_{[k]}|}(l_{[k]}|\mathcal{H}_h) = \begin{cases} f_{L_{[k]}}(l_{[k]}|\mathcal{H}_h) - f_{L_{[k]}}(-l_{[k]}|\mathcal{H}_h), & \text{if } l_{[k]} \geq 0, \\ 0, & \text{if } l_{[k]} < 0, \end{cases} \tag{9.11}$$

where $f_{L_{[k]}}(l_{[k]}|\mathcal{H}_h) = Nf_L(l_{[k]}|\mathcal{H}_h)\binom{N-1}{k-1}F_L(l_{[k]}|\mathcal{H}_h)^{(N-k)}(1-F_L(l_{[k]}|\mathcal{H}_h))^{(k-1)}$ and $f_L(l_i|\mathcal{H}_h) = \alpha\mathcal{N}(\eta_h,\beta)+(1-\alpha)\mathcal{N}(\mu_h,\beta)$, we are able to compute $\Pr\left(|L_{[k]}|<W|\mathcal{H}_h\right)$ for $W \in \left\{\frac{q_U-\xi}{N-k}, \frac{\xi-q_L}{N-k}, \min\left(\frac{q_U-\xi}{N-k}, \frac{\xi-q_L}{N-k}\right), \frac{q_L-\xi}{N-k}, \frac{\xi-q_U}{N-k}\right\}$ in (9.10) and (9.9), which is given as $\Pr\left(|L_{[k]}| < E|\mathcal{H}_h\right) = \int_{-E}^{E} f_{|L_{[k]}|}(l_{[k]}|\mathcal{H}_h)\mathrm{d}l_{[k]}$.

9.4 CEOT-Based System

In this section, we discuss another OT-based framework, called CEOT-based scheme. It was first proposed by Sriranga et al. [2018] where sensors transmit binary decisions instead of LLRs to the FC. The performance of the CEOT-based system under two types of Byzantine sensors was evaluated: decision-falsifying (DF-Byzantine) sensors, which perform pure decision-flipping, and OA-Byzantine sensors, which not only flip decisions but also change the transmission order.

To demonstrate the basic concepts of CEOT-based schemes, we again consider a binary hypothesis testing problem. Based on the local observations $\{y_i\}_{i=1}^N$, each sensor $i \in \{1,\dots,N\}$ makes a binary decision $v_i \in \{0,1\}$ regarding the true hypothesis using the LLR test $L_i \underset{v_i=0}{\overset{v_i=1}{\gtrless}} \log\left(\frac{\pi_0}{\pi_1}\right)$. Notably, sensor transmissions remain ordered according to the magnitude of their LLRs. Specifically, if the magnitudes of the LLRs are sorted as $|L_{[1]}| > |L_{[2]}| > \cdots > |L_{[N]}|$, the sensors send their local binary decisions to the FC in the order of $v_{[1]}, v_{[2]}, \dots, v_{[N]}$. Note that $v_{[k]}$ is the kth transmitted local decision which comes from the sensor with the kth largest LLR magnitude.

Thus, the optimal decision rule is given by [Sriranga et al., 2018]

$$\begin{cases} \sum_{i=1}^{k} v_{[i]} \geq T, & \text{decide } \mathcal{H}_1, \\ \sum_{i=1}^{k} v_{[i]} < T-(N-k), & \text{decide } \mathcal{H}_0, \end{cases} \tag{9.12}$$

which follows the T out of N counting rule.

9.4.1 Attack Model

Two possible types of security threats are considered in this framework: DF-Byzantine attacks and OA-Byzantine attacks. In the former, the Byzantine sensors perform pure decision flipping, while in the latter, the sensors not only alter decisions but also alter the sequence of the transmitted decisions. Each sensor is assumed to have a probability α of being a Byzantine sensor, and the Byzantines are assumed to possess perfect knowledge of the underlying true hypothesis.

- **DF-Byzantine attacks** For a DF-Byzantine sensor $i \in \{1, 2, \ldots, N\}$, we have

$$\begin{cases} v_i = 1 - x_i, & \text{with probability } \alpha p, \\ v_i = x_i, & \text{with probability } 1 - \alpha p, \end{cases} \tag{9.13}$$

  where x_i represents the actual local decision made by sensor i, v_i represents the local decision transmitted to the FC by sensor i and p is the probability that the sensor i flips its local decisions. If sensor i is honest, x_i is the same as v_i.
- **OA-Byzantine attack** Attackers falsify data in the same way as stated in Section 9.3.1.

9.4.2 CEOT-Based System with DF-Byzantines

The performance of the CEOT-based system with DF-Byzantine sensors is analyzed in terms of the detection performance and the number of transmissions saved in the network. Next, we will first discuss the detection performance under DF-Byzantine attacks, and subsequently evaluate and analyze the number of transmissions saved.

9.4.2.1 Detection Performance

The following lemma stated in Quan et al. [2023] always holds for the CEOT-based scheme under DF-Byzantine attacks:

Lemma 9.2 When the FC follows the Bayesian decision rule, the detection performance of systems with and without the use of the CEOT-based scheme is the same in the presence of data falsification attacks.

The lemma shows that the CEOT-based system can achieve equivalent detection performance under DF-Byzantine attacks as an unordered system. Thus, the detection performance of the CEOT-based system under DF-Byzantine attacks can be evaluated by analyzing the detection performance of the corresponding unordered system. The detection probability $P^{FC}_{d,CEOT}$ and the false alarm probability $P^{FC}_{f,CEOT}$ of the FC are respectively given below as (see [Quan et al., 2023])

$$P^{FC}_{d,CEOT} = \sum_{i=T+1}^{N} \binom{N}{i} Q\left(\frac{\xi - \mu_1}{\sqrt{\beta}}\right)^i \left[1 - Q\left(\frac{\xi - \mu_1}{\sqrt{\beta}}\right)\right]^{N-i} \tag{9.14}$$

and

$$P^{FC}_{f,CEOT} = \sum_{i=T+1}^{N} \binom{N}{i} Q\left(\frac{\xi - \mu_0}{\sqrt{\beta}}\right)^i \left[1 - Q\left(\frac{\xi - \mu_0}{\sqrt{\beta}}\right)\right]^{N-i}. \tag{9.15}$$

The optimal threshold T^* that can be utilized by the FC is given by

$$T^* = \left[\log\left(\frac{\pi_0}{\pi_1}\right) + N \log\left(\frac{1 - \tilde{\pi}_{1,0}}{1 - \tilde{\pi}_{1,1}}\right)\right] / \log\left(\frac{\tilde{\pi}_{1,1}(1 - \tilde{\pi}_{1,0})}{\tilde{\pi}_{1,0}(1 - \tilde{\pi}_{1,1})}\right). \tag{9.16}$$

9.4.2.2 Average Number of Transmissions Saved Under DF-Byzantine Attacks

Let $\ell_L = \arg\min_{1\le k\le N}\left\{\sum_{i=1}^{k} v_{[i]} \ge T\right\}$ and $\ell_U = \arg\min_{1\le k\le N}\left\{\sum_{i=1}^{k} v_{[i]} < T-(N-k)\right\}$ define the minimum number of transmissions required to decide $\mathcal{H}_1$ and $\mathcal{H}_0$, respectively, under DF-Byzantine attacks. Then, the ANT saved when the FC decides $\mathcal{H}_1$ is expressed as [Quan et al., 2023]

$$\overline{N}_{s,1}(\beta) = E(N-\ell_L) = \sum_{k=1}^{N}(N-k)P(\ell_L = k) \tag{9.17a}$$

$$\ge \sum_{k=1}^{\lceil T\rceil+\beta}(N-k)P(\ell_L = k) \tag{9.17b}$$

$$\ge (N-\lceil T\rceil-\beta)P(\ell_L \le \lceil T\rceil+\beta), \tag{9.17c}$$

where $\lceil T\rceil$ denotes the ceiling function, which rounds up T to the closest integer that is greater than or equal to T. In going from (9.17a) to (9.17b), some positive terms are dropped. To tighten the LB, an appropriate β should be selected since the difference between the actual ANT saved and its LB depends on the omitted terms. According to the definition of ℓ_L, $P(\ell_L \le \lceil T\rceil+\beta)$ in (9.17c) can be expressed as $P(\ell_L \le \lceil T\rceil+\beta) = \Pr\left(\sum_{k=1}^{\lceil T\rceil+\beta} v_{[k]} \ge T\right)$. Furthermore, (9.17c) can be lower bounded by $\overline{N}_{s,1}(\beta)^L = (N-\lceil T\rceil-\beta)P(\sum_{k=1}^{\lceil T\rceil+\beta} v_{[k]} \ge T|\sum_{i=1}^{\lceil T\rceil+\beta} v_{[i]} \ge T, \mathcal{H}_1)\pi_1$ due to the fact that any extra condition added will maintain or reduce the probability. When a sufficiently large signal is considered, $P\left(\sum_{k=1}^{\lceil T\rceil+\beta} v_{[k]} \ge T|\sum_{i=1}^{\lceil T\rceil+\beta} v_{[i]} \ge T, \mathcal{H}_1\right) = \sum_{i=0}^{\beta}\binom{\lceil T\rceil+\beta}{i}(\alpha p)^i(1-\alpha p)^{\lceil T\rceil+\beta-i}$ as given in Quan et al. [2023]. Similarly, for an adequately large signal, the ANT saved when the FC decides $\mathcal{H}_0$ is expressed as

$$\overline{N}_{s,2}(\beta) \ge (\lceil T\rceil-\beta)P\left(\sum_{k=1}^{N-\lceil T\rceil+\beta} v_{[k]} < \kappa|\sum_{i=1}^{N-\lceil T\rceil+\beta} v_{[i]} < T, \mathcal{H}_0\right)\pi_0 = \overline{N}_{s,2}(\beta)^L, \tag{9.18}$$

where $\lfloor T\rfloor$ denotes the floor function, which rounds down T to the nearest integer that is less than or equal to it. We can easily obtain $P(\sum_{k=1}^{N-\lceil T\rceil+\beta} v_{[k]} < \kappa|\sum_{i=1}^{N-\lceil T\rceil+\beta} v_{[i]} < T, \mathcal{H}_0) = \sum_{i=0}^{\lfloor T\rfloor-\lceil T\rceil+\beta}\binom{N-\lceil T\rceil+\beta}{i}(\alpha p)^i(1-\alpha p)^{N-\lceil T\rceil+\beta-i}$, where $\kappa = T-(\lceil T\rceil-\beta)$. Hence, a tight LB can be found by solving the following optimization problem:

$$\max_{\beta} \quad \overline{N}_{s,1}(\beta)^L + \overline{N}_{s,2}(\beta)^L \tag{9.19a}$$

$$\text{s.t.} \quad 0 \le \beta \le \min(N-\lceil T\rceil, \lceil T\rceil) \tag{9.19b}$$

$$\beta \in \mathbb{Z}, \tag{9.19c}$$

where $\mathbb{Z}$ denotes the set of integers. The constraint in (9.19b) arises because the upper index of the summations in the expressions for $\overline{N}_{s,1}(\beta)^L$ and $\overline{N}_{s,2}(\beta)^L$ must

be less than or equal to N. Even though the optimization problem in (9.19) is a non-convex optimization problem, the optimal solution can be obtained by analyzing the property of its objective function and the corresponding discussion can be found in Quan et al. [2023].

9.4.3 CEOT-Based System with OA-Byzantines

9.4.3.1 Detection Performance

Similar to the case of DF-Byzantine system, the CEOT-based system achieves the same detection performance as the corresponding unordered system under OA-Byzantine attacks. To evaluate the detection performance of the CEOT-based system under OA-Byzantine attacks, we can analyze the detection performance of the corresponding unordered distributed system. According to Quan et al. [2022a], the detection probability $P^{FC}_{d,CEOT}$ and the false alarm probability $P^{FC}_{f,CEOT}$ of a CEOT-based system are, respectively, given by $P^{FC}_{d,CEOT} = \sum_{i=T}^{N} \binom{N}{i} \pi_{1,1}^{i} \pi_{0,1}^{N-i}$ and $P^{FC}_{f,CEOT} = \sum_{i=T}^{N} \binom{N}{i} \pi_{1,0}^{i} \pi_{0,0}^{N-i}$, where $\pi_{1,h} = P(v_i = 1|\mathcal{H}_h) = \alpha Q\left(\frac{\xi - \eta_h}{\sqrt{\beta}}\right) + (1-\alpha) Q\left(\frac{\xi - \mu_h}{\sqrt{\beta}}\right)$.

9.4.3.2 Average Number of Transmissions Saved Under OA-Byzantine Attacks

Let $\overline{N}_{s,CEOT}$ denote the ANT saved in the CEOT-based scheme given as

$$\overline{N}_{s,CEOT} = E(N - \ell) = \sum_{k=1}^{N} (N-k) \Pr(\ell = k) = \sum_{k=1}^{N-1} \Pr(\ell \leq k). \tag{9.20}$$

Here, ℓ is again the minimum number of transmissions required to reach a final decision with desired accuracy. Since computing $\Pr(\ell \leq k)$ is intractable, we instead derive the UB and LB of $\overline{N}_{s,CEOT}$. Let $\Lambda = \sum_{i=1}^{N} v_i$ denote the global statistic of the distributed unordered system. Note that the final decisions of the system, whether ordered or unordered, remain the same under OA-Byzantine attacks. Consequently, $\Lambda < T$ indicates that there exists an ℓ such that $\sum_{i=1}^{\ell} v_{[i]} < T - (N - \ell)$, while $\Lambda \geq T$ indicates that there exists an ℓ such that $\sum_{i=1}^{\ell} v_{[i]} \geq T$. To determine the LB and UB of $\overline{N}_{s,CEOT}$, we consider the worst-case and best-case scenarios, respectively. They are shown as the following [Quan et al., 2022a]:

- **The worst case**: To determine the maximum ℓ required to reach a final decision based on a set of local decisions $\{v_i\}_{i=1}^{N}$. In this case, there are two possibilities that need to be considered: (i) $\Lambda < T$; (ii)$\Lambda \geq T$. Given $\Lambda < T$, the worst-case scenario would be if the local decisions are ordered in descending magnitude, i.e.

$$|r_{[1]}| \geq |r_{[2]}| \cdots \geq |r_{[N]}|, \tag{9.21}$$

where $r_{[k]} \in \{0,1\}$ is the kth largest local decision.[3] Similarly, given $\Lambda \geq T$, the worst-case scenario would occur if

$$|r_{(1)}| \leq |r_{(2)}| \cdots \leq |r_{(N)}|, \tag{9.22}$$

where $z_{(k)} \in \{0,1\}$ is the kth smallest local decision. Note that $r_{[k]}$ and $z_{(k)}$ are not the same as $v_{[k]}$. The values $v_{[1]}, v_{[2]}, \ldots, v_{[N]}$ are ordered by the magnitude of their corresponding LLRs, while $r_{[1]}, r_{[2]}, \ldots, r_{[N]}$ (or $r_{(1)}, \ldots, r_{(N)}$) are ordered by the magnitude of local decisions.

- **The best case**: To determine the minimum ℓ required to reach a final decision based on a set of local decisions $\{v_i\}_{i=1}^{N}$. We still need to consider two possibilities: (i) $\Lambda < T$; (ii)$\Lambda \geq T$. The best-case scenario when $\Lambda < T$ would occur if the magnitude of local decisions are ordered as (9.22). The best case given $\Lambda \geq T$ would occur if the magnitude of local decisions are ordered as (9.21).

  Hence, the UB $\overline{N}_{s,CEOT}^{U}$ and the LB $\overline{N}_{s,CEOT}^{L}$ are given by [Quan et al., 2022a]

$$\begin{aligned}\overline{N}_{s,CEOT}^{U} = \sum_{h=0}^{1}\sum_{k=1}^{N-1}\pi_h \Big[& P\left(\ell_0 \leq k | \Lambda \geq T, \mathcal{H}_h\right) P(\Lambda \geq T|\mathcal{H}_h) \\ & + P\left(\ell_1 \leq k | \Lambda < T, \mathcal{H}_h\right) P(\Lambda < T|\mathcal{H}_h)\Big], \end{aligned} \tag{9.23}$$

$$\begin{aligned}\overline{N}_{s,CEOT}^{L} = \sum_{h=0}^{1}\sum_{k=1}^{N-1}\pi_h \Big[& P\left(\ell_1 \leq k | \Lambda \geq T, \mathcal{H}_h\right) P(\Lambda \geq T|\mathcal{H}_h) \\ & + P\left(\ell_0 \leq k | \Lambda < T, \mathcal{H}_h\right) P(\Lambda < T|\mathcal{H}_h)\Big], \end{aligned} \tag{9.24}$$

where $P(\Lambda \geq T|\mathcal{H}_h) = \sum_{i=T}^{N} \binom{N}{i} \pi_{1,h}^{i} \pi_{0,h}^{N-i}$, $P(\Lambda < T|\mathcal{H}_h) = 1 - P(\Lambda \geq T|\mathcal{H}_h)$, and

$$P\left(\ell_0 \leq k | \Lambda \geq T, \mathcal{H}_h\right) = \sum_{i=0}^{N-T} \binom{N}{i} \pi_{0,h}^{i} \pi_{1,h}^{N-i}, \tag{9.25}$$

$$P\left(\ell_1 \leq k | \Lambda \geq T, \mathcal{H}_h\right) = \sum_{i=0}^{\min(N-T,k-T)} \binom{N}{i} \pi_{0,h}^{i} \pi_{1,h}^{N-i}, \tag{9.26}$$

when $k \geq T$, and

$$P\left(\ell_1 \leq k | \Lambda < T, \mathcal{H}_h\right) = \sum_{i=0}^{T-1} \binom{N}{i} \pi_{1,h}^{i} \pi_{0,h}^{N-i}, \tag{9.27}$$

$$P\left(\ell_0 \leq k | \Lambda < T, \mathcal{H}_h\right) = \sum_{i=0}^{\min(T-1,k-(N-T+1))} \binom{N}{i} \pi_{1,h}^{i} \pi_{0,h}^{N-i}, \tag{9.28}$$

3 $\Lambda < T$ implies that the total number of "1"s is less than T.

when $k > N - T$. Here, ℓ_0 and ℓ_1 represent the minimum number of transmissions required to reach a final decision for local decisions ordered in descending and ascending order, respectively.

9.5 Comparison of COT-Based and CEOT-Based Systems Under Attack

In this section, we compare the performance of COT-based and CEOT-based systems under OA-Byzantine and DF-Byzantine attacks. Some simulation results regarding the performance of the OT-based systems under attacks are presented below.

9.5.1 Effect of OA-Byzantine Attacks on the COT-Based and CEOT-Based Systems

Figure 9.1 demonstrates that, for the same attack parameters, the CEOT-based system demonstrates greater resilience to OA-Byzantine attacks than the COT-based system with respect to error probabilities. It shows that the quantization procedure in OT-based frameworks improves the robustness of OT-based frameworks. Figure 9.2 displays the nature of the average percentage of transmission savings with respect to the attack parameter D. Initially, the average percentage of transmission savings decreases as D increases. However, with further increases in D, the FC begins to make more erroneous decisions, resulting in a decrease in the number of transmissions needed to reach a final decision and an increase in savings. We can observe the existence of a minimum average percentage of transmission savings, which corresponds to the optimal attack strength D^* obtained from (9.6). The LB obtained from (9.10) and the UB obtained from (9.9) are also shown in Figure 9.2, and they track the changes in the actual saved ANT. The LB performs better in tracking changes compared to the UB, allowing us to infer the optimal attack strategy for the attacker, i.e. the value of D that the attacker will use to cause the most damage to the system. The UB, on the other hand, offers insights into the maximum number of transmissions saved on average in the network and alerts us to the presence of outliers.[4] These trends give us an insight into how to improve the system's robustness. Figure 9.3 shows that OA-Byzantine sensors can have less impact on the final decision-making in the CEOT-based system. As D increases sufficiently, Byzantine sensors are most likely to provide the first several local decisions received by the FC. This scenario represents the worst-case performance of the system. As D continues to increase, the influence of Byzantine sensors on the number of transmissions saved in the network does not increase further, due to

4 For example, if the ANT saved exceeds the maximum value of the UB, it indicates potential outliers where data significantly deviates from the actual, suggesting attackers are employing an excessively large value of D.

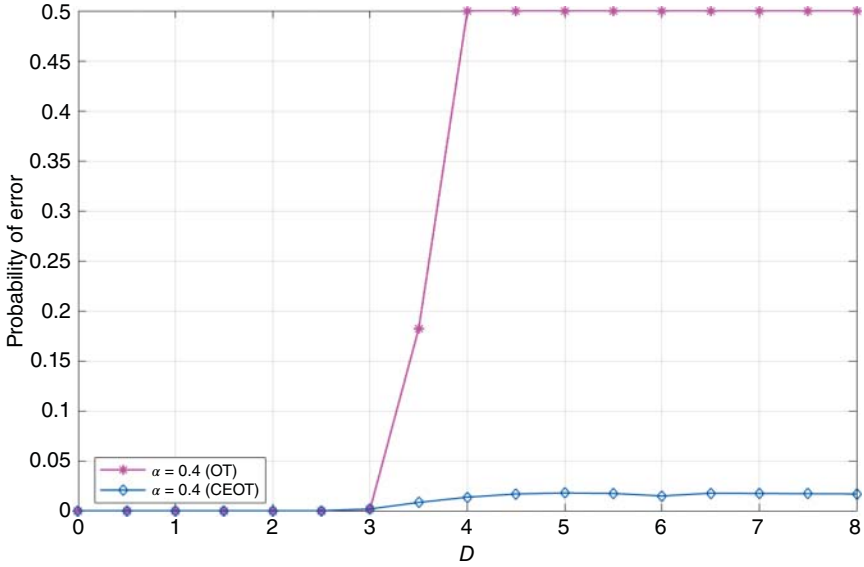

Figure 9.1 P_e as a function of D in the COT-based system and the CEOT-based system when $N = 300$, $\sigma^2 = 1$, $s = 3$ and $\pi_1 = \pi_0 = 0.5$. Source: Adapted from Quan et al. [2022a]. Please see the online version for the colored version of the figure.

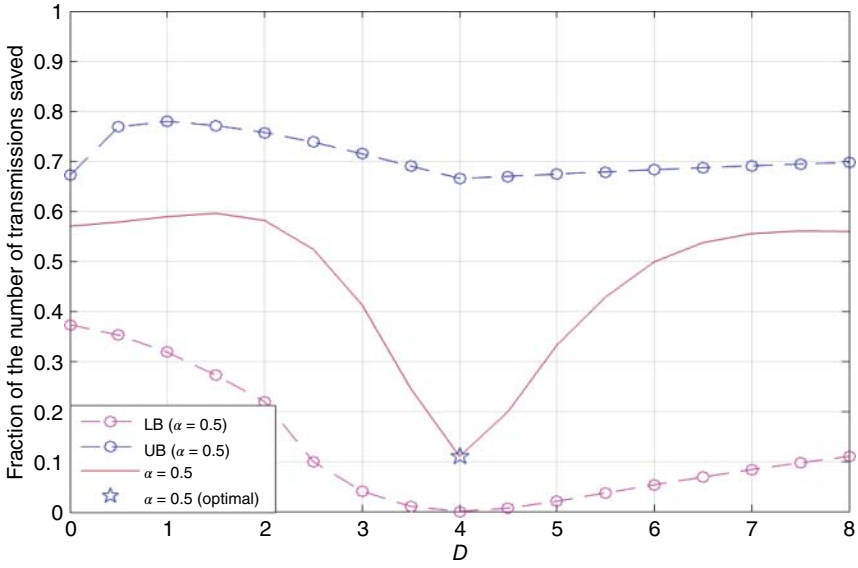

Figure 9.2 UB and LB for $\overline{N_s}/N$ as a function of D when $s = 4$, $\alpha = 0.5$, $N = 300$, $\sigma^2 = 1$ and $\pi_1 = \pi_0 = 0.5$ in the COT-based system. Source: Adapted from Quan et al. [2022a]. Please see the online version for the colored version of the figure.

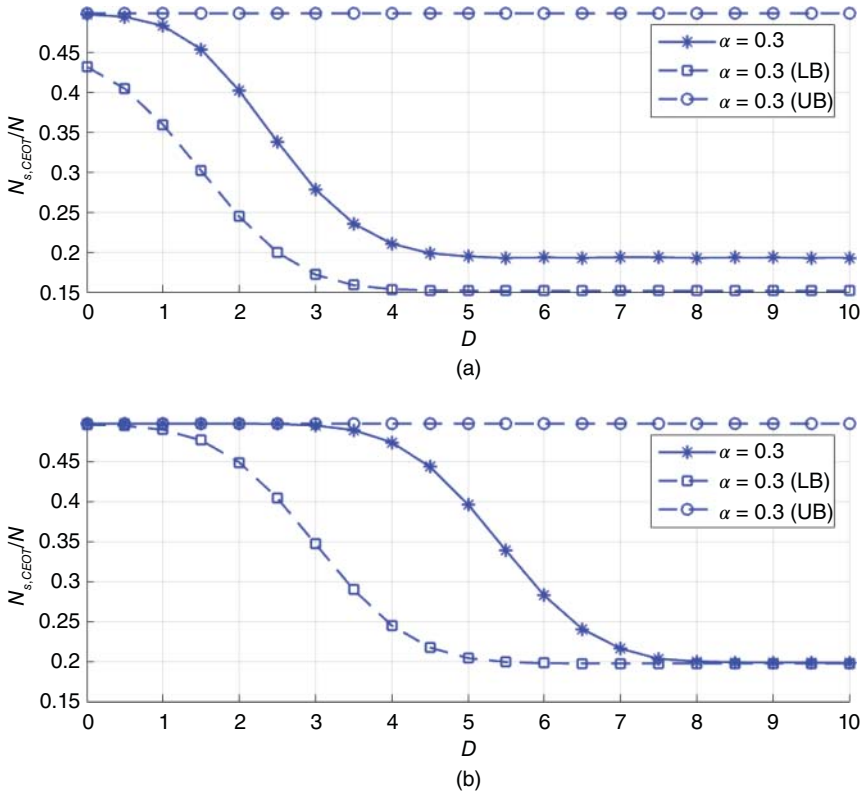

Figure 9.3 Benchmarking upper and lower bounds for $\overline{N}_{s,CEOT}/N$ as a function of D given $N = 300$ in the CEOT-based system (a) when $s = 3$; (b) when $s = 6$. Source: Adapted from Quan et al. [2022a]. Please see the online version for the colored version of the figure.

the quantization of LLRs, thereby mitigating their effects on the system. By comparing Figure 9.3a,b, we can also observe that the LB obtained in (9.24) becomes tighter as the signal strength s increases.

9.5.2 Effect of DF-Byzantine Attacks on the CEOT-Based System

Figure 9.4 shows that the optimal threshold T^* obtained from (9.16) results in the lowest possible error probability for the system.[5] Additionally, it can be

5 The threshold closest to the optimal threshold T^* is 49.5 in Figure 9.4 when $\pi_1 = 0.5$ and $\pi_1 = 0.3$.

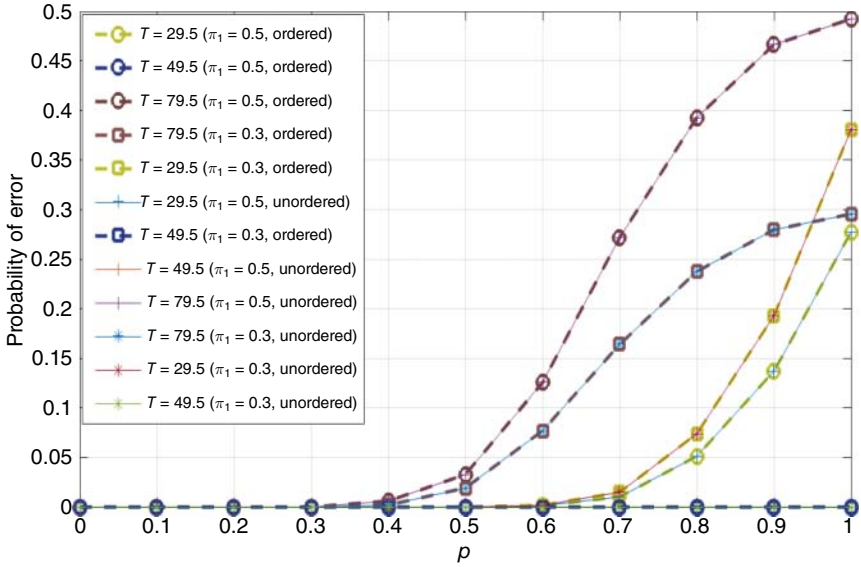

Figure 9.4 P_e as a function of p with different values of T for the CEOT-based system for $\pi_1 = 0.3$, $\pi_1 = 0.5$ and $N = 100$. Source: Adapted from Quan et al. [2023]. Please see the online version for the colored version of the figure.

observed that both the CEOT-based and unordered systems exhibit identical error probabilities for the given parameter values. This finding aligns with Lemma 9.2. In Figure 9.5, we can observe that a relatively tight UB is obtained compared with the UB obtained in the past work [Sriranga et al., 2018] for the average fraction of the number of transmissions required in the CEOT-based system. The effect of different values of prior probability and T on the performance of the CEOT-based system is shown in Figure 9.6. From Figure 9.6, it is evident that as T approaches T^* (approximately $N/2$), the system tends to require the maximum number of transmissions in the network when both hypotheses have prior probabilities of 0.5. However, variations in the prior probabilities can influence the optimal T that minimizes transmissions. A smaller T increases the transmissions needed for deciding $\mathcal{H}_0$ but reduces those for deciding $\mathcal{H}_1$. With a lower $\pi_1 < 0.5$, the likelihood of the FC deciding $\mathcal{H}_0$ increases. Consequently, a system using $T = 29.5$ requires more transmissions compared to one using $T = 49.5$, given $\pi_1 = 0.3$. Thus, the ANT needed is related to the prior probabilities of hypotheses in the system. According to Figures 9.4 and 9.6, it's possible to save transmissions while ensuring the quality of decisions by designing an appropriate threshold at the FC.

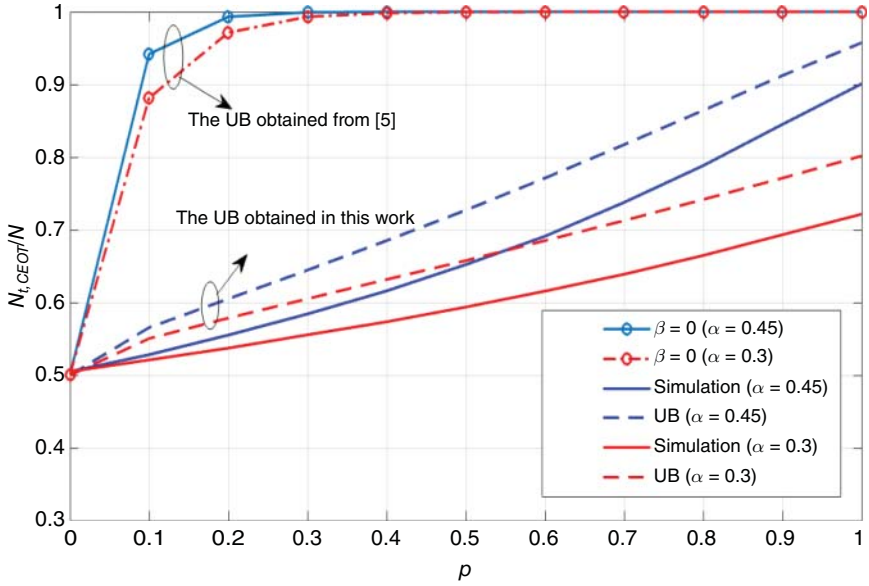

Figure 9.5 UBs for the fraction of the number of transmissions required $N_{t,CEOT}/N$ as a function of p with different values of α when $\pi_1 = 0.5$ and $N = 100$. Source: Quan et al. [2023]/IEEE. Please see the online version for the colored version of the figure.

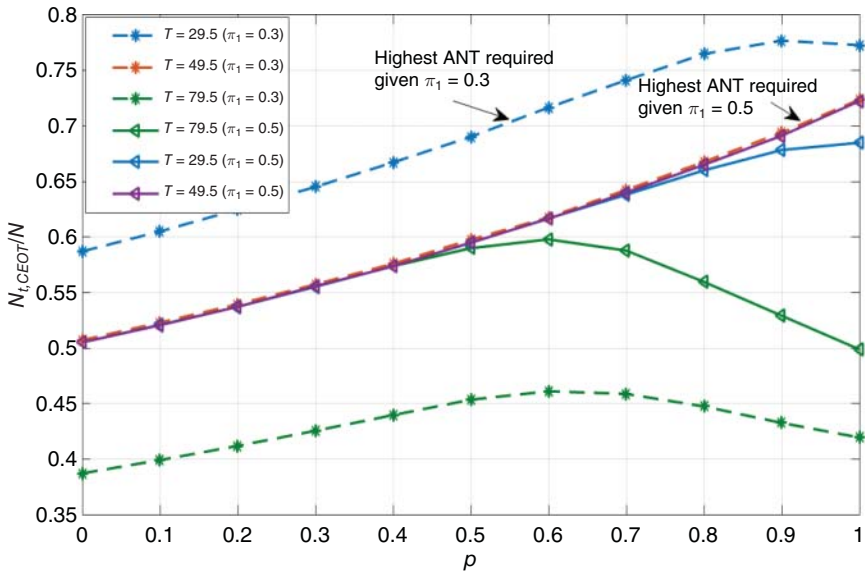

Figure 9.6 $N_{t,CEOT}/N$ as a function of p with different values of T when $\alpha = 0.3$, $\pi_1 = 0.3, 0.5$ and $N = 100$. Source: Adapted from Quan et al. [2023]. Please see the online version for the colored version of the figure.

9.5.3 Discussion

In this section, we presented simulation results illustrating the impact of OA-Byzantine attacks on both the COT-based and CEOT-based systems, as well as the effect of DF-Byzantine attacks specifically on the performance of the CEOT-based system. These performance comparisons provide valuable insights into the design of robust OT-based systems. For example, CEOT-based systems exhibit greater resilience to both OA-Byzantine and DF-Byzantine attacks compared to COT-based systems. By designing appropriate thresholds, CEOT-based systems can minimize the impact of both types of attacks on system performance. When implementing an OT-based system to optimize network transmissions, careful consideration of these factors is essential.

9.6 Conclusion

This chapter discussed several energy-efficient OT-based schemes for distributed detection in the presence of Byzantine attacks. It has been assumed in the past that OT-based framework operates in an attack-free environment. The designs for optimal decision fusion rules at the FC were discussed, and they were found to be highly effective under this assumption. However, some of the assumptions made in those works may be violated in the presence of attacks. In this chapter, the effect of Byzantine attacks on the performance of the COT-based system and the CEOT-based system were investigated in Sections 9.3 and 9.4. Moreover, a comparison of the resilience of CEOT-based and COT-based systems was made in Section 9.5, shedding light on how to employ OT-based frameworks in an attack-prone environment. Some possible countermeasures to mitigate the impact of Byzantines on OT-based systems were also discussed.

There are many open and challenging problems remain and require further research. For instance, analyzing the performance of the OT-based schemes with non-i.i.d. assumption under attacks is a very difficult problem. Designing robust OT-based schemes in distributed detection is also challenging since a fraction of multiple sensor data information is lost. Additionally, balancing energy efficiency and security in distributed systems is an open question. There are also some other promising energy-efficient schemes proposed in the literature (e.g. OT-based energy harvesting scheme [Gupta et al., 2020], censoring-based scheme [Gu et al., 2020]) by not receiving data from all the sensors all the time, which makes it difficult for the traditional intrusion detection systems to track the identity of each sensor in the networks. Therefore, further work on robust and energy-efficient schemes will be valuable.

Bibliography

S. Appadwedula, V. V. Veeravalli, and D. L. Jones. Decentralized detection with censoring sensors. *IEEE Transactions on Signal Processing*, 56(4):1362–1373, 2008.

R. G. Baraniuk. Compressive sensing [lecture notes]. *IEEE Signal Processing Magazine*, 24(4):118–121, 2007.

R. S. Blum and B. M. Sadler. Energy efficient signal detection in sensor networks using ordered transmissions. *IEEE Transactions on Signal Processing*, 56(7):3229–3235, 2008.

E. J. Candès and M. B. Wakin. An introduction to compressive sampling. *IEEE Signal Processing Magazine*, 25(2):21–30, 2008.

W.-N. Chen and I.-H. Wang. Anonymous heterogeneous distributed detection: Optimal decision rules, error exponents, and the price of anonymity. *IEEE Transactions on Information Theory*, 65(11):7390–7406, 2019.

Y. Chen, R. S. Blum, and B. M. Sadler. Optimal quickest change detection in sensor networks using ordered transmissions. In *2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 1–5. IEEE, 2020a.

Y. Chen, B. M. Sadler, and R. S. Blum. Ordered gradient approach for communication-efficient distributed learning. In *2020 IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 1–5. IEEE, 2020b.

Y. Chen, R. S. Blum, and B. M. Sadler. Ordering for communication-efficient quickest change detection in a decomposable graphical model. *IEEE Transactions on Signal Processing*, 69:4710–4723, 2021.

G. Fellouris, E. Bayraktar, and L. Lai. Efficient Byzantine sequential change detection. *IEEE Transactions on Information Theory*, 64(5):3346–3360, 2017.

Y. Gu, Y. Jiao, X. Xu, and Q. Yu. Request–response and censoring-based energy-efficient decentralized change-point detection with IoT applications. *IEEE Internet of Things Journal*, 8(8):6771–6788, 2020.

S. S. Gupta, S. K. Pallapothu, and N. B. Mehta. Ordered transmissions for energy-efficient detection in energy harvesting wireless sensor networks. *IEEE Transactions on Communications*, 68(4):2525–2537, 2020.

W. Hashlamoun, S. Brahma, and P. K. Varshney. Mitigation of Byzantine attacks on distributed detection systems using audit bits. *IEEE Transactions on Signal and Information Processing Over Networks*, 4(1):18–32, 2017.

W. Hashlamoun, S. Brahma, and P. K. Varshney. Audit bit based distributed Bayesian detection in the presence of Byzantines. *IEEE Transactions on Signal and Information Processing Over Networks*, 4(4):643–655, 2018.

L. Hesham, A. Sultan, M. Nafie, and F. Digham. Distributed spectrum sensing with sequential ordered transmissions to a cognitive fusion center. *IEEE Transactions on Signal Processing*, 60(5):2524–2538, 2012.

Y.-C. Huang, Y.-J. Huang, and S.-C. Lin. Asymptotic optimality in Byzantine distributed quickest change detection. *IEEE Transactions on Information Theory*, 67(9):5942–5962, 2021.

B. Kailkhura, S. Brahma, and P. K. Varshney. Data falsification attacks on consensus-based detection systems. *IEEE Transactions on Signal and Information Processing Over Networks*, 3(1):145–158, 2017. doi: 10.1109/TSIPN.2016.2607119.

B. Kailkhura, A. Vempaty, and P. K. Varshney. Collaborative spectrum sensing in the presence of Byzantine attacks. In P. Djuric and C. Richard (Eds.), *Cooperative and Graph Signal Processing*, pages 505–522. Elsevier, 2018.

Z. Li, Y. Mo, and F. Hao. Distributed sequential hypothesis testing with Byzantine sensors. *IEEE Transactions on Signal Processing*, 69:3044–3058, 2021.

S. Liu, H. Zhu, S. Li, X. Li, C. Chen, and X. Guan. An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum sensing. In *2012 IEEE Global Communications Conference (GLOBECOM)*, pages 603–608. IEEE, 2012.

X. Liu, T. J. Lim, and J. Huang. Optimal Byzantine attacker identification based on game theory in network coding enabled wireless ad hoc networks. *IEEE Transactions on Information Forensics and Security*, 15:2570–2583, 2020. doi: 10.1109/TIFS.2020.2972129.

A. Mustafa, M. N. U. Islam, and S. Ahmed. Dynamic spectrum sensing under crash and Byzantine failure environments for distributed convergence in cognitive radio networks. *IEEE Access*, 9:23153–23167, 2021.

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 Transactions on Signal Processing*, 62(10):2681–2695, 2014. doi: 10.1109/TSP.2014.2314072.

M. Pease, R. Shostak, and L. Lamport. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, 1982.

C. Quan, S. Bulusu, B. Geng, and P. K. Varshney. Ordered transmission-based detection in distributed networks in the presence of Byzantines. *arXiv preprint arXiv:2201.08737*, 2022a.

C. Quan, B. Geng, Y. Han, and P. K. Varshney. Enhanced audit bit based distributed Bayesian detection in the presence of strategic attacks. *IEEE Transactions on Signal and Information Processing Over Networks*, 8:49–62, 2022b.

C. Quan, Y. S. Han, B. Geng, and P. K. Varshney. Reputation and audit bit based distributed detection in the presence of Byzantines. In *2022 56th Asilomar Conference on Signals, Systems, and Computers*, pages 548–552, 2022c. doi: 10.1109/IEEECONF56349.2022.10051853.

C. Quan, N. Sriranga, H. Yang, Y. S. Han, B. Geng, and P. K. Varshney. Efficient ordered-transmission based distributed detection under data falsification attacks. *IEEE Signal Processing Letters*, 30:145–149, 2023. doi: 10.1109/LSP.2023.3244748.

Z. N. Rawas, Q. He, and R. S. Blum. Energy-efficient noncoherent signal detection for networked sensors using ordered transmissions. In *2011 45th Annual Conference on Information Sciences and Systems*, pages 1–5. IEEE, 2011.

N. Sriranga, K. G. Nagananda, R. S. Blum, A. Saucan, and P. K. Varshney. Energy-efficient decision fusion for distributed detection in wireless sensor networks. In *2018 21st International Conference on Information Fusion (FUSION)*, pages 1541–1547. IEEE, 2018.

A. Vempaty, B. Kailkhura, and P. K. Varshney. *Secure Networked Inference with Unreliable Data Sources*. Springer, 2018.

J. Wu, T. Song, Y. Yu, C. Wang, and J. Hu. Sequential cooperative spectrum sensing in the presence of dynamic Byzantine attack for mobile networks. *PLoS One*, 13(7):e0199546, 2018.

L. Yang, H. Zhu, Z. Zhu, X. Luo, and H. Qian. Distributed ordering transmissions for latency-sensitive estimation in wireless sensor networks. In *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*, pages 1–5, 2019. doi: 10.1109/VTCFall.2019.8891536.

Z. Yang, A. Gang, and W. U. Bajwa. Adversary-resilient distributed and decentralized statistical inference and machine learning: An overview of recent advances under the Byzantine threat model. *IEEE Signal Processing Magazine*, 37(3):146–159, 2020.

L. Zhang, Q. Wu, G. Ding, S. Feng, and J. Wang. Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing. *EURASIP Journal on Advances in Signal Processing*, 2014(1):1–9, 2014.

L. Zhang, G. Nie, G. Ding, Q. Wu, Z. Zhang, and Z. Han. Byzantine attacker identification in collaborative spectrum sensing: A robust defense framework. *IEEE Transactions on Mobile Computing*, 18(9):1992–2004, 2018.