Chapter 7
Moving Target Defense for Attack Mitigation in Multi-Vehicle Systems

Jairo Giraldo and Alvaro A. Cardenas

Abstract Cyber-Physical Systems (CPS) have traditionally been considered more static with more regular communication patterns when compared to classical information technology networks. Because the structure of most CPS remains unchanged during long periods of times, they become vulnerable to adversaries with the precise knowledge of the system, and who can tailor their attacks based on their knowledge about the system dynamics, communications, and control.

Moving Target Defense (MTD) has emerged as a key strategy to add uncertainty about the state and execution of a system in order to prevent attackers from having predictable effects with their attacks. In the last few years MTD has been used in different CPS scenarios by adding uncertainties into the physical characteristics of the system. Most of these applications are used to detect attacks, or to make difficult for attackers to gather information. In this chapter, we propose an MTD strategy for multi-vehicle systems that can be used to mitigate the impact caused by cyber-attacks. We characterize the trade-off between impact mitigation and performance degradation, and illustrate the viability of our approach in two applications, (1) vehicular platooning, and (2) UAV formation. Finally, we extend our results to a more general control systems framework, and we introduce different types of MTD mechanisms, i.e., at the controller level and at sensors.

J. Giraldo
Erik Jonsson School of Engineering, University of Texas at Dallas, Richardson, TX, USA
e-mail: jairo.giraldo@utdallas.edu

A. A. Cardenas (✉)
Erik Jonsson School of Engineering, University of Texas at Dallas, Richardson, TX, USA

Baskin School of Engineering, University of California, Santa Cruz, Santa Cruz, CA, USA
e-mail: alvaro.cardenas@ucsc.edu

C. Wang and Z. Lu (eds.), *Proactive and Dynamic Network Defense*, Advances in Information Security 74, https://doi.org/10.1007/978-3-030-10597-6_7

7.1 Introduction

Moving target defense (MTD) has been proposed as a way to make difficult the reliable exploitation of a system by attackers because it makes the attack surface dynamic [5]. For instance Dunlop et al. [3] proposed MT6D, an MTD mechanism for IPv6 which maintains user privacy and protects against targeted network attacks by repeatedly rotating the addresses of both the sender and receiver. Similarly, Wang et al. [22] introduced MOTAG, a strategy that defends against Internet DDoS attacks, by employing a layer of secret random proxy nodes to relay communications between clients and the protected application servers.

Most applications of MTD have been used for network protection and to secure applications. However, in the last couple of years the use of MTD techniques has been extended to protect cyber-physical systems. Several authors have used MTD approaches for state estimation in the smart grids [2, 16, 20], where the main idea consists on changing the physical topology of the power grid in order to reveal false data injection attacks. Weerakkody and Sinopoli [23] proposed the addition of an external system unknown to the attacker that uses additional sensor readings to obtain an estimate, making it harder for an adversary to design stealthy attacks. A similar approach was introduced by Valente and Cárdenas [21], where external visual challenges (e.g., a screen with extra information) are used to verify the authenticity of video footage. Closer to our work, Pang et al. [12] considered DDoS attacks that can shut down control commands; to prevent this attack, they propose the use of multiple distributed controllers so when a control command is not received, another controller is selected. On the other hand, Kanellopoulos and Vamvoudakis [6] propose a proactive MTD mechanism that consists on randomly switching among multiple controllers to increase the unpredictability of the control system. The switching probabilities are selected in order to maximize the entropy produced by the switching strategy while ensuring minimum controller cost. One of our approaches is similar, but we focus on minimizing the impact of the attack instead of the entropy. However, in our formulation it is possible to include the entropy maximization as an additional objective.

In this chapter we show how MTD can be used not only to increase the cost and difficulty of designing cyber-attacks, but also to mitigate the impact of successful attacks. We propose the use of random communication topologies for multi-vehicle systems as a moving target mechanism that can be designed to decrease the negative impact of the attack. We derive stability conditions for second-order consensus protocols in the presence of random switching topologies and we identify trade-offs between the convergence rate and the attack impact. The viability of our approach is illustrated with two case studies, (1) vehicular platooning, where a group of vehicles need to remain close enough to exploit the benefits of the platoon (i.e., decreasing CO2 emissions and fuel consumption) while avoiding collisions, and (2) Unmanned Aerial Vehicle (UAV) formation, where a group of UAVs need to maintain a formation that can be used for surveillance or exploration. Finally, we extend our analysis to a more general framework and introduce novel MTD strategies that induce random switching between different controllers, or between sensors.

We formulate optimization problems in order to obtain the optimal probability distribution that minimizes the impact of the attack.

Preliminaries and Notation
Graph theory: Let $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ represents a graph, where $\mathcal{V} = \{1, 2, \ldots, N\}$ is the set of nodes or vertices, and $\mathcal{E}\{(i, j)|i, j \in \mathcal{V}\}$ is the set of pairs called edges. If a pair $(i, j) \in \mathcal{E}$, then i, j are adjacent. The adjacency matrix $\mathcal{A} = [a_{ij}]$ is the symmetric (nonsymmetric for directed graphs) matrix $N \times N$, where $a_{ij} = 1$ if (i, j) are adjacent, $a_{ij} = 0$ otherwise. For the ith node, the set of neighbors is $N_i = \{j|(i, j) \in \mathcal{E}\}$, and the degree of a vertex d_i^s is the number of neighbors that are adjacent to i, i.e., $d_i^s = \sum_{j=1}^{N} a_{ij}$ or, for directed graphs, the number of neighbors whose direction is heading to node i. A sequence of edges (i_1, i_2), (i_2, i_3), $\ldots$, (i_{r-1}, i_r) is called a path from node i_1 to node i_r. The graph $\mathcal{G}$ is said to be connected if for any $i, j \in \mathcal{V}$ there is a path from i to j. The degree matrix is $\mathcal{D} = diag(d_1, d_2, \ldots, d_N)$, and the Laplacian of $\mathcal{G}$ is defined as $\mathcal{L} = \mathcal{D} - \mathcal{A}$. A graph is said to be a k-regular graph if all vertices have connectivity equal to k, each node is connected to k neighbors.

7.2 MTD for Multi-Agent Systems

Multi-agent systems (MAS) are systems that capture a variety of social and distributed interactions where agents make decisions based only on local information (See Fig. 7.1). One of the main components of MAS are the communication links, that indicate whether or not one agent shares information with another. Unfortu-

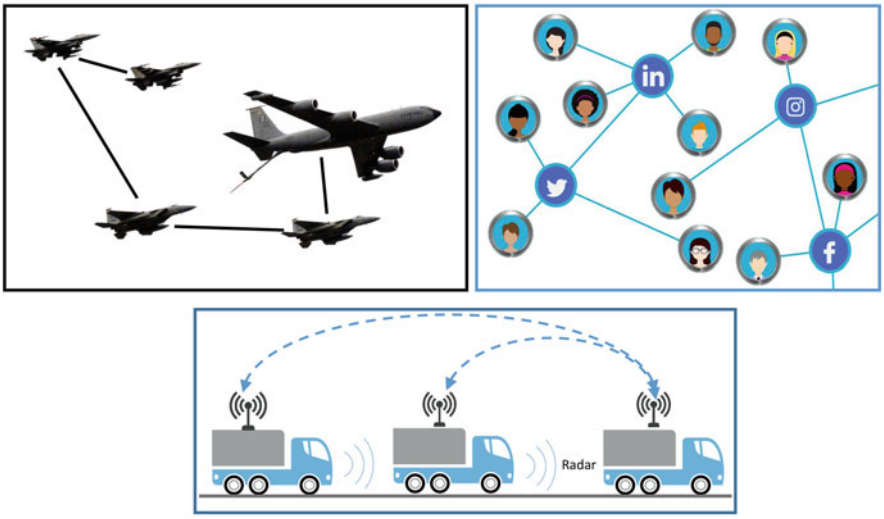

Fig. 7.1 Examples of multi-agent systems

nately, MAS are susceptible to adversaries that may gain access to a subset of communication links and inject false information. For instance, a man-in-the-middle attack can inject false data about a specific sensor, or in social networks, releasing false information to a subset of people in a group that interacts to complete a specific task. In this chapter, we propose MTD strategies to help to mitigate the effects of false data injection attacks in MAS, with emphasis on multi-vehicle systems.

Second-Order Multi-Vehicle System

Let us consider a system with n agents that update their states using the information from a set of neighbors. Each agent is represented by a discrete-time second-order integrator of the form

$$\begin{aligned} x_i(k+1) &= x_i(k) + v_i(k) \\ v_i(k+1) &= v_i(k) + u_i(k), \quad \text{for all } i \in \ell = \{1, 2, \ldots, n\}. \end{aligned} \tag{7.1}$$

where $x_i(k) \in \mathbb{R}$ and $v_i(k) \in \mathbb{R}$ are the position and velocity of each agent i at time k, respectively. Typically, a distributed control action $u_i(k)$ is designed by considering information from a set of neighbors. The communication interaction among agents is modeled by a time-varying directed graph $\mathcal{G}(k) = (\mathcal{V}, \mathcal{E}(k), \mathcal{A}(k))$, where each vertex represent an agent, and the set of communication links are described by $\mathcal{E}(k)$, where the link $e_{ij}(k) \in \mathcal{E}(k)$ if node i receives information from j. Therefore, we consider the consensus protocol adapted from [25] with dynamic communication interactions described by

$$\begin{aligned} u_i(k) = &- \alpha_1 \sum_{j=1}^{n} a_{ij}(k)(x_i(k) - x_j(k) - \delta_{ij}(k)) \\ &- \alpha_2 \sum_{j=1}^{n} a_{ij}(k)(v_i(k) - v_j(k) - \gamma_{ij}(k)) \end{aligned} \tag{7.2}$$

where $a_{ij}(k)$ are the elements of the time-varying adjacency matrix $\mathcal{A}(k)$, α_1, α_2 are parameters to be designed, and $\delta_{ij}(k)$, $\gamma_{ij}(k)$ correspond the attack injected in the information that agent i receives from its neighbor j, for $\delta_{ij}(k) \neq \delta_{ji}(k)$, and $\gamma_{ij}(k) \neq \gamma_{ji}(k)$.

Attacker Model

We consider an adversary that has knowledge about the system dynamics and parameters α_1, α_2, and he knows the fixed communication topology that represents all possible communications. Let k_a, k_f denote the initial and final time of the attack. Thus, the adversary can craft the attack sequences $\{\phi(k_a), \phi(k_a + 1), \ldots, \phi(k_f)\}$ and $\{\gamma(k_a), \ldots, u(k_f a)\}$. We assume that an adversary is able to hijack a subset of communication links and modify the information sent from agent i to agent j. This model may represent two types of attacks as depicted in Fig. 7.2: Sybil attack, where an adversary falsifies the identity of an agent and starts sending false information;

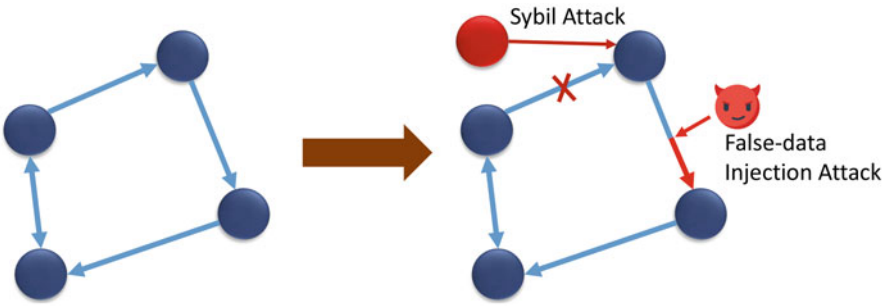

Fig. 7.2 Example of two types of attacks considered in this chapter

and false-data injection attacks, where the attacker intercepts the communications between two agents and falsify the information that is being transmitted. We do not assume that a sensor is compromised, but only the communication channel used to transmit the sensor information to a specific neighbor. For instance, for agents 1, 2, 3, the adversary may compromise the information of y_1 sent from 1 to 2, but not the information of y_1 sent from 1 to 3.

7.2.1 *Random Communication Topology*

The use of random communication topologies for first-order consensus algorithm are useful to model uncertainties in the system such as link failures or DDoS attacks [7, 13]. In this work, we propose the use of random topologies as an MTD strategy that can help to mitigate the impact of adversaries. In particular, we focus on the second-order consensus algorithm in Eq. (7.2) and we derive sufficient conditions for stability.

Let us define the total graph (or supergraph) $\mathscr{G}_T = (\mathscr{V}, \mathscr{E}_T, \mathscr{A}_T)$ as the fixed graph that represents *all possible* communications between agents, where the set $\mathscr{E}_T$ collects all the channels that can be established directly among pairs of sensors, i.e., it is the set of realizable edges. Without an MTD policy, we consider that the communication topology is represented by a fixed graph $\mathscr{G}_f$, which is a spanning connected subgraph of $\mathscr{G}_T$, such that $\mathscr{E}_f \subseteq \mathscr{E}_T$.

Now, our MTD strategy can be modeled by the time-varying graph $\mathscr{G}(k) = (\mathscr{V}, \mathscr{E}(k), \mathscr{A}(k))$ with fixed vertex set $\mathscr{V}$, and time-varying edge set $\mathscr{E}(k) \subset \mathscr{E}_T$, where the edges can vary with time either deterministically or completely random. The instantaneous Laplacian matrix is then $L(k)$.

Now, let $x(k) = [x_1(k),\ x_2(k),\ \ldots,\ x_n(k)]^\top$, $v(k) = [v_1(k),\ \ldots,\ v_n(k)]^\top$, and $z(k) = [x(k)^\top,\ v(k)^\top]$. Also, let $\boldsymbol{\delta_i}(k) = \sum_{j=1}^n a_{ij}(k)\delta_{ij}(k)$ and $\boldsymbol{\gamma_i}(k) = \sum_{j=1}^n a_{ij}(k)\gamma_{ij}(k)$ and $\boldsymbol{\delta}(k) = [\boldsymbol{\delta}_1(k),\ \ldots,\ \boldsymbol{\delta}_n]^\top$ and $\boldsymbol{\gamma}(k) = [\boldsymbol{\gamma}_1(k),\ \ldots,\ \boldsymbol{\gamma}_n(k)]^\top$. We can rewrite the system in (7.1) with the consensus protocol in (7.2) in a compact matrix form as

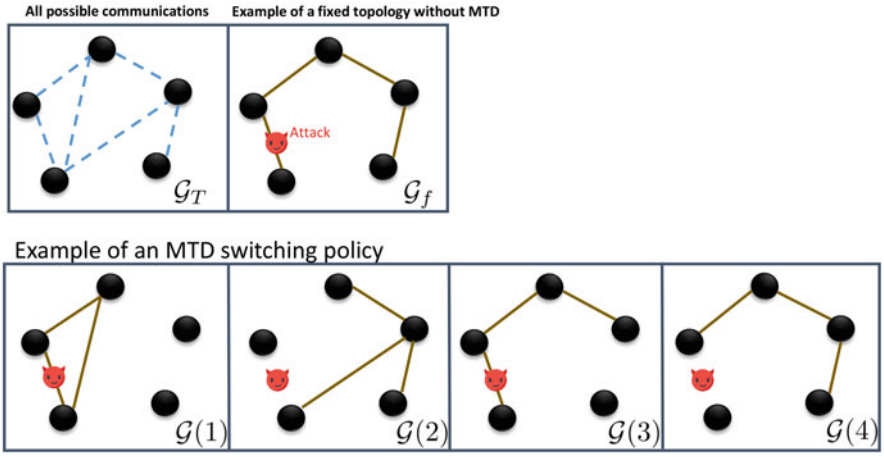

Fig. 7.3 The main idea behind the switching topology consists on changing the topology such that the number of times the compromised information is used decreases while guaranteeing stability of the system for the attack-free scenario. In this example only 50% of the times the fake compromised information can be transmitted. However, in the fixed case the attack is always affecting the communication between two nodes

$$z(k+1) = \underbrace{\begin{bmatrix} I & I \\ -\alpha_1 L(k) & I - \alpha_2 L(k) \end{bmatrix}}_{F(k)} z(k) + \underbrace{\begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \alpha_1 I_n & \alpha_2 I_n \end{bmatrix}}_{G} \boldsymbol{\phi}(k),$$

$$z(k+1) = F(k)z(k) + G\boldsymbol{\phi}(k), \tag{7.3}$$

for $\boldsymbol{\phi}(k) = [\boldsymbol{\delta}(k)^\top, \boldsymbol{\gamma}(k)^\top]^\top$.

The main idea of MTD in multi agent systems is summarized in Fig. 7.3, where a communication graph with an MTD switching policy can mitigate the impact of an attack in the communication link by minimizing the amount of time the fake information is transmitted.

7.2.2 *Random Graphs*

A random graph $\mathcal{G}(k)$ is a graph generated by some random process [13]. Typically, the set of vertices $\mathcal{V}$ is assumed constant throughout time whereas the set of edges $\mathcal{E}(k)$ varies randomly with time. A general way of modeling the randomness of the edges consists in assuming a probability of connection between two vertices i and j, such that $a_{ij}(k) = 1$ is a Bernoulli random variable with probability $0 \leq p_{ij} \leq 1$. We can define the connection probability matrix $\boldsymbol{P} \in \mathbb{R}^{n \times n}$ with entries

$$\boldsymbol{P}_{ij} = \begin{cases} p_{ij}, & i \neq j \\ 0, & i = j. \end{cases}$$

Then, a realization $\mathscr{G}(k)$ at time k can be seen as a spanning subgraph (not necessarily connected) of the super graph $\mathscr{G}_T$. Due to the random nature of $\mathscr{A}(k)$, the instantaneous Laplacian matrix $L(k)$ is also random. The expected value of the adjacency matrix $E[\mathscr{A}(k)] = \boldsymbol{P}$ and the expected Laplacian matrix is then $\bar{L} = diag(\boldsymbol{P}\mathbf{1}_n) - \boldsymbol{P}$.

Erdös-Rényi Model
Erdös and Rényi [4] introduced two models of random graphs that consider two different ways of modeling the randomness of the edges:

1. The model $\mathscr{G}(k) = (\mathscr{V}, s)$ refers to a random graph with a fixed vertex set $\mathscr{V}$, where at each realization there exists exactly s edges. In other words, at each time k a graph $\mathscr{G}(k)$ is chosen uniformly at random from the collection of graphs that have n vertices and s edges.
2. The model $\mathscr{G}(k) = (\mathscr{V}, p)$ refers to a graph with vertex set $\mathscr{V}$ where each edge exists with nonzero probability p, equal for all vertices, such that for all i, j, $p_{ij} = p$.

We focus on a special case of the second Erdös-Rényi model, where only the edges that belong to $\mathscr{E}_T$ have probability p. In other words, $E[\mathscr{A}(k)] = p\mathscr{A}_T$ and $E[L(k)] = \bar{L} = p\mathscr{L}_T$. We refer to these types of graphs as MER (Modified Erdös-Rényi) graphs.

7.2.3 Convergence of the Attack-Free Scenario

It is necessary to guarantee that the inclusion of the proposed random MTD strategy does not affect the convergence to a consensus state. First, as it was pointed out in [25], convergence to a consensus state of a second-order model depends on the correct selection of α_1, α_2 and the connectivity properties of the communication topology, according to the following theorem adapted from [25] for fixed communication graphs.

Theorem 7.1 (Collorary 1 [25]) *Consider the multi-agent system in (7.3) without attack and with an undirected and fixed communication topology. Consensus can be achieved if and only if* $\alpha_2 > \alpha_1 > 0$ *and* $\alpha_1 - 2\alpha_2 > \frac{-4}{\mu_i}$ *for all i.*

Now, the following theorem extends Theorem 7.1 and establishes sufficient conditions for convergence in expectation in the presence of random switching topologies.

Theorem 7.2 *Let* $\mathscr{G}_T = (\mathscr{V}, \mathscr{E}_T)$ *be the communication graph that describes all possible communications between n agents, and let* $\mathscr{A}_T$ *be its adjacency matrix with Laplacian matrix* $\mathscr{L}_T$. *Let* $\mu_1 = 0 < \mu_2 \leq \ldots \leq \mu_n$ *be the eigenvalues of* $\mathscr{L}_T$.

Suppose that each communication link exists with identical probability p such that $E[\mathscr{A}_T] = P = p\mathscr{A}_T$ *and* $\bar{L} = p\mathscr{L}_T$. *The consensus state* $z_c = [x_c^\top \; v_c^\top]^\top$, *for*

$$\begin{aligned} x_c &= \mathbf{1}_N \left(\frac{1}{N} \sum_{j=1}^{n} x_j(0) + \frac{k}{N} \sum_{j=1}^{n} v_j(0) \right), \\ v_c &= \mathbf{1}_N \frac{1}{N} \sum_{j=1}^{n} v_j(0) \end{aligned} \tag{7.4}$$

is reached in expectation if $\alpha_1 = \frac{p}{\mu_n}$ *and* $\alpha_2 = \frac{1+p}{\mu_n}$.

Proof Let $\bar{z}(k) = E[z(k)]$ denote the expected state vector, such that the dynamics in (7.3) without attack can be rewritten as

$$\bar{z}(k+1) = \bar{F}\bar{z}(k)$$

where

$$\bar{F} = \begin{bmatrix} I & I \\ -\alpha_1 \bar{L} & I - \alpha_2 \bar{L} \end{bmatrix}.$$

Recall that $\bar{L}$ is the Laplacian matrix of an undirected graph and that the consensus state is reached for fixed topologies if $\alpha_1 > \alpha_2 > 0$ and $\alpha_1 - 2\alpha_2 > \frac{-4}{\bar{\mu}_i}$ according to Theorem 7.1, where $\bar{\mu}_i$ is the ith eigenvalue of $\bar{L}$ for $i = 2, \ldots, n$. Since $\mathscr{L}_T$ is symmetric, we have that $\bar{\mu}_i = p\mu_i$. Thus, $\frac{p}{\mu_n} - 2\frac{1+p}{\mu_n} > \frac{-4}{p\mu_n} > \frac{-4}{p\mu_i}$. Multiplying by $p\mu_n$, we obtain $-p^2 - 2p + 4 > 0$ which is always true for $0 < p \leq 1$. □

Remark 7.1 Convergence in expectation means that the speed $v(k)$ will converge to a vicinity of v_c.

Corollary 7.1 *When the random graph is described by an Erdös-Rényi model with degree s, then the states* $z(k)$ *will converge surely to* z_c, *i.e.,* $\Pr\{\lim_{k\to\infty} z(k) = z_c\} = 1$.

We have shown convergence conditions in expectation that depend on the correct selection of α_1, α_2. However, convergence in expectation is not enough to guarantee asymptotic behavior to a consensus state. Therefore, we introduce the following definition.

Definition 7.1 (Mean Square Consensus) Under random switching topologies, the multi-agent system in (7.1) reaches mean square consensus if, for any $i \neq j$, $|x_i(k) - x_j(k)| \to 0$ and $|v_i(k) - v_j(k)| \to 0$ hold in mean square sense for any initial states, such that the consensus state belongs to the vicinity of z_c.

The notion of mean square consensus ensures that $z(k)$ will converge asymptotically to a consensus state with probability 1, and the consensus state is in the vicinity of z_c.

To find conditions for mean square consensus, we will use the results stated in the following Theorem adapted from [26] for Markovian switching topologies.

Theorem 7.3 (Theorem 4 in [26]) *Assume the switching topology is driven by an ergodic Markov process (or a Bernoulli process). There exists gains α_1, α_2, such that under the linear protocol in (7.2) the multi-agent system in (7.1) reaches mean square consensus, if and only if the union of the graphs in the topology set of size r, $\{G_1, G_2, \ldots, G_r\}$ has a globally reachable node.*

Since our edge set is random and changes at each time instant k, we do not have a fixed set of communication topologies; however, if we can show that after a finite number of switches, the union of any random graph realizations has a globally reachable node, we can ensure mean square consensus.

Lemma 7.1 *For any MER (and Erdös-Rényi) graph $\mathcal{G}(k) = (n, p)$ with $p > 0$, there exists a $k^* < \infty$ such that the union of graph realizations $\mathfrak{G} = \mathcal{G}(1) \cup \mathcal{G}(2) \cup \ldots \cup \mathcal{G}(k^*)$ is connected.*

Proof Let $\mathfrak{E} = \{\mathcal{E}(1) \cup \mathcal{E}(2) \cup \ldots \cup \mathcal{E}(k^*)\}$ be the union of the edge sets with elements $\mathfrak{e}_{ij}$. Therefore, $\mathfrak{e}_{ij} \neq \emptyset$ if, for $k = 1, \ldots, k^*$, the link $e_{ij}(k)$ has existed at least once. It is easy to see that the union of modified Erdös-Rényi graphs $\mathfrak{G}$ is also a modified Erdös-Rényi random graph with the same vertex set and probability $\widetilde{p} = \Pr[\mathfrak{e}_{ij} \neq \emptyset]$. Since the existence of the edge $e_{ij}(k) \in \mathcal{E}(k)$ at an instant k is described by a Bernoulli random variable with probability p, then the probability that the link has existed at least once after k^* realizations is described by the complement of a binomial distribution, as follows

$$\begin{aligned} \Pr[\mathfrak{e}_{ij} \neq \emptyset] &= 1 - \Pr[(e_{ij}(k) \neq \emptyset) \leq 1, k^*] \\ &= 1 - (1-p)^{k^*} - k^* p (1-p)^{k^*-1}. \end{aligned} \tag{7.5}$$

where $\Pr[(e_{ij}(k) \neq \emptyset) \leq 1, k^*]$ is the probability that e_{ij} existed at most once after k^* trials.

Notice that

$$\lim_{k^* \to \infty} 1 - (1-p)^{k^*-1} \left(1 - p + k^* p\right) = 1 \tag{7.6}$$

such that $\mathfrak{G} \to \mathcal{G}_T$. However, we need to show that there exists a finite $k^* < \infty$ such that $\mathfrak{G}$ is connected with high probability. To this end, recall that for a typical Erdös-Rényi graph $G(k) = (n, p)$, there exists a threshold $p > \frac{\log n + c}{n} < 1$ such that $\Pr[G(k) = connected] \to e^{-e^{-c}}$ [4]. The proof is based on defining a random variable X_0 that counts the number of isolated vertices when all communications are possible, and finding the probability that $P[X_0 = 0]$. Therefore, for the modified Erdös-Rényi random graph $\mathfrak{G} = (n, \widetilde{p})$, we can apply the same methodology by

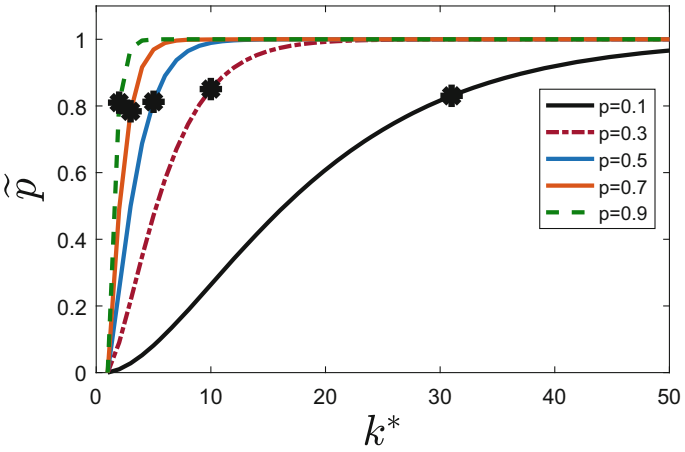

Fig. 7.4 Relationship between the instant k^* and the probability of an edge being connected after k^* iterations $\widetilde{p}$. When k^* increases, the union of random graphs (where each graph may be disconnected) forms a connected graph

restricting the edge set to $\mathscr{E}_T$, and find the specific threshold for which $\Pr[\mathfrak{G} = connected]$ with high probability. The calculation of that threshold is not an easy task, but since (7.6) holds, we know it exists. □

Example

Consider the modified ER random graph with $n = 10$, where $\mathscr{G}_T$ is a 2-regular graph. Figure 7.4 illustrates the relationship between k^* and $\widetilde{p}$ for different p. Clearly, as k^* increases, so does the probability of connection. Also, we calculated the number of iterations k^* until $\mathfrak{G}$ is connected and we repeated this process 1000 times. The asterisk indicates the maximum k^* associated to each probability. Clearly, for each p there is a finite k^* that ensures that $\mathfrak{G}$ is connected.

Now, we are able to state the following theorem.

Theorem 7.4 *The system in* (7.1) *with the consensus algorithm in* (7.2) *and with MTD policy described by the modified Erdös-Rényi graph with* $0 < p < 1$ *and total graph* $\mathscr{G}_T$ *reaches mean square consensus if* α_1, α_2 *are selected according to Theorem* 7.2, *and if* $\mathscr{G}_T$ *is connected.*

Proof Invoking Theorem 7.3, and since the union of modified Erdös-Rényi graphs is connected after a finite number of iterations for $p > 0$ according to Lemma 7.1, then there exists gains α_1, α_2 such that the second-order consensus algorithm is mean square stable and converge to a vicinity of z_c. From Theorem 7.2, we have found α_1, α_2 that guarantee stability in expectation. Thus, they also are sufficient to ensure mean square consensus. □

7.2.3.1 Convergence Rate with MTD

Using the proposed MTD strategy induces a deterioration of the convergence rate to the consensus state. Therefore, we will use the convergence rate as a measure of performance in order to identify how p and $\mathcal{G}_T$ affect the performance of the system.

Definition 7.2 The **convergence rate** in a consensus algorithm is the rate of convergence to the steady state value and it can be characterized by the spectral gap $R = 1 - \rho(F)$, where $\rho(F) = \max(|\lambda_i| : \lambda_i \neq 1)$. A convergence rate of 1 is the fastest possible convergence and 0 implies that the dynamics are not evolving at all.

In order to quantify the convergence rate in the presence of random switching, we introduce the following lemma adapted from [25].

Lemma 7.2 *Let us consider the second-order consensus algorithm described in* (7.3) *for fixed communication topology such that* $L(k) = L$ *with eigenvalues* μ_i *and* $F(k) = F$. *The eigenvalues of* F *are given by*

$$\lambda_{i1,2} = \frac{-\alpha_2\mu_i \pm \sqrt{\alpha_2^2\mu_i^2 - 4\alpha_1\mu_i}}{2} + 1$$

Proof The proof can be found in [25]. □

The degradation caused by using MTD can be calculated by comparing two cases, consensus with a fixed topology described by $\mathcal{G}_f$, and with a random topology. For the fixed topology, we consider the special case where all possible communications are active, such that $\mathcal{G}_f = \mathcal{G}_T$, as follows.

Lemma 7.3 *Let* $\mathcal{G}_T$ *be the graph that represents all possible communications and let us consider the special case where all possible communication links exist, i.e., the fixed communication topology without MTD is given by* $\mathcal{G}_f = \mathcal{G}_T$. *Applying the algorithm in* (7.3) *with fixed topology (i.e.,* $p = 1$*) the convergence rate is* $R_f = 1 - \rho(F)$, *for* $\rho(F) = \sqrt{1 - \frac{\mu_2}{\mu_n}}$.

Proof From Lemma 7.2, we have that for a fixed topology with Laplacian matrix L, the eigenvalues of F are given by

$$\lambda_{i1,2} = \frac{-\alpha_2\mu_i \pm \sqrt{\alpha_2^2\mu_i^2 - 4\alpha_1\mu_i}}{2} + 1.$$

When $p = 1$, from Theorem 7.2 we have that $\alpha_1 = \frac{2}{\mu_n}$, $\alpha_2 = \frac{1}{\mu_n}$, such that

$$\lambda_{i1,2} = \frac{-2\frac{\mu_i}{\mu_n} \pm \sqrt{4\frac{\mu_i^2}{\mu_n^2} - 4\frac{\mu_i}{\mu_n}}}{2} + 1 = -\frac{\mu_i}{\mu_n} \pm \sqrt{\frac{\mu_i}{\mu_n}\left(\frac{\mu_i}{\mu_n} - 1\right)} + 1.$$

Notice that the term inside the square root is always negative, such that the eigenvalues have a component in the imaginary axis. We then can rewrite the eigenvalues as

$$\lambda_{i1,2} = -\frac{\mu_i}{\mu_n} + 1 \pm \mathbf{j}\sqrt{\frac{\mu_i}{\mu_n}\left(1 - \frac{\mu_i}{\mu_n}\right)}.$$

The magnitude is then

$$|\lambda_i| = \sqrt{\left(1 - \frac{\mu_i}{\mu_n}\right)^2 + \frac{\mu_i}{\mu_n}\left(1 - \frac{\mu_i}{\mu_n}\right)} = \sqrt{1 - \frac{\mu_i}{\mu_n}}.$$

Since all eigenvalues μ_i are real, $\rho(F) = \sqrt{1 - \frac{\mu_2}{\mu_n}}$ and $R_f = 1 - \rho(F)$. □

Now, the upper bound of the expected convergence rate is derived in the following theorem.

Theorem 7.5 *Suppose that an MTD random mechanism is introduced such that the communication topology changes randomly over time with probability p. Therefore, the expected convergence rate $\bar{R}_{MTD} < R_f$ for any $0 < p < 1$ is given by*

$$\bar{R}_{MTD} = 1 - \sqrt{1 - p\frac{\mu_2}{\mu_n}}.$$

Proof Since $\rho(F)$ is a convex function for nonnegative matrices, from the Jensen's inequality, we have that

$$E[\rho(F(k))] \geq \rho(E[F(k)]) = \rho(\bar{F}).$$

Therefore, $\bar{R}_{MTD} = E[R_{MTD}(k)] = 1 - E[\rho(F(k))] \leq 1 - \rho(\bar{F})$.

Now, suppose $0 < p < 1$, such that the eigenvalues of $\bar{F}$ are given by

$$\bar{\lambda}_{i1,2} = \frac{-(1+p)\frac{\bar{\mu}_i}{\mu_n} \pm \sqrt{(1+p)^2\frac{\bar{\mu}_i^2}{\mu_n^2} - 4p\frac{\bar{\mu}_i}{\mu_n}}}{2} + 1,$$

where $\bar{\mu}_i$ are the eigenvalues of $\bar{L}$. Since $\mathscr{L}_T$ is symmetric, then $\bar{\mu}_i = p\mu_i$. Following the same steps as before, it is easy to see that $|\bar{\lambda}_i| = \sqrt{1 - p\frac{\mu_i}{\mu_n}}$ and $\bar{R}_{MTD} \leq 1 - \sqrt{1 - p\frac{\mu_2}{\mu_n}}$. Clearly, $\bar{R}_{MTD} < R_f$ since

$$\sqrt{1 - p\frac{\mu_2}{\mu_n}} > \sqrt{1 - \frac{\mu_2}{\mu_n}}$$

holds for any $p < 1$, and there is a degradation in the convergence rate. □

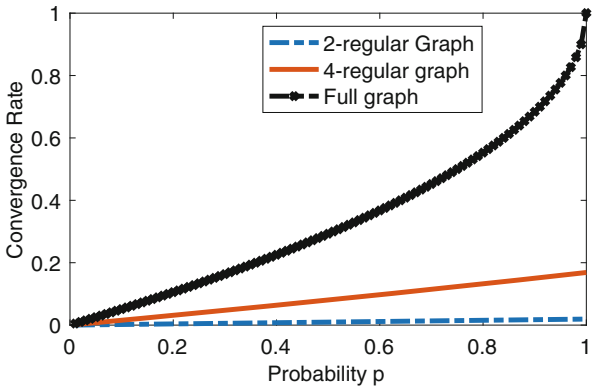

Fig. 7.5 Convergence rate for different probabilities and for several $\mathscr{G}_T$. Notice that increasing the communication capabilities in the network improves the consensus performance

Remark 7.2 Using MTD comes with a degradation in the convergence rate. Applications that require fast convergence to a consensus or a formation will need to select an appropriate large enough p.

Figure 7.5 shows the convergence rate for different graphs. Notice that the convergence rate increases with the connectivity of the communication graph, and decreases with p. As we will see next, p not only affects the convergence rate, but also the impact caused by an attacker. As a consequence, the defender needs to select appropriate p and $\mathscr{G}_T$ to maintain a good performance while making the system resilient to attacks.

7.2.4 Attack Impact with Random Switching Topology

We have calculated the convergence rate of the multi-vehicle system with a random switching communication topology in terms of the probability p. Clearly, to increase the convergence rate, it is necessary to select a large p. However, we need to quantify how the effect of a cyber-attack is affected by p in order to obtain a trade-off between the performance (convergence rate) and the impact of the attack.

Let x_c be the desired state or operational point at which the control action drives the system states. The main objective of an adversary is to deviate the system states from x_c. For instance, an adversary may intent to cause an increase on the pressure in a chemical reactor or cause that two vehicles crash. Therefore, we can define $\mathscr{I} \in \mathbb{R}_+$ as the impact that an attack can cause to the system as a function of $x(k) - x_c$. In this chapter, we define the impact as

$$\mathscr{I} = \lim_{k \to \infty} \|x(k) - x_c\|, \tag{7.7}$$

which captures effects of the attack even when stability is not compromised.

Now, suppose that the communication network in the multi-vehicle system changes randomly according to the model in (7.3). Let $E[z(k)] = \bar{z}$, $E[L(k)] = \bar{L}$, and $E[F(k)] = \bar{F}$, where

$$\bar{F} = \begin{bmatrix} I & I \\ -\alpha_1 \bar{L} & I - \alpha_2 \bar{L} \end{bmatrix}.$$

Similarly, we can define $E[\boldsymbol{\phi}(k)] = [E[\boldsymbol{\delta}(k)]^\top, E[\boldsymbol{\gamma}(k)]^\top] = \bar{\boldsymbol{\phi}}$ where

$$E[\boldsymbol{\delta}_i(k)] = p \sum_{j=1}^{n} a_{ij} \alpha_1 E[\delta_{ij}(k)]$$

and

$$E[\boldsymbol{\gamma}_i(k)] = p \sum_{j=1}^{n} a_{ij} \alpha_2 E[\gamma_{ij}(k)]$$

such that

$$\bar{z}(k+1) = \bar{F}\bar{z} + pG\boldsymbol{\phi}(k). \tag{7.8}$$

Theorem 7.6 *Let $\mathcal{G}_T = (\mathcal{V}, \mathcal{E}_T)$. be the communication graph that describes all possible communications between n agents, with Laplacian matrix $\mathcal{L}_T$. Let $\mu_1 = 0 < \mu_2 \leq \ldots \leq \mu_n$ be the eigenvalues of $\mathcal{L}_T$. Consider the system in (7.3) with a random topology with link connection probability $0 < p < 1$ and gains α_1, α_2 selected according to Theorem 7.2. The impact of the attack is given by*

$$\bar{\mathscr{I}} = \frac{p}{\mu_n} \sqrt{n(2p^2 + 2p + 1)}.$$

Proof The solution of (7.8) in the presence of an attack is given by

$$\bar{z}(k+1) = \bar{F}^k \bar{z}(0) + \sum_{l=0}^{k-1} \bar{F}^{k-l-1} pG\bar{\boldsymbol{\phi}}(k), \tag{7.9}$$

In [25] it has been shown that, if α_1, α_2 are properly selected,

$$\lim_{k\to\infty} \bar{F}^k = \begin{bmatrix} \mathbf{1}_n \xi^\top & \mathbf{1}_n \xi^\top k \\ \mathbf{0} & \mathbf{1}_n \xi^\top \end{bmatrix}, \tag{7.10}$$

where $\xi = \frac{\mathbf{1}_n}{\sqrt{n}}$ is the unique nonnegative left eigenvector of $\bar{L}$ associated with the eigenvalue 0. In order to quantify the impact of an attack, we focus our attention on how any attack can affect the vehicles speed. Thus, from (7.3), (7.9) and (7.10) we have that

$$\lim_{k\to\infty} \bar{F}^{k-l-1} pG = p \begin{bmatrix} \mathbf{1}_n \xi^\top & \mathbf{1}_n \xi^\top k \\ \mathbf{0} & \mathbf{1}_n \xi^\top \end{bmatrix} \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \alpha_1 I_n & \alpha_2 I_n \end{bmatrix} = p \begin{bmatrix} \alpha_1 \mathbf{1}_n \xi^\top k & \alpha_2 \mathbf{1}_n \xi^\top k \\ \alpha_1 \mathbf{1}_n \xi^\top & \alpha_2 \mathbf{1}_n \xi^\top \end{bmatrix}.$$

Taking only the part related to the vehicle speed for $G_2 = [\alpha_1 I, \alpha_2 I]$ and α_1, α_2 according to Theorem 7.2, the expected impact can be defined as

$$\bar{\mathscr{I}} = \|\mathbf{1}_n \xi^\top p G_2\| = \sqrt{np^2(\alpha_1^2 + \alpha_2^2)} = \frac{p}{\mu_n} \sqrt{n(2p^2 + 2p + 1)}.$$

□

Figure 7.6 shows the trade-off between the performance given by the convergence rate and the impact of the attack for different types of graphs. Notice that small probabilities will decrease the impact of the attack but at the cost of small convergence rates. On the other hand, the degree of connectivity of $\mathscr{G}_T$ has a significant impact on mitigating the effects of the attack. When $\mathscr{G}_T$ is a full graph, all communication links are possible, and the system is clearly more resilient than for any other topology. Thus, the system designer can increase the amount of possible communication channels in order to select smaller p that will not cause a significant performance degradation, while guaranteeing good resiliency to attacks. However,

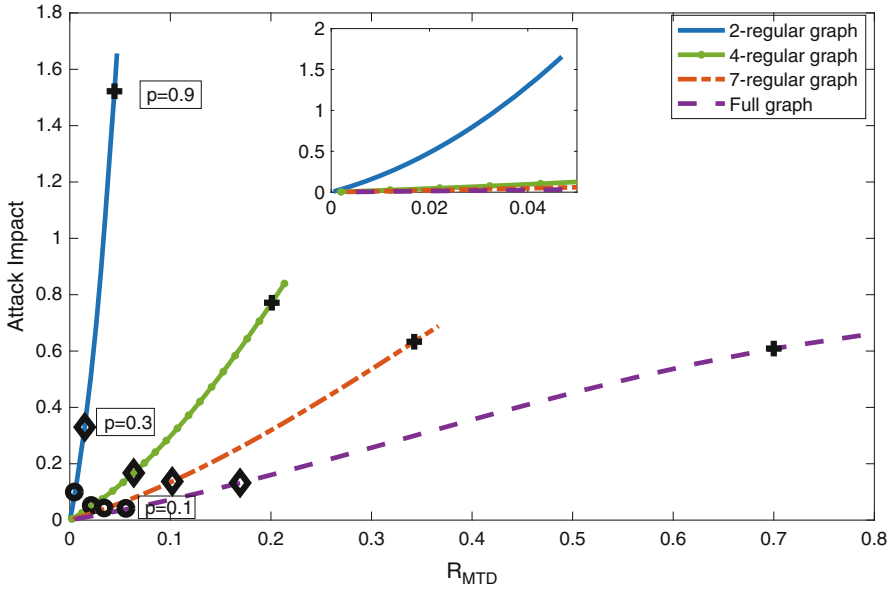

Fig. 7.6 Convergence rate vs. impact metric for different graphs with $n = 10$. Clearly, small p leads to lower vulnerability but at the cost of a decrease in the performance (decrease in the convergence rate). In particular, increasing the connectivity of the total graph, decreases considerably the impact of the attack

having a wide amount of communication channels for each vehicle may require more expensive equipment and more energy consumption.

7.3 Experiments

In order to illustrate the viability of our analysis, we consider two case studies, (1) vehicular platooning, and (2) UAVs formation control. In both scenarios, we show how the proposed random MTD strategy can be used to mitigate the impact of the attack.

7.3.1 Vehicular Platooning

We consider the problem of vehicular platooning. In particular, platooning offers many benefits over solo driving such as better reaction times, decrease of CO_2 emissions, and lower fuel consumption [18]. The objective of the platoon is to maintain an adequate distance between vehicles, such that sudden changes in the leader's speed (e.g., braking) will not cause any crash in the preceding vehicles. This is known as the string stability of the platoon and has been widely studied in the literature [11, 14, 19]. Typically, the Adaptive Cruise Control (ACC) system controls the distance and/or relative velocity between adjoining vehicles by measuring (radar/lidar) and reacting to the relative distance and/or velocity between adjacent vehicles compared to a desired setpoint. More recently, work has leveraged vehicle-to-vehicle or infrastructure-to-vehicle communication to inject feed-forward commands. Such Cooperative Adaptive Cruise Control (CACC) systems improve the string stability of the platoon and allow vehicles to follow each other with a closer distance than with ACC, thereby improving traffic flow capacity. CACC gathers information of vehicles further in front according to a specific communication network topology (Fig. 7.7).

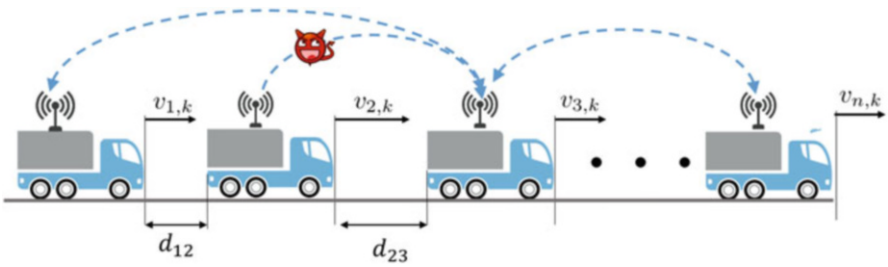

Fig. 7.7 Scheme of a platoon of n vehicles. Each vehicle is equipped with a CACC strategy using vehicle-to-vehicle communication network. An adversary can gain access to some sensors or actuator commands transmitted through the network

The dynamics of each vehicle in the platoon are dictated by (7.13) with a control strategy of the form

$$u_i(k) = -\alpha_1 \sum_{j=1}^{n} a_{ij}(k)\left(x_i(k) - x_j(k) - d_{ij}\right) - \alpha_2 \sum_{j=1}^{n} a_{ij}(k)\left(v_i(k) - v_j(k)\right),$$

where $d_{ij} = (j-i)d$ such that adjacent vehicles always have distance d [1].

In our simulations, we consider a platoon with 10 vehicles, $d = 2$m, and scenarios with and without MTD. Figure 7.8 illustrates the intra-vehicular distance $x_i - x_{i+1}$ and the speed of each vehicle. Before the attack, all intra-vehicle distances converge to $d = 2$ and to a speed of 72 km/h. Notice that including MTD affects the convergence time to the consensus state.

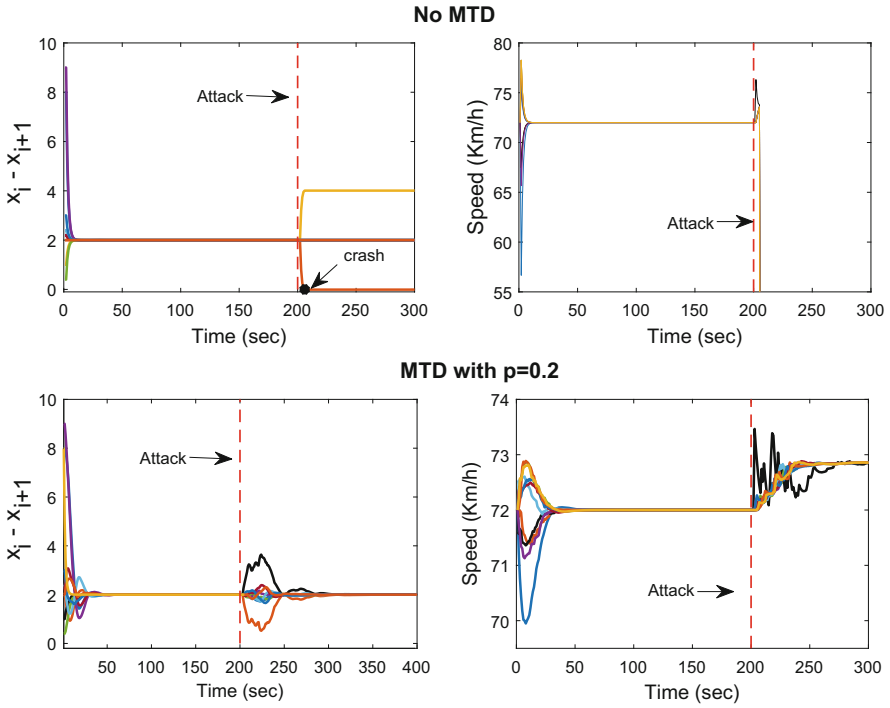

Fig. 7.8 Vehicles distance ($x_i - x_{i+1}$) and speed for the vehicular platooning problem, with desired $d = 2$ and final speed of 72 km/h. Vehicles reach the desired distance even with MTD, with a cost of slower convergence time. After 200 s an attacker compromises some of the communications received by vehicle 3 and launches a bias attack that fades over time. Without MTD, the attack causes that vehicles 2 and 3 crash (Top) causing the entire platoon to stop. On the other hand, with our proposed MTD and $p = 0.2$, the crash is avoided and the platoon speed slightly increases due to the attack (bottom)

Now, suppose that an adversary is able to compromise the information that agent 3 receives from one of its neighbors and injects a bias attack that fades over time. Without MTD, vehicles 2 and 3 crash after 5 s causing the entire platoon to stop (Fig. 7.8-Top). On the other hand, with a random MTD with $p = 0.2$, it is possible to avoid the crash and mitigate the impact of the attack. Notice that the attack only causes a slight increase in the speed and some oscillations but the consensus state is attained after the attack.

7.3.2 Formation Control of UAVs

Formations of UAVs have found use in military and civilian activities such as surveillance and exploration [8], building construction [24], and disaster management [15]. The main idea of these type of formations lies on the possibility that the group of UAVs moves as a single rigid body while performing a specific task using distributed and decentralized control strategies, where each UAV exchanges information only with a small group of agents.

To simply model the dynamics of n UAVs, we use (7.1) to represent the position and velocity in each axis, X and Y, respectively of each UAV [17], such that

$$\begin{aligned} x_{X,i}(k+1) &= x_{X,i}(k) + v_{X,i}(k) \\ v_{X,i}(k+1) &= v_{X,i}(k) + u_{X,i}(k) \\ x_{Y,i}(k+1) &= x_{Y,i}(k) + v_{Y,i}(k) \\ v_{Y,i}(k+1) &= v_{Y,i}(k) + u_{Y,i}(k), \end{aligned} \tag{7.11}$$

where $x_{X,i}(k)$, $v_{X,i}(k)$ are the position and speed in the X axis, $x_{Y,i}(k)$, $v_{Y,i}(k)$ are the position and speed in the Y axis.

For the formation control of UAVs, we assume that each UAV is able to control its speed in the X and Y axis separately, using a consensus-based algorithm of the form

$$\begin{aligned} u_{X,i}(k) = &-\alpha_1 \sum_{j=1}^{n} a_{ij}(k) \left(x_{X,i}(k) - x_{X,j} - d_{X,ij}\right) \\ &-\alpha_2 \sum_{j=1}^{n} a_{ij}(k) \left(v_{X,i}(k) - v_{X,j}(k)\right) \\ u_{Y,i}(k) = &-\alpha_1 \sum_{j=1}^{n} a_{ij}(k) \left(x_{Y,i}(k) - x_{Y,j} - d_{Y,ij}\right) \\ &-\alpha_2 \sum_{j=1}^{n} a_{ij}(k) \left(v_{Y,i}(k) - v_{Y,j}(k)\right) \end{aligned} \tag{7.12}$$

where $d_{X,ij}$, $d_{Y,ij}$ are the desired distances between each pair of agents that describe the desired formation. Since $d_{X,ij}$, dY, ij are fixed and since we assume that the states in each direction are independent, the stability analysis does not depend on the desired formation, but only on the selection of α_1, α_2 and p.

As an example, suppose we have 10 UAVs, each one with X,Y speed controls and the desired formation is a diamond shape at a height of 5 m. Each UAV possesses communication capabilities to transmit their XY position and both speeds in a single package where $\mathscr{G}_T$ is a 4-regular graph. Figure 7.9 depicts the $X-Y$ trajectories of the group of UAVs with the proposed MTD with $p=0.2$ and without attack. Clearly, even in the presence of switching topologies, the desired formation is achieved.

Now, we assume an adversary compromises only the communication links that agent 3 receives from 1 after 200 s, with $\phi_{X,31}=0.3$, $\gamma_{X,31}=0.2$ for the X axis and $\phi_{Y,31}=-0.3\gamma_{Y,31}=-0.2$. The attack causes that the formation changes its direction by increasing the speed, as depicted in Figs. 7.10 and 7.11. However, the deviation can be mitigated for small p, at the cost of larger convergence times.

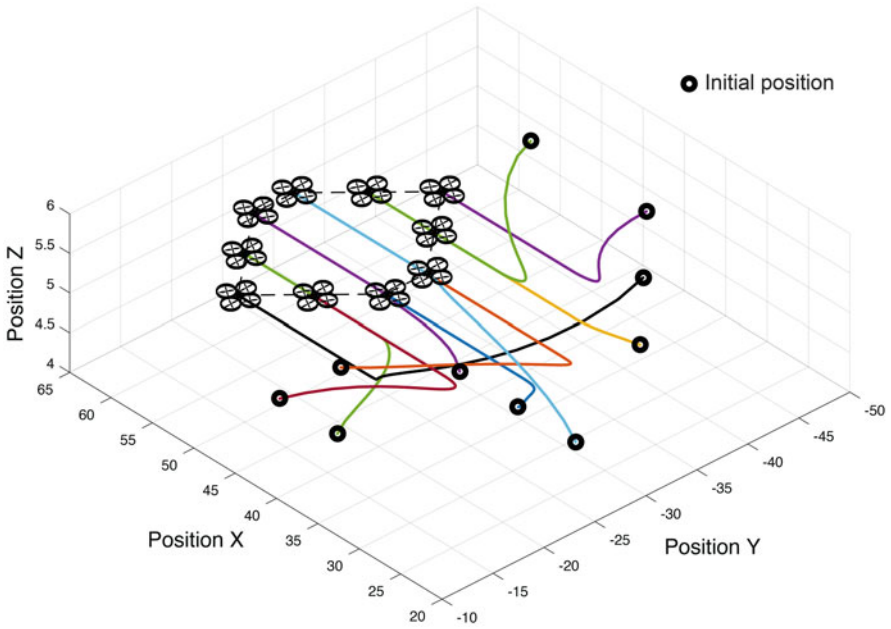

Fig. 7.9 Formation control of 10 UAVs that intend to form a diamond shape formation

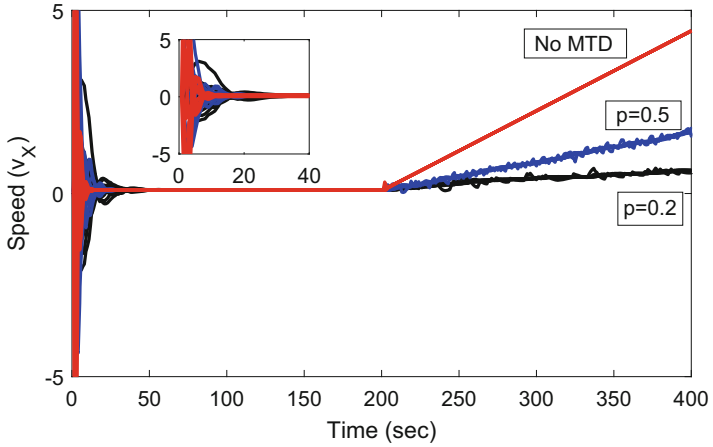

Fig. 7.10 Speed in the X axis of the group of UAVs with and without MTD. Before the attack, the control action guarantees a consensus in the speed and the desired formation is attained. After 200 s, an adversary compromises the information that agent 3 receives from one if his neighbors

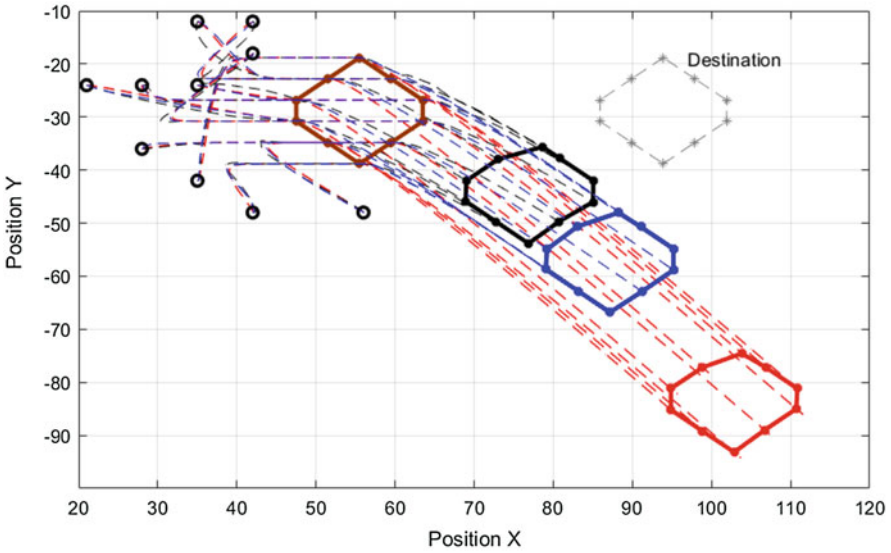

Fig. 7.11 Formation control of 10 UAVs with an MTD strategy for different $p = 0.2$ (black), $p = 0.5$ (blue), and no MTD (red) during 400 s. An attacker compromises one communication link received by agent 3 and launches a bias attack after 200 s. The group of agents is deviated from its destination at different speed rates depending on p. Clearly MTD decreases the impact caused by an attack that aims to deviate the formation

7.4 Toward Optimal Mitigation

We have shown how random switching of the communication topology in multi-agent systems can mitigate the deviation caused by cyber-attacks. Now, we want to extend the proposed strategy to a more general control systems frameworks where the switching can be performed at a sensor level (or in the communications between sensors and actuators), or at the controller level (e.g., performed by a PLC). Besides, we consider heterogeneous switching probabilities such that we can formulate optimization problems that allow us to find the *optimal probability distribution* of the switching strategy that decreases the impact caused by sensor attacks.

We consider a discrete-time linear time invariant (LTI) system described by

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) \\ y(k) &= Cx(k) + \phi(k), \end{aligned} \tag{7.13}$$

where A, B, C are matrices of proper dimensions, and $x(k) \in \mathbb{R}^n$, $y(k) \in \mathbb{R}^p$, $u(k) \in \mathbb{R}^m$ are the state, output, and input vectors, respectively. Since the sensor/control commands can be sent through a communication network, we assume that the system can be subject to additive sensor attacks $\phi(k) \in \mathbb{R}^p$.

7.4.1 MTD in the Controller

We now consider the case where uncertainties are added to the system through the controller actions. The general architecture is illustrated in Fig. 7.12, where the control action is chosen from a group of appropriate controllers. Our objective is to design the sequence of control gains that can decrease the state deviation caused by sensor attacks. A similar MTD approach has been proposed in [6], where the authors design the random switching strategies that maximizes the entropy or unpredictability caused by the MTD mechanism.

Suppose we have n_c different control modes and let $\sigma(k) \in \mathbb{Z}_+$ for $\sigma(k) \leq n_c$ be the index of the control mode at the kth time instant. Let $\Sigma = \{\sigma(0), \sigma(1), \dots\}$ denote the switching sequence or switching logic that orchestrate the different mode changes between controllers. Thus, we can define the control action as

$$u(k) = K_{\sigma(k)} y(k), \tag{7.14}$$

where at each time instant k, the control gain is given by $K_{\sigma(k)} \in \mathfrak{K}$, for $\mathfrak{K} = \{K_1, K_2, \dots, K_{n_c}\}$. Therefore, combining (7.13) and (7.14) we obtain

$$x(k+1) = (A + BK_{\sigma(k)}C)x(k) = F_{\sigma(k)}x(k) \tag{7.15}$$

where $F_{\sigma(k)} = A + BK_{\sigma(k)}C$.

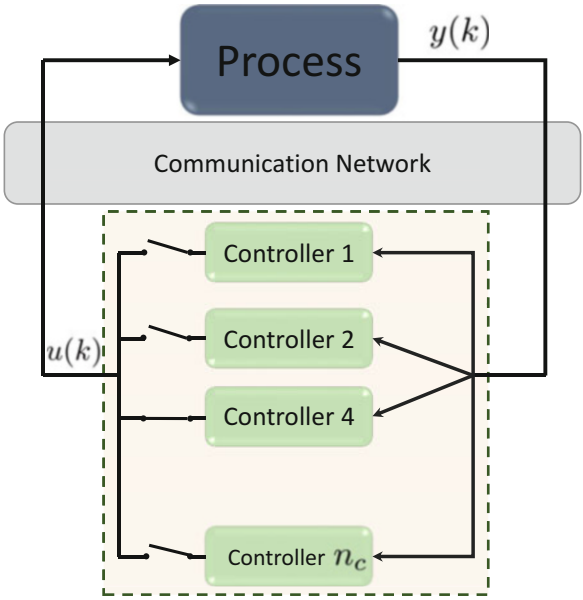

Fig. 7.12 MTD scheme for switching among different controllers

The challenge with these type of linear systems lies on guaranteeing stability for an arbitrary index sequence Σ. Lin et al. [10] summarized some important results in the stability of the switched system in (7.15). The next theorem adapted from [9] states the necessary and sufficient condition for asymptotic stability.

Theorem 7.7 *The switched system in* (7.15) *is asymptotically stable under an arbitrary switching if and only if there exists an arbitrary integer* $\boldsymbol{n}$ *such that for all* $\boldsymbol{n}$*-tuple* $F_{i_j} \in \{F_1, F_2, \ldots, F_{n_c}\}$ *for* $j = 1, \ldots, \boldsymbol{n}$

$$\| F_{i_1} F_{i_2} \ldots F_{i_n} \| < 1.$$

The question now is, how can we limit the impact of cyber-attacks by switching among controllers?

To answer this question, we need to solve two problems: (1) find the set of controllers $\mathfrak{K}$, and (2) find the switching sequence. We propose an approach that solves both problems as a motivation to show how MTD can decrease the impact of attacks. To solve the first problem, and since we are trying to limit the impact of sensor attacks, we assume that the elements of an optimal control gain (e.g., LQR controller) can be active or inactive, such that not all sensor data is used at each time instance. For instance, if an optimal control (without switching) is $K_T = [K_{T1}, K_{T2}, K_{T3}]$, we can assume that $K_1 = [0, K_{T2}, K_{T3}]$, $K_2 = [K_{T1}, 0, K_{T3}]$, and $K_3 = [K_{T1}, K_{T2}, 0]$. In this way, we do not use all the sensor information at all times. Therefore, if conditions of Theorem 7.7 are satisfied for the control set, any arbitrary switching sequence guarantees asymptotic stability. If we consider observer-based controllers, the same technique can be applied to the estimation gain L.

For the second problem, we will consider random switching, such that we can exploit some tools from stochastic systems. Let p_j be the probability that control $K_j \in \mathfrak{K}$ is active where $\sum_{j=1}^{n_c} p_j = 1$. Suppose that $\bar{x}(k) = E[x(k)]$ denotes the expected state, such that

$$\bar{x}(k+1) = \bar{F}\bar{x}(k)$$

where

$$\bar{F} = E[F_{\sigma(k)}] = A + B\bar{K}C$$

and $\bar{K} = \sum_{j=1}^{n_c} p_j K_j$. Therefore, the design of the switching mechanism becomes the design of an appropriate probability distribution that assigns probabilities to each controller.

In the presence of a sensor attack, we have

$$\bar{x}(k+1) = \bar{F}x(k) + B\bar{K}E[\phi(k)],$$

with solution

$$\bar{x}(k) = \bar{F}^k\bar{x}(0) + \sum_{l=1}^{k-1} \bar{F}^{k-l-1}B\bar{K}E[\phi(l)]. \tag{7.16}$$

Assuming that $E[\phi(k)] = \bar{\phi}$ is constant for all k, and combining (7.7) with (7.16) for $x_c = 0$ and for $\bar{x}(k)$ we can calculate the expected impact

$$\bar{\mathscr{I}} = \lim_{k\to\infty} \|\bar{x}(k)\| \leq \|(I - \bar{F})B\bar{K}\|\|\bar{\phi}\|,$$

such that we can formulate the following nonlinear optimization problem:

Problem 1

$$\min_{p_1, p_2, \ldots, p_{n_c}} \|(I - \bar{F})^{-1}B\bar{K}C\| \tag{7.17}$$

$$s.t.$$

$$\sum_{i=1}^{n_c} p_i = 1, \tag{7.18}$$

$$p_i \geq 0, \quad \text{for all } i.$$

The solution of Problem 1 provides the probability distribution of the random switching strategy that minimizes the effects of an adversary in expectation. This formulation can be extended to include performance constraints or additional objectives, such as the entropy metric proposed in [6].

Remark 7.3 When $E[\phi(k)]$ is not constant, we can consider other impact metrics such as the sensitivity of the H_∞ gain.

Example 1
Consider the linear system described by

$$A = \begin{bmatrix} 0.7 & -0.5 & 0 \\ 0.2 & 0.8 & 0.3 \\ 0.4 & 0.2 & 0.7 \end{bmatrix}, \; B = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, C = I, \quad K_T = -[0.14, 0.17, 0.16]$$

where K_T is an LQR control. Suppose that an adversary gains access to sensors 1 and 2 and injects a sensor bias attack $\phi = [1, 1, 0]^\top$. We assume that the system possesses an MTD strategy that selects between a set of controllers $K_1 = -[0, 0.17, 0.6]$, $K_2 = -[0.14, 0, 0.16]$, $K_3 = -[0.14, 0.17, 0]$. In total we have 3 possible control gains that are randomly selected at each time instant. Solving Problem 1, we found the switching probability distribution $p = [0.91, 0.04, 0.05]$. Figure 7.13 illustrates how switching among controllers can help to mitigate the effects of the attack by decreasing the deviation caused by the adversary. We use $\|x(k)\|$ to measure the total state deviation at each time instant. Notice that MTD comes with a performance cost by decreasing the convergence rate to the equilibrium, but it decreases the total state deviation.

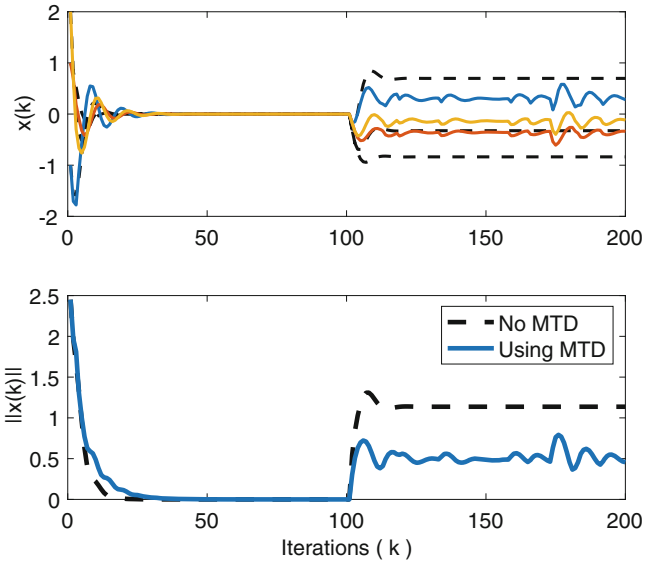

Fig. 7.13 States and energy of a linear system with an MTD that switches among three different control strategies (solid line), and with a fixed LQR control (dashed). Clearly, MTD decreases the deviation caused by the adversary at the cost of performance degradation

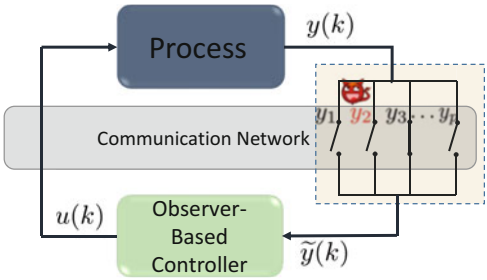

Fig. 7.14 MTD scheme for sensor switching. Each sensor can be connected (transmit data at a specific time instant) or disconnected (not transmitting)

7.4.2 MTD in Sensors

In this case, the MTD mechanism can arbitrarily break the communication between a subset of sensors and the controller at any time k, as depicted in Fig. 7.14. For instance, suppose sensor y_2 is compromised. If the probability that the communication link between y_2 and the controller exists is low, then the amount of fake information received by the controller (or estimator) will decrease and the effects of that attack in the control command may be mitigated.

Suppose we have m sensors and the communication link between any sensor and the controller may be active or inactive. Let $\mathscr{C} = \{C_1, C_2, \ldots, C_{n_s}\}$ be the desired set of matrices that combine active or inactive sensors. Let $\theta(k) \in \mathbb{Z}_+$ be the index of the output modes at the kth time instant. Let $\Theta = \{\theta(0), \theta(1), \ldots\}$ denote the switching logic that changes among different sensors subsets. The output is then given by $\widetilde{y}(k) = C_{\theta(k)}x(k)$, where $C_{\theta(k)} \in \mathscr{C}$. Therefore, the linear system in (7.13) becomes

$$x(k+1) = (A + BKC_{\theta(k)})x(k) = G_{\theta(k)}x(k). \tag{7.19}$$

Notice that (7.15) and (7.19) are similar, and the asymptotic stability of (7.19) can be guaranteed if conditions in Theorem 7.7 are satisfied for $G_{\theta(k)}$.

Similar to the case with switching actuators, we will assume that each sensor is active with probability p_i, for $i = 1, \ldots, m$, such that we can define the matrix $\boldsymbol{P} = diag(p_1, p_2, \ldots, p_m)$. To facilitate the analysis, we can define $\mathscr{S}(k)$ as the diagonal matrix with elements $s_{ii}(k) = 1$ if sensor i is active at the instant k, and 0 otherwise. When the system is subject to a sensor attack $\phi(k)$, we can rewrite (7.19) as

$$x(k+1) = (A + BKS(k)C)x(k) + BKS(k)\phi(k),$$

where C is the output matrix without MTD and $S(k)C = C_{\theta(k)}$. Notice that $E[S(k)] = \boldsymbol{P}$, such that $\bar{C} = E[S(k)C] = \boldsymbol{P}C$ and $\bar{G} = A + BK\bar{C}$. The expected state dynamics are then given by

$$\bar{x}(k+1) = \bar{G}\bar{x}(k) + BK\boldsymbol{P}\bar{\phi}.$$

Now, we can formulate an optimization problem that aims to find $\boldsymbol{P}$ that minimizes the impact of the attack while preserving performance conditions $\mathscr{F}(A, B, C, K, \boldsymbol{P}) < \beta$ (e.g., expected spectral radius $\rho(\bar{G})$) as follows:

Problem 2

$$\begin{aligned} &\min_{p_1, p_2, \ldots, p_{n_s}} \|(I - \bar{G})^{-1} B K \boldsymbol{P}\| \\ &s.t. \\ &\mathscr{F}(A, B, C, K, \boldsymbol{P}) < \beta \\ &0 \leq p_i \leq 1, \quad \text{for all } i. \end{aligned} \tag{7.20}$$

Example 2

Suppose A, B are the same from example 1, but now the system has 4 sensors, with output matrix and control gain given by

$$C \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad K = -[0.14, 0.17, 0.16, 0.13].$$

Solving Problem 2 for $\mathscr{F} = \rho(\bar{G})$ and $\beta = 0.92$ we obtain $p = [0.06, 0.11, 0.07, 0.2]$. Figure 7.14 illustrates how MTD strategies can decrease the impact caused

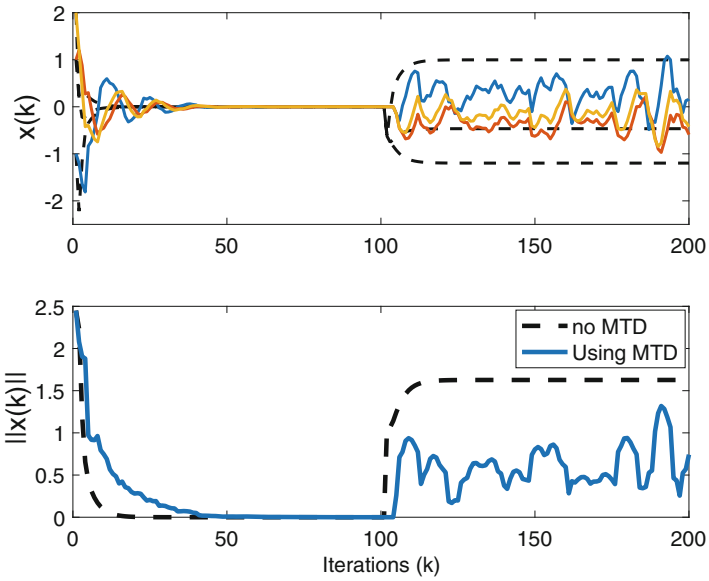

Fig. 7.15 States and energy of a linear system with an MTD with sensor switching and $p = [0.06, 0.11, 0.07, 0.2]$ (solid line), and without MTD (dashed lines). MTD mitigates the deviation caused by the adversary

by an adversary that injects an attack in all sensors $\phi = [1, 1, 1, 1]^\top$. Dashed lines correspond to the case without MTD (Fig. 7.15).

7.5 Conclusions and Future Directions

In this chapter, we have proposed an MTD strategy that randomly switches between different communication topologies in order to mitigate the deviation caused by an adversary. We have identified the trade-off between MTD and the convergence rate such that a system designer can choose adequate parameters that maintain specific levels of performance. In particular, from our analysis we found out that high connectivity of the graph $\mathscr{G}_T$ describing all possible communications and the low probability p play an important role in making the system more resilient to cyber-attacks with good convergence rate. We have also introduced two MTD strategies for more general feedback-control systems and we have proposed optimization problems that allow us to find the optimal probability distribution for the random switching mechanism.

There are many research directions that can be derived from the work presented in this chapter. In future work, we will consider heterogeneous probabilities for the multi-vehicle problem and find a relationship between the topology $\mathscr{G}_T$ and the matrix $\boldsymbol{P}$. Besides, we will consider more realistic models of multi-vehicle systems that include collision avoidance control, actuator saturation, and more complex dynamics. Finally, we will study how our proposed random MTD can affect anomaly detection mechanisms and design detection strategies that can leverage the use of MTD for CPS.

Acknowledgement This work was supported by the Air Force Office of Scientific Research under award number FA9550-17-1-0135.

References

1. S. Dadras, R.M. Gerdes, R. Sharma, Vehicular platooning in an adversarial environment, in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security* (ACM, New York, 2015), pp. 167–178
2. K.R. Davis, K.L. Morrow, R. Bobba, E. Heine, Power flow cyber attacks and perturbation-based defense, in *Proceedings of the IEEE Third International Conference on Smart Grid Communications (SmartGridComm), 2012* (IEEE, Piscataway, 2012), pp. 342–347
3. M. Dunlop, S. Groat, W. Urbanski, R. Marchany, J. Tront, Mt6d: a moving target ipv6 defense, in *Proceedings of the Military Communications Conference, 2011-Milcom 2011* (IEEE, Piscataway, 2011), pp. 1321–1326
4. P. Erdös, A. Rényi, On random graphs, I. Publ. Math. Debr. **6**, 290–297 (1959)
5. S. Jajodia, A.K. Ghosh, V. Swarup, C. Wang, X.S. Wang, *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*, vol. 54 (Springer, New York, 2011)

6. A. Kanellopoulos, K.G. Vamvoudakis, Entropy-based proactive and reactive cyber-physical security, in *Proactive and Dynamic Network Defense*, ed. by C. Wang, Z. Lu. Advances in Information Security, vol. 74 (Springer, Cham, 2019). https://doi.org/10.1007/978-3-030-10597-6_3
7. S. Kar, J.M.F. Moura, Sensor networks with random links: topology design for distributed consensus. IEEE Trans. Signal Process. **56**(7), 3315–3326 (2008)
8. T. Kopfstedt, M. Mukai, M. Fujita, C. Ament, Control of formations of UAVs for surveillance and reconnaissance missions. IFAC Proc. Vol. **41**(2), 5161–5166 (2008)
9. H. Lin, P.J. Antsaklis, Stability and persistent disturbance attenuation properties for a class of networked control systems: switched system approach. Int. J. Control **78**(18), 1447–1458 (2005)
10. H. Lin, P.J. Antsaklis, Stability and stabilizability of switched linear systems: a survey of recent results. IEEE Trans. Autom. control **54**(2), 308–322 (2009)
11. S. Öncü, J. Ploeg, N. van de Wouw, H. Nijmeijer, Cooperative adaptive cruise control: network-aware analysis of string stability. IEEE Trans. Intell. Transp. Syst. **15**(4), 1527–1537 (2014)
12. Z.-H. Pang, G.P. Liu, Z. Dong, Secure networked control systems under denial of service attacks. IFAC Proc. Vol. **44**(1), 8908–8913 (2011)
13. S.S. Pereira, A. Pagès-Zamora, Mean square convergence of consensus algorithms in random WSNs. IEEE Trans. Signal Process. **58**(5), 2866–2874 (2010)
14. J. Ploeg, D.P. Shukla, N. van de Wouw, H. Nijmeijer, Controller synthesis for string stability of vehicle platoons. IEEE Trans. Intell. Transp. Syst. **15**(2), 854–865 (2014)
15. M. Quaritsch, K. Kruggl, D. Wischounig-Strucl, S. Bhattacharya, M. Shah, B. Rinner, Networked UAVs as aerial sensor network for disaster management applications. e & i Elektrotechnik und Informationstechnik **127**(3), 56–63 (2010)
16. M.A. Rahman, E. Al-Shaer, R.B. Bobba, Moving target defense for hardening the security of the power system state estimation, in *Proceedings of the First ACM Workshop on Moving Target Defense* (ACM, New York, 2014), pp. 59–68
17. W. Ren, R.W. Beard, *Distributed Consensus in Multi-Vehicle Cooperative Control* (Springer, London, 2008)
18. C. Suthaputchakun, Z. Sun, M. Dianati, Applications of vehicular communications for reducing fuel consumption and CO_2 emission: the state of the art and research challenges. IEEE Commun. Mag. **50**(12), 108–115 (2012)
19. D. Swaroop, J.K. Hedrick, String stability of interconnected systems. IEEE Trans. Autom. Control **41**(3), 349–357 (1996)
20. J. Tian, R. Tan, X. Guan, T. Liu, Hidden moving target defense in smart grids, in *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids* (ACM, New York, 2017), pp. 21–26
21. J. Valente, A.A. Cárdenas, Using visual challenges to verify the integrity of security cameras, in *Proceedings of the 31st Annual Computer Security Applications Conference*, ACSAC 2015, New York (ACM, New York, 2015), pp. 141–150
22. H. Wang, Q. Jia, D. Fleck, W. Powell, F. Li, A. Stavrou, A moving target DDoS defense mechanism. Comput. Commun. **46**, 10–21 (2014)
23. S. Weerakkody, B. Sinopoli, Detecting integrity attacks on control systems using a moving target approach, in *Proceedings of the IEEE 54th Annual Conference on Decision and Control (CDC)* (IEEE, Piscataway, 2015), pp. 5820–5826
24. J. Willmann, F. Augugliaro, T. Cadalbert, R. D'Andrea, F. Gramazio, M. Kohler, Aerial robotic construction towards a new field of architectural research. Int. J. Archit. Comput. **10**(3), 439–459 (2012)
25. D. Xie, S. Wang, Consensus of second-order discrete-time multi-agent systems with fixed topology. J. Math. Anal. Appl. **387**(1), 8–16 (2012)
26. Y. Zhang, Y.-P. Tian, Consentability and protocol design of multi-agent systems with stochastic switching topology. Automatica **45**(5), 1195–1201 (2009)