IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 17, 2022, accepted April 27, 2022, date of publication May 3, 2022, date of current version May 9, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3172350

Containment Control of Multiagent Systems Subject to Denial of Service Attacks

SIDDIG M. ELKHIDER[1], SAMI EL-FERIK[1,2], AND ABDUL-WAHID A. SAIF[1,2]
[1]Interdisciplinary Center of Smart Mobility and Logistics, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[2]Control and Instrumentation Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

Corresponding author: Siddig M. Elkhider (siddig.elnaiem@kfupm.edu.sa)

This work was supported by the King Fahd University of Petroleum and Minerals.

ABSTRACT This article proposes a secure containment control of multi-agent systems under cyber attacks. Multiple Unmanned Aerial Vehicle Systems (UAVs) are considered in this article. The suggested approach considers denial of service (DoS) attacks, containment control of multiple UAVs, and designs a strong steering approach as well as a secure middleware for data sharing and exchange. A combination of graph theory and L1 adaptive control is utilized to ensure efficient steering and cooperation. The data distribution services (DDS) middleware handles data transfer among all the UAVs, which solves the interoperability challenge when interacting with several UAVs from various platforms and can be regarded as an enhanced security strategy depending on its quality of service (QoS). The L1 controller is used to stabilize the dynamic model of each UAV, while the graph method is used for the containment of multi UAVs. The linear matrix inequalities (LMIs) control is designed as a robust level of security to handle the influence of the DoS attack. Simulation results are utilized to validate and demonstrate the suggested technique's performance under the criteria mentioned before.

INDEX TERMS Containment control, cyber attacks, unmanned aerial vehicle system, publish-subscribe middleware.

I. INTRODUCTION

Multi-agent systems have seen widespread application in recent years [1]. Multi-UAV systems are distributed systems having more than one autonomous agent that may work together to fix challenging tasks with great robustness, reliability, and efficiency. One of the most interesting research topics in multi-agent systems is multi-UAV containment-formation control, which has a wide range of applications. Agents must exchange information (e.g., speed, and position) to keep the formation's topology. Controlling the containment-formation can be done in a variety of ways: behavior-based [2]–[4], virtual-based [5]–[7], and leader-following [8]–[10]. A multi-UAV containment-formation control can now be built for military, recreational, personal, and other purposes. Recently, more unmanned aerial vehicles are being hacked because more of them are being made that have computers integrated into their operations. This is making it harder for the military to defend its systems against cyber-attacks. This is important because it means that many military bases could potentially be under attack from the air. This is a big threat because if the UAVs can't defend the military bases, then they could potentially lose the war. This issue is hard to overcome because the military isn't even close to being able to fight against these cyber-attacks. If we can't win against simple hacking and cyber-crime, then we certainly can't win a war against cyber-attacks from other countries. These hacking attempts are becoming more common because of recent technological advances. These technological advances have made it easier for hackers to create new ways to hack systems. This is making it easier for the systems to be compromised. In the past, hacking a computer system would take extensive knowledge about coding and programming. Now, it can be done with a simple algorithm. One of the biggest things that the researchers need to do is to be sure that these UAVs are secure from cyber-attacks. If we can't do this, then it could mean a loss in the war which would make a lot of people lose their lives. An event-triggered control concerning DoS attacks has been studied in [11]. The authors have been developed a secure event triggering method that can handle a certain amount of packet damages caused by DoS attacks. The multi-agents

The associate editor coordinating the review of this manuscript and approving it for publication was Zheng Chen.

secure control in the face of DoS attacks has been introduced in [12], [13]. The authors in [12] developed a fault-tolerant approach based on coupling an event-triggered with a back-stepping approach, while the authors in [13] proposed a decentralized event-triggered strategy with a fixed topology to ensure system cooperation in the face of mode-switching denial-of-service attacks. The authors in [14] reviewed recent research on data integrity and availability attacks as a basis for information security. The multi-agents secure formation control with respect to DoS attacks has been addressed in [15], [16]. In [15], a secure formation of multiple mobile robots has been proposed, the authors developed a secure controller considering that the DoS attacks affect the multiple mobile robots' formation protocol. While in [16], a nonlinear multi-agent system's formation control under DoS attacks has been introduced. The authors have been built their work based on [17] by considering a fixed topology between the agents and the agents facing some DoS attacks. In [18]–[20], the authors developed a new methodology for multi-UAVs' containment-formation control utilizing publish-subscribe middleware. The publish-subscribe middleware was designed to address information leakage problems between the multi-UAVs, and system integration of various UAV systems. Consequently, the publish-subscribe middleware architecture dramatically increased robustness. Scientists are becoming more interested in the multi-agent system's security, as demonstrated by the previous research study. The following conclusions can be drawn from the literature review:

- Unfortunately, most of the available multi-agent system's secure consensus research has mainly focused on identifying the attacks or developing classical control to overcome the attacks with a limited study on the applications of multi-agent systems' consensus.
- The presence of cyber-attacks may have a significant impact on the multi UAV systems' performance.
- There is a scarcity of using the middleware as a secure level to solve data loss issues between multiple UAVs and the interoperability issues that occur with different UAV platforms.

This study presents a method addressing all of the points raised above. The following are meaningful contributions of this paper:

- A reliable guidance architecture for safe containment control of multiple UAVs has been proposed.
- To tackle the effects of cyber-attacks, a robust security level approach is designed.
- Publish-Subscribe middleware has been developed to provide further cyber security level and exchange of data.

The rest of the paper is arranged as follows. The preliminaries of publish-subscribe middleware, DoS attacks, and quadrotor dynamics are addressed in section 2. The secure containment control of multiple UAVs utilizing the L1 approach and Linear Matrix Inequalities (LMIs) are discussed in section 3. Section 4 and section 5 present and discuss the simulation results. Finally, the conclusions, as well as the final recommendations have been noted in section 6.

II. PRELIMINARIES

This section contains some preliminary on publish-subscribe middleware, DoS attacks, graph theory techniques, and quadrotor dynamics.

A. PUBLISH SUBSCRIBE MIDDLEWARE

Data distributed services is widely recognized as the appropriate publish-subscribe middleware for UAVs' containment control. Because of its capacity to manage data generated by real-time mission-critical and publication-subscription systems, a publish-subscribe structure encourages flexible and dynamic loose coupling between the data architecture. DDS-based systems can easily be adapted and applied to different conditions and criteria. In addition, a publish-subscribe structure is where multiple subscribers and publishers share highly typed information across a common topic. The reliable quality of service model manages the communication. Some of these QoS are:

- **Presentation**: Manage how the middleware presents the information received by the subscriber.
- **Reliability**: Indicates the middleware must transmit data that have been missing due to network failure. There are two choices for reliability: BEST EFFORT (do not transmit the lost data) or RELIABLE (transmit the lost data).
- **Time-Based-Filter**: Confirm the minimum time duration between the current information and the future information received by the subscriber.
- **History**: Indicates whether or not data receipted or transmitted by a publisher would be kept for a subscriber. History can be configured in two ways: KEEP ALL and KEEP LAST. The first option does not store an infinite amount of data.
- **Deadline**: Sets the maximum period for specimens to arrive for subscribers.
- **Lifespan**: determines for how long the middleware will accept the validity of the information sent by the publisher.
- **Ownership**: Gets to decide whether or not a subscriber would receive new samples were collected from different publishers at the same time. There are two types of ownership: EXCLUSIVE and SHARED.
- **Resource-Limits**: Sets the memory space that a publisher or subscriber could assign for storing information in cache memory.

B. DDS VS. OTHER MIDDLEWARE TECHNOLOGIES

- **DDS vs. Sockets API** The sockets application programming interface (API) is a client-server, point-to-point, connection-oriented network. It requires servers and clients to know the location of each other

for communication. It varies greatly from the DDS publish-subscribe framework. With DDS it simplifies the design of distributed systems. Regardless of the hardware architecture or operating system, DDS offers a common API. DDS performs remote endpoint detection and management. DDS manages the communication behavior details such as durability, reliability, historical information storage, identification of deadline errors, and more. All of these are functions that should not be coded, they are available through the simple DDS.

- **DDS vs. CORBA** Common Object Request Broker Architecture (CORBA) and DDS middleware have almost the same foundations as the OMG open standard, specifically, in the solid kind of safety that both technologies provide. CORBA is a client-server network that uses a remote invocations procedure. CORBA uses an Object Request Broker (ORB) to handle the communications and to provide an abstraction layer. Servers and clients need to know each other for communication.

C. DENIAL OF SERVICE (DoS) ATTACKS

Denial-of-service (DoS) is a cyber-attack in which a server or network resource is unable to handle a large number of requests, effectively crippling the system. This attack can be done by either exploiting a vulnerability in an application or networking protocol or by simply overwhelming a target with an enormous volume of requests. What constitutes ''large'' and ''enormous'' volumes of requests typically depends on the type and size of the targeted system. In general, this type of attack may be executed using any type of malware that is capable of flooding the targeted system with one or more types of interactions. A denial of service attack is an attempt to make a machine or network resource unavailable by overwhelming it with requests. For example, can keep a car's windows open by disabling window systems [21]. Nonetheless, denial of service attacks on microgrids can result in a blackout [22], [23]. A denial of service attack has been used in recent years to attack drone networks and other systems. For example, in 2017, hackers managed to carry out a DoS attack on Colombian drone manufacturer DJI. The recent increase in cyberattacks on drones has made it very difficult for these flying devices to be used safely without being hacked. Another example, in 2017, the Federal Aviation Administration (FAA) reported that ''a swarm of drones disrupted air traffic control operations around New York City's JFK airport for about an hour on January 7th, 2018''. This is an example of a denial-of-service attack. A denial of service attack may disrupt a multi-agent system's communication by causing containment protocol delays. This manuscript considers that the Denial-of-service attack causes containment protocol delays and we proposed a control method to stabilize and keep the agents in formation positions.

D. QUADROTOR's MODEL

The Euler-Lagrangian formula is used to construct the quadrotor's translational model as follows: [19], [24]

$$\ddot{\Upsilon} = \begin{bmatrix} 0 \\ 0 \\ -g \end{bmatrix} + T \begin{bmatrix} 0 & 0 & \frac{\sum_{i=1}^{4} \Omega_i^2 * k_i}{m} \end{bmatrix}^T - \frac{k_t}{m} \dot{\Upsilon} \tag{1}$$

where the transformation matrix T is as follows:

$$T = \begin{bmatrix} c\psi c\theta & -c\phi s\psi + c\psi s\theta s\phi & s\psi s\phi + c\phi s\theta c\psi \\ s\psi c\theta & c\psi c\phi + s\psi s\theta s\phi & -c\psi s\phi + c\phi s\theta s\psi \\ -s\theta & c\theta s\phi & c\phi c\theta \end{bmatrix} \tag{2}$$

where Υ denotes (x,y,z) position, while yaw, roll, and pitch angles are represented by ψ,ϕ, and θ respectively, g and m denote gravity and mass, k_t denotes the drag coefficient, Ω_i represents the motors' angular velocities, k_i indicates a constant, and $c(.) = cos, t(.) = tan, s(.) = sin$ with conditions of $\phi \neq 90°$ and $\theta \neq 90°$

The quadrotor's rotational model is as follows:

$$\dot{\nu}_2 = \text{diag}(I_x, I_y, I_z)^{-1}(-(\nu_2 \times I\nu_2) - I_R(\nu_2 \times \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}) * (-k_r \nu_2 + \tau + \Omega_1 - \Omega_2 + \Omega_3 - \Omega_4) \tag{3}$$

where ν_2 represents the angular speed, (I_x, I_y, I_z) represents the quadrotor's inertia, I_R indicates the propeller's inertia, $\times$ indicates the cross product, k_r represents the rotational drag, and the torque is indicated by $\tau = [\tau_p,\ \tau_q,\ \tau_r]^\top$.

The quadrotor has the following translational and rotational models:

$$\begin{bmatrix} \tau,\ u \end{bmatrix}^T = \begin{bmatrix} 0 & l & 0 & -l \\ l & 0 & -l & 0 \\ d & -d & d & -d \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} f_1,\ f_2,\ f_3,\ f_4 \end{bmatrix}^T \tag{4}$$

where the force is denoted by u, the forces of upward-lifting are denoted by (f_4, f_3, f_2, f_1), the distance between the center and the motors is indicated by l, and d represents the drag factor. The model provided in Equation (4) is an under-actuated model because the actuation is less than the degree of freedom's number. The under-actuated model given in this research is as follows:

$$\ddot{\eta} = Q(\eta)u + G(\eta, \dot{\eta}) \tag{5}$$

where the input matrix and the control inputs are denoted by u and Q respectively, and the coordinates vector is indicated by η, G represents the dynamic vector. Further information can be found in [19], [24].

III. CONTROL OF MULTIPLE UAVs

A. L1 CONTROLLER

The L1 controller's major feature is its ability to react fast and smoothly, and even the independence of adaptability and robustness. It also secures a time-delay edge and reduces system limitations. When utilizing the L1 controller, the

bandwidth-limited filter design has to be the most complex issue [25].

The mathematical model structure needed for implementing the L1 controller to the rotational dynamics in Equation (3) is described in the following:

$$\begin{aligned} \dot{x} &= A_m x + b(f(t, x(t)) + \omega u_{ad}), \quad x(0) = x_0 \\ y &= c^\top x(t) \end{aligned} \tag{6}$$

where

$$\begin{aligned} & x \triangleq \nu_2, \qquad \text{a known Hurwitz matrix} \triangleq A_m \in \mathbb{R}^{n\times n} \\ & \omega \triangleq I_{\mathrm{M}}^{-1}, \quad b = 1, \quad u_{ad} \triangleq \mathcal{L}_1 \text{ control} \triangleq \tau \\ & I_{\mathrm{M}}^{-1}(-(\nu_2 \times I_{\mathrm{M}}\nu_2) - I_R(\nu_2 \times z_e)\Omega - k_r\nu_2) \\ & \quad \triangleq f(t, x(t)) \\ & c^\top = I_{3\times 3} \end{aligned} \tag{7}$$

Rewrite Equation (6) as described in the following:

$$\begin{aligned} \dot{x} &= A_m x + b(\theta\|x\|_\infty + \sigma + \omega u_{ad}), \quad x(0) = x_0 \\ y &= c^\top x \end{aligned} \tag{8}$$

The predictor state of Equation (8) is as follows:

$$\begin{aligned} \dot{\hat{x}} &= A_m \hat{x} + b(\hat{\theta}\|x\|_\infty + \hat{\sigma} + \hat{\omega} u_{ad}), \quad \hat{x}(0) = x_0 \\ \hat{y} &= c^\top \hat{x} \end{aligned} \tag{9}$$

where the estimated state and estimated output are denoted by $\hat{x} \in \mathbb{R}^n$ and $\hat{y} \in \mathbb{R}^n$ and the estimated parameters are indicated by $\hat{\sigma}$ and $\hat{\theta}$

The error definitions are $\tilde{\sigma} = \hat{\sigma} - \sigma$, $\tilde{x} = \hat{x} - x$, and $\tilde{\theta} = \hat{\theta} - \theta$. The dynamic error is as follows:

$$\dot{\tilde{x}} = A_m \tilde{x} + b(\tilde{\theta}\|x\|_\infty + \tilde{\sigma}), \quad \tilde{x}(0) = 0 \tag{10}$$

The following is the formula for the adaptation law:

$$\begin{aligned} \dot{\hat{\sigma}} &= \dot{\tilde{\sigma}} = \Gamma \mathrm{Proj}(\tilde{\sigma}, -bP\tilde{x}) \\ \dot{\hat{\theta}} &= \dot{\tilde{\theta}} = \Gamma \mathrm{Proj}(\tilde{\theta}, -\|x\|_\infty bP\tilde{x}) \end{aligned} \tag{11}$$

where $\Gamma > 0$ expresses the adaption rate, see [26] for more information, the operator's projection is denoted by Proj. The following expression is satisfied when $P = P^\top > 0$ and $Q = Q^\top > 0$.

$$-Q = PA_m + A_m^\top P \tag{12}$$

Lastly, the adaptive control law is as follows:

$$u_{ad}(s) = -\frac{k}{s}(\hat{\mu}(s) - k_g r(s) + \omega u_{ad}(s)) \tag{13}$$

where the inverse Laplace transform of $\hat{\mu}(s)$ and the reference $r(s)$ is expressed by $\hat{\mu}(t) \triangleq \hat{\theta}(t)\|x\|_\infty + \hat{\sigma}(t)$ and $r(t)$ respectively, and $k_g \triangleq -\frac{1}{c^\top A_m^{-1} b}$ expresses the feed-forward gain. Details of L1 control can be seen in [19], [24], [25].

B. CONTAINMENT CONTROL

- **Containment Objective**

Consider the following multi-agent systems comprised of N agents under DoS attacks affecting the containment protocol:

$$\begin{aligned} \dot{x}_i(t) &= A_i x_i(t) + B_i u_i(t - \tau_d) \\ y_i(t) &= C_i x_i(t) \quad i = 1, 2 \ldots N \end{aligned} \tag{14}$$

where

$$A_i = diagonal(\begin{bmatrix} 0 & 1 \\ a_{21}^1 & a_{22}^1 \end{bmatrix} \ldots . \begin{bmatrix} 0 & 1 \\ a_{21}^n & a_{22}^n \end{bmatrix}),$$
$$B_i = I_n \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}, x_i(t) = \begin{bmatrix} x_{p_i} \\ x_{v_i} \end{bmatrix} and\ \dot{x}_i(t) = \begin{bmatrix} x_{v_i} \\ x_{a_i} \end{bmatrix}$$

Lemma 1: [27]

"A formation is a vector $h = h_p \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \in R^{2N}$. The N agents are in formation h if there are vectors $q, w \in R^N$ such that $(x_p)_i - (h_p)_i = q, (x_v)_i = w, i = 1, \ldots, N$ where subscript p (position) and subscript v (velocity) are components of x_i".

Therefore, the following formula is used to compute the vehicles' error:

$$e_i = -\frac{1}{|J_i|}\sum_{j\in J_i}(x_j - h_j) + (x_i - h_i) \quad i = 1, \ldots, N. \tag{15}$$

We are looking for a feedback control K_i steers the UAVs into the configuration h utilizing Laplacian $L = L_g \otimes I_N$ and achieving the given objective.

$$\lim_{t\to\infty} ||x_i - h_i|| = q, \forall i \in N \tag{16}$$

then by substituting the containment protocol $u_i(t - \tau_d) = K_i L(x_i - h_i - \tau_d)$ into Equation (14) we obtain:

$$\begin{aligned} \dot{x}_i(t) &= A_{1_i} x_i(t) + B_{1_i} K_i L(x_i - h_i - \tau_d) \\ y_i(t) &= C_{1_i} x_i(t) \qquad i = 1, 2 \ldots N \end{aligned} \tag{17}$$

with $C_{1_i} = I_N \otimes C_i$, $B_{1_i} = I_N \otimes B_i$, *and* $A_{1_i} = I_N \otimes A_i$.

- **Containment Design**

The design of the control gains K_i for each agent i using LMI approaches is discussed in this section.

Lemma 2: The containment for each agent i is asymptotically stable, if there exist matrices $P_1 > 0$, $P_2 > 0$, $S > 0$, and $K > 0$ such that:

$$\Gamma_1 = \begin{bmatrix} \bar{P}^T\bar{A} + \bar{A}^T\bar{P} + \bar{S}_1 & \bar{P}^T\bar{B}_1 \\ \bar{B_1}^T\bar{P} & \bar{S}_2 \end{bmatrix} < 0 \tag{18}$$

where

$$\bar{A} = \begin{bmatrix} A_1 & 0 \\ 0 & -I \end{bmatrix}, \ \bar{B}_1 = \begin{bmatrix} 0 & B_1 \\ 0 & 0 \end{bmatrix}, \text{and } \bar{S}_1 = \begin{bmatrix} S & 0 \\ 0 & 0 \end{bmatrix}$$
$$\bar{S}_2 = \begin{bmatrix} -S - C_1^T K^T P_2 K C_1 & C_1^T K^T P_2 \\ P_2 K C_1 & -P_2 \end{bmatrix}$$
$$\bar{P} = \begin{bmatrix} P_1 & 0 \\ -P_2 K C_1 & P_2 \end{bmatrix}$$

The close loop of the system is asymptotically stable, if there exist matrices $P_1 > 0$,$S > 0$ such that:

$$\begin{bmatrix} A_1^T P_1 + P_1 A_1 + S & P_1 B_1 KC \\ * & -S \end{bmatrix} < 0 \qquad (19)$$

The benefit of lemma 2 is the separation of matrices (system, controller gain, and Lyapunov), and the non-convex characterization will let us find K_i by tuning matrix $P_2 > 0$. Then the control gain matrix can be obtained by: $K_i = P_{2_i}^{-1} S_i$.

Proof: *See Appendix A*

IV. SIMULATION RESULTS

Simulation studies have been performed in MATLAB utilizing a group of 14 UAVs. The DDS middleware is utilized, as well as LMI, graph theory, and L1 controller. The UAV parameters utilized in this study are shown in Table 1 [24].

TABLE 1. The quadrotor characteristics.

Symbol	Value/Unit	Properties
m	0.52 kg	Mass
k_t	0.95	Drag's Translational
L	0.205 m	Arm Length
k_r	0.105	Drag's Rotational
g	9.8 m/s^2	Gravity Acceleration
I_R	3.36×10^{-5} kg $\cdot$ m^2	Propeller Inertia
d	7.5×10^{-7}	Ratio of Drag & Thrust
I_z	0.0129 kg $\cdot$ m^2	Inertia of z-axis
I_y	0.0069 kg $\cdot$ m^2	Inertia of y-axis
I_x	0.0069 kg $\cdot$ m^2	Inertia of x-axis

The controller parameters are set to be $\tau_d = 0.1$, $k_d = 10$, $k_p = 10$ and $\gamma = 10^6$. The communication network between multi-UAVs is shown in Figure 1, and the interaction among the publishers and subscribers must satisfy a group of QoS policies (Table 2).

In the simulation of containment control, the following scenarios were considered:

- **UAVs containment without cyberattacks:** In the first scenario, we supposed fourteen UAVs model without protocol time delay produced by DoS attacks. Figures 2–6 demonstrate how a set of fourteen unmanned aerial vehicles (UAVs) may establish a certain topology in 2D space without the effect of the DoS attacks. The same results are obtained without DoS attacks when we compared our proposed method with the control method in [27].
- **UAVs containment under cyberattacks:** In the second scenario, we supposed fourteen UAVs model with protocol time delay produced by DoS attacks. Figures 7–11 show how a group of fourteen unmanned aerial vehicles (UAVs) may establish a certain topology in 2D space under the effect of the DoS attacks.

  Figures 12–13 show multiple UAVs containment under DoS attacks based on the control method in [27].

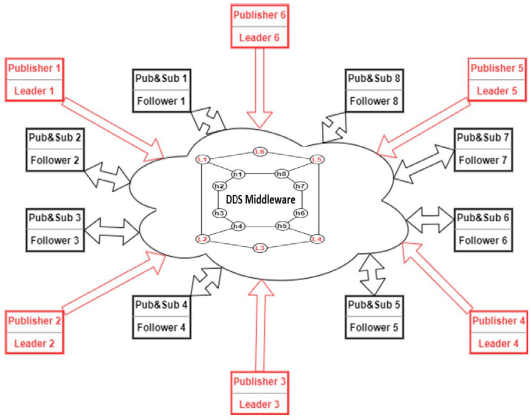

FIGURE 1. DDS communication topology.

TABLE 2. Quality of services (QoS) policies.

QoS Policies	QoS Value
	Subscriber / Publisher
Deadline	Infinite
History	Keep All
Reliability	Reliable
Ownership	Shared

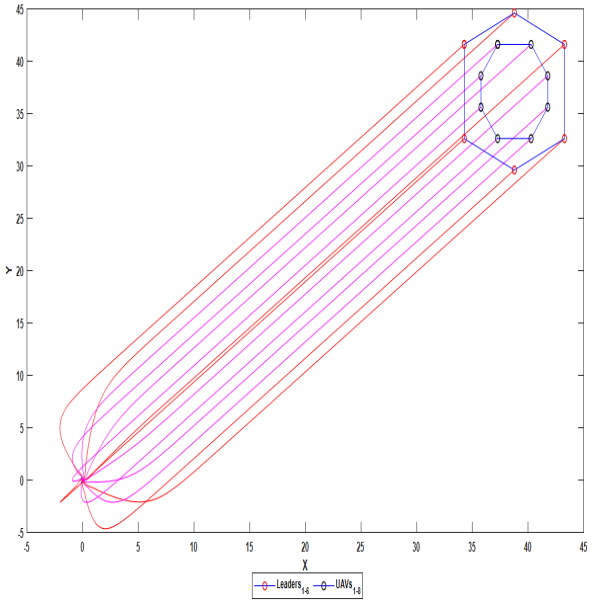

FIGURE 2. UAVs containment at the first position without DoS attacks' effects.

In details, Figures from 2–5 illustrate containment control of fourteen UAVs without the effect of DoS attacks. It is clear that eight of the UAVs were built in an octagon shape inside hexagon red leaders. Figure 6 illustrates the full path of UAVs containment without the DoS attacks' effect. It can be seen that at each time the eight UAVs are constructed in an octagon shape inside hexagon red leaders. Information was exchanged amongst the fourteen UAVs utilizing DDS

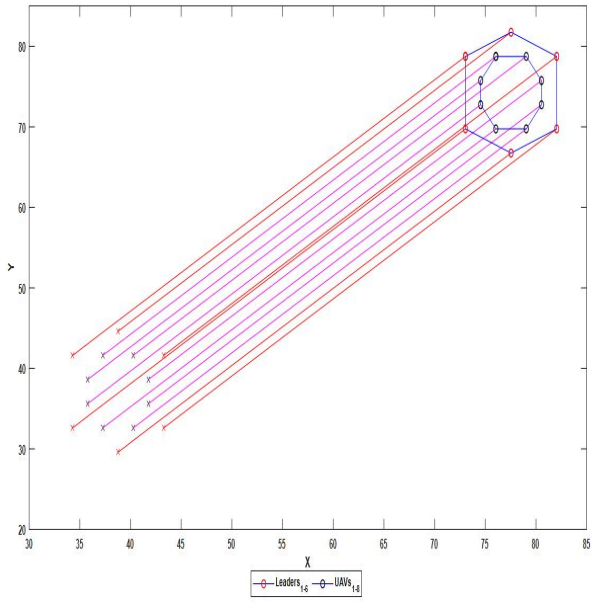

FIGURE 3. UAVs containment at the second position without DoS attacks' effects.

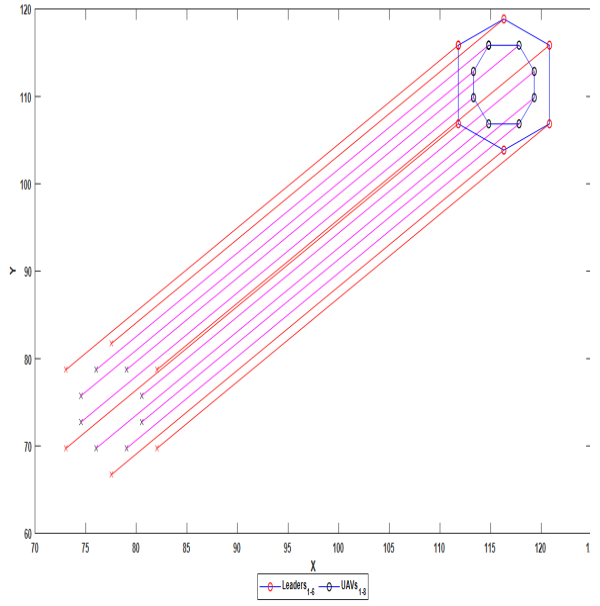

FIGURE 4. UAVs containment at the third position without DoS attacks' effects.

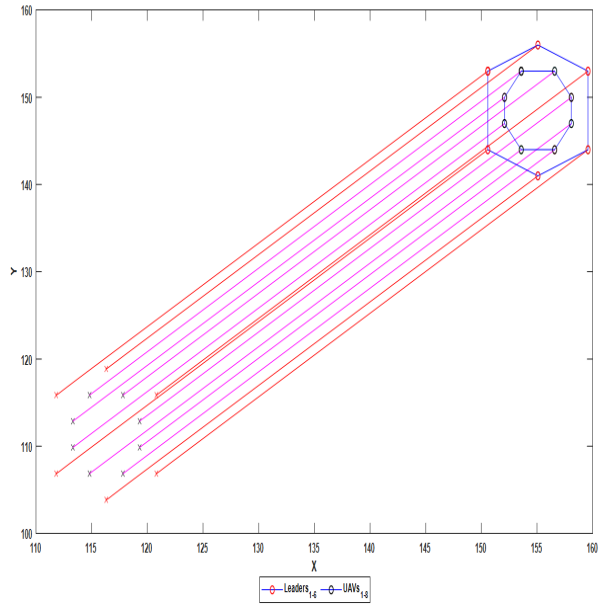

FIGURE 5. UAVs containment at the fourth position without DoS attacks' effects.

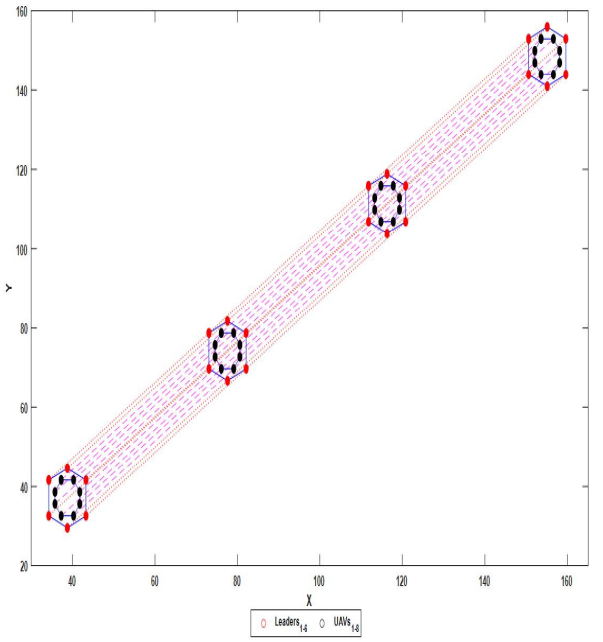

FIGURE 6. Full view map of UAVs containment without DoS attacks' effects.

middleware. When we compared our proposed method to the control method in [27] with the assumption of no DoS attacks, we got identical results.

The Figures from 7–10 show the containment control of fourteen UAVs under the effect of DoS attacks. It is clear that eight of the UAVs were recognized in an octagon shape inside hexagon red leaders. This enormous variation generated by DoS attacks did not influence the system's performance. Figure 11 shows the full map of UAVs containment with the DoS attacks' effect. It can be seen that, at each time the eight UAVs are structured in an octagon shape inside hexagon red leaders. Figures 12–13 show multiple UAVs containment under DoS attacks based on the control method in [27]. It is clear that the control method failed to form six of the UAVs in hexagon shape and drive eight of the UAVs in an octagon shape inside hexagon leaders. Information was transmitted amongst the fourteen UAVs utilizing DDS middleware.

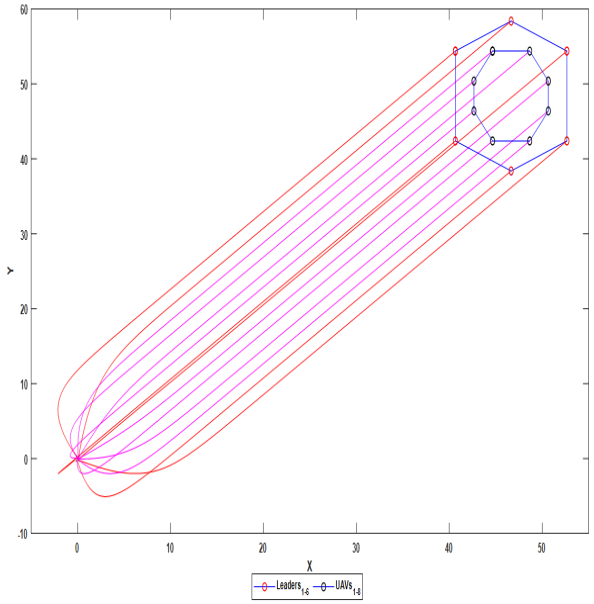

FIGURE 7. UAVs containment at the first position under DoS attacks' effect.

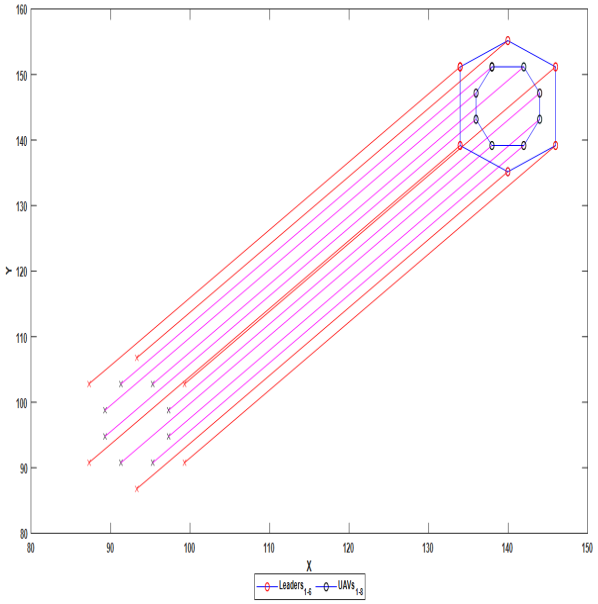

FIGURE 9. UAVs containment at the third position under DoS attacks' effect.

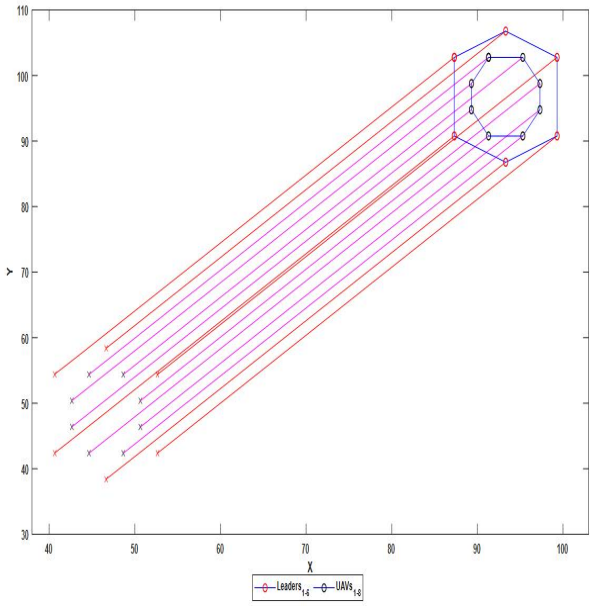

FIGURE 8. UAVs containment at the second position under DoS attacks' effect.

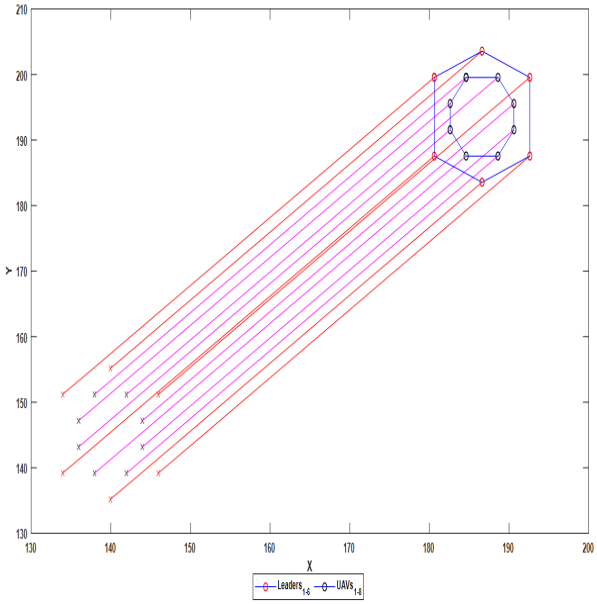

FIGURE 10. UAVs containment at the fourth position under DoS attacks' effect.

V. DISCUSSION SUMMARY

The DDS communication between multiple UAV systems is shown in Figure 1. To make this communication, some of the UAVs considers publishers' UAVs and the others a subscribers' UAVs. A set of QoS criteria must be followed when publishers' UAVs and subscribers' UAVs communicate. The containment control of fourteen UAVs in the absence of DoS attacks is illustrated in Figures 2–5. Eight of the UAVs have been positioned in formation shape within the space delineated by the six UAV leaders. The whole path of UAV containment without the influence of DoS attacks is depicted in Figure 6. The DDS middleware is used to facilitate information transmission between the UAVs. A comparison of our proposed method to the control method in [27] is made, which gave the same results in the absence of DoS attacks. The containment control of multiple UAVs under the effect of DoS attacks is shown in Figures 7–10. Some of the UAVs are identified as being in the shape of an octagon inside hexagon shape delimited by other UAVs. The whole map of UAV containment with the effect of DoS attacks is shown in

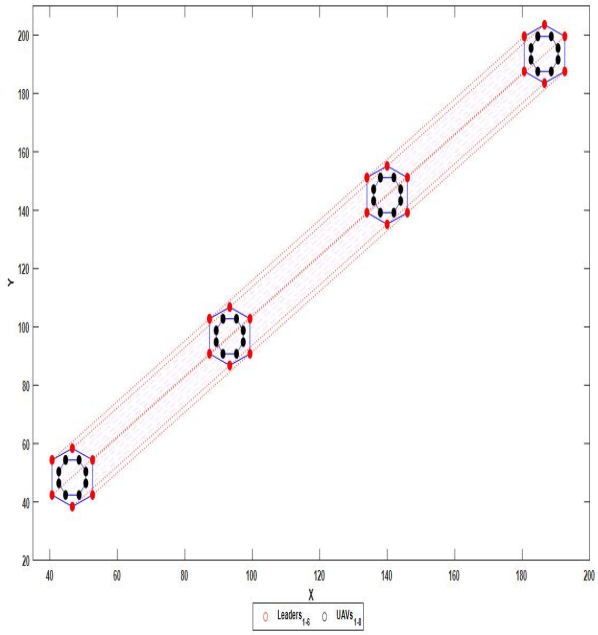

FIGURE 11. Full view map of UAVs containment under DoS attacks' effect.

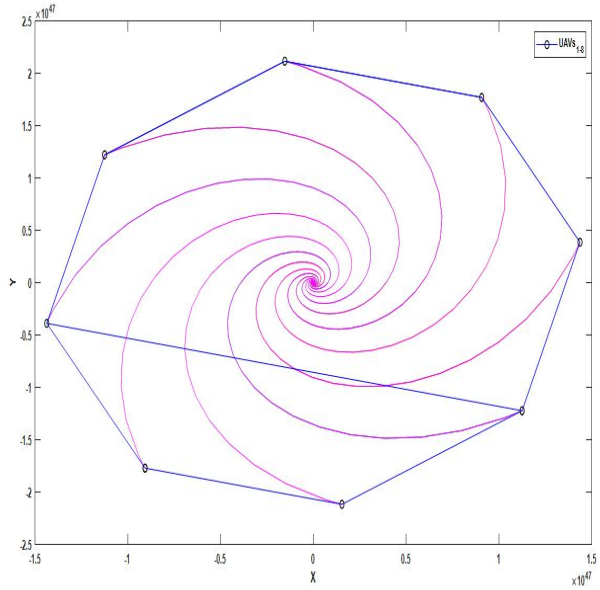

FIGURE 12. UAVs containment at the first position under DoS attacks' effect based on the method in [27].

Figure 11. Multiple UAVs' containment control based on the control approach described in [27] with the influence of DoS attacks is illustrated in Figures 12–13. The control strategy clearly failed to form six of the UAVs into hexagons and drive eight of the UAVs into octagons inside hexagon leaders. The DDS middleware is used to make data communication between the UAVs easier.

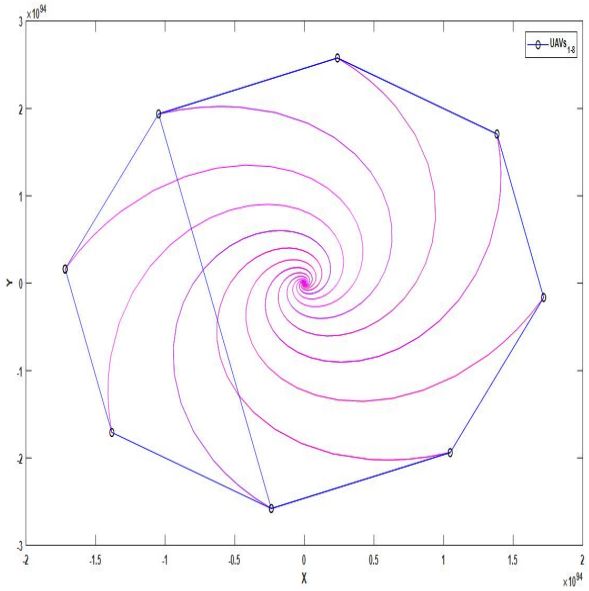

FIGURE 13. UAVs containment at the second position under DoS attacks' effect based on the method in [27].

VI. CONCLUSION

This article proposed a novel architecture for securing multi-UAVs containment control. A combination of DDS middleware, LMI controller, graph theory, and L1 controller is used to establish the containment control of multiple UAVs under cyber attacks. The DDS middleware manages the transmission of data between all the UAVs, which overcomes the interoperability difficulty when communicating with several UAVs from different platforms and can be considered as an additional security strategy that is based on its quality of service. In addition, the LMI controller is used to defeat the time delay caused by DoS attacks. Furthermore, the graph theory is used to maintain the UAVs containment control, while the L1 controller is used to stabilize the dynamic model of each UAV system. The combination technique is performed effectively when confronted with DoS attacks. The DDS middleware, LMI controller, graph theory, and L1 adaptive controller significantly improved overall performance based on the numerical simulation results.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of King Fahd University of Petroleum and Minerals and the Interdisciplinary Research Center of Smart Mobility and Logistics.

APPENDIX A STABILITY ANALYSIS OF MULTI-AGENT SYSTEMS WITH INPUT TIME DELAY

Consider the following multi-agent systems with input time delay

$$\begin{aligned} \dot{x}_i(t) &= A_i x_i(t) + B_i u_i(t - \tau_d) \\ y_i(t) &= C_i x_i(t) \quad i = 1, 2 \ldots N \end{aligned} \tag{20}$$

By substituting the static output feedback controller $u_i = K_i y_i(t)$ into Equation (20) we obtained the following close loop system

$$\dot{x}_i(t) = A_i x_i(t) + B_i K_i C_i x_i(t - \tau_d) \tag{21}$$

For simplifying suppose $A_{0_i} = A_i$, $A_{1_i} = B_i K_i C_i$ and $X_i(t) = x_i(t)$.

Then Equation (21) can be rewritten as:

$$\dot{X}_i(t) = A_{0_i} X_i(t) + A_{1_i} X_i(t - \tau_d) \tag{22}$$

By considering a Lyapunov function $V_i(X_i)$,

$$V_i(X_i(t)) = X_i^T(t) P X_i(t) + \int_{t-\tau_d}^{t} X_i^T(\xi) S X_i(\xi) d\xi \tag{23}$$

where $S > 0$ (Lyapunov-Krasovskii)

$$\dot{V}_i(X_i(t)) < 0 \text{ for stability} \tag{24}$$

By taking the derivative for the Equation (23), we get:

$$\dot{V}_i(X_i) = \dot{X_i^T} P X_i + X_i^T P \dot{X}_i + [X_i^T S X_i(t) - X_i^T(t - \tau_d) S X_i(t - \tau_d)] \tag{25}$$

Now, by substituting Equation (22) into Equation (25) we obtain:

$$\begin{aligned}\dot{V}_i(X_i) &= X_i^T A_{0_i}^T P X_i + X_i^T P A_{0_i} X_i + X_i^T(t - \tau_d) A_{1_i}^T P X_i \\ &\quad + X_i^T A_{1_i} P X_i(t - \tau_d) + X_i^T S X_i - X_i^T(t - \tau_d) \\ &\quad \times S X_i(t - \tau_d) \\ &= \begin{pmatrix} X_i^T(t) & X_i^T(t - \tau_d) \end{pmatrix} * \begin{pmatrix} A_{0_i}^T P + P A_{0_i} + S & P A_{1_i} \\ A_{1_i}^T P & -S \end{pmatrix} \\ &\quad * \begin{pmatrix} X_i^T(t) \\ X_i^T(t - \tau_d) \end{pmatrix}\end{aligned}$$

Finally, we will get the linear matrix inequality as follows:

$$\begin{pmatrix} A_{0_i}^T P + P A_{0_i} + S & P A_{1_i} \\ A_{1_i}^T P & -S \end{pmatrix} < 0 \quad \text{which it's LMI 1} \tag{26}$$

The system's close loop is asymptotically stable if we substitute $A_{0_i} = A_i$, $P = P_1$, and $A_{1_i} = B_i K_i C_i$ into Equation (26)

$$\begin{bmatrix} A_i^T P_1 + P A_i + S & P_1 B_i K_i C_i \\ * & -S \end{bmatrix} < 0 \quad \text{which it's LMI 2} \tag{27}$$

proof is completed.

REFERENCES

[1] H. Zhi-Wei, L. Jia-Hong, C. Ling, and W. Bing, "Survey on the formation control of multi-agent system," in *Proc. 31st Chin. Control Conf.*, Jul. 2012, pp. 6092–6098.
[2] M. Xiaomin, D. Yang, L. Xing, and W. Sentang, "Behavior-based formation control of multi-missiles," in *Proc. Chin. Control Decis. Conf.*, Jun. 2009, pp. 5019–5023.
[3] G. Tan, J. Zhuang, J. Zou, and L. Wan, "Coordination control for multiple unmanned surface vehicles using hybrid behavior-based method," *Ocean Eng.*, vol. 232, Jul. 2021, Art. no. 109147.
[4] D. Wang, S. S. Ge, M. Fu, and D. Li, "Bioinspired neurodynamics based formation control for unmanned surface vehicles with line-of-sight range and angle constraints," *Neurocomputing*, vol. 425, pp. 127–134, Feb. 2021.
[5] B. Khaldi and F. Cherif, "Swarm robots circle formation via a virtual viscoelastic control model," in *Proc. 8th Int. Conf. Model., Identificat. Control (ICMIC)*, Nov. 2016, pp. 725–730.
[6] V. Ruchkin, V. Fulin, D. Pikulin, A. Taganov, A. Kolesenkov, and E. Ruchkina, "Heterogenic multi-core system on chip for virtual based security," in *Proc. 8th Medit. Conf. Embedded Comput. (MECO)*, Jun. 2019, pp. 1–5.
[7] R. W. Beard, J. Lawton, and F. Y. Hadaegh, "A coordination architecture for spacecraft formation control," *IEEE Trans. Control Syst. Technol.*, vol. 9, no. 6, pp. 777–790, Nov. 2001.
[8] S. El-Ferik, S. M. Elkhider, and J. Ghommam, "Adaptive containment control of multi-leader fleet of underwater vehicle-manipulator autonomous systems carrying a load," *Int. J. Syst. Sci.*, vol. 50, no. 8, pp. 1501–1516, Jun. 2019.
[9] M. T. Nasir and S. El-Ferik, "Adaptive sliding-mode cluster space control of a non-holonomic multi-robot system with applications," *IET Control Theory Appl.*, vol. 11, no. 8, pp. 1264–1273, 2017.
[10] G. Zhang, W. Yu, J. Li, and X. Zhang, "A novel event-triggered robust neural formation control for USVs with the optimized leader–follower structure," *Ocean Eng.*, vol. 235, Sep. 2021, Art. no. 109390.
[11] C. Peng, J. Li, and M. Fei, "Resilient event-triggering H_∞ load frequency control for multi-area power systems with energy-limited DoS attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 4110–4118, Sep. 2016.
[12] X. Shao and D. Ye, "Fuzzy adaptive event-triggered secure control for stochastic nonlinear high-order MASs subject to DoS attacks and actuator faults," *IEEE Trans. Fuzzy Syst.*, vol. 29, no. 12, pp. 3812–3821, Dec. 2021.
[13] T.-Y. Zhang and D. Ye, "Distributed secure control against denial-of-service attacks in cyber-physical systems based on K-connected communication topology," *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 3094–3103, Jul. 2020.
[14] X. Zhang, Q. L. Han, X. Ge, and D. Ding, "Networked control systems: A survey of trends and techniques," *IEEE/CAA J. Automa. Sinica*, vol. 7, no. 1, pp. 1–17, Jun. 2020.
[15] Y. Yang, Y. Xiao, and T. Li, "Attacks on formation control for multiagent systems," *IEEE Trans. Cybern.*, pp. 1–13, 2021.
[16] S. Wang, S. Zheng, C. Zhao, H. Jian, and H. Li, "Formation control of nonlinear multi-agent systems with actuator and communication attacks," in *Proc. 40th Chin. Control Conf. (CCC)*, Jul. 2021, pp. 2286–2291.
[17] Y. Tang, D. Zhang, P. Shi, W. Zhang, and F. Qian, "Event-based formation control for nonlinear multiagent systems under DoS attacks," *IEEE Trans. Autom. Control*, vol. 66, no. 1, pp. 452–459, Jan. 2021.
[18] S. M. Elkhider, O. Al-Buraiki, and S. El-Ferik, "Publish and subscribe-based formation and containment control of heterogeneous robotic system with actuator time delay," *Appl. Sci.*, vol. 11, no. 19, p. 9145, Oct. 2021.
[19] S. El-Ferik, B. Almadani, and S. M. Elkhider, "Formation control of multi unmanned aerial vehicle systems based on DDS middleware," *IEEE Access*, vol. 8, pp. 44211–44218, 2020.
[20] B. Al-Madani, S. M. Elkhider, and S. El-Ferik, "DDS-based containment control of multiple UAV systems," *Appl. Sci.*, vol. 10, no. 13, p. 4572, Jul. 2020.
[21] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks-practical examples and selected short-term countermeasures," *Rel. Eng. Syst. Saf.*, vol. 96, no. 1, pp. 11–25, 2011.
[22] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, Oct. 2012.
[23] J. Jow, Y. Xiao, and W. Han, "A survey of intrusion detection systems in smart grid," *Int. J. Sensor Netw.*, vol. 23, no. 3, pp. 170–186, 2017.
[24] A. B. Koesdwiady, "Immersion and invariance control design for unmanned aerial vehicle, master thesis, king fahd university of petroleum and minerals (Saudi Arabia)," Tech. Rep., May 2013.
[25] N. Hovakimyan and C. Cao, "L_1 *Adaptive Control Theory: Guaranteed Robustness With Fast Adaptation*, vol. 21. Philadelphia, PA, USA: SIAM, 2010.
[26] J.-B. Pomet and L. Praly, "Adaptive nonlinear regulation: Estimation from the Lyapunov equation," *IEEE Trans. Autom. Control*, vol. 37, no. 6, pp. 729–740, Jun. 1992.
[27] G. Lafferriere, J. Caughman, and A. Williams, "Graph theoretic methods in the stability of vehicle formations," in *Proc. Amer. Control Conf.*, vol. 4, Jun./Jul. 2004, pp. 3729–3734.

SIDDIG M. ELKHIDER received the B.S. degree in computer engineering from El Gezira University, Sudan, and the M.Sc. and Ph.D. degrees in control and instrumentation from the Department of Control and Instrumentation Engineering, KFUPM, Saudi Arabia. He is currently a Postdoctoral Researcher with the Interdisciplinary Center of Smart Mobility and Logistics, KFUPM. His research interests include multiagent systems, cyber attacks, formation control, containment control, control applications, and optimization techniques.

SAMI EL-FERIK received the B.Sc. degree in electrical engineering from Laval University, Quebec, QC, Canada, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Ecole Polytechnique, The University of Montreal, Montreal, QC, Canada. His Ph.D. work, on flexible manufacturing systems modeling and control, was cosupervised with mechanical engineering. After completion of his Ph.D. and postdoctoral positions, he worked with Pratt and Whitney Canada as a Staff Control Analyst at the Research and Development Center of Systems, Controls, and Accessories. He is currently a Professor with the Department of Control and Instrumentation Engineering, KFUPM. He is also the Acting Director of the Interdisciplinary Center of Smart Mobility and Logistics. His research interests include sensing, monitoring, and control with strong multidisciplinary research and applications. His research contributions are in control of drug administration, process control, and control loop performance monitoring, control of systems with delays, modeling and control of stochastic systems, analysis of network stability, condition monitoring, and condition-based maintenance.

ABDUL-WAHID A. SAIF received the B.Sc. degree from the Physics Department, King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, the M.Sc. degree from the Control and Instrumentation Engineering Department, KFUPM, and the Ph.D. degree from the Control and Instrumentation Group, Department of Engineering, Leicester University, U.K. He is currently a Professor with the Department of Control and Instrumentation Engineering, KFUPM. He worked as a Principal Investigator or a Co-Investigator in many internal and external funded projects by KFUPM. He taught several courses in modeling and simulation, digital control, digital systems, microprocessor and micro-controllers in automation, optimization, numerical methods, PLC's, process control, and control system design plus other courses in EE, physics, engineering economics, and programming. He supervised and was a member of the thesis committees of many Ph.D. and M.Sc. students in systems engineering from the Computer Engineering and Electrical Engineering Department. He has published more than 100 papers in reputable journals and conferences, patents, and technical reports. His research interests include simultaneous and strong stabilization, robust control and H_∞ optimization, wire and wireless networked control, time delay systems, and instrumentation and computer control.