Spring 2020

Attack detection and mitigation in mobile robot formations

Arnold Fernandes

Department:

ATTACK DETECTION AND MITIGATION IN MOBILE ROBOT FORMATIONS

by

ARNOLD FERNANDES

A THESIS

Presented to the Graduate Faculty of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

in

ELECTRICAL ENGINEERING

2020

Approved by

Jagannathan Sarangapani, Advisor
Hamidreza Modares, Co-Advisor
Maciej Zawodniok

PUBLICATION THESIS OPTION

This thesis consists of the following articles which will be submitted for publication as follows:

Paper I: Pages 6-66 are intended for submission to a Journal.

Paper II: Pages 67-99 are intended for submission to a Journal.

ABSTRACT

A formation of cheap and agile robots can be deployed for space, mining, patrolling, search and rescue applications due to reduced system and mission cost, redundancy, improved system accuracy, reconfigurability, and structural flexibility. However, the performance of the formation can be altered by an adversary. Therefore, this thesis investigates the effect of adversarial inputs or attacks on a nonholonomic leader-follower-based robot formation and introduces novel detection and mitigation schemes.

First, an observer is designed for each robot in the formation in order to estimate its state vector and to compute the control law. Based on the healthy operation of the robot and its formation, it has been shown that in the case of false data injection (FDI) attack on the actuator of a robot, the state estimation error or residual increases thus indicating the onset of an attack. Next, a functional link neural network is incorporated into the observer to learn the attack input and to minimize its effect by modifying the controller.

Subsequently, the effects of a covert attack are studied by relaxing the assumption that sensors are attack-resilient. It is shown that the residual-based method from Paper 1 is ineffective when the sensors are injected by a signal that modifies the residual in the presence of an actuator attack. Next, an auxiliary system consisting of an observer for each robot, which is not known to the adversary, is introduced to detect covert attacks.

Performance assurance and stability of the formation during healthy and under attack are shown using Lyapunov analysis by relaxing the separation principle. Simulation results verify theoretical results for both FDI and covert attacks.

ACKNOWLEDGMENTS

I would like to thank my advisors Dr. Jagannathan Sarangapani and Dr. Hamidreza Modares without whose support this work would have never been completed. They were patient with me throughout my endeavor. I would especially like to thank Dr. Sarangapani for giving me the opportunity to learn control systems under him and encouraging me throughout the journey. I would like to thank Dr. Maciej Zawodniok for serving on my committee and making valuable suggestions to the thesis.

I would like to thank my family, my grandfather Mr. Joe Michael, mother Mrs. Vincentina Fernandes, father Mr. Anthony Fernandes and sister Miss Shimona Fernandes for being my support system. I express my sincere gratitude for supporting all my life decisions, one of which was pursuing the MS thesis.

During my MS, I have had the opportunity of meeting a lot of wonderful people who have become my dearest friends. I would like to acknowledge them in the order I met them: Priyesh Jani, Utkarsh Raj, Raghu Yelugam, Akhilesh Raj, Chandreyee Bhowmick, George Holmes Jr., Kamna Pal, Weerdhawal Chowghule, Sharon Rodrigues, Joshua Liao, Oboreh Oroghene, Chetan Sulane, Mrs. Havva Malone, Devi Lakshmidevinivas, Meryem Deniz, Abdul Ghafoor, and many more. They have made my MS a wonderful experience. Without them, my life in this humble city would be colorless.

TABLE OF CONTENTS

Page

PUBLICATION THESIS OPTION iii

ABSTRACT iv

ACKNOWLEDGMENTS v

LIST OF ILLUSTRATIONS ix

SECTION

1. INTRODUCTION 1
   - 1.1. ORGANIZATION 4
   - 1.2. CONTRIBUTION 5

PAPER

I. ACTUATOR ATTACK DETECTION AND MITIGATION IN A DYNAMIC MOBILE ROBOT FORMATION 6

   ABSTRACT 6

   1. INTRODUCTION 7
   2. PROBLEM FORMULATION 10
      - 2.1. TRAJECTORY TRACKING USING BACKSTEPPING CONTROL STRUCTURE 11
      - 2.2. FORMATION STABILITY 16
   3. OBSERVER DESIGN FOR ATTACK DETECTION 17
      - 3.1. ATTACK-FREE SCENARIO 23
      - 3.2. ACTUATOR ATTACK SCENARIO 24

4. ACTUATOR ATTACK MITIGATION 26
5. RESULTS AND DISCUSSION 29
5.1. ATTACK-FREE SCENARIO 30
5.2. ATTACK CASE 1 30
5.3. ATTACK CASE 2 32
5.4. ATTACK CASE 3 36
6. CONCLUSION AND FUTURE WORK 39
REFERENCES 40
APPENDICES
A. BOUNDS 44
B. PROOFS 47

II. COVERT ATTACK DETECTION IN A DYNAMIC MOBILE ROBOT FORMATION 67
ABSTRACT 67
1. INTRODUCTION 67
2. PROBLEM FORMULATION 71
3. COVERT ATTACK 75
4. COVERT ATTACK DETECTION 77
4.1. AUXILIARY SYSTEM DESIGN 77
4.2. AUXILIARY SYSTEM TRACKING CONTROLLER DESIGN 79
4.3. AUXILIARY SYSTEM OBSERVER DESIGN 81
5. RESULTS AND DISCUSSION 85
5.1. ATTACK-FREE SCENARIO 86
5.2. COVERT ATTACK CASE 1 89
5.3. COVERT ATTACK CASE 2 92
6. CONCLUSION AND FUTURE WORK 92

REFERENCES 95

APPENDIX 99

SECTION

2. CONCLUSIONS AND FUTURE WORK 100

2.1. CONCLUSION 101

2.2. FUTURE WORK 102

REFERENCES 103

VITA 106

LIST OF ILLUSTRATIONS

Figure Page

PAPER I

1. Formation and communication topology. 11
2. Separation-bearing formation control. 12
3. Attack detection and mitigation scheme. 19
4. Leader-follower formation under actuator attack. 30
5. Attack-free formation trajectories. 31
6. Attack-free tracking errors. 31
7. Attack-free estimation errors. 32
8. Attack case 1. 33
9. Formation trajectories with leader under attack. 33
10. Tracking error norm with leader under attack. 34
11. Estimation error norm with leader under attack. 34
12. Attack case 2. 35
13. Tracking error norm with follower 1 under attack. 35
14. Estimation errors with follower 1 under attack. 36
15. Formation distributed actuator attack mitigation. 37
16. Formation trajectories after attack mitigation. 37
17. Tracking error norm with entire formation under attack. 38
18. Estimation errors after attack mitigation. 38
19. NN weight norms after attack mitigation. 39

PAPER II

1. Leader-follower formation under covert attack. 86
2. Attack-free formation trajectories. 87

3. Attack-free tracking errors. 87
4. Attack-free estimation errors. 88
5. Attack-free auxiliary system tracking errors. 88
6. Attack-free auxiliary system residual. 89
7. Formation trajectories with leader under attack. 90
8. Tracking error norm with leader under attack. 90
9. Actual estimation error norm with leader under attack. 91
10. Falsified estimation error norm with leader under attack. 91
11. Leader attacked auxiliary system residual. 92
12. Formation trajectories with follower 1 under attack. 93
13. Tracking error norm with follower 1 under attack. 93
14. Estimation errors with follower 1 under attack. 94
15. Actual estimation error norm with follower 1 under attack. 94
16. Follower 1 auxiliary system residual under attack. 95

SECTION

1. INTRODUCTION

The need for formation arises from the necessity of deploying multiple robots to accomplish an objective. Mining, space interferometry [29], patrolling, search and rescue [21], mapping, environmental monitoring [24], are applications that require multiple robots. It could be possible to employ a single robot with multiple functionalities to accomplish the task, but adding more features to a single robot would make it bulky and expensive. Additionally, the robot would require more processing power requiring a higher mission time which would eventually translate to a high mission cost [6]. The mission would also have a single point of failure. Futhermore, a single robot cannot make use of distributed data collection schemes to improve system accuracy. It is also hard to adapt this single robot for different applications/scenarios. Therefore, the motivation to employ a group of cheaper, agile robots over a single expensive and heavy robot has become a priority.

A formation controller dictates how a group of robots should behave. Formation control can be centralized, decentralized, or distributed. Formation controllers in the literature can also be classified as behavior-based [1][2], virtual structure, consensus-based [28], neighbor and center reference, and leader-follower [31][9][4]. In behavior-based methods, each robot behaves a certain way in response to its environment consisting of obstacles, goal points, or other robots. For instance, a robot can have a move-to-goal and a move-away-from-obstacle behaviors. In virtual structure approach, all robots maintain a formation by positioning themselves at different points of a virtual geometric structure such as a triangle, a square, a circle.

The consensus-based approach, on the other hand, requires all robots to exchange individual position information with their neighbors and come to an agreement on the final position; a weighted average of the initial position. In the leader-follower strategy, a few robots are assigned the role of leader; while others, are given the role of follower. The objective of the leaders is to follow a reference trajectory, while the goal of the follower is to maintain a fixed distance from the leader while avoiding obstacles. One of the strategies by which a follower tracks its leader is the separation-bearing-based formation control [9], where the follower maintains a fixed separation and relative orientation with respect to its leader. In this effort, leader-follower separation-bearing-based formation control strategy will be considered.

Such a formation of robots (a multi-agent system (MAS))can be viewed as a cyber physical systems (CPS). This would be subject to attacks by an adversary. CPS attacks include false data injection (FDI) [22], replay [23], and others, on the sensors/actuators, blackhole, packet loss, time delay, denial of service (DOS), and so on on the communication links. Literature discussing secure control design in the presence of the aforementioned attacks include [22][23][26][19][13][25]. When it comes to MAS, specifically multi-robot formations it was noticed that attack detection and mitigation schemes are developed for linear, double-integrator, or kinematic robot models. To the best knowledge of the authors, no such work has been attempted for a dynamic, nonholonomic, communication-constrained system like the leader-follower separation-bearing-based formation which is the primary motivation of this thesis. Such a formation is typical in cooperative adaptive cruise control (CACC) or in tank formations.

Detailed work has been done with regards to kinematic control for wheel mobile robots (WMR) [18] and [35]. A dynamic backstepping-based controller for known and unknown dynamics of a single robot was developed in [14] and [15]. For the purpose of learning the unknown robot dynamics online, an artificial neural network (NN) was employed. The effort in [7] deals with the separation-bearing techniques for a kinematic

WMR. The separation-bearing technique is employed when a follower localizes itself with respect to its leader. The work [9] discuss the dynamic backstepping controller for the leader-follower case, employing the separation-bearing technique. This framework was extended to the case where the robot dynamics are unknown [10] and robot state vectors were not completely measurable [11]. Additionally, [8] extends the work to near-optimal adaptive controllers.

Though the leader-follower separation-bearing literature touches almost all the aspects of control, security has not been integrated into the framework nor has the effect of attack. This leaves the formation vulnerable to adversarial inputs from the environment or due to tampering. The effects of such attacks on this formation have not been carried out. A secondary motivation for pursuing the current work is to provide techniques to secure future vehicular transportation systems.

Threats on automated vehicles have been reported. In [5], possible attacks and attack surfaces were introduced. In [27], methods by which self-driving and cooperative self-driving vehicles could be affected by cyber-attacks is highlighted, contrasting the security and privacy measures for self-driving and cooperative self-driving vehicles. In [16], it is shown how one attacked vehicle can effect the efficiency of the entire platoon employing CACC. The paper [33] shows how an adversary could manipulate the data being transmitted from an attacked vehicle to its follower vehicle, which could ultimately lead to a crash. This effort also discusses possible attack detection and attack mitigation strategies. In [34], decision trees are used to detect attacks, and the authors in [12] use a dynamic monitor to collect information at different time instants to detect attacks. The effort in [3] uses trajectory planning to guarantee attack-resiliency in robots.

A robot formation could be destabilized by various attacks. These attacks could be on the actuator, sensor, or communication links. The attacks can also be a combination of one or more attacks. This work consists of two papers which study the effects of adversarial inputs on robot actuators and sensors, their detection and mitigation. The organization of this thesis is presented next.

1.1. ORGANIZATION

This thesis consists of two papers. Paper I discusses a residual-based approach to detect and mitigate an actuator attack for different attack scenarios. Paper II on the other hand discusses the detection of a covert attack when the residual-based approach can no longer be trusted.

In Paper I, under the assumptions that the robot dynamic model was known and the communication networks and the sensors were attack-resilient, the attack detection and mitigation scheme was proposed to secure the leader and follower robots from attacks on the actuator and/or the signals sent from the CPU of the robot to the actuators in case of tampering [5]. This attack-resilient framework was built for nonlinear, nonholonomic leader-follower formation on top of the system designed in [9]. For detecting the attack an observer was designed on every robot in the formation. Based on the residual generated by comparing the robot output vector and the observer output vector the robot checks if it was under attack. If under attack, it activated the attack mitigation scheme; which learned the attack signal and canceled the effect of the attack by increasing the control torque.

In Paper II, the sensor resiliency assumption was relaxed and the scenario where the actuators and sensors of a robot could simultaneously be compromised was considered. The motivation being to study the formation when it was attacked by a smart adversary; one that can attack the actuators while simultaneously modifying the sensor data; thereby staying undetected [32]. The goal of this paper was to design a detection scheme if such a ‘covert’ attack were to occur.

1.2. CONTRIBUTION

In Paper I, a novel observer was designed for each robot in the formation. The observer designed had dynamics similar to the robot but it had a dual tracking objective; to track the assigned leader (if it was a follower robot; the virtual cart if it was a leader robot) as well as to track the robot output vector on the basis of the residual. The observer also computed the control torque estimate. Using Lyapunov analysis, it was shown that this observer-based control torque gave zero tracking and zero estimation errors in the absence of actuator attacks. This information was used to detect attacks (by monitoring the estimation error or residual). Based on the fact that NN's are universal function approximators, a novel attack mitigation scheme was designed by using the attack affected observer tracking error and the residual to tune an NN online such that it learnt the attack signal (assumed to be smooth). This attack signal estimate was used to cancel out the effect of the attack signal at the actuator. Apart from this, the leader backstepping-based control was modified from [10] and [14]. The new leader control has better stability properties (Lyapunov tracking error function is negative definite rather than negative semi-definite).

Paper II was concerned with designing a novel covert attack, which includes an actuator attack combined with a sensor attack, to deceive the residual-based attack detection scheme of Paper I. The purpose of the actuator attack is to destabilize the tracking objective whereas the purpose of the sensor attack is to keep the robot unaware of the actuator attack so that a feedback control/mitigating signal is not asserted. Next a novel attack detector was designed by extending the robot dynamics [30] with an auxiliary system consisting of a linear spring-mass-damper (LSMD) and a torsional spring-mass-damper (TSMD). A filter-tracking error based controller [20] and an observer-based residual was constructed for the auxiliary system which successfully detected the covert attack.

PAPER

I. ACTUATOR ATTACK DETECTION AND MITIGATION IN A DYNAMIC MOBILE ROBOT FORMATION

A. Fernandes*, S. Jagannathan*, H. Modares**

* Department of Electrical & Computer Engineering

Missouri University of Science and Technology

Rolla, Missouri 65409

** Department of Mechanical Engineering

Michigan State University

East Lansing, Michigan 48824

ABSTRACT

In this paper, the effects of actuator attacks and their mitigation on a nonholonomic leader-follower-based robot formation are discussed. The robots use dynamic backstepping-based tracking controllers to achieve their formation objectives. An observer is designed for each robot in the formation to estimate its state and consequently to compute its control law. It is shown that in the case of a false data injection (FDI) attack on the actuator of a robot, the state estimation error or residual increases, indicating the onset of an attack. Next, a functional link neural network (FLNN) is incorporated into the observer to learn the attack input and to minimize its effect by modifying the controller. Performance assurance and stability of the formation during healthy and under attack are shown using Lyapunov analysis by relaxing the separation principle.

Keywords: Attack detection, attack estimation, Lyapunov stability, formation control, distributed control, security, autonomous systems, nonholonomic system, nonlinear control

1. INTRODUCTION

Tasks that are difficult to be accomplished by an expensive and bulky robot can be accomplished by a group of cheap, agile robots. Such tasks could be applicable to mining, space interferometry [29], patrolling, search and rescue [21], mapping, environmental monitoring [25], etc. Benefits of using multiple robots include reduced system and mission cost, redundancy, improved system accuracy, reconfigurability, and structural flexibility [6]. Formation control techniques, which are utilized to manage such a group of robots, include behavior-based [1][2], virtual structure, consensus [28], neighbor and center reference, leader-follower [31][9][4], and so on.

In behavior-based methods, each robot switches between different controllers (behaviors) in response to different stimulus, such as obstacles, goal points, or other robots. In virtual structure approach, all robots maintain a formation by positioning themselves at different points of a virtual structure. Consensus requires all robots to exchange individual position information with their neighbors and come to an agreement on the final position, which will be a weighted average of the initial position. In the leader-follower strategy, each robot takes on the role of a leader or a follower. The behavior of the leader is not affected by the followers and it follows a desired reference trajectory, while the goal of the followers is to follow the leader while maintaining a desired formation and avoiding obstacles. One of the strategies by which followers can follow the leader is the separation-bearing-based formation control [9]. The leader-follower approach will be utilized in the current work.

Adversarial inputs can effect the sensors, the actuators, or the communication. At the actuator/sensor, fault data injection (FDI) [22], replay attacks [23], and on the communication network attacks such as blackhole, packet loss, time delay, denial of service (DOS) can be observed. Literature [[22][23][25][19][13][26]] discusses the design of a secure

controller in the presence of the aforementioned attacks. In the following, the literature on the type of attacks that can adversely affect the formation will be analyzed to highlight the importance of designing secure formation control protocols. Subsequently, the literature for separation-bearing-based formation control where a dynamic robot representation that captures the nonholonomic and nonlinear properties of a car-like vehicle will be reviewed. In this work, the interest is in securing the formation control of multi-robot systems. In [5] and [27], methods by which self-driving and cooperative self-driving vehicles can be affected by cyber-attacks are highlighted. In [16], it is demonstrated how a compromised vehicle can destroy the efficiency of the entire platoon in the presence of cooperative adaptive cruise control (CACC). In [33], it was shown how an adversary can manipulate the data being transmitted from a vehicle under attack to its followers leading to a crash and possible attack detection and mitigation strategies. In [34], decision trees are used to detect attacks, whereas [12] uses a dynamic monitor that collects information at different time instants to detect attacks, and [3] uses trajectory planning to guarantee that the robots are resilient to attacks. The objective of this paper is to design a distributed attack detection and mitigation scheme for each robot in the formation and the entire formation.

In [18] and [35], the trajectory-tracking controllers are designed by considering the kinematic models and assuming perfect velocity tracking. In [14], a dynamic backstepping-based position and velocity controller was developed by incorporating the robot dynamic model. Torque control was designed, removing the perfect velocity tracking assumption. The authors of [15] took the idea further by considering the robot dynamics to be unknown and a neural network (NN) is utilized. In [7], separation-bearing and separation-separation-bearing techniques are introduced by considering the kinematics of the wheeled mobile robot (WMR).

In [9], the dynamic backstepping controller of [14] is extended to the leader-follower case by employing the separation-bearing [7] techniques. This framework was extended to the case of leader and the follower framework when the dynamics are unknown [10] with

state and output feedback [11]. An NN-based robust integral of the sign of the error (RISE) feedback was utilized in [10] for the purpose of learning the unmodeled dynamics while making sure the formation errors go to zero asymptotically.

In [11], one NN is used to estimate the robot's angular and linear velocities while the other NN is used to estimate the unknown robot dynamics online. The paper [8] discusses near-optimal adaptive control of leader-follower formation. In contrast, the objective here is to design an attack-resilient framework for nonlinear, nonholonomic leader-follower formation by extending the work of [9] under the assumption that the dynamics are known. No such work exists in the literature. An assumption that the communication networks and the sensors are resilient to attacks is made. Attacks are assumed only on the leader and follower robot actuators and/or the signals sent from the CPU of the robot to the actuators. The latter could occur in case of a malware onboard the robot CPU [5].

The paper is organized as follows. In Section, 2 the dynamic, nonholonomic, and separation-bearing-based formation control framework is introduced. In Section 3, an observer is designed for each robot. Note the purpose of the observer is to estimate the state vector of the robot and to design the control input. Additionally, the difference between the measured and observed state vector defined as the residual is used to design a threshold for attack detection. By comparing the residual against this threshold, an attack can be detected. Upon detection, the mitigation scheme designed in Section 4 will be applied. Simulations are used to verify the mathematical results in section 5 and conclusions are drawn in Section 6.

2. PROBLEM FORMULATION

The robot kinematics and dynamics are given by

$$\begin{aligned} \dot{x}_p^k &= \begin{bmatrix} \cos\theta^k & -d^k \sin\theta^k \\ \sin\theta^k & d^k \cos\theta^k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} v^k \\ \omega^k \end{bmatrix}, \\ \dot{\overline{V}}^k &= -\overline{M}^{k-1}(\overline{V}_m^k(x_p^k, \dot{x}_p^k)\overline{V}^k + \overline{F}^k(\overline{V}^k)) + \overline{M}^{k-1}\overline{\tau}^k, \\ y^k &= x^k, \end{aligned} \tag{1}$$

where k denotes if the robot is a leader or follower. The superscript i is used to denote the leader, and the superscript j is used for the follower, where $j = \{1, \ldots, \ldots, N\}$ with N being the total number of followers. Ignoring the superscript k, $x = \left[x_p^T, \overline{V}^T\right]^T \in \mathbb{R}^{(p+c)}$ and $x_p = \left[\chi, y, \theta\right]^T \in \mathbb{R}^p$, with χ, y, and θ being the robots X-Y position in the Cartesian coordinates and the orientation respectively. Here $\overline{V} = [v, \omega]^T \in \mathbb{R}^c$ is the velocity vector with v and ω being the robot's linear and angular velocity respectively. The transformed robot mass matrix, the centripetal and Coriolis matrix, and the surface friction are denoted as $\overline{M}$, $\overline{V}_m(q, \dot{q})$ and $\overline{F}(\overline{V})$, respectively. For details on how the transformed system and matrices are obtained, the readers are referred to [14].

Remark 1. *For the nonholonomic system given by (1) with p generalized coordinates q, m independent constraints, and c actuators, the number of actuators is equal to the number of degrees of freedom ($c = p - m$).*

Remark 2. *The transformed mass matrix $\overline{M}$ is a constant matrix and the transformed Coriolis matrix $\overline{V}_m(q, \dot{q})$ is a zero matrix.*

Based on Remark 2, the Coriolis matrix is not considered. The following assumptions are stated as follows.

Assumption 1. *The robot kinematics and dynamics are known.*

Assumption 2. *There is one-way communication in a leader-follower pair with zero communication delay.*

Remark 3. *Every follower robot is assigned a leader robot. The assigned leader robot for the follower robot 'j' will be denoted by the superscript 'π.'*

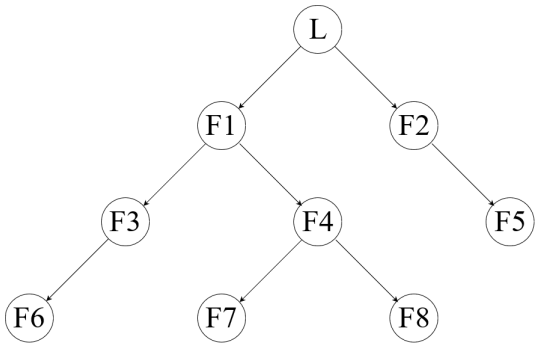

Figure 1. Formation and communication topology.

Next an attack detection and mitigation scheme on the robot formation utilizing the backstepping-based trajectory-tracking controller [9] is designed. A brief overview is given next so as to give the reader a continuity from the previous work done in leader-follower separation-bearing formation control to the present work.

2.1. TRAJECTORY TRACKING USING BACKSTEPPING CONTROL STRUCTURE

For navigation, the leader i tracks a reference cart with unicycle dynamics. This reference cart has linear and angular velocities as decided by the path-planner [14]. The following assumption on the velocities is made.

Assumption 3. *The linear and angular velocities of the reference cart are bounded with the linear velocity* $v^r(t) \geq 0$ *for all* t.

The reference cart dynamics are

$$\dot{\chi}^r = v^r \cos\theta^r \quad \dot{y}^r = v^r \sin\theta^r \quad \dot{\theta}^r = \omega^r, \tag{2}$$

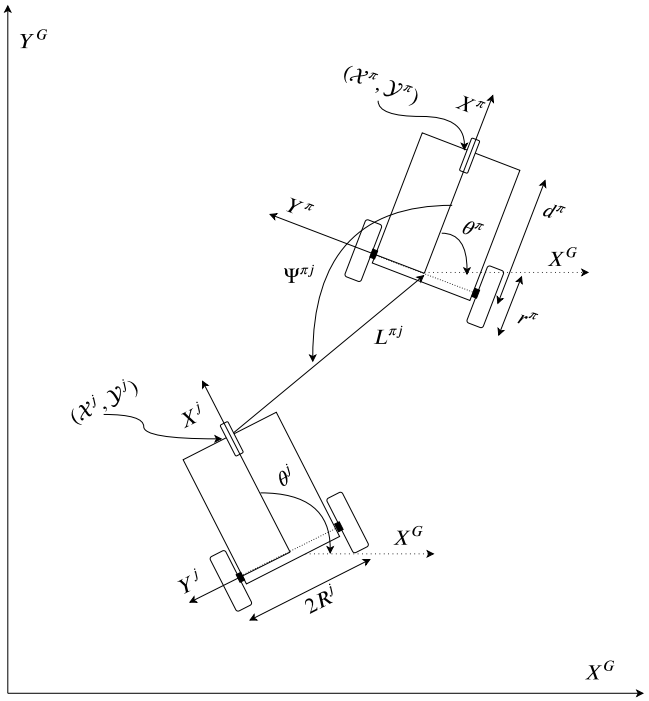

Figure 2. Separation-bearing formation control.

where $x^r = \left[x^r, y^r, \theta^r, v^r, \omega^r\right]^T$ with x^r and y^r being the reference cart's X and Y Cartesian coordinates, respectively, θ^r being the orientation of the reference cart, and ω^r being the reference cart's angular velocity. Now the separation-bearing technique is used by the follower j to track its leader π with the objective being to design a backstepping controller such that

$$\lim_{t\to\infty}(L^{\pi jd} - L^{\pi j}) = 0 \quad \lim_{t\to\infty}(\Psi^{\pi jd} - \Psi^{\pi j}) = 0, \tag{3}$$

is satisfied, where $L^{\pi j}$ is the separation and $\Psi^{\pi j}$ is the bearing of the follower j with respect to the π robot in front of it. Here $L^{\pi jd}$ is the desired separation and $\Psi^{\pi jd}$ is the desired bearing. A network wide extended Kalman filter (EKF) [22] can be used to obtain $L^{\pi j}$ and $\Psi^{\pi j}$. In this paper, the following assumptions are made.

Assumption 4. *The follower 'j' can measure its separation and bearing with respect to its assigned leader robot 'π' by using its onboard sensor suite.*

Assumption 5. *The linear and angular velocities of the 'π^{th}' robot are bounded and $v^{\pi}(t) \geq 0$ for all time 't'.*

For the separation-bearing methodology to work for tracking some information has to be sent from the πth robot to the jth robot. To facilitate this, the assumption is introduced.

Assumption 6. *The 'πth' robot communicates its linear and angular velocity (v^{π},w^{π}) as well as its orientation 'θ^{π}' and linear and angular acceleration ($\dot{v}^{\pi}$,$\dot{\omega}^{\pi}$) to its follower 'j'.*

The state vector of the robot will be used for computing the control velocity. To ensure the availability of the states, the following assumption is introduced next.

Assumption 7. *Each robot is equipped with sensors to measure the robot's own linear velocity 'v', angular velocity 'ω' and orientation 'θ'.*

Since the follower robot is not aware of its global location, it is impossible to use the regular robot kinematics. Instead, the kinematics for the follower is developed on the basis of (3). The follower kinematics are given by

$$\dot{x}_p^j = f_p^j(x^j, x^{\pi}), \tag{4}$$

where

$$f_p^j = \begin{bmatrix} v^j \cos\gamma^j - v^{\pi} \cos\Psi^{\pi j} + d^j w^j \sin\gamma^j \\ \frac{1}{L^{\pi j}} \left(v^{\pi} \sin\Psi^{\pi j} - v^j \sin\gamma^j + d^j w^j \cos\gamma^j \right) - w^{\pi} \\ \omega^j \end{bmatrix},$$

with the function $f_p^j(x^j, x^{\pi})$ representing the kinematics of the j^{th} follower with respect to the π^{th} robot, $\gamma^j = \Psi^{\pi j} + \theta^{\pi j}$ and $\theta^{\pi j} = \theta^{\pi} - \theta^j$.

The position and velocity tracking error for the leader and the follower are defined in [14] and [9]. The tracking errors and the control laws will be covered briefly as they will be part of the proofs. The position-tracking error for a robot tracking its assigned leader is

given by

$$e_p^k = \begin{bmatrix} e_1^k \\ e_2^k \\ e_3^k \end{bmatrix} = \begin{bmatrix} \cos\theta^k & \sin\theta^k & 0 \\ -\sin\theta^k & \cos\theta^k & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_r^k - x^k \\ y_r^k - y^k \\ \theta_r^k - \theta^k \end{bmatrix}, \tag{5}$$

where $x_r^k = x^r, y_r^k = y_r$, for the leader and $x_r^k = x^\pi, y_r^k = y^\pi$, for the follower. For the follower, $\begin{bmatrix} x_r^\pi - x^j \\ y_r^\pi - y^j \end{bmatrix}$ is transformed to the separation-bearing coordinates [9]. θ_r^k is the dynamic reference orientation for the robot. The dynamics of θ_r^k are given by

$$\dot{\theta}_r^i = \frac{1}{d^i}\left(v^r \sin(\theta^r - \theta_r^i) - k_3^i e_3^i\right), \tag{6}$$

for the leader and

$$\dot{\theta}_r^j = \frac{1}{d^j}\left(\omega^\pi L^{\pi jd} \cos(\Psi^{\pi jd} + \theta^{\pi j}) + v^\pi \sin(\theta^\pi - \theta_r^j) + k_2^j e_2^j\right), \tag{7}$$

for the follower. Here d^k is the diameter of the robots wheels. The velocity tracking error is given by

$$e_c^k = \begin{bmatrix} e_4^k \\ e_5^k \end{bmatrix} = \overline{V}_c^k - \overline{V}^k = \begin{bmatrix} v_c^k \\ \omega_c^k \end{bmatrix} - \begin{bmatrix} v^k \\ \omega^k \end{bmatrix}, \tag{8}$$

with $\overline{V}_c^k$ being the control velocity that achieves the tracking objectives of the robot. The leader control velocity is given by

$$\overline{V}_c^i = \begin{bmatrix} v_c^i \\ \omega_c^i \end{bmatrix} = \begin{bmatrix} v^r \cos(\theta^r - \theta^i) + k_1^i e_1^i \\ \frac{1}{d^i}\left(v^r \sin(\theta^r - \theta_r^i) + k_2^i e_2^i\right) \end{bmatrix}, \tag{9}$$

while the follower control velocity is given by

$$\overline{V}_c^j = \begin{bmatrix} v_c^j \\ \omega_c^j \end{bmatrix} = \begin{bmatrix} v^\pi \cos\theta^{\pi j} + k_1^j e_1^j - \omega^\pi L^{\pi jd} \sin(\Psi^{\pi jd} + \theta^{\pi j}) \\ \frac{1}{d^j}\left(\omega^\pi L^{\pi jd} \cos(\Psi^{\pi jd} + \theta^{\pi j}) + v^\pi \sin(\theta^\pi - \theta_r^j) + k_2^j e_2^j + k_3^j e_3^j\right) \end{bmatrix}. \tag{10}$$

In this work, $\overline{V}_c^i$ and θ_r^i help with the stability analysis. The position-tracking error dynamics are obtained by differentiating (5) and substituting equations (1), (2), and (6) to get

$$\dot{e}_p^i = \begin{bmatrix} -k_1^i e_1^i + \omega^i e_2^i + e_4^i \\ -k_2^i e_2^i - \omega^i e_1^i + d^i e_5^i \\ -\frac{1}{d^i}(k_2^i e_2^i + k_3^i e_3^i) + e_5^i \end{bmatrix} + \begin{bmatrix} 0 \\ 2v^r \sin\left(\frac{e_3^i}{2}\right) \cos\left(\theta^r - \frac{\theta_r^i + \theta^i}{2}\right) \\ 0 \end{bmatrix}, \tag{11}$$

$$\dot{e}_p^j = \begin{bmatrix} -k_1^j e_1^j + \omega^j e_2^j + e_4^j \\ -k_2^j e_2^j - k_3^j e_3^j - \omega^j e_1^j + d^j e_5^j \\ -\frac{k_3^j}{d^j} e_3^j + e_5^j \end{bmatrix} + \begin{bmatrix} 0 \\ 2v^\pi \sin\left(\frac{e_3^j}{2}\right) \cos\left(\theta^\pi - \frac{\theta_r^j + \theta^j}{2}\right) \\ 0 \end{bmatrix}, \tag{12}$$

$$\dot{e}_c^k = -K_4^k e_c^k, \tag{13}$$

with $K^k = [k_1^k, k_2^k, k_3^k, k_4^k]$ being a vector of positive gains, and $K_4^k = k_4^k I_{2\times 2}$.

The feedback linearizing control torque $\overline{\tau}^k$ that cancels the robot nonlinearities and introduces the auxiliary control u^k has the structure given by

$$\overline{\tau}^k = \overline{M}^k u^k + \overline{F}^k(\overline{V}^k), \tag{14}$$

$$u^k = \dot{\overline{V}}_c^k + k_4^k(\overline{V}_c^k - \overline{V}^k). \tag{15}$$

Next the following lemmas are stated.

Lemma 1 (Leader Backstepping Control)**.** *Given the nonholonomic robot system with dynamics (1) tracking the reference cart (2), let a smooth velocity control* $\overline{V}_c^i$*, torque control* $\overline{\tau}^i$*, and control input* u^i *for the leader i be given by (9), (14), and (15), respectively. Then, there exists a vector of positive constants* $K^i = [k_1^i, k_2^i, k_3^i, k_4^i]^T$ *such that the leader position and velocity tracking errors, (5) and (8) respectively, go to zero asymptotically.*

Proof. See Appendix. □

Lemma 2 (Follower Backstepping Control)**.** *[10] Given the nonholonomic robot system with dynamics (4) adhering to the leader-follower criterion of (3), let a smooth velocity control* $\overline{V}_c^j$*, torque control* $\overline{\tau}^j$*, and control input* u^j *for the follower j be given by (10), (14), and (15), respectively. Then, there exists a vector of positive constants* $K^j = [k_1^j, k_2^j, k_3^j, k_4^j]^T$ *such that the follower position and velocity tracking errors, (5) and (8) respectively, go to zero asymptotically.*

Proof. See the Appendix. □

2.2. FORMATION STABILITY

Now that the stability with respect to tracking of the individual robots have been shown, the desired formation stability is discussed next.

Theorem 1 (Formation Stability)**.** *Consider a formation of* $N + 1$ *robots with a leader i and N followers with each follower receiving information from its assigned leader. If the hypotheses of Lemma 1 and Lemma 2 hold then the formation error* ($e^{ij} = [e^{i^T} e^{1^T} \dots e^{N^T}]^T$) *where* $e^{ij} \in \mathbb{R}^{(p+c)(1+N)\times 1}$ *the augmented position, and velocity tracking error systems for the leader i and N followers, respectively goes to zero asymptotically.*

Proof. See Appendix. □

3. OBSERVER DESIGN FOR ATTACK DETECTION

Before proceeding, the following assumptions are stated.

Assumption 8. *Sensors and the communication links of the robots do not experience attacks. Attacks only take place on the robot actuators or on the control signals received by the actuator.*

Since the goal of present attack detection and mitigation scheme is distributed, the following assumption is made.

Assumption 9. *The adversary can attack multiple robots at a time.*

The next assumption is made keeping in mind that the attacker is not interested in putting the robots out of commission.

Assumption 10. *The robots in the formation do not collide with other robots in the presence of attacks. Conversely, the formation is input-to-state stable during the onset of actuator attack input.*

In this section, an observer is designed to estimate the robot state vector. The estimated state vector will then be used to compute the backstepping control estimate $\hat{u}^k$. A residual is generated by comparing the estimated robot states with the actual robot states. This residual can be used to design a threshold for the attack-free case. Lemmas 3 and 4 show that in the attack-free condition, the observer-based control law asymptotically stabilizes the tracking and estimation error in the leader and follower, respectively, relaxing the separation principle. Theorem 2 shows the asymptotic stability (AS) of the formation if Lemmas 3 and 4 hold. In the latter part of this section, it will be seen how the residual can be monitored for actuator attack detection.

Before designing the observer, with some abuse of notation and using (1) and (4), the robot dynamics for the leader and follower can be rewritten in a compact form as

$$\begin{aligned} \dot{x}^i &= f^i(x^i) + B^i \hat{\tau}^i, \\ \dot{x}^j &= f^j(x^j, x^\pi) + B^j \hat{\tau}^j. \end{aligned} \tag{16}$$

Here, $B^k = \begin{bmatrix} \mathbf{0} \\ \overline{M}^{k-1} \end{bmatrix}$, $\hat{\tau}^k$ is the torque designed by using the observer state information, and $f^i(x^i)$ and $f^j(x^j, x^{\pi j})$ capture the kinematics and dynamics of the leader and follower robot, respectively. In the presence of an attack, the robot dynamics change to

$$\begin{aligned} \dot{x}^i &= f^i(x^i) + B^i \hat{\tau}^i + B^i w^i, \\ \dot{x}^j &= f^j(x^j, x^\pi) + B^j \hat{\tau}^j + B^j w^j, \end{aligned} \tag{17}$$

where w^k is assumed to be a smooth and bounded attack signal (i.e., $\|w^k\| \leq w_b^k$). The observer dynamics takes the form

$$\begin{aligned} \dot{\hat{x}}^i &= f^i(\hat{x}^i) + B^i \hat{\tau}^i - L^i \tilde{x}^i, \\ \dot{\hat{x}}^j &= f^j(\hat{x}^j, x^\pi) + B^j \hat{\tau}^j - L^j \tilde{x}^j, \end{aligned} \tag{18}$$

where $\hat{x}^k$, is the estimated state, $L^k = \text{diag}\{l_1^k, l_2^k, l_3^k, l_4^k, l_5^k\} > 0$, is a user defined gain matrix, and

$$\tilde{x}^k = \hat{x}^k - x^k, \tag{19}$$

is the residual. From (18), it is clear that the observer has the same form as the robot. It will be seen that the trajectory-tracking objectives of the follower are the same as the robot with the additional objective of estimating the robot state vector. The position-tracking error for

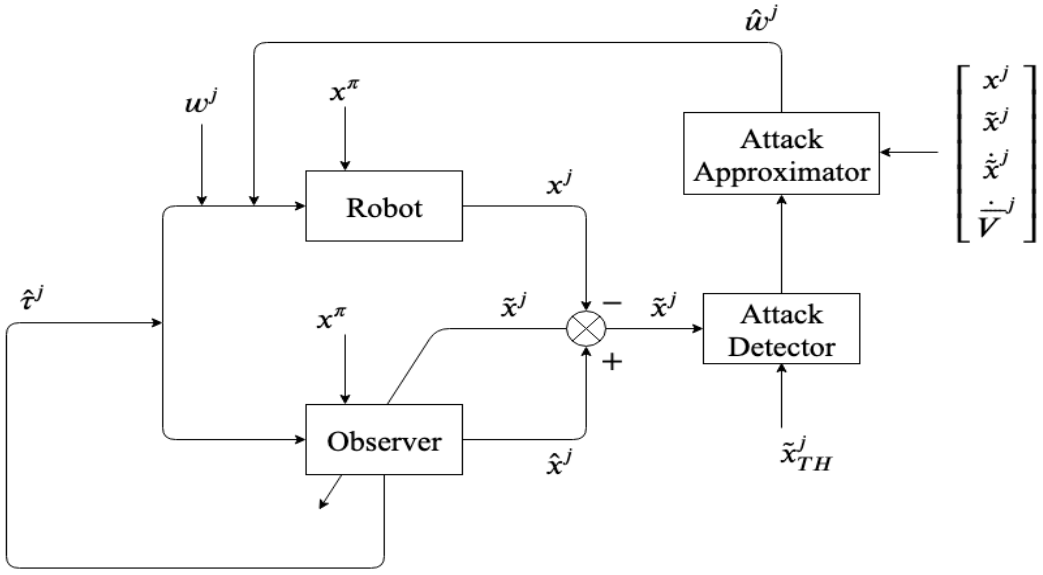

Figure 3. Attack detection and mitigation scheme.

the observer is similar to (5) and is given by

$$\begin{bmatrix} \hat{e}_1^k \\ \hat{e}_2^k \\ \hat{e}_3^k \end{bmatrix} = \begin{bmatrix} \cos\hat{\theta}^k & \sin\hat{\theta}^k & 0 \\ -\sin\hat{\theta}^k & \cos\hat{\theta}^k & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_r^k - \hat{x}^k \\ y_r^k - \hat{y}^k \\ \hat{\theta}_r^k - \hat{\theta}^k \end{bmatrix}, \tag{20}$$

with x_r^k and y_r^k having the same definitions as before. $\hat{\theta}_r^k$ is the dynamic reference orientation of the observer. The dynamics of $\hat{\theta}_r^k$ are

$$\dot{\hat{\theta}}_r^i = \frac{1}{d^i}\left(v^r \sin(\theta^r - \hat{\theta}_r^i) - k_3^i \hat{e}_3^i\right), \tag{21}$$

for the leader robot's observer and

$$\dot{\hat{\theta}}_r^j = \frac{1}{d^j}\left(\omega^\pi L^{\pi jd} \cos(\Psi^{\pi jd} + \hat{\theta}^{\pi j}) + v^\pi \sin(\theta^\pi - \hat{\theta}_r^j) + k_2^j \hat{e}_2^j\right), \tag{22}$$

for the follower robot's observer. The velocity-tracking error $\hat{e}_c^k$ is

$$\begin{bmatrix} \hat{e}_4^k \\ \hat{e}_5^k \end{bmatrix} = \hat{\overline{V}}_c^k - \hat{\overline{V}}^k = \begin{bmatrix} \hat{v}_c^k \\ \hat{\omega}_c^k \end{bmatrix} - \begin{bmatrix} \hat{v}^k \\ \hat{\omega}^k \end{bmatrix}, \tag{23}$$

with $\hat{\overline{V}}_c^k$ being the desired control velocity. The augmented observer position and velocity tracking error dynamics are given by

$$\begin{aligned} \dot{\hat{e}}^i = & \begin{bmatrix} -k_1^i \hat{e}_1^i + \hat{\omega}^i \hat{e}_2^i + \hat{e}_4^i \\ -k_2^i \hat{e}_2^i - \hat{\omega}^i \hat{e}_1^i + d^i \hat{e}_5^i \\ -\frac{1}{d^i}(k_2^i \hat{e}_2^i + k_3^i \hat{e}_3^i) + \hat{e}_5^i \\ -k_4^i \hat{e}_4^i \\ -k_4^i \hat{e}_5^i \end{bmatrix} + \begin{bmatrix} 0 \\ 2v^r \sin\left(\frac{\hat{e}_3^i}{2}\right) \cos\left(\theta^r - \frac{\hat{\theta}_r^i + \hat{\theta}^i}{2}\right) \\ \mathbf{0}_{3\times 1} \end{bmatrix} \\ & + \begin{bmatrix} \begin{bmatrix} \cos\hat{\theta}^i & \sin\hat{\theta}^i & 0 \\ -\sin\hat{\theta}^i & \cos\hat{\theta}^i & 0 \\ 0 & 0 & 1 \end{bmatrix} & \mathbf{0}_{3\times 2} \\ \mathbf{0}_{2\times 3} & \mathbf{I}_{2\times 2} \end{bmatrix} L^i \tilde{x}^i, \end{aligned} \tag{24}$$

$$\begin{aligned} \dot{\hat{e}}^j = & \begin{bmatrix} -k_1^j \hat{e}_1^j + \hat{\omega}^j \hat{e}_2^j + \hat{e}_4^j \\ -k_2^j \hat{e}_2^j - k_3^j \hat{e}_3^j - \hat{\omega}^j \hat{e}_1^j + d^j \hat{e}_5^j \\ -\frac{k_3^j}{d_j} \hat{e}_3^j + \hat{e}_5^j - k_4^j \hat{e}_4^j \\ -k_4^j \hat{e}_5^j \end{bmatrix} + \begin{bmatrix} 0 \\ 2v^\pi \sin\left(\frac{\hat{e}_3^j}{2}\right) \cos\left(\theta^\pi - \frac{\hat{\theta}_r^j + \hat{\theta}^j}{2}\right) \\ \mathbf{0}_{3\times 1} \end{bmatrix} \\ & + \begin{bmatrix} \begin{bmatrix} \cos\hat{\gamma}^j & -\hat{L}^{\pi j} \sin\hat{\gamma}^j & -\hat{e}_2^j \\ \sin\hat{\gamma}^j & \hat{L}^{\pi j} \cos\hat{\gamma}^j & \hat{e}_1^j \\ 0 & 0 & 1 \end{bmatrix} & \mathbf{0}_{3\times 2} \\ \mathbf{0}_{2\times 3} & \mathbf{I}_{2\times 2} \end{bmatrix} L^j \tilde{x}^j, \end{aligned} \tag{25}$$

where $\hat{e}^k = \begin{bmatrix} \hat{e}_p^k \\ \hat{e}_c^k \end{bmatrix}$. The estimate of the desired control velocity for the leader is given by

$$\hat{\overline{V}}_c^i = \begin{bmatrix} v^r \cos(\theta^r - \hat{\theta}^i) + k_1^i \hat{e}_1^i \\ \frac{1}{d^i}\left(v^r \sin(\theta^r - \hat{\theta}_r^i) + k_2^i \hat{e}_2^i\right) \end{bmatrix}, \tag{26}$$

and the estimate of the desired control velocity for the follower is given by

$$\hat{\overline{V}}_c^j = \begin{bmatrix} v^\pi \cos\hat{\theta}^{\pi j} + k_1^j \hat{e}_1^j - \omega^\pi L^{\pi jd} \sin(\Psi^{\pi jd} + \hat{\theta}_{\pi j}) \\ \frac{1}{d_j}\left(\omega^\pi L^{\pi jd} \cos(\Psi^{\pi jd} + \hat{\theta}^{\pi j}) + v^\pi \sin(\hat{\theta}^{\pi jr}) + k_2^j \hat{e}_2^j + k_3^j \hat{e}_3^j\right) \end{bmatrix}. \tag{27}$$

Since the estimated desired control velocity $\hat{\overline{V}}_c^k$ is being used to stabilize the tracking error dynamics instead of the desired control velocity $\overline{V}_c^k$, the velocity tracking error throughout the rest of this work is defined to be

$$e_c^k = \hat{\overline{V}}_c^k - \overline{V}^k. \tag{28}$$

Taking equation (28) into consideration, the position tracking error dynamics of the robot become

$$\begin{aligned} \begin{bmatrix} \dot{e}_1^i \\ \dot{e}_2^i \\ \dot{e}_3^i \end{bmatrix} &= \begin{bmatrix} -k_1^i e_1^i + \omega^i e_2^i + e_4^i \\ -k_2^i e_2^i - \omega^i e_1^i + d^i e_5^i \\ -\frac{1}{d^i}(k_2^i e_2^i + k_3^i e_3^i) + e_5^i \end{bmatrix} \\ &+ \begin{bmatrix} -\tilde{v}_c^i \\ 2v^r \sin\left(\frac{e_3^i}{2}\right) \cos\left(\theta^r - \frac{\theta_r^i + \theta^i}{2}\right) - d^i \tilde{\omega}_c^i \\ -\tilde{\omega}_c^i \end{bmatrix}, \end{aligned} \tag{29}$$

for the leader and

$$\begin{bmatrix} \dot{e}_1^j \\ \dot{e}_2^j \\ \dot{e}_3^j \end{bmatrix} = \begin{bmatrix} -k_1^j e_1^j + \omega^j e_2^j + e_4^j \\ -k_2^j e_2^j - k_3^j e_3^j - \omega^j e_1^j + d^j e_5^j \\ -\frac{k_3^j}{d^j} e_3^j + e_5^j \end{bmatrix} + \begin{bmatrix} -\tilde{v}_c^j \\ 2v^\pi \sin\left(\frac{e_3^j}{2}\right) \cos\left(\theta_\pi - \frac{\theta_r^j + \theta^j}{2}\right) \\ -d^j \tilde{\omega}_c^j \\ -\tilde{\omega}_c^j \end{bmatrix}, \tag{30}$$

for the follower robot with $\tilde{\overline{V}}_c^k = \hat{\overline{V}}_c^k - \overline{V}_c^k$. The estimated control torque is given by

$$\hat{\overline{\tau}}^k = \overline{M}^k \hat{u}^k + \overline{F}^k(\hat{\overline{V}}^k), \tag{31}$$

with $\hat{u}^k$ being the estimated auxiliary control input defined as

$$\hat{u}^k = \dot{\hat{\overline{V}}}_c^k + k_4^k(\hat{\overline{V}}_c^k - \hat{\overline{V}}^k), \tag{32}$$

Due to the change of the control torque of (1) to $\hat{\overline{\tau}}^i$, the robot velocity dynamics $\dot{\overline{V}}^i$ is given by

$$\begin{aligned} \dot{\overline{V}}^k &= \overline{M}^{k^{-1}}(-\overline{F}^k(\overline{V}^k) + \overline{M}^k \hat{u}^k + \overline{F}^k(\hat{\overline{V}}^k)) \\ &= \hat{u}^k + \overline{M}^{k^{-1}}(\overline{F}^k(\hat{\overline{V}}^k) - \overline{F}^k(\overline{V}^k) + w^k). \end{aligned}$$

The substitution $\overline{M}^{k^{-1}}(\overline{F}^k(\hat{\overline{V}}^k) - \overline{F}^k(\overline{V}^k)) = \tilde{N}^k(\tilde{\overline{V}}^k) = \begin{bmatrix} \tilde{n}_v^k \\ \tilde{n}_\omega^k \end{bmatrix}$ simplifies equation () to

$$\dot{\overline{V}}^k = \dot{\hat{\overline{V}}}_c^k + K_4^k(\hat{\overline{V}}_c^k - \overline{V}_k) - K_4^k \tilde{\overline{V}}^k + \tilde{N}^k(\tilde{\overline{V}}^k) + \overline{M}^{k^{-1}} w^k, \tag{33}$$

and the velocity tracking error dynamics of the robot become

$$\dot{e}_c^k = -K_4^k e_c^k + K_4^k \tilde{\bar{V}}^k - \tilde{N}^k(\tilde{\bar{V}}^k) - \overline{M}^{k^{-1}} w^k. \tag{34}$$

The estimation error dynamics is given by

$$\dot{\tilde{x}}^k = \dot{\hat{x}}^k - \dot{x}^k, \tag{35}$$

which can be further simplified for the leader and follower robot as

$$\begin{aligned} \dot{\tilde{x}}^i =& \tilde{f}^i(\tilde{x}^i) - L^i \tilde{x}^i - B^i w^i, \\ \dot{\tilde{x}}^j =& \tilde{f}^j(\tilde{x}^j, x^\pi) - L^j \tilde{x}^j - B^j w^j, \end{aligned} \tag{36}$$

by substituting equations (17) and (18). Here $\tilde{f}^i(\tilde{x}^i) = f^i(\hat{x}^i) - f^i(x^i)$, and $\tilde{f}^j(\tilde{x}^j, x^\pi) = f^i(\hat{x}^j, x^\pi) - f^i(x^j, x^\pi)$. The velocity estimation error dynamics are given by

$$\dot{\tilde{\bar{V}}}^k = -\tilde{N}^k(\tilde{\bar{V}}^k) - L_c^k \tilde{\bar{V}}^k - \overline{M}^{-1^k} w^k \tag{37}$$

with $L_c^k = \text{diag}\{l_4^k, l_5^k\}$

3.1. ATTACK-FREE SCENARIO

In the absence of attack, the following two Lemmas and Theorem are defined.

Lemma 3. *Given the nonholonomic robot system with dynamics (1) tracking the reference cart (2), let a smooth velocity control estimate $\hat{\bar{V}}_c^i$, control input estimate $\hat{u}^i$, and torque control estimate $\hat{\tau}^i$ for the leader i be given by (26),(32) and (31) respectively. Then there exists vector of positive constants $K^i = [k_1^i, k_2^i, k_3^i, k_4^i]^T$ and $L^i = [l_1^i, l_2^i, l_3^i, l_4^i, l_5^i]^T$ such that the leader position and redefined velocity tracking errors, and the leader state estimation error given by (5), (28) and (19) respectively go to zero asymptotically.*

Proof. See the Appendix. □

Lemma 4. *Given the nonholonomic robot system with dynamics (4) adhering to the leader follower criterion of (3), let a smooth velocity control estimate $\hat{\bar{V}}_c^j$, control input estimate $\hat{u}^j$, and torque control estimate $\hat{\tau}^j$ for the follower j be given by (27),(32) and (31) respectively. Then there exists vector of positive constants $K^j = [k_1^j, k_2^j, k_3^j, k_4^j]^T$ and $L^j = [l_1^j, l_2^j, l_3^j, l_4^j, l_5^j]^T$ such that the follower tracking errors, and the follower state estimation error given by (5), (8) and (19) respectively go to zero asymptotically.*

Proof. See the Appendix. □

For calculating the attack detection threshold, the stability of the leader-follower formation in Theorem 2 is considered.

Theorem 2. *Consider a formation of $N + 1$ robots with a leader i and N followers with each follower receiving information from its assigned leader. If the hypotheses of Lemma 3 and Lemma 4 hold then the formation error e^{ij} and the formation estimation error $\tilde{x}^{ij} = [\tilde{x}^{i^T} \tilde{x}^{1^T} \dots \tilde{x}^{N^T}]^T$ where $\tilde{x}^{ij} \in \mathbb{R}^{(p+c)\times(1+N)}$ which is the augmented position and orientation, and velocity estimation error for the leader i and N followers, respectively goes to zero asymptotically.*

Proof. See the Appendix. □

3.2. ACTUATOR ATTACK SCENARIO

In the case of an attack the following Lemmas and Theorem hold.

Lemma 5. *Given the nonholonomic robot system with dynamics (1) tracking the reference cart (2), let a smooth velocity control estimate $\hat{\bar{V}}_c^i$, control input estimate $\hat{u}^i$, and torque control estimate $\hat{\tau}^i$ for the leader i be given by (26),(32) and (31) respectively. Then there exists vector of positive constants $K^i = [k_1^i, k_2^i, k_3^i, k_4^i]^T$ and $L^i = [l_1^i, l_2^i, l_3^i, l_4^i, l_5^i]^T$ such that*

the leader's position and orientation, redefined velocity tracking errors, and the observer state estimation error given by (5), (28) and (19) respectively are UUB with bounds as per (B-29).

Proof. See the Appendix. □

Lemma 6. *Given the nonholonomic robot system with dynamics (4) adhering to the leader follower criterion of (3), let a smooth velocity control estimate* $\hat{\bar{V}}_c^j$*, control input estimate* $\hat{u}^j$*, and torque control estimate* $\hat{\bar{\tau}}^j$ *for the follower j be given by (27),(32) and (31) respectively. Then there exists vector of positive constants* $K^j = [k_1^j, k_2^j, k_3^j, k_4^j]^T$ *and* $L^j = [l_1^j, l_2^j, l_3^j, l_4^j, l_5^j]^T$ *such that the follower position and orientation, redefined velocity tracking errors, and the observer state estimation error given by (5), (28) and (19) respectively are UUB with bounds as per (B-32).*

Proof. See the Appendix. □

Theorem 3. *Consider a formation of* $N + 1$ *robots with a leader i and N followers with each follower receiving information from its assigned leader. If the hypotheses of Lemma 5 and Lemma 6 hold then the formation tracking error* e^{ij} *and the formation estimation* $\tilde{x}^{ij}$ *for the leader i and N followers, respectively is UUB with bounds (B-34)*

Proof. See the Appendix. □

Based on Theorems 2 and 3 the following corollary can be stated.

Corollary 1. *The estimation error bounds given in Theorem 2 can be used by the formation robots as a threshold for attack detection.*

From a practical standpoint, a small constant δ can be used for attack detection instead of zero.

4. ACTUATOR ATTACK MITIGATION

In this section an attack mitigating input $\hat{w}^k$ for the robots is designed so as to learn the attack by using a function approximator such as a neural network for the purpose of compensation. The attack input on the actuator can be approximated by using a NN defined by

$$w^k = {W^k}^T \phi(\overline{x}^k) + \varepsilon^k, \tag{38}$$

where W^k is the target weight matrix assumed to be bounded above such that $\|W^k\| \leq W_M^k$ for a standard bounded actuator attack and $\phi(.) \in \mathbb{R}^{s\times 1}$ is a basis function, $\overline{x}^k = [{x^k}^T, x_r^T, {\tilde{x}^k}^T, {\dot{\tilde{x}}^k}^T]^T$ is the input to the basis function, and ε^k is the error in function approximation s.t. $\|\varepsilon^k\| \leq \varepsilon_b^k$. The norm of the weights $\|W^k\|$ is assumed to be bounded and $\phi(.)$ is known to be bounded as it is a standard basis function such as the logistic sigmoid, or the tangent sigmoid. The estimated attack signal can now be expressed by

$$\tau_{mit} = \hat{w}^k = {\hat{W}^k}^T \phi(\overline{x}^k) - L_{mit}^k e_c^k. \tag{39}$$

where $\hat{W}^k$, is an estimate of the target weight matrix and $L_{mit}^k = \overline{M}^k \,\mathrm{diag}\{l_{1mit}^k, l_{2mit}^k\}$, is a diagonal gain matrix. The weight estimation error is defined as $\tilde{W}^k = \hat{W}^k - W^k$.

Remark 4. *The tracking error e_c^k in equations (39), (48) and (49) is introduced for the purpose of analysis. In the actual implementation e_c^k will be rewritten in terms of $\hat{e}_c^k$ and $\tilde{\overline{V}}^k$.*

$$e_c^k = \tilde{\overline{V}}^k + \hat{e}_c^k. \tag{40}$$

The control torque is now appended by $-\tau_{mit}$ to compensate the attack input. The robot velocity dynamics are now given by

$$\begin{aligned}\dot{\overline{V}}^k =& \dot{\overline{V}}_c^k + K_4^k e_c^k - K_4^k \tilde{\overline{V}}^k + \tilde{N}^k(\tilde{\overline{V}}^k) + \overline{M}^{k^{-1}}\left(W^{k^T}\phi(\overline{x}^k) + \varepsilon^k\right) - \overline{M}^{k^{-1}}\hat{W}^{k^T}\phi(\overline{x}^k) \\ &+ \overline{M}^{k^{-1}} L_{mit}^k e_c^k \\ =& \dot{\overline{V}}_c^k + \left(K_4^k + \overline{M}^{k^{-1}} L_{mit}^k\right) e_c^k - K_4^k \tilde{\overline{V}}^k + \tilde{N}^k(\tilde{\overline{V}}^k) - \overline{M}^{k^{-1}}\tilde{W}^{k^T}\phi(\overline{x}^k) + \overline{M}^{k^{-1}}\varepsilon^k, \end{aligned} \tag{41}$$

and the tracking error dynamics are given by

$$\dot{e}_c^k = -\left(K_4^k + \overline{M}^{k^{-1}} L_{mit}^k\right) e_c^k + K_4^k \tilde{\overline{V}}^k - \tilde{N}^k(\tilde{\overline{V}}^k) + \overline{M}^{k^{-1}}\tilde{W}^{k^T}\phi(\overline{x}^k) - \overline{M}^{k^{-1}}\varepsilon^k. \tag{42}$$

The overall robot dynamics are now given by

$$\begin{aligned}\dot{x}^i =& f^i(x^i) + B^i\hat{\tau}^i - B^i\tilde{W}^{i^T}\phi(\overline{x}^i) + B^i\varepsilon^i + B^i L_{mit}^i e_c^i, \\ \dot{x}^j =& f^j(x^j, x^\pi) + B^j\hat{\tau}^j - B^j\tilde{W}^{j^T}\phi(\overline{x}^j) + B^j\varepsilon^j + B^j L_{mit}^j e_c^j, \end{aligned} \tag{43}$$

The estimation error dynamics in (36) changes to

$$\begin{aligned}\dot{\tilde{x}}^i =& \tilde{f}^i(\tilde{x}^i) - L^i\tilde{x}^i + B^i\tilde{W}^{i^T}\phi(\overline{x}^i) - B^i L_{mit}^i e_c^i - B^i\varepsilon^i, \\ \dot{\tilde{x}}^j =& \tilde{f}^j(\tilde{x}^j, x^\pi) - L^j\tilde{x}^j + B^j\tilde{W}^{j^T}\phi(\overline{x}^j) - B^j L_{mit}^j e_c^j - B^j\varepsilon^j \end{aligned} \tag{44}$$

For the stability of the estimation error dynamics, the structure of the observer is changed from (18) to

$$\begin{aligned}\dot{\hat{x}}^i =& f^i(\hat{x}^i) + B^i\hat{\tau}^i - L^i\tilde{x}^i + B^i L_{mit}^i\hat{e}_c^i, \\ \dot{\hat{x}}^j =& f^j(\hat{x}^j, x^\pi) + B^j\hat{\tau}^j - L^j\tilde{x}^j + B^j L_{mit}^j\hat{e}_c^j, \end{aligned} \tag{45}$$

when the attack is detected. The equations (40) and (45) and (44) expressed as

$$\begin{aligned}\dot{\tilde{x}}^i &= \tilde{f}^i(\tilde{x}^i) - L^i\tilde{x}^i + B^i\tilde{W}^{i^T}\phi(\overline{x}^i) - B^i L^i_{mit}\tilde{\overline{V}}^i - B^i\varepsilon^i,\\ \dot{\tilde{x}}^j &= \tilde{f}^j(\tilde{x}^j, x^\pi) - L^j\tilde{x}^j + B^j\tilde{W}^{j^T}\phi(\overline{x}^j) - B^j L^j_{mit}\tilde{\overline{V}}^j - B^j\varepsilon^j.\end{aligned} \tag{46}$$

The velocity estimation error dynamics during mitigation is given by

$$\dot{\tilde{\overline{V}}}^k = -\tilde{N}^k(\tilde{\overline{V}}^k) - L^k_c\tilde{\overline{V}}^k + \overline{M}^{-1^k}\tilde{W}^{k^T}\phi(\overline{x}^k) - \overline{M}^{-1^k}\varepsilon^k. \tag{47}$$

Lemma 7. *Given the attacked nonholonomic robot system in (17), by modifying the control law so that the tracking error dynamics is modified to (42), the estimation error dynamics to (46), and the tuning law for the FLNN selected as (48), the attack affected tracking and estimation error bound given in Lemma 5 is reduced to (B-39) and the NN weight estimation error $\tilde{W}^i$ is uniformly ultimately bounded (UUB).*

$$\dot{\hat{W}}^i = -F^i\phi(\overline{x}^i)\left(\tilde{\overline{V}}^i + e^i_c\right)^T\overline{M}^{i^{-1}} - \kappa^i F^i\hat{W}^i. \tag{48}$$

Proof. See the Appendix. □

Lemma 8. *Given the attacked nonholonomic robot system in (17), by modifying the control law so that the tracking error dynamics is modified to (42), the estimation error dynamics to (46), and by selecting the tuning law for the FLNN as per (49), the tracking and estimation error bound given in Lemma 6 is reduced to B-44 and the NN weight estimation error $\tilde{W}^j$ is UUB.*

$$\dot{\hat{W}}^j = -F^j\phi(\overline{x}^j)\left(\tilde{\overline{V}}^j + e^j_c\right)^T\overline{M}^{j^{-1}} - \kappa^j F^j\hat{W}^j. \tag{49}$$

Proof. See the Appendix. □

Next the formation stability is assessed in the following theorem.

Theorem 4. *Consider a formation of $N+1$ robots with a leader i and N followers. Let a spanning tree exist with the leader as the root node. If the hypotheses of Lemma 7 and Lemma 8 hold then the formation tracking error e^{ij} and the formation estimation error $\tilde{x}^{ij}$, and $\tilde{W}^{ij} = \operatorname{diag}\left(\tilde{W}^{i}, \tilde{W}^{1}, \ldots, \tilde{W}^{N}\right)$ where $\tilde{W}^{ij} \in \mathbb{R}^{s\times c\times(1+N)}$ is the augmented NN weight estimation error for the leader i and N followers, respectively is UUB with bounds (B-48) and (B-49).*

Proof. See the Appendix. □

5. RESULTS AND DISCUSSION

For the purpose of simulation, a right-wing formation consisting of a leader robot i and two follower robots $j = \{1, 2\}$ is taken as per Figure 4. The robots parameters are chosen as [9] mass $m = 5$, moment of inertia $I = 3$, perpendicular distance of the wheels from the center of mass $R = 0.175$, wheel radius $r = 0.08$, distance from center of mass to the rear axle $d = 0.4$, linear coefficient of static friction $\mu_1 = 0.2$, linear coefficient of dynamic friction $\mu_2 = 0.2$, angular coefficient of static friction $\mu_3 = 0.2$, angular coefficient of dynamic friction $\mu_4 = 0.2$, the transformed mass matrix $\overline{M} = \begin{bmatrix} m & 0 \\ 0 & I \end{bmatrix}$, $\overline{F} = \begin{bmatrix} \mu_1 \operatorname{sign} v + \mu_2 v \\ \mu_3 \operatorname{sign} \omega + \mu_4 \omega \end{bmatrix}$. The control gains are selected as $k_1 = 3$, $k_2 = 2$, $k_3 = 2$ and $k_4 = 2$. The observer gains are selected as $l_1 = 1$, $l_2 = 1$, $l_3 = 1$, $l_4 = 3$ and $l_5 = 3$. Note that the subscripts have been removed wherever the values for the leader and follower robots are identical. The reference cart linear velocity is given by $v^r = 0.8$ and the angular velocity is given by $\omega^r = \begin{cases} 0.15 & 10 \le t \le 25 \\ -0.15 & 40 \le t \le 55 \\ 0 & \text{otherwise} \end{cases}$. The separation between a leader and follower is $L^{\pi j} = 2m$ and the bearing is $\Psi^{\pi j} = -120^\circ$. The actuator attacks performed by the

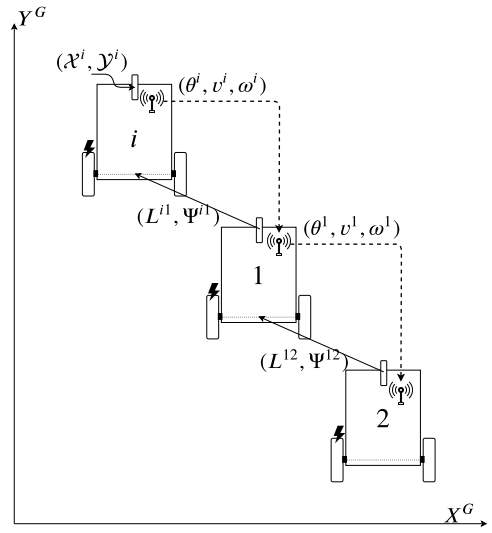

Figure 4. Leader-follower formation under actuator attack.

attacker on the robot formation are given by $w^i = \begin{bmatrix} 2.0 + 1\sin 2t \\ 0.5 + 2\sin 5t \end{bmatrix}$, $w^1 = \begin{bmatrix} 4 + 0.1\sin 0.5t \\ 1 + 0.1\sin 0.5t \end{bmatrix}$, and $w^2 = \begin{bmatrix} 4 + 0.1\sin 0.5t \\ 1 + 0.1\sin 0.5t \end{bmatrix}$. The NN gain matrix F is taken as $10 \times I$ and the scalar gain $\kappa = 0.1$.

5.1. ATTACK-FREE SCENARIO

Figure 5 shows the formation trajectories of the formation given in Figure 4 in a no-attack scenario. Figure 6 gives the euclidean norm of the tracking errors while Figure 7 gives the euclidean norm of the estimation errors.

5.2. ATTACK CASE 1

In the case there is an attack on the formation leader robot at $t = 90s$, the formation trajectory deviates from its original trajectory which is evident in Figure 9. The tracking and estimation errors can be seen in Figures 10 and 11. Notice that the formation estimation

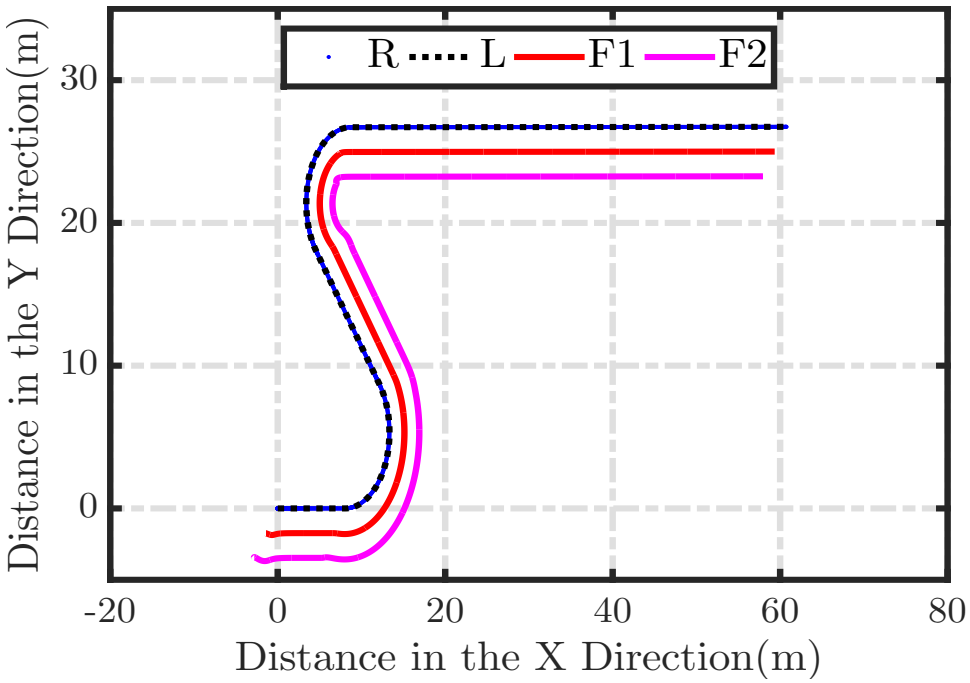

Figure 5. Attack-free formation trajectories.

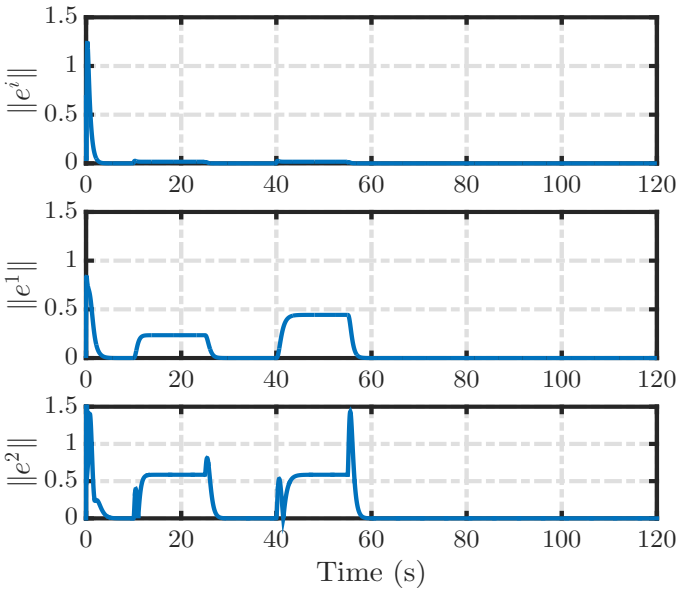

Figure 6. Attack-free tracking errors.

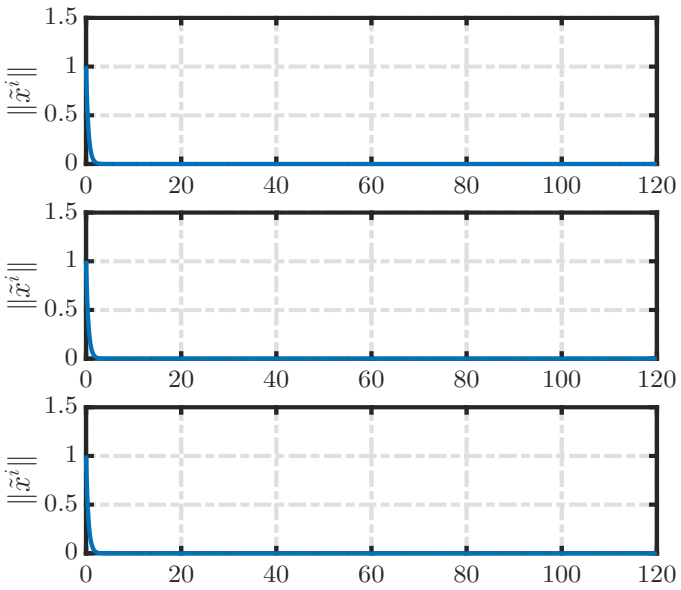

Figure 7. Attack-free estimation errors.

errors are unaffected by this attack but the tracking errors are slightly affected. This could be explained by the fact that the attack on the leader causes the leader to change its velocity suddenly but the follower cannot change it's course instantaneously due to physical and actuator limitations. In addition the follower is unaware of the attack on the leader due to minimal communication among the robots in the formation.

5.3. ATTACK CASE 2

When an attack occurs on the follower 1 at $t = 80s$, the tracking error of the follower 2 is temporarily affected as observed in Figure 13. If the attack had a fast time-varying component, then the follower 2 will be effected accordingly. The tracking errors of the leader are completely unaffected as expected. The estimation errors can be observed in Figures 14. Just like in attack case 1, only the estimation error of the robot under attack increases whereas the estimation errors of other robots are unaffected.

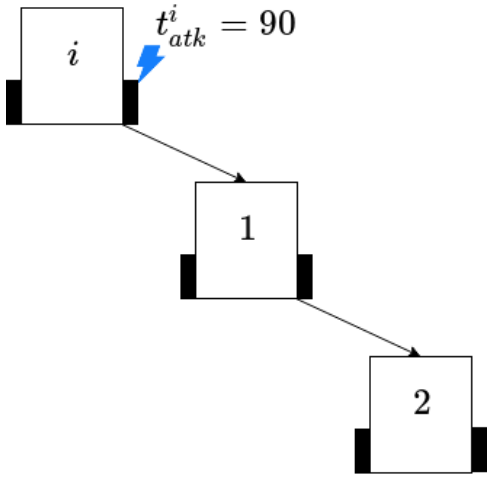

Figure 8. Attack case 1.

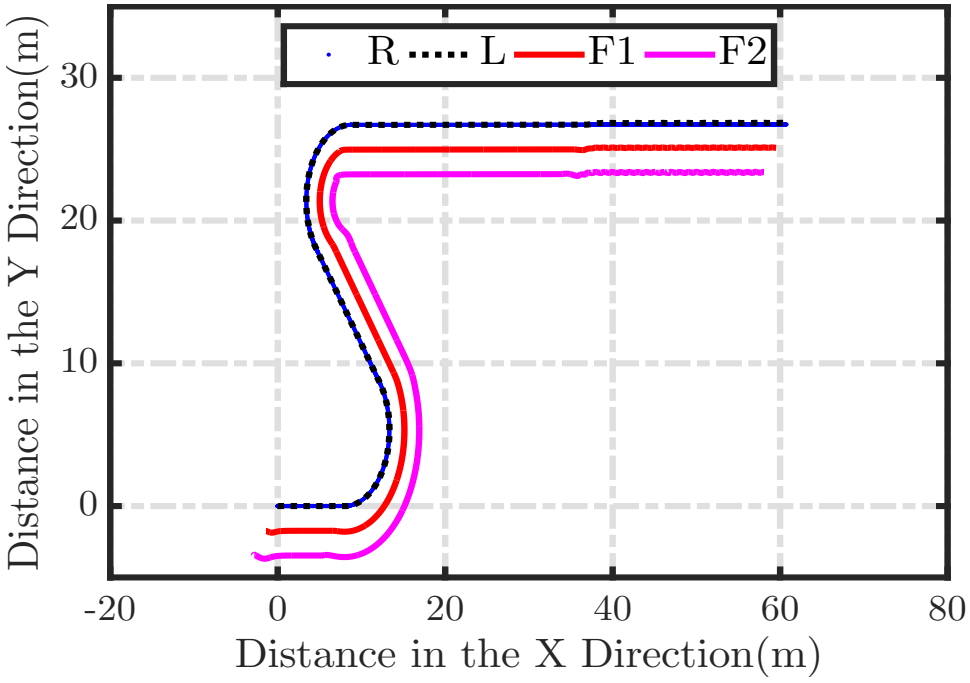

Figure 9. Formation trajectories with leader under attack.

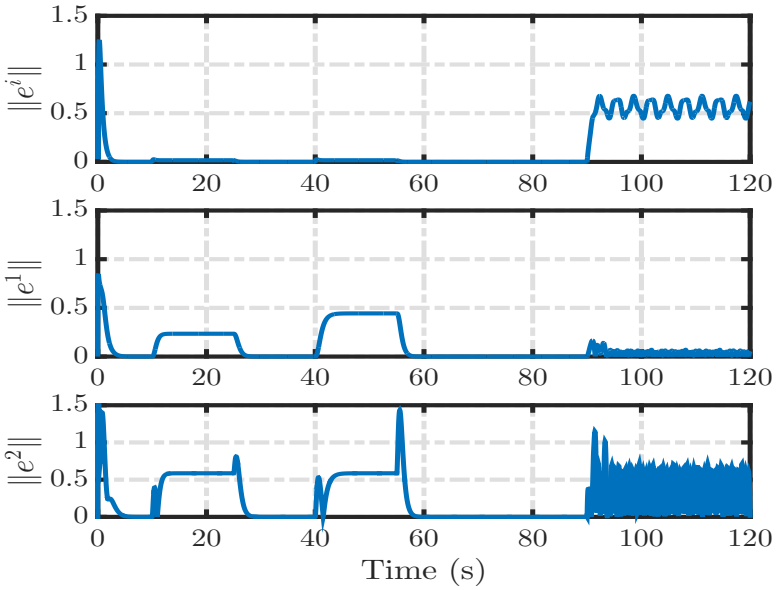

Figure 10. Tracking error norm with leader under attack.

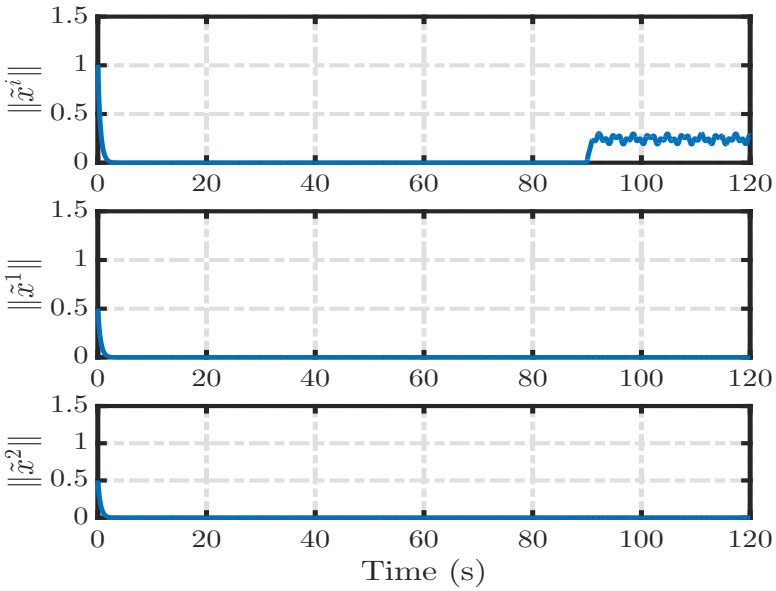

Figure 11. Estimation error norm with leader under attack.

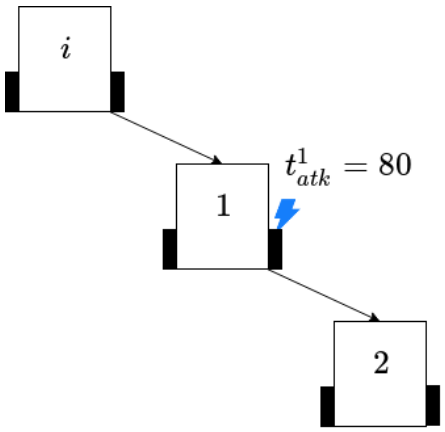

Figure 12. Attack case 2.

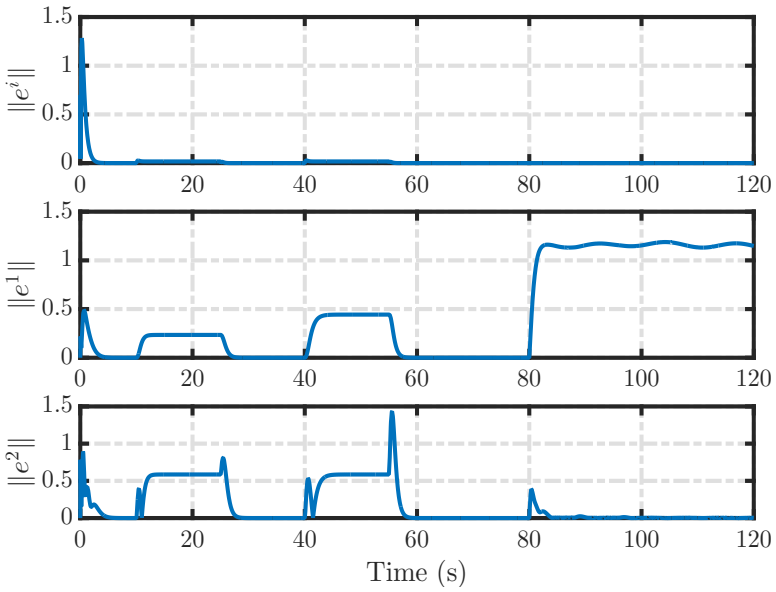

Figure 13. Tracking error norm with follower 1 under attack.

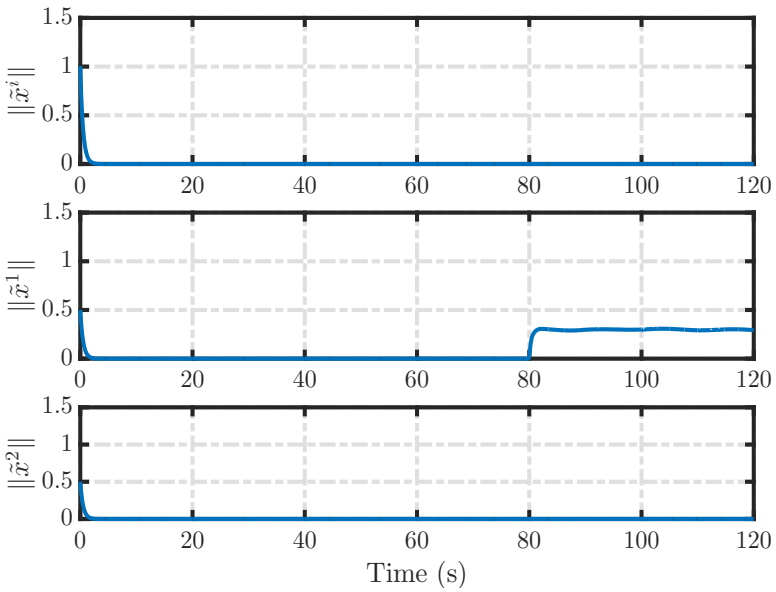

Figure 14. Estimation errors with follower 1 under attack.

5.4. ATTACK CASE 3

In this case, distributed attacks occurring on different robots of the formation at varying time instants is considered. The attack on robot i occurs at $t = 90$, at $t = 80$ on robot 1, and at $t = 100$ on robot 2. The mitigation is initiated $5 seconds$ after the attack in order to study the effect of the attack. Figure 16 shows the effect of the attacks and the mitigation on the formation trajectory. Figure 17 shows the effect of attack on all the tracking errors before and post-mitigation.

The tracking error of follower 2 is effected the most due to cumulative effect of attacks on the robots preceding it. After mitigation is initiated, the tracking error has a much lower bound than the case when attack happens in case 1 and 2. The estimation error for all the three robots behaves as expected as depicted in Figure 18. Finally, Figure 19 illustrates the norm of the NN weights. Each NN is initialized at zero and only begins learning the attack 5 seconds after the attack begins. The weights of the follower NN converge very quickly whereas the leader NN weight convergence takes time due to the selection of gain matrices.

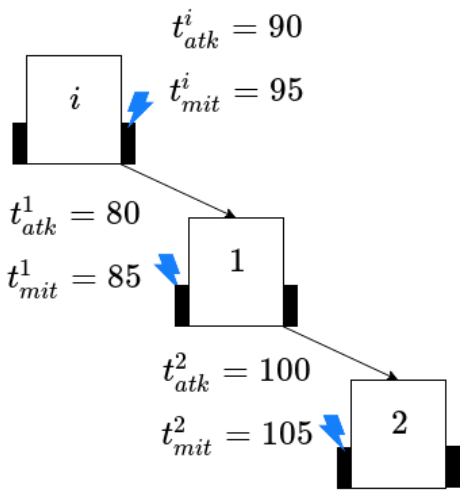

Figure 15. Formation distributed actuator attack mitigation.

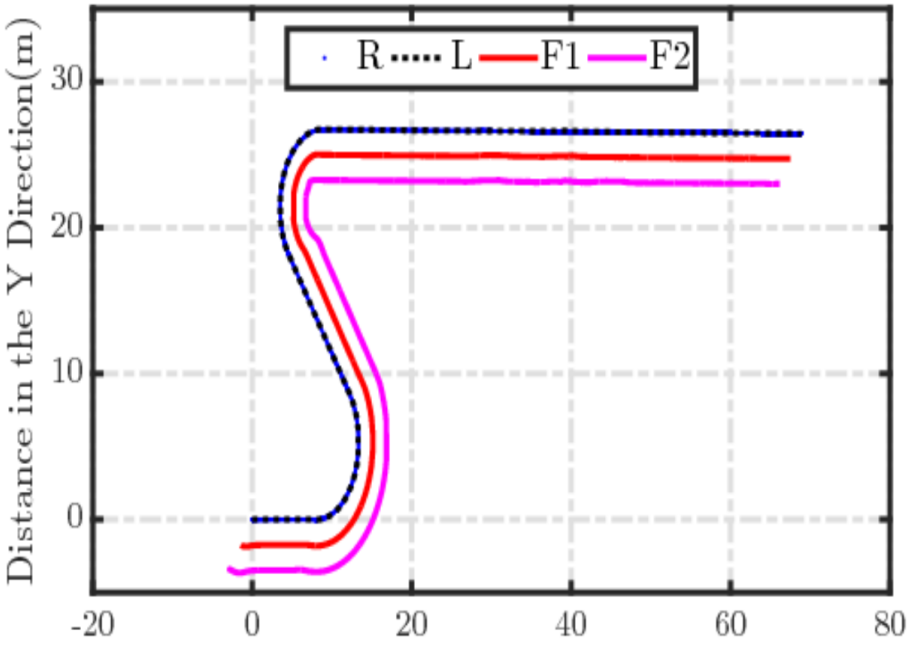

Figure 16. Formation trajectories after attack mitigation.

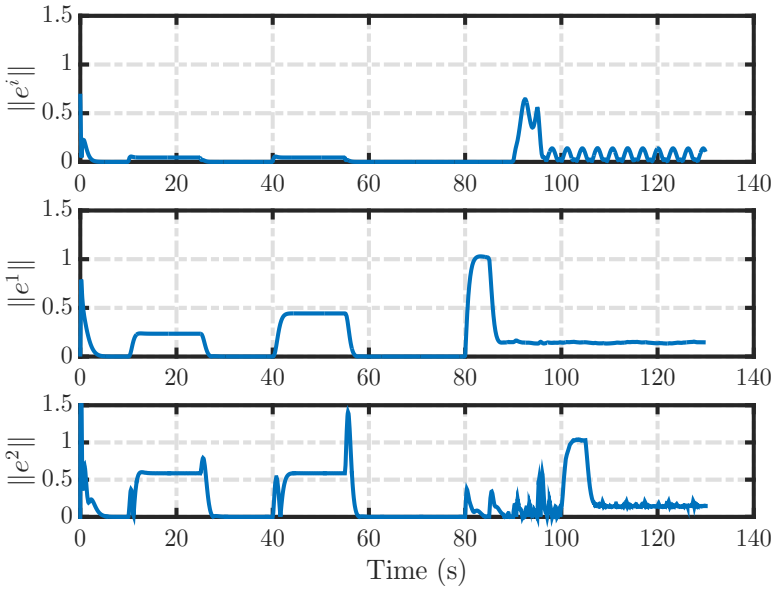

Figure 17. Tracking error norm with entire formation under attack.

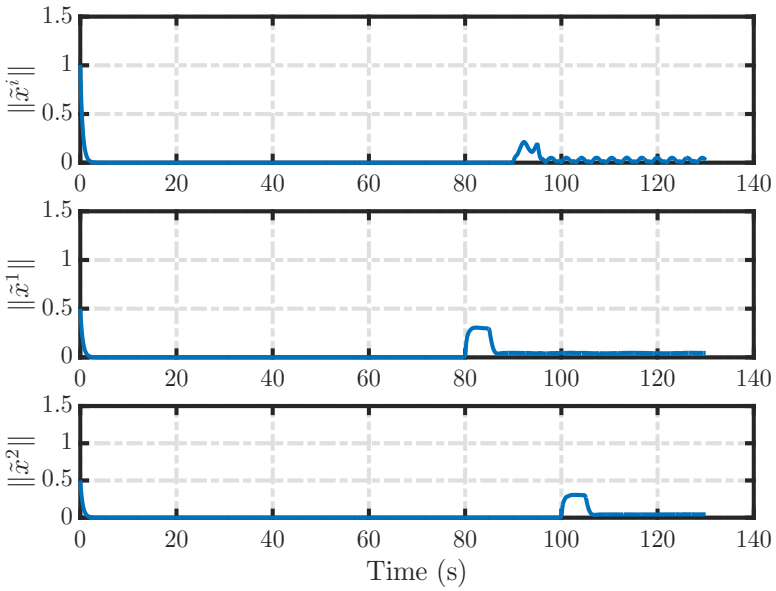

Figure 18. Estimation errors after attack mitigation.

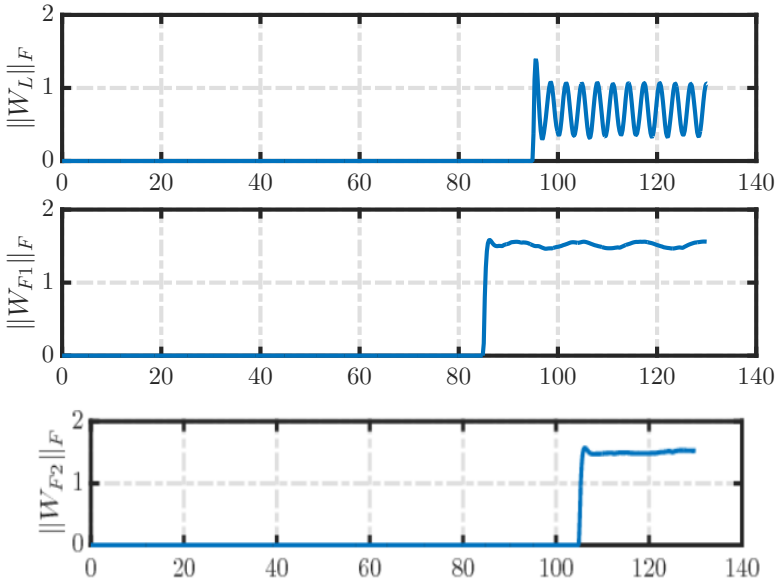

Figure 19. NN weight norms after attack mitigation.

6. CONCLUSION AND FUTURE WORK

In this work, an observer for the leader and the follower are designed that effectively estimated the state vector of the robots, and computed the torque required for tracking the assigned leader. For the given values of control gains k_p^o and observer gains l_p^o where $o = (i, j)$, and $p = (1, 2, \ldots, 5)$, the residual was found to converge asymptotically inn an attack-free scenario provided $\omega^r = 0$. In the instances when the tracking error norm of an assigned leader was non-zero, the tracking error norm of the follower was almost twice the tracking error of the assigned leader indicating that perturbations increase from the leader to all the followers at different levels whereas no such trend was seen for the residual signals. The residual stayed at zero as expected for the healthy case without attacks due to known dynamics but in the case of an actuator attack, the residual was shown to increase indicating the presence of an attack. Once the attack was detected, a mitigation scheme was initiated using an FLNN to learn the attack input online in order to reduce the effect of the attack input by modifying the controller.

Lyapunov stability analysis was used to prove that the overall closed-loop system has a much lower tracking and estimation error bound after the mitigation scheme is applied. It is important to obtain this tracking error bound as small as possible because the tracking errors after mitigation will still propagate down the hierarchy from the leaders to the followers at all levels. Simulation results show that the formation returns to close to normal conditions in a short duration once the attack input has been learned and mitigated.

It is important to note that there are no attacks on the sensors, communication network or the computation unit of the robots which may not be realistic. In addition, in this paper, the formation dynamics are considered to be known which is stringent. Future work will include relaxing the assumption that the sensors are attack-resilient.

REFERENCES

[1] Balch, T. and Arkin, R. C., 'Behavior-based formation control for multirobot teams,' IEEE transactions on robotics and automation, 1998, 14(6), pp. 926–939.

[2] Barnes, L., Fields, M., and Valavanis, K., 'Unmanned ground vehicle swarm formation control using potential fields,' in '2007 Mediterranean Conference on Control & Automation,' IEEE, 2007 pp. 1–8.

[3] Bianchin, G., Liu, Y.-C., and Pasqualetti, F., 'Secure navigation of robots in adversarial environments,' IEEE Control Systems Letters, 2019, 4(1), pp. 1–6.

[4] Brandao, A. S., Sarcinelli-Filho, M., Carelli, R., and Bastos-Filho, T. F., 'Decentralized control of leader-follower formations of mobile robots with obstacle avoidance,' in '2009 IEEE International Conference on Mechatronics,' IEEE, 2009 pp. 1–6.

[5] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., et al., 'Comprehensive experimental analyses of automotive attack surfaces.' in 'USENIX Security Symposium,' volume 4, San Francisco, 2011 pp. 447–462.

[6] Chen, Y. Q. and Wang, Z., 'Formation control: a review and a new consideration,' in '2005 IEEE/RSJ International conference on intelligent robots and systems,' IEEE, 2005 pp. 3181–3186.

[7] Desai, J. P., Ostrowski, J., and Kumar, V., 'Controlling formations of multiple mobile robots,' in 'Robotics and Automation, 1998. Proceedings. 1998 IEEE International Conference on,' volume 4, IEEE, 1998 pp. 2864–2869.

[8] Dierks, T., Brenner, B., and Jagannathan, S., 'Near optimal control of mobile robot formations,' in '2011 IEEE Symposium on Adaptive Dynamic Programming and Reinforcement Learning (ADPRL),' IEEE, 2011 pp. 234–241.

[9] Dierks, T. and Jagannathan, S., 'Control of nonholonomic mobile robot formations: Backstepping kinematics into dynamics,' in '2007 IEEE International Conference on Control Applications,' IEEE, 2007 pp. 94–99.

[10] Dierks, T. and Jagannathan, S., 'Neural network control of mobile robot formations using rise feedback,' IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2009, 39(2), pp. 332–347.

[11] Dierks, T. and Jagannathan, S., 'Neural network output feedback control of robot formations,' IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2010, 40(2), pp. 383–399.

[12] Fagiolini, A., Babboni, F., and Bicchi, A., 'Dynamic distributed intrusion detection for secure multi-robot systems,' in '2009 IEEE International Conference on Robotics and Automation,' IEEE, 2009 pp. 2723–2728.

[13] Fawzi, H., Tabuada, P., and Diggavi, S., 'Secure estimation and control for cyber-physical systems under adversarial attacks,' IEEE Transactions on Automatic control, 2014, 59(6), pp. 1454–1467.

[14] Fierro, R. and Lewis, F. L., 'Control of a nonholomic mobile robot: Backstepping kinematics into dynamics,' Journal of robotic systems, 1997, 14(3), pp. 149–163.

[15] Fierro, R. and Lewis, F. L., 'Control of a nonholonomic mobile robot using neural networks,' IEEE Transactions on neural networks, 1998, 9(4), pp. 589–600.

[16] Gerdes, R. M., Winstead, C., and Heaslip, K., 'Cps: an efficiency-motivated attack against autonomous vehicular transportation,' in 'Proceedings of the 29th Annual Computer Security Applications Conference,' ACM, 2013 pp. 99–108.

[17] Griffioen, P., Weerakkody, S., and Sinopoli, B., 'A moving target defense for securing cyber-physical systems,' arXiv preprint arXiv:1902.01423, 2019.

[18] Kanayama, Y., Kimura, Y., Miyazaki, F., and Noguchi, T., 'A stable tracking control method for an autonomous mobile robot,' in 'Proceedings., IEEE International Conference on Robotics and Automation,' IEEE, 1990 pp. 384–389.

[19] Kwon, C., Liu, W., and Hwang, I., 'Security analysis for cyber-physical systems against stealthy deception attacks,' in '2013 American control conference,' IEEE, 2013 pp. 3344–3349.

[20] Lewis, F. L., Dawson, D. M., and Abdallah, C. T., Robot manipulator control: theory and practice, CRC Press, 2003.

[21] Luo, C., Espinosa, A. P., Pranantha, D., and De Gloria, A., 'Multi-robot search and rescue team,' in '2011 IEEE International Symposium on Safety, Security, and Rescue Robotics,' IEEE, 2011 pp. 296–301.

[22] Mo, Y., Garone, E., Casavola, A., and Sinopoli, B., 'False data injection attacks against state estimation in wireless sensor networks,' in '49th IEEE Conference on Decision and Control (CDC),' IEEE, 2010 pp. 5967–5972.

[23] Mo, Y. and Sinopoli, B., 'Secure control against replay attacks,' in '2009 47th annual Allerton conference on communication, control, and computing (Allerton),' IEEE, 2009 pp. 911–918.

[24] Osterloh, C., Pionteck, T., and Maehle, E., 'Monsun ii: A small and inexpensive auv for underwater swarms,' in 'ROBOTIK 2012; 7th German Conference on Robotics,' VDE, 2012 pp. 1–6.

[25] Pajic, M., Weimer, J., Bezzo, N., Sokolsky, O., Pappas, G. J., and Lee, I., 'Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators,' IEEE Control Systems Magazine, 2017, 37(2), pp. 66–81.

[26] Pasqualetti, F., Dörfler, F., and Bullo, F., 'Attack detection and identification in cyber-physical systems,' IEEE transactions on automatic control, 2013, 58(11), pp. 2715–2729.

[27] Petit, J. and Shladover, S. E., 'Potential cyberattacks on automated vehicles,' IEEE Transactions on Intelligent Transportation Systems, 2014, 16(2), pp. 546–556.

[28] Ren, W., Beard, R. W., and Atkins, E. M., 'Information consensus in multivehicle cooperative control,' IEEE Control systems magazine, 2007, 27(2), pp. 71–82.

[29] Roberts, J. A., 'Satellite formation flying for an interferometry mission,' 2005.

[30] Schellenberger, C. and Zhang, P., 'Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system,' in '2017 IEEE 56th Annual Conference on Decision and Control (CDC),' IEEE, 2017 pp. 1374–1379.

[31] Shao, J., Xie, G., and Wang, L., 'Leader-following formation control of multiple mobile vehicles,' IET Control Theory & Applications, 2007, 1(2), pp. 545–552.

[32] Smith, R. S., 'A decoupled feedback structure for covertly appropriating networked control systems,' IFAC Proceedings Volumes, 2011, 44(1), pp. 90–95.

[33] van der Heijden, R., Lukaseder, T., and Kargl, F., 'Analyzing attacks on cooperative adaptive cruise control (cacc),' in '2017 IEEE Vehicular Networking Conference (VNC),' IEEE, 2017 pp. 45–52.

[34] Vuong, T. P., Loukas, G., Gan, D., and Bezemskij, A., 'Decision tree-based detection of denial of service and command injection attacks on robotic vehicles,' in '2015 IEEE International Workshop on Information Forensics and Security (WIFS),' IEEE, 2015 pp. 1–6.

[35] Wit, C. C. d., Khennouf, H., Samson, C., and Sordalen, O. J., 'Nonlinear control design for mobile robots,' in 'Recent trends in mobile robots,' pp. 121–156, World Scientific, 1993.

APPENDIX A.

BOUNDS

Bounds frequently used in the proofs are established here. The subscripts are intentionally ignored to avoid repetition.

$$\|v\| \leq v_{max} \quad \|\omega\| \leq \omega_{max} \quad \|\tau\| \leq \tau_{max}$$
$$\|\dot{v}\| \leq a_{max} \quad \|\dot{\omega}\| \leq \alpha_{max}$$
$$\theta, \theta^r, \theta^{\pi jr}, \theta_{rir} \epsilon (-\pi, \pi]$$
$$\tilde{n}_v = \frac{\mu_2}{m}\tilde{v}$$
$$\tilde{n}_\omega = \frac{\mu_4}{I}\tilde{\omega}.\|\overline{M}\|_F \leq M_b \tag{A-1}$$

Bounds for j^{th} follower robot are given by

$$|\tilde{v}_c^j| \leq \alpha_1^j|\tilde{L}^{\pi j}| + \alpha_2^j|\tilde{\Psi}^{\pi j}| + \alpha_3^j|\tilde{\theta}^j|$$
$$|\tilde{\omega}_c^j| \leq \frac{1}{d^j}\left\{\beta_1^j|\tilde{L}^{\pi j}| + \beta_2^j|\tilde{\Psi}^{\pi j}| + \beta_3^j|\tilde{\theta}^j|\right\}, \tag{A-2}$$

where $\alpha^j = \alpha_1^j + \alpha_2^j + \alpha_3^j$, and $\beta^j = \beta_1^j + \beta_2^j + \beta_3^j$, with α^j and α_p^j, $p = \{1,2,3\}$, being computable constants. The following functions are assumed to have Lipschitz bounds

$$|\tilde{f}_1^j| \leq \eta_2^j|\tilde{\Psi}^{\pi j}| + \eta_3^j|\tilde{\theta}^j| + \eta_4^j|\tilde{v}^j| + \eta_5^j|\tilde{\omega}^j|$$
$$|\tilde{f}_2^j| \leq \kappa_1^j|\tilde{L}^{\pi j}| + \kappa_2^j|\tilde{\Psi}^{\pi j}| + \kappa_3^j|\tilde{\theta}^j| + \kappa_4^j|\tilde{v}^j| + \kappa_5^j|\tilde{\omega}^j|, \tag{A-3}$$

where $\eta^j = \eta_2^j + \eta_3^j + \eta_4^j + \eta_5^j$ and $\kappa^j = \kappa_1^j + \kappa_2^j + \kappa_3^j + \kappa_4^j + \kappa_5^j$, with η^j, η_p^j for $p = \{2,3,4,5\}$ and κ_s^j for $s = \{1,2,3,4,5\}$ being computable constants.

Bounds for i^{th} leader robot are given by

$$|\tilde{v}_c^i| \leq \alpha_1^i|\tilde{\chi}^i| + \alpha_2^i|\tilde{y}^i| + \alpha_3^i|\tilde{\theta}^i|$$
$$|\tilde{\omega}_c^i| \leq \frac{1}{d^i}\left\{\beta_1^i|\tilde{\chi}^i| + \beta_2^i|\tilde{y}^i| + \beta_3^i|\tilde{\theta}^i|\right\}, \tag{A-4}$$

where $\alpha^i = \alpha_1^i + \alpha_2^i + \alpha_3^i$ and $\beta^i = \beta_1^i + \beta_2^i + \beta_3^i$, with α^i and α_p^i, $p = \{1,2,3\}$ being computable constants. The following functions are assumed to have Lipschitz bounds

$$
\begin{aligned}
|\tilde{f}_1^i| &\leq \eta_3^i|\tilde{\theta}^i| + \eta_4^i|\tilde{v}^i| + \eta_5^i|\tilde{\omega}^i| \\
|\tilde{f}_2^i| &\leq \kappa_3^i|\tilde{\theta}^i| + \kappa_4^i|\tilde{v}^i| + \kappa_5^i|\tilde{\omega}^i|,
\end{aligned} \tag{A-5}
$$

where $\eta^i = \eta_3^i + \eta_4^i + \eta_5^i$ and $\kappa^i = \kappa_3^i + \kappa_4^i + \kappa_5^i$, with η^i, η_p^i for $p = \{2,3,4,5\}$ and κ_s^i for $s = \{1,2,3,4,5\}$ being computable constants.

APPENDIX B.

PROOFS

Proof for Lemma 1. Let the Lyapunov function for the leader robot be given by

$$V_{x^i} = \frac{1}{2}({e_1^i}^2 + {e_2^i}^2 + d^i {e_3^i}^2 + {e_4^i}^2 + {e_5^i}^2). \tag{B-1}$$

Taking the derivative of (B-1) and substituting the position and orientation (11), and the velocity tracking error dynamics (13) gives

$$\begin{aligned}\dot{V}_{x^i} =& e_1^i \left(-k_1^i e_1^i + \omega^i e_2^i + e_4^i\right) + e_2^i \left(-k_2^i e_2^i - \omega^i e_1^i + d^i e_5^i + 2v^r \sin\left(\frac{e_3^i}{2}\right) \cos\left(\theta^r - \frac{\theta_r^i + \theta^i}{2}\right)\right) \\ &+ d^i e_3^i \left(-\frac{1}{d^i}(k_2^i e_2^i + k_3^i e_3^i) + e_5^i\right) + e_4^i \left(-k_4^i e_4^i\right) + e_5^i \left(-k_4^i e_5^i\right)\end{aligned}$$

$$\begin{aligned}\dot{V}_{x^i} =& - k_1^i {e_1^i}^2 - k_2^i {e_2^i}^2 - k_3^i {e_3^i}^2 - k_4^i {e_4^i}^2 - k_4^i {e_5^i}^2 + e_1^i e_4^i - k_2^i e_2^i e_3^i + d^i e_2^i e_5^i \\ &+ 2v^r e_2^i \sin(\frac{e_3^i}{2}) \cos(\theta^r - \frac{\theta_r^i + \theta^i}{2}) + d^i e_3^i e_5^i.\end{aligned} \tag{B-2}$$

The cross-terms can be simplified as

$$\begin{aligned} e_1^i e_4^i &= -\left(\frac{e_1^i}{\sqrt{2}} - \frac{e_4^i}{\sqrt{2}}\right)^2 + \frac{{e_1^i}^2}{2} + \frac{{e_4^i}^2}{2} \\ d^i e_2^i e_5^i &= -d^i \left(\frac{e_2^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}}\right)^2 + d^i \frac{{e_2^i}^2}{2} + d^i \frac{{e_5^i}^2}{2} \\ -k_2^i e_2^i e_3^i &= -k_2^i \left(\frac{e_2^i}{\sqrt{2}} + \frac{e_3^i}{\sqrt{2}}\right)^2 + k_2^i \frac{{e_2^i}^2}{2} + k_2^i \frac{{e_3^i}^2}{2} \\ d^i e_3^i e_5^i &= -d^i \left(\frac{e_3^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}}\right)^2 + d^i \frac{{e_3^i}^2}{2} + d^i \frac{{e_5^i}^2}{2}, \end{aligned} \tag{B-3}$$

which when back-substituted in (B-2) gives

$$\begin{aligned}\dot{V}_{x^i} =& -k_1^i {e_1^i}^2 + \frac{{e_1^i}^2}{2} - k_2^i {e_2^i}^2 + d^i \frac{{e_2^i}^2}{2} + k_2^i \frac{{e_2^i}^2}{2} - k_3^i {e_3^i}^2 + k_2^i \frac{{e_3^i}^2}{2} + d^i \frac{{e_3^i}^2}{2} - k_4^i {e_4^i}^2 \\ &+ \frac{{e_4^i}^2}{2} - k_4^i {e_5^i}^2 + d^i \frac{{e_5^i}^2}{2} + d^i \frac{{e_5^i}^2}{2} + 2v^r e_2^i \sin(\frac{e_3^i}{2}) \cos(\theta^r - \frac{\theta_r^i + \theta^i}{2}) \\ &- \left(\frac{e_1^i}{\sqrt{2}} - \frac{e_4^i}{\sqrt{2}}\right)^2 - d^i \left(\frac{e_2^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}}\right)^2 - k_2^i \left(\frac{e_2^i}{\sqrt{2}} + \frac{e_3^i}{\sqrt{2}}\right)^2 - d^i \left(\frac{e_3^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}}\right)^2. \end{aligned} \tag{B-4}$$

Bounding $2v^r e_2^i \sin(\frac{e_3^i}{2}) \cos(\theta^r - \frac{\theta_r^i + \theta^i}{2})$ by $v_{max}^r |e_2^i||e_3^i|$ since $|\sin\frac{e_3^i}{2}| \leq \frac{e_3^i}{2}$ $\forall e_3^i$ and applying Young's inequality gives

$$\begin{aligned}\dot{V}_{x^i} \leq& -\left(k_1^i - \frac{1}{2}\right) {e_1^i}^2 - \frac{1}{2}\left(k_2^i - d^i - v_{max}^r\right) {e_2^i}^2 \\ &- \left(k_3^i - \frac{k_2^i + v_{max}^r + d^i}{2}\right) {e_3^i}^2 - \left(k_4^i - \frac{1}{2}\right) {e_4^i}^2 - \left(k_4^i - d_i\right) {e_5^i}^2 \\ \leq& -\Gamma_1^i {e_1^i}^2 - \Gamma_2^i {e_2^i}^2 - \Gamma_3^i {e_3^i}^2 - \Gamma_4^i {e_4^i}^2 - \Gamma_5^i {e_5^i}^2. \end{aligned} \tag{B-5}$$

By selecting the appropriate gains k_1^i,k_2^i,k_3^i and k_4^i, positive Γ_p^i's ($p = 1, 2, ...5$), are obtained. Thus the derivative of the positive-definite Lyapunov function candidate in equation (B-1) is negative definite. Hence the tracking errors converge to zero asymptotically. □

Proof of Lemma 2. Let the Lyapunov function for the follower robot be given by

$$V_{x^j} = \frac{1}{2}(e_1^{j\,2} + e_2^{j\,2} + d^j e_3^{j\,2} + e_4^{j\,2} + e_5^{j\,2}). \tag{B-6}$$

Taking the derivative of (B-6) and substituting the position and orientation tracking error dynamics (12), and the velocity error dynamics (13) gives

$$\begin{aligned}\dot{V}_{x^j} =& -k_1^j {e_1^j}^2 - k_2^j {e_2^j}^2 - k_3^j {e_3^j}^2 - k_4^j {e_4^j}^2 - k_4^j {e_5^j}^2 + e_1^j e_4^j - k_3^j e_2^j e_3^j + d_j e_2^j e_5^j \\ &+ d^j e_3^j e_5^j + 2v^\pi e_2^j \sin(\frac{e_3^j}{2}) \cos(\theta_\pi - \frac{\theta_{jr} + \theta_j}{2}). \end{aligned} \tag{B-7}$$

The cross-terms are simplified in a similar manner as Lemma 1. The term $2v^{\pi}e_2^j \sin(\frac{e_3^j}{2})\cos(\theta^{\pi} - \frac{\theta_r^j+\theta^j}{2})$ is also simplified similarly, bounding it by $v_{max}^{\pi}|e_2^j||e_3^j|$ since $|\sin\frac{e_3^j}{2}| \leq \frac{e_3^j}{2}\ \forall e_3^j$. Next Young's Inequality is applied to (B-7) giving

$$\begin{aligned}\dot{V}_{x^j} \leq & -\left(k_1^j - \frac{1}{2}\right)e_1^{j\,2} - \left(k_2^j - \frac{k_3^j + v_{max}^{\pi} + d_j}{2}\right)e_2^{j\,2} \\ & - \frac{1}{2}\left(k_3^j - v_{max}^{\pi} - d_j\right)e_3^{j\,2} - \left(k_4^j - \frac{1}{2}\right)e_4^{j\,2} - \left(k_4^j - d_j\right)e_5^{j\,2} \\ \leq & -\Gamma_1^j e_1^{j\,2} - \Gamma_2^j e_2^{j\,2} - \Gamma_3^j e_3^{j\,2} - \Gamma_4^j e_4^{j\,2} - \Gamma_5^j e_5^{j\,2}. \end{aligned} \tag{B-8}$$

By selecting the appropriate gains k_1^j,k_2^j,k_3^j and k_4^j, positive Γ_p^j's $(p = 1, 2, ...5)$, are obtained. Thus the derivative of the Lyapunov in equation (B-6) is negative definite. Hence the tracking errors converge to zero asymptotically. □

Proof for Theorem 1. The Lyapunov candidate that shows the stability of the entire formation could be given by

$$V^{ij} = V_{x^i} + \sum_{j=1}^{N} V_{x^j}. \tag{B-9}$$

Taking the derivative of equation (B-9) gives

$$\dot{V}^{ij} = \dot{V}_{x^i} + \sum_{j=1}^{N} \dot{V}_{x^j}. \tag{B-10}$$

Lemma 1 and Lemma 2 shows that by the proper selection of gains k_p^o $(o = i, j = (1, \ldots, N))$, $(p = 1, 2, \ldots, 5)$, the position, orientation, and velocity tracking errors for the i^{th} leader and the j followers converge to zero asymptotically. After substituting equations (B-4) and (B-8) in equation (B-10), and stacking all the individual robot trajectory-tracking error vectors to get the augmented trajectory-tracking-error vector, the Lyapunov derivative can be rewritten as

$$\dot{V}^{ij} \leq \sum_{k} e^{k^T}\Gamma^k e^k \leq e^{ij^T}\Gamma e^{ij} - \lambda_{min}(\Gamma)\|e^{ij}\|^2, \tag{B-11}$$

where $\Gamma = \text{diag}\left(\Gamma^i, \Gamma^1, ..., \Gamma^N\right)$, and $\Gamma^o = \text{diag}\left(\Gamma^o_1, \Gamma^o_2, ..., \Gamma^o_5\right)$. Thus it can be seen that the Lyapunov function (B-9) has a N.D. derivative. Thus the formation is shown to be aymptotically stable when Lemmas 1 and 2 hold. This concludes the proof. □

Proof for Lemma 3. Let the Lyapunov candidate for showing the stability of the reference cart-leader tracking error dynamics and leader state estimation error dynamics is

$$V^i = V_{x^i} + V_{\tilde{x}^i}, \tag{B-12}$$

where V_{x^i} is itself a Lyapunov-like positive-definite function given by (B-1), and A positive-definite Lyapunov function candidate was considered to show the stability of the estimation error dynamics for the leader robot. It is given by

$$V_{\tilde{x}^i} = \frac{1}{2}\left(\tilde{x}^{i2} + \tilde{y}^{i2} + \tilde{\theta}^{i2} + \tilde{v}^{i2} + \tilde{\omega}^{i2}\right). \tag{B-13}$$

From Lemma 1, (34), (29), and bounds (A-1) and (A-5), the derivative of V_{x^i} is given by

$$\begin{aligned}\dot{V}_{x^i} =& -k^i_1 {e^i_1}^2 - k^i_2 {e^i_2}^2 - k^i_3 {e^i_3}^2 - k^i_4 {e^i_4}^2 - k^i_4 {e^i_5}^2 + e^i_1 e^i_4 - k^i_2 e^i_2 e^i_3 \\ &+ d^i e^i_2 e^i_5 + 2v^r e^i_2 \sin(\frac{e^i_3}{2}) \cos(\theta^r - \frac{\theta^i_r + \theta^i}{2}) + d^i e^i_3 e^i_5 - e^i_1 \tilde{v}^i_c - d^i e^i_2 \tilde{w}^i_c \\ &- d^i e^i_3 \tilde{w}^i_c + (k^i_4 - \frac{\mu^i_2}{m^i}) e^i_4 \tilde{v}^i + (k^i_4 - \frac{\mu^i_4}{I^i}) e^i_5 \tilde{\omega}^i. \end{aligned} \tag{B-14}$$

Some of the cross-terms can be simplified as per (B-3). Additional cross-terms can be simplified as

$$\begin{aligned}(k^i_4 - \frac{\mu^i_2}{m^i}) e^i_4 \tilde{v}^i &= -(k^i_4 - \frac{\mu^i_2}{m^i}) \left(\frac{e^i_4}{\sqrt{2}} - \frac{\tilde{v}^i}{\sqrt{2}}\right)^2 + (k^i_4 - \frac{\mu^i_2}{m^i}) \frac{{e^i_4}^2}{2} + (k^i_4 - \frac{\mu^i_2}{m^i}) \frac{\tilde{v}^{i2}}{2}, \\ (k^i_4 - \frac{\mu^i_4}{I^i}) e^i_5 \tilde{\omega}^i &= -(k^i_4 - \frac{\mu^i_4}{I^i}) \left(\frac{e^i_5}{\sqrt{2}} - \frac{\tilde{w}^i}{\sqrt{2}}\right)^2 + (k^i_4 - \frac{\mu^i_4}{I^i}) \frac{{e^i_5}^2}{2} + (k^i_4 - \frac{\mu^i_4}{I^i}) \frac{\tilde{w}^{i2}}{2}. \end{aligned} \tag{B-15}$$

Substituting these cross-terms in (B-14),

$$
\begin{aligned}
\dot{V}_{x^i} =& -k_1^i {e_1^i}^2 + \frac{{e_1^i}^2}{2} - k_2^i {e_2^i}^2 + d^i \frac{{e_2^i}^2}{2} + k_2^i \frac{{e_2^i}^2}{2} - k_3^i {e_3^i}^2 + k_2^i \frac{{e_3^i}^2}{2} + d^i \frac{{e_3^i}^2}{2} - k_4^i {e_4^i}^2 \\
&+ \frac{{e_4^i}^2}{2} + (k_4^i - \frac{\mu_2^i}{m^i}) \frac{{e_4^i}^2}{2} - k_4^i {e_5^i}^2 + d^i \frac{{e_5^i}^2}{2} + d^i \frac{{e_5^i}^2}{2} + (k_4^i - \frac{\mu_4^i}{I^i}) \frac{{e_5^i}^2}{2} \\
&+ 2v^r e_2^i \sin(\frac{e_3^i}{2}) \cos(\theta^r - \frac{\theta_r^i + \theta^i}{2}) - \left(\frac{e_1^i}{\sqrt{2}} - \frac{e_4^i}{\sqrt{2}} \right)^2 - d^i \left(\frac{e_2^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}} \right)^2 \\
&- k_2^i \left(\frac{e_2^i}{\sqrt{2}} + \frac{e_3^i}{\sqrt{2}} \right)^2 - d^i \left(\frac{e_3^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}} \right)^2 - (k_4^i - \frac{\mu_2^i}{m^i}) \left(\frac{e_4^i}{\sqrt{2}} - \frac{\tilde{v}^i}{\sqrt{2}} \right)^2 \\
&- (k_4^i - \frac{\mu_4^i}{I^i}) \left(\frac{e_5^i}{\sqrt{2}} - \frac{\tilde{w}^i}{\sqrt{2}} \right)^2 + (k_4^i - \frac{\mu_2^i}{m^i}) \frac{\tilde{v}^{i2}}{2} + (k_4^i - \frac{\mu_4^i}{I^i}) \frac{\tilde{w}^{i2}}{2} \\
&- e_1^i \tilde{v}_c^i - d^i e_2^i \tilde{w}_c^i - d^i e_3^i \tilde{w}_c^i \\
=& -\left(k_1^i - \frac{1}{2} \right) {e_1^i}^2 - \frac{1}{2} \left(k_2^i - d^i \right) {e_2^i}^2 - \left(k_3^i - \frac{k_2^i + d^i}{2} \right) {e_3^i}^2 - \frac{1}{2} \left(k_4^i + \frac{\mu_2^i}{m^i} - 1 \right) {e_4^i}^2 \\
&- \frac{1}{2} \left(k_4^i + \frac{\mu_4^i}{I^i} - 2d^i \right) {e_5^i}^2 + 2v^r e_2^i \sin(\frac{e_3^i}{2}) \cos(\theta^r - \frac{\theta_r^i + \theta^i}{2}) \\
&- \left(\frac{e_1^i}{\sqrt{2}} - \frac{e_4^i}{\sqrt{2}} \right)^2 - d^i \left(\frac{e_2^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}} \right)^2 - k_2^i \left(\frac{e_2^i}{\sqrt{2}} + \frac{e_3^i}{\sqrt{2}} \right)^2 - d^i \left(\frac{e_3^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}} \right)^2 \\
&- \left(k_4^i - \frac{\mu_2^i}{m^i} \right) \left(\frac{e_4^i}{\sqrt{2}} - \frac{\tilde{v}^i}{\sqrt{2}} \right)^2 - \left(k_4^i - \frac{\mu_4^i}{I^i} \right) \left(\frac{e_5^i}{\sqrt{2}} - \frac{\tilde{w}^i}{\sqrt{2}} \right)^2 \\
&+ (k_4^i - \frac{\mu_2^i}{m^i}) \frac{\tilde{v}^{i2}}{2} + (k_4^i - \frac{\mu_4^i}{I^i}) \frac{\tilde{w}^{i2}}{2} - e_1^i \tilde{v}_c^i - d^i e_2^i \tilde{w}_c^i - d^i e_3^i \tilde{w}_c^i. \qquad \text{(B-16)}
\end{aligned}
$$

Substituting the estimation dynamics from (35), the derivative of $V_{\tilde{x}^i}$ is given by

$$
\begin{aligned}
\dot{V}_{\tilde{x}^i} =& \tilde{\chi}^i \left(\tilde{f}_1^i - l_1^i \tilde{\chi}^i \right) + \tilde{y}^i \left(\tilde{f}_2^i - l_2^i \tilde{y}^i \right) + \tilde{\theta}^i \left(\tilde{f}_3^i - l_3^i \tilde{\theta}^i \right) + \tilde{v}^i \left(-l_4^i \tilde{v}^i - \tilde{n}_v^i \right) \\
&+ \tilde{\omega}^i \left(-l_4^i \tilde{\omega}^i - \tilde{n}_\omega^i \right) \\
\dot{V}_{\tilde{x}^i} =& -l_1^i \tilde{\chi}^{i2} - l_2^i \tilde{y}^{i2} - l_3^i \tilde{\theta}^{i2} - l_4^i \tilde{v}^{i2} - l_5^i \tilde{\omega}^{i2} + \tilde{\chi}^i \tilde{f}_1^i + \tilde{y}^i \tilde{f}_2^i + \tilde{\theta}^i \tilde{\omega}^i - \frac{\mu_2^i}{m^i} \tilde{v}^{i2} - \frac{\mu_4^i}{I^i} \tilde{\omega}^{i2}
\end{aligned}
$$

$$\dot{V}_{\tilde{x}^i} = -l_1^i \tilde{\chi}^{i2} - l_2^i \tilde{y}^{i2} - l_3^i \tilde{\theta}^{i2} - (l_4^i + \frac{\mu_2^i}{m^i})\tilde{v}^{i2} - (l_5^i + \frac{\mu_4^i}{I^i})\tilde{\omega}^{i2} + \tilde{\chi}^i \tilde{f}_1 + \tilde{y}^i \tilde{f}_2 + \tilde{\theta}^i \tilde{\omega}^i. \tag{B-17}$$

From (B-17) and (B-16), the derivative of (B-12) is

$$\begin{aligned}
\dot{V}^i = & -\left(k_1^i - \frac{1}{2}\right) {e_1^i}^2 - \frac{1}{2}\left(k_2^i - d^i\right) {e_2^i}^2 - \left(k_3^i - \frac{k_2^i + d^i}{2}\right) {e_3^i}^2 - \frac{1}{2}\left(k_4^i + \frac{\mu_2^i}{m^i} - 1\right) {e_4^i}^2 \\
& - \frac{1}{2}\left(k_4^i + \frac{\mu_4^i}{I^i} - 2d^i\right) {e_5^i}^2 - l_1^i \tilde{\chi}^{i2} - l_2^i \tilde{y}^{i2} - l_3^i \tilde{\theta}^{i2} - (l_4^i + \frac{\mu_2^i}{m^i})\tilde{v}^{i2} + (k_4^i - \frac{\mu_2^i}{m^i})\frac{\tilde{v}^{i2}}{2} \\
& - (l_5^i + \frac{\mu_4^i}{I^i})\tilde{\omega}^{i2} + (k_4^i - \frac{\mu_4^i}{I^i})\frac{\tilde{w}^{i2}}{2} + 2v^r e_2^i \sin(\frac{e_3^i}{2})\cos(\theta^r - \frac{\theta_r^i + \theta^i}{2}) \\
& - \left(\frac{e_1^i}{\sqrt{2}} - \frac{e_4^i}{\sqrt{2}}\right)^2 - d^i \left(\frac{e_2^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}}\right)^2 - k_2^i \left(\frac{e_2^i}{\sqrt{2}} + \frac{e_3^i}{\sqrt{2}}\right)^2 - d^i \left(\frac{e_3^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}}\right)^2 \\
& - (k_4^i - \frac{\mu_2^i}{m^i})\left(\frac{e_4^i}{\sqrt{2}} - \frac{\tilde{v}^i}{\sqrt{2}}\right)^2 - (k_4^i - \frac{\mu_4^i}{I^i})\left(\frac{e_5^i}{\sqrt{2}} - \frac{\tilde{w}^i}{\sqrt{2}}\right)^2 \\
& - e_1^i \tilde{v}_c^i - d^i e_2^i \tilde{w}_c^i - d^i e_3^i \tilde{w}_c^i + \tilde{\chi}^i \tilde{f}_1 + \tilde{y}^i \tilde{f}_2 + \tilde{\theta}^i \tilde{\omega}^i \\
= & -\left(k_1^i - \frac{1}{2}\right) {e_1^i}^2 - \frac{1}{2}\left(k_2^i - d^i\right) {e_2^i}^2 - \left(k_3^i - \frac{k_2^i + d^i}{2}\right) {e_3^i}^2 - \frac{1}{2}\left(k_4^i + \frac{\mu_2^i}{m^i} - 1\right) {e_4^i}^2 \\
& - \frac{1}{2}\left(k_4^i + \frac{\mu_4^i}{I^i} - 2d^i\right) {e_5^i}^2 - l_1^i \tilde{\chi}^{i2} - l_2^i \tilde{y}^{i2} - l_3^i \tilde{\theta}^{i2} - \left(l_4^i + \frac{3\mu_2^i}{2m^i} - \frac{k_4^i}{2}\right)\tilde{v}^{i2} \\
& - \left(l_5^i + \frac{3\mu_4^i}{2I^i} - \frac{k_4^i}{2}\right)\tilde{\omega}^{i2} + 2v^r e_2^i \sin(\frac{e_3^i}{2})\cos(\theta^r - \frac{\theta_r^i + \theta^i}{2}) \\
& - \left(\frac{e_1^i}{\sqrt{2}} - \frac{e_4^i}{\sqrt{2}}\right)^2 - d^i \left(\frac{e_2^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}}\right)^2 - k_2^i \left(\frac{e_2^i}{\sqrt{2}} + \frac{e_3^i}{\sqrt{2}}\right)^2 - d^i \left(\frac{e_3^i}{\sqrt{2}} - \frac{e_5^i}{\sqrt{2}}\right)^2 \\
& - (k_4^i - \frac{\mu_2^i}{m^i})\left(\frac{e_4^i}{\sqrt{2}} - \frac{\tilde{v}^i}{\sqrt{2}}\right)^2 - (k_4^i - \frac{\mu_4^i}{I^i})\left(\frac{e_5^i}{\sqrt{2}} - \frac{\tilde{w}^i}{\sqrt{2}}\right)^2 \\
& - e_1^i \tilde{v}_c^i - d^i e_2^i \tilde{w}_c^i - d^i e_3^i \tilde{w}_c^i + \tilde{\chi}^i \tilde{f}_1 + \tilde{y}^i \tilde{f}_2 + \tilde{\theta}^i \tilde{\omega}^i
\end{aligned}$$

$$
\begin{aligned}
\leq & -\left(k_1^i - \frac{1}{2}\right) {e_1^i}^2 - \frac{1}{2}\left(k_2^i - d^i\right) {e_2^i}^2 - \left(k_3^i - \frac{k_2^i + d^i}{2}\right) {e_3^i}^2 - \frac{1}{2}\left(k_4^i + \frac{\mu_2^i}{m^i} - 1\right) {e_4^i}^2 \\
& - \frac{1}{2}\left(k_4^i + \frac{\mu_4^i}{I^i} - 2d^i\right) {e_5^i}^2 - l_1^i \tilde{\chi}^{i2} - l_2^i \tilde{y}^{i2} - l_3^i \tilde{\theta}^{i2} - \left(l_4^i + \frac{3\mu_2^i}{2m^i} - \frac{k_4^i}{2}\right) \tilde{v}^{i2} \\
& - \left(l_5^i + \frac{3\mu_4^i}{2I^i} - \frac{k_4^i}{2}\right) \tilde{\omega}^{i2} + |2v^r e_2^i \sin(\frac{e_3^i}{2}) \cos(\theta^r - \frac{\theta_r^i + \theta^i}{2})| \\
& + |e_1^i||\tilde{v}_c^i| + d^i|e_2^i||\tilde{w}_c^i| + d^i|e_3^i||\tilde{w}_c^i| + |\tilde{\chi}^i||\tilde{f}_1| + |\tilde{y}^i||\tilde{f}_2| + |\tilde{\theta}^i||\tilde{\omega}^i|. \qquad \text{(B-18)}
\end{aligned}
$$

Using bounds (A-4) and (A-5), and applying Young's inequality,

$$
\begin{aligned}
& |e_1^i||\tilde{v}_c^i| + d^i|e_2^i||\tilde{w}_c^i| + d^i|e_3^i||\tilde{w}_c^i| + |\tilde{\chi}^i||\tilde{f}_1| + |\tilde{y}^i||\tilde{f}_2| + |\tilde{\theta}^i||\tilde{\omega}^i| \\
& \leq |e_1^i| \left\{\alpha_1^i|\tilde{\chi}^i| + \alpha_2^i|\tilde{y}^i| + \alpha_3^i|\tilde{\theta}^i|\right\} + d^i|e_2^i| \times \frac{1}{d^i}\left\{\beta_1^i|\tilde{\chi}^i| + \beta_2^i|\tilde{y}^i| + \beta_3^i|\tilde{\theta}^i|\right\} \\
& \quad + d^i|e_3^i| \times \frac{1}{d^i}\left\{\beta_1^i|\tilde{\chi}^i| + \beta_2^i|\tilde{y}^i| + \beta_3^i|\tilde{\theta}^i|\right\} + |\tilde{\chi}^i|\left\{\eta_3^i|\tilde{\theta}^i| + \eta_4^i|\tilde{v}^i| + \eta_5^i|\tilde{\omega}^i|\right\} \\
& \quad + |\tilde{y}^i|\left\{\kappa_3^i|\tilde{\theta}^i| + \kappa_4^i|\tilde{v}^i| + \kappa_5^i|\tilde{\omega}^i|\right\} + |\tilde{\theta}^i||\tilde{\omega}^i| \\
& \leq \frac{\alpha^i}{2}{e_1^i}^2 + \frac{\beta^i}{2}{e_2^i}^2 + \frac{\beta^i}{2}{e_3^i}^2 + \frac{1}{2}\left(\eta^i + \alpha_1^i + 2\beta_1^i\right)\tilde{\chi}^{i2} + \frac{1}{2}\left(\kappa^i + \alpha_2^i + 2\beta_2^i\right)\tilde{y}^{i2} \\
& \quad + \frac{1}{2}\left(\eta_3^i + \kappa_3^i + \alpha_3^i + 2\beta_3^i + 1\right)\tilde{\theta}^{i2} + \frac{1}{2}\left(\eta_4^i + \kappa_4^i\right)\tilde{v}^{i2} + \frac{1}{2}\left(\eta_5^i + \kappa_5^i + 1\right)\tilde{\omega}^{i2}. \qquad \text{(B-19)}
\end{aligned}
$$

It was seen in Lemma 1 that $|2v^r e_2^i \sin(\frac{e_3^i}{2}) \cos(\theta^r - \frac{\theta_r^i + \theta^i}{2})| \leq v_{max}^r |e_2^i||e_3^i|$. Substituting the results from (B-19) in (B-18) gives

$$
\begin{aligned}
\dot{V}^i \leq & -\left(k_1^i - \frac{1}{2} - \frac{\alpha^i}{2}\right) {e_1^i}^2 - \frac{1}{2}\left(k_2^i - d^i - v_{max}^r - \beta^i\right) {e_2^i}^2 - \left(k_3^i - \frac{k_2^i + d^i + v_{max}^r + \beta^i}{2}\right) {e_3^i}^2 \\
& - \frac{1}{2}\left(k_4^i + \frac{\mu_2^i}{m^i} - 1\right) {e_4^i}^2 - \frac{1}{2}\left(k_4^i + \frac{\mu_4^i}{I^i} - 2d^i\right) {e_5^i}^2 - \left(l_1^i - \frac{1}{2}\left(\eta^i + \kappa_1^i + \alpha_1^i + 2\beta_1^i\right)\right) \tilde{\chi}^{i2} \\
& - \left(l_2^i - \frac{1}{2}\left(\kappa^i + \alpha_2^i + 2\beta_2^i\right)\right) \tilde{y}^{i2} - \left(l_3^i - \frac{1}{2}\left(\eta_3^i + \kappa_3^i + \alpha_3^i + 2\beta_3^i + 1\right)\right) \tilde{\theta}^{i2} \\
& - \left(l_4^i + \frac{3\mu_2^i}{2m^i} - \frac{1}{2}\left(\eta_4^i + \kappa_4^i + k_4^i\right)\right) \tilde{v}^{i2} - \left(l_5^i + \frac{3\mu_4^i}{2I^i} - \frac{1}{2}\left(\eta_5^i + \kappa_5^i + k_4^i + 1\right)\right) \tilde{\omega}^{i2}
\end{aligned}
$$

$$\dot{V}^i \leq -\Lambda_1^i {e_1^i}^2 - \Lambda_2^i {e_2^i}^2 - \Lambda_3^i {e_3^i}^2 - \Lambda_4^i {e_4^i}^2 - \Lambda_5^i {e_5^i}^2 - \Omega_1^i {\tilde{\chi}^i}^2 - \Omega_2^i {\tilde{y}^i}^2 - \Omega_3^i {\tilde{\theta}^i}^2 - \Omega_4^i {\tilde{v}^i}^2 - \Omega_5^i {\tilde{\omega}^i}^2. \tag{B-20}$$

Thus, $\dot{V}_i$ is negative definite (N.D.). Thus by proper selection of the observer and controller gains the control velocity estimate makes the robot tracking error and the estimation error converge to zero asymptotically. This concludes the proof. □

Proof for Lemma 4. Let the Lyapunov candidate chosen for showing the stability of the leader-follower tracking error dynamics and estimation error dynamics be given as

$$V^j = V_{x^j} + V_{\tilde{x}^j}. \tag{B-21}$$

Consider the positive-definite Lyapunov function candidate for the follower robot state estimation error given by

$$V_{\tilde{x}^j} = \frac{1}{2}\left(\tilde{L}^{\pi j 2} + \tilde{\Psi}^{\pi j 2} + \tilde{\theta}^{j 2} + \tilde{v}^{j 2} + \tilde{\omega}^{j 2}\right), \tag{B-22}$$

and let the Lyapunov function for the follower be chosen as in (B-6). From Lemma 2, (34) and (30)

$$\begin{aligned}\dot{V}_{x^j} = &-\left(k_1^j - \frac{1}{2}\right) {e_1^j}^2 - \left(k_2^j - \frac{k_3^j + d_j}{2}\right) {e_2^j}^2 - \frac{1}{2}\left(k_3^j - d_j\right) {e_3^j}^2 \\ &- \frac{1}{2}\left(k_4^j + \frac{\mu_2^j}{m^j} - 1\right) {e_4^j}^2 - \frac{1}{2}\left(k_4^j + \frac{\mu_4^j}{I^j} - 2d^j\right) {e_5^j}^2 \\ &+ 2v^\pi e_2^j \sin(\frac{e_3^j}{2}) \cos(\theta_\pi - \frac{\theta_{jr} + \theta_j}{2}) - e_1^j \tilde{v}_c^j - d^j e_2^j \tilde{\omega}_c^j - d^j e_3^j \tilde{\omega}_c^j.\end{aligned} \tag{B-23}$$

Substituting the estimation error dynamics from equation (35),

$$\dot{V}_{\tilde{x}^j} = \tilde{L}^{\pi j}\left(\tilde{f}_{j1} - l_1^j \tilde{L}^{\pi j}\right) + \tilde{\Psi}^{\pi j}\left(\tilde{f}_{j2} - l_2^j \tilde{\Psi}^{\pi j}\right) + \tilde{\theta}^j\left(\tilde{f}_{j3} - l_3^j \tilde{\theta}_j\right) + \tilde{v}^j\left(-l_4^j \tilde{v}_j - \tilde{n}_v\right)$$

$$
\begin{aligned}
&+ \tilde{\omega}^j \left(-l_4^j \tilde{\omega}_j - \tilde{n}_\omega\right) \\
\dot{V}_{\tilde{x}_j} =& - l_1^j \tilde{L}^{\pi j^2} - l_2^j \tilde{\Psi}^{\pi j^2} - l_3^j \tilde{\theta}^{j^2} - l_4^j \tilde{v}^{j^2} - l_5^j \tilde{\omega}^{j^2} + \tilde{L}^{\pi j} \tilde{f}_{j1} + \tilde{\Psi}^{\pi j} \tilde{f}_{j2} + \tilde{\theta}_j \tilde{\omega}^j - \frac{\mu_2^j}{m} \tilde{v}^{j^2} \\
&- \frac{\mu_4^j}{I} \tilde{\omega}^{j^2} \\
\dot{V}_{\tilde{x}_j} =& - l_1^j \tilde{L}^{\pi j^2} - l_2^j \tilde{\Psi}^{\pi j^2} - l_3^j \tilde{\theta}^{j^2} - (l_4^j + \frac{\mu_2^j}{m}) \tilde{v}^{j^2} - (l_4^j + \frac{\mu_4^j}{I}) \tilde{\omega}^{j^2} + \tilde{L}^{\pi j} \tilde{f}_{j1} + \tilde{\Psi}^{\pi j} \tilde{f}_{j2} \\
&+ \tilde{\theta}_j \tilde{\omega}^j . \qquad \text{(B-24)}
\end{aligned}
$$

From (B-24) and (B-23)

$$
\begin{aligned}
\dot{V}_j =& - \left(k_1^j - \frac{1}{2}\right) e_1^{j^2} - \left(k_2^j - \frac{k_3^j + d_j}{2}\right) e_2^{j^2} - \frac{1}{2} \left(k_3^j - d_j\right) e_3^{j^2} \\
&- \frac{1}{2} \left(k_4^j + \frac{\mu_2^j}{m^j} - 1\right) e_4^{j^2} - \frac{1}{2} \left(k_4^j + \frac{\mu_4^j}{I^j} - 2d^j\right) e_5^{j^2} \\
&+ 2v^\pi e_2^j \sin(\frac{e_3^j}{2}) \cos(\theta_\pi - \frac{\theta_{jr} + \theta_j}{2}) - e_1^j \tilde{v}_c^j - d^j e_2^j \tilde{\omega}_c^j - d^j e_3^j \tilde{\omega}_c^j \\
&- l_1^j \tilde{L}^{\pi j^2} - l_2^j \tilde{\Psi}^{\pi j^2} - l_3^j \tilde{\theta}^{j^2} - (l_4^j + \frac{\mu_2^j}{m}) \tilde{v}^{j^2} - (l_4^j + \frac{\mu_4^j}{I}) \tilde{\omega}^{j^2} + \tilde{L}^{\pi j} \tilde{f}_{j1} \\
&+ \tilde{\Psi}^{\pi j} \tilde{f}_{j2} + \tilde{\theta}_j \tilde{\omega}^j + \frac{1}{2} (k_4^j - \frac{\mu_2^j}{m^j}) \tilde{v}^{j^2} + \frac{1}{2} (k_4^j - \frac{\mu_4^j}{I^j}) \tilde{\omega}^{j^2} . \qquad \text{(B-25)}
\end{aligned}
$$

Substituting bounds (A-1)-(A-3), (A-5) and applying Young's inequality,

$$
\begin{aligned}
\dot{V}^j \leq& - \left(k_1^j - \frac{1}{2} - \frac{\alpha^j}{2}\right) e_1^{j^2} - \left(k_2^j - \frac{k_3^j + d_j}{2} - \frac{\beta^j}{2}\right) e_2^{j^2} - \frac{1}{2} \left(k_3^j - d_j - \frac{\beta^j}{2}\right) e_3^{j^2} \\
&- \frac{1}{2} \left(k_4^j + \frac{\mu_2^j}{m^j} - 1\right) e_4^{j^2} - \frac{1}{2} \left(k_4^j + \frac{\mu_4^j}{I^j} - 2d^j -\right) e_5^{j^2} \\
&- \left(l_1^j - \frac{1}{2} \left(\eta^j + \kappa_1^j + \alpha_1^j + 2\beta_1^j\right)\right) \tilde{L}^{\pi j^2} - \left(l_2^j - \frac{1}{2} \left(\eta_2^j + \kappa_2^j + \kappa^j + \alpha_2^j + 2\beta_2^j\right)\right) \tilde{\Psi}^{\pi j^2} \\
&- \left(l_3^j - \frac{1}{2} \left(\eta_3^j + \kappa_3^j + \alpha_3^j + 2\beta_3^j + 1\right)\right) \tilde{\theta}^{j^2} - \left(l_4^j + \frac{3\mu_2^j}{2m^j} - \frac{1}{2} \left(\eta_4^j + \kappa_4^j + k_4^j\right)\right) \tilde{v}^{j^2} \\
&- \left(l_5^j + \frac{3\mu_4^j}{2I^j} - \frac{1}{2} \left(\eta_5^j + \kappa_5^j + k_4^j + 1\right)\right) \tilde{\omega}^{j^2}
\end{aligned}
$$

$$\dot{V}^j \leq -\Lambda_1^j {e_1^j}^2 - \Lambda_2^j {e_2^j}^2 - \Lambda_3^j {e_3^j}^2 - \Lambda_4^j {e_4^j}^2 - \Lambda_5^j {e_5^j}^2 - \Omega_1^j {\tilde{L}^{\pi j}}^2 - \Omega_2^j {\tilde{\Psi}^{\pi j}}^2 - \Omega_3^j {\tilde{\theta}^j}^2 - \Omega_4^j {\tilde{v}^j}^2 - \Omega_5^j {\tilde{\omega}^j}^2. \quad \text{(B-26)}$$

Thus, by proper selection of observer and controller gains the control velocity estimate makes the robot tracking error and the estimation error go to zero asymptotically. This concludes the proof. □

Proof for Theorem 2. The Lyapunov candidate that shows the stability of the entire formation could be taken as (B-9), The derivative is, $\dot{V}^{ij} = \dot{V}^i + \sum_{j=1}^{N} \dot{V}^j$. Therefore,

$$\dot{V}^{ij} \leq -\lambda_{min}(\Lambda^i)\|e^i\|^2 - \lambda_{min}(\Omega^i)\|\tilde{x}^i\|^2 + \sum_{j=1}^{N} \left(-\lambda_{min}(\Lambda^j)\|e^j\|^2 - \lambda_{min}(\Omega^j)\|\tilde{x}^j\|^2\right)$$

Let $\Lambda = \text{diag}\left(\Lambda^i, \Lambda^1, ..., \Lambda^N\right)$, and $\Omega = \text{diag}(\Omega^i, \Omega^1, ..., \Omega^N)$.

$$\therefore \dot{V}^{ij} \leq -\lambda_{min}(\Lambda)\|e^{ij}\|^2 - \lambda_{min}(\Omega)\|\tilde{x}^{ij}\|^2$$

$$\therefore \dot{V}^{ij} \leq 0$$

It has been shown that the healthy residual threshold for each robot in the formation is zero. This is logical since the dynamics are known. Therefore, by the proper selection of control gains k_{op}, and observer gains l_{op}, where $(o = (i, j), j = (1, ..., N))$, and $(p = 1, 2, ..., 5)$, the augmented tracking errors and estimation errors for the formation goes to zero asymptotically. Alternatively, the robot tracking and estimation errors can be said to be bounded by $\rho_{b1}^i = 0$. This concludes the proof. □

Proof for Lemma 5. In the presence of actuator attack on the leader, the derivative of the Lyapunov candidate used to prove stability in Lemma 3 is modified as

$$\begin{aligned}\dot{V}^i \leq & -\Lambda_1^i {e_1^i}^2 - \Lambda_2^i {e_2^i}^2 - \Lambda_3^i {e_3^i}^2 - \Lambda_4^i {e_4^i}^2 - \Lambda_5^i {e_5^i}^2 - \Omega_1^i \tilde{\chi}^{i2} - \Omega_2^i \tilde{y}^{i2} - \Omega_3^i \tilde{\theta}^{i2} \\ & - \Omega_4^i \tilde{v}^{i2} - \Omega_5^i \tilde{\omega}^{i2} + |e_4^i \frac{w_v^i}{m^i}| + |e_5^i \frac{w_\omega^i}{I^i}| + |\tilde{v}^i \frac{w_v^i}{m^i}| + |\tilde{\omega}^i \frac{w_\omega^i}{I^i}|. \end{aligned} \tag{B-27}$$

Using Young's inequality on the cross-terms,

$$\begin{aligned}\dot{V}^i \leq & -\Lambda_1^i {e_1^i}^2 - \Lambda_2^i {e_2^i}^2 - \Lambda_3^i {e_3^i}^2 - \Lambda_4^i {e_4^i}^2 - \Lambda_5^i {e_5^i}^2 - \Omega_1^i \tilde{\chi}^{i2} - \Omega_2^i \tilde{y}^{i2} - \Omega_3^i \tilde{\theta}^{i2} \\ & - \Omega_4^i \tilde{v}^{i2} - \Omega_5^i \tilde{\omega}^{i2} + \frac{1}{2m^i} {e_4^i}^2 + \frac{{w_v^i}^2}{2m^i} + \frac{1}{2I^i} {e_5^i}^2 + \frac{{w_\omega^i}^2}{2I^i} + \frac{1}{2m^i} \tilde{v}^{i2} + \frac{{w_v^i}^2}{2m^i} \\ & + \frac{1}{2I^i} \tilde{\omega}^{i2} + \frac{{w_\omega^i}^2}{2I^i} \\ \leq & -\Lambda_1^i {e_1^i}^2 - \Lambda_2^i {e_2^i}^2 - \Lambda_3^i {e_3^i}^2 - (\Lambda_4^i - \frac{1}{2m^i}) {e_4^i}^2 - (\Lambda_5^i - \frac{1}{2I^i}) {e_5^i}^2 - \Omega_1^i \tilde{\chi}^{i2} - \Omega_2^i \tilde{y}^{i2} \\ & - \Omega_3^i \tilde{\theta}^{i2} - (\Omega_4^i - \frac{1}{2m^i}) \tilde{v}^{i2} - (\Omega_5^i - \frac{1}{2I^i}) \tilde{\omega}^{i2} + \frac{{w_{vb}^i}^2}{m^i} + \frac{{w_{\omega b}^i}^2}{I^i}. \end{aligned} \tag{B-28}$$

Taking $\rho_{b2}^i = \frac{{w_{vb}^i}^2}{m^i} + \frac{{w_{\omega b}^i}^2}{I^i}$, $\dot{V}_i \leq 0$ if the following error bounds with an OR condition are satisfied,

$$\begin{aligned} |e_p^i| \geq & \sqrt{\frac{\rho_{b2}^i}{\Lambda_{ip}}} & |e_4^i| \geq & \sqrt{\frac{\rho_{b2}^i}{\Lambda_4^i - \frac{1}{2m^i}}} \\ |e_5^i| \geq & \sqrt{\frac{\rho_{b2}^i}{\Lambda_5^i - \frac{1}{2I^i}}} & |\tilde{\chi}^i| \geq & \sqrt{\frac{\rho_{b2}^i}{\Omega_1^i}} \\ |\tilde{y}^i| \geq & \sqrt{\frac{\rho_{b2}^i}{\Omega_2^i}} & |\tilde{\theta}^i| \geq & \sqrt{\frac{\rho_{b2}^i}{\Omega_3^i}} \\ |\tilde{v}^i| \geq & \sqrt{\frac{\rho_{b2}^i}{\Omega_4^i - \frac{1}{2m^i}}} & |\tilde{\omega}^i| \geq & \sqrt{\frac{\rho_{b2}^i}{\Omega_5^i - \frac{1}{2I^i}}}, \end{aligned} \tag{B-29}$$

where $p = (1, 2, 3)$. Comparing these bounds with the bounds obtained previously ($\rho^i_{b1} = 0$), it can be shown that the bounded actuator attack signal w_i increases the error bound but, the system stays UUB. Alternately,

$$||e^i|| \geq \sqrt{\frac{\rho^i_{b2}}{\lambda_{min}(\overline{\Lambda}^i)}} \quad \text{OR} \quad ||\tilde{x}^i|| \geq \sqrt{\frac{\rho^i_{b2}}{\lambda_{min}(\overline{\Omega}^i)}}, \tag{B-30}$$

where $\overline{\Lambda}^k = \text{diag}\left\{\Lambda^k_1, \Lambda^k_2, \Lambda^k_3, \left(\Lambda^k_4 - \frac{1}{2m^k}\right), \left(\Lambda^k_5 - \frac{1}{2I^k}\right)\right\}$, and
$\overline{\Omega}^k = \text{diag}\left\{\Omega^k_1, \Omega^k_2, \Omega^k_3, \left(\Omega^k_4 - \frac{1}{2m^k}\right), \left(\Omega^k_5 - \frac{1}{2I^k}\right)\right\}$. This concludes the proof. □

Proof for Lemma 6. In the presence of actuator attack on the follower, the derivative of the Lyapunov candidate used to prove stability in Lemma 4 is modified as

$$\begin{aligned}
\dot{V}_j \leq & -\Lambda^j_1 {e^j_1}^2 - \Lambda^j_2 {e^j_2}^2 - \Lambda^j_3 {e^j_3}^2 - \Lambda^j_4 {e^j_4}^2 - \Lambda^j_5 {e^j_5}^2 - \Omega^j_1 {\tilde{L}^{\pi j}}^2 - \Omega^j_2 {\tilde{\Psi}^{\pi j}}^2 - \Omega^j_3 {\tilde{\theta}^j}^2 \\
& - \Omega^j_4 {\tilde{v}^j}^2 - \Omega^j_5 {\tilde{\omega}^j}^2 + |e^j_4 \frac{w^j_v}{m^j}| + |e^j_5 \frac{w^j_\omega}{I^j}| + |\tilde{v}^j \frac{w^j_v}{m^j}| + |\tilde{\omega}^j \frac{w^j_\omega}{I^j}| \\
\leq & -\Lambda^j_1 {e^j_1}^2 - \Lambda^j_2 {e^j_2}^2 - \Lambda^j_3 {e^j_3}^2 - \Lambda^j_4 {e^j_4}^2 - \Lambda^j_5 {e^j_5}^2 - \Omega^j_1 {\tilde{L}^{\pi j}}^2 - \Omega^j_2 {\tilde{\Psi}^{\pi j}}^2 - \Omega^j_3 {\tilde{\theta}^j}^2 - \Omega^j_4 {\tilde{v}^j}^2 \\
& - \Omega^j_5 {\tilde{\omega}^j}^2 + \frac{1}{2m^j} {e^j_4}^2 + \frac{{w^j_v}^2}{2m^j} + \frac{1}{2I^j} {e^j_5}^2 + \frac{{w^j_\omega}^2}{2I^j} + \frac{1}{2m^j} {\tilde{v}_j}^2 + \frac{{w^j_v}^2}{2m^j} + \frac{1}{2I^j} \tilde{\omega}^2_j + \frac{{w^j_\omega}^2}{2I^j} \\
\leq & -\Lambda^j_1 {e^j_1}^2 - \Lambda^j_2 {e^j_2}^2 - \Lambda^j_3 {e^j_3}^2 - (\Lambda^j_4 - \frac{1}{2m^j}) {e^j_4}^2 - (\Lambda^j_5 - \frac{1}{2I^j}) {e^j_5}^2 - \Omega^j_1 {\tilde{L}^{\pi j}}^2 \\
& - \Omega^j_2 {\tilde{\Psi}^{\pi j}}^2 - \Omega^j_3 {\tilde{\theta}^j}^2 - (\Omega^j_4 - \frac{1}{2m^j}) {\tilde{v}^j}^2 - (\Omega^j_5 - \frac{1}{2I^j}) {\tilde{\omega}^j}^2 + \frac{{w^j_{vb}}^2}{2m^j} + \frac{{w^j_{\omega b}}^2}{2I^j}.
\end{aligned} \tag{B-31}$$

Taking $\rho^j_{b2} = \frac{{w^j_{vb}}^2}{2m^j} + \frac{{w^j_{\omega b}}^2}{2I^j}$, $\dot{V}_j \leq 0$ if the following error bounds are satisfied,

$$|e^j_p| \geq \sqrt{\frac{\rho^j_{b2}}{\Lambda^j_p}} \qquad |e^j_4| \geq \sqrt{\frac{\rho^j_{b2}}{\Lambda^j_4 - \frac{1}{2m^j}}}$$

$$|e^j_5| \geq \sqrt{\frac{\rho^j_{b2}}{\Lambda^j_5 - \frac{1}{2I^j}}} \qquad |\tilde{L}^{\pi j}| \geq \sqrt{\frac{\rho^j_{b2}}{\Omega^j_1}}$$

$$|\tilde{\Psi}^{\pi j}| \geq \sqrt{\frac{\rho_{b2}^{j}}{\Omega_{2}^{j}}} \qquad |\tilde{\theta}^{j}| \geq \sqrt{\frac{\rho_{b2}^{j}}{\Omega_{3}^{j}}}$$
$$|\tilde{v}^{j}| \geq \sqrt{\frac{\rho_{b2}^{j}}{\Omega_{4}^{j} - \frac{1}{2m^{j}}}} \qquad |\tilde{\omega}^{j}| \geq \sqrt{\frac{\rho_{b2}^{j}}{\Omega_{5}^{j} - \frac{1}{2I^{j}}}}, \tag{B-32}$$

where $p = (1, 2, 3)$

Comparing these bounds with the bounds obtained previously (ρ_{b2}^{j}) it can be shown that the bounded actuator attack signal w_j increases the error bound but, the system stays UUB. Alternately,

$$||e^{j}|| \geq \sqrt{\frac{\rho_{b2}^{j}}{\lambda_{min}(\overline{\Lambda}^{j})}} \quad \text{OR} \quad ||\tilde{x}^{j}|| \geq \sqrt{\frac{\rho_{b2}^{j}}{\lambda_{min}(\overline{\Omega}^{j})}}. \tag{B-33}$$

This concludes the proof. □

Proof for Theorem 3. The Lyapunov candidate that shows the stability of the entire formation could be taken as (B-9), The derivative is, $\dot{V}^{ij} = \dot{V}^{i} + \sum_{j=1}^{N} \dot{V}^{j}$. From Lemma 5 and Lemma 6,

$$\begin{aligned}\dot{V}^{ij} \leq & -\lambda_{min}(\overline{\Lambda}^{i})\|e^{i}\|^{2} - \lambda_{min}(\overline{\Omega}^{i})\|\tilde{x}^{i}\|^{2} + \rho_{b2}^{i} \\ & + \sum_{j=1}^{N}\left(-\lambda_{min}(\overline{\Lambda}^{j})\|e^{j}\|^{2} - \lambda_{min}(\overline{\Omega}^{j})\|\tilde{x}^{j}\|^{2} + \rho_{b2}^{j}\right).\end{aligned}$$

Let $\rho_{b2} = \rho_{b2}^{i} + \sum_{j=1}^{N} \rho_{b2}^{j}$, $\overline{\Lambda} = \text{diag}\left(\overline{\Lambda}^{i}, \overline{\Lambda}^{1}, ..., \overline{\Lambda}^{N}\right)$, and $\overline{\Omega} = \text{diag}(\overline{\Omega}^{i}, \overline{\Omega}^{1}, ..., \overline{\Omega}^{N})$. The derivative $\dot{V}^{ij}$ is given by

$$\begin{aligned}\dot{V}^{ij} \leq & -\lambda_{min}(\overline{\Lambda})\|e^{ij}\|^{2} - \lambda_{min}(\overline{\Omega})\|\tilde{x}^{ij}\|^{2} + \rho_{b2} \\ \dot{V}^{ij} \leq & 0,\end{aligned}$$

if and only if the following error bounds are met for the formation tracking error and formation estimation error.

$$\|e^{ij}\| \geq \sqrt{\frac{\rho_{b2}}{\lambda_{min}(\overline{\Lambda})}} \quad \text{OR} \quad \|\tilde{x}^{ij}\| \geq \sqrt{\frac{\rho_{b2}}{\lambda_{min}(\overline{\Omega})}} = \gamma_1. \tag{B-34}$$

Alternately, the residual threshold under attack for each robot in the formation with an OR condition now becomes,

$$\|\tilde{x}^{o}\| \geq \sqrt{\frac{\rho_{b2}}{\lambda_{min}(\overline{\Omega}^{o})}}. \tag{B-35}$$

Therefore, comparing the estimation error bounds in Theorem 2 with the ones just obtained, it is clearly evident that the error bound has increased (i.e. $\gamma_2 > \gamma_1 = 0$). This concludes the proof. □

Proof for Lemma 7. The Lyapunov function is taken as in (B-1) with an additional term for the stability of the NN. Another difference to be noted is that the terms in the Lyapunov are redistributed to help with the proof:

$$V^i = V_{x_p^i} + V_{\tilde{x}_p^i} + V_{NN}^i, \tag{B-36}$$

where $V_{NN}^i = \frac{1}{2}{e_4^i}^2 + \frac{1}{2}{e_5^i}^2 + \frac{1}{2}\tilde{v}^{i2} + \tilde{\omega}^{i2} + \frac{1}{2}\,\mathrm{tr}\{\tilde{W}^{iT}F^{i^{-1}}\tilde{W}^i\}$.

$$\begin{aligned}
\dot{V}_{NN}^i =& -(k_4^i + l_{1mit}^i){e_4^i}^2 - (k_4^i + l_{2mit}^i){e_5^i}^2 - (l_4^i + l_{1mit}^i)\tilde{v}^{i2} - (l_5^i + l_{2mit}^i)\tilde{\omega}^{i2} + k_4^i e_4^i \tilde{v}^i \\
&- e_4^i \tilde{n}_v^i + k_4^i e_5^i \tilde{\omega}^i - e_5^i \tilde{n}_\omega^i - \tilde{v}^i \tilde{n}_v^i - \tilde{\omega}^i \tilde{n}_\omega^i + \frac{1}{m^i} e_4^i \tilde{w}_v^i - \frac{1}{m^i}\varepsilon_v^i e_4^i + \frac{1}{I^i} e_5^i \tilde{w}_\omega^i \\
&- \frac{1}{I^i}\varepsilon_\omega^i e_5^i + \frac{1}{m^i}\tilde{v}^i \tilde{w}_v^i - \frac{1}{m^i}\varepsilon_v^i \tilde{v}^i + \frac{1}{I^i}\tilde{\omega}^i \tilde{w}_\omega^i - \frac{1}{I^i}\varepsilon_\omega^i \tilde{\omega}^i + \mathrm{tr}\{\tilde{W}^{iT}F^{i^{-1}}\dot{\tilde{W}}^i\} \\
=& -(k_4^i + l_{1mit}^i){e_4^i}^2 - (k_4^i + l_{2mit}^i){e_5^i}^2 - (l_4^i + l_{1mit}^i)\tilde{v}^{i2} - (l_5^i + l_{2mit}^i)\tilde{\omega}^{i2} + k_4^i e_4^i \tilde{v}^i \\
&- e_4^i \tilde{n}_v^i + k_4^i e_5^i \tilde{\omega}^i - e_5^i \tilde{n}_\omega^i - \tilde{v}^i \tilde{n}_v^i - \tilde{\omega}^i \tilde{n}_\omega^i - \frac{1}{m^i}\varepsilon_v^i e_4^i - \frac{1}{I^i}\varepsilon_\omega^i e_5^i - \frac{1}{m^i}\varepsilon_v^i \tilde{v}^i
\end{aligned}$$

$$
\begin{aligned}
&- \frac{1}{I^i}\varepsilon^i_\omega\tilde{\omega} + {e^i_c}^T\overline{M}^{i-1}\tilde{W}^{iT}\phi(\overline{x}^i) + \tilde{\overline{V}}^{iT}\overline{M}^{i-1}\tilde{W}^{iT}\phi(\overline{x}^i) + \mathrm{tr}\{\tilde{W}^{iT}F^{i-1}\dot{\hat{W}}^i\} \\
&= -(k^i_4 + l^i_{1mit}){e^i_4}^2 - (k^i_4 + l^i_{2mit}){e^i_5}^2 - (l^i_4 + l^i_{1mit})\tilde{v}^{i2} - (l^i_5 + l^i_{2mit})\tilde{\omega}^{i2} + k^i_4 e^i_4\tilde{v}^i \\
&- e^i_4\tilde{n}^i_v + k^i_4 e^i_5\tilde{\omega}^i - e^i_5\tilde{n}^i_\omega - \tilde{v}^i\tilde{n}^i_v - \tilde{\omega}^i\tilde{n}^i_\omega - \frac{1}{m^i}\varepsilon^i_v e^i_4 - \frac{1}{I^i}\varepsilon^i_\omega e^i_5 - \frac{1}{m^i}\varepsilon^i_v\tilde{v}^i - \frac{1}{I^i}\varepsilon^i_\omega\tilde{\omega} \\
&+ \mathrm{tr}\left\{\tilde{W}^{iT}\phi(\overline{x}^i)\left({e^i_c}^T + \tilde{\overline{V}}^{iT}\right)\overline{M}^{i-1}\right\} + \mathrm{tr}\left\{\tilde{W}^{iT}F^{i-1}\dot{\hat{W}}^i\right\}.
\end{aligned}
$$

Selecting the tuning law in (49),

$$
\begin{aligned}
\dot{V}^i_{NN} = &-(k^i_4 + l^i_{1mit}){e^i_4}^2 - (k^i_4 + l^i_{2mit}){e^i_5}^2 - (l^i_4 + l^i_{1mit})\tilde{v}^{i2} - (l^i_5 + l^i_{2mit})\tilde{\omega}^{i2} + k^i_4 e^i_4\tilde{v}^i \\
&- e^i_4\tilde{n}^i_v + k^i_4 e^i_5\tilde{\omega}^i - e^i_5\tilde{n}^i_\omega - \tilde{v}^i\tilde{n}^i_v - \tilde{\omega}^i\tilde{n}^i_\omega - \frac{1}{m^i}\varepsilon^i_v e^i_4 - \frac{1}{I^i}\varepsilon^i_\omega e^i_5 - \frac{1}{m^i}\varepsilon^i_v\tilde{v}^i - \frac{1}{I^i}\varepsilon^i_\omega\tilde{\omega}^i \\
&- \kappa^i\,\mathrm{tr}\{\tilde{W}^{iT}\hat{W}^i\}.
\end{aligned}
\tag{B-37}
$$

The time derivative of the overall Lyapunov can now be written as,

$$
\begin{aligned}
\dot{V}^i \leq &-\Lambda^i_1{e^i_1}^2 - \Lambda^i_2{e^i_2}^2 - \Lambda^i_3{e^i_3}^2 - (\Lambda^i_4 + l^i_{1mit} - \frac{1}{2m^i}){e^i_4}^2 - (\Lambda^i_5 + l^i_{2mit} - \frac{1}{2I^i}){e^i_5}^2 \\
&- \Omega^i_1\tilde{L}^{\pi j2} - \Omega^i_2\tilde{\Psi}^{\pi j2} - \Omega^i_3\tilde{\theta}^{i2} - (\Omega^i_4 + l^i_{1mit} - \frac{1}{2m^i})\tilde{v}^{i2} - (\Omega^i_5 + l^i_{2mit} - \frac{1}{2I^i})\tilde{\omega}^{i2} \\
&- \kappa^i\left(\|\tilde{W}^i\| - \frac{W^i_M}{2}\right)^2 + \frac{{\varepsilon^i_{vb}}^2}{2m^i} + \frac{{\varepsilon^i_{\omega b}}^2}{2I^i} + \kappa^i\frac{{W^i_M}^2}{4}.
\end{aligned}
\tag{B-38}
$$

Taking $\rho^i_{b3} = \frac{{\varepsilon^i_{vb}}^2}{2m^i} + \frac{{\varepsilon^i_{\omega b}}^2}{2I^i} + \kappa^i\frac{{W^i_M}^2}{4}$, $\dot{V}^i \leq 0$ if the following error bounds are satisfied

$$
|e^i_p| \geq \sqrt{\frac{\rho^i_{b3}}{\Lambda_{ip}}} \qquad |e^i_4| \geq \sqrt{\frac{\rho^i_{b3}}{\Lambda^i_4 + l^i_{1mit} - \frac{1}{2m^i}}}
$$

$$
|e^i_5| \geq \sqrt{\frac{\rho^i_{b3}}{\Lambda^i_5 + l^i_{2mit} - \frac{1}{2I^i}}} \qquad |\tilde{\chi}^i| \geq \sqrt{\frac{\rho^i_{b3}}{\Omega^i_1}}
$$

$$|\tilde{y}^i| \geq \sqrt{\frac{\rho^i_{b3}}{\Omega^i_2}} \qquad |\tilde{\theta}^i| \geq \sqrt{\frac{\rho^i_{b3}}{\Omega^i_3}}$$
$$|\tilde{v}^i| \geq \sqrt{\frac{\rho^i_{b3}}{\Omega^i_4 + l^i_{1mit} - \frac{1}{2m^i}}} \qquad |\tilde{\omega}^i| \geq \sqrt{\frac{\rho^i_{b3}}{\Omega^i_5 + l^i_{2mit} - \frac{1}{2I^i}}},$$

$$\|\tilde{W}^i\| \geq \frac{1}{2}W^i_M + \frac{1}{\kappa^i}\sqrt{\rho^i_{b3}} \tag{B-39}$$

where $p = (1, 2, 3)$. It is apparent that if the gain κ^i is small, and if L^i_{mit} is large enough $(\rho^i_{b1} = 0) < \rho^i_{b3} < \rho^i_{b2}$. Thus the error bounds obtained here are smaller compared to the attacked case. Alternately,

$$||e^i|| \geq \sqrt{\frac{\rho^i_{b3}}{\lambda_{min}(\overline{\Lambda}^i + B^i L^i_{mit})}} \quad \text{OR} \quad ||\tilde{x}^i|| \geq \sqrt{\frac{\rho^i_{b3}}{\lambda_{min}(\overline{\Omega}^i + B^i L^i_{mit})}}. \tag{B-40}$$

Therefore it can be said that the actuator attack in the leader has been mitigated. This concludes the proof. □

Proof for Lemma 8. The Lyapunov function is taken as in (B-6) with an additional term for the stability of the NN. Another difference to be noted is that the terms in the Lyapunov are redistributed to help with the proof:

$$V^j = V_{x^j_p} + V_{\tilde{x}^j_p} + V^j_{NN}, \tag{B-41}$$

where $V^j_{NN} = \frac{1}{2}{e^j_4}^2 + \frac{1}{2}{e^j_5}^2 + \frac{1}{2}\tilde{v}^{j2} + \tilde{\omega}^{j2} + \frac{1}{2}\,\mathrm{tr}\{\tilde{W}^{jT} F^{j-1} \tilde{W}^j\}$.

$$\begin{aligned}\dot{V}^j_{NN} = &-(k^j_4 + l^i_{1mit}){e^j_4}^2 - (k^j_4 + l^j_{2mit}){e^j_5}^2 - (l^j_4 + l^j_{1mit})\tilde{v}^{j2} - (l^j_5 + l^j_{2mit})\tilde{\omega}^{j2} + k^j_4 e^j_4 \tilde{v}^j \\ &- e^j_4 \tilde{n}^j_v + k^j_4 e^j_5 \tilde{\omega}^j - e^j_5 \tilde{n}^j_\omega - \tilde{v}^j \tilde{n}^j_v - \tilde{\omega}^j \tilde{n}^j_\omega + \frac{1}{m^j} e^j_4 \tilde{w}^j_v - \frac{1}{m^j}\varepsilon^j_v e^j_4 + \frac{1}{I^j} e^j_5 \tilde{w}^j_\omega - \frac{1}{I^j}\varepsilon^j_\omega e^j_5 \\ &+ \frac{1}{m^j}\tilde{v}^j \tilde{w}^j_v - \frac{1}{m^j}\varepsilon^j_v \tilde{v}^j + \frac{1}{I^j}\tilde{\omega}^j \tilde{w}^j_\omega - \frac{1}{I^j}\varepsilon^j_\omega \tilde{\omega} + \mathrm{tr}\{\tilde{W}^{jT} F^{j-1} \dot{\tilde{W}}^j\}\end{aligned}$$

$$
\begin{aligned}
&= -(k_4^j + l_{1mit}^j){e_4^j}^2 - (k_4^j + l_{2mit}^j){e_5^j}^2 - (l_4^j + l_{1mit}^j){\tilde{v}^j}^2 - (l_5^j + l_{2mit}^j){\tilde{\omega}^j}^2 + k_4^j e_4^j \tilde{v}^j \\
&\quad - e_4^j \tilde{n}_v^j + k_4^j e_5^j \tilde{\omega}^j - e_5^j \tilde{n}_\omega^j - \tilde{v}^j \tilde{n}_v^j - \tilde{\omega}^j \tilde{n}_\omega^j - \frac{1}{m^j}\varepsilon_v^j e_4^j - \frac{1}{I^j}\varepsilon_\omega^j e_5^j - \frac{1}{m^j}\varepsilon_v^j \tilde{v}^j - \frac{1}{I^j}\varepsilon_\omega^j \tilde{\omega} \\
&\quad + {e_c^j}^T {\overline{M}^j}^{-1} {\tilde{W}^j}^T \phi(\overline{x}^j) + {\tilde{\overline{V}}^j}^T {\overline{M}^j}^{-1} {\tilde{W}^j}^T \phi(\overline{x}^j) + \mathrm{tr}\{{\tilde{W}^j}^T {F^j}^{-1} \dot{\tilde{W}}^j\} \\
&= -(k_4^j + l_{1mit}^j){e_4^j}^2 - (k_4^j + l_{2mit}^j){e_5^j}^2 - (l_4^j + l_{1mit}^j){\tilde{v}^j}^2 - (l_5^j + l_{2mit}^j){\tilde{\omega}^j}^2 + k_4^j e_4^j \tilde{v}^j \\
&\quad - e_4^j \tilde{n}_v^j + k_4^j e_5^j \tilde{\omega}^j - e_5^j \tilde{n}_\omega^j - \tilde{v}^j \tilde{n}_v^j - \tilde{\omega}^j \tilde{n}_\omega^j - \frac{1}{m^j}\varepsilon_v^j e_4^j - \frac{1}{I^j}\varepsilon_\omega^j e_5^j - \frac{1}{m^j}\varepsilon_v^j \tilde{v}^j - \frac{1}{I^j}\varepsilon_\omega^j \tilde{\omega} \\
&\quad + \mathrm{tr}\left\{ {\tilde{W}^j}^T \phi(\overline{x}^j) \left({e_c^j}^T + {\tilde{\overline{V}}^j}^T \right) {\overline{M}^j}^{-1} \right\} + \mathrm{tr}\left\{ {\tilde{W}^j}^T {F^j}^{-1} \dot{\tilde{W}}^j \right\}.
\end{aligned}
$$

Selecting the tuning law in (49),

$$
\begin{aligned}
\dot{V}_{NN}^j = &-(k_4^j + l_{1mit}^j){e_4^j}^2 - (k_4^j + l_{2mit}^j){e_5^j}^2 - (l_4^j + l_{1mit}^j){\tilde{v}^j}^2 - (l_5^j + l_{2mit}^j){\tilde{\omega}^j}^2 \\
&+ k_4^j e_4^j \tilde{v}^j - e_4^j \tilde{n}_v^j + k_4^j e_5^j \tilde{\omega}^j - e_5^j \tilde{n}_\omega^j - \tilde{v}^j \tilde{n}_v^j - \tilde{\omega}^j \tilde{n}_\omega^j - \frac{1}{m^j}\varepsilon_v^j e_4^j - \frac{1}{I^j}\varepsilon_\omega^j e_5^j \\
&- \frac{1}{m^j}\varepsilon_v^j \tilde{v}^j - \frac{1}{I^j}\varepsilon_\omega^j \tilde{\omega} - \kappa^j \|\tilde{W}^j\|_F^2 + \kappa^j \|\tilde{W}^j\|_F W_M^j. \qquad \text{(B-42)}
\end{aligned}
$$

The time derivative of the overall Lyapunov can now be written as

$$
\begin{aligned}
\dot{V}^j \leq &-\Lambda_1^j {e_1^j}^2 - \Lambda_2^j {e_2^j}^2 - \Lambda_3^j {e_3^j}^2 - (\Lambda_4^j + l_{1mit}^j - \frac{1}{2m^j}){e_4^j}^2 - (\Lambda_5^j + l_{2mit}^j - \frac{1}{2I^j}){e_5^j}^2 \\
&- \Omega_1^j {\tilde{L}^{\pi j}}^2 - \Omega_2^j {\tilde{\Psi}^{\pi j}}^2 - \Omega_3^j {\tilde{\theta}^j}^2 - (\Omega_4^j - \frac{1}{2m^j}){\tilde{v}^j}^2 - (\Omega_5^j - \frac{1}{2I^j}){\tilde{\omega}^j}^2 \\
&- \kappa^j \left(\|\tilde{W}^j\| - \frac{W_M^j}{2} \right)^2 + \frac{{\varepsilon_{vb}^j}^2}{2m^j} + \frac{{\varepsilon_{\omega b}^j}^2}{2I^j} + \kappa^j \frac{{W_M^j}^2}{4}. \qquad \text{(B-43)}
\end{aligned}
$$

Taking $\rho_{b3}^j = \frac{{\varepsilon_{vb}^j}^2}{2m^j} + \frac{{\varepsilon_{\omega b}^j}^2}{2I^j} + \kappa^j \frac{{W_M^j}^2}{4}$, $\dot{V}^j \leq 0$ if the error bounds with an OR condition are

$$
|e_p^j| \geq \sqrt{\frac{\rho_{b3}^j}{\Lambda_p^j}} \qquad |e_4^j| \geq \sqrt{\frac{\rho_{b3}^j}{\Lambda_4^j + l_{1mit}^j - \frac{1}{2m^j}}}
$$

$$
|e_5^j| \geq \sqrt{\frac{\rho_{b3}^j}{\Lambda_5^j + l_{2mit}^j - \frac{1}{2I^j}}} \qquad |\tilde{L}^{\pi j}| \geq \sqrt{\frac{\rho_{b3}^j}{\Omega_1^j}}
$$

$$|\tilde{\Psi}^{\pi j}| \geq \sqrt{\frac{\rho^j_{b3}}{\Omega^j_2}} \qquad |\tilde{\theta}^j| \geq \sqrt{\frac{\rho^j_{b3}}{\Omega^j_3}}$$

$$|\tilde{v}^j| \geq \sqrt{\frac{\rho^j_{b3}}{\Omega^j_4 + l^j_{1mit} - \frac{1}{2m^j}}} \qquad |\tilde{\omega}^j| \geq \sqrt{\frac{\rho^j_{b3}}{\Omega^j_5 + l^j_{2mit} - \frac{1}{2I^j}}},$$

$$\|\tilde{W}^j\| \geq \frac{1}{2} W^j_M + \frac{1}{\kappa^j}\sqrt{\rho^j_{b3}} \tag{B-44}$$

where $p = (1,2,3)$ are satisfied. It is apparent that if the gain κ_j is not very large, and if the NN reconstruction errors are negligible, $(\rho_{jb1} = 0) < \rho^j_{b3} < \rho^j_{b2}$. Thus the error bounds obtained here are smaller compared to (B-32) and the actuator attack has been mitigated. This concludes the proof. □

Proof for Theorem 4.

Before proceeding with the proof the augmented vectors are $e^{ij}_p = [{e^i_p}^T {e^1_p}^T \ldots {e^N_p}^T]^T$, $e^{ij}_c = [{e^i_c}^T {e^1_c}^T \ldots {e^N_c}^T]^T$, $\tilde{x}^{ij}_p = [{\tilde{x}^i_p}^T {\tilde{x}^1_p}^T \ldots {\tilde{x}^N_p}^T]^T$ where $\tilde{x}^i_p = [\chi^i, y^i, \theta^i]^T$ and $\tilde{x}^j_p = [L^{\pi j}, \Psi^{\pi j}, \theta^j]^T$, $\tilde{x}^{ij}_c = \tilde{\overline{V}}^{ij} = [{\tilde{\overline{V}}^i}^T {\tilde{\overline{V}}^1}^T \ldots {\tilde{\overline{V}}^N}^T]^T$, $\phi^{ij} = [\phi(\overline{x}^i)^T \phi(\overline{x}^1)^T \ldots \phi(\overline{x}^N)^T]^T$, the augmented matrices $\overline{M}^{ij} = \text{diag}\left(\overline{M}^i, \overline{M}^1, \ldots, \overline{M}^N\right)$, $L_{mit} = \text{diag}\left(L^i_{mit}, L^1_{mit}, \ldots, L^N_{mit}\right)$, $\overline{B} = \text{diag}\left(B^i, B^1, \ldots, B^N\right)$, $F^{ij} = \text{diag}\left(F^i, F^1, \ldots, F^N\right)$, $W^{ij} = \text{diag}\left(W^i, W^1, \ldots, W^N\right)$ and $\hat{W}^{ij} = \text{diag}\left(\hat{W}^i, \hat{W}^1, \ldots, \hat{W}^N\right)$, and scalar gain $\kappa = \min\left(\kappa^i, \kappa^1, \ldots, \kappa^N\right)$. Let $\|W^{ij}\| \leq W^{ij}_M$. The augmented NN tuning law is now given by

$$\dot{\hat{W}}^{ij} = -F^{ij}\phi^{ij}\left(\tilde{\overline{V}}^{ij} + e^{ij}_c\right)^T \overline{M}^{ij\,-1} - \kappa F^{ij}\hat{W}^{ij} \tag{B-45}$$

The Lyapunov function candidate to prove the stability of the formation after applying the attack mitigation scheme is given by

$$V^{ij} = V_{x_p^i} + V_{\tilde{x}_p^i} + \left(\sum_{j=1}^{N} V_{x_p^j} + V_{\tilde{x}_p^j} \right) + V_{NN}^{ij},$$
$$V_{NN}^{ij} = \frac{1}{2} \operatorname{tr} \left\{ \tilde{W}^{ij^T} F^{ij^{-1}} \tilde{W}^{ij} \right\}, \tag{B-46}$$

where the term V_{NN}^{ij} is considered to show the stability of the augmented NN estimation error $\tilde{W}^{ij}$. The derivative of the Lyapunov function can be simplified and obtained as

$$\begin{aligned} \dot{V}^{ij} = & - \Omega_p \|e_p^{ij}\|^2 - (\Omega_c + L_{mit} - \frac{1}{2}\overline{M}^{ij^{-1}}) \|e_c^{ij}\|^2 - \Gamma_p \|\tilde{x}_p^{ij}\|^2 \\ & - (\Gamma_c + L_{mit} - \frac{1}{2}\overline{M}^{ij^{-1}}) \|\tilde{\overline{V}}^{ij}\|^2 - \kappa \left(\|\tilde{W}^{ij}\| - \frac{1}{2} W_M^{ij} \right)^2 \\ & + \frac{1}{2} \|\varepsilon_b\|^2 \|\overline{M}^{ij^{-1}}\| + \frac{1}{4} \kappa W_M^{ij^2}. \end{aligned} \tag{B-47}$$

Taking $\rho_{b3} = \frac{1}{2}\|\varepsilon_b\|^2 \|\overline{M}^{ij^{-1}}\| + \frac{1}{4}\kappa W_M^{ij^2}$, the following error bounds are obtained

$$\|e^{ij}\| \geq \sqrt{\frac{\rho_{b3}}{\lambda_{min}\left(\overline{\Lambda} + \overline{B} L_{mit}\right)}} \quad \text{OR} \quad \|\tilde{x}^{ij}\| \geq \sqrt{\frac{\rho_{b3}}{\lambda_{min}\left(\overline{\Omega} + \overline{B} L_{mit}\right)}} = \gamma_3, \tag{B-48}$$

and the NN weights are also bounded with an OR condition as

$$\|\tilde{W}^{ij}\| \geq \frac{1}{2} W_M^{ij} + \frac{1}{\kappa} \sqrt{\frac{1}{2}\|\varepsilon_b\|^2 \|\overline{M}^{ij^{-1}}\| + \frac{1}{4}\kappa W_M^{ij^2}} \tag{B-49}$$

The matrix L_{mit} can be used to decrease the error bounds. Also, the bound can be reduced by decreasing κ. Thus by proper selection of F^{ij}, κ and L_{mit}, it can be ensured that $\gamma_1 \leq \gamma_3 \leq \gamma_2$. Thus the actuator attack on the formation has been mitigated. This concludes the proof. □

II. COVERT ATTACK DETECTION IN A DYNAMIC MOBILE ROBOT FORMATION

A. Fernandes*, S. Jagannathan*, H. Modares**

* Department of Electrical & Computer Engineering

Missouri University of Science and Technology

Rolla, Missouri 65409

** Department of Mechanical Engineering

Michigan State University

East Lansing, Michigan 48824

ABSTRACT

In this paper, the effects of smart attacks on a nonholonomic robot formation is studied by using dynamic backstepping based tracking controllers for achieving their formation objectives by relaxing the assumption that sensors are attack resilient. It is shown that residual based method is ineffective when a signal is injected in the sensors that modifies the residual in the presence of an actuator attack. Next an auxiliary system consisting of an observer for each robot, which is not known to the adversary, is introduced to detect covert attacks. Simulation results verify theoretical results.

Keywords: Attack detection, attack estimation, Lyapunov stability, formation control, distributed control, security, autonomous systems, nonholonomic system, nonlinear control

1. INTRODUCTION

The need for formation control arises from the necessity of controlling multiple robots to accomplish objectives such as mining, space interferometry [29], patrolling, search and rescue [21], mapping, environmental monitoring [24], and so on. It may be

possible to employ a single robot to accomplish the task at hand, but a single robot will be more bulky and expensive. Also, the single robot will have a higher mission time which will translate to a higher mission cost [6]. Moreover, if the single robot fails the entire mission fails. The single robot cannot make use of distributed data collection schemes to improve system accuracy. It is hard to adapt this single robot for different applications/scenarios. Therefore, a group of cheaper, agile robots is preferred over a single expensive and heavier robot.

Examples of formation controllers in the literature include behavior-based methods [1][2], virtual structure approach, consensus approach [28], neighbor and center reference, and leader-follower strategy [31][9][4]. In behavior-based methods, each robot behaves a certain way in response to its environment. The environment could be obstacles, goal points, or other robots. In virtual structure approach, all robots maintain a formation by positioning themselves at different points of a virtual structure. Consensus requires all robots to exchange individual position information with their neighbors and come to an agreement on the final position, which will be a weighted average of the initial position. In the leader-follower strategy, a few of the robots take on the role of leader while the rest take on the role of follower. The objective of the leaders is to follow a reference trajectory, while the goal of the follower is to maintain a fixed distance from the leader while avoiding obstacles. One of the strategies by which a follower tracks its leader is the separation-bearing-based formation control [9]. The current work just like the previous paper will be focusing on this formation strategy.

The literature on types of attacks on the formation and the necessity of security will be reviewed first before introducing the literature for separation-bearing-based formation control in which a dynamic robot model that captures the nonholonomy and nonlinear properties of a car-like vehicle will be considered. Adversarial inputs can affect sensors, actuators, or the communication links. The actuator/sensor attacks can be fault data injection (FDI) [22], replay [23], and others. The attacks on the communication links include

blackhole, packet loss, time delay, denial of service (DOS) and others. Past literature presents designing a secure controller in the presence of the aforementioned attacks (e.g., [22][23][25][26][19][13]).

Next, the following threats on automated vehicles are reported. In [5], possible attacks and attack surfaces are introduced. In [27], methods by which self-driving and cooperative self-driving vehicles could be affected by cyberattacks is highlighted contrasting the security and privacy measures for self-driving and cooperative self-driving vehicles. In [16], it is shown how one attacked vehicle can effect the efficiency of the entire platoon when employing cooperative adaptive cruise control (CACC). The paper [33] shows how an adversary could manipulate the data being transmitted from an attacked vehicle to its following vehicle and how this could lead to a crash. This effort also discusses possible attack detection and attack mitigation strategies.

In [34], decision trees are used to detect attacks, and the authors in [12] use a dynamic monitor to collect information at different time instants to detect attacks. The effort in [3] uses trajectory planning to guarantee that the robots are resilient to attacks. Before getting into the separation-bearing formation control literature, a brief review on the controller development for an individual robot is presented next.

The papers [18] and [35] are concerned about trajectory-tracking controllers designed for WMR considering the kinematic models and assuming perfect velocity tracking. In [14], a dynamic backstepping-based position and velocity controller was developed by including the robot dynamic model. Torque control was designed, removing the perfect velocity tracking assumption. The authors of [15] took the idea further by considering the robot dynamic model to be unknown. For the purpose of learning the robot dynamics online, an artificial neural network was employed. The paper [7] came up with the separation-bearing and separation-separation-bearing techniques considering the kinematic WMR model.

The separation-bearing technique is employed when every follower robot is localizing itself with respect to its leader robot while the separation-separation-bearing technique is considered when a follower robot is localizing itself with respect to two leader robots. In [9], the dynamic backstepping controller of [14] was extended to the leader-follower case by employing the separation-bearing techniques developed in [7]. This framework was extended to case when the dynamics of the leader and the follower were unknown [10] and state vector of the leader-follower was not measurable [11].

A neural network (NN) based robust integral of the sign of the error (RISE) feedback was developed in [10] for the purpose of learning the unmodeled dynamics while making sure the formation errors go to zero asymptotically. In [11], two NNs are used where one NN is used to estimate the robot's angular and linear velocities while the other NN is used to estimate the unknown robot dynamics online. The paper [8] discusses near-optimal adaptive controllers for the leader-follower formation. Though dynamics of the robots are considered in each robot, the formation is susceptible to attacks.

In paper 1, under the assumption that all the dynamics were known, communication networks and the sensors were resilient to attacks, the attack detection and mitigation scheme was proposed to protect the leader and follower robots from attacks on the actuator and/or the signals sent from the CPU of the robot to the actuators. The latter could occur in the case of a malware onboard the robot CPU [5]. This attack-resilient framework was built for nonlinear, nonholonomic leader-follower formation on top of the system designed in [9].

In this work, the sensor resiliency assumption is relaxed and actuators and sensors of the robot can be compromised at the same time. The special case when all the sensors and actuators have been compromised by the attacker is considered. A smart adversary can attack the actuators while simultaneously modifying the sensor data so as to stay undetected [32]. In this paper, the authors are interested in designing a detection scheme if such a covert attack were to occur. The literature provides various techniques where one could detect a covert attack. One approach could be to add an authentication signal [23] to the

system control torque. This authenticating signal could be a zero mean Gaussian random signal generated using a random seed not known to the adversary. Another method is to extend the system dynamics by a switched auxiliary system [30] and then detect the attack using the residual generated by the switched auxiliary system. Here the switching sequence is assumed to be unknown to the adversary. Yet another approach is moving target defense (MTD) [17]. The MTD introduces statistical time-varying modifications to the system dynamics, thus making it hard for the adversary to have perfect knowledge of the system and to appropriate it. For more information refer to [17].

In Section 2, the residual-based attack detection and mitigation scheme for the nonholonomic robot formation as discussed in paper 1 is briefly discussed. In Section 3 it is shown that in presence of a covert attack the residual-based attack detection scheme can no longer be used for detecting adversarial attacks. In Section 4 the robot dynamics are extended by the use of an auxiliary system. Since the robot mechanics are affected by the actuator attacks an auxiliary system that is similarly affected is designed. This work also assumes that the adversary has no knowledge of the auxiliary system and so will not be able to appropriate it. A covert attack detection scheme is designed based on the residual generated by the auxiliary system. Section 5 provides simulation to verify the claims made in this work and discusses the results. Section 6 gives the conclusion and a brief of the work to be carried out in the future.

2. PROBLEM FORMULATION

The dynamics of the formation control and the assumptions made in the previous paper hold. In addition, the following assumptions are needed in order to proceed.

Assumption 1. *The communication links of the robots do not experience attacks. Attacks only take place on the robot actuators, control signals received by the actuator, and sensors, or on the measurement signals transmitted by the sensors.*

Assumption 2. *The covert attack happens after the formation is converged.*

The observer-based attack detection and mitigation scheme implemented in the previous paper will be discussed to provide a continuity. The reader is advised to refer to the previous paper to gain an insight into the robot dynamics and the trajectory-tracking-based backstepping control scheme. With some abuse of notation the robot dynamics can be written in a compact form as

$$\begin{aligned} \dot{x}^i &= f^i(x^i) + B^i \hat{\tau}^i, \\ \dot{x}^j &= f^j(y^j, y^\pi) + B^j \hat{\tau}^j, \\ y^k &= x^k, \end{aligned} \tag{1}$$

where x^k is the state vector of a robot, with $k = i$ when the robot is a leader and $k = j$ when the robot is a follower. The vector $x^i = \begin{bmatrix} \chi^i & y^i & \theta^i & v^i & \omega^i \end{bmatrix}^T$, where χ^i is the position of the leader robot in the X global coordinate, y^i is the position of the leader robot in the Y global coordinate, θ^i is the orientation of the leader robot with respect to the X axis, v^i is the linear velocity of the leader robot, and ω^i is the angular velocity of the leader robot. The vector $x^j = \begin{bmatrix} L^{\pi j} & \Psi^{\pi j} & \theta^j & v^j & w^j \end{bmatrix}^T$, where $L^{\pi j}$ is the separation between the jth robot and its assigned leader π, $\Psi^{\pi j}$ is the bearing of the jth robot from its assigned leader π, and θ^j, v^j and ω^j are defined for the follower as θ^i, v^i, and ω^i was defined for the leader. The vector $\overline{V}^k = \begin{bmatrix} v^k & \omega^k \end{bmatrix}^T$ is the robot velocity vector and $\overline{V}^k$ is the acceleration vector.

The robot output vector is given by y^k, control matrix is given by $B^k = \begin{bmatrix} \mathbf{0} \\ \overline{M}^{-1k} \end{bmatrix}$, and $\hat{\tau}^k$ is the torque designed by using the observer state vector and tasked with the objective of making a robot track its assigned leader π (the virtual cart in case of the leader). The functions $f^i(x^i)$ and $f^j(y^j, y^\pi)$ capture the kinematics and dynamics of the leader and follower robot, respectively. Note that in the previous paper f^j was a function of the robot

state vector x^j and the assigned leader state vector x^π (i.e. $f^j(x^j, x^\pi)$). As the separation-bearing dynamics depends highly on the sensor information and since in this paper the effect of attack on the sensors is investigated, function has been rewritten as $f^j(y^j, y^\pi)$.

The observer dynamics are given by

$$\begin{aligned}\dot{\hat{x}}^i &= f^i(\hat{x}^i) + B^i\hat{\tau}^i - L^i\tilde{y}^i,\\ \dot{\hat{x}}^j &= f^j(\hat{y}^j, y^\pi) + B^j\hat{\tau}^j - L^j\tilde{y}^j,\\ \hat{y}^k &= \hat{x}^k,\end{aligned} \tag{2}$$

where $\hat{x}^k$ is the estimate of the state vector x^k, $\hat{y}^k$ is the estimated output vector, $L^k = \text{diag}\{l_1^k, l_2^k, l_3^k, l_4^k, l_5^k\} > 0$, is a user defined gain matrix, and

$$\tilde{y}^k = \hat{y}^k - y^k, \tag{3}$$

is the residual. In the previous paper, the residual was defined as $\tilde{x}^k$ as the state vector of the robot was measured perfectly. Here it is assumed that the state vector measurement can be corrupted by attacks and so for the purpose of analysis the residual is taken as $\tilde{y}^k$. $\tilde{x}$ will be referred to as the state estimation error to avoid confusion. In the presence of an actuator attack, the robot dynamics change to

$$\begin{aligned}\dot{x}^i &= f^i(x^i) + B^i\hat{\tau}^i + B^i w^i,\\ \dot{x}^j &= f^j(y^j, y^\pi) + B^j\hat{\tau}^j + B^j w^j,\\ y^k &= x^k,\end{aligned} \tag{4}$$

where w^k is assumed to be a smooth and bounded attack signal (i.e., $\|w^k\| \leq w_b^k$).

The estimation error dynamics are given by

$$\dot{\tilde{x}}^k = \dot{\hat{x}}^k - \dot{x}^k, \tag{5}$$

which can be further simplified for the leader and follower robot as

$$\begin{aligned}\dot{\tilde{x}}^i &= \tilde{f}^i(\tilde{x}^i) - L^i\tilde{y}^i - B^i w^i,\\ \dot{\tilde{x}}^j &= \tilde{f}^j(\tilde{y}^j, y^\pi) - L^j\tilde{y}^j - B^j w^j.\end{aligned} \tag{6}$$

Here $\tilde{f}^i(\tilde{x}^i) = f^i(\hat{x}^i) - f^i(x^i)$, and $\tilde{f}^j(\tilde{y}^j, y^\pi) = f^i(\hat{y}^j, y^\pi) - f^i(y^j, y^\pi)$. Since there is no sensor attack $\tilde{x}^k = \tilde{y}^k$. Therefore, equation (6) can also be given by

$$\begin{aligned}\dot{\tilde{y}}^i &= \tilde{f}^i(\tilde{y}^i) - L^i\tilde{y}^i - B^i w^i,\\ \dot{\tilde{y}}^j &= \tilde{f}^j(\tilde{y}^j, y^\pi) - L^j\tilde{y}^j - B^j w^j.\end{aligned} \tag{7}$$

In the previous paper it was proven that in the absence of an actuator attack the robot's residual and the trajectory-tracking errors converged to zero asymptotically. When there was an attack on the actuators it was noticed that the trajectory-tracking errors and residual though uniformly ultimately bounded (UUB) increased under the assumtion that the attack was not intended to put the formation out of commission. This fact was used to detect an attack by comparing the residual against a threshold. Upon detection, a mitigation scheme was designed so as to use the residual and tracking error estimate to tune an NN. The NN learned the actuator attack signal online and compensate it effectively. Due to the NN reconstruction error, the residual was proven to be UUB. By selecting proper gains, the trajectory-tracking error bounds and the residual bounds after the mitigation were proven to be smaller than the case of an attack but higher than the healthy case.

The following section describes covert attacks and invalidates the attack detection and mitigation scheme designed in Paper I for detecting such attacks. The robot dynamics under the effect of a generic actuator and sensor attack are given by

$$\begin{aligned}\dot{x}^i &= f^i(x^i) + B^i\hat{\tau}^i + B^i w^i,\\ \dot{x}^j &= f^j(y^j, y^\pi) + B^j\hat{\tau}^j + B^j w^j,\\ y^k &= x^k + v_a^k,\end{aligned} \tag{8}$$

where w^k is assumed to be a bounded actuator attack signal. i.e.$\|w^k\| \leq w_b^k$ and v^k is a sensor attack signal designed by a smart attacker which is also assumed to be bounded $\|v^k\| \leq v_b^k$. The observer dynamics stay the same as it is not directly affected by the attack. On the other hand, the residual changes as

$$\tilde{y}^k = \hat{y}^k - y^k = \tilde{x}^k - v_a^k, \tag{9}$$

and the residual dynamics are now given as

$$\begin{aligned} \dot{\tilde{y}}^i &= \tilde{f}^i(\tilde{x}^i) - L^i(\tilde{y}^i) - B^i w^i - \dot{v}_a^i \\ \dot{\tilde{y}}^j &= \tilde{f}^j(\tilde{y}^j, y^\pi) - L^j \tilde{y}^j - B^j w^j - \dot{v}_a^j. \end{aligned} \tag{10}$$

If the adversary injects attacks at random in the actuators and sensors, it can be shown from the previous paper and by using equation (10) that the attacks can still be detected. But since the sensor data is not reliable, the mitigation discussed in the previous paper is not applicable. In this paper, a mitigation scheme for sensor and actuator attacks that were injected at random on the robot formation is not discussed. Instead the focus will be towards designing a covert attack detector.

3. COVERT ATTACK

In this section, a covert attack from the perspective of the adversary is designed. Here the attack will be designed such that even though the robot is not following its assigned leader, the residual will stay small thus avoiding being detected. The following assumption is made with respect to the adversary.

Assumption 3. *The adversary knows the robot system dynamics and the robot control torque. Additionally, the adversary can modify all the sensor measurements, and inject actuator attacks.*

Since the adversary knows the system dynamics, the adversary could construct false data in a smart way and inject it in the sensors. One possible way is to construct a virtual dynamical system [21] and replace the robot sensor readings with the output of this virtual system. The virtual system could have the a model of the robot dynamics

$$\begin{aligned} \dot{x}^i_{virt} &= f^i(x^i_{virt}) + B^i \hat{\tau}^i, \\ \dot{x}^j_{virt} &= f^j(y^j_{virt}, y^\pi) + B^j \hat{\tau}^j, \\ y^k_{virt} &= x^k_{virt}, \end{aligned} \tag{11}$$

where x^k_{virt} is the state of the virtual system and y^k_{virt} is the output of the virtual system. Based on (11), the sensor attack can be designed as

$$v^k_a = x^k_{virt} - x^k. \tag{12}$$

When this attack is injected at the output of the kth robot, it changes the robot output to reflect the output of the virtual system as

$$y^k = x^k_{virt}. \tag{13}$$

The residual of the robot is affected as well. In the presence of smart sensor attack, the residual for the robot now becomes the residual of the virtual dynamical system with respect to the observer (denoted by $\tilde{y}^k_{virt}$). i.e.

$$\tilde{y}^k = \tilde{y}^k_{virt}. \tag{14}$$

It has been shown in Paper I Theorem 2 that the residual of the robot in the attack-free scenario approaches zero asymptotically. Since the virtual system itself doesn't have an attack, by Theorem 2 the residual generated by the attack appropriated observer will become

zero and so it is not possible to detect the attack. The robot thus is unaware that it is under any attack. As discussed in Section 1, a covert attack can be detected by adding an auxiliary system to every robot in the formation thus extending the robot dynamics.

4. COVERT ATTACK DETECTION

Before proceeding, a couple of supporting assumptions are stated.

Assumption 4. *The auxiliary system dynamics do not affect the robot dynamics.*

Assumption 5. *The auxiliary system dynamics and measurements are unknown to the adversary.*

4.1. AUXILIARY SYSTEM DESIGN

Since the attacks are aimed at misguiding the robot from its tracking objective, the attack will introduce unwanted accelerations to the robot and possibly to the formation. If the auxiliary system can capture these accelerations, it may be possible to detect an attack. Each wheeled mobile robot (WMR) has a linear acceleration $\dot{v}$ and an angular acceleration $\dot{\omega}$ (Note that the robot indices will not be mentioned throughout this section as the auxiliary system design is exactly the same for the leader and the follower). A linear spring-mass-damper (LSMD) can be placed on the robot chassis such that it oscillates in the direction of the robots linear motion. This will ensure that whenever the robot accelerates linearly, the LSMD's oscillations are effected. Additionally, a torsional spring-mass-damper (TSMD) can be placed on the robot's axis of rotation. This TSMD's oscillations will be affected by the angular accelerations on the system in the same manner. Together, the LSMD and the TSMD capture the effect of accelerations on the robot dynamics and can therefore be used as an auxiliary system of the robot.

The auxiliary system dynamics are now given by

$$\begin{bmatrix} M_{LSMD} & 0 \\ 0 & J_{TSMD} \end{bmatrix} \ddot{z}_{Aux} = - \begin{bmatrix} b_{LSMD} & 0 \\ 0 & b_{TSMD} \end{bmatrix} \dot{z}_{Aux} - \begin{bmatrix} k_{LSMD} & 0 \\ 0 & k_{TSMD} \end{bmatrix} z_{Aux} + \begin{bmatrix} M_{LSMD} & 0 \\ 0 & J_{TSMD} \end{bmatrix} \dot{\overline{V}}, \tag{15}$$

where M_{LSMD} is the mass, b_{LSMD} is the damping coefficient and k_{LSMD} is the spring constant of the LSMD, J_{TSMD} is the moment of inertia about the axis of rotation, b_{TSMD} is the damping coefficient and k_{TSMD} is the spring constant of the TSMD. The vector $z_{Aux} = [z_{LSMD}\, z_{TSMD}]^T$, where z_{LSMD} is the position of the LSMD with respect to a fixed support and z_{TSMD} is the orientation of the TSMD with respect to an initial orientation. The robot acceleration vector $\dot{\overline{V}}$ was defined earlier in equation (1). Equation (15) can be further simplified as

$$M_{Aux}\ddot{z} = -B_{Aux}\dot{z} - K_{Aux}z + M_{Aux}\overline{M}^{-1}\left(-\overline{F}(\overline{V}) + \hat{\tau} + w\right), \tag{16}$$

with $M_{Aux} = \begin{bmatrix} M_{LSMD} & 0 \\ 0 & J_{TSMD} \end{bmatrix}$, $B_{Aux} = \begin{bmatrix} b_{LSMD} & 0 \\ 0 & b_{TSMD} \end{bmatrix}$, $K_{Aux} = \begin{bmatrix} k_{LSMD} & 0 \\ 0 & k_{TSMD} \end{bmatrix}$. Taking $z_{Aux} = z_{1Aux}$ and $\ddot{z}_{Aux} = \dot{z}_{1Aux} = z_{2Aux}$, equation (16) gives the state-space model in the Brunovsky canonical form

$$\begin{aligned} \dot{z}_{1Aux} &= z_{2Aux} \\ \dot{z}_{2Aux} &= -M_{Aux}^{-1}B_{Aux}z_{2Aux} - M_{Aux}^{-1}K_{Aux}z_1 + \overline{M}^{-1}\left(-\overline{F}(\overline{V}) + \hat{\tau} + w\right). \end{aligned} \tag{17}$$

Equation (17) is finally written in a compact form as

$$\begin{aligned} \dot{Z}_{Aux} &= H_{Aux} Z_{Aux} + G_{Aux} \overline{M}^{-1} (-\overline{F}(\overline{V}) + \hat{\overline{\tau}} + w), \\ Y_{Aux} &= Z_{Aux}, \end{aligned} \tag{18}$$

where $Z_{Aux} = [z_{1Aux}\, z_{2Aux}]^T$, is the state vector of the auxiliary system, Y_{Aux} is the output vector of the auxiliary system, $H_{Aux} = \begin{bmatrix} 0 & I \\ -M_{Aux}^{-1} K_{Aux} & -M_{Aux}^{-1} B_{Aux} \end{bmatrix}$, is the state transition matrix of the auxiliary system and $G_{Aux} = \begin{bmatrix} \mathbf{0}_{2\times 2} \\ I_{2\times 2} \end{bmatrix}$, is the input matrix of the auxiliary system with respect to the acceleration of the robot. Equations (16)-(18) all show the effect of the robot dynamics on the auxiliary system dynamics which also includes the affect of the attack signal. If an observer is built for the auxiliary system then it could be possible to detect the attack using the residual formed by comparing the output vector of the observer and the output vector of the auxiliary system.

4.2. AUXILIARY SYSTEM TRACKING CONTROLLER DESIGN

The Auxiliary System is given a tracking objective just like the robot it is on. The auxiliary system could also have a regulation objective but this will not be considered here. The auxiliary system will be made to track an ideal oscillating spring-mass reference system without any damping. The dynamics of the reference system are given by

$$\begin{aligned} \dot{Z}_{Aux}^{r} &= H_{Aux}^{r} Z_{Aux}^{r}, \\ Y_{Aux}^{r} &= Z_{Aux}^{r}, \end{aligned} \tag{19}$$

with $Z^r_{Aux} = \left[z^r_{1Aux}\, z^r_{2Aux}\right]^T$ being the state vector of the reference system, $H^r_{Aux} = \begin{bmatrix} 0 & I \\ -{M^r_{Aux}}^{-1} K^r_{Aux} & 0 \end{bmatrix}$, is the state transition matrix with M^r_{Aux} and K^r_{Aux} defined just like the auxiliary system. The auxiliary system with the tracking controller is given by

$$\begin{aligned} \dot{Z}_{Aux} =& H_{Aux} Z_{Aux} + G_{Aux} \overline{M}^{-1} (-\overline{F}(\overline{V}) + \hat{\overline{\tau}} + w) + G_{Aux} U_{Aux}, \\ Y_{Aux} =& Z_{Aux}, \end{aligned} \tag{20}$$

where the tracking control U_{Aux} is given by

$$U_{Aux} = M^{-1}_{Aux} K_{Aux} z_{1Aux} + M^{-1}_{Aux} B_{Aux} z_{2Aux} + \dot{z}^r_{2Aux} + \Lambda_{Aux} \dot{e}_{Aux} + K_{vAux} r_{Aux}. \tag{21}$$

Here

$$e_{Aux} = z^r_{1Aux} - z_{1Aux}, \tag{22}$$

where e_{Aux} is the position tracking error between the reference system and the auxiliary system

$$\dot{e}_{Aux} = z^r_{2Aux} - z_{2Aux}, \tag{23}$$

where $\dot{e}_{Aux}$ is the velocity tracking error between the reference system and the auxiliary system, and

$$r_{Aux} = \dot{e}_{Aux} + \Lambda_{Aux} e_{Aux}, \tag{24}$$

where r_{Aux} is the filtered tracking error [20], Λ_{Aux} and K_{vAux} are user-defined positive-definite gains. From equations (19)-(24), the derivative of $\dot{r}_{Aux}$ can be given by

$$\dot{r}_{Aux} = -K_{vAux} r_{Aux} - \overline{M}^{-1} \left(-\overline{F}(\overline{V}) + \hat{\overline{\tau}} + w\right). \tag{25}$$

It can be proven that in the absence of attacks on the robot, the auxiliary system tracks its reference robot. However, in the presence of an actuator attack on the robot, the auxiliary system is not able to faithfully accomplish its tracking objective. The auxiliary system tracking-control stability along with the auxiliary system estimation stability will be shown in Theorem 1 in the next subsection.

4.3. AUXILIARY SYSTEM OBSERVER DESIGN

The observer designed for the auxiliary system estimates the state vector of the auxiliary system in the absence of an attack on the robot i.e. the residual of the auxiliary system will converge to zero asymptotically. But in the event of an attack on the robot, the residual of the auxiliary system will be non-zero. Next, an observer will be designed and it is shown that in the attack-free case the auxiliary system residual converges to zero. It will also be shown in the coming theorem that this threshold can be used for detecting a covert attack. The observer dynamics for the auxiliary system are given by

$$\begin{aligned}\dot{\hat{Z}}_{Aux} =& H_{Aux}\hat{Z}_{Aux} + G_{Aux}\overline{M}^{-1}(-\overline{F}(\hat{\overline{V}}) + \hat{\overline{\tau}}) + G_{Aux}U_{Aux} - \overline{L}_{Aux}\tilde{Z}_{Aux},\\ \hat{Y}_{Aux} =& \hat{Z}_{Aux},\end{aligned} \tag{26}$$

where $\tilde{Z}_{Aux} = \hat{Z}_{Aux} - Z_{Aux}$, $\overline{L}_{Aux}$ is the user designed positive-definite gain matrix. The estimate of the friction vector is $\overline{F}(\hat{\overline{V}})$ (see Paper I). The $\tilde{Z}_{Aux}$ dynamics are

$$\dot{\tilde{Z}}_{Aux} = (H_{Aux} - \overline{L}_{Aux})\tilde{Z}_{Aux} + G_{Aux}\overline{M}^{-1}\left(-\left(\overline{F}(\hat{\overline{V}}) - \overline{F}(\overline{V})\right) - w\right). \tag{27}$$

By substituting $\overline{M}^{-1}(\overline{F}(\hat{\overline{V}}) - \overline{F}(\overline{V})) = \tilde{N}(\tilde{\overline{V}})$, (from Paper I) and $H_{Aux} - \overline{L}_{Aux} = \mathcal{H}_{Aux}$, equation (27) can be written as

$$\dot{\tilde{Z}}_{Aux} = \mathcal{H}_{Aux}\tilde{Z}_{Aux} + G_{Aux}\left(-\tilde{N}(\tilde{\overline{V}}) - \overline{M}^{-1}w\right). \tag{28}$$

Remark 1. *The term $\tilde{N}(\tilde{\overline{V}})$ converges to zero in the attack-free scenario by Paper I Theorem 2.*

By suitably choosing the gain $\overline{L}_A ux$ it can be shown that in the absence of any attack the auxiliary residual converges to zero. This is not the case in the presence of an attack.

Remark 2. *Since the attack takes place after the robot formation has achieved its desired configuration (Assumption 2), when the desired formation is achieved, $\dot{\overline{V}} = -\overline{F}(\overline{V}) + \hat{\overline{\tau}} = 0$.*

Theorem 1. *The auxiliary system designed as per (20) placed onboard the nonholonomic mobile robot with dynamics given by (1), tracking a reference system (19) by using the control law in (21), can be used to detect a covert attack taking place on the robot by designing an observer for the auxiliary system and monitoring any deviations in the auxiliary system residual.*

Proof. Let the Lyapunov candidate function for finding out the detection threshold be given by

$$V_{aux} = \tilde{Z}_{Aux}^T P_{Aux} \tilde{Z}_{Aux} + \frac{1}{2} r_{Aux}^T r_{Aux}, \tag{29}$$

where P is a positive definite symmetric matrix. It can be seen that this function is monotonically increasing and is zero only at $Z_{Aux} = 0$ and $r_{Aux} = 0$. For finding the detection threshold it can be assumed that the system is attack-free. Therefore equations (25) and (28) simplify to obtain

$$\dot{r}_{Aux} = -K_{vAux} r_{Aux}, \tag{30}$$

and

$$\dot{\tilde{Z}}_{Aux} = \mathcal{H}_{Aux} \tilde{Z}_{Aux}, \tag{31}$$

respectively (see Remarks 1 and 2). The derivative of equation (29) is given by

$$\dot{V}_{Aux} = \tilde{Z}_{Aux}^T \left(\mathcal{H}_{Aux}^T P_{Aux} + P_{Aux} \mathcal{H} \right) \tilde{Z}_{Aux} - r_{Aux}^T K_{vAux} r_{Aux}. \tag{32}$$

Taking $Q_{Aux} > 0$ such that

$$\mathcal{H}_{Aux}^T P_{Aux} + P_{Aux}\mathcal{H} = -Q_{Aux}, \tag{33}$$

the equation (32) can be simplified as

$$\dot{V}_{Aux} = -\tilde{Z}_{Aux}^T Q_{Aux} \tilde{Z}_{Aux} - r_{Aux}^T K_{vAux} r_{Aux}. \tag{34}$$

From equation (34) it can be seen that the time derivative of the Lyapunov candidate in (29) is negative definite. Therefore the auxiliary system filter tracking error converges to zero, implying that the auxiliary system tracks the auxiliary reference system. Additionally the auxiliary system residual converges to zero. Conversely, in the presence of attack the derivative of the Lyapunov candidate after substituting the dynamics from equation (25), (28) and using the result (33) is given by

$$\begin{aligned}
\dot{V}_{Aux} =& -\tilde{Z}_{Aux}^T Q_{Aux} \tilde{Z}_{Aux} + \left(-\tilde{N}(\tilde{\overline{V}}) - \overline{M}^{-1} w\right)^T G_{Aux}^T P_{Aux} \tilde{Z}_{Aux} \\
&+ G_{Aux}\left(-\tilde{N}(\tilde{\overline{V}}) - \overline{M}^{-1} w\right) - r_{Aux}^T K_{vAux} r_{Aux} - r_{Aux}^T \overline{M}^{-1}\left(-\overline{F}(\overline{V}) + \hat{\overline{\tau}} + w\right) \\
\leq& -\lambda_{min}\left(Q_{Aux}\right)\left\|\tilde{Z}_{Aux}\right\|^2 + 2\left(\mu_{max}\left\|\tilde{\overline{V}}\right\| + 2\mu_3 + w_b\right)\left\|G\overline{M}^{-1}\right\| \lambda_{max}\left(P_{Aux}\right)\left\|Z_{Aux}\right\| \\
&- K_{vAux}\left\|r\right\|^2 + \frac{\tau_b + w_b}{M_b}\left\|r\right\|.
\end{aligned} \tag{35}$$

In the case of the covert attack, the Remark 2 no longer holds. Instead the robot dynamics now have a new equilibrium given by $\dot{\overline{V}} = -\overline{F}(\overline{V}) + \hat{\overline{\tau}} + w = 0$. Since the robot is unaware of the attack, the torque before the attack and after the attack stays the same and is therefore bounded. The friction term $\overline{F}(\overline{V})$ can be expected to vary slightly. But the overall term $-\overline{F}(\overline{V}) + \hat{\overline{\tau}}$ is assumed to be bounded by $\tau_b > 0$. In the presence of an actuator attack the robot estimation and tracking error are bounded (Paper I Theorem 3). The velocity tracking error is bounded by $\sqrt{\frac{\rho_{b2}}{\lambda_{min}(\Omega_4,\Omega_5) - \frac{1}{M_b}}} = \tilde{\overline{V}}_b$. After substituting the bounds (See Appendix)

and completing the squares

$$\begin{aligned}\dot{V}_{Aux} \leq & -\lambda_{min}\left(Q_{Aux}\right)\left(\left\|\tilde{Z}_{Aux}\right\| - \frac{\lambda_{max}(P_{Aux})\left(\mu_{max}\bar{\tilde{V}}_b + 2\mu_3 + w_b\right)}{\lambda_{min}(Q_{Aux})M_b}\right)^2 \\ & - \lambda_{min}\left(K_{vAux}\right)\left(\|r\| - \frac{\tau_b + w_b}{2\lambda_{min}\left(K_{vAux}\right)M_b}\right)^2 \\ & + \frac{\lambda^2_{max}(P_{Aux})\left(\mu_{max}\bar{\tilde{V}}_b + 2\mu_3 + w_b\right)^2}{\lambda_{min}(Q_{Aux})M_b^2} + \frac{(\tau_b + w_b)^2}{4\lambda_{min}\left(K_{vAux}\right)M_b^2} \end{aligned} \tag{36}$$

$$\therefore \dot{V}_{Aux} \leq 0 \implies \|r\| \geq \sqrt{\frac{\lambda^2_{max}(P_{Aux})\left(\mu_{max}\bar{\tilde{V}}_b + 2\mu_3 + w_b\right)^2}{\lambda_{min}(Q_{Aux})\lambda_{min}\left(K_{vAux}\right)M_b^2} + \frac{(\tau_b + w_b)^2}{4\lambda^2_{min}\left(K_{vAux}\right)M_b^2}} + \frac{\tau_b + w_b}{2\lambda_{min}\left(K_{vAux}\right)M_b}$$

OR

$$\begin{aligned}\|z\| \geq & \quad \frac{\lambda_{max}(P_{Aux})\left(\mu_{max}\bar{\tilde{V}}_b + 2\mu_3 + w_b\right)}{\lambda_{min}(Q_{Aux})M_b} \\ & + \sqrt{\frac{\lambda^2_{max}(P_{Aux})\left(\mu_{max}\bar{\tilde{V}}_b + 2\mu_3 + w_b\right)^2}{\lambda^2_{min}(Q_{Aux})M_b^2} + \frac{(\tau_b + w_b)^2}{4\lambda_{min}\left(K_{vAux}\right)\lambda_{min}(Q_{Aux})M_b^2}}. \end{aligned} \tag{37}$$

Hence it can be seen that in the presence of attack the auxiliary system residual and auxiliary system tracking error are bounded but converge to zero in the case of a covert attack. This fact can be used to detect the covert attack. This concludes the proof. □

5. RESULTS AND DISCUSSION

For the purpose of simulation, the right-wing formation considered in Paper I, consisting of a leader robot i and two follower robots $j = \{1, 2\}$ is taken as per Figure 1. The robots parameters just like in Paper I are chosen as [9] with mass of the robot $m = 5\,kg$, moment of inertia of the robot $I = 3\,kg\,m^2$, perpendicular distance of the wheels from the center of mass $R = 0.175m$, robot wheel radius $r = 0.08m$, distance from the robot's center of mass to the robot's rear axle $d = 0.4m$, linear coefficient of static friction $\mu_1 = 0.2$, linear coefficient of dynamic friction $\mu_2 = 0.2$, angular coefficient of static friction $\mu_3 = 0.2$, angular coefficient of dynamic friction $\mu_4 = 0.2$, the transformed robot mass matrix $\overline{M} = \begin{bmatrix} m & 0 \\ 0 & I \end{bmatrix}$, the friction matrix $\overline{F} = \begin{bmatrix} \mu_1 \operatorname{sign} v + \mu_2 v \\ \mu_3 \operatorname{sign} \omega + \mu_4 \omega \end{bmatrix}$. The control gains are selected as $k_1 = 3$, $k_2 = 2$, $k_3 = 2$ and $k_4 = 2$. The observer gains are selected as $l_1 = 1$, $l_2 = 1$, $l_3 = 1$, $l_4 = 3$ and $l_5 = 3$. Note that the subscripts have been removed wherever the values for the leader and follower robots are identical. The reference cart linear velocity is given by $v^r = 0.8$ and the angular velocity is given by $\omega^r = \begin{cases} 0.15 & 10 \le t \le 25 \\ -0.15 & 40 \le t \le 55 \\ 0 & \text{otherwise} \end{cases}$.

The mass, damping coefficient, and the spring constant of the LSMD is $m_{LSMD} = 0.2kg$, $b_{LSMD} = 0.01kg$, and $k_{LSMD} = 0.2$, respectively. The moment of inertia, damping coefficient, and the torsional spring constant of the TSMD is $J_{TSMD} = 0.2kg\,m^2$, $b_{TSMD} = 0.01$, and $k_{TSMD} = 0.2$, respectively. The reference auxiliary system has the same mass, inertia, spring constant and torsional spring constant as the auxiliary system but it has a zero damping coefficient. The actuator attacks performed by the attacker on the robot formation are given by $w^i = \begin{bmatrix} 0.5 \\ 0.5 \end{bmatrix}$ $90s \le t \le 92s$, and $w^1 = \begin{bmatrix} 0.5 \\ -0.5 \end{bmatrix}$ $80s \le t \le 82s$. The sensor attack on the robot takes place on the leader i from $t > 90s$, while the sensor attack on the follower 1 takes place from $t > 80s$

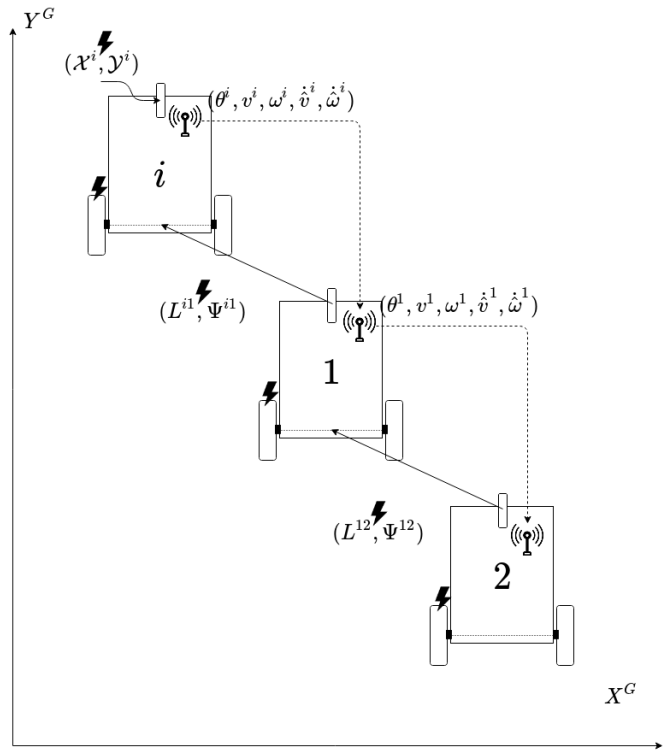

Figure 1. Leader-follower formation under covert attack.

5.1. ATTACK-FREE SCENARIO

Figures 2, 3, and 4 are the figures of the same attack-free case as presented in Paper I with Figures 5 and 6 additionally showing the auxiliary system tracking errors and the auxiliary system residual, respectively. Figure 5 shows the response of the auxiliary system when the robot it is on accelerates or decelerates. The spikes show how the accelerations hinder the tracking objective of the auxiliary system. Since the auxiliary system observer also has a similar response to accelerations, the auxiliary residual is unaffected and stays at zero once it converges.

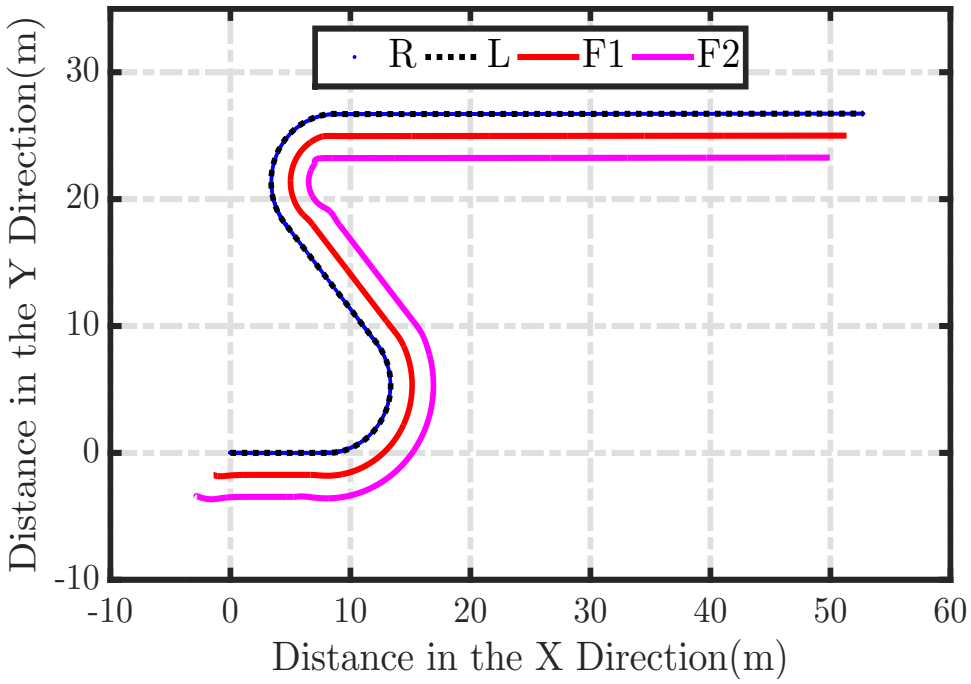

Figure 2. Attack-free formation trajectories.

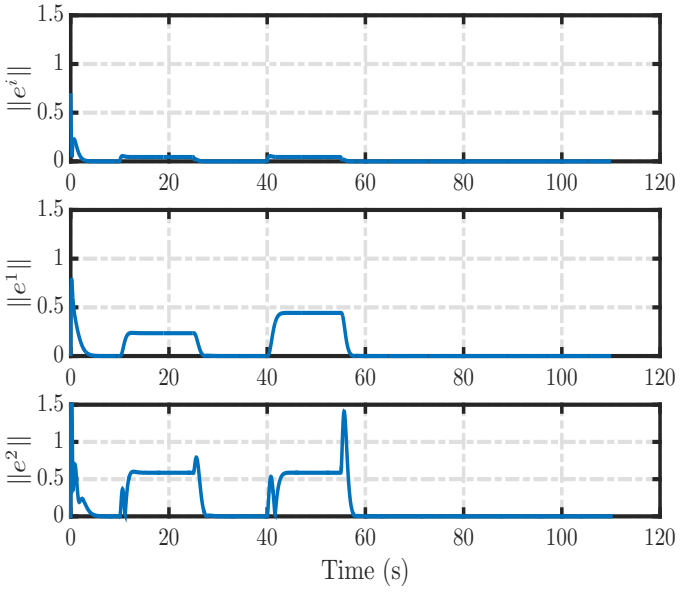

Figure 3. Attack-free tracking errors.

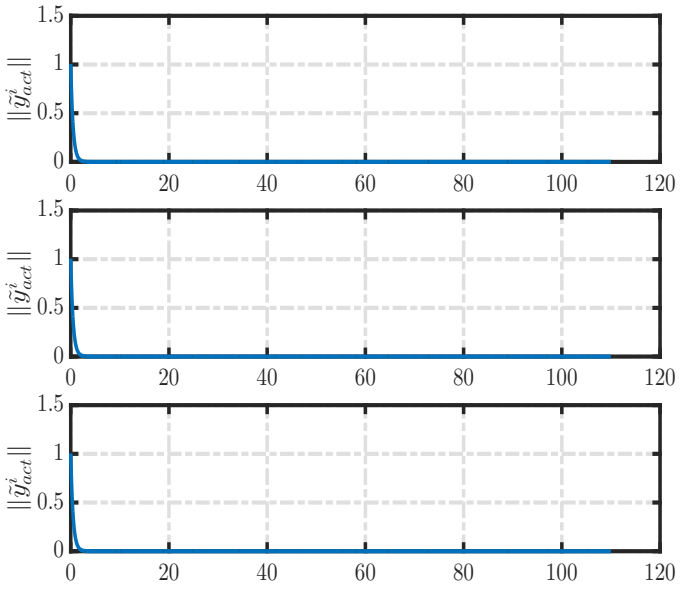

Figure 4. Attack-free estimation errors.

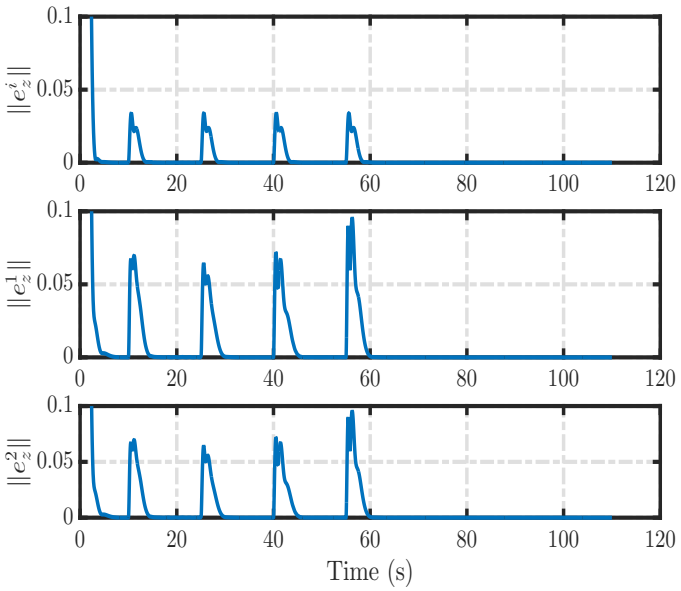

Figure 5. Attack-free auxiliary system tracking errors.

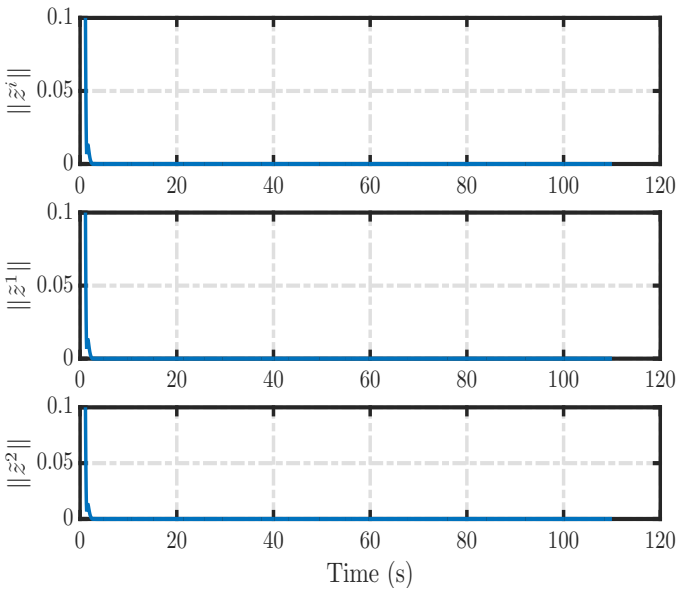

Figure 6. Attack-free auxiliary system residual.

5.2. COVERT ATTACK CASE 1

Similar to Paper I, here at $t = 90$ an attack occurs on the leader robot i whereas the attack magnitude is smaller compared to that in Paper I but the effect is significant. In the case of an actuator attack, the robot backstepping control law keeps the robot from deviating significantly from its trajectory. As seen in Figure 7, an actuator attack applied for a duration of $2s$ can change the direction of the formation permanently. Figure 8 shows the tracking error increasing in the leader as it no longer tracks the reference cart. The follower 1 is unaware of the attack on it's leader so it tries to reduce the sudden increase in tracking error. Figure 9 shows the actual robot residual keeps increasing but due to the covert attack, the leader i only observes the attack residual shown in Figure 10. Figure 11 shows how the auxiliary system residual can detect the covert attack while the observer-based residual method designed in Paper I fails.

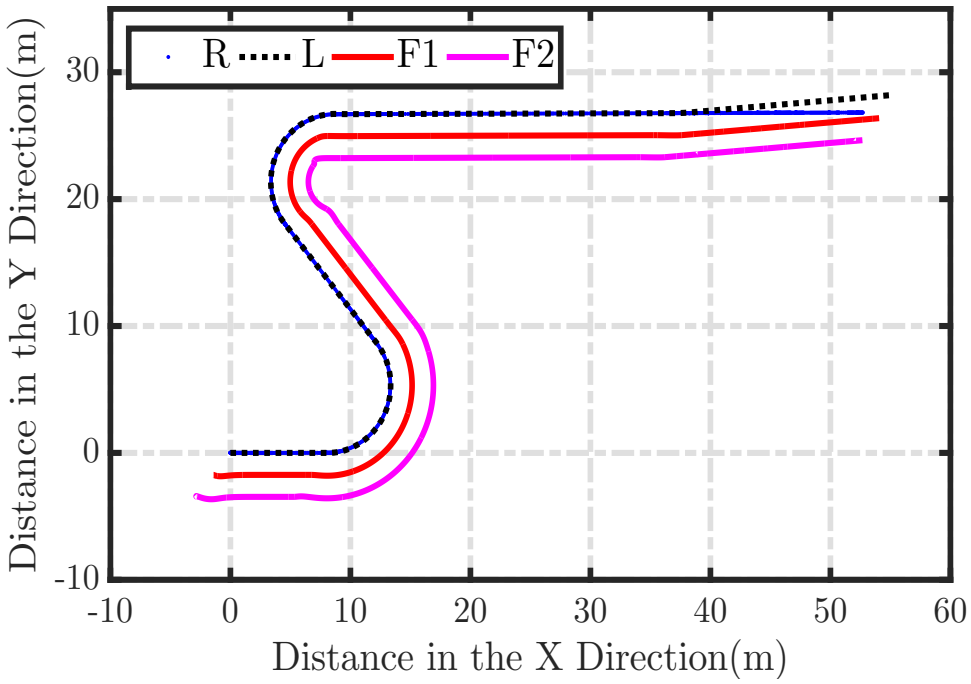

Figure 7. Formation trajectories with leader under attack.

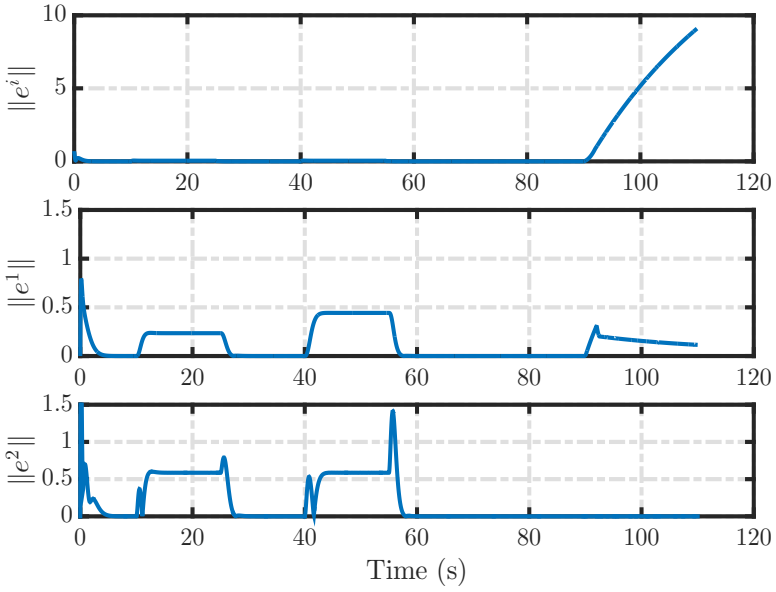

Figure 8. Tracking error norm with leader under attack.

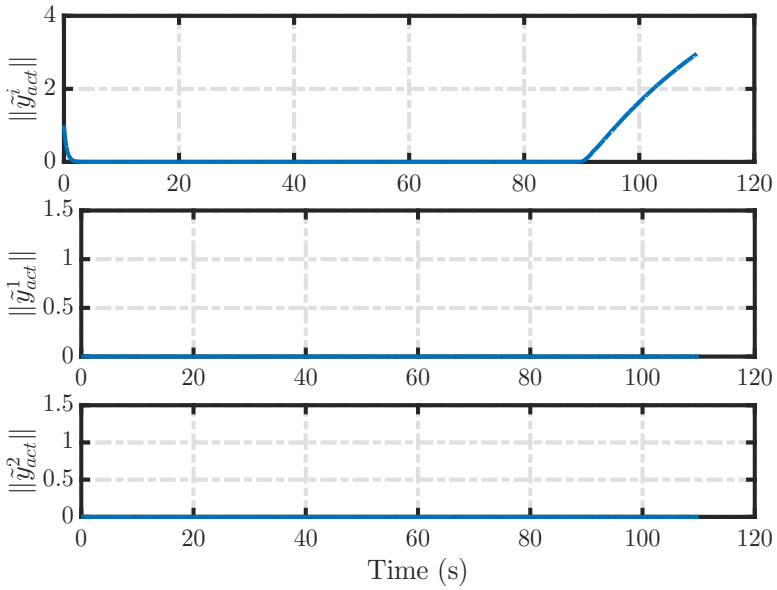

Figure 9. Actual estimation error norm with leader under attack.

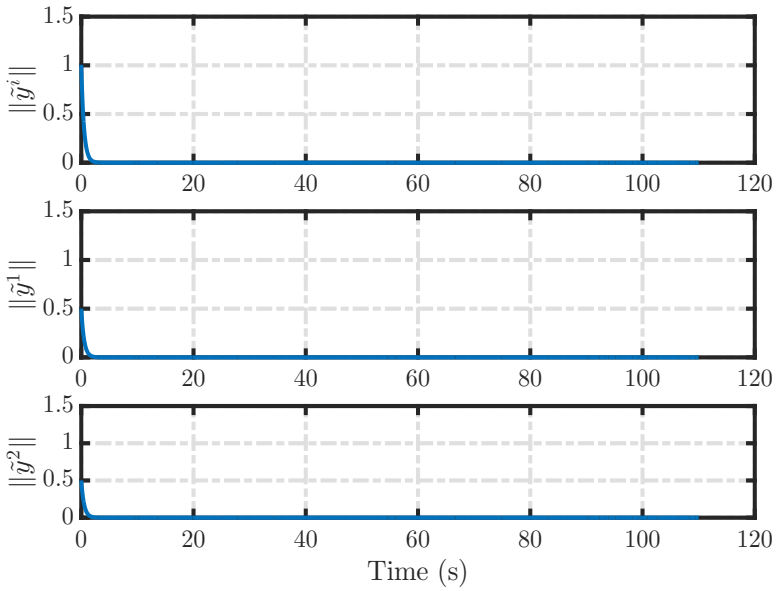

Figure 10. Falsified estimation error norm with leader under attack.

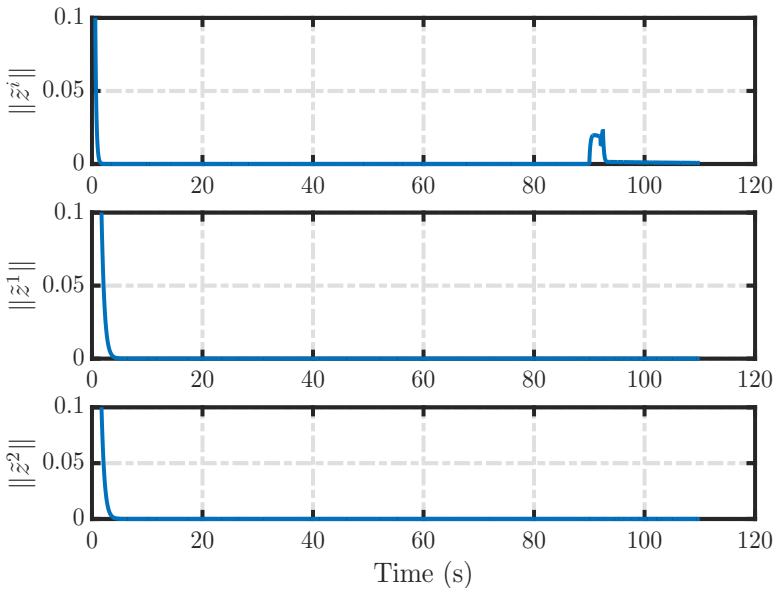

Figure 11. Leader attacked auxiliary system residual.

5.3. COVERT ATTACK CASE 2

An attack occurs on the Follower 1 at $t = 80s$. Similar to leader i, a $2s$ actuator attack causes the follower robot 1 to deviate from its trajectory significantly as observed in Figure 12. The follower 2 unaware that it's follower 1 is changing trajectory because of an attack follows suit. The deviation in trajectory causes the follower to be ahead of its desired separation-bearing. This is noticeable in the follower 2 tracking error in Figure 13. Even though the actual residual is increasing as per Figure 14, the follower 1 is only aware of the residual in Figure 15. The auxiliary residual shows the presence of an attack as seen in Figure 16.

6. CONCLUSION AND FUTURE WORK

In this paper, a covert attack detection scheme is presented. It was shown that when there is no attack mitigation scheme, then a covert attack over finite time actuator attack can change the formation trajectories permanently. Since the output residual fails to detect such

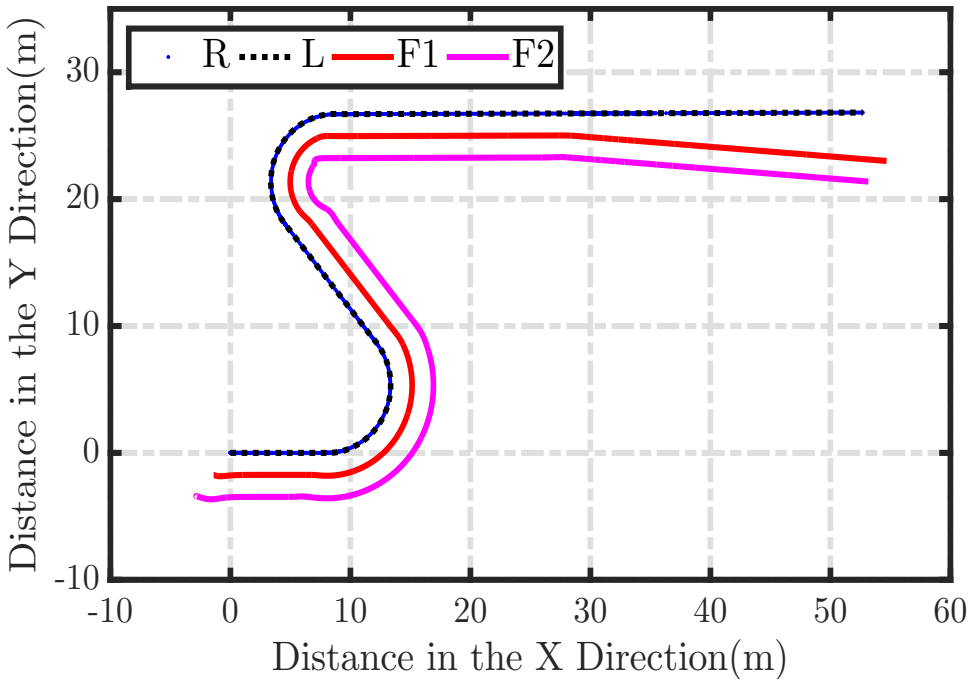

Figure 12. Formation trajectories with follower 1 under attack.

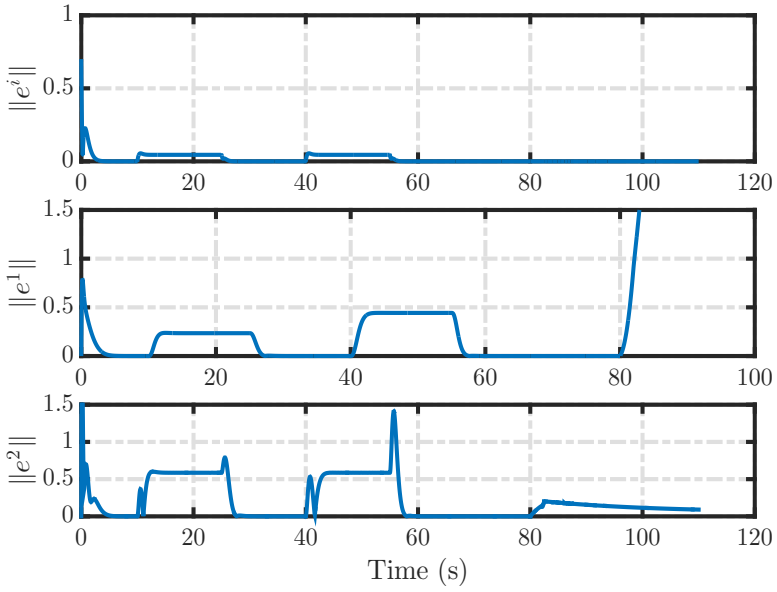

Figure 13. Tracking error norm with follower 1 under attack.

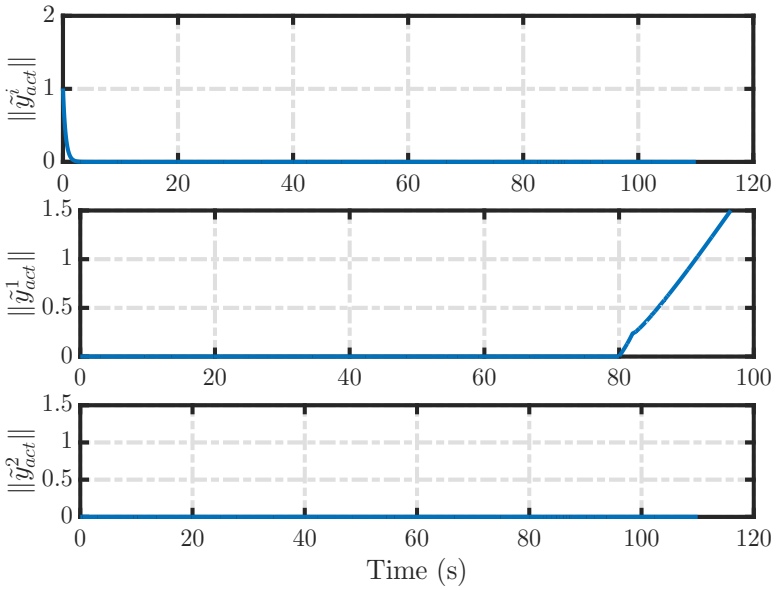

Figure 14. Estimation errors with follower 1 under attack.

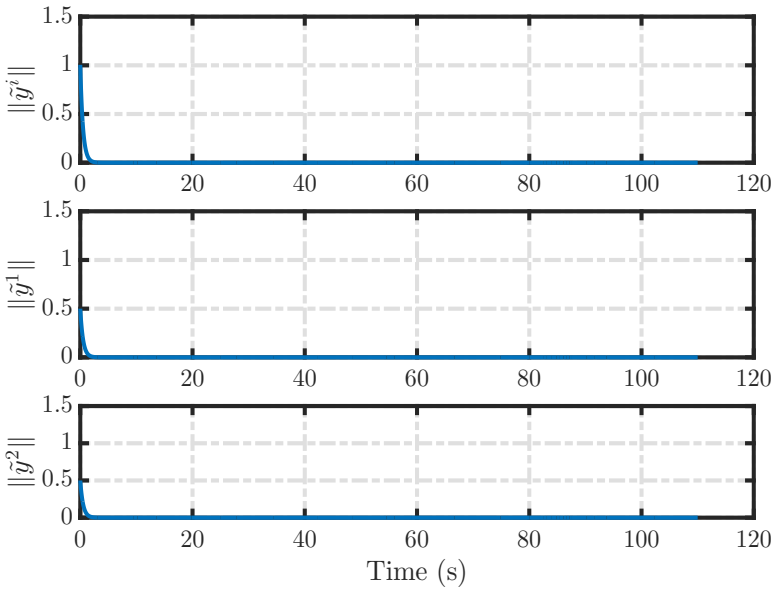

Figure 15. Actual estimation error norm with follower 1 under attack.

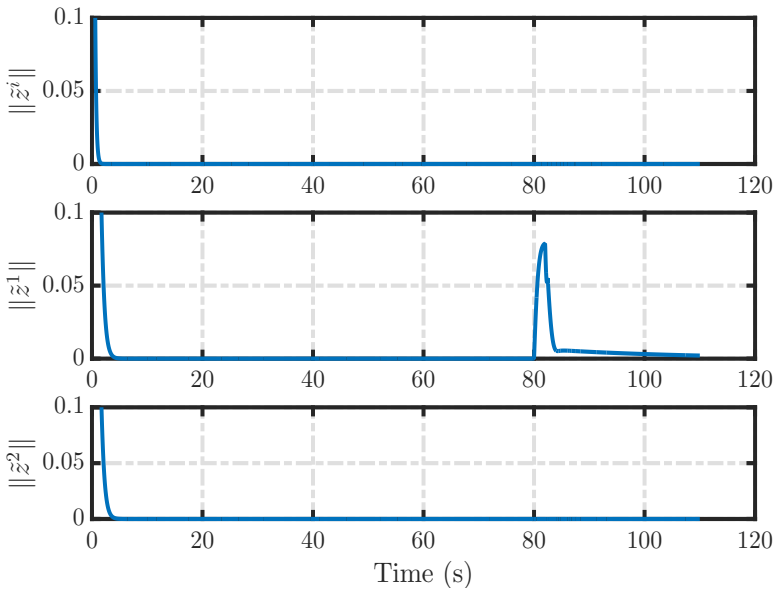

Figure 16. Follower 1 auxiliary system residual under attack.

attacks, an auxiliary system introduced detects the attack and its residual is modified in the presence of the actuator attack. From Paper I Theorem 3, it is evident that in the presence of an actuator attack the estimation and tracking errors increase. If the sensors on the robot are reliable then the robot becomes aware of this attack and it can correct its course. Even if there is no mitigation, the errors stay bounded because of the backstepping-based control law. In Theorem 1, it was shown that in the case of a covert attack the robot never realises it is under attack due to spurious sensor data and so it can not take any corrective measures.

Thus, the robot estimation error keeps increasing as the backstepping-based control law no longer stabilizes the actual robot but the virtual robot. Future work will deal with making the auxiliary system have statistical time varying properties so that even if the attacker is able to gain access to the auxiliary system model, input, and measurements, they can still be detected.

REFERENCES

[1] Balch, T. and Arkin, R. C., 'Behavior-based formation control for multirobot teams,' IEEE transactions on robotics and automation, 1998, 14(6), pp. 926–939.

[2] Barnes, L., Fields, M., and Valavanis, K., 'Unmanned ground vehicle swarm formation control using potential fields,' in '2007 Mediterranean Conference on Control & Automation,' IEEE, 2007 pp. 1–8.

[3] Bianchin, G., Liu, Y.-C., and Pasqualetti, F., 'Secure navigation of robots in adversarial environments,' IEEE Control Systems Letters, 2019, 4(1), pp. 1–6.

[4] Brandao, A. S., Sarcinelli-Filho, M., Carelli, R., and Bastos-Filho, T. F., 'Decentralized control of leader-follower formations of mobile robots with obstacle avoidance,' in '2009 IEEE International Conference on Mechatronics,' IEEE, 2009 pp. 1–6.

[5] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., et al., 'Comprehensive experimental analyses of automotive attack surfaces.' in 'USENIX Security Symposium,' volume 4, San Francisco, 2011 pp. 447–462.

[6] Chen, Y. Q. and Wang, Z., 'Formation control: a review and a new consideration,' in '2005 IEEE/RSJ International conference on intelligent robots and systems,' IEEE, 2005 pp. 3181–3186.

[7] Desai, J. P., Ostrowski, J., and Kumar, V., 'Controlling formations of multiple mobile robots,' in 'Robotics and Automation, 1998. Proceedings. 1998 IEEE International Conference on,' volume 4, IEEE, 1998 pp. 2864–2869.

[8] Dierks, T., Brenner, B., and Jagannathan, S., 'Near optimal control of mobile robot formations,' in '2011 IEEE Symposium on Adaptive Dynamic Programming and Reinforcement Learning (ADPRL),' IEEE, 2011 pp. 234–241.

[9] Dierks, T. and Jagannathan, S., 'Control of nonholonomic mobile robot formations: Backstepping kinematics into dynamics,' in '2007 IEEE International Conference on Control Applications,' IEEE, 2007 pp. 94–99.

[10] Dierks, T. and Jagannathan, S., 'Neural network control of mobile robot formations using rise feedback,' IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2009, 39(2), pp. 332–347.

[11] Dierks, T. and Jagannathan, S., 'Neural network output feedback control of robot formations,' IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2010, 40(2), pp. 383–399.

[12] Fagiolini, A., Babboni, F., and Bicchi, A., 'Dynamic distributed intrusion detection for secure multi-robot systems,' in '2009 IEEE International Conference on Robotics and Automation,' IEEE, 2009 pp. 2723–2728.

[13] Fawzi, H., Tabuada, P., and Diggavi, S., 'Secure estimation and control for cyber-physical systems under adversarial attacks,' IEEE Transactions on Automatic control, 2014, 59(6), pp. 1454–1467.

[14] Fierro, R. and Lewis, F. L., 'Control of a nonholomic mobile robot: Backstepping kinematics into dynamics,' Journal of robotic systems, 1997, 14(3), pp. 149–163.

[15] Fierro, R. and Lewis, F. L., 'Control of a nonholonomic mobile robot using neural networks,' IEEE Transactions on neural networks, 1998, 9(4), pp. 589–600.

[16] Gerdes, R. M., Winstead, C., and Heaslip, K., 'Cps: an efficiency-motivated attack against autonomous vehicular transportation,' in 'Proceedings of the 29th Annual Computer Security Applications Conference,' ACM, 2013 pp. 99–108.

[17] Griffioen, P., Weerakkody, S., and Sinopoli, B., 'A moving target defense for securing cyber-physical systems,' arXiv preprint arXiv:1902.01423, 2019.

[18] Kanayama, Y., Kimura, Y., Miyazaki, F., and Noguchi, T., 'A stable tracking control method for an autonomous mobile robot,' in 'Proceedings., IEEE International Conference on Robotics and Automation,' IEEE, 1990 pp. 384–389.

[19] Kwon, C., Liu, W., and Hwang, I., 'Security analysis for cyber-physical systems against stealthy deception attacks,' in '2013 American control conference,' IEEE, 2013 pp. 3344–3349.

[20] Lewis, F. L., Dawson, D. M., and Abdallah, C. T., Robot manipulator control: theory and practice, CRC Press, 2003.

[21] Luo, C., Espinosa, A. P., Pranantha, D., and De Gloria, A., 'Multi-robot search and rescue team,' in '2011 IEEE International Symposium on Safety, Security, and Rescue Robotics,' IEEE, 2011 pp. 296–301.

[22] Mo, Y., Garone, E., Casavola, A., and Sinopoli, B., 'False data injection attacks against state estimation in wireless sensor networks,' in '49th IEEE Conference on Decision and Control (CDC),' IEEE, 2010 pp. 5967–5972.

[23] Mo, Y. and Sinopoli, B., 'Secure control against replay attacks,' in '2009 47th annual Allerton conference on communication, control, and computing (Allerton),' IEEE, 2009 pp. 911–918.

[24] Osterloh, C., Pionteck, T., and Maehle, E., 'Monsun ii: A small and inexpensive auv for underwater swarms,' in 'ROBOTIK 2012; 7th German Conference on Robotics,' VDE, 2012 pp. 1–6.

[25] Pajic, M., Weimer, J., Bezzo, N., Sokolsky, O., Pappas, G. J., and Lee, I., 'Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators,' IEEE Control Systems Magazine, 2017, 37(2), pp. 66–81.

[26] Pasqualetti, F., Dörfler, F., and Bullo, F., 'Attack detection and identification in cyber-physical systems,' IEEE transactions on automatic control, 2013, 58(11), pp. 2715–2729.

[27] Petit, J. and Shladover, S. E., 'Potential cyberattacks on automated vehicles,' IEEE Transactions on Intelligent Transportation Systems, 2014, 16(2), pp. 546–556.

[28] Ren, W., Beard, R. W., and Atkins, E. M., 'Information consensus in multivehicle cooperative control,' IEEE Control systems magazine, 2007, 27(2), pp. 71–82.

[29] Roberts, J. A., 'Satellite formation flying for an interferometry mission,' 2005.

[30] Schellenberger, C. and Zhang, P., 'Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system,' in '2017 IEEE 56th Annual Conference on Decision and Control (CDC),' IEEE, 2017 pp. 1374–1379.

[31] Shao, J., Xie, G., and Wang, L., 'Leader-following formation control of multiple mobile vehicles,' IET Control Theory & Applications, 2007, 1(2), pp. 545–552.

[32] Smith, R. S., 'A decoupled feedback structure for covertly appropriating networked control systems,' IFAC Proceedings Volumes, 2011, 44(1), pp. 90–95.

[33] van der Heijden, R., Lukaseder, T., and Kargl, F., 'Analyzing attacks on cooperative adaptive cruise control (cacc),' in '2017 IEEE Vehicular Networking Conference (VNC),' IEEE, 2017 pp. 45–52.

[34] Vuong, T. P., Loukas, G., Gan, D., and Bezemskij, A., 'Decision tree-based detection of denial of service and command injection attacks on robotic vehicles,' in '2015 IEEE International Workshop on Information Forensics and Security (WIFS),' IEEE, 2015 pp. 1–6.

[35] Wit, C. C. d., Khennouf, H., Samson, C., and Sordalen, O. J., 'Nonlinear control design for mobile robots,' in 'Recent trends in mobile robots,' pp. 121–156, World Scientific, 1993.

APPENDIX

BOUNDS

To begin with, some bounds which are used in the proofs are established here. The subscripts are intentionally ignored to avoid repetition.

$$\|v\| \leq v_{max} \quad \|\omega\| \leq \omega_{max} \quad \|\tau\| \leq \tau_{max}$$

$$\|\dot{v}\| \leq a_{max} \quad \|\dot{\omega}\| \leq \alpha_{max}$$

$$\theta, \theta^r, \theta^{\pi jr}, \theta_r^{ir} \epsilon (-\pi, \pi]$$

$$\|\tilde{\overline{F}}(\tilde{\overline{V}})\| \leq \mu_{max}\|\tilde{\overline{V}}\| + 2\mu_3; \mu_{max} = \lambda_{max}(\mu_2, \mu_4)$$

$$\|\tilde{\overline{V}}\| \leq \tilde{\overline{V}}_b$$

$$\|\overline{M}\|_F \leq M_b \tag{A-1}$$

SECTION

2. CONCLUSIONS AND FUTURE WORK

In this thesis, a suite of detection and mitigation schemes were developed for mobile robot formation control in the presence of an adversary. In Paper I, an observer for the leader and the follower robots was designed that effectively estimated the state vector of the robots, and computed the torque required for tracking the assigned leader. By properly selecting the control gains k_p^o and observer gains l_p^o where $o = (i, j)$, and $p = (1, 2, \ldots, 5)$, it was demonstrated that in an attack-free scenario, the residual would converge asymptotically provided the reference-cart angular velocity $\omega^r = 0$. During an actuator attack, it was noticed that the residual was non-zero but bounded provided the attack magnitude is finite. Boundedness of the residual in the presence of an attack is utilized for detection. Upon detection, a mitigation scheme was initiated using an FLNN to learn the attack input online in order to reduce its effect by modifying the controller.

On the other hand, in Paper II, a covert attack detection scheme was presented. The goal of this scheme was to detect attack on sensors and actuators in a leader/follower robot formation. It was shown that the residual-based attack detection-scheme designed in Paper I was not able to detect these covert attacks. An auxiliary system unknown to the adversary was affected by the attack on the robot. A residual-based detection scheme was then built on this auxiliary system to successfully detect covert attacks.

2.1. CONCLUSION

It was observed in Paper I that the tracking error norm of the follower was almost twice the tracking error of its assigned leader indicating that a change in the leader's trajectory increase from the leader to its follower and to other levels. In other words, the adversary could slightly destabilize a robot higher-up in the formation and cause high instability to the followers at the end of the formation. The residual of a follower robot however was unaffected by an actuator attack on its leader robot; and stayed at zero as expected since the dynamics were known to the controller. The residual-based approach was successfully able to detect actuator based attacks; the mitigation scheme reduced the robot tracking error and residual to near healthy bounds on both the leader and the follower. Simulation results demonstrated that the formation returned close to normal conditions in a short duration once the attack input was learned and corrected for.

It was observed in Paper II that when the residual detection scheme fails, then a covert attack consisting of a finite time actuator attack can change the formation trajectories permanently. From Paper I Theorem 3, it is evident that in the presence of an actuator attack, the estimation and tracking errors increase. If the sensors on the robot are reliable then the robot can be aware of this attack and it can correct its course. Even if there is no mitigation, the errors stay bounded because of the backstepping-based control law. In Paper II Theorem 1, it was shown that in the case of a covert attack, the robot cannot take any corrective measures as it is unaware of the attack. Thus, the robot estimation error keeps increasing as the backstepping-based control law no longer stabilizes the formation. On the other hand, defining an auxiliary system and making it sensitive can help detect the type of attacks.

2.2. FUTURE WORK

One aspect of future work is to design a mitigation scheme when a few of the sensors of the formation robots are attacked by the adversary. In addition, the assumptions made that the communication links are resilient and known dynamics can be relaxed in the presence of adversary. Another aspect of future work can include making the auxiliary system resilient even when the adversary gains access to it. This could be done using moving target defense (MTD) techniques [17]. Additionally, the proposed methods have to be evaluated in an obstacle ridden environment. Further, the follower robots of a covertly attacked robot no longer participate in accomplishing the formation objective. Techniques would have to be developed to make the follower realize whether it should trust its leader.

REFERENCES

[1] Balch, T. and Arkin, R. C., 'Behavior-based formation control for multirobot teams,' IEEE transactions on robotics and automation, 1998, **14**(6), pp. 926–939.

[2] Barnes, L., Fields, M., and Valavanis, K., 'Unmanned ground vehicle swarm formation control using potential fields,' in '2007 Mediterranean Conference on Control & Automation,' IEEE, 2007 pp. 1–8.

[3] Bianchin, G., Liu, Y.-C., and Pasqualetti, F., 'Secure navigation of robots in adversarial environments,' IEEE Control Systems Letters, 2019, **4**(1), pp. 1–6.

[4] Brandao, A. S., Sarcinelli-Filho, M., Carelli, R., and Bastos-Filho, T. F., 'Decentralized control of leader-follower formations of mobile robots with obstacle avoidance,' in '2009 IEEE International Conference on Mechatronics,' IEEE, 2009 pp. 1–6.

[5] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., *et al.*, 'Comprehensive experimental analyses of automotive attack surfaces.' in 'USENIX Security Symposium,' volume 4, San Francisco, 2011 pp. 447–462.

[6] Chen, Y. Q. and Wang, Z., 'Formation control: a review and a new consideration,' in '2005 IEEE/RSJ International conference on intelligent robots and systems,' IEEE, 2005 pp. 3181–3186.

[7] Desai, J. P., Ostrowski, J., and Kumar, V., 'Controlling formations of multiple mobile robots,' in 'Robotics and Automation, 1998. Proceedings. 1998 IEEE International Conference on,' volume 4, IEEE, 1998 pp. 2864–2869.

[8] Dierks, T., Brenner, B., and Jagannathan, S., 'Near optimal control of mobile robot formations,' in '2011 IEEE Symposium on Adaptive Dynamic Programming and Reinforcement Learning (ADPRL),' IEEE, 2011 pp. 234–241.

[9] Dierks, T. and Jagannathan, S., 'Control of nonholonomic mobile robot formations: Backstepping kinematics into dynamics,' in '2007 IEEE International Conference on Control Applications,' IEEE, 2007 pp. 94–99.

[10] Dierks, T. and Jagannathan, S., 'Neural network control of mobile robot formations using rise feedback,' IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2009, **39**(2), pp. 332–347.

[11] Dierks, T. and Jagannathan, S., 'Neural network output feedback control of robot formations,' IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2010, **40**(2), pp. 383–399.

[12] Fagiolini, A., Babboni, F., and Bicchi, A., 'Dynamic distributed intrusion detection for secure multi-robot systems,' in '2009 IEEE International Conference on Robotics and Automation,' IEEE, 2009 pp. 2723–2728.

[13] Fawzi, H., Tabuada, P., and Diggavi, S., 'Secure estimation and control for cyber-physical systems under adversarial attacks,' IEEE Transactions on Automatic control, 2014, **59**(6), pp. 1454–1467.

[14] Fierro, R. and Lewis, F. L., 'Control of a nonholomic mobile robot: Backstepping kinematics into dynamics,' Journal of robotic systems, 1997, **14**(3), pp. 149–163.

[15] Fierro, R. and Lewis, F. L., 'Control of a nonholonomic mobile robot using neural networks,' IEEE Transactions on neural networks, 1998, **9**(4), pp. 589–600.

[16] Gerdes, R. M., Winstead, C., and Heaslip, K., 'Cps: an efficiency-motivated attack against autonomous vehicular transportation,' in 'Proceedings of the 29th Annual Computer Security Applications Conference,' ACM, 2013 pp. 99–108.

[17] Griffioen, P., Weerakkody, S., and Sinopoli, B., 'A moving target defense for securing cyber-physical systems,' arXiv preprint arXiv:1902.01423, 2019.

[18] Kanayama, Y., Kimura, Y., Miyazaki, F., and Noguchi, T., 'A stable tracking control method for an autonomous mobile robot,' in 'Proceedings., IEEE International Conference on Robotics and Automation,' IEEE, 1990 pp. 384–389.

[19] Kwon, C., Liu, W., and Hwang, I., 'Security analysis for cyber-physical systems against stealthy deception attacks,' in '2013 American control conference,' IEEE, 2013 pp. 3344–3349.

[20] Lewis, F. L., Dawson, D. M., and Abdallah, C. T., *Robot manipulator control: theory and practice*, CRC Press, 2003.

[21] Luo, C., Espinosa, A. P., Pranantha, D., and De Gloria, A., 'Multi-robot search and rescue team,' in '2011 IEEE International Symposium on Safety, Security, and Rescue Robotics,' IEEE, 2011 pp. 296–301.

[22] Mo, Y., Garone, E., Casavola, A., and Sinopoli, B., 'False data injection attacks against state estimation in wireless sensor networks,' in '49th IEEE Conference on Decision and Control (CDC),' IEEE, 2010 pp. 5967–5972.

[23] Mo, Y. and Sinopoli, B., 'Secure control against replay attacks,' in '2009 47th annual Allerton conference on communication, control, and computing (Allerton),' IEEE, 2009 pp. 911–918.

[24] Osterloh, C., Pionteck, T., and Maehle, E., 'Monsun ii: A small and inexpensive auv for underwater swarms,' in 'ROBOTIK 2012; 7th German Conference on Robotics,' VDE, 2012 pp. 1–6.

[25] Pajic, M., Weimer, J., Bezzo, N., Sokolsky, O., Pappas, G. J., and Lee, I., 'Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators,' IEEE Control Systems Magazine, 2017, **37**(2), pp. 66–81.

[26] Pasqualetti, F., Dörfler, F., and Bullo, F., 'Attack detection and identification in cyber-physical systems,' IEEE transactions on automatic control, 2013, **58**(11), pp. 2715–2729.

[27] Petit, J. and Shladover, S. E., 'Potential cyberattacks on automated vehicles,' IEEE Transactions on Intelligent Transportation Systems, 2014, **16**(2), pp. 546–556.

[28] Ren, W., Beard, R. W., and Atkins, E. M., 'Information consensus in multivehicle cooperative control,' IEEE Control systems magazine, 2007, **27**(2), pp. 71–82.

[29] Roberts, J. A., 'Satellite formation flying for an interferometry mission,' 2005.

[30] Schellenberger, C. and Zhang, P., 'Detection of covert attacks on cyber-physical systems by extending the system dynamics with an auxiliary system,' in '2017 IEEE 56th Annual Conference on Decision and Control (CDC),' IEEE, 2017 pp. 1374–1379.

[31] Shao, J., Xie, G., and Wang, L., 'Leader-following formation control of multiple mobile vehicles,' IET Control Theory & Applications, 2007, **1**(2), pp. 545–552.

[32] Smith, R. S., 'A decoupled feedback structure for covertly appropriating networked control systems,' IFAC Proceedings Volumes, 2011, **44**(1), pp. 90–95.

[33] van der Heijden, R., Lukaseder, T., and Kargl, F., 'Analyzing attacks on cooperative adaptive cruise control (cacc),' in '2017 IEEE Vehicular Networking Conference (VNC),' IEEE, 2017 pp. 45–52.

[34] Vuong, T. P., Loukas, G., Gan, D., and Bezemskij, A., 'Decision tree-based detection of denial of service and command injection attacks on robotic vehicles,' in '2015 IEEE International Workshop on Information Forensics and Security (WIFS),' IEEE, 2015 pp. 1–6.

[35] Wit, C. C. d., Khennouf, H., Samson, C., and Sordalen, O. J., 'Nonlinear control design for mobile robots,' in 'Recent trends in mobile robots,' pp. 121–156, World Scientific, 1993.

VITA

Arnold Fernandes received his Bachelor of Technology in Electrical Engineering from Pandit Deendayal Petroleum University, Raisan, Gandhinagar, Gujarat, India, in 2015. He then moved to the USA to pursue his MS degree in Electrical Engineering at Missouri University of Science and Technology. He received his master's degree in Electrical Engineering in May 2020 from Missouri S&T. He started his PhD in Electrical Engineering at Missouri University of Science and Technology in Spring 2020.