Model-based resilient control for a multi-agent system against Denial of Service attacks

Conference Paper · July 2016

DOI: 10.1109/WAC.2016.7582963

3 authors:

Esther Amullen
Tennessee State University
4 PUBLICATIONS **15** CITATIONS
SEE PROFILE

Sachin Shetty
Old Dominion University
174 PUBLICATIONS **923** CITATIONS
SEE PROFILE

Lee Keel
Northeastern University
174 PUBLICATIONS **3,576** CITATIONS
SEE PROFILE

Model-based resilient control for a multi-agent system against Denial of Service attacks

Esther M. Amullen, Sachin Shetty, and Lee H. Keel
Tennessee State University
3500 John A Merritt Blvd
Nashville, Tennessee 37209
Email: eamullen@my.tnstate.edu, sshetty@tnstate.edu, lkeel@tnstate.edu

[1]

***Abstract*—The computerization of critical infrastructure such as control systems means that these systems interact with information technology (IT) to an extent that makes them susceptible to malicious attacks. While IT security places emphasis on data accuracy easily attainable through simple error correction schemes such as packet re-transmission, control systems emphasize timely and accurate transmission of control signals in which delays or re-transmissions can have detrimental effects on the system. This motivates the need for resilient control algorithms that guarantee normal operation of critical infrastructure subject to malicious attacks and disturbances both at the physical layer and communication layer. In this paper, a team of networked autonomous agents whose collective objective is formation control is used to represent a cyber-physical system. A distributed formation control algorithm in which each agent depends only on its local information and that received from one neighbor to cooperatively carry out the group mission is employed. We develop a model-based resilient control algorithm that enables the team of autonomous agents accomplish their formation task even in the presence of a malicious denial of service (DOS) attack disrupting inter-agent communication. The technique is demonstrated through a laboratory experiment with 6 pioneer 3DX robots.**

I. Introduction

Today's society increasingly relies on computerized control systems to automate key industrial operations and delivery of critical services. While increased computer interconnectivity over networks has great benefits, a hostile cyber environment poses a security risk to critical infrastructure such as water distribution networks, the power grids and transport infrastructure that is now largely supported by computer systems [1]. Research and recent events have shown that such systems are vulnerable to failure resulting from malicious attacks targeting both physical and communication infrastructure.

Recent studies including [5], [6], [7], [12] show these attacks to be feasible and propose various detection schemes for such attacks. Denial of Service (DOS) attacks on cyber-physical systems particularly have drawn much attention in recent years as these affect the transmission of data packets comprising control signals critical for systems operations both at the communication layer and physical layer. The impact of DOS attacks on critical infrastructure has been shown by research and real world events presented in [2], [3], [4]. Motivated by the issues mentioned above, strategies that ensure normal operation of networked control systems subject to disturbances and malicious attacks are essential. These are called resilient control Strategies in which the controller is designed to ensure system security. Our objective is to develop a resilient control strategy that ensures normal operation of a multi-agent system in the presence of a DOS attack. We consider a formation control problem for a team of autonomous agents that share control signals through a network that can easily be compromised by an adversary. [13], [14], [15], [16], [17] among others have proposed resilient control strategies. In [15], the authors propose a variation of the receding-horizon control law in which the plant stores the computed control sequence and uses it in the near future as a countermeasure against replay attacks. An attack-resilient distributed formation control algorithm was proposed by Zhu et. al. in [13] in which vehicles under attack collect information about the attackers and exploit this information to adapt their control law to still achieve their objective. In [14], an aerial jammer attacks the communication channel of a team of UAVs in formation. The attack is modeled as a continuous time pursuit evasion game between the UAVs and the attacker. The authors propose a game theoretic approach for the agents to compute optimal control strategies to evade the attacker and achieve their objective. [16] considers a networked multi-agent system with misbehaving agents and proposes a distributed adaptive control architecture that utilizes a local state estimator to retrieve the dynamic behavior of the system under normal conditions to ensure resilient control in the presence of misbehaving agents. In [17] Zeng et. al. study the consensus problem for a multi-agent system with misbehaving agents. They propose a reputation-based resilient distributed control algorithm for a leader-follower consensus network and a leaderless consensus network that embeds a resilience mechanism into the control process enabling each agent to detect and isolate misbehaving agents.

Directly related to our work are [13], [14], [15], [16], [17]. While [16] and [17] deal with multi-agent systems in which one of the agents is the adversary, their strategy is to identify and isolate the misbehaving agent so that the rest of the agents can achieve consensus, in our approach however, we consider

[1]*This work was supported in part by DoD Grant W911NF-08-0514

an external adversary and a formation problem in which each agent is critical for mission completion; rather than remove an impacted agent, our approach will enable an agent correct its behavior and complete the mission with the rest of the agents. In [15] the plant uses a stored pre-designed sequence of control laws used when the system is under attack, in our approach, the plant only requires state information from the previous time step. Finally, the approach we propose is distributed with individual agents, detecting anomalies and carrying out corrective actions based on their local information and information from a single neighbor which in comparison to employing a centralized control strategy is flexible, robust in a sense that there is only one point of failure and is not limited to the size of the network. Unlike [17] in which the resilient control mechanism is embedded into the consensus algorithm, our resilient control strategy is a stand alone mechanism employed along side the primary algorithm and thus can be easily adapted to any system without redesigning the main algorithm.

In this paper, we develop a distributed model-based resilient control algorithm that enables each agent determine its respective corrective control action when under a DOS attack. To demonstrate the effectiveness of the proposed technique, we consider a team of autonomous agents whose mission is to cooperatively achieve and maintain formation. Each agent only uses its local information and that received from a single neighbor to determine its control action so as to achieve formation. The algorithm can be adapted to different types of networked control systems.

II. Control Objective

Formation control is an important problem in multi-agent systems and has been under consideration by the research community for decades. It is defined as the coordination of a group of agents to get into and maintain formation. It is known that a multi-agent formation problem requires accurate and precise data exchange between agents to achieve the goal of formation. As a result, data distortion due to intrusion on any communication link makes it impossible for the system to reach desired formation. In this paper, we show that our proposed resilient control algorithm given in the next section ensures that the system achieves its goal despite the DOS attack on some communication links between agents. In the following section, we briefly describe the plant (or system) we consider, that is, a multi-agent system whose group objective is formation control by cyclic pursuit (see [18], [19], [20], [21], [22] and references therein). Consider n autonomous agents whose positions at time $t \geq 0$ is given by $z_i(t) = [x_i(t), y_i(t)]^T \in \mathbb{R}^2$ for $i = 1, 2, \ldots, n$, for the case of 2D coordinates. Let $\mathcal{N}$ denote all the agents immediately adjacent to agent i and $i+1$ be a single agent adjacent to i. If each agent pursues the next $modulo^2$ n at constant speed, they will trace out logarithmic spirals and eventually meet at the polygon's center. Agent dynamics are given by the single integrator model

$$\dot{z}_i(t) = u_i(t) \tag{1}$$

where

$$u_i(t) = z_{i+1}(t) - z_i(t). \tag{2}$$

Theorem II.1. *Assume that graph $\mathcal{G}$ is connected and symmetric. Then the continuous-time average consensus algorithm for a multiple agent system globally asymptotically solves the average consensus problem*

$$\dot{z}_i(t) = -\sum_{i+1 \in \mathcal{N}} (z_i(t) - z_{i+1}(t))\, eq : z \tag{3}$$

$$z_i^* := \lim_{t \to \infty} z_i(t) = \frac{1}{n} \sum_{i=1}^{n} z_i(0), \quad \textit{for } i = 1, 2, \cdots, n. \tag{4}$$

A small modification to the agreement problem results into various types of agent formations. To achieve a particular formation, an agent pursues the next agent with a virtual displacement. Let c denote the virtual displacement between agents required to achieve formation such that (11) becomes;

$$\dot{z}_i(t) = -\sum (z_i(t) - z_{i+1}(t) - c_i), \quad \text{for } i = 1, 2, \cdots, n-1 \tag{5}$$

$$\dot{z}_n(t) = -\sum (z_n(t) - z_1(t) - c_n). \quad \text{for } i = n \tag{6}$$

Consequently, agent dynamics can be written as

$$\dot{\mathbf{z}}(t) = \underbrace{\begin{bmatrix} -1 & 1 & 0 & \cdots & 0 \\ 0 & -1 & 1 & & \vdots \\ \vdots & & \ddots & & \vdots \\ 1 & 0 & \cdots & \cdots & -1 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} z_1(t) \\ z_2(t) \\ \vdots \\ z_n(t) \end{bmatrix}}_{\mathbf{z}(t)} + \underbrace{\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}}_{\mathbf{c}} \tag{7}$$

or

$$\dot{\mathbf{z}}(t) = A\mathbf{z}(t) + \mathbf{c}. \tag{8}$$

The points $c_1, c_2, \cdots, c_n$ define the geometry of the desired formation. For the agents to achieve formation, the centroid O_c of the points $c_1, c_2, \cdots, c_n$ where

$$O_c = \frac{\sum_i c_i}{n} \tag{9}$$

must be at the origin. Let $\mathcal{E}$ denote the eigenspace of A. For formation, $c \in \mathcal{E}$ corresponding to eigenvalues with negative real parts. Then there exists unique d such that $d \in \mathcal{E}$ and

$$Ad + c = 0. \tag{10}$$

From (5) and (10),

$$\dot{z}(t) = A(z(t) - d). \tag{11}$$

This leads to following in [22]

Theorem II.2. *Assume that the centroid of the points $c_1, c_2, \cdots, c_n$ is at the origin. It follows that for all initial conditions, the centroid of the points $z_1(t), \cdots, z_n(t)$ is fixed and $z_i(t)$ for all i converges to this centroid with a displacement d_i.*

III. Proposed Resilient Control

Fig. 1 depicts the proposed resilient control strategy. A mathematical model of the system created based on the formation algorithm is implemented alongside the actual system. It is set to continuously track the true and correct states of agents for resilient control. However, due to the unavoidable difference between the mathematical model and the actual system, the error between the states of the model and the system at any given time can grow significantly large as the states depend on values of the past states. As a result, the model and the system can even reach different steady state values. Our strategy to limit the error between these two sets of states is to use the states of the actual system for calculating the next states of the mathematical model as long as the states of the actual system are not altered or corrupted by attacks. To achieve resilient control, when an attack is detected, the state of the model is used to determine the control action for the agent and the corrupted information coming through the network is ignored. To better illustrate the proposed resilient control strategy, let the actual system be

$$\dot{z}_s(t) = A_s z_s(t) + Bu(t) \tag{12}$$

and the mathematical model representing (12) be

$$\dot{z}_m(t) = A_m z_m(t) + Bu(t) \tag{13}$$

where $A_s \in \mathbb{R}^{n\times n}$, $A_m \in \mathbb{R}^{n\times n}$, are the state matrix for the actual system and mathematical model, respectively, $B \in \mathbb{R}^{n\times m}$ is the input matrix, $u \in \mathbb{R}^m$ is the control input, $z_s \in \mathbb{R}^n$ is the state vector *measured* from the actual system, and $z_m \in \mathbb{R}^n$ is the state vector *calculated* from the mathematical model. The mathematical model state matrix A_m is the adjacency matrix representing the position of an agent relative to its immediate neighbor according to the cyclic pursuit formation control strategy. Agent dynamics are not taken into account only their graph topology is considered.

Assumption III.1. *Under the conditions $z_s(t) = z_m(t)$ at any given time t, we make the following assumption:*

$$\|z_s(t+\Delta t) - z_m(t+\Delta t)\| < \epsilon \tag{14}$$

with a small value of Δt for sufficiently small ϵ.

Note that for a small value of Δt, $z_s(t) \approx z_m(t)$. Thus, we believe that the assumption made above is reasonable and practical. It is important to note that the above assumption does not guarantee the error between the states of the two systems (the actual system and the model) remains small for all t. Thus, we make the following proposition.

Proposition 1. *Without loss of generality, we consider the case $u(t) = 0$. For any given t, we write*

$$z_s(t+\Delta t) = f\left(A_s, z_s(t)\right) \tag{15}$$

and

$$z_m(t+\Delta t) = f\left(A_m, z_m(t)\right). \tag{16}$$

Then

$$\|z_s(t) - \overline{z}_m(t)\| < \epsilon \tag{17}$$

for each and every t where

$$\overline{z}_m(t+\Delta t) = f\left(A_m, z_s(t)\right) \tag{18}$$

Proof. Consider

$$z_s(t+\Delta t) = A_s z_s(t)\Delta t + z_s(t) \tag{19}$$

$$z_m(t+\Delta t) = A_m z_m(t)\Delta t + z_m(t). \tag{20}$$

Let

$$\overline{z}_m(t+\Delta t) = A_m z_s(t)\Delta t + z_s(t)). \tag{21}$$

From Assumption III.1, we have

$$\begin{aligned}\|z_s(t+\Delta t) - \overline{z}_m(t+\Delta t)\| &= \|(A_s - A_m) z_s(t)\Delta t\| \\ &< \epsilon \end{aligned} \tag{22}$$

for all t □

The proposed strategy is summarized in Algorithm 1

Algorithm 1 Model-based resilient control

Require: Initial state of the actual system $z_s(0)$, Initial state of the Mathematical model $z_m(0) = z_s(0)$

Ensure: Final actual system state z_s^* to accomplish the formation

procedure Model-based resilient control
  for each time step $t \geq 0$ **do**
    $z_m(t) \leftarrow z_s(t)$ (when no attacks present)
    $z_s(t) \leftarrow z_m(t)$ ((when an attacks present)
    repeat for $t = t + \Delta t$
  end for
end procedure

IV. A Laboratory Experiment

In order to test the proposed control strategy, we set up an experimental platform including real-world hardware. The experimental platform comprises six pioneer 3-DX robots each equipped with an on-board computer, a Wi-Fi network adapter and a serial communication port to facilitate communication with the robot micro-controller. The software used to interact with robot hardware is referred to as the robot operating system (ROS) [23] which works alongside traditional operating systems facilitating distributed computing enabling simultaneous control of multiple robots.

A directed communication graph topology is setup among the agents over an adhoc-network. The objective of the multi-agent system is formation control by cyclic pursuit. Each agent only communicates with one other agent and uses the information it receives to determine its control action.

While the agents are carrying out their mission, A DOS attack is carried out on Agent 1. Communication is blocked to the point that the agent cannot receive or transmit any information to the rest of the team. This disrupts the group

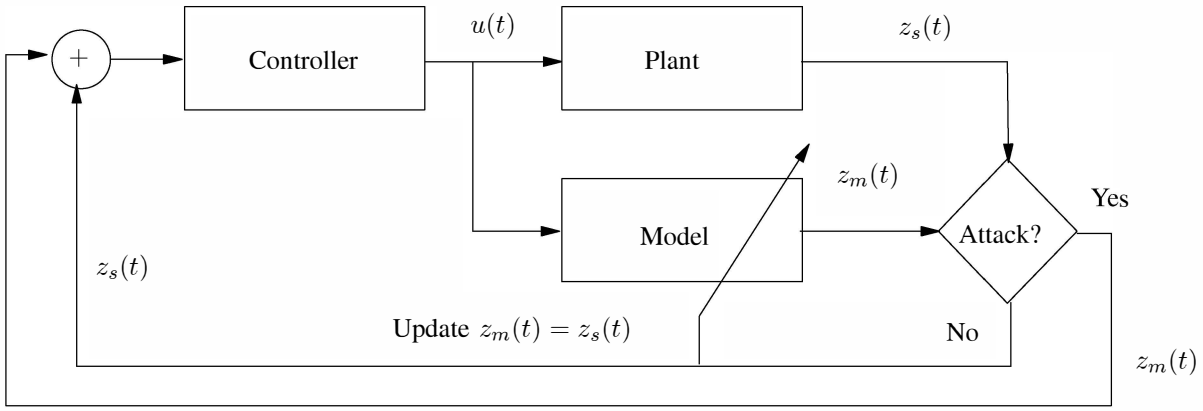
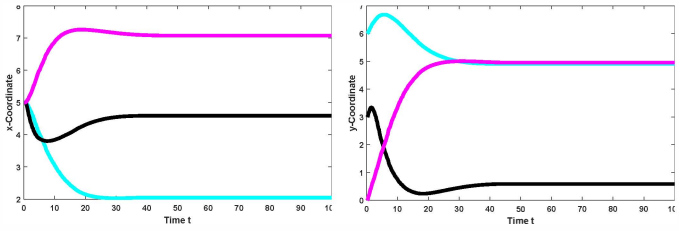


Fig. 1: Proposed resilient control strategy.

Fig. 2: Pioneer 3-DX robot

objective. The proposed resilient control algorithm is then implemented and it is shown that the agents achieve their objective while under attack. We now examine the experimental results obtained.

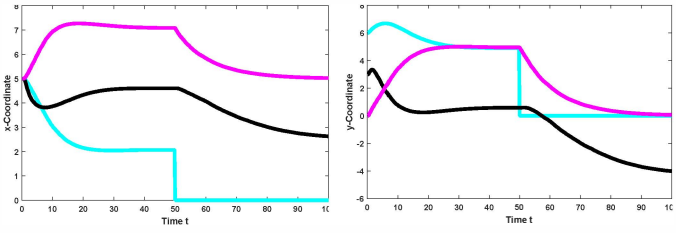
Example 1. 3-Agent System with one agent under attack
Consider a multi-agent system with 3 agents at arbitrary initial positions trying to achieve formation. The steady state values of the 3-agents form an equilateral triangle under normal operating conditions with no attack implemented. Fig. 3 is a 2-D plot of agents x, y values against time t under normal operation. Fig. 3a illustrates the $x-$coordinate information



(a) Agents position x-coordinate (b) Agents position y-coordinate

Fig. 3: 3-agent system under normal operation showing Position information recieved from designated neighbors

received by each of agents against time while Fig. 3b illustrates the $y-$coordinate information received by each of the agents against time. Agents reach steady state by $t = 30$. With all 3 agents in steady state as shown in Fig. 3, a DOS attack is applied to Agent 1 so that it cannot receive or transmit any information to and from its designated neighbors. Fig. 4 shows the impact of the DOS attack on agents' x, y position received by each agent from its designated neighbor. Although the attack is carried out on just Agent 1, but since the agents pursue each other with $modulo^2 n$ when the DOS attack is carried out, agents receive incorrect position information and thus all agent positions are impacted. The DOS attack is carried out starting at $t = 50$ to $t = 100$.

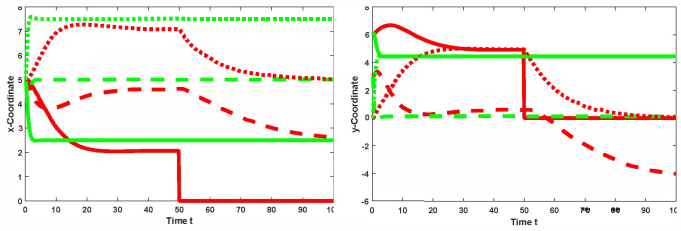


(a) Agents position x-coordinate (b) Agents position y-coordinate

Fig. 4: 3-agent system with a DOS attack affecting 1 agent showing position information received from designated neighbors

We now show how the proposed resilient control strategy corrects robot behavior during intrusion. First, we examine a case where the DOS attack is carried out on a single agent at steady state as illustrated in Fig. 4 from $t = 50$ to $t = 100$. Although the agent's communication link is impaired, it follows the correct trajectory by using values generated by the mathematical model implemented alongside the actual system in our proposed resilient control strategy. The algorithm thus accurately determines the agent position and desired control action according to Equation (13). It is important to note that the resilient control approach proposed gives the agent access to its own model predicted value and that of it's adjacent neighbor in the directed communication graph.

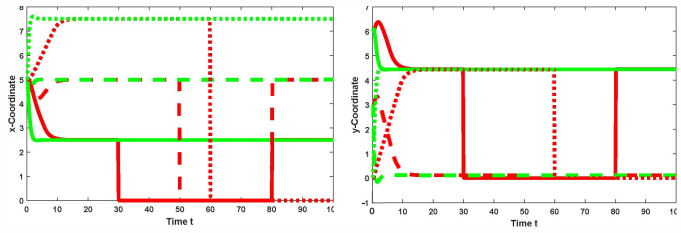
Example 2. 3-Agent System with all agents under attack
Now we look at a case in which all the agents in a 3-agent



(a) System and model x-coordinate(b) System and model y-coordinate

Fig. 5: 3-agent system with a DOS attack affecting 1 agent with resilient control implemented. The green lines are correct state values generated from the resilient control algorithm that the agents use to still achieve formation. The red lines indicate agent position information received by each agent from its designated neighbor impacted by the DOS attack.

multi-agent system are simultaneously under attack. With our resilient control strategy in place, the agents still achieve their formation objective. Each agent independently determines its control action with local information and that provided by its neighbor.



(a) Agents $x-$coordinate (b) Agents $y-$coordinate

Fig. 6: 3-agent system with a DOS attack affecting all agents. The attack on agent 1 is carried out from $t = 30$ to $t = 80$. The attack on agent 2 is carried out from $t = 50$ to $t = 70$ and the attack on Agent 3 is carried out from $t = 60$ to $t = 100$. With the resilient control strategy in place, the agents still achieve their formation objective. The green lines are correct state values generated from the resilient control algorithm that the agents use to still achieve formation. The red lines indicate agent position information received by each agent from its designated neighbor impacted by the DOS attack.

Example 3. 6-Agent System with one agent under attack
6 agents with arbitrary initial positions form a hexagon as shown in Fig. 7. The intermediate behavior of the robots as they transition into a hexagon is illustrated, each vertex represents the location of agents at a specific time. As the formation algorithm is executed, agents keep adjusting their positions until they reach desired formation. Throughout this section, the blue color polygons indicate that the formation has been achieved. Likewise, the red color polygons indicate unsuccessful formation observed when an attack is implemented and during system transient state.

With the 6 agents in Fig. 7 at steady state, a DOS attack is carried out on one of the agents so that it can not receive

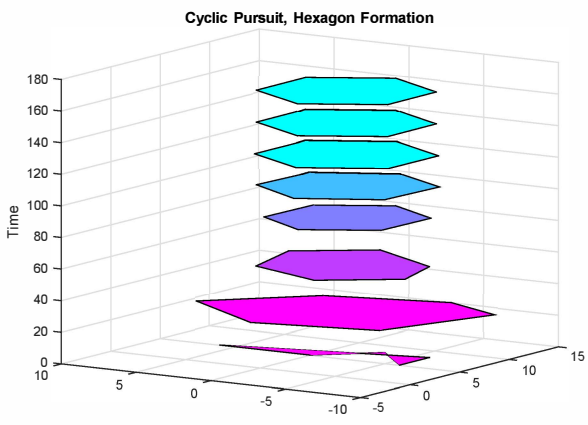


Fig. 7: 3D Hexagon Formation with cyclic pursuit

any information from its designated neighbor. Figure 8 is a corresponding 3D plot of the transient behavior of the agents in formation while under attack. The robot formation gradually gets distorted. The mark $(*)$ denotes Agent 1 that is under attack.

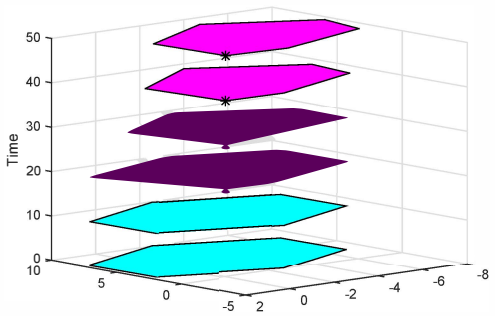


Fig. 8: 3D illustration of robot transient behavior during attack

The setup in Fig. 8 subject to the DOS attack is implemented but this time with our resilient control strategy in place. As shown in Fig. 9 the agents achieve their formation objective. The attack is carried out on agent 1 while the rest of the agents are in steady state.

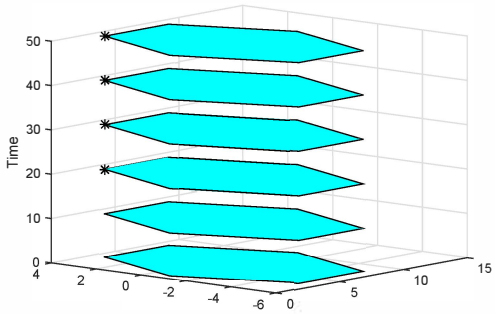


Fig. 9: 3D illustration of robot transient behavior with resilient control

V. Conclusion

In this paper, we proposed a model-based resilient control algorithm that enables a group of agents achieve and maintain formation while under attack. The proposed strategy does not require a highly accurate mathematical model that is often difficult to obtain. Our algorithm makes up for such inaccuracies by using both true system states measured and the states calculated from the mathematical model. The algorithm is demonstrated in a formation control problem. Using a testbed of 6 Pioneer 3DX robots, We have successfully demonstrated that agents achieve their cooperative objective despite the presence of a deliberate intrusion attack. Since the focus of this work was to develop and implement a resilient control algorithm, we limited the attack to a basic DOS attack which is easily detectable in our platform. Individual robot dynamics are also not included in the system model because they are not necessary as our objective is to maintain formation in steady state. For formation problems like leader follower in which steady state is not constant, robot dynamics must be included. Some preliminary results are reported in [24]. In our future work, the impact of other attacks such as covert attacks, false data injection attacks, stealth attacks and other deception attacks on multi-agent systems will be considered in order to extend our resilient control algorithm.

References

[1] David A. Powner GA0, *Critical Infrastructure Protection*, Department of Homeland Security Faces Challenges in Fulfilling Cyber-security Responsibilities. Government Report GAO-06 − 1087T, September 2006.

[2] Y. L. Huang, A. A. Cardenas, S. Amin, Z. S. Lin, H. Y. Tsai, and S. Sastry, *Understanding the physical and economic consequences of attacks on control systems*, International Journal of Critical Infrastructure Protection, vol. 2, no. 3, pp. 7383, October 2009.

[3] M. Long, C. H. Wu, and J. Y. Hung,*Denial of service attacks on network-based control systems: impact and mitigation*, IEEE Trans. on Industrial Informatics, vol. 1, no. 2, pp. 8596, May 2005.

[4] D. Geer, *Security of critical control systems sparks concern*, Computer, vol. 39, no. 1, pp. 2023, January 2006.

[5] S. Amin, A. Cárdenas, and S. Sastry. *Safe and secure networked control systems under denial-of-service attacks.* Hybrid Systems: Computation and Control, pp. 31-45, Apr., 2009.

[6] S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen. *Stealthy deception attacks on water SCADA systems.* Hybrid Systems: Computation and Control, pp. 161-170, Stockholm, Sweden, Apr. 2010.

[7] A. Cárdenas, S. Amin, B. Sinopoli, A. Giani, A. A. Perrig, and S. S. Sastry. *Challenges for securing cyber physical systems.* In Workshop on Future Directions in Cyber-physical Systems Security, Newark, NJ, USA, July 2009.

[8] A. Cárdenas, S. Amin, and S. S. Sastry. *Research challenges for the security of control systems.* In Proceedings of the 3rd Conference on Hot Topics in Security, pages 6:1-6:6, Berkeley, CA, USA, 2008.

[9] R. Metke and R. L. Ekl. *Security technology for smart grid networks.* IEEE Transactions on Smart Grid, 1(1): 99-107, 2010.

[10] J. Slay and M. Miller. *Lessons learned from the Maroochy water breach.* Critical Infrastructure Protection, 253: 73-82, 2007.

[11] S. Sridhar, A. Hahn, and M. Govindarasu. *Cyber-physical system security for the electric power grid.* Proceedings of the IEEE, 99 (1): 1-15, 2012.

[12] Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. Sastry. *Cyber security analysis of state estimators in electric power systems.* IEEE Conference on Decision and Control, pp. 5991-5998, Atlanta, GA, USA, Dec. 2010.

[13] Zhu, Minghui, and Sonia Martínez, *Attack-resilient distributed formation control via online adaptation.* Proceedings of the IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), 2011.

[14] Bhattacharya, Sourabh, and Tamer Basar, *Game-theoretic analysis of an aerial jamming attack on a UAV communication network.* Proceedings of the American Control Conference, pp. 818-823, 2010.

[15] Zhu, Minghui, and Sonia Martínez, *On the performance analysis of resilient networked control systems under replay attacks.* IEEE Transactions on Automatic Control, 59 (3): 804-808, 2014.

[16] De La Torre, Gerardo, Tansel Yucelen, and John Daniel Peterson. *Resilient networked multiagent systems: A distributed adaptive control approachy.* Proceedings of the 2014 IEEE 53rd Conference on Decision and Control, pp. 5367-5372, 2014.

[17] Zeng, W. and Chow, M.Y., 2014. *Resilient distributed control in the presence of misbehaving agents in networked control systems.* Cybernetics, IEEE Transactions on, 44(11), pp.2038-2049.

[18] Tanner, Herbert G., George J. Pappas, and Vijay Kumar. *Leader-to-formation stability.* IEEE Transactions on Robotics and Automation, 20 (3): 443-455, 2004.

[19] Balch, Tucker, and Ronald C. Arkin. *Behavior-based formation control for multi-robot teams.* IEEE Transactions on Robotics and Automation, 2 (6): 926-939 (1998).

[20] Lewis, M. Anthony, and Kar-Han Tan. *High precision formation control of mobile robots using virtual structures.* Autonomous Robots, 4: 387-403, 1997.

[21] A. M. Bruckstein, N. Cohen, and A. Efrat, *Ants, crickets and frogs in cyclic pursuit*, Center Intell. Syst., Technion-Israel Inst. Technol., Haifa, Israel, Tech. Rep. 9105, 1991.

[22] Lin, Zhiyun, Mireille Broucke, and Bruce Francis. *Local control strategies for groups of mobile autonomous agents.* IEEE Transactions on Automatic Control, 49 (4): 622-629, 2004.

[23] M. Quigley, K. Conley, B. Gerkey, J. Faust, T. B. Foote, J. Leibs, R. Wheeler, and A. Y. Ng, *ROS: an open-source Robot Operating System*, in International Conference on Robotics and Automation, ser. Open-Source Software workshop, 2009.

[24] Esther M. Amullen, Sachin Shetty, and Lee H. Keel *Secured Formation Control for Multi-agent Systems Under DoS Attacks* Technologies for Homeland Security (HST), 2013 IEEE International Symposium on, Waltham, MA, 2016, In press.