# Secured formation control for multi-agent systems under DoS attacks

**Conference Paper** · May 2016

DOI: 10.1109/THS.2016.7568947

CITATIONS
7

READS
50

**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

# Secured Formation Control for Multi-agent Systems Under DoS 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

***Abstract*—This paper proposes a secured formation control strategy that ensures acceptable operation of a multi-agent system in the presence of Denial of Service (DOS) attacks. We consider a team of autonomous agents whose mission is to cooperatively achieve and maintain formation by cyclic pursuit where each agent depends only on information from a single neighbor for mission completion. Agents communicate through a wireless interface that is susceptible to adversarial attacks. The attacker can target any number of communication links with the aim of corrupting information transmitted between agents disrupting their collective mission. The proposed secured formation control strategy is based on continuous on-line system identification. An Identified model of the multi-agent system is locally implemented alongside the actual system for each agent enabling agents retrieve their desired dynamic behavior in the presence of a DOS attack. The proposed technique is demonstrated through a laboratory experiment with a team of 5 pioneer 3DX robots.**

## I. Introduction

The range of applications for formation control in multi-vehicle systems employing robots, unmanned aerial vehicles or unmanned underwater vehicles is rapidly growing in both military and civilian applications. In military missions, a group of autonomous agents are required to keep in a specified formation for area coverage and reconnaissance. In small satellite clustering, formation control helps to reduce fuel consumption for propulsion and expand satellite sensing capabilities. In automated highway systems, the throughput of the transportation network can be greatly increased if vehicles can form platoons at a desired velocity while keeping a specified distance from each other. Other applications of formation control include security patrols, search and rescue in hazardous environments.

Formation control in multi-agent systems heavily relies upon accurate information exchange between agents. The tight integration of systems physical infrastructure with computational and communication infrastructure makes multi-agent systems susceptible to malicious attacks targeting both physical and communication infrastructure. [1] Kasperksy discovered a computer worm Stuxnet that targeted network programmable logic controllers. In [2], [3], [4], [5], [6] denial of service attacks, false data injection attacks, replay attacks and covert attacks respectively that affect traditional computational systems also affect the underlying networked control systems. Security for computational systems aims at protecting data confidentiality, preserving data accuracy and ensuring data availability for authorized users. For control systems however, in addition to confidentiality accuracy and availability, delays and re-transmissions whose impact on computational systems maybe negligible can be detrimental to control systems performance. For this reason, attacks on any communication link between agents can distort the entire formation and/or prevent agents from achieving their desired objective.

With a recent increase in research directed towards security of networked control systems, several secure control strategies have been proposed. In [7] for example, a linear system whose actuators and sensors are under attack by a malicious adversary is studied. The authors show that the control system can be made more resilient to sensor attacks by designing an appropriate state feedback gain. In [8], an attack resilient horizon-control law for a single loop remotely-controlled system under replay attacks is considered. In the strategy proposed, at each instant in time, the plant stores a control sequence computed during normal system operation which it then employs in response to replay attacks, the authors also characterize system stability and performance degradation under the receding horizon control law. Along the same line of research [9] considers resilient formation control for a networked multi-agent system comprising misbehaving agents affected by both exogenous and endogenous disturbances. To achieve secure control, the authors propose a distributed adaptive approach employing a local observer that estimates the state of an agent under normal system operation and uses this information to ensure resilient control in the presence of misbehaving agents. In [10], Zeng et. al. study a consensus problem for a multi-agent system with misbehaving agents proposing a reputation-based resilient distributed control algorithm. The algorithm embeds a resilience mechanism into the control process enabling each agent to detect and isolate misbehaving agents. Finally, [11] considers a UAV formation problem with an aerial jammer targeting the communication channel of the team. The attack

*The work of Sachin Shetty was supported in part by the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E) under agreement number FAB750-15-2-0120.

* The work of L.H. Keel was supported in part by DoD Grant W911NF-08-0514.

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.

Departing from the notable contributions in the literature, we present a model-based secured formation control strategy that ensures acceptable operation of a multi-agent system in the presence of DOS attacks on any number of communication links targeting information exchange between agents. To achieve secured control we employ continuous on-line system identification for each agent. The identified system is locally implemented alongside the actual system enabling agents retrieve their desired dynamic behavior in the presence of a DOS attack. To test the proposed control strategy, an experimental platform including pioneer 3DX robots and a camera-based 3D indoor localization system are used. We demonstrate that our proposed model-based control strategy enables the team of agents successfully maintain a desired formation despite DOS attacks on one or more communication links between agents.

## II. Control Objective

Formation control is an important problem in distributed control systems and has been under consideration by the research community for decades. The general objective of formation control is for a group of autonomous agents (wheeled robots, aerial vehicles and underwater vehicles) to achieve a specific formation and/or move while maintaining the formation. (see [12], [13] and references therein). Consider a communication graph $\mathbb{G}$ with $n$ distributed nodes [16]. Let the nodes represent agents with identical dynamics. For agent $i$,

$$\dot{x}_i(t) = Ax_i(t) + Bu_i(t), \quad i = 1, 2, \ldots, n \tag{1}$$

$x_i(t) \in \mathbb{R}^n$ is the state of agent $i$ and $u_i(t) \in \mathbb{R}^m$ is its control input. The agents follow consensus by cyclic pursuit such that the control input $u_i(t)$ becomes

$$u_i(t) = K\left(a_{i,i+1}\left(x_{i+1}(t) - x_i(t)\right)\right), \quad i = 1, 2, \ldots, n-1 \tag{2}$$

and for agent $n$

$$u_n(t) = K\left(a_{n,1}\left(x_1(t) - x_n(t)\right)\right) \tag{3}$$

where $K \in \mathbb{R}^{mxn}$ is the feedback gain matrix and is identical for all agents, $a_{i,i+1}$ is the graph edge weight between agent $i$ and agent $i+1$ and $a_{n,1}$ is the graph edge weight between agent $n$ and agent 1. With control input (2), the closed loop dynamics for (1) become

$$\begin{aligned}\dot{x}_i(t) &= Ax_i(t) + Bu_i(t) \\ &= Ax_i(t) + BKa_{i,i+1}\left(x_{i+1}(t) - x_i(t)\right), \quad i = 1, 2, \ldots, n-1\end{aligned} \tag{4}$$

and the closed loop dynamics for agent $n$ become

$$\begin{aligned}\dot{x}_n(t) &= Ax_n(t) + Bu_n(t) \\ &= Ax_n(t) + BKa_{n,1}\left(x_1(t) - x_n(t)\right).\end{aligned} \tag{5}$$

For all $n$ agents, global closed-loop graph dynamics can be written using the Kronecker product $\otimes$.

$$\dot{\mathbf{x}}(t) = \underbrace{\left[(I_n \otimes A) - L \otimes BK\right]}_{A_c}\mathbf{x}(t), \tag{6}$$

where the global state $\mathbf{x}(t) = [x_1^T(t), x_2^T(t), \ldots, x_n^T(t)]^T$ and $L$ is graph Laplacian matrix. The stability of $A_c$ depends on the local closed-loop system matrix $A - BK$ and the graph Laplacian $L$[16].

All the agents in (6) will converge to a common value, the consensus point. Let agent $i$ pursues a displacement $c_i$ relative to agent $i+1$,

$$u_i(t) = K\left(a_{i,i+1}\left(x_{i+1}(t) - x_i(t) - c_i\right)\right) \tag{7}$$

for $i = 1, 2, \ldots, n-1$ and

$$u_n(t) = K\left(a_{n,1}\left(x_1(t) - x_n(t) - c_n\right)\right). \tag{8}$$

for agent $n$. Formations with specific patterns and geometric shapes can be attained from the following system.

$$\dot{\mathbf{x}}(t) = [(I_n \otimes A) - L \otimes BK]\mathbf{x}(t) + \mathbf{c} \tag{9}$$

where $\mathbf{c} = [c_1^T, c_2^T, \ldots, c_n^T]^T$ is a vector describing desired relative positions for all agents.

## III. Proposed Secured Formation Control Strategy

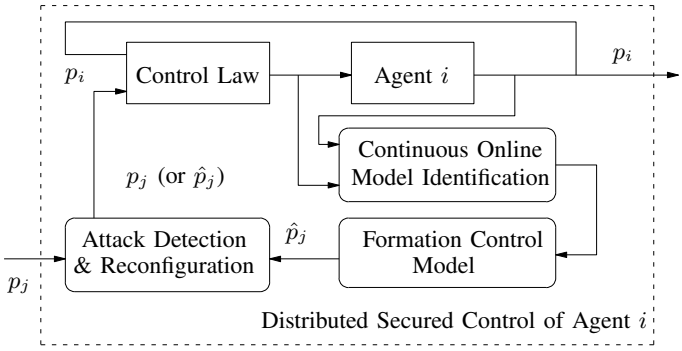



Fig. 1: Secured Control Strategy

Fig. 1 depicts the Proposed Secured Formation Control Strategy. Note that $p_i$ and $p_j$ are position information for agent $i$ and agent $j$, respectively, and $\hat{p}_i$ is the estimated position information at any given time. It employs continuous on-line system identification for a connected agent during the course of its mission. Under normal operation agents have an identical model and thus self-identification of the model for each agent is carried out. The amount of input/output data used for system identification depends on the pre-defined order of the model. Although we identify a linear time-invariant model, this continuous on-line system identification ensures that the identified model is reliable for a reasonable period of time when control must rely on the identified model.

When an attack is detected, agents locally determine their control action based on state values provided by the identified system discarding values coming through the network. To illustrate this strategy we consider the formation control problem for a multi-agent system

$$\dot{\mathbf{z}}_s(t) = A_c^s \mathbf{z}_s(t) + Bu(t) \tag{10}$$

and the identified model representing (10)

$$\dot{\mathbf{z}}_m(t) = A_c^m \mathbf{z}_m(t) + Bu(t) \tag{11}$$

where $A_c^s$ and $A_c^m$ are the state matrix for the actual multi-agent system including agent dynamics and the multi-agent system with an identified model of an agent, respectively, $B$ is the input matrix, $u(t)$ is the control input for formation, $\mathbf{z}_s(t)$ is the state vector *measured* from the actual system, and $\mathbf{z}_m(t)$ is the state vector *calculated* from the system with an identified model.

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

$$\|z_s(t + \Delta t) - z_m(t + \Delta t)\| < \epsilon \tag{12}$$

*with a small value of $\Delta t$ for sufficiently small $\epsilon$.*

The assumption will hold and be practical when an identified model is reasonably accurate. However, the assumption may not hold as $\Delta t$ increases. Consequently, we make the following proposition.

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

$$z_s(t + \Delta t) = f\left(A_c^s, z_s(t)\right) \tag{13}$$
$$z_m(t + \Delta t) = f\left(A_c^m, z_m(t)\right). \tag{14}$$

*Then*

$$\|z_s(t) - \overline{z}_m(t)\| < \epsilon \tag{15}$$

*for each and every $t$ where*

$$\overline{z}_m(t + \Delta t) = f\left(A_c^m, z_s(t)\right) \tag{16}$$

*Proof.* Consider

$$z_s(t + \Delta t) = A_c^s z_s(t)\Delta t + z_s(t) \tag{17}$$
$$z_m(t + \Delta t) = A_c^m z_m(t)\Delta t + z_m(t). \tag{18}$$

Let

$$\overline{z}_m(t + \Delta t) = A_c^m z_s(t)\Delta t + z_s(t). \tag{19}$$

From Assumption III.1, we have

$$\begin{aligned}\|z_s(t + \Delta t) - \overline{z}_m(t + \Delta t)\| &= \|\left(A_c^s - A_c^m\right) z_s(t)\Delta t\| \\ &< \epsilon \end{aligned} \tag{20}$$

for all $t$ □

The proposed strategy is summarized in Algorithm 1

**Algorithm 1** Secured Formation Control

**Require:** Model Identification $M_0$ with input/output data for $\bar{T} = [0, t_0]$.
Initialize state of the identified model $M_0$, $z_m(t_0) = z_s(t_0)$
**Ensure:** Final actual system state $z_s^*$ to accomplish the formation
**procedure** SECURED FORMATION CONTROL
**for** Each time step $t \geq t_0$ **do**
**if** No attacks present **then**
Model Identification $M_t$
$z_m(t) \leftarrow z_s(t)$
**else** Attacks present
$z_s(t) \leftarrow z_m(t)$
**end if**
repeat for $t = t + \Delta t$
**end for**
**end procedure**

## IV. EXPERIMENTAL TESTBED

To test control strategies for mutli-agent systems theoretically and practically, we developed an indoor experimental platform that facilitates design, testing and implementation of various corporative control and security strategies for networked control systems.

(a) Pioneer 3-DX robot

(b) Optitrack Prime 17W Camera

Fig. 2: Testbed Hardware

The experimental platform comprises ten 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 and other agents [14]. To obtain real time position and orientation for each of the agents, we employ an overhead indoor vision-based system that comprises twenty one optitrack prime 17w cameras shown in Fig. 2b mounted close to the ceiling. The prime 17w camera tracks markers attached to objects up to 50 inches away from the camera. It tracks markers down to sub-millimeter movements with high accuracy. The position of the markers is used to determine the position of the object they are attached to.

### A. Testbed Software

The on-board computers for the pioneer 3-DX robots run a Linux-based operating system with the Robot Operating

System (ROS) installed [15]. ROS is a Linux based framework that provides low-level abstraction for robot hardware. Each robot is equipped various ROS packages that facilitate inter-agent communication and distributed control. To control and interact with the over-head indoor vision-based system comprising optitrack prime 17w cameras, an optical motion capture software called motive is used. Additional software used includes MATLAB and SIMULINK. Two APIs MOCAP OPTITRACK and the NATURAL POINT MATLAB API are employed to enable interaction between ROS and MOTIVE then MOTIVE and MATLAB repectively. Fig. 3 is a basic illustration of the testbed.

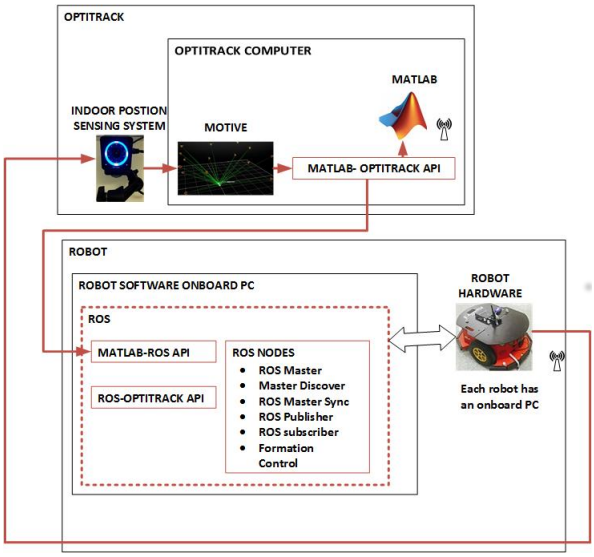



Fig. 3: Experimentation Testbed

## V. Secured Formation Control Experiment

To demonstrate the effectiveness of the proposed control strategy, a laboratory experiment is designed using the testbed discussed in Section V. Five of the robotic agents are used along with the optitrack motion capture system. The experiment is setup as illustrated in Fig. 4.

The MOCAP OPTITRACK and NATURAL POINT MATLAB APIs recieve data from MOTIVE and associate it which each agent. They then extract the meaningful position data and transmit it to ROS or MATLAB.ROS nodes are created for each agent to facilitate inter agent communicatio. Fig. 4 illustrates the interactions implemented for agent 1. The same interaction is implemented for each of the 5 agents. In cyclic pursuit formation control, agent 1 communicates its position to agent 5 which in turn communicates to agent 4 and so forth. Agent 2 finally communicates to agent 1 as in Fig. 5. Agents use the information they receive from their respective neighbors to determine their control action in a traditional cyclic pursuit implementation. While agents are carrying out their formation objective, a jamming DOS attack is carried out on the system using a broadband jammer device that consumes the communication channel with Gaussian white noise generated at very high amplitude. The jamming scenario employed targets specific communication links by matching the transmission frequencies of these links and relentlessly transmitting noise signals until the link is completely unavailable for receiving or transmitting. Fig. 6 illustrates the jamming DOS attack implemented.

## VI. Experimental Results

The agents start at arbitrary initial positions as shown in Fig. 7 and achieve formation as in Fig. 8. At steady state, the 5-agents form a pentagon under normal operating conditions with no attack implemented. Fig. 9 shows agent intermediate behavior as they transition into a pentagon. Each vertex represents the location of an agent at a specific time; the blue colored polygons indicate that the formation has been achieved while, the red colored polygons indicate unsuccessful formation observed when an attack is implemented and during system transient state.

With all 5 agents in steady state as shown in Fig. 9, a DOS attack is carried out against Agent 1. Fig. 10 shows the impact of the DOS attack on agents' positions and Fig. 15 shows the communication link of the impacted Agent. Since the agents pursue each other's relative positions communicated, a DOS attack on a single communication link affects all agent positions. The DOS attack is carried out starting at $t = 10$ to $t = 100$. For a DOS attack carried out during transient state, the agents do not achieve formation as illustrated in Fig. 11

Online system identification carried out along side the actual system during normal system operation generates a system model that tracks actual system states as illustrated in Fig. 12 with minimal error.

For the two attack scenarios described, steady state and transient state, we implement our proposed secured control strategy. We show that despite a denial of service attack affecting agent communication links, agents achieve their formation objective as illustrated in Fig 13 and Fig 14. Agents independently determine their control action based on values calculated from the identified model.

The steady state attack in Fig 13 is carried out from $t = 10$ The asterisk shows the agent under attack. Formation holds despite the agents being under attack.

To test the effectiveness of the secured control strategy during transient state, a DOS attack is carried out at $t = 10$. Agents are still able to achieve formation despite the attack.

Fig 15 shows the agent communicated positions and their actual positions provided by the identified model.

## VII. Conclusion

In this paper, we proposed a model-based secured formation control algorithm that enables a group of agents achieve and maintain formation while under a DOS attack. The proposed strategy employs continuous on-line system identification to create a system model whose states are identical to actual system states during normal operation to enable agents recover their states during attack. An experimental platform developed for testing various control and distributed algorithms is also

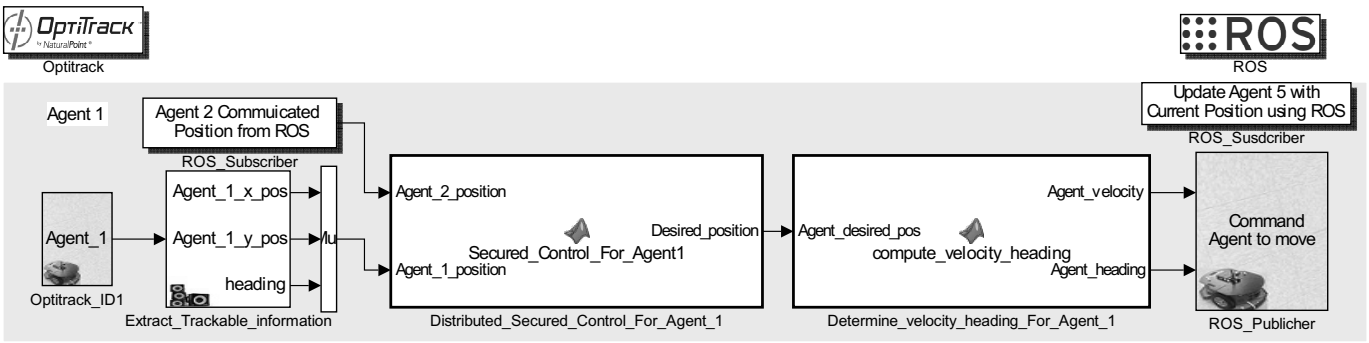



Fig. 4: Secured Formation Control Experiment Setup

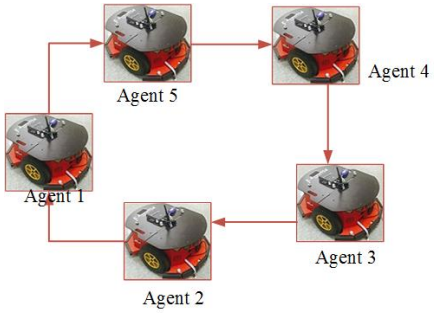



Fig. 5: Cyclic Pursuit Communication Topology

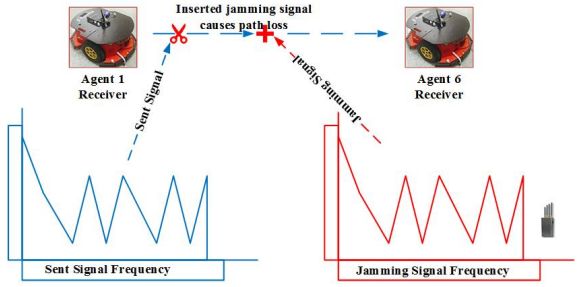
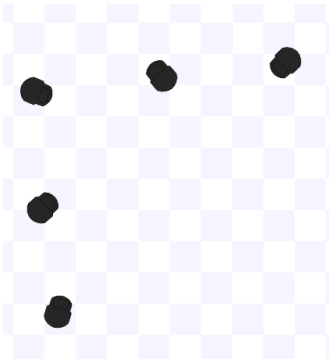



Fig. 6: Jamming DOS attack

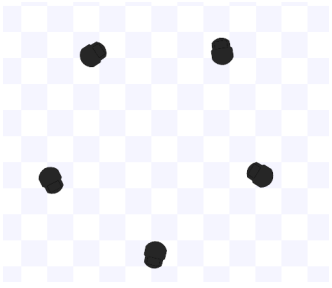
presented. Using this testbed, the effectiveness of our control strategy is demonstrated. In future work, the impact of other attacks such as covert attacks, false data injection attacks, stealth attacks and other deception attacks on multi-agent systems will be tested using the experimental platform. Our formation control strategy will be extended to various attacks and tested for a smart grid.



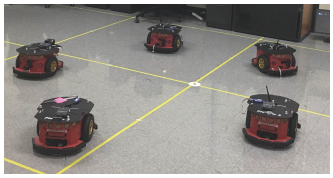
(a) Initial Positions for Simulated Agents

(b) Initial Positions for Actual Agents

Fig. 7: 5-agent system under normal operation showing agent initial position. In 7a, the agents are simulated using the Stage simulator. In 7b actual agent initial positions are illustrated



(a) Simulated Agents in Pentagon Formation



(b) Actual Agents in Pentagon Formation

Fig. 8: 5-agent system under normal operation showing agents in Formation. In 8a, the agents are simulated using the Stage simulator. In 8b actual agents at steady state are illustrated

## REFERENCES


[1] *"The Real Story Of Stuxnet"*. Spectrum.ieee.org. N.p., 2009. Web. 21 Mar. 2016.

[2] 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.

[3] 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.

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

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

[6] 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.

[7] Fawzi, Hamza, Paulo Tabuada, and Suhas Diggavi. *Security for control systems under sensor and actuator attacks.* Decision and Control (CDC), 2012 IEEE 51st Annual Conference on. IEEE, 2012.

[8] Zhu, Minghui, and Sonia Martínez, *On the performance analysis of resilient networked control systems under replay attacks.* IEEE

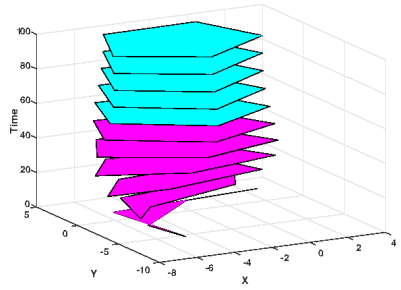



Fig. 9: 3D Pentagon Formation with cyclic pursuit

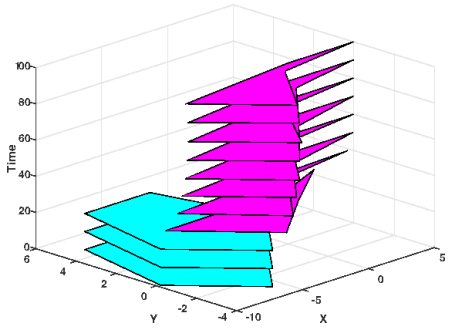



Fig. 10: DOS Jamming attack carried out against Agent 1 at steady state

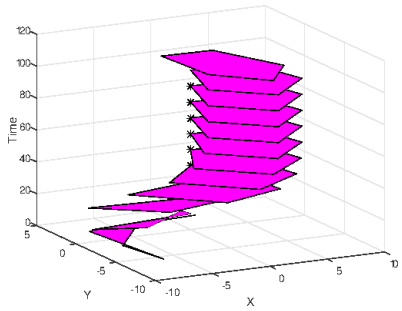



Fig. 11: DOS Jamming attack carried out against Agent 1 during transient state

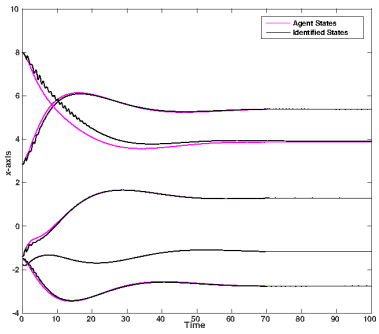



Fig. 12: System Identified States and actual system states converge.

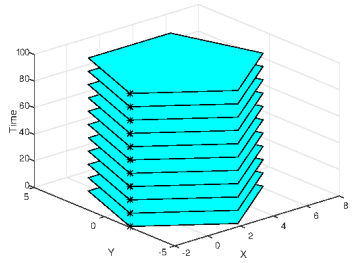



Fig. 13: DOS Jamming attack carried out against Agent 1 at steady state with secured formation control implemented

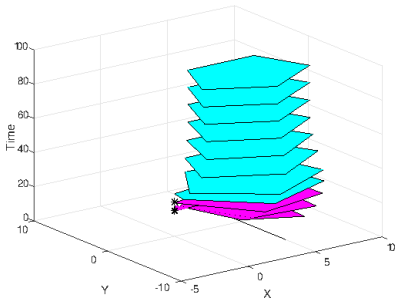
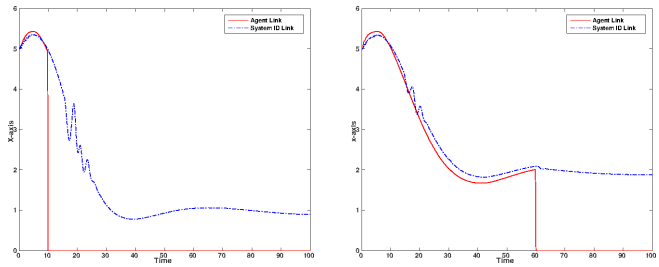



Fig. 14: DOS Jamming attack carried out against Agent 1 at steady state with secured formation control implemented




(a) Transient State Attack (b) Steady State Attack

Fig. 15: DOS Jamming attack with secured formation control implemented. The identified system provides a basis for the gent to determine a correct response.

Transactions on Automatic Control, 59 (3): 804-808, 2014

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] *Pioneer 3DX Operational Manual,* Mobile Robot Inc., Tech. Rep., 2007.

[15] Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., Wheeler, R. and Ng, A.Y. *ROS: an open-source Robot Operating System.* In ICRA workshop on open source software Vol. 3, No. 3.2, p. 5, 2009, May.

[16] Frank L. Lewis, Hongwei Zhang, Kristian Hengster-Movric, and Abhijit Das. *Cooperative Control of Multi-Agent Systems: Optimal and Adaptive Design Approaches.* Springer Publishing Company, Incorporated, 2014.