Proceedings of the ASME 2017 36th International Conference on Ocean, Offshore and Arctic Engineering
OMAE2017
June 25-30, 2017, Trondheim, Norway

OMAE2017-61771

CYBER SECURITY ISSUES IN NAVIGATION SYSTEMS OF MARINE VESSELS FROM A CONTROL PERSPECTIVE

Vahid Hassani
NTNU*/ SINTEF Ocean†
vahid.hassani@ntnu.no
Trondheim, Sør-Trønderlag, Norway

Naveena Crasta
LARSyS‡/Univ. Lisbon
ncrasta@isr.ist.utl.pt
Lisbon, Portugal

António M. Pascoal
LARSyS/Univ. Lisbon
antonio@isr.ist.utl.pt
Lisbon, Portugal

ABSTRACT

Autonomous marine vessels are the way forward to revolutionize maritime operations. However, the safety and success of autonomous missions depend critically on the availability of a reliable positioning system and time information generated using global positioning system (GPS) data. GPS data are further used for guidance, navigation, and control (GNC) of vehicles. At a mission planning level GPS data are commonly assumed to be reliable. From this perspective, this article aims to highlight the perils of maritime navigation attacks, showing the need for the enhancement of standards and security measures to intercept any serious threats to marine vessels emanating from cyber attacks and GPS spoofing. To this end, we consider a case where a cyber attacker blocks the real GPS signals and dupes the GPS antennas on board the marine vehicle with fake signals. Using the Nomoto model for the steering dynamics of a marine vessel and exploiting tools from linear control theory we show analytically, and verify using numerical simulations, that it is possible to influence the state variables of the marine vessel by manipulating the compromised GPS data.

1 INTRODUCTION

Marine vehicles are an essential instrument in a vast majority of scientific and commercial missions at sea that have tremendous economic impact across the globe. In order to execute complex missions safely, most surface vehicles rely heavily on a global navigation satellite system (GNSS) for their positioning purposes. Currently, the global positioning system (GPS), GLONASS, and Galileo are the only globally functional GNSSs. These positioning systems have proved to be instrumental in the successful operation of the guidance, navigation and control (GNC) units and dynamic-positioning (DP) systems of marine vehicles [1].

The grounding of Royal Majesty[1] [2] due to the loss of a GPS signal is a prime example of the crucial role that GNSS data play in navigation systems. Moreover, the recent experiments reported in [3] highlight the vulnerability of GPS signals, wherein the authors show how an inexpensive portable GPS jamming device [4] can be used to drift the position of a 65-meter custom-built super-yacht [5] without raising any alarms for the captain or the crew. Thus, the success of GNC and DP systems hinge upon the key assumption that the position signals from GNSSs are reliable and intact.

*Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway.

†SINTEF Ocean, formerly Known as Norwegian Marine Technology Research Institute (MARINTEK), is outcome of a merging process internally in the SINTEF Group from 1st January 2017.

‡Laboratory for Robotics and Engineering Systems (LARSyS), Institute for Systems and Robotics (ISR), Instituto Superior Técnico (IST), Univ. Lisboa, Portugal. The work of N. Crasta was supported in part by FCT [UID/EEA/50009/2013] and the European Commission under the H2020-ICT-2014 WiMUST Project (Grant Agreement No. 645141).

[1]In June 9, 1995 the Royal Majesty departed Bermuda for Boston Harbor. One hour after voyage, the GPS antenna cable broke away. Not receiving any GPS data the positioning system defaulted to dead reckoning, activating a one second alarm chirp sound which nobody heard. Soon the navigator, under the false assumption that GPS data were intact, set the autopilot in navigation mode. Almost 9 hours later when the actual ship position and (false) GPS positions were about 25 (km) apart, the passenger ship Royal Majesty grounded on Rose and Crown Shoal about 16 (km) east of Nantucket Island.

While over 90 percent of world trade takes place through waterways and oceans, autonomous ships are getting increasing attention as the means to revolutionize shipping industry by increasing efficiency and reducing both the cost and environmental impact of common transport operations. Developing secure data exchange channels are of paramount importance in autonomous shipping to prevent cyber attacks. In fact, with computer networks providing the communication media for data exchange in many applications, cyber security has emerged as a significant research topic for academia and the industry [6]. Nowadays, cyber threats are occurring more frequently and with greater sophistication than ever before [7]. The advent of cyber physical systems (CPS) [8] as an integration of widespread sensing, computation, communication, control and physical systems with many safety-critical applications such as the smart power grid, process control systems, and medical tele-operation, etc. has been another reason to carefully analyze the issue of cyber threats and cyber wars [9, 10, 11, 12, 13, 14, 15].

With this background, this paper aims at developing simple mechanisms to demonstrate the potential dangers of ignoring any machinery to verify the reliability of GPS data in GNC of marine vessels. To this end, we assume that the cyber attacker is able to jam the real GPS signals and dupe the GPS antennas on-board the marine vehicle with fake signals. Borrowing tools from control theory, we show how it is possible to manipulate the state of a system by applying fake signals instead of the real measurements in a feedback loop. To do so, we show the adopted plant model is controllable with respect to the newly introduced input (fake GPS signals). We consider three distinct scenarios:

i) In the first case, the marine vessel is completely dependent on the GPS for its orientation.
ii) In the second case, the vessel depends on the GPS and the on-board compass for yaw rate and heading measurements, respectively.
iii) In the third case, the vessel relies on an inertial navigation system (INS) with inputs from a gyro and GPS for estimating its heading, that will be used in control loop.

For each case, we show that the adopted plant model is controllable with respect to a fake signal introduced into the feedback loop by the cyber attacker. As a result, the attacker is able to drive the states of the system, i.e. heading and yaw rate, to any desired point. Furthermore, we simulate numerically our theoretical findings on how one can easily manipulate the heading of a marine vessel by using GPS spoofing.
At this stage we would like to highlight that the current article does not provide any solution to enhance the cyber security of marine vehicles. The goal of this article it to draw special attention to the existing imperfection in GNC systems. The work reported in this paper is only a starting point and is far from being completed. Elaborating other cyber security issues in marine systems and providing possible solutions for them warrants further research work.

The paper is organized as follows. We begin by briefly recalling the controllability of LTI systems in Section 2. In Section 3 we present a simple model of ship steering system using the Nomoto model and in Section 4 we analyze the controllability of the attacked system through a fake input, inserted by attacker, in each of the above mentioned three cases. In Section 5 we provide simulation results to validate our findings. Finally, the conclusions and future work are summarized in Section 6.

2 Controllability LTI Systems

In this section we review briefly the concept of controllability of linear dynamic systems which will be used in the following sections as our main tool to analyze the possibility of controlling the ship's heading by hijacking the GPS signal. Consider a MIMO linear time invariant (LTI) system described by

$$\sum\nolimits_{\text{LTI}} : \begin{cases} \dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{u}(t) \\ \mathbf{y}(t) = C\mathbf{x}(t) \end{cases} \tag{1}$$

with state $\mathbf{x}(t) \in \mathbb{R}^n$, input $\mathbf{u}(t) \in \mathbb{R}^m$, and output $\mathbf{y}(t) \in \mathbb{R}^q$, where $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$ and $C \in \mathbb{R}^{q\times n}$ are constant matrices. The solution to (1) at time $t \geq t_0$ for the initial condition $\mathbf{x}(t_0) = \mathbf{x}_0$ and the input function $\mathbf{u}(\cdot)$ is given by

$$\mathbf{x}(t) = e^{A(t-t_0)}\mathbf{x}_0 + \int_{t_0}^{t} e^{A(t-\tau)}B\mathbf{u}(\tau)\,\mathrm{d}\tau,\ t \geq t_0. \tag{2}$$

Controllability is one of the fundamental concepts in system theory. For the sake of completeness, we discuss briefly this concept which is well understood by now. We refer the reader to [16] for further details.

In this paper, we are mainly concerned with the controllability issue, that is, the problem of steering any initial state to any terminal state in a finite time. We recall the following definition of controllability.

Definition 2.1 (Controllability). *Given $T > 0$, the LTI system (1) is controllable, or simply the pair (A,B) is controllable on $[0,T]$, if for every pair of initial and terminal state $\mathbf{x}_0 \in \mathbb{R}^n$ and $\mathbf{x}_T \in \mathbb{R}^n$, there exists an input $\mathbf{u}\colon [0,T] \to \mathbb{R}^m$ such that $\mathbf{x}(T) = \mathbf{x}_T$.*

In what follows, in order to determine the controllability of a LTI system, we define the *controllability matrix* $\mathscr{C} \in \mathbb{R}^{n\times nm}$ by

$$\mathscr{C} = \begin{bmatrix} B & AB & A^2B & \cdots & A^{n-1}B \end{bmatrix}.$$

A necessary and sufficient condition for the controllability of a LTI system is that the controllability matrix be full rank, that is $\text{rank}(\mathscr{C}) = n$.

In the next section, we focus on the problem formulation and show analytically that state variables can be manipulated by hijacking the feedback measurement and inserting a new signal in the feedback loop.

3 Vessel Model

Motivated by [17], in this paper we consider the Nomoto model that describes the steering equation for marine vessels. For a large class of marine vessels, the Nomoto model provides a reasonable accurate description of the course-keeping behavior and even today, this simple and effective model is used in the literature of guidance and control systems.

The first order Nomoto model is given by

$$\ddot{\psi}(t) + \tau^{-1}\dot{\psi}(t) = \alpha\tau^{-1}\delta(t),\ t \geq 0, \tag{3}$$

where $\psi(t)$ and $\delta(t)$ denote the instantaneous yaw angle and rudder angle of the ship, respectively, and $\tau > 0$ and α are the effective time constant and gain constant of the model, respectively. In what follows we use $r(t) = \dot{\psi}(t)$ to denote the yaw rate of the ship.

To derive a state-space model, let $x_1 := \psi$ and $x_2 := r$. Then, a state-space realization for (3) is described by

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + \mathbf{b}u(t), \tag{4}$$

where $\mathbf{x} := \begin{bmatrix} x_1 & x_2 \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^2$, $u := \delta \in \mathbb{R}$,

$$A := \begin{bmatrix} 0 & 1 \\ 0 & -\tau^{-1} \end{bmatrix} \in \mathbb{R}^{2\times 2} \text{ and } \mathbf{b} := \alpha\tau^{-1}\begin{bmatrix} 0 \\ 1 \end{bmatrix} \in \mathbb{R}^2.$$

For this system the controllability matrix $\mathscr{C} \in \mathbb{R}^{2\times 2}$ is given by

$$\mathscr{C} = \begin{bmatrix} \mathbf{b} & A\mathbf{b} \end{bmatrix} = \alpha\tau^{-1}\begin{bmatrix} 0 & 1 \\ 1 & -\tau^{-1} \end{bmatrix}.$$

Clearly, $\mathscr{C}$ is full rank and consequently the system (4) is controllable.

4 Case studies

In what follows, we consider three distinct cases and for each of the cases we demonstrate how the state variables can be manipulated by simple operations of scaling and shifting the actual output function. For all of the following cases, we assume that the state vector is known. Thus, the output $\mathbf{y} \in \mathbb{R}^2$ is given by

$$\mathbf{y} = C\mathbf{x}$$

with $C = I_2$, where I_2 is the identity matrix of size two. Further, we also assume that there is no process or measurement noise.

In the usual output feedback, that is, $u = f(\mathbf{y})$, it is assumed that the signal $\mathbf{y}$ is reliable. Unfortunately, there are no mechanisms to ensure its reliability. However, in the absence of such mechanisms, the signal $\mathbf{y}$ can be counterfeited using some mechanisms, for instance a GPS jammer, that is, $\underline{\mathbf{y}} = \phi(\mathbf{y})$. Now the output feedback law, unaware of such deception, functions according to the new signal $\underline{\mathbf{y}}$, that is, $u = f(\underline{\mathbf{y}})$. In what follows, we assume that the autopilot is of a proportional derivative (PD) controller form (i.e. $u = P\psi + Dr$ where P and D are proportional and derivative gains, respectively).[2] It is worth mentioning that in the case of linear feedback, the existence of a stabilizing $\mathbf{k}$ is ensured by the controllability of the pair $(A, \mathbf{b})$.

4.1 Case 1

To begin with, we assume that the marine vessel is completely dependent on the GPS for its orientation. In this case the autopilot can be described as $u = \mathbf{k}_1^{\mathrm{T}}\mathbf{y}$, where $\mathbf{k}_1 = \begin{bmatrix} k_{11} & k_{12} \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^2$. Now, assume that a cyber attacker hijacks the GPS signal and overrides (fake) new heading and yaw measurements ($\underline{\psi}$ and $\underline{r}$ instead of ψ and r); see Figure 1. The autopilot, unaware of this deception, will compute the control action (rudder angle) according to $u = \mathbf{k}_1^{\mathrm{T}}\underline{\mathbf{y}}$. Let $\underline{\mathbf{y}} = \phi(\mathbf{y})$ be a simple shifting, i.e. $\phi(\mathbf{y}) = \mathbf{y} + \mu_1$, where $\mu_1 = \begin{bmatrix} \mu_{11} & \mu_{12} \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^2$ is a reference signal.

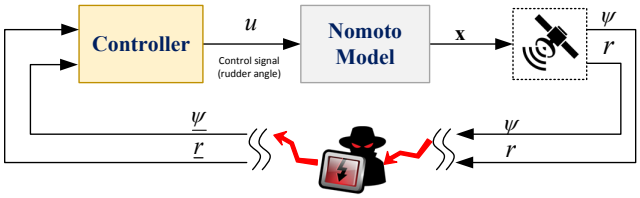

FIGURE 1. Case 1

Now that the GPS signals are compromised, the closed-loop system becomes

$$\dot{\mathbf{x}} = A\mathbf{x} + \mathbf{b}\mathbf{k}_1^{\mathrm{T}}(\mathbf{x} + \mu_1).$$

[2] For the sake of simplicity, in the presentation we use a vector representation for the autopilot controller in the form of $u = f(\mathbf{y}) = \mathbf{k}^{\mathrm{T}}\mathbf{y}$.

Simplifying the above equation further yields

$$\dot{\mathbf{x}} = F_1\mathbf{x} + B_1\mu_1, \tag{5}$$

where $F_1 := A + \mathbf{b}\mathbf{k}_1^{\mathrm{T}}$ and $B_1 := \mathbf{b}\mathbf{k}_1^{\mathrm{T}}$. It is easy to verify that the pair (F_1, B_1) is controllable, that is, the rank of the controllability matrix

$$\begin{bmatrix} B_1 & F_1B_1 \end{bmatrix} = \frac{\alpha}{\tau}\begin{bmatrix} 0 & 0 & k_{11} & k_{12} \\ k_{11} & k_{12} & \frac{k_{11}}{\tau}(\alpha k_{12}-1) & \frac{k_{12}}{\tau}(\alpha k_{12}-1) \end{bmatrix}$$

is two. In fact, by showing that system (5) is controllable, we have proved that there exist $\mu_1(\cdot)$ signal that the attacker can apply to drive the states of the system (i.e. heading and yaw rate) to any desired point. This concludes our discussion on the case 1 scenario.

4.2 Case 2

For this case, we consider that the vessel depends on the GPS and the on-board compass for yaw rate and heading measurements, respectively. See Figure 2 for the schematic representation of this scenario. Let us assume that the PD autopilot

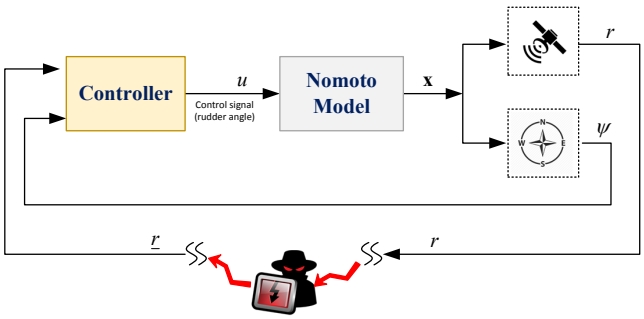

FIGURE 2. Case 2

is in the form of $u = \mathbf{k}_2^{\mathrm{T}}\mathbf{y}$ where $\mathbf{k}_2 = \begin{bmatrix} k_{21} & k_{22} \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^2$. As in subsection 4.1, assume that a cyber attacker hijacks the GPS signal and overrides a fake yaw rate instead of the real measured yaw rate (that is, $\underline{r}$ instead of r). This means that the new measurement to the controller will take the form $\underline{\mathbf{y}} = \phi(\mathbf{y}) = \mathbf{y} + \mu_2$, where $\mu_2 = \begin{bmatrix} 0 & \mu_{22} \end{bmatrix}^{\mathrm{T}} \in \mathbb{R}^2$ is a reference signal. With this new (fake) output measurement and the above-mentioned feedback control law, the closed-loop system becomes

$$\dot{\mathbf{x}} = A\mathbf{x} + \mathbf{b}\mathbf{k}_2^{\mathrm{T}}(\mathbf{x} + \mu_2).$$

Equivalently,

$$\dot{\mathbf{x}} = F_2\mathbf{x} + B_2\mu_2, \tag{6}$$

where $F_2 := A + \mathbf{b}\mathbf{k}_2^{\mathrm{T}}$ and $B_2 := \mathbf{b}\mathbf{k}_2^{\mathrm{T}}$. It can be easily verified that the pair (F_2, B_2) is controllable. This follows from the fact that the controllability matrix

$$\begin{bmatrix} B_2 & F_2B_2 \end{bmatrix} = \frac{\alpha}{\tau}\begin{bmatrix} 0 & 0 & k_{21} & k_{22} \\ k_{21} & k_{22} & \frac{k_{21}}{\tau}(\alpha k_{22}-1) & \frac{k_{22}}{\tau}(\alpha k_{22}-1) \end{bmatrix}$$

is full rank. The controllability of the hijacked system (6) (with respect to input μ_2) proves that there exist a $\mu_2(\cdot)$ signal that attacker can apply to drive the states of the system (i.e. heading and yaw rate) to any desired point.

4.3 Case 3

In the final case, the vessel relies on an inertial navigation system (INS) with input from a gyro and GPS for estimating the heading that will be used in the control loop. See Figure 3 for a graphical representation of this scenario. In this case the control

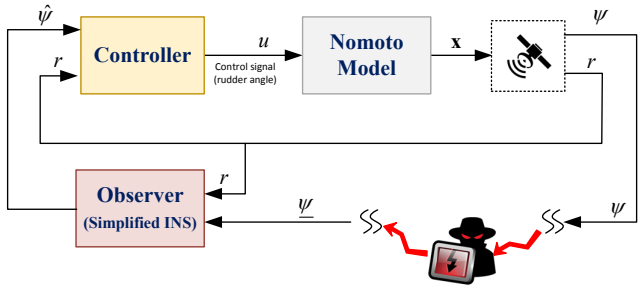

FIGURE 3. Case 3

signal from the autopilot is computed as $u = k_1\hat{\psi} + k_2 r$, where $\hat{\psi}$ is the estimate of the state $x_1 = \psi$. Since we have used a single degree of freedom model in the current paper, we simplify the INS equations to a kinematic estimator of the form

$$\dot{\hat{x}}_1 = x_2 + \tilde{k}_1(y_\psi - \hat{x}_1). \tag{7}$$

Assume that a cyber attacker hijacks the GPS signals and overrides the real measured heading y_ψ with a compromised signal $\underline{y_\psi}$. In this case, the augmented system becomes

$$\begin{bmatrix} \dot{\mathbf{x}} \\ \dot{\hat{x}}_1 \end{bmatrix} = \tilde{A}\begin{bmatrix} \mathbf{x} \\ \hat{x}_1 \end{bmatrix} + \tilde{\mathbf{b}}\underline{y_\psi}, \tag{8}$$

where

$$\tilde{A} := \begin{bmatrix} 0 & 1 & 0 \\ 0 & \tau^{-1}(\alpha k_2 - 1) & \alpha k_1 \tau^{-1} \\ 0 & 1 & -\tilde{k}_1 \end{bmatrix} \text{ and } \tilde{\mathbf{b}} := \begin{bmatrix} 0 \\ 0 \\ \tilde{k}_1 \end{bmatrix}.$$

Consider

$$\begin{bmatrix} \tilde{\mathbf{b}} & \tilde{A}\tilde{\mathbf{b}} & \tilde{A}^2\tilde{\mathbf{b}} \end{bmatrix} = \tilde{k}_1 \begin{bmatrix} 0 & 0 & \alpha k_1 \tau^{-1} \\ 0 & \alpha k_1 \tau^{-1} & \alpha k_1 \tau^{-1}\left(\tau^{-1}(\alpha k_2 - 1) - 1\right) \\ 1 & -\tilde{k}_1 & \alpha k_1 \tau^{-1} + (\tilde{k}_1)^2 \end{bmatrix}.$$

It can be easily shown that

$$\det\left(\begin{bmatrix} \tilde{\mathbf{b}} & \tilde{A}\tilde{\mathbf{b}} & \tilde{A}^2\tilde{\mathbf{b}} \end{bmatrix}\right) = -\alpha^2(\tilde{k}_1)^3(k_1)^2\tau^{-2} \neq 0.$$

Thus, the pair $(\tilde{A}, \tilde{\mathbf{b}})$ is controllable. This means that there exists an appropriate signal y_ψ which, if applied by the cyber attacker, can drive the state of the system to any desired point.

To summarize, the closed-loop system in all the three cases is controllable with respect to the external signal injected by the cyber attacker. Thus, the state variables heading ψ and heading rate r can be steered to any state using the external signal using either partial or full state information.

5 Numerical Simulations

Figure 4 presents numerical simulation of the case 3 where the marine vessel uses an INS for estimating the heading of the vessel (to be used in the PD autopilot.) In this Simulation, the vessel has 10 (deg) heading in the first 200 seconds. At this point the cyber attacker hijacks the GPS measured heading signal y_ψ and replaces it by $\underline{y_\psi}$. By modifying the signal $\underline{y_\psi}$ over the next 600 seconds, the heading of the vessel will change to -20 (deg).

6 Conclusions

In this paper, using linear control theory we demonstrated how the state of a marine vehicle can be manipulated in the absence of any preventive mechanism from cyber attacks. For three envisioned cases, we used the Nomoto model for the steering dynamics of a marine vessel and showed that with a simple linear output feedback the closed loop system is controllable with respect to the compromised output signal, thereby demonstrating that the state can be steered to any desired value.

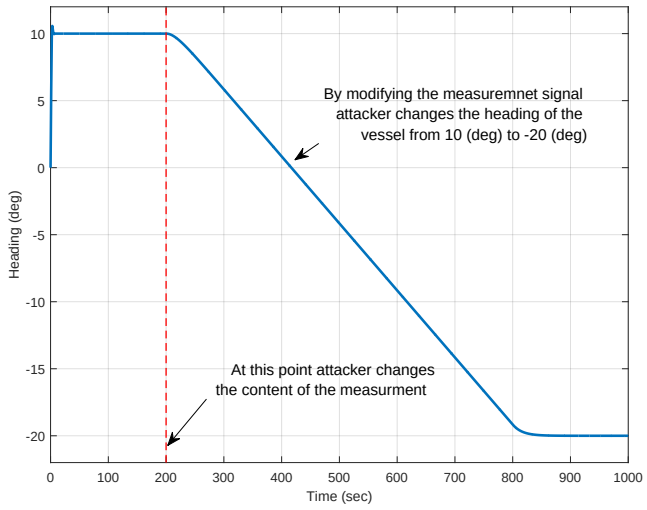

FIGURE 4. Numerical simulation for Case 3

REFERENCES

[1] Fossen, T. I., 2011. *Handbook of marine craft hydrodynamics and motion control*. John Wiley & Sons.

[2] Degani, A., 2003. "The grounding of the royal majesty". In *Taming HAL*. Springer, pp. 100–120.

[3] Bhatti, J., and Humphreys, T., 2015. "Hostile control of ships via false GPS signals: Demonstration and detection". *Submitted to Navigation, in review*. Available at `https://radionavlab.ae.utexas.edu/images/stories/files/papers/yacht.pdf` Accessed: 2017-01-09.

[4] Kerns, A. J., Shepard, D. P., Bhatti, J. A., and Humphreys, T. E., 2014. "Unmanned aircraft capture and control via GPS spoofing". *Journal of Field Robotics,* ***31***(4), pp. 617–636.

[5] White Rose Yacht (formerly White Rose Of Drachs). `http://www.superyachts.com/motor-yacht-4061/white-rose.htm`. Accessed: 2017-04-07.

[6] Adams, M. D., Hitefield, S. D., Hoy, B., Fowler, M. C., and Clancy, T. C., 2013. "Application of cybernetics and control theory for a new paradigm in cybersecurity". *Computing Research Repository (CoRR),* ***abs/1311.0257***.

[7] Farwell, J. P., and Rohozinski, R., 2011. "Stuxnet and the future of cyber war". *Survival,* ***53***(1), pp. 23–40.

[8] Lee, E. A., 2008. "Cyber physical systems: Design challenges". In 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), pp. 363–369.

[9] Mo, Y., and Sinopoli, B., 2009. "Secure control against replay attacks". In 47th IEEE Annual Allerton Conference on Communication, Control, and Computing, pp. 911–918.

[10] Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., and Sastry, S., 2009. "Challenges for securing cyber physical systems". In Workshop on future directions in cyber-

physical systems security, p. 5.
[11] Mo, Y., Chabukswar, R., and Sinopoli, B., 2014. "Detecting integrity attacks on SCADA systems". *IEEE Transactions on Control Systems Technology,* ***22***(4), pp. 1396–1407.
[12] Mo, Y., Hespanha, J. P., and Sinopoli, B., 2014. "Resilient detection in the presence of integrity attacks". *IEEE Transactions on Signal Processing,* ***62***(1), pp. 31–43.
[13] Mo, Y., and Sinopoli, B., 2015. "Secure estimation in the presence of integrity attacks". *IEEE Transactions on Automatic Control,* ***60***(4), pp. 1145–1151.
[14] Mo, Y., Weerakkody, S., and Sinopoli, B., 2015. "Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs". *IEEE Control Systems,* ***35***(1), pp. 93–109.
[15] Mo, Y., and Sinopoli, B., 2016. "On the performance degradation of cyber-physical systems under stealthy integrity attacks". *IEEE Transactions on Automatic Control,* ***61***(9), pp. 2618–2624.
[16] Hespanha, J. P., 2009. *Linear Systems Theory*. Princeton Press, New Jersey.
[17] Nomoto, K., Taguchi, T., Honda, K., and Hirano, S., 1957. "On the steering qualities of ships". *International Shipbuilding Progress,* ***4***(4), pp. 354–370.