IJRCS

International Journal of Robotics and Control Systems
Vol. 3, No. 1, 2023, pp. 19-31
ISSN 2775-2658
http://pubs2.ascee.org/index.php/ijrcs

ASCEE

Deep Learning-Based Attack Detector for Bilateral Teleoperation Systems

Yousif Ahmed Al-Wajih [a,1], Mutaz M. Hamdan [b], Turki Bin Mohaya [a], Magdi S. Mahmoud [a,2,*], Nezar M. Al-Yazidi [a]

[a] Control and Instrumentation Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
[b] Department of Mechanical Engineering, National University College of Technology, Amman 11592, Jordan
[1] alwajihyousif@gmail.com; [2] magdisadekmahmoud@gmail.com
[*] Corresponding Author

ARTICLE INFO

Article History
Received October 19, 2022
Revised November 24, 2022
Accepted December 01, 2022

Keywords
Bilateral teleoperation system;
Attack detection;
False data injection;
Deep learning

ABSTRACT

A teleoperation system is referred to as a plant that is controlled remotely, and it is often composed of a human operator, a local master manipulator, and a remote slave manipulator, all connected by a communication network. Bilateral teleoperation systems (BTOS) include transmissions in both the forward and backward directions between the master and slave. This paper discusses a class of (BTOS) focusing on the security of the system after modeling the master and slave robots mathematically. The false data injection attack is examined, where the attacker may inject false data into the states that are being exchanged between the master and slave robots. The vulnerability of BTOS, where the attack destabilizes the system, is presented. A deep learning-based detection technique is proposed to detect the presence of false data injection attacks. The deep learning model with convolution neural network structure is trained and tested with considering complex attacks where the attacker has full knowledge of the system and proficiency to emanate and control the target system. The proposed model achieves 96% validation accuracy, and the efficacy of the proposed deep learning detector is demonstrated and tested into the BTOS.

This is an open access article under the CC-BY-SA license.

1. Introduction

Bilateral teleoperations systems (BTOS) have widely spread in the world recently. The technology offers valuable features that assess humans in many areas. It simply has a set of actuators and motors that allows humans to robotically manipulate an environment through a master, slave, and communication link. These systems serve many purposes in areas such as in toxic environment [1], [2], [3]. In space and deep water scientific studies and sometimes it can be as handy as performing a remote surgery operation [4]. A BTOS system is shown in Fig. 1 to show the structure of the system. As shown in Fig. 1 the structure starts with the master robot. All input of the system gets translated in variable form during the human operator's interference with the master robot. Mainly, the input variables of the system are joint position q_m and velocity $\dot{q}_m$. The human operator's goal is to control the salve robot by the actions performed on the master-slave, which are the variables of joint position and velocity. Then, the variables of q_m and $\dot{q}_m$ are transmitted through a communication network that allows the master to send actions to the slave and for the slave to send feedback on the action.

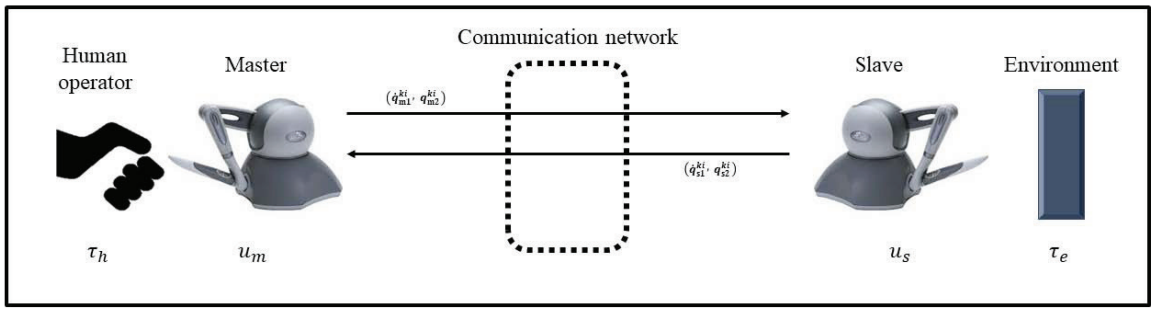

Fig. 1. Structure of the BTOS

As the research on this topic has progressed, In the bilateral teleoperation system, network medium is frequently employed as the communication channel especially the wireless communication network via the internet [5]. It is advantageous to have internet-based communication that provides more flexibility in the system, but also there are some disadvantages concerning the reliability of the data. Dealing with a robot's communication through the internet can pose disruption between the master and slave robots' data, which results in poor behavior of the system. Many research works have addressed these issues and experiments were conducted to solve them in the past. The results overcame the unreliability issues and established a better performing communication in BTOS as [6], [7], [8], [9], [10], [11] indicates. Currently, there are various issues that threaten the performance of BTOS that need to be studied such as cyber-attacks. They are extremely dangerous and can lead to major consequences.

Recently, more focus is brought on eliminating threats from cyber attacks as well as enhancing the safety and security of the cyber-physical system (CPS). CPSs are a crucial part of the system and their failure causes severe damage to the process and the capital. An example of CPS importance in BTOS, is when Stuxnet malware entered Iran's nuclear plant [12], causing the water system [13] and the power transmission [14] to fail. Preventing cyber-physical attacks cannot be performed using the traditional method of cryptography since it is not compatible. CPS requires its own system to be modeled because of the nature of its behavior and constraints. If a cyber attack happens, it will impact the physical system it is connected to. It also dangers people if the BTOS was implemented in a plant that contains nuclear reactors or toxic materials. For this reason, information system security is limited to operating in desktop and server applications and it cannot provide security for BTOS [15].

As mentioned earlier, the cyber-physical system has a different approach from the information system. They are two main parts to the system to implement a secure network. The first is to model and design the attack. Second, model and design the defense mechanism, so the system does not fail or behave abnormally. Many research in this area have been conducted to implement a secure network and communication regarding identifiability and detectability of attacks [16], [17], [18]. In [19], a survey on control design for the BTOS in nominal situations and in the presence of cyber-attacks has been conducted. This work concluded that the presented methods in the control of BTOS are to achieve the stability of a delayed bilateral teleoperation system in the presence of several kinds of cyber attacks. In reference [20], false data injection attacks in the communication channel are recognized using an offline identification method based on the least squares. In this study, in order to represent the network's packet dropouts and false data injection attacks, two Bernoulli distributed variables are introduced.

It is crucial that the desired performance of the physical process is achieved in CPS through the secure integration of computation, communication, and control. If they are not met by the CPS, the

physical system behaves unexpectedly. Allowing for failures and loss of control to the plant [21]. In [22], a survey on communication networks and the challenges related to controlling systems was highlighted with focusing on wireless communication. Especially, the CPS now has progressed along with the advanced technology that is present in recent times. It can be found in essential and complex processes all over the world. Examples of CPS being deployed in recent technologies involve smart cities, transportation systems, medical systems, and many other applications that are sensitive to failure [23]. However, various research methods have been conducted to overcome the issues of CPS and further improve its performance. CPS can perform three actions in the defense mechanism when an attack is present. They are Denial of Attack, Deception of Attack, and Replay of Attack [24].

Recent research focus on BTOS examines output feedback synchronization control of unsteady bilateral teleoperation system with synchronization error limitations, time-varying delay, actuator backlash-like hysteresis, and unknown control tendency [25]. In [26], the implementation of an intelligent system using deep learning for network control and monitoring was a focus of this work, with the end objective of improving the level of precision inside the network and its applications. In [27], authors proposed a methodology for developing a generalized machine learning-based model for detecting DDoS attacks where the generalized behavior of the developed model is justified by demonstrating a trade-off between high variance and high bias ML models. In this study, the authors claimed that they achieved an improvement of around 20% compared to the previously achieved metrics. Authors in [28] analyzed the performance of bilateral teleoperation systems under constant transmission delays and random denial-of-service (DoS) attacks, and they suggested a mode-dependent switching controller in order to reduce the impact of DoS attacks. In addition authors in [29] described a unique Hidden Markov Model-based method for continuous operator authentication in teleoperated robotic operations.

Most plants and industrial processes require safety in every aspect of the system. There should be no tolerance for faults as a variety of subsystems is coupled with other subsystems. The presence of wrongful data may carry unprecedented consequences to the process or even to humans. Therefore, safety in the process should be implemented to guarantee no attacks and faulty data occur in the process. CPS is responsible as mentioned earlier for the computation, communication, and control of physical systems. In every process, these three elements are what make the automated process function. If CPS was fragile, the physical system is vulnerable to cyber-physical attacks and doomed to fail. Some potential hazards can be caused in supervisory control as the attacks ought to happen in this area of control. Almost all systems have supervisory control embedded to allow control ability to the operators. Attacks in this area mean the attacker can input faulty data, shut down, or even trip the system. Such systems with supervisory control are water systems, power utilities, trains, pipelines for gas and oil, and many other important systems [30], [31], [32], [33], [34]. In this regard, a powerful tool like deep learning is required to tackle such challenges, since deep learning is a suitable technique to solve the complexity of BOTS and any attack scenario a class of deep learning called Convolutional Neural Networks (CNN) is proposed and studied in this article.

The main contribution of this work is proposing the Convolutional Neural Networks model to detect a false data injection attack on a class of teleoperation systems. Bilateral Teleoperation Systems involving two nonlinear revolute robotic manipulators joined via a communication channel are presented. On-content modification attacks are formalized and implemented on the BTOS system.

The remaining of the paper is structured as follows: In Section 2, the concerned BTOS system, and On Content Modification Attacks model are presented. In Section 3, the detection methodology and the proposed deep learning model are discussed, while the simulation and the numerical analysis are shown in Section 4. Finally, the conclusion is drawn in Section 5.

2. On Content Modification Attacks

2.1. The Concerned System

In this brief, the BTOS involves two non-linear revolute robotic manipulators joined via a communication channel. The block diagram is shown in Fig. 1. In this work external disturbances and friction. The mathematical model of this system is given as [35]. Where the system is consisting an n-link in both the master and slave robot.

$$\begin{aligned} M_m(q_m)\ddot{q_m} + C_m(q_m, \dot{q_m})\dot{q_m} + G_m(q_m) &= \tau_h + \tau_m \\ M_s(q_s)\ddot{q_s} + C_s(q_s, \dot{q_s})\dot{q_s} + G_s(q_s) &= \tau_s - \tau_e \end{aligned} \tag{1}$$

The subscripts m and s represent the master and the slave robot, respectively. To make things short we denote subscripts m, and s by i. So, q_i, $\dot{q_i}$, $\ddot{q_i} \in R^n$ are the position, velocity, and angular acceleration, respectively, $C_i(q_i)$, $\dot{q_i} \in R^{(n\times n)}$ is the centrifugal and Coriolis matrix, $M_i(q_i) \in R^{(n\times n)}$ is the inertia matrix, $G_i(q_i) \in R^{(n\times n)}$ is the gravitational torque, $\tau_i \in R^n$ is the control input, and τ_e, $\tau_h \in R^{(n\times n)}$ are torques exerted by the environment, human operator, respectively.

From the robotic manipulator's point of view, the system has the following two fundamental properties due to the Lagrangian dynamics structure [36]. P1: The inertia matrix $M_i(q_i)$ is symmetric positive definite with the following binderies:

$$\lambda_m I_n <= M_i(q_i) <= \lambda_M I_n \tag{2}$$

Both the λ_M, λ_m are the maximum and minimum positive eigenvalues of the inertia matrix $M_i(q_i)$ for the whole range of q_i. P2: For the matrix $\dot{M_i}(q_i) - 2C_i(q_i, q_i)$ is skew-symmetric matrix under a proper definition of $C_i(q_i, q_i)$. Three assumptions are made on the BTOS to simplify the theoretical analysis of the attack implemented in this work.

Assumption 1 *The network channel is stable and perfect, meaning the data losses and delay are not reflected in the theoretical design of the attack.*

Assumption 2 *Both the environment and the human operator are exhibited as passive systems.*

Assumption 3 *To simplify the mathematical system of the BOTS expressed in (1), the gravitational torques are pre rewarded such the following:*

$$\begin{aligned} \tau_m &= u_m + G_m(q_m) \\ \tau_s &= u_s + G_s(q_s) \end{aligned} \tag{3}$$

By substituting (3) in (1) the BTOS dynamics is compact to the following mathematical model:

$$\begin{aligned} M_m(q_m)\ddot{q_m} + C_m(q_m, \dot{q_m})\dot{q_m} &= \tau_h + u_m \\ M_s(q_s)\ddot{q_s} + C_s(q_s, q_s)\dot{q_s} &= u_s - \tau_e \end{aligned} \tag{4}$$

From the system structure and its mathematical model above. The data transferred between the master and slave robot are the position and velocity signals $(q_i^T, \dot{q_i}^T)$. In the normal operation stage where there is no attack, we can design a PD-like compensator for the BTOS system as [37] and [9]. This led to the following controller one for the master robot and the second one for the slave robot.

$$\begin{aligned} u_m &= -K_d(\dot{q_m} - \dot{\tilde{q}_s}) - K_p(q_m - \tilde{q}_s) - K_{dm}\dot{q_m} \\ u_s &= -K_d(\dot{q_s} - \dot{\tilde{q_m}}) - K_p(q_s - \tilde{q_m}) - K_{dm}\dot{q_s} \end{aligned} \tag{5}$$

where K_d, K_p, and K_{dm} are the tuned parameters of the PD-like controller. K_d, K_p, $K_{dm} \in R^{(n+)}$, Consequently, the resulting instructions hold.

The error in position is constrained $(e_q := q_m - q_s)$, and the error in velocity $(\dot{e_q} := \dot{q_m} - \dot{q_s})$, is asymptotically converges to zero. Meaning the limit of $\dot{e_q}$ goes to zero. $\lim(n \to \infty)\dot{e}_q = 0$. The states synchronized in case of free motion. $\lim_{n\to\infty} \dot{e}_q = \lim_{n\to\infty} e_q = 0$. when: $(\tau_e = \tau_h = 0)$ The contact of the environment force is transmitted back to the human operator accurately if $\ddot{q}_i = \dot{q}_i = 0$. Both Assumptions 1 and 2 are required so the PD-like control scheme can be considered for the attack design. However, Assumption 1 is used only in the theoretical design of the attack.

2.2. On Content Modification Attacks

The attachment conceded in this work is a false data injection. A formal description of the attacker reflected in this work is described with the following assumptions

Assumption 4 *The attacker has information on the controller gain, controller structure, and system dynamics structure.*

Assumption 5 *The attacker can interpret, manipulate, forward, and receive the data across the robots.*

From these, we can define the attacker in this work to be an external hacker with the two Assumptions 4 and 5. the attacker can launch a false data $(d \in R^P)$ and inject it into the target system this attack is named a false data injection attack. As a result, the original data $d \in R^P$ is modified to be:

$$d = d + \hat{d} \tag{6}$$

From this definition, we consider the BTOS with the mathematical model in (1) that is controlled by the PD-like controller described in (4). In this context, the attack is modifying the states across the two robots

$$\tilde{q} = q + \hat{q} = q + Kq \tag{7}$$

Where $\tilde{q} = (\tilde{\dot{q_m}}, \tilde{q_m}, \tilde{\dot{q}_s}, \tilde{q_s}), q = (\dot{q_m}, q_m, \dot{q}_s, q_{ss})$, and the gain K is a destabilizing false data injection attack (DFDIA) with respect to the storage function given in (8). Where this storage function can be considered a Lyapunov-like function for the system under concern.

$$\begin{aligned} V = {} & 1/2\dot{q_s}^T M_s \dot{q}_s + 1/2\dot{q_m}^T M_m \dot{q_m} \\ & + 1/2(q_s - q_m)^T K_p (q_s - q_m) \\ & - \int_0^t \dot{q_m}^T \tau_h dt + \beta_h + \int_0^t \dot{q_s}^T \tau_e dt + \beta_e \end{aligned} \tag{8}$$

In this context, the derivative of the storage function is given by

$$\begin{aligned} \dot{V} = {} & -\dot{q_s}^T K_{dm} \dot{q}_s - \dot{q}_m^T K_{dm} \dot{q}_m - \dot{q_s}^T (K_d(\dot{q}_s - \tilde{\dot{q_m}}) \\ & + K_p(q_s - \tilde{q_m})) - \dot{q_m}^T (K_d(\dot{q_m} - \tilde{\dot{q}_s}) \\ & + K_p(q_m - \tilde{q}_s)) + (\dot{q}_s - \dot{q_m})^T K_p (q_s - q_m) \end{aligned} \tag{9}$$

This attack is fully discussed with proof in [38]. The contribution in this work is done on attack detection using the DL techniques. The detection scheme is assumed to be placed with the encoding-decoding structure. The false data detection in this work can detect any type of this class of attack. We assume the detection is implemented in the discrete sequences.

$$\widetilde{q_s} = \gamma_s q_s + \alpha_s q_m, \widetilde{q_m} = \gamma_m q_m + \alpha_m q_s, \tag{10}$$

$$\widetilde{\dot{q}}_s = \widehat{\gamma}_s q_s + \widehat{\alpha}_s q_m + \gamma_s \dot{q}_m \widetilde{\dot{q}}_m = \widehat{\gamma}_m q_m + \widehat{\alpha}_m q_s + \gamma_m \dot{q}_s \tag{11}$$

$$\alpha_i(t) = \sum_{k=0}^{\infty} \alpha_0 e^{(-K_p/K_d)(t-kT))} U_k(t), \tag{12}$$

$$\widehat{\alpha}_i(t) = (-K_p/K_d)\alpha_i(t), \tag{13}$$

$$\gamma_i(t) = \sum_{k=0}^{\infty} ((\gamma_0 - 1)e^{(-K_p/K_d)(t-kT))} + 1)U_k(t), \tag{14}$$

$$\widehat{\gamma}_i(t) = (-K_p/K_d)(\gamma_i(t) - 1), \tag{15}$$

where

$$\gamma_0 < 0, \gamma_0 + \alpha_0 > 1 + K_d m/K_d \tag{16}$$

$$K_p \alpha_i(t) - K_p + K_d \widehat{\alpha}_i(t) = -K_p \tag{17}$$

$$K_d \alpha_i(t) - K_d - K_d m = K'_d(t) + K''_d(t) \tag{18}$$

$$U(t) = \begin{cases} 1 & t \geq 0 \\ 0 & t < 0 \end{cases} \tag{19}$$

$$U_k(t) = U(t - kT) - U(t - (k+1)T) \tag{20}$$

$$K_p \gamma_i(t) + K_d \widehat{\gamma}_i(t) = K_p, K_d \gamma_i(t) = -K'_d(t) \tag{21}$$

$$K'_d(t) = -K_d \sum_{k=0}^{\infty} ((\gamma_0 - 1)e^{(-K_p/K_d)(t-kT))} + 1)U_k(t) \tag{22}$$

$$K''_d(t) = \sum_{k=0}^{\infty} (K_d((\alpha_0 + \gamma_0 - 1)e^{(-K_p/K_d)(t-kT))} U_k(t) \tag{23}$$

3. Detection Methodology Using Deep Learning

The proposed deep learning model for false data detection is illustrated in this part. In this work, the target system is the BTOS system as explained above. The simple illustration of the system with the proposed deep learning model is shown in Fig. 2. The deep learning model is placed before the slave because of the reasons listed below. However, the deep learning model could be placed at the top of the communication network but in this case, we have to consider the communication network since the attacker may block the communication of the deep learning model. In this regard, the appropriate place is to attach the deep learning model to the slave to protect the slave from any attack. Furthermore, the slave is more important to defend since it reacts directly with the environment. the main goal of adding the deep learning model is to detect if there is any abnormality in the system or is a false data attack. The deep learning model will be discussed in detail in the coming section. The model utilizes the simulation data we crate from the system simulation as will be explained in the simulation section.

3.1. Detection Procedure

In this brief, the detection is executed in a discrete time. So, for each received data sequence $k_i = 1, 2, 3, \ldots$. First, the data $(\dot{q}^k_{m1}, q^k_{m2})$ sent to the target end. In our case, the data was sent from the master robot to the slave robot via the communication network. Then, the data will be received at the target end. When the data is received it has to pass through the proposed DL Model for detection. If the DL Model detects an attack it rejects the received data, then immediately the Deep Learning post-attack compensator starts controlling the system and puts the system in a save mode. If not, the DL Model can pass the received data and let the system work normally.

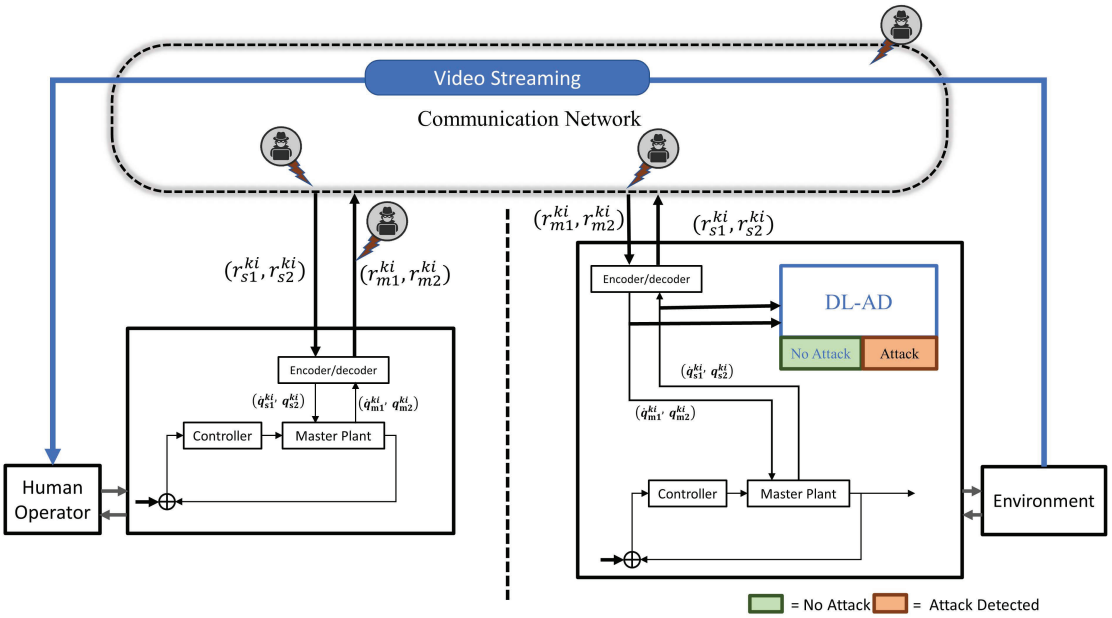

Fig. 2. The Block Diagram of the Proposed System

3.2. Deep Learning Attack Detection (DL-AD) Model

In this section, we cover the process of designing and implementing the DL Detection model. First, we illustrate the topology of the proposed model and it is hidden in deep layers. Then, an explanation of the process of collecting the required data to implement the model is emphasized. The training results and the model performance are discussed in Section VI.

Our proposed detection model is a Convolutional Neural Network (CNN) that consists of 7 fully-connected deep layers each followed by a batch normalization emphasized [39] except the output layer. Dropout layers are implemented in the design to prevent over-fitting [36]. The Rectified Linear Unit (ReLU) [40] is the used activation function except for the output layer. Fig. 3 is illustrating the proposed CNN model structure where the input of the model is given as

$$\tilde{q}(t)^T = [\tilde{q_m}(t), \tilde{q_s}(t), \tilde{\dot{q_m}}(t), \tilde{\dot{q_s}}(t)] \tag{24}$$

Algorithm 1 Deep Learning Detection Algorithm

for $k = 1, 2, 3, ..$ **do**
  On sending end:
  Send $(\dot{q}^k_{m1}, q^k_{m2})$
  On receiving end:
  Receive $(\dot{q}^k_{m1}, q^k_{m2})$
  Input $(\dot{q}^k_{m1}, q^k_{m2})$ to the DL Detector
  if (DL-AD = 1) **then**
    Reject the received data, and raise the attack alarm.
  else
    Use the received data $(\dot{q_{m1}}^k_i, q_m 2^k_i)$.
  end if
end for

The loss function is the BCEWithLogitsLoss which combines both the sigmoid activation function and the Binary Cross Entropy Loss function. The adaptive moment estimation (Adam) [41] optimizer is used as the optimization algorithm. The following model variables are considered hyperparameters: learning rate, number of hidden neurons, dropout probability, and batch size. We consider the inputs to the model to be $q(t)$ is defined in (24).

The data preparation stage included generating it by simulating the system performance as described by (3) under the two described On Content Modification Attacks (7)-(23). After that, the values of $\tilde{q}(t)$ were recorded for random step inputs in the range [1 10] and labeled with either no attack (0) or attack (1). Then, these data samples were arranged into 51102 patterns each having a dimension of (5×1) with 95% training data set and 5% testing data set.

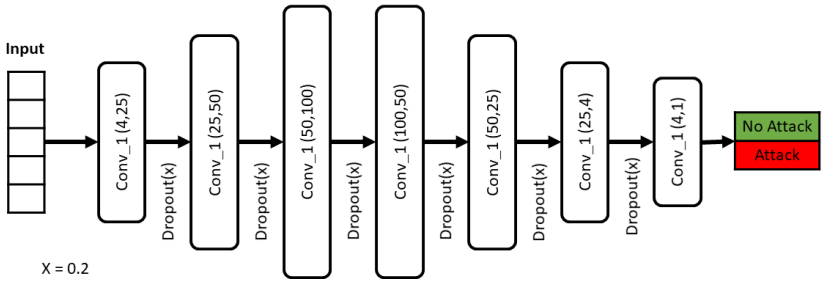

Fig. 3. Proposed CNN model structure

Remark 1 *The proposed CNN model plays a crucial role in both identifying dynamic systems and detecting faults in addition it gives a post-fault model of the system [42]. In this manner, the CNN model is proposed and tested in the BTOS in order to identify and isolate an attack in the system.*

Remark 2 *The target of this work is to detect the false data attack on the transmitted states through the communication links. The proposed model applied in this paper is used for detecting the attached system without using the attached states.*

4. Numerical Analysis and Simulation

In this section, we discuss the results and the performances of the proposed DL attack detection model as well as the DL post-attack compensator. The dynamics for the master and slave robot are obtained by substituting $M_i = ml^2, C_i = 0, G_i(q_i) = -mglsin(q_i)$ in textcolorRoyalBlue(1), where g is the gravity constant. The PD-like controller gains in (3) are $Kp = 1$, $Kd = 0.5$, and $K_{dm} = 0.5$. The simulation time is 30 (sec). The initial conditions for BTOS are chosen as $q_m = 0.5$, $\dot{q_m} = 0$, $q_s = -0.5$, $\dot{q_s} = 0$. The system operating in the normal situation is presented in Fig. 5, and all states are stable. In Fig. 6, the attack characterized in Section 2.2 was implemented and applied to the system. The system states were unstable in the presence of an attack.

The gains Kp, Kd, and K_{dm} used in the simulation are the tuned parameters of the PD-like controller. The values of these parameters are obtained from [43]. The dataset has been collected

and labelled into two categories (attack, and no attack). The dataset consists of 51102 samples half coming from the attack category and the other half is labelled as no attack.

After training the model on 95% of the dataset, the proposed CNN model is Trained using Google Collaboratory GPU resources and then integrated with the BTOS system in MATLAB and Simulink. The minimum training loss (error) is 0.104338. Fig. 4 illustrating the training and validation losses with respect to the epochs.

The proposed CNN model was able to classify attacks in the unseen testing dataset with 96% accuracy and a loss of 0.073149. Hence, we conclude that our approach guarantees the detection of cyber-physical content modification textcolorRoyalBlue(7)-(23) attacks with a high probability of 96%. The performance of the proposed model is shown in Fig. 7. The attack is started at time 10s and the proposed model detects the attack with a 100% probability after 2s.

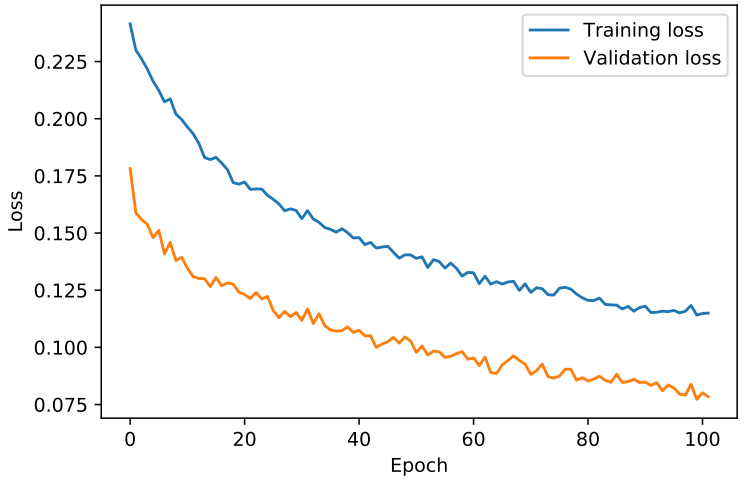

Fig. 4. Training and Validation Losses (Error)

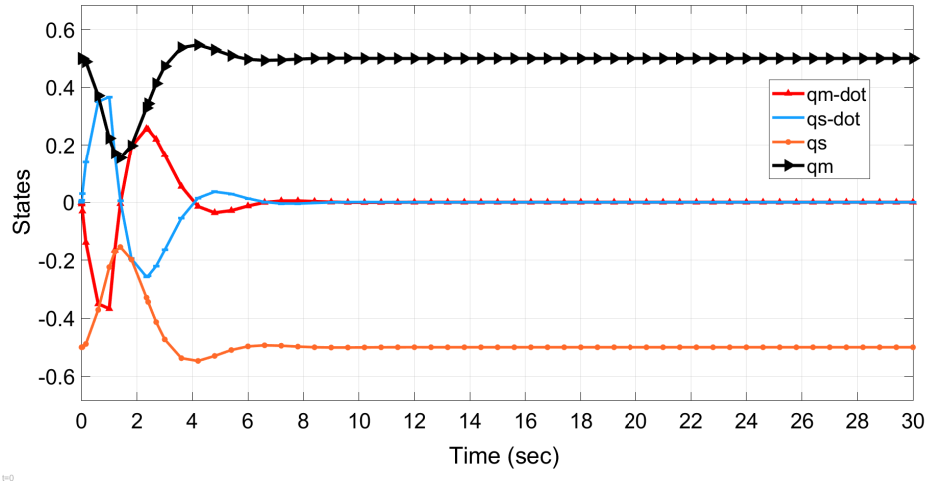

Fig. 5. States Trajectory in Normal Situation (No Attack)

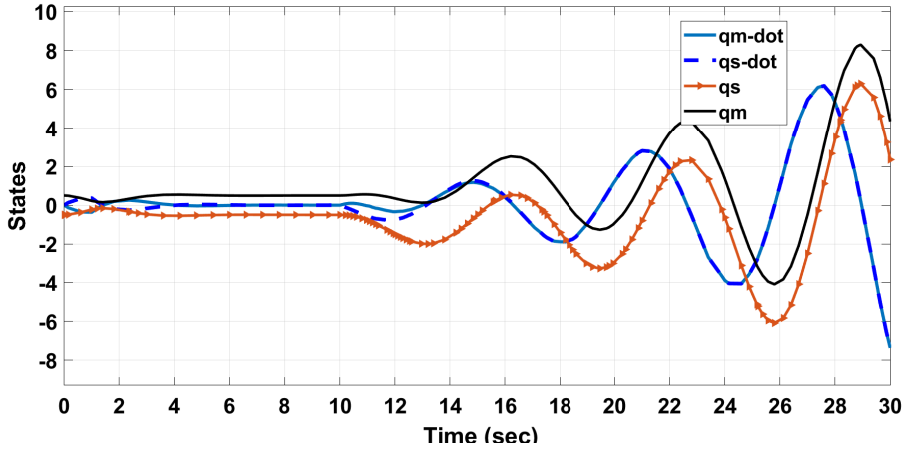

Fig. 6. States Trajectory Under Attack

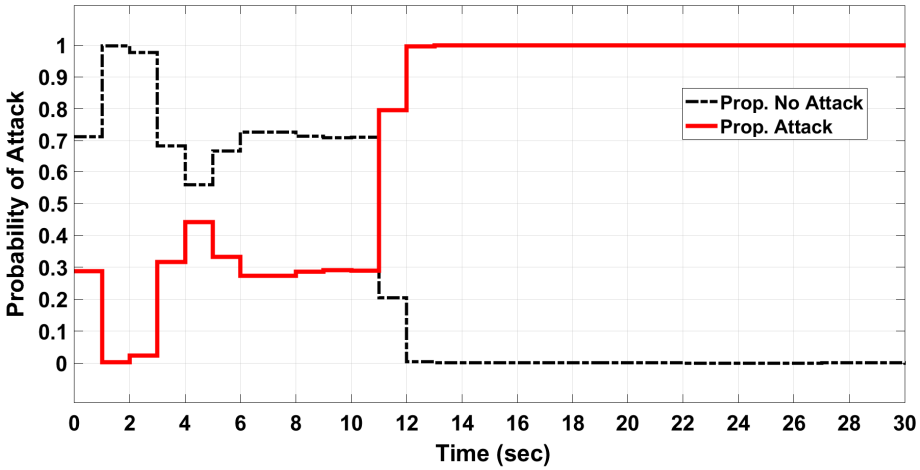

Fig. 7. Probability of Attack

Remark 3 *The aim of this work is to detect and identify the attack using a deep learning model. In this regard, the PI-like Controller gains are taken from work done by authors in [43], and the controller challenge is considered for future work.*

5. Conclusion

A teleoperation system is referred to as a plant that is controlled remotely, and it is often composed of a human operator, a local master manipulator, and a remote slave manipulator, all connected by a communication network. Bilateral teleoperation systems (BTOS) include transmissions in both the forward and backward directions between the master and slave. The cyber-physical system in the bilateral teleportation system is infiltration-proof after applying deep learning attack detection. DA-LD underwent data requisition and data recognition processes that enhanced the detection ability of attacks. The recognition of the attack where the attacker contained internal dynamic information about the system was prevented as well as the attack in the communication link. Such attacks can cripple the slave robot, which directly impacts the physical system and the environment sounded the slave robot. The proposed deep learning model with Convolutional Neural Network (CNN) architecture was trained and tested by considering complex attacks where the attacker has full knowledge

of the system. The proposed model achieves 96% accuracy on the unseen dataset. Furthermore, the efficacy of the proposed deep learning detector was demonstrated and tested in the BTOS.

As a future work, the technology of deep learning and attack detection can be improved to operate on larger applications such as multi-agent robots. To test and effectiveness of the method and the satisfactory performance it achieves, using different detection methods based on different variables can show intriguing results. trying different Artificial intelligence also counts as future work. Testing the detection of the attack on different obstacles and showing reliability in operation will be considered future work in addition to hardware implementation.

References

[1] W. Wei and Y. Kui, "Teleoperated manipulator for leak detection of sealed radioactive sources," in *IEEE International Conference on Robotics and Automation*, pp. 1682–1687, 2004, https://doi.org/10.1109/ROBOT.2004.1308066.

[2] W.-K. Yoon, T. Goshozono, H. Kawabe, M. Kinami, Y. Tsumaki, M. Uchiyama, M. Oda, and T. Doi, "Model-based space robot teleoperation of ets-vii manipulator," *IEEE Transactions on Robotics and Automation*, vol. 20, no. 3, pp. 602–612, 2004, https://doi.org/10.1109/TRA.2004.824700.

[3] J. Funda and R. P. Paul, "A symbolic teleoperator interface for time-delayed underwater robot manipulation," in *OCEANS 91 Proceedings*, pp. 1526–1533, 1991, https://doi.org/10.1109/OCEANS.1991.606520.

[4] S. Kumar and J. Marescaux, *Telesurgery*. Springer Science & Business Media, 2008, https://books.google.co.id/books?id=F_R_u_0vUSUC&hl=en.

[5] S. Kimura, T. Nozaki, and T. Murakami, "Admittance control-based bilateral control system considering position error," in *2021 IEEE International Conference on Mechatronics (ICM)*, pp. 1–6, 2021, https://doi.org/10.1109/ICM46511.2021.9385683.

[6] P. F. Hokayem and M. W. Spong, "Bilateral teleoperation: An historical survey," *Automatica*, vol. 42, no. 12, pp. 2035–2057, 2006, https://doi.org/10.1016/j.automatica.2006.06.027.

[7] D. Lee and M. W. Spong, "Passive bilateral teleoperation with constant time delay," *IEEE transactions on robotics*, vol. 22, no. 2, pp. 269–281, 2006, https://doi.org/10.1109/TRO.2005.862037.

[8] N. Chopra, M. W. Spong, and R. Lozano, "Synchronization of bilateral teleoperators with time delay," *Automatica*, vol. 44, no. 8, pp. 2142–2148, 2008, https://doi.org/10.1016/j.automatica.2007.12.002.

[9] E. Nuño, L. Basañez, R. Ortega, and M. W. Spong, "Position tracking for non-linear teleoperators with variable time delay," *The International Journal of Robotics Research*, vol. 28, no. 7, pp. 895–910, 2009, https://doi.org/10.1177/0278364908099461.

[10] J.-H. Ryu, J. Artigas, and C. Preusche, "A passive bilateral control scheme for a teleoperator with time-varying communication delay," *Mechatronics*, vol. 20, no. 7, pp. 812–823, 2010, https://doi.org/10.1016/j.mechatronics.2010.07.006.

[11] H.-C. Hu and Y.-C. Liu, "Passivity-based control framework for task-space bilateral teleoperation with parametric uncertainty over unreliable networks," *ISA transactions*, vol. 70, pp. 187–199, 2017, https://doi.org/10.1016/j.isatra.2017.07.024.

[12] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011, https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.

[13] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water scada systems—part i: Analysis and experimentation of stealthy deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 5, pp. 1963–1970, 2012, https://doi.org/10.1109/TCST.2012.2211873.

[14] S. Gorman, "Electricity grid in us penetrated by spies," *The wall street journal*, vol. 8, 2009, https://www.wsj.com/articles/SB123914805204099085.

[15] K. McKay, L. Bassham, M. Sönmez Turan, and N. Mouha, "Report on lightweight cryptography," tech. rep., National Institute of Standards and Technology, 2016, https://csrc.nist.gov/CSRC/media/Publications/nistir/8114/draft/documents/nistir_8114_draft.pdf.

[16] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 20–23, 2015, https://doi.org/10.1109/MCS.2014.2364708.

[17] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 110–127, 2015, https://doi.org/10.1109/MCS.2014.2364725.

[18] E. Eyisi and X. Koutsoukos, "Energy-based attack detection in networked control systems," in *Proceedings of the 3rd international conference on High confidence networked systems*, pp. 115–124, 2014, https://doi.org/10.1145/2566468.2566472.

[19] M. M. Hamdan and M. S. Mahmoud, "Control of teleoperation systems in the presence of cyber attacks: A survey," *IAES International Journal of Robotics and Automation*, vol. 10, no. 3, p. 235, 2021, http://doi.org/10.11591/ijra.v10i3.pp235-260.

[20] C. Cai, Y. Zhang, and Q. Chen, "Adaptive control of bilateral teleoperation systems with false data injection attacks and attacks detection," in *2022 41st Chinese Control Conference (CCC)*, pp. 4407–4412, 2022, https://doi.org/10.23919/CCC55666.2022.9902043.

[21] E. A. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pp. 363–369, 2008, https://doi.org/10.1109/ISORC.2008.25.

[22] M. M. Hamdan and M. M. Mahmoud, "Analysis and challenges in wireless networked control system: A survey," *International Journal of Robotics and Control Systems*, vol. 2, no. 3, pp. 492–522, 2022, https://doi.org/10.31763/ijrcs.v2i3.731.

[23] K.-D. Kim and P. Kumar, "An overview and some challenges in cyber-physical systems," *Journal of the Indian Institute of Science*, vol. 93, no. 3, pp. 341–352, 2013, http://journal.library.iisc.ernet.in/index.php/iisc/article/view/1693.

[24] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: a survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, 2019, https://doi.org/10.1016/j.neucom.2019.01.099.

[25] M. S. Mahmoud and M. Maaruf, "Prescribed performance output feedback synchronisation control of bilateral teleoperation system with actuator nonlinearities," *International Journal of Systems Science*, pp. 1–13, 2021, https://doi.org/10.1080/00207721.2021.1921308.

[26] J. F. Yonan, "An examination of the secure chaos of 5g wireless communication based on the intelligent internet of things," *International Journal of Robotics and Control Systems*, vol. 2, no. 4, pp. 618–627, 2022, https://doi.org/10.31763/ijrcs.v2i4.769.

[27] M. Marvi, A. Arfeen, and R. Uddin, "A generalized machine learning-based model for the detection of ddos attacks," *International Journal of Network Management*, vol. 31, no. 6, p. e2152, 2021, https://doi.org/10.1002/nem.2152.

[28] L. Hu, K. Wang, D. Hu, and Y. Wang, "Mode-dependent switching control of bilateral teleoperation against random denial-of-service attacks," *IET Cyber-Physical Systems: Theory & Applications*, vol. 7, no. 1, pp. 16–29, 2022, https://doi.org/10.1049/cps2.12015.

[29] J. Yan, K. Huang, K. Lindgren, T. Bonaci, and H. J. Chizeck, "Continuous operator authentication for teleoperated systems using hidden markov models," *ACM Transactions on Cyber-Physical Systems (TCPS)*, vol. 6, no. 1, pp. 1–25, 2022, https://doi.org/10.1145/3488901.

[30] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in *International conference on critical infrastructure protection*, pp. 73–82, 2007, https://doi.org/10.1007/978-0-387-75462-8_6.

[31] R. Esposito, "Hackers penetrate water system computers," *ABC News, Nov*, vol. 1, 2006.

[32] A. Greenberg, "Hackers cut cities' power," *Forbes, January*, 2008, https://www.forbes.com/2008/01/18/cyber-attack-utilities-tech-intel-cx_ag_0118attack.html.

[33] J. Leyden, "Polish teen derails tram after hacking train network," *The Register*, vol. 11, 2008, https://www.theregister.com/2008/01/11/tram_hack/.

[34] S. E. Schechter, J. Jung, and A. W. Berger, "Fast detection of scanning worm infections," in *International Workshop on Recent Advances in Intrusion Detection*, pp. 59–81, 2004, https://doi.org/10.1007/978-3-540-30143-1_4.

[35] M. W. Spong, S. Hutchinson, and M. Vidyasagar, *Robot modeling and control*. John Wiley & Sons, 2020, https://books.google.co.id/books?id=DdjNDwAAQBAJ&hl=en.

[36] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: a simple way to prevent neural networks from overfitting," *The journal of machine learning research*, vol. 15, no. 1, pp. 1929–1958, 2014, https://jmlr.org/papers/volume15/srivastava14a/srivastava14a.pdf.

[37] T. Hatanaka, N. Chopra, M. Fujita, and M. W. Spong, *Passivity-based control and estimation in networked robotics*. Springer Cham, 2015, https://doi.org/10.1007/978-3-319-15171-7.

[38] Y. Dong, N. Gupta, and N. Chopra, "False data injection attacks in bilateral teleoperation systems," *IEEE Transactions on Control Systems Technology*, vol. 28, no. 3, pp. 1168–1176, 2019, https://doi.org/10.1109/TCST.2019.2903446.

[39] S. Ioffe and C. Szegedy, "Batch normalization: Accelerating deep network training by reducing internal covariate shift," *arXiv preprint arXiv:1502.03167*, 2015, https://doi.org/10.48550/arXiv.1502.03167.

[40] B. Xu, N. Wang, T. Chen, and M. Li, "Empirical evaluation of rectified activations in convolutional network," *arXiv preprint arXiv:1505.00853*, 2015, https://doi.org/10.48550/arXiv.1505.00853.

[41] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014, https://doi.org/10.48550/arXiv.1412.6980.

[42] A.-N. Sharkawy, "Principle of neural network and its main types," *Journal of Advances in Applied & Computational Mathematics*, vol. 7, pp. 8–19, 2020, https://doi.org/10.15377/2409-5761.2020.07.2.

[43] Y. Dong, N. Gupta, and N. Chopra, "On content modification attacks in bilateral teleoperation systems," in *2016 American Control Conference (ACC)*, pp. 316–321, 2016, https://doi.org/10.1109/ACC.2016.7524934.