A Temporal-Pattern Backdoor Attack to Deep Reinforcement Learning

Yinbo Yu†∗, Jiajia Liu∗, Shouqing Li‡, Kepu Huang∗, Xudong Feng∗
†Research & Development Institute of Northwestern Polytechnical University in Shenzhen, Shenzhen 518057, China
‡Academy of Industrial Internet, Shaanxi Branch of China United Network Communications Group Co., Ltd., Xi’an, China
Email: {yinboyu, liujiajia}@nwpu.edu.cn, {lishq45@chinaunicom.cn, {huangkepu, dfnjkd}@mail.nwpu.edu.cn

Abstract—Deep reinforcement learning (DRL) has made significant achievements in many real-world applications. But these real-world applications typically can only provide partial observations for making decisions due to occlusions and noisy sensors. However, partial state observability can be used to hide malicious behaviors for backdoors. In this paper, we explore the sequential nature of DRL and propose a novel temporal-pattern backdoor attack to DRL, whose trigger is a set of temporal constraints on a sequence of observations rather than a single observation, and effect can be kept in a controllable duration rather than in the instant. We validate our proposed backdoor attack to a typical job scheduling task in cloud computing. Numerous experimental results show that our backdoor can achieve excellent effectiveness, stealthiness, and sustainability. Our backdoor’s average clean data accuracy and attack success rate can reach 97.8% and 97.5%, respectively.

Index Terms—Backdoor attack, deep reinforcement learning, temporal feature

I. INTRODUCTION

Deep reinforcement learning (DRL) embraces deep neural networks (DNN) to overcome the limitations of reinforcement learning techniques in their convergence speed and performance, and has made significant achievements in various fields, e.g., networking, computer vision, and speech recognition [1]. The key factors to DRL success are large amounts of training data and increasing computational power. But existing models require expensive hardware and long training time. Hence, to reduce the overhead, users tend to use third-party resources to conduct training processes or directly use pre-trained networks provided by third-parties. However, this brings a new security threat of backdoor attack (also called “neural trojan”, or “trojan attack”) to perform DRL [2], [3].

A backdoored DNN model behaves normally on benign samples, but can produce malicious results once an attacker-specified trigger is presented in the input. Unlike supervised learning (e.g., image classification), DRL is required to address sequential decision-making problems according to immediate rewards instead of supervision on long-term reward. Backdoors on DRL are more challenging since the backdoored agent needs to disrupt the sequential decisions rather than isolated decision while maintaining good performance in absence of backdoor triggers [3]. Kiourti et al. [3] use image patches as the backdoor trigger and manipulate the corresponding action and reward when the trigger is present. Ashcraft et al. [4] studied a DRL backdoor that uses the action trajectory presented in the image observation as the trigger. While these backdoor triggers are useful for DRL, they lack stealthiness and are visible for users.

The DRL agent learns its optimal policy through interaction with the environment. Most DRL methods assumes the state of the environment is fully observable for the agent. However, in many real world cases, the agent can only glimpse a part of the system state due to occlusions and noisy sensors. A partially observable Markov decision process (POMDP) [5] can better capture the dynamics of many real world environments, but finding an optimal policy for POMDP is notoriously difficult. Existing methods aggregate histories of observations over time by integrating a recurrent neural network (RNN) [6] or a generative model [7] to find hidden states for optimal policy generation. POMDP and these DRL methods have been used as a powerful tool to effectively address various problems and challenges, e.g., cognitive radio [8], edge computing [9], automatic driving [10], etc. However, the partial observability can make better hackers [11]. We think that a backdoor trigger can be hidden in unobservable states, which is invisible and hard to be detected.

Based on the above finding, in this paper, we propose a novel temporal-pattern trigger and a backdoor with controllable duration to DRL. A temporal-pattern trigger is a set of temporal constraints on a sequence of observations \((d_1, \ldots, d_s)\) rather than a single instant observation used in existing neural Trojans. For instance, a trigger \((d_1 - d_2 < 20 \land d_3 - d_2 > 10)\) describes the correlation among three consecutive data. Such a trigger is invisible in a single epoch. Besides, most existing backdoor effects are activated instantly only when a trigger is present. Yang et al. [12] presented a backdoor attack that persistently affects DRL performance once a trigger occurs. Persistent attack effect, however, destroys the stealthiness of the attack. We design a backdoor manipulating sequential decisions in a controllable duration. The adversary can specify the duration depending on the target DRL environment. With a temporal-pattern trigger and controllable attack duration, our DRL backdoor can achieve better stealthiness and practicality than existing works. To the best of our knowledge, this is the first that explores backdoor attacks to DRL in the time domain both regarding to trigger and attack effect. To evaluate our backdoor attacks, we use the task of job scheduling in cloud computing as a study case.
Our experimental results demonstrate that the average clean data accuracy (CDA) and attack success rate (ASR) of our backdoor attacks is 97.8% and 97.5%, respectively. Besides, we demonstrate that state-of-the-art defense mechanisms for backdoored DNN fail to detect Trojans in our DRL case.

The remainder of the paper is organized as follows. We discuss the related work in §II. We present our proposed backdoor in §III. §IV describes the experimental design and the performance evaluation results, and provides analytical insights. Lastly, we conclude the paper and outline our future work in §V.

II. RELATED WORK

Backdoors in DNN have been widely studied in the domain of image classification [2], [13], where a trigger can be an image patch, a physical accessory, facial characteristic, or invisible noise. There are 6 major methods to insert backdoors into DNN: code poisoning, outsourcing, pretrained, data collection, collaborative learning, and post-deployment [13]. While these experiences can be applied to DRL, DRL aims to solve sequential decision-making problems which are different from classification tasks.

Currently, there are only few works that have studied backdoors in DRL. Kiourti et al. [3] use image patches as the trigger and train a DRL policy to output fixed action and reward when the trigger is present. Wang et al. [14] design two backdoor attacks on DRL-based autonomous vehicles (AV) controllers. They set a specific set of combinations of positions and speeds of vehicles in the observation as the trigger. When the trigger is present, the AV controller could generate malicious deceleration to cause a physical crash and traffic congestion. We call these backdoors in these two work instant backdoors since their triggers and actions do not consider sequential dependencies.

Since the state space of many real-world environments is partial observable, introducing RNN into DRL can capture sequential dependencies to improve the performance of DRL. Yang et al. [12] examined the persistent effect of backdoors in proximal policy optimization (PPO) algorithm equipped with LSTM for POMDP problems. They use a timestep $t$ as the trigger and setup a normal and a trojan environment to feedback the reward before and after $t$ respectively to train the backdoored policy. Similarly, Ashcraft et al. [4] also study backdoors in this network, but the trigger they used is a sequence of action following a specific pattern. These two backdoor attacks are only applicable to simple games with totally tractable environments. Wang et al. [15] study backdoors in reinforcement Learning used for two-player competitive games. They train two different policies (normal and Trojan), and hard-encode them to generate the backdoored trajectories which can lead to fast fail the game when a specific series of trigger actions (i.e., trigger) appears. Then, they use imitation learning to train an LSTM-based policy to mimic the behavior of generated trajectories. We also propose a backdoor attack on the LSTM-based DRL policy, but we study temporal constraints and controllable attack durations to build backdoors. These features ensure the practicality and stealthiness of our attack to DRL.

Since existing DNN backdoor attacks are majorly designed for classification tasks, most existing backdoor defense mechanisms are geared towards classification networks [2], [13]. Tran et al. [16] studied how to filter poisoned samples from the training set and demonstrated that poisoned samples tend to often contain detectable traces in their feature covariance spectrum. STRIP [17] can detect whether an input contains Trojan trigger by adding strong perturbation to the input. Neural Cleanse [18] identifies backdoored DNN models through reversing engineers for each input, so that all inputs stumped with the pattern are classified to the same label. However, these defense mechanisms are designed for isolated inputs rather than sequential inputs and have been shown low accuracy of detecting backdoors in DRL [3]. Recently, Guo et al. [19] propose a backdoor detection method in competitive DRL by training a separate policy with a reversed reward function given by the Trojan agent. More sophisticated defense methods for DRL are desired to develop.

III. TEMPORAL-PATTERN BACKDOOR ATTACK

A. Threat model

Attacker’s Capacities. Similar to existing DRL backdoors [3], [4], [12], we consider the outsourcing scenario, in which a user defines the model architecture, provides training data, and outsources the model training to a third party due to her lack of DRL skills or computational resources. In this scenario, attackers are allowed to poison some training data, control the training process, and manipulate the reward to the poisoning state. The security threat exists in many DNN-based applications, including DRL, autonomous driving, and face recognition [13], [20].

Attacker’s Goals. With these above capacities, backdoor attackers aim to embed hidden backdoors into DRL policies. In particular, these inserted backdoors should have effectiveness, stealthiness, and sustainability [13]. The effectiveness requires that the backdoored model can perform no different from a normally-trained model in absence of backdoor triggers and have degraded performance when the trigger is present. The stealthiness requires that backdoor triggers should be concealed; The sustainability requires that the attack should still be effective under some common backdoor defenses.

B. Temporal-Pattern Trigger

The DRL agent is typically driven by fluctuating states in many real-world cases, e.g., job requests of cloud resources [21], network bandwidth for adaptive video streaming [22], and surrounding vehicle information [10]. These states are not affected by DRL decisions and thus, are uncontrollable for the DRL agent. But these states may be possible to manipulate by malicious users or attackers. For example, a cloud user builds a series of service requests containing a backdoor trigger to send to the cloud provider who uses a DRL model for service provision. Hence, we aim to hide backdoor triggers into these states, which ensure that the backdoor is realistic and cannot
be removed by adjusting actions generated by the DRL policy. We define our temporal-pattern trigger as follows:

These fluctuating states are time series data and can be denoted by \( s_{t}^{1}, s_{t}^{2}, \ldots, s_{t}^{N} \), where \( t \in \mathbb{N} \) is the timestep at which the DRL agent makes a decision (i.e., action \( a_{t} \)) according to the state \( s_{t} \) provided by the environment. The state \( s_{t} \) includes the fluctuating state \( d_{t} \) and other partial states of the system. We encode backdoor triggers in the form of temporal logic formula over a sequence of time series data. Given two time series states \( s_{t}^{1} \) and \( s_{t}^{2} \), we define a formula \( \varphi(1,2) := f(s_{t}^{1}, s_{t}^{2}) \sim c \) to describe a constraint over \( s_{t}^{1} \) and \( s_{t}^{2} \), where \( f \) is a binary operation (e.g., \( +, -, \times, \div \)), \( \sim \in \{=, \neq, >, \geq, <, \leq \} \), and \( c \in \mathbb{R} \) is constant. The syntax of a temporal-pattern trigger is defined as follows:

**Definition 1.** Given a set \( \{s_{t-N+1}^{N_1}, s_{t-N_2+1}^{N_2}, \ldots, s_{t-N_N+1}^{N_N}\} \) of time series states with length \( N \) ending at timestep \( t \), a temporal-pattern trigger is a temporal logic formula \( \varphi \) over constraints \( \Psi \) of these time series states:

\[
\tau := \varphi(i,j) \vee \varphi(k,s) \land \mathit{ite}(\varphi(i,j), \varphi(k,s), \varphi(p,q)),
\]

where \( \varphi(i,j), \varphi(k,s), \varphi(p,q) \in \Psi \); \( \land \) is a Boolean operator, including disjunction \( \lor \) ("or") and conjunction \( \land \) ("and"); \( \mathit{ite} \) denotes \( \phi \)-assignment, e.g., \( \tau := \mathit{ite}(\varphi_1, \varphi_2, \varphi_3) \) means if \( \varphi_1 \) is true, \( \tau := \varphi_2 \); otherwise \( \tau := \varphi_3 \). With the formula, attackers can define a backdoor trigger over time series data.

**Example 1.** For instance, given a trigger \( \{s_{t=4}^{N_1} = 4\} \) \( \tau := \varphi(1,2) \land \varphi(2,3) \land \mathit{ite}(\varphi(1,3), \varphi(2,4), \varphi(1,1)) \), where \( \varphi(1,2) := d_{1} - d_{2} < 0.01, \varphi(2,3) := d_{2} - d_{3} > 0.4, \varphi(3,4) := d_{3} - d_{4} < -0.1, \varphi(4,2) := d_{4} - d_{2} > -0.35, \varphi(1,1) := d_{4} - d_{1} < 0.1 \), the normalized time series data \((0.21, 0.83, 0.42, 0.47, 0.05, 0.17, 0.8)\) contains a trigger at \( t_{17} \) (i.e., \( 0.42, 0.47, 0.05, 0.17 \)).

**Remark 1.** Triggers of previous backdoor attacks to DRL are temporal-specific [3] or observable in a single observation [4], [12] rather than over a period of time.

### C. The Proposed Attack

In this section, we illustrate our proposed attack. We first describe how to generate temporal-pattern triggers and then present how to train the backdoored DRL model with the pseudocode shown in Alg. 1.

First, attackers specify a temporal-pattern trigger \( \tau \) over a series of data with \( N_{l} \) timesteps (i.e., \( \tau(N_{l}) \)) and a backdoor duration \( L \). Note that although with LSTM, DRQN can have long memory effects, LSTM is not that ideal and require more complex neurons and longer training time for memorizing longer historical features [23]. Hence, we keep only \( N_{l} \) and \( L \) no more than 10 timesteps. Solutions, like [7], [23], can address this limitation and thereby, make our backdoor attacks have longer effects, but are out of our scope. Then, attackers randomly choose a set \( \Sigma \) of \( N_{l} \) timesteps in the time series data with length \( N \), in which the time series data is randomly changed to satisfy with \( \tau \) (Line 4). To keep the balance between CDA and ASR of the backdoored model, we set a poisoning rate \( \lambda \) such that \( \frac{N_{l} || \Sigma \|}{N_{l}} < \lambda \).

![Algorithm 1: Temporal-Pattern Backdoored DRQN.](image)

During each training iteration, in general, the agent selects an action at each timestep using the \( \epsilon \)-greedy method (Line 7), stores interactions (Line 8 and 14), and updates the network with a MSE loss \( ||y_{t} - Q(s_{t}, a_{t})||^{2} \) (Line 14-18), where \( y \) is the target function:

\[
y_{t} = r_{t+1} + \gamma \max_{a_{t+1}} Q(s_{t+1}, a_{t+1}; \theta'),
\]

where \( \tilde{Q} \) is a target network with parameters \( \theta' \); \( \gamma \in [0, 1] \) is the discount factor and specifies the importance between future rewards and the current reward. Once the current timestep \( t \) is the last timestep of a trigger in the generated \( \Sigma \) set, we change the reward \( r_{t} \in [0, 1] \) returned from the environment to be \( 1 - r_{t} \) within a poisoning duration \( L \) (Line 9-13) as our backdoor behavior. This behavior leads the network to being updated in the opposite direction of the clean training process, thereby is undesired. Besides, at each time to update the network, we sample a sequential batch from the memory \( D \) rather than a random batch. Such a batch can help DRQN learn more sequential features and also ensure the ASR of our backdoor attacks.

### IV. Evaluation

#### A. Case study

In our experiment, we use the typical job scheduling problem in clouds as the study case. The scheduling system consists of users, job queues, job scheduler, and virtual machines (VMs). A job (i.e., user request) can be represented by a 4-tuple \((J_{ID}, J_{AT}, J_{TP}, J_{ID})\) describing its id, arrival time, type (I/O or computing intensive), and instruction length respectively. To process jobs, the system provides 3 VM instances, each can be denoted by a tuple \((V_{ID}, V_{TP}, V_{PS})\) representing its id, instance type, average instruction processing speed respectively. At each timestep \( t \), the job scheduler
takes a user job $J_i$ ($i \in I$) and assign to a VM instance $V_j$. $J_i$ will enter a waiting FIFO queue of the instance. Each VM can only handle one job at a timestep. Hence, the response time ($J_{WT}^j$) of $J_i$ is composed of waiting time ($J_{WT}^{j'}$) in the queue and execution time ($J_{ET}^j$) of VM. To encourage the matching of $J_{WT}^{j'}$ and $V_j$, we design $J_{WT}^{j'} = J_{WT}^{j} / (V_j)$, where $V_j$ is the available time of $V_j$ for job $J_i$. If $V_j$ is greater than its $J_{ET}^j$, $V_j$ will enter a waiting FIFO queue of the instance.

B. Experiment Setup

In our experiment, we set the number of VM instances $N = 10$ and the number of jobs to $|I| = 1000$ (i.e., $N = 1000$). Similar to [21], we have 5 computing intensive VM instances ($V_{TP} = 0$) and 5 I/O intensive VM instances ($V_{TP} = 1$) respectively, and the average processing speeds of these VM is 2000 MIPS (million instructions per second). Besides, we set that job requests arrive according to a Poisson distribution and their arrival rate is varied from 10 to 30 requests/s. The instruction lengths of jobs obey the normal distribution with mean 200 MI (million instructions) and standard deviation 20 MI. The ratio of computing intensive jobs and I/O intensive jobs is 1:1. Our implementation is available at https://github.com/EboYu/DRLBackdoor.

We use the following linear DNN network: $|O| \rightarrow 64 \rightarrow 64 \rightarrow 64 \rightarrow 64 \rightarrow |A|$ to train a DRQN policy for job scheduling. The network contains a fully connected hidden layer with 64 neurons. Between the input and hidden layer, it has a LSTM network with 2 layers. Besides, we set the capacity of replay memory $M = 10000$, the size of batch 64, discount factor $\gamma = 0.9$, and steps of updating target network $C = 50$. Adam algorithm is adopted to update the network $Q$ with the learning rate of $\alpha = 0.001$. We set $\epsilon$ to be decreased from 0.9 by 0.002 in each learning iteration. We specify 4 temporal-pattern triggers to validate our backdoor attacks:

- $\tau_1(N_t = 4, L = 4)$ := $\varphi_{(1,0)} \land \varphi_{(2,1)} \land \varphi_{(3,2)} \land \varphi_{(3,0)}$,
  where $\varphi_{(1,0)} := d_1 - d_0 > -3$ and $\varphi_{(2,1)} := d_2 - d_1 > -20$ and $\varphi_{(3,2)} := d_3 - d_2 > -25$ and $\varphi_{(3,0)} := d_4 - d_3 > -25$.
- $\tau_2(N_t = 4, L = 4)$ := $\varphi_{(1,1)} \land \varphi_{(2,2)} \land \varphi_{(3,3)}$,
  where $\varphi_{(1,1)} := d_1 - d_0 > 80$ and $\varphi_{(2,2)} := d_2 - d_1 > 80$ and $\varphi_{(3,3)} := d_3 - d_2 > 80$.
- $\tau_3(N_t = 5, L = 6)$ := $\varphi_{(1,0)} \land \varphi_{(2,1)} \land \varphi_{(3,1)} \land \varphi_{(4,2)} \land \varphi_{(4,3)}$,
  where $\varphi_{(1,0)} := d_1 - d_0 > 20$ and $\varphi_{(2,1)} := d_2 - d_1 > -8$ and $\varphi_{(3,1)} := d_3 - d_2 > -5$ and $\varphi_{(4,2)} := d_4 - d_3 > -5$ and $\varphi_{(4,3)} := d_5 - d_4 > -5$.
- $\tau_4(N_t = 6, L = 3)$ := $\varphi_{(2,0)} \land \varphi_{(3,1)} \land \varphi_{(3,2)}$, where $\varphi_{(2,0)} := d_2 - d_1 > 1.4$ and $\varphi_{(3,1)} := d_3 - d_2 > -27$ and $\varphi_{(3,2)} := d_4 - d_3 > -26$.

C. Numerous results

Given these above network settings and four different triggers, we randomly generate training data containing poison

![Fig. 1: Convergence of training clean and backdoored models. H and N is the neuron size and number of LSTM layer, respectively.](image-url)

**TABLE I: Average ASR/APR/CDA of four backdoor attacks**

| Rate | $\tau_1$ | $\tau_2$ | $\tau_3$ | $\tau_4$ |
|------|----------|----------|----------|----------|
| 10   | 0.99/0.99/0.97 | 0.97/0.98/0.97 | 0.91/0.93/0.96 | 0.99/0.99/0.97 |
| 15   | 0.98/0.98/0.97 | 0.99/0.98/0.97 | 0.97/0.97/0.97 | 0.99/0.99/0.97 |
| 20   | 0.98/0.98/0.97 | 0.98/0.98/0.98 | 0.97/0.98/0.96 | 0.99/0.99/0.98 |
| 25   | 0.98/0.99/0.97 | 0.97/0.98/0.98 | 0.96/0.97/0.97 | 0.99/0.99/0.97 |
| 30   | 0.98/0.98/0.97 | 0.98/0.98/0.97 | 0.98/0.98/0.97 | 0.98/0.98/0.97 |

---

2713
data to train backdoored models under different request rates \{10, 15, 20, 25, 30\} requests/s. Fig. 1 shows the convergence ratios of training clean and backdoored models at the request rate 10 and 30, respectively. We can find that since \(\tau_4\) has a smaller temporal constraint space (longer constraint timesteps and smaller constraint range) than other triggers, the training processing for \(\tau_4\) can achieve lower loss values than others. Besides, we can find that most of the training process can converge in about 500 iterations, except for trigger \(\tau_2\). This is because the semantic \textit{ite} in \(\tau_3\) is more complex than other semantics. Although LSTM can memorize temporal dependencies, the memory capacity is limited to the neuron size and layers. Hence, we further use 128 neurons or 4 LSTM layers to train \(\tau_3\) backdoored models, shown in Fig. 1 (a). We can find that more neurons and LSTM layers both can improve the convergence, in which the effect of adding LSTM layers is better than adding neurons.

With these above trained backdoored models, we compare their average ASR, APR and CDA under different request rates, as shown in Table I. We can find that at average, the backdoor attack \(\tau_1\) can achieve better performance than other three attacks. \(\tau_4\) can also achieve the performance a little lower than \(\tau_1\). But it has a shorter duration \(L^\tau = 3\) that may cause that the backdoored policy cannot sufficiently disrupt the previous sequential decisions and lead to a lower ASR and APR, but a higher CDA. We will discuss this phenomenon with Fig. 2. The ASR and APR of \(\tau_2\) are both lower than \(\tau_4\) at average since \(\tau_2\) contains an OR operator which breaks the continuity of the temporal constraint space, thereby decreasing ASR and APR. The CDA of \(\tau_2\) is better than \(\tau_1\), but lower than \(\tau_3\) since \(L^\tau = 4\). These metrics achieved by \(\tau_3\) are the worst, and as the request rate increases, the performance of \(\tau_3\) can be improved since a higher request rate (i.e., workload) make it easier for backdoored DRL to find attack actions.

We further show the attack performance and response time under different backdoor attacks in Fig. 2. For each trigger, we generate a testing data containing 4 temporal-pattern attacks within 100 epochs. Fig. 2 mainly shows scheduling results at rate 20. We can find that after a trigger appears, a backdoor attack can generate actions to prominently and continuously decrease rewards returned by the environment and job response times. Hence, a longer attack duration can result in a higher response time, see Fig. 2 (b) and (f). After the attack duration, the reward and response time can go back to be normal quickly. If two attacks are close in time (e.g., Fig. 2 (b)), the second attack is easy to lead to a higher response time since the effect of the first attack has not yet been disrupted by actions for these requests between two attacks. We further increase the poison length \(L\) to 42 and the request rate to 55 to validate \(\tau_1\), respectively and show results in Fig. 2 (i-l). We can see that both a higher attack duration or workload can improve the influence of our backdoored attacks. That is why response times under attacks \(\tau_2\) and \(\tau_4\) increases less than these ones under \(\tau_1\) and \(\tau_3\), and \(\tau_2\) and \(\tau_4\) have lower effect on clean data (i.e., higher CDA). But on the contrary, longer attack duration (\(\tau_1\)) can achieve higher ASR and APR.

Fig. 2: Attack performances and response time under different triggers and attack durations. Note that the Label shows the attack duration.
TABLE II: Trojan detection results

| Defense                   | Accuracy | Precision | Recall | F1     |
|---------------------------|----------|-----------|--------|--------|
| Spectral signature [16]   | 0.014    | 0.014     | 1.0    | 0.081  |
| Activation clustering [25] | 0.8412   | 0.0579    | 0.6768 | 0.1066 |

D. Defense

To evaluate the sustainability of our backdoor attacks, we adopt the start-of-the-art neuron Trojan detector to check whether the injected Trojan can be identified in a trained model. We analyze 160000 samples, in which 2240 samples are poisoned. In our experiment case, we divide these samples into 10 sets according to the action. We detect Trojan via spectral signature [16] and activation clustering [25]. This two methods all require access to the training data including the poisoned labels. Table II demonstrates the Trojan detection results. With method [16], we analyze the spectral signature for each set. But, we can find that it clustered all states in a set into the same cluster and hence, cannot distinguish the clean and poison samples. With method [25], we extract the activations of the penultimate layer of the trained model and detect Trojan by performing independent component analysis and K-means clustering on activations. The detection performance of activation clustering is better than spectral signature for our backdoor attack (higher accuracy). But its F1 score is also low since this method has high false positives in our experiment case. The fundamental reason why these methods failed to detect our backdoor attack is that we hide the trigger into a sequence of states defined by temporal logic, rather than in an instant state, and malicious actions are generated by poison rewards, rather than fixed.

V. CONCLUSIONS AND FUTURE

In this paper, we present a novel backdoor to DRL policies that has a temporal pattern trigger hidden in a sequence of observations and has a controllable attack duration. We use the typical job scheduling problem in the cloud computing as a case study and we show that our temporal-pattern backdoor attacks can achieve great clean data accuracy and attack success rate. Our proposed backdoor can be applied in many real-world DRL applications since observations in these applications are partial and our triggers can be easily hide in unobservable temporal observations. In the future, we aim to explore the effect of our attacks in more real-world DRL application scenarios (e.g., networking, automatic driving, UAV, etc.), introduce more meaningful temporal features (e.g., entropy and Mann Kendall trend) as attack triggers, as well as design defense mechanisms suitable for DRL backdoors.

ACKNOWLEDGEMENT

This work was supported in part by the GuangDong Basic and Applied Basic Research Foundation under Grant 2021A1515110279; in part by the Natural Science Basic Research Program of Shaanxi under Grant 2022JQ-611; and in part by the Fundamental Research Funds for the Central Universities under Grant D5000210588.