






# Learning the Propagation of Worms in Wireless Sensor Networks

Yifan Wang<sup>(✉)</sup>, Siqi Wang, and Guangmo Tong

University of Delaware, Newark, DE 19711, USA  
{yifanw, wsqbit, amotong}@udel.edu

**Abstract.** Wireless sensor networks (WSNs) are composed of spatially distributed sensors and are considered vulnerable to attacks by worms and their variants. Due to the distinct strategies of worms propagation, the dynamic behavior varies depending on the different features of the sensors. Modeling the spread of worms can help us understand the worm attack behaviors and analyze the propagation procedure. In this paper, we design a communication model under various worms. We aim to learn our proposed model to analytically derive the dynamics of competitive worms propagation. We develop a new searching space combined with complex neural network models. Furthermore, the experiment results verified our analysis and demonstrated the performance of our proposed learning algorithms.

**Keywords:** Wireless sensor network · Multi-worm propagation · Complex neural network

## 1 Introduction

Due to the recent advances in wireless and micro-mechanical sensor technologies, wireless sensor networks (WSNs) have been widely used in various real-time applications, for example, target tracking, biological detection, health care monitoring, environmental sensing and etc. [9, 16, 17, 22, 26, 29]. WSNs are composed of the spatially distributed sensors that are low-cost, small-sized, low-energy, and multi-functional [10, 16, 35]. Each sensor is designed to sense and collect environmental information. It has the ability to carry out a local computation to obtain the required data and will transfer the required data to a higher-level host [3, 35]. Besides, the communication paradigm of WSNs is based on the broadcasting such that each sensor can communicate with its neighbors directly [3, 32].

The computer worms are the programs that can be disseminated across the network by self-replicating to exploit the security or policy flaws [28, 36]. Although many advantages of the sensors are proposed, WSNs are vulnerable to attacks by worms and variants. One reason is that sensor network protocols primarily concentrate on power conservation, and each sensor is usually assigned to a limited resource. Therefore it generally has a weak defense mechanism [19, 30]. Besides, since the spread of worms usually relies on the information involved in the infected

sensors and WSNs often embed an efficient propagation mechanism, the worms can achieve a rapid propagation speed [2, 4, 16]. Furthermore, some worms will upgrade and be more complicated in order to propagate successfully, which will result in a widespread destruction [35]. Therefore, worms and variants become one of the main threats to network security.

In order to control the spreading of worms, people seek to understand the dynamic behaviors of worms. In practice, worms utilize different propagation strategies. For example, scan-based techniques will identify the vulnerable sensors based on the IP address [34, 39]. Topology-based techniques allow worms to spread through the topology neighbors [35]. Many studies have modeled these propagation procedures mathematically. Most researchers proposed propagation models based on the classic epidemic models, for example, SIR and SEIR models [12, 15]. In recent works, extensions to the epidemic models have been proposed: Some studies considered the hybrid dynamic of worms and antivirus propagation [1, 6, 11]. Some works investigated the virus behavior containing the stability analysis of WSNs [14, 27, 38].

Considering a WSN composed of a number of sensors, the transmission rates for different worms vary based on the distinct mechanism embedded in the sensors. That means that for different worms and sensors, the dynamic behavior will vary [7, 37]. Meanwhile, both scan-based and topology-based propagation strategies select the targets based on the features related to the sensors [25, 35]. Since there is a basic similarity between worm propagation through wireless devices and the information diffusion process over the regular network, from this standpoint, we propose a discrete communication model based on the competitive diffusion models under multiple worms. We seek to learn our proposed model to derive the dynamics of competitive worms propagation analytically. Our contributions can be summarized as follows.

- **Propagation Model Design.** We design a communication model that simulates the propagation of the competitive worm. Our model includes the special case with the hybrid dynamics with virus and patch, which provides a new aspect to the antivirus protection design.
- **Searching Space Analysis.** We develop a new searching space combined with the complex-valued neural network. To our best knowledge, this provides a starting point for analyzing the worms propagation model.
- **Empirical Studies.** We provide experimental validation of our model compared with some baseline methods.

The paper is organized as follows. In the next section, we introduce some related works of the different propagation models. Section 3 illustrates the structure of the communication model and formulates the learning problem. Section 4 describes the learning framework, including the searching space design and the learning algorithm. Experiments are given in Sect. 5.

## 2 Related Work

A large number of models have been proposed to analyze the dynamics of worm propagation in WSNs based on epidemic models. Kephart et al. first proposed the idea of formulating the worm's propagation based on simple epidemic models. They assumed each sensor or host stays in one of two states: susceptible or infectious. And the infected sensor will not change its infectious state [15]. In recent works, Abdel et al. proposed an extension SIR model by considering antivirus dynamics that add the antidotal state to each sensor [1]. And the authors present a unified study of the epidemic-antivirus nonlinear dynamical system. The work in [2] designed a fractional-order compartmental epidemic model by accounting for the global stability analysis. Several studies added the quarantined constraints for each sensor to the epidemic models [16, 20, 21].

For multiple worms propagation, authors in [32] proposed a model that supports the sleep and work interleaving schedule policy for the sensor nodes. They assigned different infect probabilities to each worm when the infected nodes attempted to infect other nodes. However, they did not specify the relationship among these worms, and it is hard to track the dynamic of different worms. [24] developed a SEjIjR-V Epidemic Model with differential exposure, infectivity, and communication Range. Besides, they generate the epidemic thresholds for each sensor corresponding to different worms. In our work, we formulate a worms propagation model based on the works in [23, 33]. And inspired by them, we develop an explicitly complex-valued neural network to exactly simulate the worms' propagation process.

## 3 Preliminaries

In this section, we present the communication model and problem settings.

### 3.1 Communication Model

We consider the wireless network as a directed graph  $G = (V, E)$ , where  $V$  and  $E$  denote the sensors and the communication links, respectively. Let  $|V| = N$  and  $|E| = M$ . For each node  $v$ , its in-neighbors is denoted by  $N_v \subseteq V$ . It is assumed that  $K$  different worms are spread over the network, and each worm  $k \in [K]$  propagates from a set of sensors  $S^k \in V$ . For each node  $v \in V$ , there is a set of threshold  $\Theta_v = \{\theta_v^1, \dots, \theta_v^K\}$  that represents its vulnerabilities to different worms, where  $\theta \in [0, \infty)$ . For each edge  $(u, v) \in E$ , there is a set of weights  $W_{(u,v)} = \{w_{(u,v)}^1, \dots, w_{(u,v)}^K\}$  indicates its levels of transmission with different worms, where  $w \in [0, \infty)$ . We assume that a node can only be infected by one worm and suppose that the spread of worms continuous step by step based on the following rules.

- Initialization. For nodes  $v \in S^k$ , they are  $k$ -infected; Otherwise, the nodes stay innocent.

- Step  $t$ . There are two stages during each step. Let  $S_{t-1}^k \subseteq V$  be the  $k$ -infected nodes at the end of step  $t-1$ .
  - Stage 1. For each innocent node  $v$ , it can be possibly infected by the worms in set  $P_v^t \subseteq [K]$ , where

$$P_v^t = \left\{ k \mid \sum_{u \in N_v \cap S_{t-1}^k} w_{(u,v)}^k \geq \theta_v^k \right\}. \quad (1)$$

- Stage 2. Node  $v$  will finally be infected by worm  $k^*$  such that

$$k^* = \arg \max_{k \in P_v^t} \sum_{u \in N_v \cap S_{t-1}^k} w_{(u,v)}^k \quad (2)$$

Once a node is infected, its status will not change during the propagation. For tie breaking, each node is more vulnerable with the worm with a large index.

- Termination. The propagation process ends when no nodes can be infected. We can observe that  $t \leq N$ .

### 3.2 Problem Settings

We begin by presenting some notations that are used in the rest of the paper.

**Notations.** For a complex number  $a+ib$ ,  $a$  is the real part and  $b$  is the imaginary part, where  $a, b \in \mathbb{R}$ . For convenience, we use  $(a, b)$  to simplify the notation. During the propagation process, for a step  $t \in [N]$ , we denoted the status of each node  $v \in V$  by a complex-valued vector  $I_t(v) \in \mathbb{C}^K$ : If  $v$  is  $k$ -infection, then the  $k_{th}$  element in  $I_t(v)$  is  $1 + i0$  and the rest elements are  $0 + i0$ ; If  $v$  is a innocent node, then all the elements in  $I_t(v)$  are  $0 + i0$ . The status over all nodes, named all-infection status, is then formulated as a matrix  $\mathcal{I}_t \in \mathbb{C}^{K \times N}$  by concatenating  $I_t$  for each node, where  $\mathcal{I}_{t,v} = I_t(v)$ . Furthermore, to simplify, we assume that  $K = 2^p$  where  $p \in \mathbb{Z}^+$ .

We are interested in learning propagation functions given the collected propagation data.

**Definition 1.** Given a network graph and a communication model, the propagation function  $F : \mathbb{C}^{K \times N} \rightarrow \mathbb{C}^{K \times N}$  maps from initial all-infection status  $\mathcal{I}_0$  to the final status  $\mathcal{I}_N$ .

**Definition 2.** The propagation data set  $D$  is a set of initial-final status pairs with size  $Q \in \mathbb{Z}^+$ , where

$$D = \{(\mathcal{I}_0, \mathcal{I}_N)^i\}_{i=1}^Q. \quad (3)$$

Given a new initial-final status pair  $(\mathcal{I}_0, \mathcal{I}_N)$ , let  $\hat{\mathcal{I}}_N$  be the predicted final all-infection status, we use  $l$  to measuring the loss.

$$l(\hat{\mathcal{I}}_N, \mathcal{I}_N) = \frac{1}{N} |\{v : \hat{\mathcal{I}}_{N,v} \neq \mathcal{I}_{N,v}, v \in V\}| \quad (4)$$

The problem can be formally defined as follows.

*Problem 1.* Given the graph structure  $G$  and a set of propagation data  $D$  draw from some distribution  $\mathcal{D}$ , we wish to find a propagation function  $F: \mathbb{C}^{K \times N} \rightarrow \mathbb{C}^{K \times N}$ , that minimizes the generalization error  $L$ , where

$$L(F) = \mathbb{E}_{(\mathcal{I}_0, \mathcal{I}_N) \sim \mathcal{D}} l(F(\mathcal{I}_0), \mathcal{I}_N) \quad (5)$$

## 4 A Learning Framework

In this section, for the communication model, we first design a searching space that composed by the complex neural network. Then the learning algorithm is proposed given such searching space.

### 4.1 Hypothesis Space Design

In this section, we construct the hypothesis space for Problem 1 by simulating the propagation process as a finite complex-valued Neural Network (CVNNs) from local to global. Assume that for the complex-valued neuron  $n$  at layer  $l+1$ , it is linked with  $m$  numbers of neurons in the previous layer, then the output of neuron  $n$  is described as follows:

$$H_n^{l+1} = \sigma_n^{l+1} \left( \sum_{i=1}^m W_{in}^l H_i^l + T_n^l \right) \quad (6)$$

Here  $W_{in}^l$  denotes the weight connecting the neuron  $n$  and the neuron  $i$  from the previous layer,  $\sigma_n^{l+1}$  denotes the activation function on neuron  $n$ ,  $T_n^l$  is the bias term.

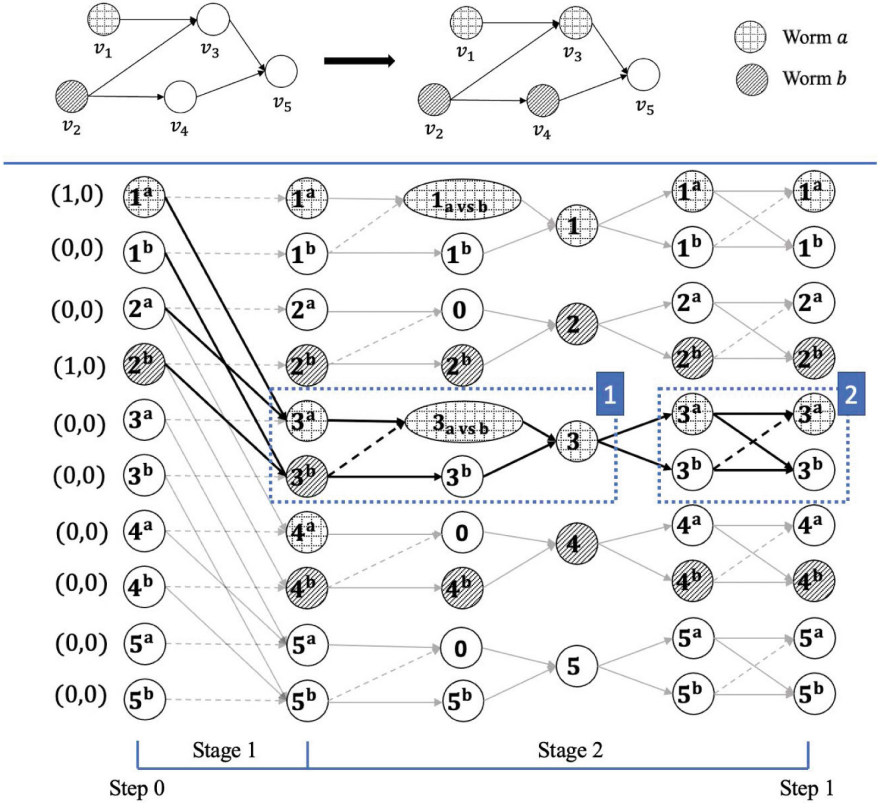
**Local Propagation.** For the local propagation, it simulates the diffusion process during every step  $t$ . It starts by receiving the all-infection status  $\mathcal{I}_t \in \mathbb{C}^{K \times N}$  at the end of step  $t$ . Figure 1 illustrates an example of local propagation process.

**Stage 1.** We aim to find out all the possible worms that can infect the each innocent nodes. During this stage, each worm diffuses separately and follows a linear threshold process. Therefore, we wish the links between the layers represents the topology in the WSNs and the activation function can be simply defined as the threshold functions. In addition, the communication model indicates that once a node is affected, it will never change the status. Therefore, for each node, we add one link towards it self at the next layer with a relatively large value. The propagation can be simulated by

$$\mathbf{H}^2 = \sigma^1(\mathbf{W}^1 \mathbf{H}^1 + \mathbf{T}^1), \quad (7)$$

where for  $i, j \in [N]$  and  $k, l \in [K]$ , we have

$$\mathbf{W}_{i \cdot K+k, j \cdot K+l}^1 := \begin{cases} (w_{(i,j)}^k, 0) & \text{if } (i, j) \in E \text{ and } k = l \\ 1000 & \text{if } i = j \text{ and } k = l \\ (0, 0) & \text{otherwise} \end{cases}$$



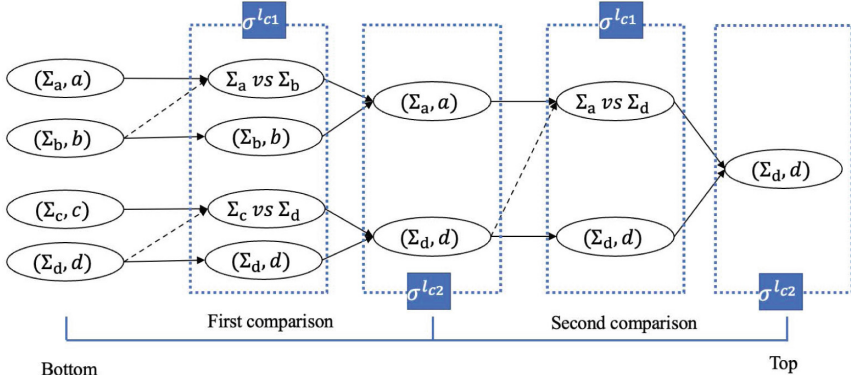
**Fig. 1. Local propagation structure.** Suppose that two competitive worms are disseminated in the network. The top part of the figure shows the propagation process during one step across a small WSN. The neural network below shows the corresponding designed neural network during one step and each stages are simulated by several layers. We focus on the activation flow on node 3 using highlight lines. Specially, the idea of the structure in the boxes labeled with 1 and 2 are discussed in Fig. 2 and 3.

$$\sigma_{j \cdot K+l}^1(x) := \begin{cases} x & \text{if } \text{Re}(x) \geq \theta_j^l \\ (0, 0) & \text{Otherwise} \end{cases}. \quad (8)$$

$$T_{j \cdot K+l}^1(x) := (0, l) \quad (9)$$

**Stage 2.** With the input  $\mathbf{H}^2$  from phase 1, this stage determines the final infect status of each node. That is for a node  $i \in V$ , we want to find out the largest value among the sub-array

$$\left[ \text{Re}(\mathbf{H}_{i+1}^2), \text{Re}(\mathbf{H}_{i+2}^2), \dots, \text{Re}(\mathbf{H}_{i+K}^2) \right]. \quad (10)$$



**Fig. 2. Hierarchy structure of pairwise comparisons.** This figure shows the structure of box 1 in Fig. 1. To better illustration, suppose that there are four different worms:  $a, b, c$  and  $d$  and thereby with two pairwise comparison. The nodes in the bottom layer represent the sub-array 10. All the weights on the solid links are  $1 + i0$  and the weights on the dash links are  $-1 + i0$ . During each comparison process, the first layer implements the activation function in Eq. 11 such that: if the prior one has the larger value of real part, the node returns the difference; Otherwise, it will return  $(0, 0)$ . Therefore, by combining the second layer  $l^{c2}$ , the output is exactly the larger value between two nodes.

Intuitively, finding the largest value among Eq. 10 can be implemented through a hierarchy structure of pairwise comparisons. Starting from the sub-array, each hierarchy compares every two neighboring elements and passing the larger value to the next level, which leads to a  $P$  hierarchy levels structure.

From bottom to top, for node  $v \in [N]$ , in each hierarchy level  $p \in [P]$ , the size of input elements  $I_p = \frac{K}{2^{p-1}}$  and the size of output elements  $O_p = \frac{K}{2^p}$ . Each level can be decoded by two layers:  $l^{c1}$  and  $l^{c2}$ .

In  $l^{c1}$ , for  $i, j \in [I_p]$ ,

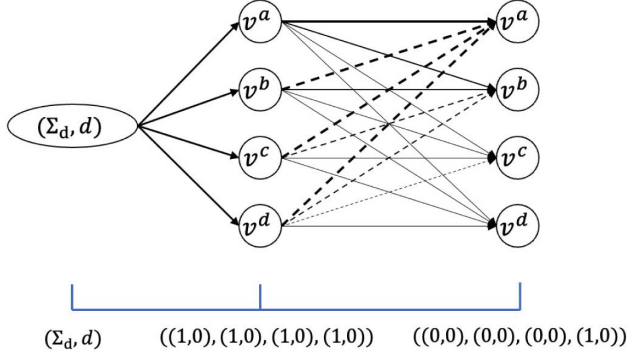
$$\mathbf{W}_{i,j}^{l^{c1}} := \begin{cases} (1, 0) & \text{if } i = j \\ (0, -1) & \text{if } j = i - 1 \text{ for } j = 2n + 1 \text{ where } n \in \{0, 1, 2, \dots, I_p - 1\} \\ (0, 0) & \text{otherwise} \end{cases}$$

$\sigma^{l^{c1}}$  is defined as follows:

$$\sigma^{l^{c1}}(x) := \begin{cases} (\text{Im}(x), \text{Re}(x)) & \text{if } \text{Im}(x) \geq 0 \\ (0, 0) & \text{otherwise} \end{cases} \quad (11)$$

In  $l^{c2}$ , for  $i \in [I_p]$  and  $j \in [O_p]$ ,

$$\mathbf{W}_{i,j}^{l^{c2}} := \begin{cases} (1, 0) & \text{if } i = 2 \cdot j \text{ or } i = 2 \cdot j - 1 \\ (0, 0) & \text{otherwise} \end{cases}$$



**Fig. 3. Structure of the format adjustment.** This figure shows the structure of box 2 in Fig. 1. Suppose that there are four different worms:  $a, b, c$  and  $d$ . For a node  $v \in V$ , at the end of one step, we assume it is  $d$ -active. All the weights on the solid links are  $1+i0$  and the weights on the dash links are  $-1+i0$ . In addition, the threshold on each node  $v^k$  of each layer is  $k$ , where  $k \in \{a, b, c, d\}$ . The bottom vectors in the figure below shows the format of each layer.

$\sigma^{l_{c_2}}$  is defined as follows.

$$\sigma^{l_{c_2}}(x) := x$$

By repeatedly using these two layers  $P$  times, the output of stage 2 is  $\mathbf{H}^{2P+2} \in \mathbb{C}^N$ . For  $i \in [N]$  and  $k \in [K]$ , each node in  $\mathbf{H}^{2P+2}$  holds the value as follows,

$$\mathbf{H}_i^{2P+2} = \left( \max_{k \in K} \{\text{Re}(\mathbf{H}_{i+k}^2)\}, \arg \max_{k \in K} \{\text{Re}(\mathbf{H}_{i+k}^2)\} \right), \quad (12)$$

where the real part for each node  $i$  indicates the largest incoming weights among all the worms, and the imaginary part is the corresponding worm index.

**Format Adjustment.** In order to simulate the global worm propagation process, we need to make the format of the output at the end of local propagation be same as the input, that is  $\mathbf{H}^{2Z+3} = \mathcal{I}_{t+1} \in \mathbb{C}^{K \times N}$ . Two layers are added. Figure 3 shows an example of the structure of the format adjustment. The two layers can be formulated as follows.

$$\mathbf{H}^{2P+2+i} = \sigma^{2Z+2+i}(\mathbf{W}^{2Z+2+(i-1)} \mathbf{H}^{2Z+2+(i-1)}), \quad (13)$$

where  $i = \{1, 2\}$ . The first layer can be seen as a transition layer. The number of the output nodes will be recovered as the input, and the real number of each node are set to 0. For the imaginary part, its value will be equal to 1 if the node's corresponding worm's index is no large than the real part in Eq. 12. Therefore, it is formulated as follows. For each  $i, j \in [N]$ ,  $k \in [K]$ , we have

$$\mathbf{W}_{i \cdot K, j \cdot K+k}^{2P+3} := \begin{cases} (1, 0) & \text{if } i = j \\ (0, 0) & \text{otherwise} \end{cases}$$

and

$$\sigma_{j \cdot K+k}^{2P+3}(x) := \begin{cases} (1, 0) & \text{if } \text{Im}(x) \text{ and } \text{Im}(x) \geq k \\ (0, 0) & \text{Otherwise} \end{cases}. \quad (14)$$

The last layer are designed to extract the all-infection status at the end of local propagation, and that is  $\mathbf{H}^{2P+4} = \mathcal{I}_t$

where for each  $i, j \in [N]$ ,  $k, l \in [K]$ , we have

$$\mathbf{W}_{i \cdot K+k, j \cdot K+l}^{2P+4} := \begin{cases} (1, 0) & \text{if } i = j \text{ and } l \geq k \\ (-1, 0) & \text{if } i = j \text{ and } l < k \\ (0, 0) & \text{otherwise} \end{cases}$$

and

$$\sigma_{j \cdot K+l}^{2P+4}(x) := \begin{cases} (1, 0) & \text{if } \text{Re}(x) > l \\ (0, 0) & \text{Otherwise} \end{cases}. \quad (15)$$

We can then obtain the following lemma.

**Lemma 1.** *The local propagation under transmission model can be simulated by a complex neural network with  $2P + 4$  layers.*

**From Local to Global.** The output of local propagation complex neural network can be viewed as the input for the next time step. We can repeatedly using the local network to exactly simulated the whole propagation process. We denoted such global complex neural network by  $M_C$ . Therefore, we can obtain our hypothesis space of Problem 1.

**Definition 3.** *Taking the weights  $W_{(u,v)}$  for  $(u, v) \in E$  and thresholds  $\Theta_v$  for  $v \in V$  as the parameters, the hypothesis space  $\mathcal{F}$  is the set of all possible  $M_C$ .*

## 4.2 Learning Algorithm

Given the hypothesis space  $\mathcal{F}$ , the propagation function  $F$  based on the propagation model is now implemented as a complex neural network model. Instead of directly learning the  $F$ , we seek to learn a complex neural network model from  $\mathcal{F}$  that can minimize the generalization error in Eq. 5. Same as the neural network, learning in complex neural networks refers to the process of modifying the parameters involved in the network such that the learning objectives can be achieved. And it is natural to use a gradient-based approach to reach our learning goals. [13] shows that it is unnecessary to limit using the activation functions that are complex differentiable, or holomorphic, and they state that those functions that are differentiable with respect to the real part and the imaginary part of each parameter are also compatible with backpropagation. Following this idea,

**Table 1. Main results.** Each simulation is implemented with 600 training samples, 400 testing samples and 4 worms.

		F1 score	Precision	Recall	Accuracy
ER graph	Proposed method	0.469 <sub>(6.E-03)</sub>	0.419 <sub>(6.E-03)</sub>	0.629 <sub>(6.E-03)</sub>	0.727 <sub>(3.E-03)</sub>
	RegularNN	0.408 <sub>(4.E-03)</sub>	0.329 <sub>(4.E-03)</sub>	0.590 <sub>(6.E-03)</sub>	0.695 <sub>(3.E-03)</sub>
	SVM	0.184 <sub>(0)</sub>	0.192 <sub>(0)</sub>	0.201 <sub>(0)</sub>	0.498 <sub>(1.E-03)</sub>
	Random	0.182 <sub>(2.E-03)</sub>	0.200 <sub>(2.E-03)</sub>	0.200 <sub>(2.E-03)</sub>	0.200 <sub>(2.E-03)</sub>
Sensors network	Proposed method	0.408 <sub>(1.E-02)</sub>	0.372 <sub>(1.E-02)</sub>	0.575 <sub>(1.E-02)</sub>	0.684 <sub>(6.E-03)</sub>
	RegularNN	0.208 <sub>(1.E-02)</sub>	0.302 <sub>(6.E-02)</sub>	0.450 <sub>(3.E-02)</sub>	0.597 <sub>(3.E-03)</sub>
	SVM	0.146 <sub>(8.E-04)</sub>	0.117 <sub>(3.E-03)</sub>	0.205 <sub>(3.E-04)</sub>	0.537 <sub>(3.E-03)</sub>
	Random	0.176 <sub>(7.E-03)</sub>	0.200 <sub>(4.E-03)</sub>	0.200 <sub>(8.E-03)</sub>	0.199 <sub>(7.E-03)</sub>

we initialized two groups of parameters corresponding to the real and imaginary parts and trained them separately. And we utilize the complexPytorch package, a high-level API of PyTorch, to implement layers and functions [5, 18, 31]. Note that, in the activation function 8, 14 and 15, they are not differentiable everywhere. We use a tanh function to approximately return the gradients during the training.

## 5 Experiments

In this section, we evaluated our proposed method by experiments. We compare our method with several baseline algorithm on synthetic and real worlds networks.

### 5.1 Settings

**WSN Data.** We adopt two types of graph structures to evaluate our proposed method: one synthetic graph and a real-world WSN. One synthetic graph is a randomly generated Erdős-Rényi (ER) graph with 200 nodes and 0.2 edge probability [8]. The real-world WSN is collected from 54 sensors deployed in the Intel Berkeley Research lab<sup>1</sup>.

**Communication Model and Sample Generating.** The number of worms are select from 2, 4, 8. For each node  $v$ , the threshold value of worm  $k$ ,  $\theta_v^k$ , is generated uniformly random from  $[0, 1]$ . The weight on each edge  $(u, v)$  of worm  $k$  is set as  $w_{(u,v)}^k = \frac{1}{|N_v|+k}$ . For each graph, we generate a sample pool  $D = \{(\mathcal{I}_0, \mathcal{I}_N)^i\}_i^{1000}$  with  $N/2$  seeds and each seed is selected uniformly at random. Each selected seed node is assigned to worm uniformly at random. Given  $\mathcal{I}_0, \mathcal{I}_N$  is generated follow the communication model (Table 3).

<sup>1</sup> <http://db.csail.mit.edu/labdata/labdata.html>.

**Table 2. Impact of the different number of worms.** Each simulation is implemented with 600 training samples, 400 testing samples, and 100 seeds.

Number of worms	F1	Precision	Recall	Accuracy
2	0.717 <sub>(3.E-02)</sub>	0.657 <sub>(1.E-02)</sub>	0.948 <sub>(3.E-02)</sub>	0.803 <sub>(2.E-02)</sub>
4	0.469 <sub>(6.E-03)</sub>	0.419 <sub>(6.E-03)</sub>	0.629 <sub>(6.E-03)</sub>	0.727 <sub>(3.E-03)</sub>
8	0.277 <sub>(4.E-03)</sub>	0.206 <sub>(5.E-03)</sub>	0.313 <sub>(5.E-03)</sub>	0.656 <sub>(3.E-03)</sub>

**Table 3. Impact of the different number of seeds.** Each simulation is implemented with 600 training samples, 400 testing samples, and 4 worms.

Number of seeds	F1 score	Precision	Recall	Accuracy
50	0.332 <sub>(4.E-03)</sub>	0.277 <sub>(4.E-03)</sub>	0.579 <sub>(7.E-03)</sub>	0.676 <sub>(4.E-03)</sub>
100	0.469 <sub>(6.E-03)</sub>	0.419 <sub>(6.E-03)</sub>	0.629 <sub>(6.E-03)</sub>	0.727 <sub>(3.E-03)</sub>
150	0.549 <sub>(5.E-03)</sub>	0.524 <sub>(4.E-03)</sub>	0.626 <sub>(4.E-03)</sub>	0.733 <sub>(3.E-03)</sub>

**Baseline Method.** We consider two baseline algorithms: RegularNN and Support Vector Machine (SVM). RegularNN is a real-valued deep neural network model with  $4 \cdot N$  layers. The activation functions are set as a combination of linear, ReLU, and sigmoid. We aim to compare ComplexNN, which explicitly simulates the diffusion process, with the regular designed neural network. Since the proposed problem is a binary classification task, we implement the SVM algorithm. Besides, the random method with a random prediction is also considered.

**Implementation.** The size of the training set is selected from  $\{200, 400, 600\}$  and the testing size is 400. During each simulation, the train and test samples are randomly selected from the sample pool. For each method, we use F1 score, precision, recall, and accuracy to evaluate the performance. Besides, the number of simulations for each setting is set to 5, and we report the average performance together with the standard deviation.

## 5.2 Observations

Table 1 shows the main results. Each cell includes the average value and its corresponding standard deviation. We can observe that our method outperforms other methods. Compared to the RegularNN, the proposed method are able to improve the prediction errors. And this shows the advantage of using an explicit model. Besides, it shows that the performance of each algorithm is increased given a larger graph.

**Impact of Number of Worms.** Table 2 gives the simulation results for our proposed method under the different numbers of worms. We can observe that with a lower number of worms, the performance is improved. One plausible reason is that the number of worms determines the size of the number of input

and output features for our model. And it meets the nature of neural network training properties.

**Imbalanced Class Distribution.** The simulation results for our proposed method under the different number of seeds are given in Table 2. We see that the performance is increased when more seeds are provided. Since our model is a binary classifier, a small number of seeds leads to an imbalance class distribution. It is an inherent issue in predicting the node status in that the majority of the nodes tend to be inactive.

## 6 Conclusion

In this paper, we formulate a propagation model for multiple worms and propose a complex-valued neural network model. In particular, our designed complex-valued neural network model simulates the propagation process exactly. Overall our method outperforms classic supervised learning methods. However, it is not sufficiently stable for different data within the different numbers of worms and seeds. And it is possible that there exists an advanced representation strategy for the neural network design that can achieve a better performance, which is one direction for our future work. In addition, encouraged by the possibility of using a complex-valued neural network to simulate the worms' propagation models, we believe it would be interesting to apply our method to the traditional epidemic model.

## References

1. Abdel-Gawad, H.I., Baleanu, D., Abdel-Gawad, A.H.: Unification of the different fractional time derivatives: an application to the epidemic-antivirus dynamical system in computer networks. *Chaos, Solitons Fractals* **142**, 110416 (2021)
2. Achar, S.J., Baishya, C., Kaabar, M.K.: Dynamics of the worm transmission in wireless sensor network in the framework of fractional derivatives. *Math. Methods Appl. Sci.* **45**(8), 4278–4294 (2022)
3. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. *Comput. Netw.* **38**(4), 393–422 (2002)
4. Awasthi, S., Kumar, N., Srivastava, P.K.: A study of epidemic approach for worm propagation in wireless sensor network. In: Solanki, V.K., Hoang, M.K., Lu, Z.J., Pattnaik, P.K. (eds.) *Intelligent Computing in Engineering. AISC*, vol. 1125, pp. 315–326. Springer, Singapore (2020). [https://doi.org/10.1007/978-981-15-2780-7\\_36](https://doi.org/10.1007/978-981-15-2780-7_36)
5. Bassey, J., Qian, L., Li, X.: A survey of complex-valued neural networks. arXiv preprint [arXiv:2101.12249](https://arxiv.org/abs/2101.12249) (2021)
6. Behal, K.S., Gakkhar, S., Srivastava, T.: Dynamics of virus-patch model with latent effect. *Int. J. Comput. Math.* **99**, 1–16 (2022)
7. Chakrabarti, D., Leskovec, J., Faloutsos, C., Madden, S., Guestrin, C., Faloutsos, M.: Information survival threshold in sensor and p2p networks. In: *IEEE INFOCOM 2007–26th IEEE International Conference on Computer Communications*, pp. 1316–1324. IEEE (2007)

8. Erdős, P.: Graph theory and probability. *Can. J. Math.* **11**, 34–38 (1959)
9. Galluccio, L., Morabito, G.: Impact of worm propagation on vehicular sensor networks exploiting v2v communications. In: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 1–6. IEEE (2019)
10. Gulati, K., Boddu, R.S.K., Kapila, D., Bangare, S.L., Chandnani, N., Saravanan, G.: A review paper on wireless sensor network techniques in internet of things (IoT). *Mater. Today Proc.* **51**, 161–165 (2021)
11. Haghghi, M.S., Wen, S., Xiang, Y., Quinn, B., Zhou, W.: On the race of worms and patches: modeling the spread of information in wireless sensor networks. *IEEE Trans. Inf. Forensics Secur.* **11**(12), 2854–2865 (2016)
12. Han, X., Tan, Q.: Dynamical behavior of computer virus on internet. *Appl. Math. Comput.* **217**(6), 2520–2526 (2010)
13. Hirose, A., Yoshida, S.: Generalization characteristics of complex-valued feedforward neural networks in relation to signal coherence. *IEEE Trans. Neural Netw. Learn. Syst.* **23**(4), 541–551 (2012)
14. Hu, Z., Wang, H., Liao, F., Ma, W.: Stability analysis of a computer virus model in latent period. *Chaos, Solitons Fractals* **75**, 20–28 (2015)
15. Kephart, J.O., White, S.R., Chess, D.M.: IEEE spectrum. *Comput. Epidemiol.* **30**(5), 20–26 (1993)
16. Khanh, N.H.: Dynamics of a worm propagation model with quarantine in wireless sensor networks. *Appl. Math. Inf. Sci* **10**(5), 1739–1746 (2016)
17. Krishnamachari, B.: *Networking Wireless Sensors*. Cambridge University Press, Cambridge (2005)
18. Matthès, M.W., Bromberg, Y., de Rosny, J., Popoff, S.M.: Learning and avoiding disorder in multimode fibers. *Phys. Rev. X* **11**(2), 021060 (2021)
19. Mishra, B.K., Keshri, N.: Mathematical model on the transmission of worms in wireless sensor network. *Appl. Math. Model.* **37**(6), 4103–4111 (2013)
20. Mishra, B.K., Tyagi, I.: Defending against malicious threats in wireless sensor network: a mathematical model. *Int. J. Inf. Technol. Comput. Sci.* **6**(3), 12–19 (2014)
21. Mishra, B.K., Srivastava, S.K., Mishra, B.K.: A quarantine model on the spreading behavior of worms in wireless sensor network. *Trans. IoT Cloud Comput.* **2**(1), 1–12 (2014)
22. Nain, M., Goyal, N.: Localization techniques in underwater wireless sensor network. In: 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 747–751. IEEE (2021)
23. Narasimhan, H., Parkes, D.C., Singer, Y.: Learnability of influence in networks. In: *Advances in Neural Information Processing Systems*, vol. 28 (2015)
24. Nwokoye, C., Umeugoji, C., Umeh, I.: Evaluating degrees of differential infections on sensor networks' features using the seijjr-v epidemic model. *Egypt. Comput. Sci. J.* **44**(3) (2020)
25. Nwokoye, C.N.H., Madhusudanan, V.: Epidemic models of malicious-code propagation and control in wireless sensor networks: an indepth review. *Wirel. Per. Commun.* **125**, 1–30 (2022). <https://doi.org/10.1007/s11277-022-09636-8>
26. Ojha, R.P., Srivastava, P.K., Sanyal, G., Gupta, N.: Improved model for the stability analysis of wireless sensor network against malware attacks. *Wirel. Pers. Commun.* **116**(3), 2525–2548 (2021)
27. Qin, P.: Analysis of a model for computer virus transmission. *Math. Prob. Eng.* **2015** (2015)

28. Rajesh, B., Reddy, Y.J., Reddy, B.D.K.: A survey paper on malicious computer worms. *Int. J. Adv. Res. Comput. Sci. Technol.* **3**(2), 161–167 (2015)
29. Regin, R., Rajest, S.S., Singh, B.: Fault detection in wireless sensor network based on deep learning algorithms. *EAI Trans. Scalable Inf. Syst.* **8**, e8 (2021)
30. Srivastava, A.P., Awasthi, S., Ojha, R.P., Srivastava, P.K., Katiyar, S.: Stability analysis of SIDR model for worm propagation in wireless sensor network. *Indian J. Sci. Technol.* **9**(31), 1–5 (2016)
31. Trabelsi, C., et al.: Deep complex networks. In: *International Conference on Learning Representations* (2018). <https://openreview.net/forum?id=H1T2hmZAb>
32. Wang, X., Li, Q., Li, Y.: EiSiRS: a formal model to analyze the dynamics of worm propagation in wireless sensor networks. *J. Comb. Optim.* **20**(1), 47–62 (2010)
33. Wang, Y., Tong, G.: Learnability of competitive threshold models. In: Raedt, L.D. (ed.) *Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence, IJCAI-22*, pp. 3985–3991. *International Joint Conferences on Artificial Intelligence Organization* (2022). <https://doi.org/10.24963/ijcai.2022/553>. main Track
34. Wang, Y., Wen, S., Cesare, S., Zhou, W., Xiang, Y.: The microcosmic model of worm propagation. *Comput. J.* **54**(10), 1700–1720 (2011)
35. Wang, Y., Wen, S., Xiang, Y., Zhou, W.: Modeling the propagation of worms in networks: a survey. *IEEE Commun. Surv. Tutorials* **16**(2), 942–960 (2013)
36. Weaver, N., Paxson, V., Staniford, S., Cunningham, R.: A taxonomy of computer worms. In: *Proceedings of the 2003 ACM workshop on Rapid Malcode*, pp. 11–18 (2003)
37. Yao, Y., Sheng, C., Fu, Q., Liu, H., Wang, D.: A propagation model with defensive measures for PLC-PC worms in industrial networks. *Appl. Math. Model.* **69**, 696–713 (2019)
38. Zarin, R., Khaliq, H., Khan, A., Khan, D., Akgül, A., Humphries, U.W.: Deterministic and fractional modeling of a computer virus propagation. *Results Phys.* **33**, 105130 (2022)
39. Zou, C.C., Towsley, D., Gong, W., Cai, S.: Routing worm: A fast, selective attack worm based on IP address information. In: *Workshop on Principles of Advanced and Distributed Simulation (PADS'05)*, pp. 199–206. *IEEE* (2005)