Performance-aware Malware Epidemic Confinement in Large-Scale IoT Networks

Rakibul Hassan*, Setareh Rafatirad†, Houman Homayoun†, and Sai Manoj Pudukotai Dinakarrao*
*Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA, USA
†Department of Electrical and Computer Engineering, University of California Davis, Davis, CA, USA
*{rhassa2, spudukot}@gmu.edu; †{srafatir, hhomayoun}@ucdavis.edu

ICC 2021 - IEEE International Conference on Communications | 978-1-7281-7122-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICC42927.2021.9500476

***Abstract*—As millions of IoT devices are interconnected together for better communication and computation, compromising even a single device opens a gateway for the adversary to access the network leading to an epidemic. It is pivotal to detect any malicious activity on a device and mitigate the threat. Among multiple feasible security threats, malware (malicious applications) poses a serious risk to modern IoT networks. A wide range of malware can replicate itself and propagate through the network via the underlying connectivity in the IoT networks making the malware epidemic inevitable. There exist several techniques ranging from heuristics to game-theory based technique to model the malware propagation and minimize the impact on the overall network. The state-of-the-art game-theory based approaches solely focus either on the network performance or the malware confinement but does not optimize both simultaneously. In this paper, we propose a throughput-aware game theory-based end-to-end IoT network security framework to confine the malware epidemic while preserving the overall network performance. We propose a two-player game with one player being the attacker and other being the defender. Each player has three different strategies and each strategy leads to a certain gain to that player with an associated cost. A tailored min-max algorithm was introduced to solve the game. We have evaluated our strategy on a 500 node network for different classes of malware and compare with existing state-of-the-art heuristic and game theory-based solutions.**

I. Introduction

In the recent years, the number of IoT devices is increasing tremendously at a pace never imagined. It is expected that by the year 2025, the number of IoT device will reach to 75 billion [1]. The concept of IoT has brought revolutionary impact in various domains such as smart homes, smart grid, mobile health, as well as military applications. Unfortunately, a majority of the IoT devices lack the security measures and capabilities due to cost and complexity trade-offs. As a consequence, these devices are vulnerable and experiencing an ever increasing security threats [2].

Several reasons account for the IoT devices being a potential target to the attackers for injecting threats. Firstly, security measures are minimally embedded in the IoT devices due to resource and cost constraints [2]. Thus, they become a soft target to the attackers. Further, given that there are millions of interconnected devices and majority of them have insufficient security measures, make the attack surface even larger. One compromised device can function as a gateway and facilitate the threat to propagate throughout the network leading to a catastrophe. Among multiple threats, malware is a prominent threat to IoT networks and devices [3], [4]. For instance, Mirai IoT bots launched a Distributed Denial-of-Service (DDoS) attack by hacking the CCTVs that lead to partial shut down of the internet on the east coast of the USA in 2017 [5]. Some other recent attacks that targeted IoT devices are wannacry ransomware, Petya cyberattacks to name a few. Such threats are exacerbating at an alarming rate, with IoT malware increased by 20% in Q2 of 2020 compared to that of first quarter [6].

We have learned from the recent attacks [5], a cyber-attack can be launched from a single compromised node such as router, surveillance camera, smartphone or even a smart bulb [7] and be able to propagate to the whole network. The connectivity and the scale of the networks make the mitigation challenging, and given the scale of networks, traditional solutions such as rebooting or isolation of a device are ineffective, costly and impractical. To that context, isolating a device will not be an intelligent confinement strategy as that could cripple the communication between the devices and lower the desired performance metrics such as throughput and latency of the network. On the contrary, leaving the devices connected in the presence of malware can severely hamper the network integrity and facilitate malware to propagate throughout the network. To strike a balance between these contradictory goals, we propose a performance-aware game theory-based technique to confine the spread of the malware.

Recent works on malware confinement such as [8] focuses only to limit the infection without considering the performance enhancement and integrity of the network. Thus, we address a critical problem of confining the malware epidemic spread while preserving the network performance. The contributions of this work to limit the spread as well as maintaining the overall performance metrics can be outlined in two-fold manner as follows:

- We propose a game-theoretic framework with a payoff function that considers the network performance along with the attacker's and the defender's cost for implementing their strategy. Thus, the optimal payoff value among all the possible payoff combinations ensures the malware confinement while maintaining the network throughput.
- Our evaluation on different epidemic models show that the proposed solution not only confines the malware spread but also maintains a higher throughput with minimal defense cost.

II. State-of-the-Art

Significant number of works have analyzed the adverse impacts of malware spreading and possible confinement strategies in the IoT networks in the recent times [9]. Two major approaches are explored to confine the malware in networks: a) control theory; and b) game theory. Some of the preliminary

978-1-7281-7122-7/21/$31.00 ©2021 IEEE

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:38:50 UTC from IEEE Xplore. Restrictions apply.

works utilizes control theory for malware confinement. For instance, [10] formulates the malware epidemic as a Pontryagin's maximum principle and perform receiver gain modification to confine the malware where quarantining of malware through power control is proposed. In a similar manner, confinement of malware by optimizing the rate of communication between nodes is proposed in [11], limiting the communication to the peers. Though these works intend to confine the malware, they are primarily based on the heuristics and simplifications which does not lead to optimal solutions [9].

Game-theory based confinement solution has gained popularity among the researchers in the recent times as the solutions obtained from the game-theory lead to minimize the damage from the attacker with minimum cost. Furthermore, the game-theory based solutions are relatively less complex compared to that of control theory-based solutions for large-scale networks. A dynamic zero-sum game is proposed in [12] where the attacker and the defender can adopt their strategies dynamically targeting to obtain maximum gain for themselves. They formed their game to model the strategic confrontations of malware and limit the propagation through annihilation, patching and adapting reception rates as a defense. They obtained a saddle point for their game and showcase that implementation of a robust dynamic defense approach is practical where the saddle-point strategies can be considered as simple threshold-based policies. An attack-defense game (ADG) model is formed in where the game is a two-player, non-cooperative, zero-sum game and the solution of game was to find the optimal defense strategies that leads to minimize the cost. Very similar approaches are explored in [13]. A malware-defense differential game-based solution for confinement of malware epidemics is explored in [14], where the network tries to minimize the overall cost by choosing it's strategy dynamically.

A non-cooperative non-zero-sum game-based solution is provided in [15] for a Heterogeneous Wireless Sensor Networks (HWSNs) where malware propagation follows the Susceptible-Infected-Susceptible (SIS) model. Their solution predicts the infection behavior of the malware and given the diffusion cost incurred by the malware, they analysed the reliability and availability of the HWSNs. A normal form game is formulated between a malvertiser and the advertising-network in [16] where both pure strategy and mixed-strategy Nash equilibrium was obtained for the proposed non-zero-sum game.

Undoubtedly, the existing works emphasize on minimizing the spread of malware, with the focus on obtaining the equilibrium point (such as Nash equilibrium or saddle point) to ensure the malware propagation is confined. However, the network performance constraint is neither considered nor they emphasize on ensuring the network performance constraints are met when confining the malware.

III. Background

This section presents a brief introduction of the two commonly used malware propagation models, namely Susceptible-Infected-Susceptible (SIS) [17] and Susceptible-Exposed Infected Susceptible (SEIS) [18]. The rationale behind choosing these two models is that both of them are well justified in the literature [19] to illustrate the malware diffusion process for large-scale network.

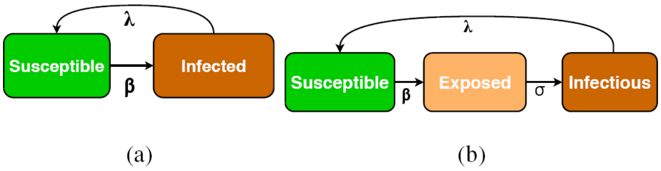

Fig. 1: State transition of malware models (a) State transition of SIS model, (b) State transition of SEIS model

1) The SIS Model: The SIS model has two sets of population, susceptible nodes (S) and infected nodes (I), as shown in Figure 1a. During the propagation, a susceptible node can be converted into an infected one, given by infection rate, β and the infected node can return to the susceptible state with a recovery rate λ. The rate of change of the susceptible and the infected nodes follows Equation (1).

$$\frac{dS}{dt} = -\beta IS + \lambda I; \quad \frac{dI}{dt} = \beta IS - \lambda I \tag{1}$$

2) The SEIS Model: In the SEIS malware propagation model, a node in the network can be one of the three states: Susceptible, Exposed, or Infected. The acceptable state transition for a given node should be from Susceptible (S) to Exposed (E) to Infected (I) and return back to Susceptible (S) state. Here, during the propagation, if a susceptible node is being exposed to an infected node, the node enters into an exposed state with probability β, where that node is infected but can not infect others. The probability of converting a exposed node to become an infectious one is represented by σ. The infected individual can return back to the susceptible state with a recovery rate, given by λ. Equation (2) shows the rate of change of susceptible, exposed, and infected nodes.

$$\frac{dS}{dt} = -\beta IS + \lambda I; \quad \frac{dE}{dt} = \beta IS - \sigma E; \quad \frac{dI}{dt} = \sigma E - \lambda I \tag{2}$$

IV. Threat Model

In this work, we assume the attack surface comprises of an IoT network with hundreds of interconnected devices. The target of the adversary is to get access to a node by breaching the security of the node. After getting access to a single node, the adversary tries to infect other neighboring nodes in a similar fashion. We assume that the attacker successfully infects few other neighboring nodes and this process continues with a probability p. For the malware propagation process, we assume that the propagation follows both the SIS and SEIS models, similar to the existing works [19]. While successfully connected to a node, the attacker analyses the payoffs for each of the feasible strategies aiming to minimize the network performance, i.e., network throughput, that leads to maximize the gains. We also assume that the attacker has the network topology and connectivity information.

On the other hand, the defender can opt multiple defense strategies to minimize the impact of malware. To determine which strategy will provide optimal solution, the defender executes our proposed game-theoretic method. The game-solver solves for the optimal strategy that the defender should take to

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:38:50 UTC from IEEE Xplore. Restrictions apply.

maintain the network performance while minimizing the threat of malware propagation.

V. Proposed Network-Malware Confinement

We propose a network-malware game (NMG) theory where the network (admin and devices) is the defender and malware is the attacker. As aforementioned, the malware's goal is to take control of a node and propagate throughout the network to cause performance degradation or control the network. In contrast, the defender tries to minimize the damage by confining the spread and maximize the network performance while keeping the incurred costs as low as possible. We assume that both the attacker and the defender aim to maximize their gains, while they choose their optimal strategy in response to the other players' strategy.

A. Network-Malware game

Definition 1. We define our network-malware game as a 3-tuple game where $NMG = (N, S, P)$. Here, $N = (1, 2, \cdots, z)$ is the number of players (attackers or defenders) and $S = (S_1, S_2, \cdots, S_z)$ is the strategy spaces of the participating players. Let's consider a NMG game where *Player(a)* is the attacker and *player(d)* is the the defender. *Player(a)* has $(s_1, s_2, ..., s_{att})$ strategies and *Player(d)* has $(s_1, s_2, ..., s_{def})$ strategies. If S_d is the defenders strategy set and S_a is the attacker's strategy set then s_j^d is a single defense strategy and s_i^a is an single attack strategy. This relationship is represented in Equation (3)

$$S_d = (s_1^d, s_2^d, ..., s_{def}^d); S_a = (s_1^a, s_2^a, ..., s_{att}^a) \quad (3)$$

where, d and a stand for the defender and the attacker, respectively. In our NMG game, $P = (P_1, P_2, \cdots, P_z)$ is the payoff function of the players.

Definition 2. Our network-malware game is a non-cooperative, dynamic, complete information, and zero-sum game. Between the players, there is no co-operation as both players want to maximize their own gain by damaging resources of the other player. The game is a complete information game as the players know the opponent's strategy-set and related cost for a given strategy. The game is dynamic in nature as the players evaluate their strategies after a given time and adjust their strategy to increase the gain. It is an imperfect game as the players choose their action without knowing the other players action, although, they know each other's strategy set and corresponding cost. This is a zero-sum game as the attacker's gain comes from the defender's loss.

B. Defining the Player's Strategies

In our game, the attacker has three strategies, a) "to kill a node instantaneously (denoted as *kill*)", b) "to infect the node, propagate to other nodes and wait before killing the source node (denoted as *wait-kill*)", c) "to propagate throughout the network (denoted as *propagate*)". Each strategy has its own benefit to the attacker. For instance, if the attacker's goal is to kill as many node as possible then adopting that strategy would benefit him more. If the attacker's plan is to infect as many node as possible and take control over the network to reduce the network performance then opting this strategy would give the best outcome.

In a similar manner, the defender also has three strategies, a) "to reboot and patch a set of infected nodes randomly (denoted as *reboot-random*)", b) "to reboot and patch a set of infected nodes based on the high degree centrality (denoted as *reboot-high-degree*)", c) "to reboot and patch a set of infected nodes based on the low degree centrality(denoted as *reboot-low-degree*)". In a similar fashion, for defender, each strategy has its own benefit. The defender can choose to reboot and patch a number of infected nodes based on random selection. Or the defender could pick a set of infected nodes that has high degree centrality (high number of interconnection with the other nodes in the network) and reboot them to slow the spread of the malware propagation. Or the defender could pick infected nodes to be rebooted and patched based on the low degree centrality.

C. Players' Gain, Cost, and Payoffs

Before formulating the payoff function, first, we quantify the relevant gain and cost associated with each strategy.

1) Defining players' gain: In this NMG game, two players aim to take control over the nodes so that the network performance is affected. We define the players' gain as the network performance impacted by the player. In this work, we consider the overall network throughput as the network performance metric. The attacker wants to reduce the network throughput by infecting nodes with malware which propagates throughout the network. The network throughput is inversely related with the number of infected nodes. If I is the number of infected nodes of the network then the increase of I results in higher gain for the attacker. Attacker's gain increases when the network throughput decreases. In contrast, increasing the network throughput leads to a higher gain to the defender. We define $G_i(t)$ as the gain of player i.

2) Defining players' cost: Each player needs to pay a cost to deploy his strategy. We develop our cost model based on several factors.

Table I and Table II represent the associated cost for each attack and defense strategy, respectively.

TABLE I: Attacker's strategies and related cost

Severity Level	Attack-Strategy	Attack-Cost	Remarks
Level1	propagate	1	Needs to pay the cost only due to infect a node. No additional access is required from the system.
Level2	wait-kill	10	Cost related to infect nodes and gain access to kill the node.
Level3	kill	100	More aggressive strategy and requires full access of the system.

The cost of the related strategies are chosen based on the logical-reasoning for both the attack and defense strategies. If different values are chosen then it is possible that the solution of the game-solver might change.

3) Defining players' payoff: The payoff is a function of player's gain and the related cost. Each player's gain is determined by the instantaneous value of the network throughput for a given time.

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:38:50 UTC from IEEE Xplore. Restrictions apply.

TABLE II: Defender's strategies and related cost

Severity Level	Defense-Strategy	Defense-Cost	Remarks
Level1	reboot-low-degree	1	Patching of less connected nodes has less impact on the network performance. Thus, rebooting those nodes require lower cost.
Level2	reboot-random	10	Patching is provided randomly irrespective of the connectivity consideration. As obtaining this strategy might have moderated impact on network, cost will be higher
Level3	reboot-high-degree	100	Patching is provided to those nodes who have high connectivity. Disconnecting a highly connected node will cause stability issue on the overall network performance.

Let's consider that the network has a maximum throughput capacity of T_{n_max}. When under attack, the network throughput for a given time becomes T_n. Here the attacker's gain at that time is determined by the following equation:

$$G_a(t) = T_{n\_max} - T_n(t) \tag{4}$$

As this is a zero sum game, the attacker's gain is the loss to the defender and vice-versa. Let's take an example where the attacker degrades the network throughput by T units. As a result, the attacker will gain T units and the defender will lose T units.

The attacker's total cost is the summation of the number of infected nodes and the number of nodes that the attacker implements his strategy multiplied by the corresponding cost for each action. We define the attacker's total cost for a given strategy as $C_a(t)$, represented in Equation (5)

$$C_a(t) = N_{an} \times C_{attck} + C_{inf} \times N_{a\_inf} \tag{5}$$

where, C_{attck} = Attack Strategy cost
N_{an} = Number of infected nodes to be killed by the attacker
C_{inf} = Cost related to infecting a node
N_{a_inf} = Number of infected nodes
The defender's total cost $(C_d(t))$ is a multiplication of the strategy and total number of nodes that are being patched is given by Equation (6).

$$C_d(t) = N_{dm} \times C_{defns} \tag{6}$$

Where,
N_{dm} = Number of nodes to be rebooted by the defender
C_{defns} = Defense strategy cost
Each player's payoff for a given strategy is the total gain minus the related cost (Equation (7)). This can be represented as: $P_a(S_i^a, S_j^d) = -P_d(S_i^a, S_j^d)$

$$P_i(t) = G_i(t) - C_i(t) \tag{7}$$

Where,
$G_i(t)$ = Player's gain for a given strategy
$C_i(t)$ = Total cost of the player

Our payoff function considers the network throughput as the players' gains and the associated cost to achieve that gain as the players' cost. Thus, finding a game-theoretic solution will lead us to lower the malware propagation while maintaining the network throughput with a lower cost.

In our NMG game model, we form a $m \times n$ payoff matrix with all the combination of network-malware strategies, where P = $\begin{pmatrix} s_{11} & \cdots & s_{1def} \\ \vdots & \ddots & \vdots \\ s_{att1} & \cdots & s_{attdef} \end{pmatrix}$; $s_{ij} = P(s_i, s_j)$. For our game, we have three network-malware strategies and a total of nine payoff combinations.

D. Solve the NMG game

Here we present the solution method of the NMG game. After forming the payoff matrix we call our NMG solver to solve the game. The solver tries to find out if there exists a saddle point for the game. If the row minimum and the column maximum are same then the value is the saddle point and both the players will play the corresponding strategy.
If a pure Nash Equilibrium is found then both the players adopts their corresponding strategy. Otherwise, they need to mix their strategy to obtain maximum gain. In that case, the attacker picks the optimal strategy from his strategy set with probability distribution, x , such that $x = (x_1, x_2, ...x_m)$ where $x_1, x_2, ...x_m$ are probabilities for a given attack-strategy-set and $\sum_{i=1}^{m} X_i = 1$. The defender obtains it's mixed strategy with a probability distribution, y, such that $y = (y_1, y_2, ...y_n)$ where $y_1, y_2, ...y_n$ are probabilities for a given defense-strategy-set and $\sum_{j=1}^{n} Y_i = 1$.
Let V be the solution of the game. Let us derive the upper bound and the lower bound of the game payoffs. We denote V_{low} and V_{up} as the lower bound and the upper bound of the payoff function, respectively. The lower bound of the game is obtained where the attacker minimizes the maximum payoff value obtained by the defender subject to minimizing the network throughput. In contrast, upper bound of the game is achieved when the defender tries to maximize the minimum payoff values obtained subject to minimizing the network throughput. This can be represented as follows:

$$\begin{gathered} V_{low} = \min_x \max_y P(s_i^a, s_j^d) \\ \text{subject to} \min(Network\_Throughput(T_n)) \end{gathered} \tag{8}$$

On the other hand, the upper value of the game is achieved when,

$$\begin{gathered} V_{up} = \max_y \min_x P(s_i^a, s_j^d) \\ \text{subject to} \max(Network\_Throughput(T_n)) \end{gathered} \tag{9}$$

The solver tries to solve the game that leads to achieve maximum gain to the defender as well as maximize the network throughput with minimum cost.

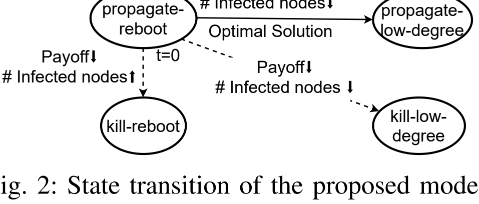

Fig. 2: State transition of the proposed model

Figure 2 shows the state transition of the optimal strategy based on the game solver's solution. For simplicity, we only show two attack strategies and two defense strategies that makes a 2 × 2matrix. At $t = 0$, the game solver picks the

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:38:50 UTC from IEEE Xplore. Restrictions apply.

propagate-reboot strategy as the optimal one. At $t = 1$, the game solver has a new payoff matrix with all the possible payoff values. From the state-diagram, we can observe that the solver can change its state to three different state or remain in the same state based on the payoff values. The optimization goal is to increase the payoff value (that also leads to higher network throughput) while reducing the number of infected nodes. From $t = 0$ to $t = 1$, the *propagate-low-degree* strategy has higher payoff value and less infected nodes making this strategy optimal. Thus, the solver adopts the best strategy that maximizes the network performance with minimal cost.

VI. Evaluation

In this section, we discuss the experimental setup and the analysis of our proposed game-theoretic based malware confinement model.

A. Experimental Setup

We employ the NetworkX[1] Python package to generate a random graph with 500 nodes with an edge probability of 0.3 using the Erdos Renyi Algorithm. The SIS and the SEIS malware epidemic models are generated using the Ndlib[2] python package. We begin the experiment with 0.05% of the total population being infected. At first, we calculate the maximum throughput of the network (which is 200 Mbps). After each iteration, when both the players have applied their strategies on the nodes that they have control over then we calculate the network throughput again. As both the players have three strategies, we develop a 3×3 payoff matrix. This payoff matrix represents all the combination of the strategies for the attacker and the defender. Then, we apply a min-max algorithm based on the developed payoff and cost functions to solve the game. As our primary goal was to lower the malware propagation while preserving the network throughput, the algorithm picks the best strategy for the defender (network) that returns optimal payoff considering both the infected nodes and network throughput.

B. Experimental Evaluation

We evaluate our proposed model with four other state-of-the-art techniques named Max-throughput [20], Min-infected [12], Max-payoff [21], and heuristic-based model [19]. The Max-throughput technique only optimizes for throughput maximization but does not put constraint on the malware confinement. In contrast, the Min-infected technique tries to confine the malware only but does not optimize the network performance. The Max-payoff technique accounts only for maximizing the payoff while considering neither the network performance nor the spread reduction. The heuristic-based model only focuses on the malware confinement issue without considering the network performance.

1) Evaluation for SIS Model Malware: Here, we evaluate our model on SIS malware propagation model. Fig. 3 shows the malware propagation trend for our proposed game-theoretic model on SIS epidemic model. This trend is achieved by exploiting our game-solver algorithm that not only considers to slow the spread but also considers to maintain the network throughput. By applying our proposed method we can observe from Fig. 3 that the propagation of the malware spread is confined, i.e., the network is converged.

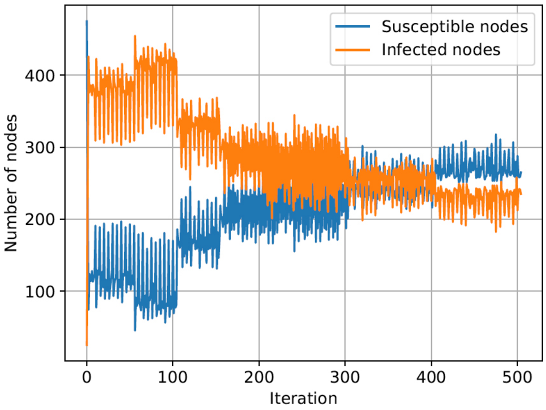

Fig. 3: Malware propagation trend applying our proposed game-theoretic solution on SIS model.

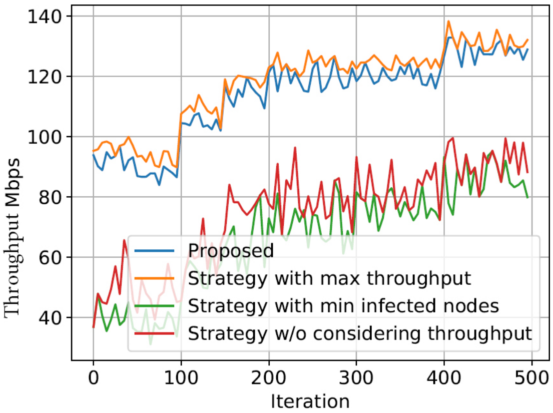

Fig. 4: Throughput trend comparison on SIS model.

a) Comparison: Table III reports our proposed model's experimental results compared other state-of-the-art techniques. While, comparing our proposed model with max-throughput model, both achieves similar performance on the number of infected nodes and the throughout but our model has 152 % higher payoff than that model. Having high payoff means we achieve similar performance on network throughput with lower cost compared to that model. The Max-throughput strategy has negative payoff as that strategy only considers to achieve maximum throughput but does not consider to confine the infection rate. As the number of infected node is higher, this strategy has a diminishing return that yields a negative payoff value. When compared with Min-infected strategy, we observe that we achieve approximately 70% higher throughput putting less constraint on the malware propagation which leads to a 42% higher infected node than the aforementioned model. The throughput trend for the SIS model is presented in Fig. 4 where the throughput trend for the proposed model clearly outperforms the ”Strategy with min infected nodes” and the ”Strategy w/o considering throughput” strategies and follows the ”Strategy with max throughput” trend very closely. As our game-solver tries to achieve an optimal strategy at each iteration, thus optimizing for both the throughput and infection rate, the number of infections is confined while the throughput

[1] https://networkx.org/

[2] https://ndlib.readthedocs.io/

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:38:50 UTC from IEEE Xplore. Restrictions apply.

TABLE III: Comparison of our proposed model

	SIS-model					SEIS-model				
	Proposed	Max-throughput [20]	Min-Infected [12]	Max-Payoff [21]	Heuristic [19]	Proposed	Max-throughput [20]	Min-Infected [12]	Max-Payoff [21]	Heuristic [19]
Throughput [Mbps]	113.35	117.18	67.08	74.47	23.89	122.25	123.48	79.02	93.25	29.85
Infected nodes	288	288	202	217	293	139	140	100	105	181
Payoff	1494.89	-2828.61	4450.01	10342.43	1488.79	1533.93	-798.26	4431.57	8565.44	1154.9

is maintained close to the maximum possible state.

2) Evaluation for SEIS Model Malware: We also evaluate our game-theoretic solution on the SEIS model. Similar to the SIS model, the SEIS model showed a similar malware spread trend and is not shown for the purpose of brevity. However, we showcase a numerical analysis (in Table III and the throughput trend visualization of our proposed model compared with other techniques.

a) Comparison: In Table III, while comparing our proposed model with Max-throughput method, we observe that our proposed model achieves similar average throughput value than the aforementioned method. We observe better throughput performance of our proposed model compared to all other strategies except for the ”Max-throughput” strategy. Our model achieves a 54%, 31%, and 309.5% higher throughput than the Min-infected, Max-payoff, and the Heuristic model, respectively. We traded this better performance of throughput value with number of infected nodes by putting less constraint on the malware confinement. In terms of infected nodes number, our model shows higher infected nodes than the Min-Infected nodes and Max-payoff method. On the other hand, our model has lower infected nodes than the Max-throughput and Heuristic model, respectively. Fig. 5 depicts the throughput trend for the SEIS model where proposed model achieves network throughout similar to the max-throughout strategy and shows superior performance on the the other two strategies.

Above discussion bolsters our claim that our model confines the malware spread while the network throughput is maintained and the network provider needs to pay minimum cost.

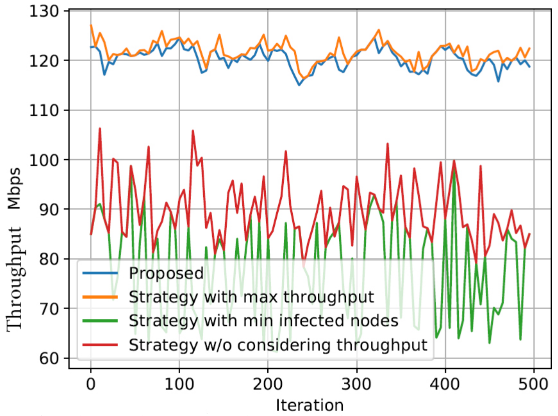

Fig. 5: Throughput trend comparison on SEIS model.

VII. Conclusion

In this work, we address the malware confinement problem in IoT network aiming to minimize the spread while maximizing the network performance. We develop a game-theoretic framework which not only confines the malware propagation but also maintains the network performance with a minimal cost. We evaluate our solution on several malware propagation model and showcase that our solution outperforms them considering all the performance metrics. In future work, we will implement a heterogeneous network where different types of IoT devices will be introduced to evaluate their impact on the malware propagation and network performance.

References

[1] G. D. Mayaan. The iot rundown for 2020: Stats, risks, and solutions. [Online]. Available: https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2

[2] W. Zhou *et al.*, “Discovering and understanding the security hazards in the interactions between iot devices, mobile apps, and clouds on smart home platforms,” in *USENIX Security Symp.*, 2019.

[3] McAfee Labs, “Infographic: Mcafee labs threats report,” July 2020.

[4] H. Sayadi *et al.*, “Ensemble learning for effective run-time hardware-based malware detection: A comprehensive analysis and classification,” in *55th Design Automation Conf.* IEEE, 2018, pp. 1–6.

[5] M. Antonakakis *et al.*, “Understanding the mirai botnet,” in *26th {USENIX} security Symp.*, 2017.

[6] A. P. Labs. Malware threat report: Q2 2020 statistics and trends. [Online]. Available: https://www.avira.com/en/blog/malware-threat-report-q2-2020-statistics-and-trends

[7] W. Wei, “Casino gets hacked through its internet-connected fish tank thermometer,” Online, 2018, accessed 20 September 2020.

[8] D. Zhao *et al.*, “Virus propagation and patch distribution in multiplex networks: modeling, analysis, and optimal allocation,” *IEEE Tran. on Information Forensics and Security*, vol. 14, no. 7, pp. 1755–1767, 2018.

[9] S. M. P. Dinakarrao *et al.*, “Cognitive and scalable technique for securing iot networks against malware epidemics,” *IEEE Access*, vol. 8, pp. 138 508–138 528, 2020.

[10] M. Khouzani *et al.*, “Optimal quarantining of wireless malware through power control,” in *Information Theory and Applications W.* IEEE, 2009.

[11] C. Wong *et al.*, “Dynamic quarantine of internet worms,” in *Int. Conf. on Dependable Systems and Networks.* IEEE, 2004.

[12] M. Khouzani *et al.*, “A dynamic game solution to malware attack,” in *Proceedings IEEE INFOCOM.* IEEE, 2011.

[13] V. A. Kumar *et al.*, “Existence theorems and approximation algorithms for generalized network security games,” in *30th Int. Conf. on Distributed Computing Systems.* IEEE, 2010.

[14] S. Shen *et al.*, “Differential game-based strategies for preventing malware propagation in wireless sensor networks,” *IEEE Tran. on Information Forensics and Security*, vol. 9, no. 11, pp. 1962–1973, 2014.

[15] S. Shen *et al.*, “A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous wsns with malware diffusion,” *Journal of Network and Computer Applications*, vol. 91, pp. 26–35, 2017.

[16] C.-T. Huang *et al.*, “A game theoretic approach for inspecting web-based malvertising,” in *IEEE Int. Conf. on Communications.* IEEE, 2017.

[17] C. Nowzari *et al.*, “Analysis and control of epidemics: A survey of spreading processes on complex networks,” *IEEE Control Systems Magazine*, vol. 36, no. 1, pp. 26–46, 2016.

[18] C. Gan *et al.*, “The spread of computer virus under the effect of external computers,” *Nonlinear Dynamics*, vol. 73, no. 3, pp. 1615–1620, 2013.

[19] S. M. P. Dinakarrao *et al.*, “Lightweight node-level malware detection and network-level malware confinement in iot networks,” in *Design, Automation & Test in Europe Conf. & Exhibition.* IEEE, 2019.

[20] T. Spyridopoulos *et al.*, “A game theoretical method for cost-benefit analysis of malware dissemination prevention,” *Information Security Journal: A Global Perspective*, vol. 24, no. 4-6, pp. 164–176, 2015.

[21] C.-T. Huang *et al.*, “A game theoretic approach for inspecting web-based malvertising,” in *IEEE Int. Conf. on Communications.* IEEE, 2017.

Authorized licensed use limited to: Univ of Calif Davis. Downloaded on October 11,2022 at 02:38:50 UTC from IEEE Xplore. Restrictions apply.