Honeypot Allocation for Cyber Deception in Internet of Battlefield Things Systems

Ahmed H. Anwar*, Nandi O. Leslie†, and Charles A. Kamhoua*
*US Army Research Laboratory, Adelphi, Maryland 20756
†Raytheon Technologies, USA
Email: a.h.anwar@knights.ucf.edu, nandi.o.leslie@raytheon.com, charles.kamhoua.civ@mil.gov

MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM) | 978-1-6654-3956-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/MILCOM52596.2021.9652927

***Abstract*—Cyber deception plays an important role in both proactive and reactive defense systems. Internet of Battlefield things connecting smart devices of any military tactical network is of great importance. The goal of cyber deception is to provide false information regarding the network state, and topology to protect the IoBT's network devices. In this paper, we propose a novel deceptive approach based on game theory that takes into account the topological aspects of the network and the criticality of each device. To find the optimal deceptive strategy, we formulate a two-player game to study the interactions between the network defender and the adversary. The Nash equilibrium of the game model is characterized. Moreover, we propose a scalable game-solving algorithm to overcome the curse of dimensionality. This approach is based on solving a smaller in-size subgame per node. Our numerical results show that the proposed deception approach effectively reduced the impact and the reward of the attacker**

I. Introduction

Traditional networks are rigid and inflexible because of their large scale and complex technical system. In this context, we focus on cyber deception as a proactive defense to mitigate attacks on Internet of Battlefield Networks (IoBTs) [1]–[3]. A proactive defense with more a rigorous approach such as game theory and artificial intelligence is needed to study the effectiveness of deception in IoBT systems. Using a game theoretic approach to cyber deception has shown strong capabilities in developing defensive deceptive strategies to defend networks against adversaries in various attack/defense scenarios [4], [5]. Leveraging the advances of Software Defined Networks (SDN) technologies in cybersecurity can enhance the network dynamic resilience and mitigate the reconnaissance abilities of attackers via deception. Deception techniques aim to disguise valuable network information to create uncertainty to prevent attackers from launching damaging attacks [6]. Moreover, deception leads attackers to spend more time in reconnaissance activities (increasing the chances of detection), or to attempt infiltration tactics that are less effective. Sophisticated targeted attacks, such as Advanced Persistent Threat (APT) attacks depend on fingerprinting of organizational networks to identify hosts and vulnerabilities necessary for the development of a battle plan and the execution of further attack maneuvers. We aim to deceive such malicious reconnaissance and network inference techniques by strategically placing fake nodes and using honeypots to hide the true underlying network topology and its potential vulnerabilities that can be exploited by attackers. The above challenges and the high risk and consequence of cyber-attacks drive the need to accelerate basic research on cyber deception.

In this paper, we propose a cyber deception approach based on honeypot allocation and software diversity to protect networks against adversaries capable of launching effective attacks. As attackers gather information about the networks ahead of starting any malicious activities [7], deception is of great significance to misrepresent the network state and information that could be collected during the reconnaissance stage. Moreover, attackers can obtain information that about the structure and connectivity of the targeted network via insider help [8]. An adversary can map out the network using available scanning tools such as Nmap [9] or via more advanced network inference techniques [10]. The network administrator needs to protect the network resources as early as possible. Hence, cyber deception is essential in defending against malicious activities in deceiving the attacker during the reconnaissance stage via manipulating the network interfaces and usage of honeypots and decoy devices. To this end, we develop a game theoretic framework to find the optimal deception (i.e., honeypot allocation) policy.

Recently, Cyber Deception based on game theory has become a hot topic for researcher as well as IoBT networks. The work mainly allow for modeling attack scenarios based on the existing records of the network defender. In these scenarios, the network defender protects the network using decoy devices or manipulating the network state, or via deceptive signals to decive the adversary [11]–[13], [13]–[16]. The defender on the other side may hide critical networked devices using camouflage techniques or via directing malicious data to a deceptive network [6], [17], [18]. Authors in [19], [20] considered a Stackelberg game to increase the level of uncertainty regarding the system from the attacker side, and to disrupt the outcome of scanning tools.

Our contribution in this paper can be summarized as follows: First, we propose a honeypot allocation game-theoretic approach that takes into account the network topology and the criticality of each node. The formulated game studies an important tradeoff to know where to place the honeypot devices to protect the network important assets while deceiving the adversary whose goal is to compromise the most valuable nodes in the network as well. Second, we characterize the Nash equilibrium and find the optimal allocation probabilistic allocation strategy for cyber deception. Third, we develop a

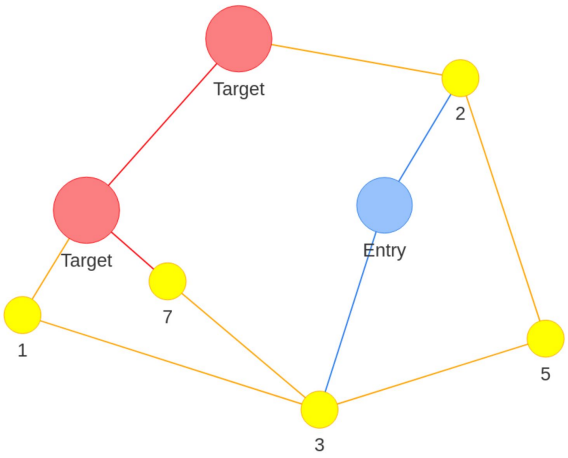

Fig. 1. An 7-node network topology with one entry nodes and two target nodes.

scalable game solving algorithm based on solving multiple subgames that are smaller in size to avoid the curse of dimensionality that emerges as the network size grows. Finally, we provide numerical evaluation to the proposed deception approach that shows its effectiveness in mitigating the impact of the attacker.

The rest of the paper is organized as follows: In Section II we describe the system model. In Section III we formulate the game between the two players and characterize the solution concept. Then in Section IV we present the scalable game solver algorithm. Finally, we present numerical results in Section V and conclude the paper in Section VI.

II. System Model

In this section, we introduce our network model, and the game model including the defender and attacker models.

A. Network Model

In this context, we consider a network topology-based deception system. Let $G(\mathcal{N}, \mathcal{E})$ represent the network as a directed graph of $|\mathcal{N}|$ nodes, and $|\mathcal{E}|$ edges. Each node $v \in \mathcal{N}$ belongs to one of three disjoint subsets. The subset of entry nodes is denoted as $\mathcal{N}_0$, and the subset of target nodes is denoted by $\mathcal{T}$, and the remaining nodes are labeled as intermediate nodes $\mathcal{I}$ such that $\mathcal{N} = \mathcal{N}_0 \uplus \mathcal{I} \uplus \mathcal{T}$. The network defender classifies each node into the three mentioned groups. A node is considered a target node according to its importance, criticality, and functionality. Also, the network intrusion detection system (NIDS) data enables the defender to identify the most vulnerable nodes at which an attacker would start his attack(i.e., the subset of entry nodes). The remaining nodes represents internal nodes in the considered tactical IoBT network.

Each node $u \in \mathcal{N}$ is assigned a value, w_v that represents its importance in an abstract and concise form. Such that, for any two nodes $u \in \mathcal{I}$ and $v \in \mathcal{T}$, $w_v > w_u$. The defender aims to protect high valued nodes via deception since the attacker would be interested in compromising them to maximize his/her reward along the way before reaching the target node.

B. Defender Model

The defender classifies the nodes into one of the three groups, where the goal of the defender is to place honeypot(s) along the most valuable path to protect important target nodes. However, deception and installing honeypots into the network come at a cost [21]. Therefore, we assume that the defender can only allocate a limited number of honeypots denoted as B. Hence, the defender can choose either to allocate one or more and up to B honeypots. The defender should make a judicial selection to the location of the honeypots. Honeypots are assumed to be placed on top of the edges connecting the different nodes. As such, a honeypot represents an interface to each node that receipts the incoming data. Honeypots will be placed along the edges capturing the reachability attempts from one node to another while preserving the network topology. From the attacker's side, in order to compromise any node, this node should be reached by one of its immediate parents. The defender should consider the node values, the honeypot allocation cost, and the different routes to be compromised in order to optimally allocate honeypots.

Let $\mathcal{A}_d$ denote the defender action space that includes all possible allocation policies. In other words, if the defender is choosing to allocate a single honeypot, then $\mathcal{E}$ would be the defender's action space. However, for up to B honeypots, the action space $\mathcal{A}_d = \{\mathbf{e} \in 2^{\mathcal{E}} \quad s.t \quad \mathbf{1}^T\mathbf{e} \leq B\}$, where $\mathbf{1}^T\mathbf{e}$ represents the inner product of two vectors. $\mathbf{e} \in \mathcal{E}$ is a binary vector of length $|\mathcal{E}|$, with an entry is set to 1 if a honeypot is allocated on this edge, and is set to 0, otherwise.

We design the payoff function such that it captures the cost of allocation and the loss due to successful attacks. When the attacker tries to compromise a node that is already protected via a honeypot the defender, is considered an unsuccessful attack, and the location of the adversary is revealed to the defender to continue monitoring this malicious activity. On the other hand, if the attacked node belongs to an unprotected path, the attack is considered successful, which is a loss for the defender. The loss is penalized by the value of the node being compromised. Therefore, in real scenarios the attacker assumes that the defender tends to protect high-valued nodes more than others to avoid high loss. However, if the node is successfully protected the defender gains higher gain from high-value nodes as well. The reward received by the defender depends on the attacker's action. Next, we model the attacker action space.

C. Attacker Model

We assume a powerful adversary that can map out the network topology using network scanning tools. Hence, the adversary has the information needed to establish all the possible paths from the entry node to the target node. The set $\mathcal{P}$ contains all the paths between the entry nodes and the end nodes in the network (i.e., target nodes). In other words,

$\forall u \in \mathcal{N}_0$ and $\forall v \in \mathcal{T}$, $P_{u,v} \in \mathcal{P}$ exists if there is a route to reach target node v starting from an entry node u and depending on the network structure, multiple paths could exist for the same pair of nodes.

Given his entry node $v_0 \in \mathcal{N}_0$, and the target node $t \in \mathcal{T}$ the attacker action space $\mathcal{A}_a$ is the set of all paths in $\mathcal{P}$ from v_0 and t. In practice, the defender does not know the exact target node, therefore, we formulate the game by taking all target nodes into account. We assume that the network intrusion detection system can alert the defender regarding the attack starting node v_0. Otherwise, if the NIPS failed to raise such alert, the attacker action space $\mathcal{A}_a$ is all the paths in $\mathcal{P}$. The attacker goal is to reach on of the target nodes while avoiding deceptive and fake nodes. However, it is more likely from the attacker's perspective that high-value nodes are more likely to be protected and surrounded by fake nodes and honeypots. This tradeoff is what our game model is studying, and is captured in the formulation of the players reward function defined next. Whenever used, the subscripts 'd' refers to an action or reward that belongs to the defender, and the subscript 'a' refers to the attacker's actions or reward.

D. Payoff Function

Focusing on the network topological aspects in this game, we are interested in finding the critical paths between entry nodes and target nodes. The reward function for the defender and the attacker are capturing the same tradeoff. In other words, the defender gains upon protected an attacked node, while the attacker rewards from compromising unprotected nodes. The defender payoff is expressed as follows,

$$R_d(a_d, a_a) = \sum_{t \in \mathcal{T}} \sum_{(u,v) \in \mathcal{P}_t} w_v . 1_{(u,v) \in a_d} 1_{(u,v) \in a_a} Cap \quad (1)$$
$$- w_v . 1_{(u,v) \in a_d} 1_{(u,v) \notin a_a} Esc,$$

where $\mathcal{P}_t$ is a subset of paths leading to target node t. $1_{(u,v) \in a_d}$ is an indicator function that is equals to 1, if the honeypot allocation action selected the edge (u, v), and is 0 otherwise. Similarly, $1_{(u,v) \in a_a} = 1$ if the (u, v) edge is part of the attack path selected by the attacker. If the attacker hits a honeypot, the defender receives a reward amount which is denoted by Cap. Otherwise, the defender receives a loss due to a successful attack denoted by Esc which represent the loss incurred by the defender when the attacker escapes a honeypot by going through another route. As a result, placing more honeypots will increase the reward of the defender. Hence, the defender will always prefer to increase the honeypot allocation budget B. The same tradeoff is considered from the attacker side with a conflicting interest, hence we consider $R_a = -R_d$. In other words, the game is zerosum and the attacker gain is directly considered a loss to the defender and vice versa.

Next we formulate this problem as a game model and characterize the best game-theoretic honeypot allocation policy.

III. Game Model

We formulate a two-player zerosum game between the network defender and the attacker. The end goal of his game is to provide the network admin with an allocation policy to be implemented initially given the network topology and the node values.

A two-player game defined as a tuple $\Gamma(\mathcal{K}, \mathcal{A}, \mathcal{R})$, where:

- $\mathcal{K} = \{Defender, Attacker\}$ denotes the set of the two players.
- $\mathcal{A} = \mathcal{A}_d \times \mathcal{A}_a$ is the game action space. The defender action space $\mathcal{A}_d = \{\mathbf{e} \in 2^{\mathcal{E}} \quad s.t \quad \mathbf{1}^T \mathbf{e} \leq B\}$ and the attacker action space is $\mathcal{A}_a = \mathcal{P}(v_0)$ where, $v_0 \in \mathcal{N}_0$ is the first node to be compromised by the attacker.
- $\mathcal{R} = \{R_d, R_a\}$ is the game reward $\mathcal{R} : \mathcal{A}_d \times \mathcal{A}_a \to \mathbb{R}$.

As explained in (1), the reward of each player depends not only on his sole action but on the action profile played by both players. Therefore, the defender should consider all the actions that his opponent may play (i.e., all the possible paths from the entry node v_0 to the subset of target nodes $\mathcal{T}$) in order to find his optimal honeypot allocation policy. If there exists an optimal location to place the honeypot, it would be against the basic idea of deception to keep placing the fake idea all the time in the same location. Hence, we rather consider a probabilistic allocation policy to solve the game. Solving the game in the probabilistic sense is referred to as solving the game in mixed strategies.

Specifically, we assume that each action $a_d^i \in \mathcal{A}_d$ is played with probability x_i such that $i = 1, 2, ..., |\mathcal{A}_d|$. Similarly, the attacker choose to play any action $a_a^j \in \mathcal{A}_a$ with probability y_j, where $j = 1, 2, ..., |\mathcal{A}_a|$. Now the game outcome value is the expected reward which is expressed as, $\sum_{i=1}^{|\mathcal{A}_d|} \sum_{j=1}^{|\mathcal{A}_a|} x_i R_d(a_d^i, a_a^j) y_j$. For simplicity, we re-write the game value in a matrix form as: $\mathbf{x}^T \mathbf{R}_d \mathbf{y}$, where $\mathbf{R}_d$ is a matrix of size $|\mathcal{A}_d| \times |\mathcal{A}_a|$. Next we present the game optimization problem for the defender player.

$$\begin{aligned} \underset{\mathbf{x}}{\text{maximize}} \quad & \mathbf{x}^T \mathbf{R}_d \mathbf{y} \\ \text{subject to} \quad & \sum_{i=1}^{|\mathcal{A}_d|} R_d(a_d^i, a_a^j) x_i \geq \mathbf{x}^T \mathbf{R}_d \mathbf{y}, \ \forall j = 1, .., |\mathcal{A}_a| \\ & \sum_{i=1}^{|\mathcal{A}_d|} x_i = 1, \\ & \mathbf{x} \geq 0. \end{aligned} \quad (2)$$

The goal of the defender is to maximize the expected payoff against each possible action played by the adversary which is guaranteed via the first condition. This condition ensures that x_i is giving a higher reward than the game value at each attacker's action $a_a \in \mathcal{A}_a$. Hence, it represents a set of $|\mathcal{A}_a|$ conditions to be satisfied. The other conditions ensure that $\mathbf{x}$ is a proper probability distribution vector. The game is a linear program to be solved in terms of $\mathbf{x}$.

Similarly, the attacker's game is another LP in terms of $\mathbf{y}$ to maximize $\mathbf{R}_a$) (i.e., minimizing the defender expected payoff)

$$\begin{aligned} \underset{\mathbf{y}}{\text{maximize}} \quad & \mathbf{x}^T \mathbf{R}_a \mathbf{y} \\ \text{subject to} \quad & \sum_{j=1}^{|\mathcal{A}_a|} R_a(a_d^i, a_a^j) y_j \geq \mathbf{x}^T \mathbf{R}_a \mathbf{y}, \ \forall i = 1, .., |\mathcal{A}_d| \\ & \sum_{j=1}^{|\mathcal{A}_a|} y_j = 1, \\ & \mathbf{y} \geq 0. \end{aligned} \tag{3}$$

The solution of these LPs yields the best mixed strategy $\mathbf{x}^*$ for the defender against any strategy of the adversary. On the other side, the solution of the LP in (3) yields $\mathbf{y}^*$. The joint strategy $(\mathbf{x}^*, \mathbf{y}^*)$ is the Nash equilibrium [22], of the game in mixed strategies which is the most well known and widely used solution concept in game theory. The immediate question now is how can we be sure that such an equilibrium exists for the formulated game Γ, hence we provide the following results to this question.

Theorem 1: For the finite game, Γ defined above there exists at least one point ($\mathbf{x}^*$,$\mathbf{y}^*$) of equilibrium in mixed strategies. Since game is finite in terms of the number of actions for both players, then the proof follows from game theory as shown,

Proof 1: The proof follows Nash's theory in [22], [23] directly.

which ensures that at least one equilibrium point exists and hence a honeypot allocation policy $\mathbf{x}^*$ can be deployed.

Game Complexity: One of challenges that may limit applying game theoretic models on graphs is the game complexity. More specifically, as the size of the network grows, the size of the game explodes in terms of the size of the action sames, $\mathcal{A}_d$ and $\mathcal{A}_a$. The number of possible paths between entry nodes and the subset of target nodes depends on the network structure. Moreover, as $\mathcal{A}_d$ is expressed in Section II-B, the number of possible locations exponentially increases in terms of the number of edges which increases with the number of nodes (i.e., the number of IoBT devices). In military tactical networks, the number of nodes is expected to reach a size of a platoon of a military unit, which is about 20 to 50 nodes or more. Hence, the dimension of the linear programs explodes in the size of the network which adversely affects the runtime of the game solver. Therefore, we propose a scalable algorithm to solve the formulated game via avoiding the curse of dimensionality.

IV. Decomposition-based Scalable Approach

In order to avoid the curse of dimensionality we propose a scalable approach to solve the game based on subgraphs. In other words, instead of playing the game over the full graph, the defender will opt to solve a single subgame per each node in parallel. At each node $v \in \mathcal{N}$, the defender generates a subgraph that starts from node v considering all single hop neighboring nodes communicating with this node. Consider the scenario shown in Fig. 2. At v_0, the defender solves a game that only considers 3 possible actions, that are to place the honeypots along which of the three edges, the defender simply disregard the rest of the network topology at this subgame. Next, we reformulate the game to be played per each node starting from the original game formulation in eqns (1), (2), and (3).

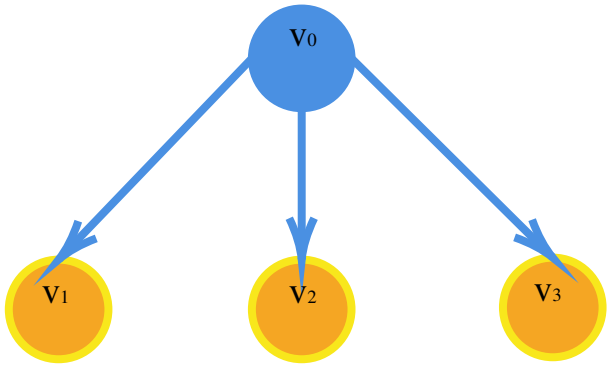

Fig. 2. Subgraph generated at an arbitrary starting node v_0 that has 3 immediate neighbors

Revisiting the reward function defined in (1), and the expected payoff of the defender at each action profile (a_d, a_a), can be expressed as, $xR_d(a_d, a_a)y$

Decomposing the defender action a_d vector per each edge in the network. Let $a_d^{(u,v)}$ denote the entry of a_d such that $a_d^{(u,v)} = 1$ if the defender place a honeypot at along the edge connecting node u to v, and $a_d^{(u,v)} = 0$, otherwise.

Along the same lines, we decompose the mixed strategies of $\mathbf{x}$ and $\mathbf{y}$ into the probability of playing $a_d^{(u,v)}$ as denoted by $x^{(u,v)}$. Similarly, for the attacker the probability to compromise neighbor node v after node u (i.e., $a_a^{(u,v)} = 1$ is denoted by $y^{(u,v)}$. Labeling each subgame by its generating node u, the subgame expected payoff function as $\bar{R}_d^{(u)}$ can be expressed as:

$$\bar{R}_d^{(u)} = \sum_{v \in \mathcal{N}_u} w_v x^{(u,v)}.y^{(u,v)}.Cap - w_v.x^{(u,v)}.(1 - y^{(u,v)}).Esc, \tag{4}$$

where $\mathcal{N}_u$ denotes the set of neighboring nodes of u.

The game expected payoff defined in (1) can be expressed in terms of subgame reward functions as follows:

$$\hat{x} R_d(a_d, a_a) \hat{y} = \sum_{t \in \mathcal{T}} \sum_{(u) \in \mathcal{P}_t} \bar{R}_d^{(u)}, \tag{5}$$

where $\hat{x}$ and $\hat{y}$ are computed from the collection of $x^{(u,v)}$ and $y^{(u,v)}$ after normalizing it to ensure that $\mathbf{1}^T \hat{\mathbf{x}} = 1$ and $\mathbf{1}^T \hat{\mathbf{y}} = 1$. So instead of solving one single game on a graph of size $|\mathcal{N}|$, we propose to solve an equivalent $|\mathcal{N}|$ subgames. The preceding derivation shows this equivalence. The key of our decomposition approach hinges upon the structure of the reward function defined earlier in (1). Each subgame is played on a graph of size $|\mathcal{N}_u|$ for each $u \in \mathcal{N}$.

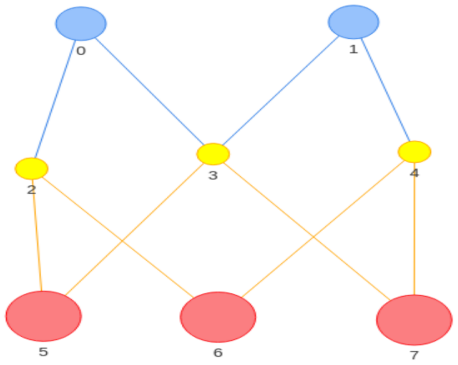

Fig. 3. An 8-node network topology with three target nodes all within same distance from the entry node

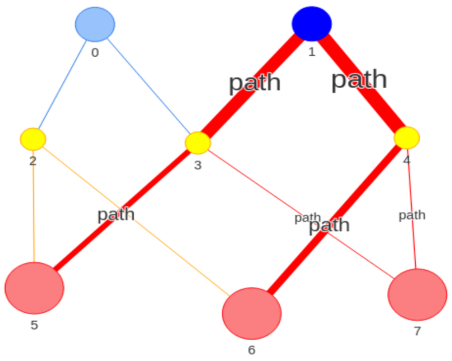

Fig. 4. The attacker tends to avoid the high value node expecting it to be fake or protected by honeypot along the way.

Next, we propose our numerical results.[1]

V. Numerical Results

In this section we present our numerical results that validates the proposed honeypot allocation approach and show its effectiveness to mitigate the effect of the adversary in the network. Our analysis and game model also provides a clear understanding of the attacker's preference in terms of most preferred paths to carry an attack.

First, we consider a network of size 8 nodes that is shown in Fig. 3. In this network topology there are two entry nodes, $\mathcal{N}_0 = \{0, 1\}$ in blue, and three target nodes, $\mathcal{T} = \{5, 6, 7\}$ plotted in red. Each intermediate node a value of 10, while we assigned the target nodes as to be $100, 100, 200$, respectively. Also, the two game metrics Esc and Cap are set to 5 and 10 to ensure that the defender capturing reward is more valuable. In this simulation the attacker started his attack at node 1, as shown in Fig. 4. For this setup, solving the game yields the following attacking mixed strategies, the attacker will attack path [1, 3, 5] at 30%, [1, 4, 6] at 35%, [1, 3, 7] and [1, 4, 7] at 17.5% of the time each. In Fig. 4, we show the probability of attack per edge as shown in red. This equilibrium attacking strategy shows that, the attacker tends to avoid nodes of high values knowing that they are more likely to be fake or be protected by honeypots.

The defender is assumed to have a limited budget $B = 1$ honeypot to place. At equilibrium, the defender will choose to place this honeypot along the following edges $(3, 5), (3, 7), (4, 6), (4, 7)$ with the following probabilities, [0.1499, 0.31965, 0.1855, 0.3449], respectively. In Fig. 5, we graphically illustrates this allocation strategy based on the weight of each edge in green. As shown, the defender is likely to protect the high valued node more often than other nodes through all the possible paths that may lead to it. The attacker expected reward at equilibrium is 101.74. If the defender deviated away and decided to randomly place the honeypot, on average the attacker expected reward jumps to 136.15. Adopting a random allocation policy will be even worse as the size of the network grows. Hence, the defender needs to solve the formulated game to compute the optimal honeypot allocation strategy. Similarly, it is always better for the attacker not to deviate from the NE attacking policy.

[1]If accepted for publication, in its final version we plan to include additional simulation results.

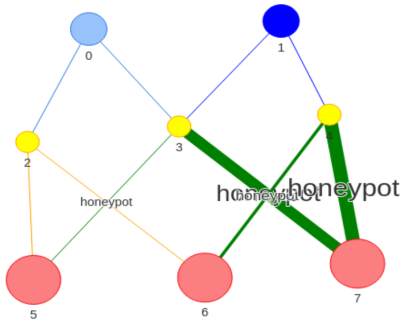

Fig. 5. Given a single honeypot to allocate, the defender protects the high valued node more often.

Moreover, if the defender can allocate 2 honeypots, the attacker reward drops from 101.74 to 35. Showing that, the defender can always enhance the level of the network security by placing more honeypots. The impact of the number of allocated honeypots is shown in Fig. 6 in terms of the defender expected reward.

Finally, we show the NE honeypot allocation strategy when the game is played on a 21-node network. The defender protects the target nodes by placing the honeypots along the path leading to it since the budget is limited and the defender cannot protect the immediate edges leading to the target nodes.

VI. Conclusion

We proposed a honeypot-based deception game-theoretic approach to mitigate the impact of adversaries and provide a false network view. We formulate a two-player zerosum game between the network defender and the adversary. The game is played on a graph and we obtain the Nash equilibrium honeypot allocation strategies. Since games on graphs are known to suffer the curse of dimensionality, in this paper we proposed a decomposition-based game solving algorithm. This scalable approach is based on solving a smaller in-size subgame per

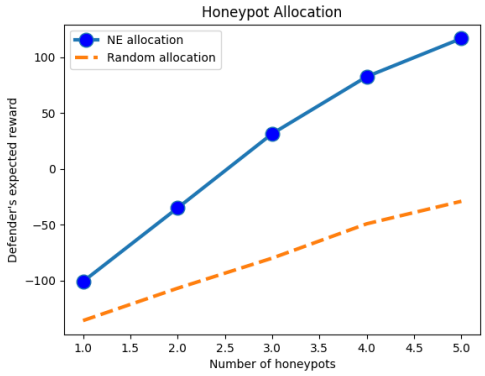

Fig. 6. The effect of the number of honeypots on the defender's expected reward

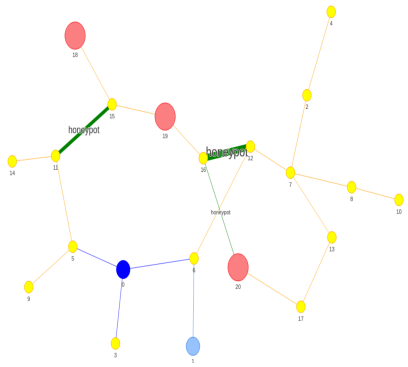

Fig. 7. The defender protects the paths to high valued node with a single honeypot in a 21-node network.

node. Our numerical results show that the proposed deception approach effectively reduced the impact and the reward of the attacker and answering the question of where to place fake nodes and deceptive devices for any network topology. Our ongoing research considers a more general game model that can leverage the advances of SDN technologies to change the network view in addition to honeypot generation for cyber deception.

Acknowledgment

Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-19-2-0150. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

References

[1] S. Russell and T. Abdelzaher, "The internet of battlefield things: the next generation of command, control, communications and intelligence (c3i) decision-making," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*, pp. 737–742, IEEE, 2018.

[2] T. Abdelzaher, N. Ayanian, T. Basar, S. Diggavi, J. Diesner, D. Ganesan, R. Govindan, S. Jha, T. Lepoint, B. Marlin, *et al.*, "Toward an internet of battlefield things: A resilience perspective," *Computer*, vol. 51, no. 11, pp. 24–36, 2018.

[3] A. H. Anwar, C. Kamhoua, and N. Leslie, "A game-theoretic framework for dynamic cyber deception in internet of battlefield things," in *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 522–526, 2019.

[4] J. Pawlick and Q. Zhu, *Game Theory for Cyber Deception: From Theory to Applications*. Springer Nature, 2021.

[5] A. H. Anwar and C. Kamhoua, "Game theory on attack graph for cyber deception," in *International Conference on Decision and Game Theory for Security*, pp. 445–456, Springer, 2020.

[6] H. Çeker, J. Zhuang, S. Upadhyaya, Q. D. La, and B.-H. Soong, "Deception-based game theoretical approach to mitigate dos attacks," in *International Conference on Decision and Game Theory for Security*, pp. 18–38, Springer, 2016.

[7] N. C. Rowe and H. C. Goh, "Thwarting cyber-attack reconnaissance with inconsistency and deception," in *Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC*, pp. 151–158, IEEE, 2007.

[8] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures," *ACM Computing Surveys (CSUR)*, vol. 52, no. 2, pp. 1–40, 2019.

[9] G. F. Lyon, *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure, 2009.

[10] R. De Smet and K. Marchal, "Advantages and limitations of current network inference methods," *Nature Reviews Microbiology*, vol. 8, no. 10, pp. 717–729, 2010.

[11] T. E. Carroll and D. Grosu, "A game theoretic investigation of deception in network security," *Security and Communication Networks*, vol. 4, no. 10, pp. 1162–1172, 2011.

[12] Y. Li, Y. Xiao, Y. Li, and J. Wu, "Which targets to protect in critical infrastructures-a game-theoretic solution from a network science perspective," *IEEE Access*, vol. 6, pp. 56214–56221, 2018.

[13] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pp. 46–57, ACM, 2005.

[14] A. Clark, Q. Zhu, R. Poovendran, and T. Başar, "Deceptive routing in relay networks," in *International Conference on Decision and Game Theory for Security*, pp. 171–185, Springer, 2012.

[15] S. Jajodia, P. Shakarian, V. Subrahmanian, V. Swarup, and C. Wang, *Cyber warfare: building the scientific foundation*, vol. 56. Springer, 2015.

[16] A. H. Anwar, C. Kamhoua, and N. Leslie, "Honeypot allocation over attack graphs in cyber deception games," in *2020 International Conference on Computing, Networking and Communications (ICNC)*, pp. 502–506, IEEE, 2020.

[17] M. Bilinski, R. Gabrys, and J. Mauger, "Optimal placement of honeypots for network defense," in *International Conference on Decision and Game Theory for Security*, pp. 115–126, Springer, 2018.

[18] T. Zhang and Q. Zhu, "Hypothesis testing game for cyber deception," in *International Conference on Decision and Game Theory for Security*, pp. 540–555, Springer, 2018.

[19] A. Schlenker, O. Thakoor, H. Xu, F. Fang, M. Tambe, L. Tran-Thanh, P. Vayanos, and Y. Vorobeychik, "Deceiving cyber adversaries: A game theoretic approach," in *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, pp. 892–900, International Foundation for Autonomous Agents and Multiagent Systems, 2018.

[20] J. Letchford and Y. Vorobeychik, "Optimal interdiction of attack plans," in *Proceedings of the 2013 international conference on Autonomous agents and multi-agent systems*, pp. 199–206, International Foundation for Autonomous Agents and Multiagent Systems, 2013.

[21] Q. Duan, E. Al-Shaer, and M. Islam, "Conceal: a strategy composition for resilient cyber deception: framework, metrics, and deployment," in *Autonomous Cyber Deception*, pp. 101–124, Springer, 2019.

[22] T. Basar and G. J. Olsder, *Dynamic noncooperative game theory*, vol. 23. Siam, 1999.

[23] J. F. Nash *et al.*, "Equilibrium points in n-person games," *Proceedings of the national academy of sciences*, vol. 36, no. 1, pp. 48–49, 1950.