IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 April 2023, accepted 14 May 2023, date of publication 22 May 2023, date of current version 19 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3278744

RESEARCH ARTICLE

D3GF: A Study on Optimal Defense Performance Evaluation of Drone-Type Moving Target Defense Through Game Theory

SANG SEO[1], HEAEUN MOON[1], SUNHO LEE[1], DONGHYEON KIM[1], JAEYEON LEE[2], BYEONGJIN KIM[2], WOOJIN LEE[2], AND DOHOON KIM[3]

[1]RedAlert Team, NSHC Company Ltd., Seoul 08502, South Korea
[2]Cyber Battlefield Team, Hanwha Systems Company Ltd., Seongnam-si 13524, South Korea
[3]Department of Computer Science, Kyonggi University, Suwon-si 16227, South Korea

Corresponding author: Dohoon Kim (karmy01@kyonggi.ac.kr)

This work was supported by the Challengeable Future Defense Technology Research and Development Program through the Agency for Defense Development (ADD) funded by the Defense Acquisition Program Administration (DAPA), in 2023, under Grant 915024201.

ABSTRACT Based on the paradigm shift in modern warfare, ground forces conduct pilot operations of wireless unmanned maneuvering systems, such as tactical drones, in the form of manned and unmanned cooperative tactics after deploying the relevant systems in the battlefield. However, security considerations for relevant systems are limited to the scope of using only the existing end-to-end encryption and public key authentication modules, and no defense strategy to actively respond to specialized cyber-electronic warfare threats has been officially established. To drastically reduce both the potential attack surface and security vulnerabilities of drones employed in network-centric-warfare, a proactive defense technology that expires the effectiveness of attacks by avoiding invasive action at the target is expected to be essential. Accordingly, this paper proposes the concept of active moving-target-defense (MTD), an element of cyber deception that minimizes the rate of success of cyber-attacks while conversely maximizing both defense predominance and attack complexity asymmetrically, exclusive according to partially observable Markov decision process (POMDP)-based threat modeling that considers both the internal and external operation sequences of target drones. To optimally design the proposed drone-type MTD based on the Pareto frontier, we additionally advanced and simulated a drone-based defensive deception game framework (D3GF), which represents a general-sum combat framework reflecting decision logics such as the perfect Bayesian Nash equilibrium, stochastic Stackelberg, and partial signal game. This study was conducted to compare and calculate the efficiencies of the drone-type MTD's deceptive defense, which had not been considered in prior studies, by unique environmental features inside and outside the drone. Furthermore, we conducted a detailed performance evaluation considering game metrics based on sensitivity analysis. Hereafter, the drone-type MTD will be extended into an actual active drone protection technology combining cyber flare-type avoidance strategies and cyber camouflage-type disarrangement strategies by expanding its optimization domain as a hypergame, while integrating it with drone decoy elements.

INDEX TERMS Cyber deception, moving-target-defense, drone, cyber-electronic-warfare, game theory.

I. INTRODUCTION

To adaptively respond to transitions in the battlefield in the form of modern multi-domain operation (MDO) [1], ground task forces are currently introducing advanced unmanned maneuvering systems such as tactical drones [2], [3]. Furthermore, to simultaneously ensure the multi-purpose mission continuity and multi-layer engagement efficiency of the ground combat platform, as well as quickly secure the continuation ofs individual battles in the form of command

The associate editor coordinating the review of this manuscript and approving it for publication was Tiago Cruz.

decisions, the application of protection technologies to detect, prevent, and respond to potential limiting factors according to offensive soft-kill [4] threats is desirable.

At present, however, only the classical end-to-end encryption and concept of public key authentication [5] are limitedly adopted within small- and medium-sized communication systems, thereby focusing only on securing the availability and integrity of the target force. The establishment of self-defense strategies to fully respond to and neutralize specialized cyber-electronic-warfare [6] attacks aiming at target drone platforms remains at an extremely early stage. In addition, wireless remote tactical drones exhibit properties that are extremely unfavorable to continuous security in the presence of Command and Control Center (CCC), such as passivity, heterogeneity, dependency of decision-making, and environmental hostility. The vulnerability of attack surfaces and threat sequences that can potentially increase sharply as tactical drones become common throughout operating systems has not been analyzed.

If sufficient countermeasures to ensure high levels of cyber agility [8] and resilience [9] in tactical drones are not established, mission continuation efficiency is expected to sharply decrease. To alleviate these limitations, moving-target-defense [12], which represents a defensive deception approach [10], [11], must be appropriately configured for all internal and external drone structured, detailed processes, attack surfaces [13], and vulnerabilities. In addition, the analysis of quantitative protection performance in contrast to conventional security must be considered via combat damage evaluation according to the real-time engagement of target rugged drones.

In the present study, a drone-type MTD was designed to minimize the success utility of attackers that utilize the defender's intelligence by periodically mutating the unique fingerprints possessed by the wireless tactical drones, simultaneously inducing high levels of cognitive disturbance on the attackers via deceptive perturbation. In parallel, a general-sum game framework was structured to evaluate and verify the normalized drone-type MTD defense based on mixed integer quadratic programming (MIQP) [16] with perfect Bayesian Nash equilibrium [14], considering constraint conditions, stochastic Stackelberg [15], uniform distribution, and exponential distribution random sampling. The partially observable Markov decision process (POMDP) [17] and partial signaling game [18] components were additionally also configured to simulate competitive engagement and state-transition relations according to the cyber kill chain (CKC) sequence [19] based on the internal and external threat modeling of drones. Finally, the deception defense performance of the drone-type MTD were analyzed via game metric.

The following primary contributions were achieved within this study. First, by ensuring the deceptive MTD concept's exclusivity based on the drone's threat modeling, enabling it to be operated independently of other security standards, a novel tactical drone security strategy can be established and standardized. Second, as an element of defensive deception, the MTD resolves the issue of spatiotemporal asymmetry advantageous to the attacker, which could not be solved with conventional security elements. Attack surfaces potentially possessed by tactical drones can also be forcibly configured to be disadvantageous to attackers. Third, by simulating engagements through an optimization framework composed of general-sum game-based components, the defense performance of the drone-type MTD was analyzed by game metrics considering both the Pareto frontiers and trade-off. Finally, based on results of the preemptive analysis, an active response strategy also can be referred to considering the resilience and agility of tactical drone prototypes under the command decision system.

The rest of this paper was structured as follows. Chapter 2 investigates and compares previous study cases related to defensive cyber deception and MTD. To derive an optimal MTD deception strategy for the drone operation environment, Chapter 3 presents D3GF, an optimization framework that combines the perfect Bayesian Nash equilibrium, stochastic Stackelberg, partial signal game-based general-sum game foreground module, and POMDP-based state-transition matrix background module. This framework is presented along with game metrics and formulas, as well as a parallel analysis threat modeling for the inside and outside of drones based on the STRIDE standard [20]. Chapter 4 describes the attack and defense scenarios that will be available in D3GF. Subsequently, the drone's topology is specified in the form of a POMDP-based CKC considering common vulnerabilities, exposures (CVE) [21], and the common vulnerability scoring system (CVSS) [22]. In addition. major game parameters are configured to generally analyze the sensitivity of the drone-type MTD. Finally, Chapter 5 concludes this paper by discussing the obtained results, expected effects, and future directions of research.

II. RELATED WORK

The following section presents conceptual descriptions of defensive cyber deception and MTD to amplify the concept of deceptive protection in tactical drones. Several relevant studies based on game theory that provided the main inspiration for this study are investigated, analyzed, and compared with the proposed D3GF.

A. DEFENSIVE CYBER DECEPTION AND MTD

Defensive cyber deception has emerged as a major game-changing concept that could potently replace conventional technologies in domestic and foreign cyber security subdivisions starting from the 2011 US White House's "Trustworthy Cyberspace: Strategic Plan for The Federal Cybersecurity Research and Development Program" [23]. It is an uncooperative decision-making-contamination technology designed to confound the attacker's cognition based on static information asymmetry and dynamic

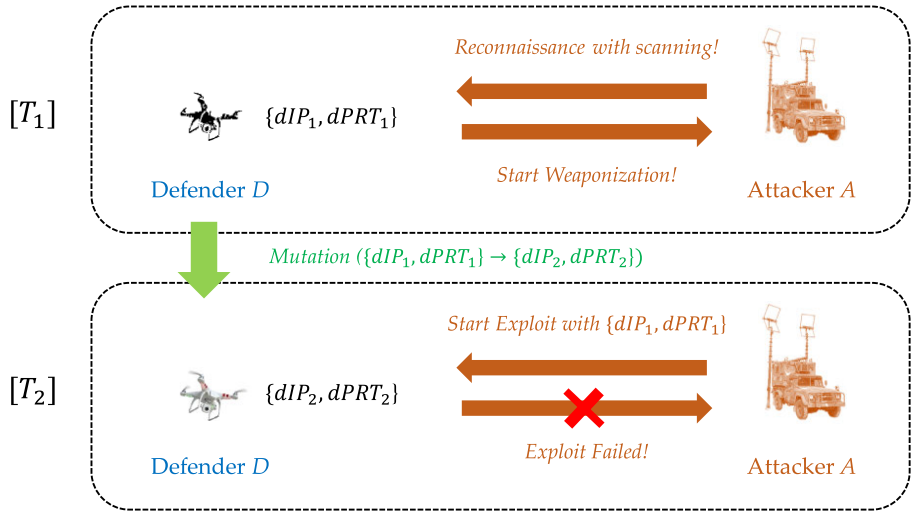

FIGURE 1. Primary mechanism of MTD.

disinformation, causing attackers to sustain erroneous post-action strategies. According to these social engineering [24] characteristics, defensive cyber deception involves unique features such as guidance, isolation, backtracking, and mutation, making kill chains by mission critical environment such as the national defense and public domains. Thus, defensive cyber deception is clearly distinct from conventional security. In addition, while actively reducing the temporospatial inferiority of defenders within conventional perimeter-based security, defensive cyber deception can inherently secure the standardization of cyber threat intelligence [25], as required by attack analysis, using a small quantity of resources.

The defensive cyber deceptions could be classified among MTD, Honey-X [26], and decoys [27] according to operational goals, defense purposes, implementation directions, remaining resources, and roles. MTD – which is constructed based on attributes of cyber mobility with shuffling, shifting, diversity, and redundancy – does not expose defender's sensitive information, instead operating in a form that significantly limits the validity of surface information. Consequently, the observable attack/exploration surfaces are actively increased by the defender in the temporal and spatial dimensions, thereby avoiding the advanced attack independently. Because MTD addresses the information asymmetry issue disadvantageous to the defender while processing the formation of the attack chain to induce uncertainty and complexity for the attacker, it uniquely realizes proactive defense based on preemptive cyber immunity. In addition, depending on the mutation cycle and shuffling set selection, MTD can prevent post-fact damage by diverting the attack directly outside the victim, or advance to tolerate penetration by intentionally lowering the mutation intensity for cyber traceback analysis and information collection.

The design principles of MTD [29] correspond to three conceptual elements: 'When-to-Move,' which pertains to the mutation cycle; 'What-to-Move,' which refers to the defender fingerprint set groups to be mutated; and 'How-to-Move,' which encompasses the mobility functions and sampling mutation methods to prioritize the shuffling selection of candidate groups for mutation sets. The MTD mechanism is designed as illustrated in Figure 1.

When an attacker A identifies through reconnaissance that the IP address possessed by legitimate network server D at time T_1 is dIP_1, and the corresponding port is $dPRT_1$, A initiates weaponization mode. However, because D has already applied the MTD of the network layer target – which operates independently regardless of compromise or invasion detection, and involves the MT ($MT < T_{n+1} - T_n$) parameter, which is a mutation cycle optimized so that seamless connection [30] to the communication channel of T_n, the cycle of previous time point n, is maintained at least – $\langle dIP_1, dPRT_1 \rangle$ shifts to $\langle dIP_2, dPRT_2 \rangle$ *at times* T_2. Accordingly, A's attempt to invade intends to exploit through the intelligence of $\langle dIP_1, dPRT_1 \rangle$, resulting in a failure from the stage of initial attempt for socket communication, as D has already alternated to $\langle dIP_2, dPRT_2 \rangle$.

Thus, the MTD can be ultimately defined as a representative active-defense paradigm [31] that efficiently diversifies the configurations of internal networks and heterogeneous system hosts by digital domain to be protected based on cyber mobility. This maintains the availability of major services (when multiplexed MTD channels to support seamless connection) provided to legitimate users while increasing confusion and uncertainty in attackers, thereby preventing the formation of attack chains.

However, most reported studies pertaining to MTD are limited to theoretical evaluations of defense performance in wired legacy network environments, or restrictive designs within constructed virtualized SDN communication topology environments [32]. In addition, the few existing MTD study cases on wireless communication environments or drone-based unmanned vehicles are limited to the use of

radio frequency (RF)-based received signal strength indicators (RSSI), and detailed performance evaluations according to engagement between competitive actors have been reported to be slightly inadequate [33]. Therefore, the introduction of a defense strategy for tactical drones based on the domain limitations of existing studies and new research goals, a unique threat modeling configuration is necessary to identify potential vulnerabilities in the drones' internal and external environments. A quantitative sensitivity analysis following MTD application is also required preemptively.

B. GENERAL GAME THEORETIC MTD

To carry out a study on drone-type MTD, game-theory-based MTD study cases were compared and analyzed. The scope of investigation for selected studies was determined as 'general game theoretic MTD,' 'Bayesian Stackelberg game theoretic MTD,' and 'stochastic game theoretic MTD.'

The primary finding point is that previous game-theory-based academic studies using MTD were conducted to model competing CKC-based intrusion and MTD-based avoidance in order to achieve imperfect goals independently possessed by attacking and defending actors, respectively. Another objective of these studies is the microscopic optimization of the main MTD parameters, including the mutation cycle, shuffling sets, and sampling methods. In addition, when increasing the defender's gains by minimizing performance degradation and maximizing security, the normalization of the macroscopic MTD strategy also aims to minimize the attacker's gains, such as lateral movement or target occupation.

Among the general game-theory-based MTD study cases, Zhu et al. [34] first applied two-person game-based sequential attack-defense competition formulas and metrics to the concept of MTD mutation, thereby quantifying the trade-off relationship based on both the defender's security and operation degradation. Ge et al. [35] proposed an incentive-compatible MTD game based on user-to-user communication mapping during migration to characterize cyber agility elements that can secure availability while ensuring high service visibility and throughput for legitimate users based on the MTD. Neti et al. [36] designed an anti-coordination game as a guided framework to observe interaction between scalabilities and quantify the diversity-based deceptive measure in MTD. Wright et al. [37] constructed a heuristic two-person game environment to optimize all necessary preconditions, mutation parameters, and target stability criteria, thereby constructing an active MTD strategy against adaptive distributed denial-of-service (DDoS) attacks. Carter et al. [38] presented a dedicated MTD game architecture to determine a migration methodology that guarantees non-terminating connectivity to legitimate users' services while minimizing the suspicion of attackers guided and isolated in the sandbox. As an additional counterexample study, Colbaugh and Glass et al. [39] argued that rather uniform randomization is the optimal strategy for diversity tactics.

C. BAYESIAN STACKELBERG GAME THEORETIC MTD

The following section examines Bayesian Stackelberg game theoretic MTD study cases that aimed to limit the follower's optimization behavior according to the leader's behavior.

Hasan et al. [40] proposed a co-resident attack mitigation and prevention (CAMP) architecture, representing a Nash equilibrium game model that detects co-resident attacks in a virtual environment where the same temporospatial resources are shared, as well as minimizing the impact of internal and external threats. Feng et al. [18] presented an artificial information disclosure model that enhances the defender's agility by disturbing and deflecting the attackers' initial decision-making process with the MTD defender's deliberate expose of false information based on the Stackelberg game. By considering the follower's dependent relationship with the leader's signal, this approach also represents an interactive decision strategy. In a follow-up study, Zhu et al. [41] proposed an advanced MTD model to improve the efficiency of the attacker guidance and isolation mechanism based on the routing protocol, while generating false packets specialized to the reconnaissance operations of attackers based on the unique fingerprint of the target defense organization.

Sengupta et al. [42] proposed an MTD optimization strategy model that maximizes active avoidance security using the system configuration candidate set while minimizing performance degradation for defenders, who could have limited available resources within the web and cloud-based organizational topologies. A study on MTD strategies for zero- and general game-based competition [43] was conducted to secure defense against advanced persistent threat (APT) attacks within the cloud network. As a separate follow-up study, Li et al. [16] proposed a Markov Stackelberg model using average-cost semi-Markov decision process (SMDP) and discrete time Markov decision process (DTMDP)-based optimization formulas to calculate the defender's spatiotemporal MTD mutation decision-making process simultaneously with the potential attack surface.

Seo et al. [44], [45] added a dynamic cognitive disturbance function that the existing MTD concept was not contain, and combined it with layered social engineering decoy as an organizational open-source intelligence (OSINT) element, thereby strategizing a defensive deception process discretely optimized for real operational goals. In a follow-up study [46], IoT-based organizational deception modeling (IoDM), which represents a partial general-sum-based lightweight deception modeling designed to protect Internet-of-Things (IoT)-based organizational networks built by domain, was presented.

D. STOCHASTIC GAME THEORETIC MTD

Among cases of stochastic game-theory-based MTD studies that reflect the correlations among multi-agents through stochastic state transitions, Manadhata et al. [47] proposed a game model that diversifies the dynamics according to real-time battles based on stochastic transitions in accordance with decision-making flows, and reflects the multifaceted

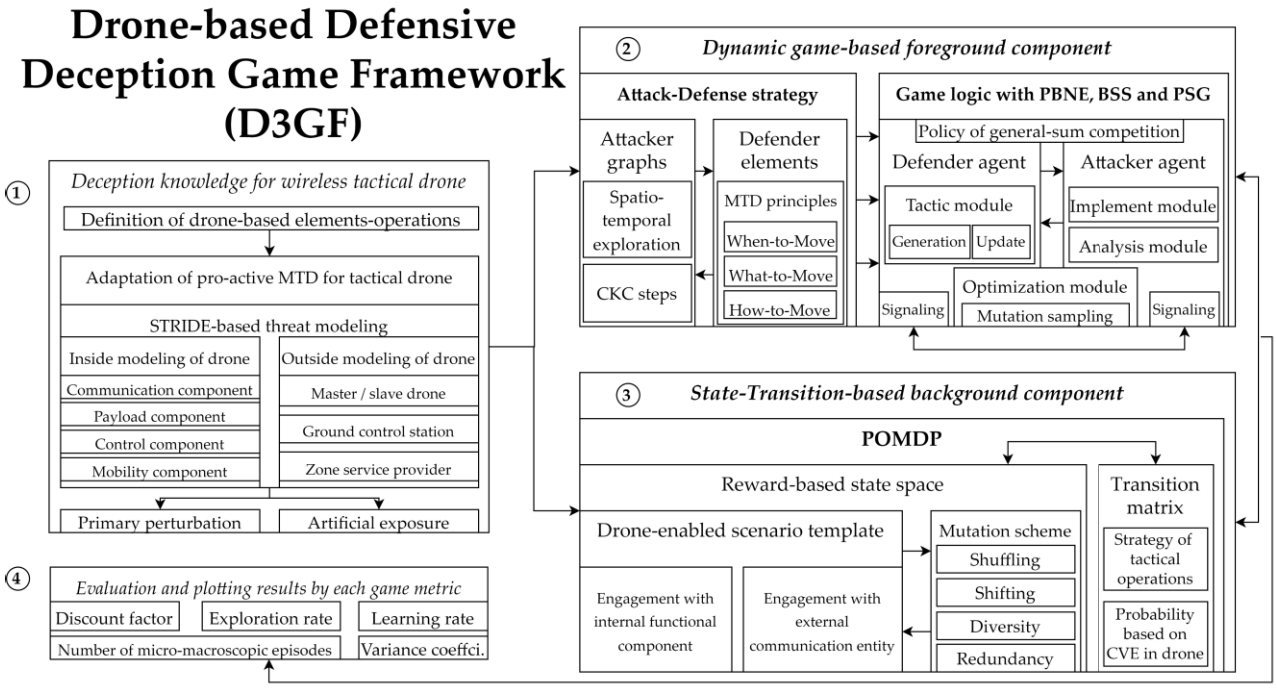

FIGURE 2. Main overview of D3GF for performance evaluation with drone-type MTD.

causality on the MTD strategies. The optimal MTD strategies are formalized based on the vulnerable surface configurations characterized environmentally.

Finally, Zhang et al. [48] proposed the Nash-Q learning algorithm, based on a stochastic reward matrix constructed by capturing the attacker's strategy selection frequency and value distribution, thereby resolving the issue of incomplete information asymmetry by actor. According to this previous study, the Nash theory was proven to accurately reflect actual operational scenarios compared to other game theories, and the availability-based trade-off relationship due to the calculation of MTD factors could also be quantified.

E. COMPARATIVE ANALYSIS BY PREVIOUS STUDIES FOR PROPOSED MODEL

Previous game-theory-based MTD studies limited the defense performance evaluation only to the MTD concept, and thereafter also only performed sensitivity analysis limited by some shuffling set. In addition, they did not adaptively optimize the MTD strategies to fit the unique characteristics of the target network or organizational environment, or consider hierarchical state-transition couplings with other deception elements in detail. Seo et al. [44], [45], [46] attempted to mitigate these limitations by additionally selecting the unique organizational OSINT elements as the primary mutation set groups of MTD while constructing a virtualized sandbox container-based social engineering decoy, thereby formalizing the game logic framework combined with the MTD sequence.

However, same as previous researches, because these supplemented studies consider engagement logic architecture with MTD only for wired-network-based organizational operations, reliable evaluation results cannot be guaranteed for all drone-related sub-entities, wireless communication elements, detailed specification information, or indicators. In addition, the analysis of MTD-based threat modeling design, which must be preemptively configured to identify potential security vulnerabilities of drones and other lightweight unmanned vehicles, is still extremely inadequate.

In contrast to the aforementioned studies, the drone-type MTD sequences presented in the present research account for the dedicated threat modeling concept with formal method-based standard. We also present a performance analysis of deceptive MTD defenses considering all correlations between internal functional components of drones and communication entities external to drones, which can be quantified utilizing the multi-sum game engagement logic-based D3GF.

III. PROPOSED D3GF FOR PERFORMANCE EVALUATION OF DRONE-TYPE MTD

The following section presents a novel drone-type MTD algorithm that introduces the concept of deceptive protection to internal and external environments of tactical drones. D3GF, a model-free type general-sum framework for competitive engagement simulation, is formalized in detail with respect to major modules and components. All metrics and formulas related to decision logic, such as PBNE and BSS scheme applied in D3GF, are likewise defined.

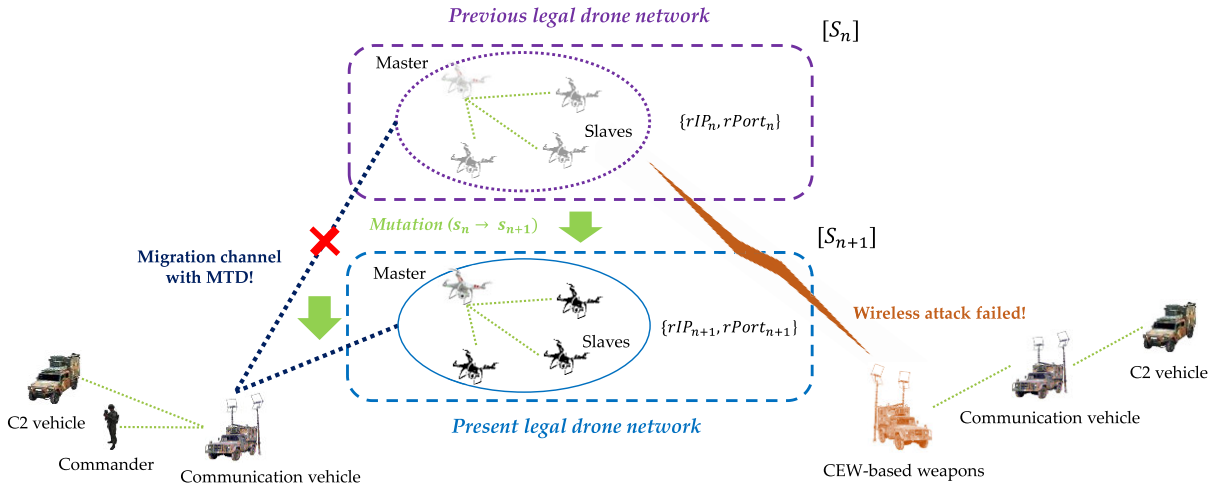

FIGURE 3. Conceptual diagram of drone-type MTD.

A. DESIGN PRINCIPLE

As shown in Figure 2, the main structure of D3GF, which is a general-sum-based game simulation framework with drone-type MTD, is representatively composed of four modules.

The deceptive knowledge module (①) performs overall formal method-based threat modeling for the pre-identified functional elements of internal components of drones, communication elements of external entities, and related interoperable sequences. In addition, the social engineering schemes (perturbation, disclosure) to apply drone-type MTDs by vulnerable elements are formalized, and major factors to determine the three principles of MTD ('When-to-Move', 'What-to-Move', 'How- to-Move') are configured in detail for use in the dynamic game-based foreground module (②) and state-transition-based background module (③).

In the foreground module, mutation sampling optimization is carried out by establishing engagement modeling based on perfect Bayesian Nash equilibrium (PBNE), Bayesian stochastic Stackelberg (BSS), and partial signal game (PSG). Subsequently, general-sum-based competition simulation is performed based on attack/defense sequences by actor. In the background module, to maintain the asymmetric predominance of defense drones and assess combat damage, the CVE-based vulnerabilities of targets internal and external to drones are specified, and CVSS-based quantification is implemented. Thereafter, the POMDP is formalized based on established scenario templates for targets and related matrices, and the decision behaviors are schematized by each actor.

And, based on a detailed consideration of the Pareto frontier-based optimal payoff and related competition game equilibrium entry states in accordance with MIQP-based constraint conditions, an evaluation of deceptive defense performance is carried out in parallel with analyses of sensitivity by key metrics (discount factor, exploration rate, learning rate, macroscopic episode, microscopic step, variance coefficient), finally deriving the results of related comparisons and analyses.

B. CONCEPTUALIZATION OF DRONE-TYPE MTD

The drone-type MTD, based on the perturbation and disclosure designed in the proposed D3GF, is determined from the conceptual outline drawing shown in Figure 3 based on Figure 1.

Here, the drone-type MTD – which was introduced to alleviate issues such as unsecured wireless operability in existing MTD and the exclusiveness, lightness, non-independence, and non-regularization of drones – is a concept of the MTD selection strategy to determine an appropriate deceptive sampling method to select the shuffling cycle, mutation strength, and gene sets suitable for the drone network. Specifically, the defender manually selects the MTD mutation sampling tactic and adjusts the strength of active avoidance against invading forces realizing cognitive disarrangement based on passive perturbation [26] and active disinformation [44], [45], [46].

That is, the drone-type MTD is constructed with Bellman value iteration-based concept of artificial disclosure (*AD*). This approach combines the concept of perturbation (*P*), which asymmetrically imposes noise on the attacker's cognitive directivity, and the adaptation of mutation according to varies in offensive actions, and is configured in detail as *P*-based Equation 1 and *AD*-based Equation 2, respectively.

$$P = Pr[F_t = f|O_t = \mu(o)], \tag{1}$$

Here, F_t is a set of fake elements that is dynamically signaled by the defender to distort and deflect the reflection threshold for the exploit step at the time of weaponization, using the attack surface of the drone identified by the external attacker at time t in favor of the drone-type MTD defender. O_t is a set of actual drone information groups that minimize the attacker's suspicion of the defender's juggle while improving

TABLE 1. Pseudo-code-based drone-type MTD algorithm.

Perturbation (Equation 1)	Artificial Disclosure (Equation 2)
INPUT: $\hat{f}, \check{f}, f_0, \theta$	INPUT: $T, \hat{a}, \check{a}, C, \theta$
	$x \in T, \quad t = 0, \quad AD^D(x) = 0, \quad \tilde{d} = 0$
$t = 0, \quad avg_{list} = \emptyset, \quad \mu(s) = [F = f_0]$	***WHILE*** $C \times \widetilde{AD} > \widehat{AD} - \widetilde{AD}$:
FOR $f = \check{f}\,;\ f \le \hat{f}\,;\ f = f + \theta$:	$t = t + 1$
$t = t + 1$	***FOR*** $x \in T$:
	$V = \infty$
$\hat{P} = \max_{f_0} \lvert\mu(s) \mid \sum_f P(f \mid s) LC\rvert$	***FOR*** $a = \check{a}\,;\ a \le \hat{a}\,;\ a = a + \theta$:
$\check{P} = \min_{f_0} \lvert\mu(s) \mid \sum_f P(f \mid s) LC\rvert$	$\widehat{d*} = \operatorname{argmin}_d \lvert AD^t(x, \hat{d}, a)\rvert$
	$V* = \lvert AD^t(x, \widehat{d*}, a)\rvert$
IF $\hat{P} - \check{P} < LC \times P$	***IF*** $V* < V$
$avg_{list} = \hat{P} - \check{P}$	$\hat{d}_x^* = \widehat{d*}, a_x^* = a, V = V*$
ELSE	$AD^t(x) = V$
CONTINUE	
RETURN $P = P \times \max(avg_{list})$	$\widehat{AD} = \max_{x \in T} \lvert AD^t(x) - AD^{t-1}(x)\rvert$
	$\widetilde{AD} = \min_{x \in T} \lvert AD^t(x) - AD^{t-1}(x)\rvert$
	RETURN $\widehat{d*} = \widehat{AD} - \widetilde{AD}$

the efficiency of the MTD of F_t utilized at time t. $\mu(o)$ is a function that calculates the probability that the attacker predicts the drone's information considering the cognitive impact of o, which is an actual random information group partially observable by the attacker, such as F_t.

$$AD_e^t(i) = \min_{\tau_i, S_i, \in S} \left[c_{i,j} + \sum \tilde{d}_{i,j} AD^{t-1}(j) \right], \tag{2}$$

Next, $c_{i,j}$ is a function to derive the expected mutation cost when moving from index i for the attack surface of the drone in episode e, to index j for the potential attack surface. This function is used to optimize the selection of mutation candidate groups at time t within the networks internal and external to the drone involving limited security resources. $\tilde{d}_{i,j}$ signifies the distinguishability of the external attacker according to i and j, and is configured to minimize the suspicion of an attacker that continuously examines the state of the target drone hierarchically. τ_i is the mutation time slot length-based total temporospatial cost consumed to maintain the defender's predominance until the mutation of the drone attack surface element F for i is complete, and s_i is a drone surface element sampled and optimized based on i within S, a set of deceptive attack surfaces formalized through mutation.

Therefore, the algorithm formalized from Equations 1 and 2 is shown in Table 1. Among the parameters added to construct the algorithm of Equation 1, $\hat{f}$ denotes the maximum number of false elements capable of perturbation, $\check{f}$ is the minimum number thereof, f_0 represents the group of false elements selected to maximize the initial cognitive bias at first time, and LC denotes the total leakage cost by the drone-type MTD. Among the parameters added to construct the algorithm of Equation 2, T encompasses all time point set groups available based on the mutation time slot length throughout the drone's operation, $\hat{a}$ is the supremum of the defender's response time, $\check{a}$ is the lower limit thereof, C is the total mutation cost for the drone-type MTD in the current game, and V the attack surface of the drone identified by the attacker. θ, which is commonly used by individual formulas, denotes the time required until the drone-type MTD responds.

To normalize the designed drone-type MTD as the main proactive defense process in the tactical rugged drone, the corresponding MTD scheme is specified using atomic variables that are required for all competitive behaviors in the dynamic game foreground and POMDP state-transition background modules.

C. CONSTRUCTION OF MULTI-SUM GAME-BASED DRONE-TYPE MTD MODELING

By modeling a dynamic game-based foreground module that performs general-sum-based competitive attack-defense simulations within the proposed D3GF, we achieve the optimization of mutation performance in the drone-type MTD. Because this foreground module includes game-based optimization components take in decision logics with PBNE, BSS, and PSG, as well as drone attack-defense strategy component based on the state-transition probability matrices by actor, the corresponding dynamic game module is representatively constructed as shown in Figure 4.

First, the optimization component with general-sum game includes the PBNE-based decision tactic that maximizes the drone defender's payoff for each episode by considering the privatized asymmetric decision relationship based on

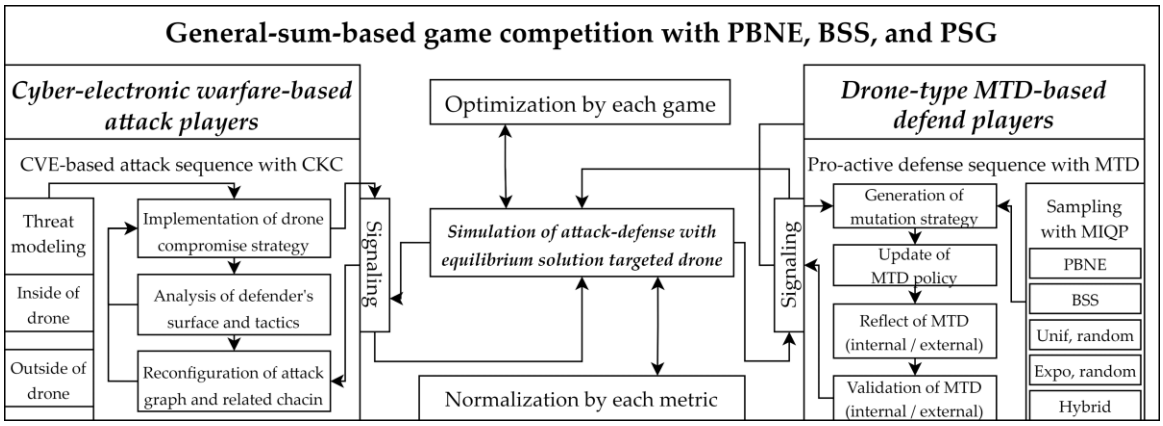

FIGURE 4. Detailed overview of dynamic game-based foreground module in D3GF.

incomplete information constructed between the drone defender and attacker. Utilizing the ratchet-type causality between the active leader and passive follower, the BSS-based decision tactic that optimizes the quantitative sequential relationship for the micro/macroscopically calculated reward is also applied. Furthermore, the PSG-based decision tactic is adopted to enforce the drone attacker's priori belief and confusion with the defender's advantage, as well as maintain the initiative.

Next, the attack-defense strategy component is configured to refer to the internal/external configuration topology, detailed sensors, specifications, equipment, communication channels, detailed vulnerabilities, attack graphs, and related scenarios pre-defined in the state-transition-based background module. From this configuration, the engagement flow is competitively designed and simulated considering the goals (invasion, protection), techniques (breaching, avoidance), and sequences (attack, defense) calculated for each drone actor.

In this case, the foreground module is configured a total of 15 tuples as follows.

- $N = (N_A, N_D)$ is a set of drone actors, N_A is a cyber-electronic-warfare drone attacker, and N_D is a drone-type MTD-based drone defender. According to the game scenario and present engagement situation of the detailed episode, the payoffs calculated by the actor in N, signaling, and causality between the leader and follower are determined individually.
- $TS = \left(TS_{N_A}, TS_{N_D}\right), TS_{N_A} = (\rho), TS_{N_D} = (ts_i \mid i = 1, 2, \ldots, n)$ are the sets of intelligence elements uniquely possessed by individual drone actors, TS_{N_A} is selected as an attack-graph-based private information element group identified by drone attacker N_A, and TS_{N_D} is selected as a threat-modeling-based element group identified by the drone defender N_D to apply MTD inside and outside the drone. TS_{N_A} and TS_{N_D} are combined or divided based on the payoff that variates according to episodic development. Unlike the defender, the attacker additionally considers ρ as the effective indicator of the attack surface based on the threshold, thereby dynamically contributing to the composition of the element groups.
- $GS = \left(GS_{N_A}, G\,S_{N_D}\right), G\,S_{N_A} = \left(gS_{N_{Aj}}[j = 1, 2, \ldots), GS_{N_D} = \left(gs_{N_{Di}} \mid i = 1, 2, \ldots\right)\right.$ are the sets of decision tactics for general-sum engagement between drone attacker $N_{A|}$ and defender N_D, determined according to the payoffs derived by the actor and a priori causality. That is GS_{N_A} is a set of invasive decision tactics composed by adopting elements in TS_{N_A} as main attack surface information, and GS_{N_D} is dynamically determined as a set of avoidant decision tactics that regulate the elements in TS_{N_D} as major subjects of active defense by the MTD.
- $SS = \left(SS_{N_A}, S\,S_{N_D}\right), S\,S_{N_A} = \left(SS_{N_{Aj}} \mid j = 1, 2, \ldots\right), SS_{\mathrm{V}} = \left(SS_{N_D}(i = 1, 2\ S\ S_{N_D} = \left(ss_{N_D}[i = 1, 2, \ldots\right)\right.$ are sets of PSG-based signaling possessed by drone attacker N_A and defender N_D, respectively. Whether to refer to them is selected according to the signaling initiative. That is, SS_{N_A} is an attack signal set group that is asymmetrically activated when N_A acquires the signaling initiative, and SS_{N_D} is formalized as a proactive deception signal set maintained when N_D continuously achieves protection against the drone network.
- ω is a threshold-based signal attenuation factor that determines the degree of activation of SS_{N_D} of drone defender N_D according to the development of general-sumbased engagement episodes.
- $GB = \left(GB_A, \widetilde{GB}_A\right), G\,B_A = \left(GB_A\left(gs_{N_D}\right) \mid i = 1, 2, \ldots\right), G\widetilde{B}_A = GB_A\left(gs_{N_{D_i}} \cdot \omega\right)$ denote the game belief sets of drone attacker N_A based on the PSG-based cognitive dependence relationship, and GB_A represents the prior belief set of N_A before the signaling of defender $N_D \cdot \widetilde{B}_A$ is the posterior belief set of N_A dynamically determined according to Bayes' theorem following cognitive intervention of N_D spoofed based on SS_{N_D}

- $S = (s_i \mid i = 0, 1, \ldots k)$ is a set of finite states determined based on GS and SS in the general-sum-based dynamic game module, involving multilevel properties to structure the act of drone-based engagement in the state-transition probability matrix as POMDP with formal methods.
- $A = \left(A_{N_A}, A_{N_D}\right), A_{N_A} = \left(a^j_{N_{A_i}}[j = 1, 2, \ldots y), A_{N_D} = -A = \left(A_{N_A}, A_{N_D}\right), A_{N_A} = \left(a_{N_A} j = 1, 2, \ldots y\right), A_{N_D} = \left(a^i_{N_{D_i}}\, i = 1, 2, \ldots x\right)$ are sets of finite actions of drone attacker N_A and defender N_D for $S.A_{N_D}$ defines N_D 's drone-type MTD avoidance-based acts of protection for s_i as and A_{N_A} constructs N_4 erability-based acts of compromise of CKC (reconnaissance and exploration, weaponization, exploit, lateral movement, privilege escalation, final compromise, occupation, and action on objectives) as a half-duplex transition relationship.
- $\theta(S_k, a_x, a_y, S_{k*})$ is a probability distribution function to discretely calculate the probabilities for drone attacker N_A and defender N_D to reach the next period goal state S_{k*} when they perform acts $a_x$and a_y.
- $R(S_k, a_x, a_y)$ is a function to calculate the reward obtainable in the current combat episode when drone attacker N_A and defender N_D perform acts a_x and a_y, respectively, in an arbitrary state S_k. Here, $N_{D,}$ competes with N_A to maximize R as a pre-constraint condition before entering the general-sum game-based equilibrium.
- $U = (U_A, U_D)$ is a general-sum-based discount factor function that cuts off the solution space to limit the ranges of cognitive decision by actor, thereby indirectly copying competing tactics such as limiting surface by actor, distortion of intelligence, disinformation, artificial disclosure, and perturbation.
- $CU = (CU_A, CU_D)$is a utility function that indicates the resources and costs by actor charged when performing a general-sum-based act of competition.
- $P_{rx} = -10 \times n \log_{10} D + P_{tx}, D = |D_{rx} - D_{tx}|$is an RF and WiFi-based wireless communication availability indicator for evaluation of the MTD performance of subjects external to drones. Using trilateration considering the locations of drone defender N_D, attacker N_A, and other access point-based beacons conceptualized for signal analysis, the strength of the follower's received signals based on PSG is calculated. In this case, D_{rx} indicates the 2D position of the signal receiver, D_{tx} represents the position of the signal sender, and P_{tx} denotes the signal transmission power. In addition, n is the constant of path loss based on the Friis propagation loss model.
- $P_L(D) = (10 \times \log({}^{P_{tx}}/_{1mW})) - (10 \times \log({}^{P_{rx}}/_{1mW}))$ is a power density function for the linear application of communication signal attenuation in the wireless communication space, and a variable of loss to amplify the environmental hostility of n in P_{rx}.
- $SMF = w_1 + w_2 \leftleftarrows$ is a probability factor within the [0,1] section to monitor the subject's security state in the drone, and w_1 denotes the weight when the drone-type MTD fails in the defense of profiling for its internal components. w_2 represents the weight when the actions on objectives for internal components are allowed.

Using these tuples, the general-sum game logic in D3GF is normalized in the form of PBNE, BSS, and PSG. In addition, decision sequences to optimize the payoff by competing drone actors are determined from the game equilibrium state. From an episodic defensive behavior perspective, if the drone defender is selected as an active deceptive leader, it is possible to force the drone attacker to identify false attack surfaces created using drone-type MTD-based disinformation, artificial exposure, and perturbation. When a deceptive signal is transmitted, only the attack surface information biased to the defender's advantage is provided to the attacker, who is a passive successor and recipient of the signal. Accordingly, a decision sequence based on the BSS-PSG is configured so that both the total attack success probability and spatio-temporal attack asymmetry are attenuated. The PBNE-based a priori decision sequence is designed under consideration of the temporal and spatial cutting of decision range with Pareto optimality according to the predefined discount coefficient.

In the dynamic game module of D3GF, the reward optimization concept related to dependent reasoning acts according to the leading actor is organized in detail as a Q-Value scheme expressed in Equation 3.

$$\begin{aligned} Q\left(S_k, a_x, a_y\right) = R\left(S_k, a_x, a_y\right) \\ + U \sum\nolimits_{S_{k*}} \theta(S_k, a_x, a_y, S_{k*}) \cdot TS \\ \cdot OPT\left(S_{k*}\right) + CU, \end{aligned} \tag{3}$$

Because $OPT\left(S_{k*}\right)$ is also calculated through all SSs and GBs utilizable in S_{k*}, an optimized reward value can be obtained.

$$\begin{aligned} OPT\left(S_{k*}\right) = \max_{SS} \min_{a_x} \sum_{ay} Q\left(S_k, a_x, a_y\right) \\ \cdot \left(SS_{N_{D_i}} \mid i = 1, 2, \ldots\right) \cdot GB, \end{aligned} \tag{4}$$

In this case, this optimization method based on (3) and (4) is divided among Equations 5 and 6, considering the drone's internal operation and external communication environments, respectively. That is, Equation 5 adjusts the optimal value by adding SMF in (4) to consider the operational security state inside the drone, whereas Equation 6 amplifies both P_{rx} and $P_L(D)$ to conceptualize the unique wireless communication characteristics outside the drone for equilibrium.

$$OPT_{internal}\left(S_{k*}\right) = OPT\left(S_{k*}\right) \cdot SMF, \tag{5}$$

$$OPT_{external}\left(S_{k*}\right) = OPT\left(S_{k*}\right) \cdot P_{rx} \cdot P_L(D), \tag{6}$$

The decision to enter the equilibrium state based on constraint conditions is also determined with OD and OA in Equations 9-10 based on Equations 3-8. Here, DP_D is the decision probability of drone defender N_D based on the prior probability for TS_{N_D} related to SS_{N_A}, and DP^*_D denotes the

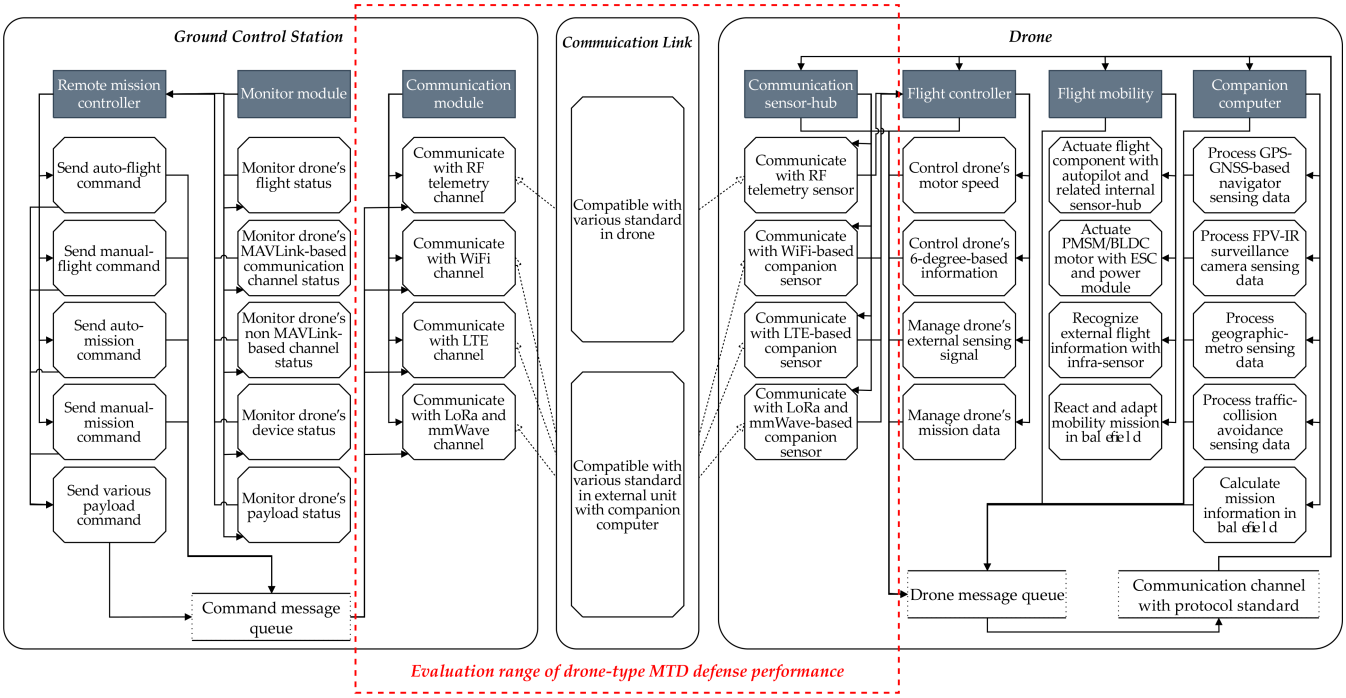

FIGURE 5. STRIDE-based conceptual data flow diagram with threat modeling on tactical drone.

posterior probability-based inference probability for SS_{N_D} reconstructed by N_D according to the MTD rule after reactively receiving the signal. In addition, the fine-tuning of DP_D and DP_D^* also relates to metacognition, and is therefore controlled according to the U_A and U_D configurations, closely related to signal initiative and equilibrium state entry time.

$$DP_D = \left(p_D \cdot \left(TS_{N_{D_i}}\right) \mid i = 1, 2, \ldots n\right) \tag{7}$$

$$DP_D^* = p_D^* \left(\left(TS_{N_{D_i}} \mid i = 1, 2, \ldots n\right) \mid SS_{N_A}\right), \tag{8}$$

$$OD\left(SS_{N_{A_j}}\right) = arg \max_{SS_{N_{D_k}} \in SS_{N_D}} \sum_{TS_{N_{D_i}} \in TS_{N_D}} DP_D^* \cdot F\left(TS_{N_{D_i}}, S\ S_{N_{Aj}}, S\ S_{N_{D_k}}\right), \tag{9}$$

$$OA\left(TS_{N_{A_i}}\right) = arg\ max_{SS_{N_A} \in SS_{N_A}} \mid F\left(TS_{N_{A_i}}, SS_{N_{Aj}}, O\ D\left(SS_{N_{A_j}}\right)\right), \tag{10}$$

D. DEFINITION OF DRONE VULNERABILITIES AND THREATS FOR MTD ANALYSIS

1) CONFIGURATION OF VULNERABILITIES IN TACTICAL DRONES

Formal threat modeling with STRIDE and POMDP is performed in order to identify elements internal and external to drones that can realize the aforementioned active protection effect at the highest level according to vulnerabilities. Prior to construction of threat modeling considering the functional components internal to drones and external communication entity relationships, security vulnerabilities that could ensue during tactical drone operations must be preemptively analyzed under theoretical conditions [49].

Because all communications and security actions of tactical drones deployed in combat operate via remote control in the presence of commanders, in cases of electronic warfare attacks, the simultaneous response and protection against the relevant threat would be impractical. Specifically, related drone performance issues remain because existing channel and end-to-end encryption technologies protect only part of the payload area and status flags where the data and main authentication values in an arbitrary packet are located. Furthermore, the header area where transmission/reception routing information is placed remains unprotected. Consequently, the perimeter-based defense effect cannot be derived against the type of cyber-electronic-warfare that exploits header field information in drone transmission and reception packets, parts of MAVLink (Micro Air Vehicle Link) [50] message standards, or communication functionality. In addition, most unique fingerprints, including wireless specification characteristics, equipment information, and public CVE-based vulnerabilities of drones, already be disclosed by commercial vendors. Therefore, attackers could apply the dazzling fingerprints to the weaponization chain for target drones by making them into intelligence based on dictionary attacks. In particular, because most relevant data transmission and reception protocols are based on communication standards open to private domains, such as WiFi [51] or LTE [52], additional side effects could be caused owing to the vulnerabilities inherent to the relevant standards.

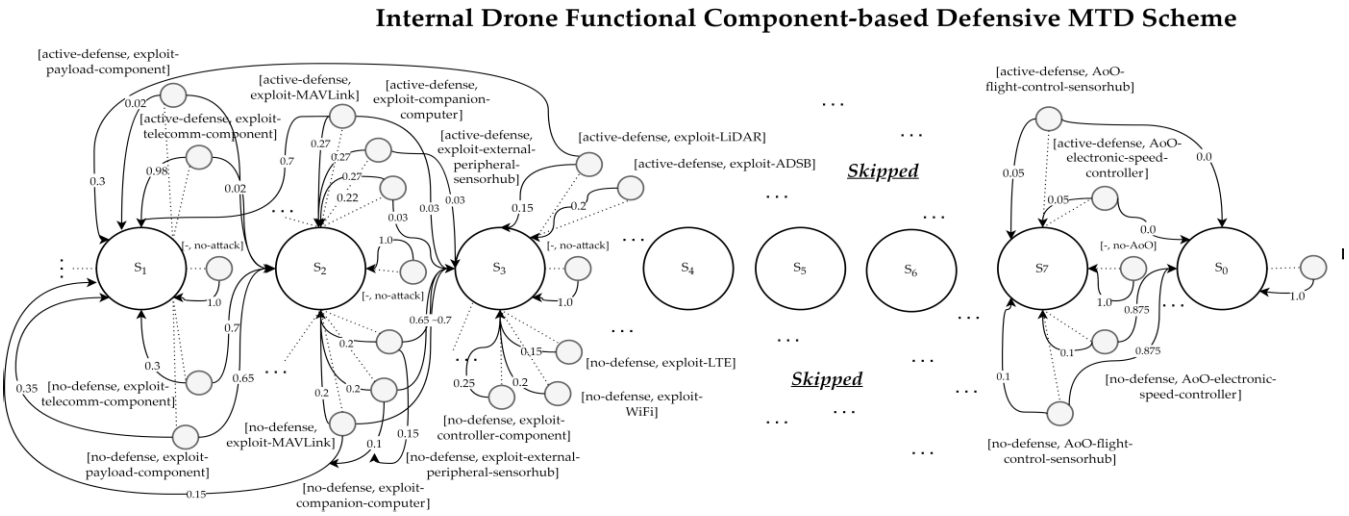

FIGURE 6. Detailed overview of MTD-based POMDP considering the inside of rugged drone.

TABLE 2. Table of CVE-CVSS by internal function component in rugged drone.

Category	Vulnerable Point	CVE ID	Vulnerability and Related Weakness	Target Device	Exploitability Score in CVSS 2.0
Controller	Flight controller	CVE-2019-14236	Privilege escalation with RCE	STM32F765 chip	10.0
	Flight sensor-hub	CVE-2020-8004	Information disclosure	STM32F100 chip	10.0
	Data storage	CVE-2017-2161	Privilege escalation with RCE	FlashAirTM SDHC	5.1
Mobility	Electronic speed controller	CVE-2013-4598	Privilege escalation with IAC	Zubax Orel 20	10.0
Communication	RF telemetry	CVE-2020-10281	Weak encryption	Holybro Sik Radio	10.0
	MAVLink sensor	CVE-2020-10282	Weak authentication	Pixhawk4	10.0
Payload	Mission companion	CVE-2022-0847	Privilege escalation with RCE	Raspberry pi 4 B	3.9
	WiFi	CVE-2019-13916	Memory corruption with OOB	BCM4345C0/6 chip	6.5
	LTE	CVE-2021-31698	Command injection with RCE	Quectel LTE EG25-G	10.0
	mmWave	CVE-2022-26147	Privilege escalation with CI	Quectel RG502Q-EA	10.0
	LiDAR	CVE-2018-20536	Information disclosure & DoS	Lidar-Lite v3	8.6
	ADS-B	CVE-2016-2107	Weak encryption	FLARM ATOM UAV	4.9
	FPV camera	CVE-2022-29945	Information disclosure	DJI Zenmuse X5s	10.0
	IR	CVE-2020-25785	Stack-based buffer overflow	Accfly Wireless IR	10.0

In addition, the combat space where tactical drones operate is considered hostile communication environment where the available tactical bandwidth is extremely limited in real time, as propagation losses and communication noise occur irregularly due to rapid temporospatial fluctuations. That is, the target force operating tactical drones in real time is conservative in securing security by applying conventional technologies (firewall, IDS, IPS), which has a great impact on network performance. Because this approach depends upon the practical operation manual, there could continue to be conflicts of interest in improving the security of drones.

Based on this theoretical preemptive analysis, we conclude that cyber-electronic-warfare threats to drones can potentially occur. Among the elements that establish the drones' internal functions, threats could target communication, payload components, mobility components, and control components. Among the entities that determine external communications, vulnerabilities could be intensified in the context of master/slave drones, GCS, and ZSP entities.

Therefore, the data flow diagram shown in Figure 5 is formalized to independently derive drone elements to which the drone-type MTD is applicable, as well as determine the threat propagation sequences related to competitive attack-defense.

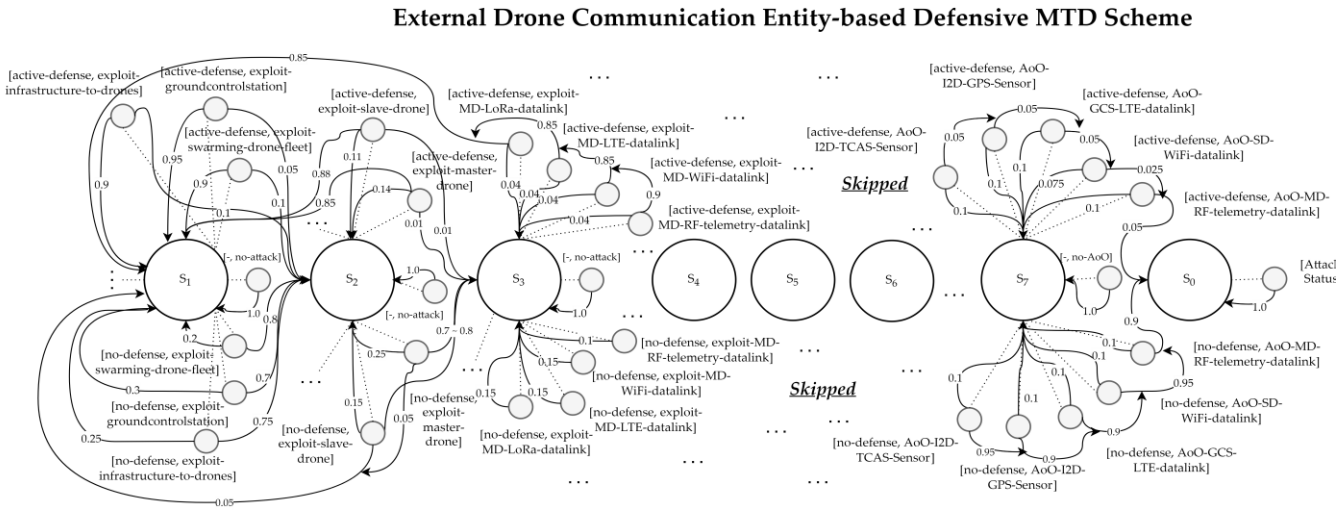

FIGURE 7. Detailed overview of MTD-based POMDP considering the outside of rugged drone.

TABLE 3. Table of CVE-CVSS by external communication entity in rugged drone.

Category	Vulnerable Point	CVE ID	Vulnerability and Related Weakness	Target Device	Exploitability Score in CVSS 2.0
Master drone	Downlink of RF	CVE-2020-10282	Weak authentication	RFDesign RFD 900	10.0
	Downlink of WiFi	CVE-2019-15894	Privilege escalation with IEC	ESP32 chip	3.9
	Downlink of LTE	CVE-2022-34059	Privilege escalation with RCE	Sixfab Base Hat	10.0
	Downlink of LoRa	CVE-2020-4060	Use-After-Free	Adafruit Feather M0	8.0
Slave drone	Uplink of RF	CVE-2020-10281	Weak encryption	Holybro Sik Radio	10.0
	Uplink of WiFi	CVE-2019-12587	Privilege escalation	ESP8266 chip	6.5
	Uplink of LTE	CVE-2022-34059	Privilege escalation with RCE	Sixfab Base Hat	10.0
	Uplink of LoRa	CVE-2020-11068	Buffer overflow with OOB	Adafruit Feather M0	8.0
Ground control station (GCS)	Datalink of RF	CVE-2020-10283	Weak authentication	Holybro Sik Radio	10.0
	Datalink of WiFi	CVE-2020-12638	Improper authentication	ESP8266 chip	5.5
	Datalink of LTE	CVE-2018-6311	Privilege escalation	FOXCOM Femtocell AP-FC4064-T	3.9
	Datalink of LoRa	CVE-2020-28349	Denial-of-service	ChirpStack LoRaWan	8.0
Zone service provider (ZSP)	Weather sensor-link	CVE-2018-18878	Privilege escalation with OOB	Columbia Weather	10.0
	GIS sensor-link	CVE-2014-5121	Cross-site-scripting	ESRI ArcGIS	8.6
	ATM sensor-link	CVE-2020-16124	Integer overflow in XML RPC	OpenRobotics ROS	10.0
	GPS sensor-link	CVE-2019-5748	XML external entity attack	Traccar GPS Tracker	10.0
	Electro-optical sensor-link	CVE-2018-10660	Command injection	AXIS Surveilance IP	10.0
	TCAS sensor-link	CVE-2019-13566	Buffer overflow with OOB	OpenRobotics ROS	10.0
	Gas sensor-link	CVE-2015-7907	Directory traversal attack	Honeywell Midas	10.0

In this case, STRIDE is threat modeling standard [53], [54] primarily used when the target system's security is evaluated and validated based on vulnerability analysis focusing on six properties, - authentication, integrity, non-repudiation, confidentiality, availability, and authorization. Therefore, various vulnerabilities inside and outside the drone that must be

TABLE 4. Major simulation parameters in D3GF.

Category	Parameter	Value
Common	Simulation time	Until the end of all allowed episodes
	Number of scenarios	2^1
	Number of states in POMDP	2^3
	Major general-sum-based game solver	Gurobi optimizer 9.0
	Language	Python 3.9.13 (Anaconda)
Drone-type MTD	Mutation set ('What-to-Move')	Component (internal), Entity (external)
	Mutation set range	2^5-2^{24}
	Mutation period ('When-to-Move') (s)	1-86400
	Mutation shuffling tactic ('How-to-Move')	Random
	Decision scheme for mutation period	Fixed
	Maximum number of attack graphs to be defended	2^3
	Probability of perturbation (%)	1-100
	Probability of artificial disclosure (%)	1-100
	Probability of disinformation (%)	1-100
	Probability of reliability of deceptive signal (%)	1-100
Decision strategy for e equilibrium	Competition type	Two-person
	Optimization model	MIQP with constraints (MIQCP)
	Optimization factor	Model-free type Q-value
	Matrix queue size for MIQP	10^7
	Enabled game logic for equilibrium	PBNE, BSS, PSG, uniform random, exponential random
	Discount factor (%)	0-100
	Exploration rate with attacker and defender (%)	5-45
	Learning rate	0.0001-0.001
	Learning rate decay	0.95-0.98
	Number of microscopic episodes	100-1000
	Number of macroscopic episodes	500-5000
	Number of trial with variance coefficient	5-100
	Batch size of decision strategy set	50

protected by the drone-type MTD can be identified, and the preprocessing before the attacker reconnaissance stage can also be conceptually simulated.

2) MATERIALIZATION OF POMDP-BASED DRONE THREAT MODELING

To stratify the general-sum-based drone attack-defense competition game in D3GF with state-transition matrix, as well as reflect the concept of formal threat modeling of targets internal and external to drones, the POMDP-based state-transition background module specified in Figure 2 is illustrated in Figures 6-7.

Figure 6 presents the form of the POMDP based on correlations between individual functional components internal to the rugged drone, which are quantified based on the CVE-CVSS vulnerabilities listed in Table 2 and the state-transition matrix presented in Table 5. Figure 7 also shows POMDP based on correlations between seperate external communication entities that can be closely connected to a rugged drone. The channel transition probability and reward values are determined in accordance with Tables 3 and 6.

IV. EXPERIMENTS OF ENGAGEMENT THROUGH DRONE-TYPE MTD

The following section presents optimal simulations of the competitive act of encounter between cyber-electronic-warfare drone attackers and MTD defenders within a general-sum-based solution of equilibrium normalized in D3GF. Sensitivity analyses by parameter were conducted in parallel to evaluate the defensive efficiency of the drone-type MTD according to scenarios for the inside and outside of the drone.

A. DETERMINATION OF MAJOR EXPERIMENTAL PARAMETERS IN D3GF

Before conducting the experiment, the simulation parameters were set according to Table 4.

In the case of drone-type MTD, three primary principles based on the mutation set and shuffling cycle were determined at the constant factor level, whereas the gene sampling range were detailed at the variable level of sub-parameters. And, in relation to perturbation, disclosure, and disinformation, the elements of total deceptive acts of the drone-type MTD were further amplified stochastically. Next,

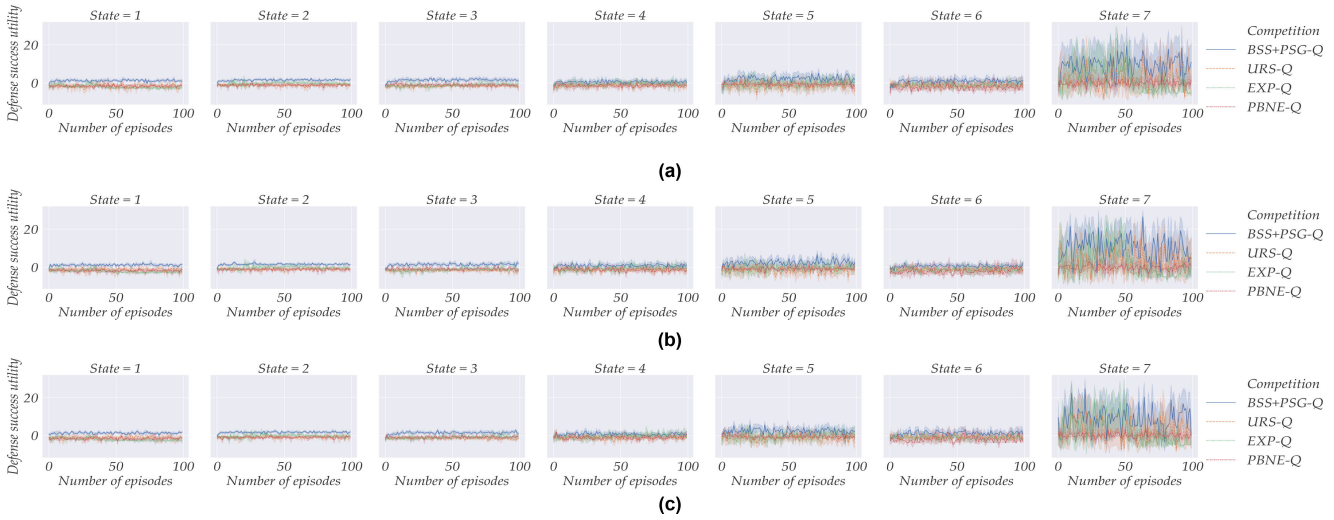

FIGURE 8. Comparison of MTD-based defense success utility inside rugged drone by each discount factor. (a) discount factor=0.9, (b) discount factor=0.8, (c) discount factor=0.7.

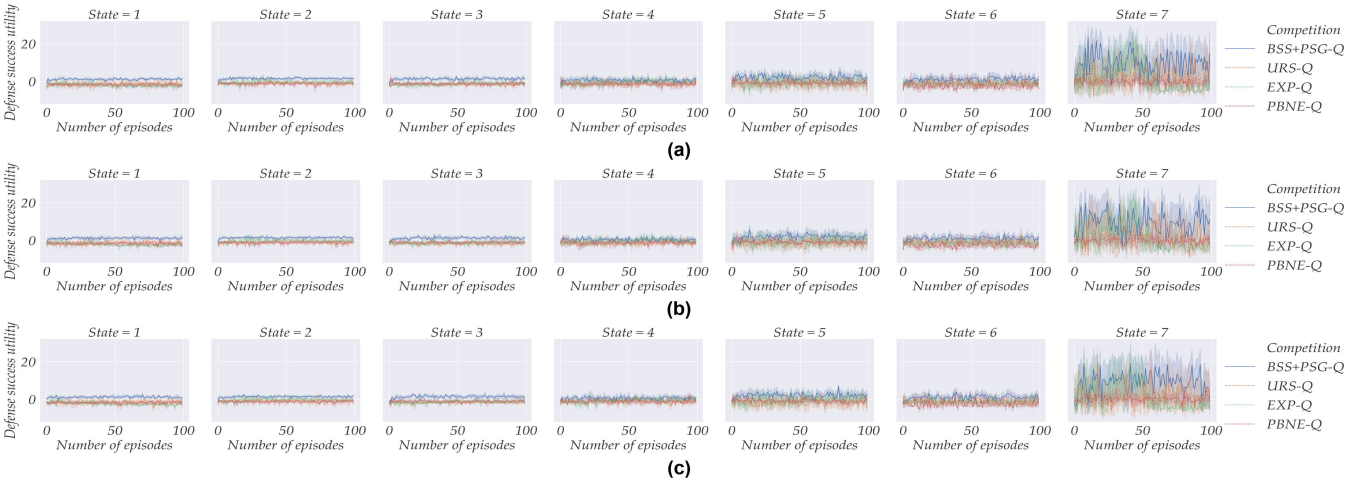

FIGURE 9. Comparison of MTD-based defense success utility inside rugged drone by each exploration rate (attacker). (a) exploration rate with attacker=0.05, (b) exploration rate with attacker =0.1, (c) exploration rate with attacker =0.15.

the two-player-based general-sum game strategy was applied to determine competitive engagement modeling by actor, mainly using the MIQP model based on the model-free type Q value, thereby determining that the model contributes to the calculation of MTD optimization considering PBNE, BSS, and PSG. In addition, game metrics such as discount factors, exploration rates, learning rates, macroscopic episodes, microscopic steps, and variance coefficients were dynamically introduced for sensitivity analysis based on random variables.

As the PBNE-based 'PBNE-Q' assumes complete knowledge of the drone attacker and defender rewards, it produces an arbitrary drone-type MTD that can be applied at all times as a Q-based mixed strategy. Because BSS and PSG-based 'BSS+PSG-Q' selectively assume partial knowledge of reward and greedy scheme based on the signal relationship between the leader and followers, the drone-type MTDs are normalized by episode. Finally, 'URS-Q' and 'EXP-Q' determine the drone-type MTD based on uniform and exponential distribution randomization, respectively.

B. COMPARATIVE RESULTS 1—SENSITIVITY ANALYSIS OF MTD FOR DRONE INTERIOR

By reflecting the defined encounter simulation parameters, the adaptive MTD mutation according to decision boundary was experimented. After classifying the defense efficiency of the MTD applied for independent protections of separate elements by POMDP state, the analytical scope was limited to comparing and analyzing only S_7, the final target state by major indicator. Accordingly, results of drone-type MTD performance analysis was formalized in the form of average values considering both the suprema and infima, as shown in Figure 8-13.

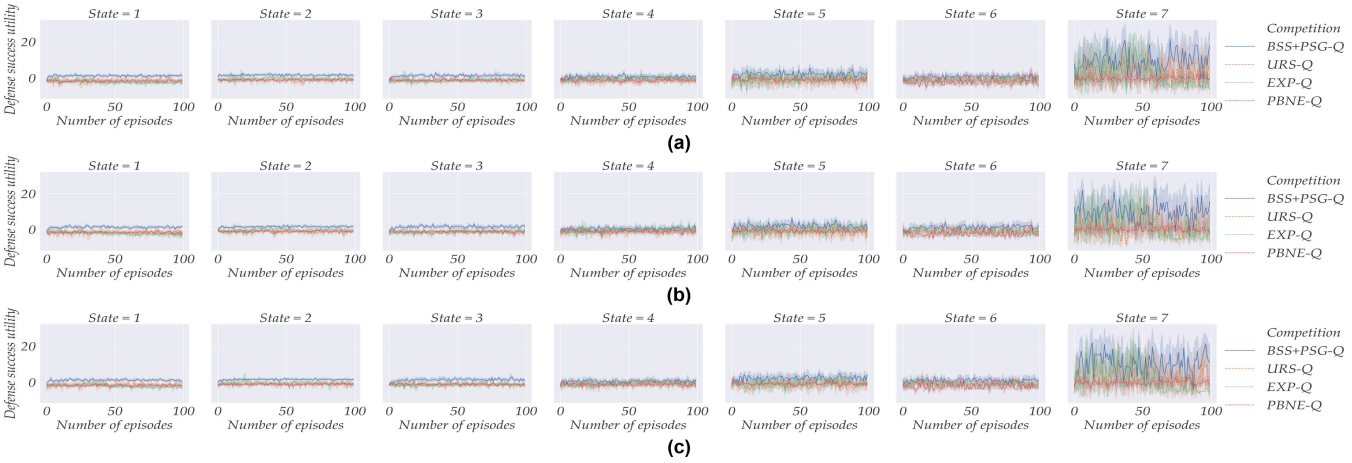

FIGURE 10. Comparison of MTD-based defense success utility inside rugged drone by each exploration rate (defender) (a) exploration rate with defender=0.05, (b) exploration rate with defender =0.1, (c) exploration rate with defender=0.15.

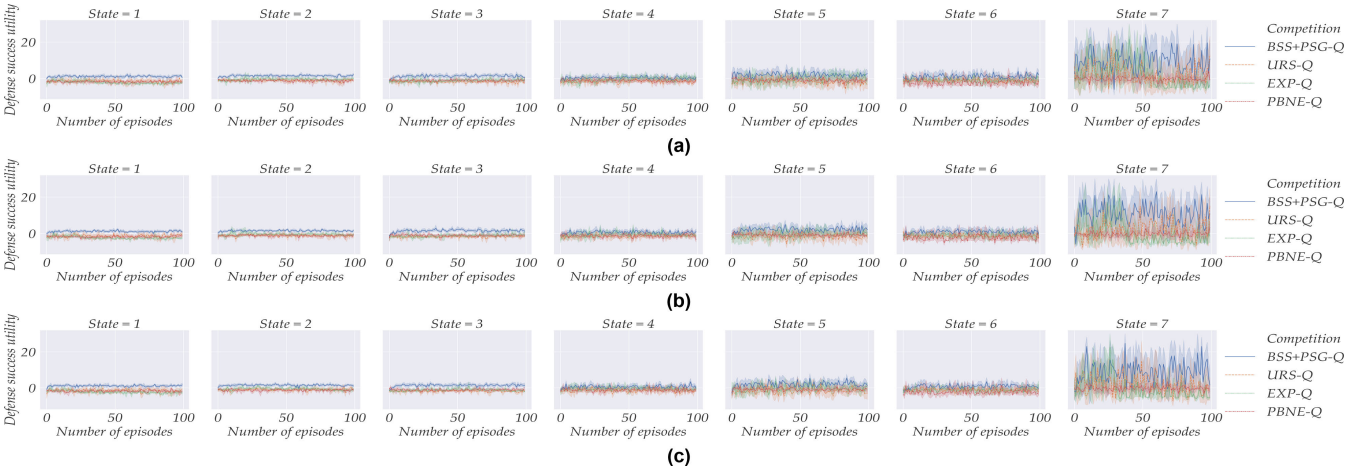

FIGURE 11. Comparison of MTD-based defense success utility inside rugged drone by each learning rate. (a) learning rate=0.0001, (b) learning rate=0.0002, (c) learning rate=0.0003.

In Figure 8, when the discount factor decreased from 0.9 to 0.8, the total defense success utility of the drone-type MTD exhibited an average increase of 15%. When this defense success utility was divided by game decision logic, we observed it to increase by 15% on average in the case of PBNE, 26% in the cases of BSS and PSG, and not more than 5% and 3%, respectively, in the cases of URS and EXP. However, when the discount factor decreased from 0.8 to 0.7, although the defense success utility was still higher than when the discount factor was 0.9, the total defense success utility exhibited a linear decrease of 9% on average. In Figure 9, when the exploration rate factor – which converts the arbitrary attack surface possessed by the target drone into intelligence from the attacker's perspective – increased from 0.05 to 0.15, the total defense success utility increased by 12% on average. Simultaneously, all reward values obtainable by episode were clustered in approximation of a normal distribution. This could indicate that despite although the drone-type MTDs were applied by internal functional components, the temporospatial asymmetry exploited by the attacker is inevitably formed slightly advantageously to said attacker. These comparative results were fundamentally reflected together with the concept of the drone-type MTD, which exhibits adaptive improvement.

Figure 10 shows that when the exploration rate factor used by the drone-type MTD defender increased 0.05 to 0.15, enabling passive perturbation and active expose to execute in parallel by projecting deceptive signals that are advantageous to the defender, the total defense success utility increased by approximately 7% on average. Furthermore, the defense success utility linearly increased by 3% on average in the case of PBNE, by 9% in the cases of BSS and PSG, and by approximately 2% in the cases of URS and EXP. This quantitatively proves that the inferior act, which the inherent drone-type MTD deliberately shows to the outside, can deceive attackers according to the defender's intention.

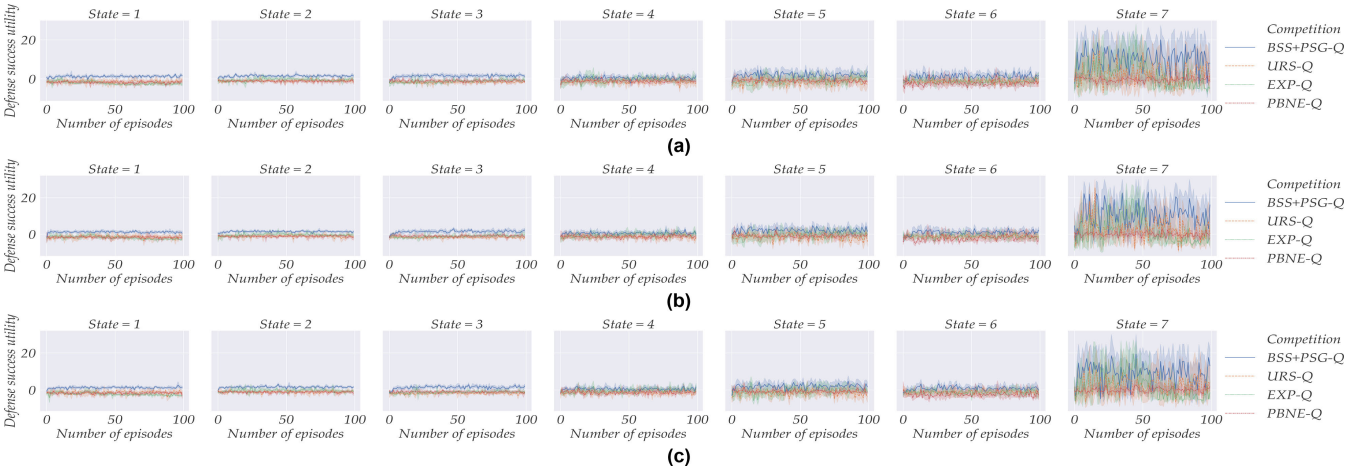

FIGURE 12. Comparison of MTD-based defense success utility inside rugged drone by each microscopic episode. (a) number of microscopic steps=500, (b) number of microscopic steps=600, (c) number of microscopic steps=700.

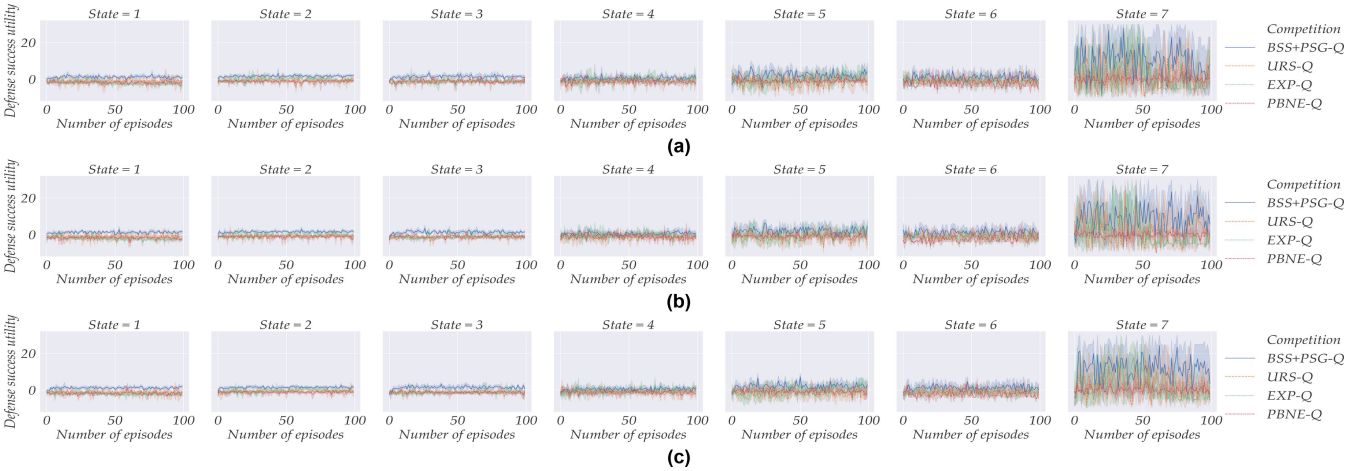

FIGURE 13. Comparison of MTD-based defense success utility inside rugged drone by each variance coefficient. (a) constant value of coefficient=5, (b) constant value of coefficient=6, (c) constant value of coefficient=7.

Figure 11 shows that when the learning rate factor introduced to reflect the improvement in performance increases from 0.0001 to 0.0003, the total defense success utility decreases by 27% on average. This indicates that the direction of this MTD supplement does not correspond to stable convergence towards the actual optimum value. Instead, it is based on the stochastic gradient issue wherein the range of momentum is determined in the form of convergence toward other Local minima with saddle point. In particular, these comparative results show that because the general-sum engagement simulation based on model-free Q is repeatedly carried out based on a Monte Carlo simulation, side effects based on the learning rate that did not consider the Global minima can propagate to all subsequent competition episodes. As shown in Figure 12, when the micro-episode factor – which indicates the maximum number of attack-defense attempts allowed by an actor in a random engagement episode – increased from 500 to 700, the total defense success utility of the drone-type MTD drastically decrease to 21% on average. Furthermore, the defense success utility converges toward 18% on average in the case of PBNE, 27% in the cases of BSS and PSG, and approximately 4% and 3% in the cases of URS and EXP, respectively. This result could be explained by the fact that the occurrence of competitive encounter between the attacker and defender is simulated after a part of the proactive shifting concept already implied within the MTD is assumed to have been neutralized by a specialized attacker. Therefore, the importance of active shuffling sequences achievable with MTD-based mutations can also be analyze.

Finally, Figure 13 presents comparison results of the variance coefficient factor, which relates to the attack efficiency constant when constructing the attack surface information identified by the drone attacker. We observe that when the variance coefficient increased from 5 to 7, the total defense success utility of the drone linearly increased by

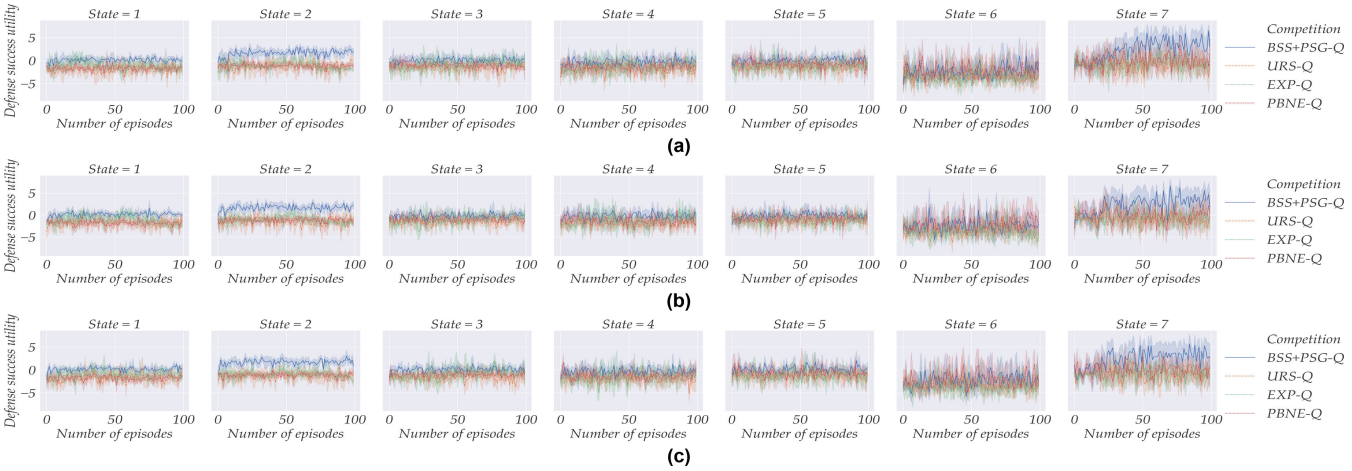

FIGURE 14. Comparison of MTD-based defense success utility outside rugged drone by each discount factor. (a) discount factor=0.9, (b) discount factor=0.8, (c) discount factor=0.7.

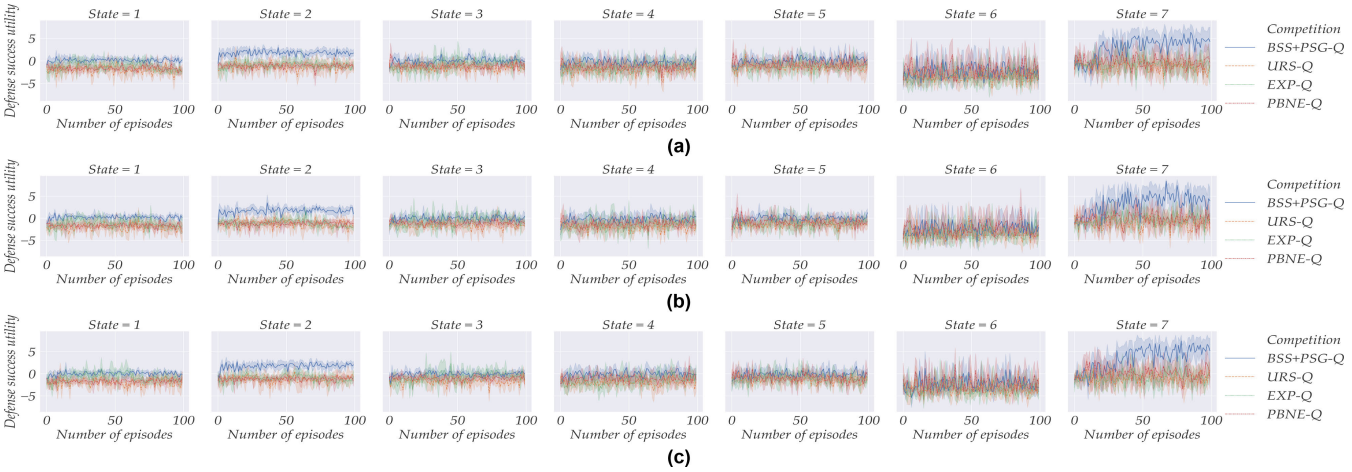

FIGURE 15. Comparison of MTD-based defense success utility outside rugged drone by each exploration rate (attacker). (a) exploration rate with attacker=0.05, (b) exploration rate with attacker =0.1, (c) exploration rate with attacker =0.15.

approximately 5∼7% on average, and uniformization toward the form of a normal distribution was also achieved gradually.

C. COMPARATIVE RESULTS 2—SENSITIVITY ANALYSIS OF MTD FOR DRONE OUTSIDE

Figures 14-19 presents the results of performance analyses in an environment where separate bi-directional communication channels were constructed so that target drone was as a subordinate command control entity connected to other command-auxiliary entities. These results are also shown in the form of mean graphs applied with suprema and infima.

Figure 14 shows that when the discount factor that adjusts the optimization range by cutting the ranges of cognitive judgment by actor decreased from 0.9 to 0.8, the total defense success utility of the drone-type MTD increased by 11% on average. Furthermore, the defense success utility linearly increased by 9% on average in the case of PBNE, 17% on average in the case of BSS and PSG, and 8% and 7% in the cases of URS and EXP, respectively. Unlike the inside of the drone as shown in Figure 8, even when the defense success utility additionally decreased from 0.8 to 0.7, the total defense success utility increased by approximately 6% on average. And the uniformity of reward values calculated by decision logic also gradually clustered in the form of a normal distribution. This result could be explained by the fact that the ranges of optimal judgment calculated by drone element were largely configured outside rather than inside the drome, and mutual dependencies between entities outside the drone connected in the form of communication channels. Furthermore, the temporospatial characteristic that the mutual dependency between entities external to the drone is lower than the hierarchical dependencies by component belonging to the inside of the drone was reflected.

From Figure 15, we observe that when the exploration rate factor based on the drone attacker increased from 0.05 to 0.1, the total defense success rate of the MTD increased

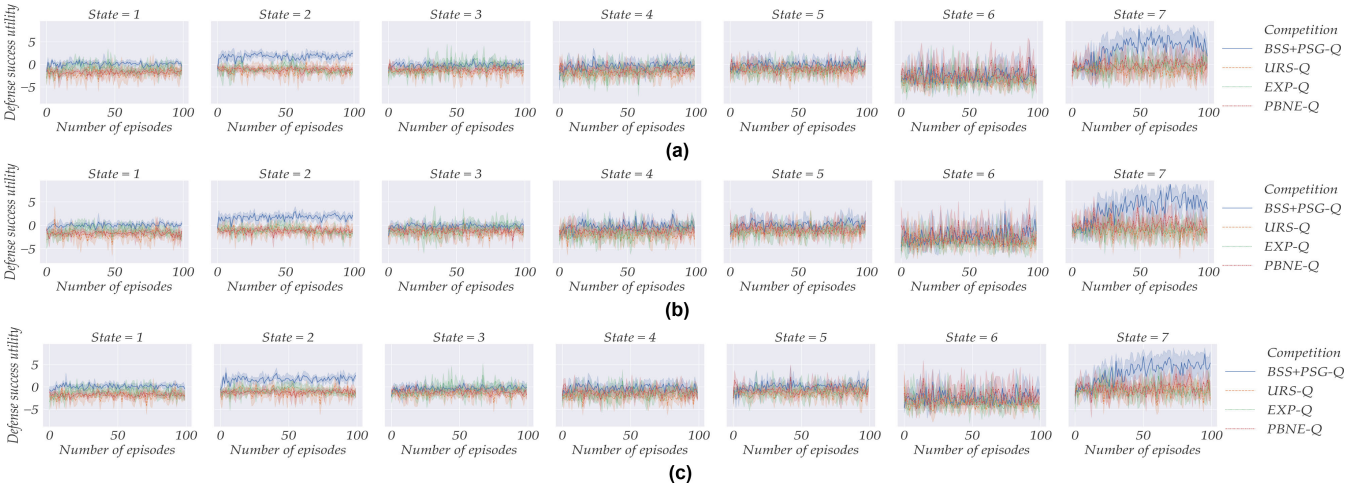

FIGURE 16. Comparison of MTD-based defense success utility outside rugged drone by each exploration rate (defender). (a) exploration rate with defender=0.05, (b) exploration rate with defender =0.1, (c) exploration rate with defender=0.15.

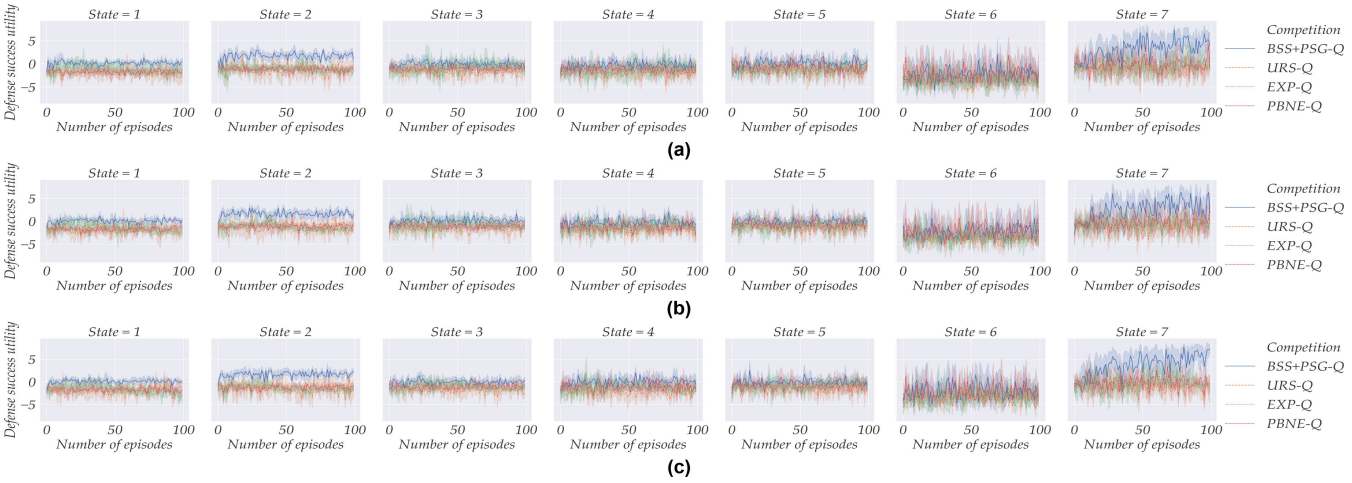

FIGURE 17. Comparison of MTD-based defense success utility outside rugged drone by each learning rate. (a) learning rate=0.0001, (b) learning rate=0.0002, (c) learning rate=0.0003.

by an average of 16%. In cases where the exploration rate increased from 0.1 to 0.15, the total defense success rate linearly increased by approximately 8% on average. When divided in higher detail than game concept, the defense success rate was shown to converge toward 5% on average in the case of PBNE, 15% on average in the cases of BSS and PSG, and 4% and 6% in the cases of URS and EXP, respectively. In Figure 16, when the drone defender-based exploration rate factor increased from 0.05 to 0.1, the total defense success utility of the MTD for a target outside the drones increased slightly to within 3% on average. However, when the exploration rate increased from 0.1 to 0.15, the total defense success utility linearly increased sharply by not more than 11% on average. This tendency proves that the range of influence of the attacker's threat is more limited in the external wireless environment than inside the drone based on wired modules, while the range of judgment of surface unique to the defender also can expand drastically when the range outside the drone is protected.

Unlike Figure 11, Figure 17 shows that when the learning rate factor increases from 0.0001 to 0.0003, the total defense success utility of the drone-type MTD is maintained in the form of a linear increase or decrease by approximately 3% on average. Also, based on the reduced solution space range according to non-dependency secured by the drone's external elements, the total defense success utility is relatively independent of the Local-minima-based gradient decision and side effect spread issues.

As shown in Figure 18, even when the microscopic episode factor sequentially increased from 500 to 700, the total defense success utility of the target MTD outside the drone exhibited linear increases and decreases of approximately 2% on average. This also quantitatively proves that the issue of asymmetry in favor of the attacker caused by competitive

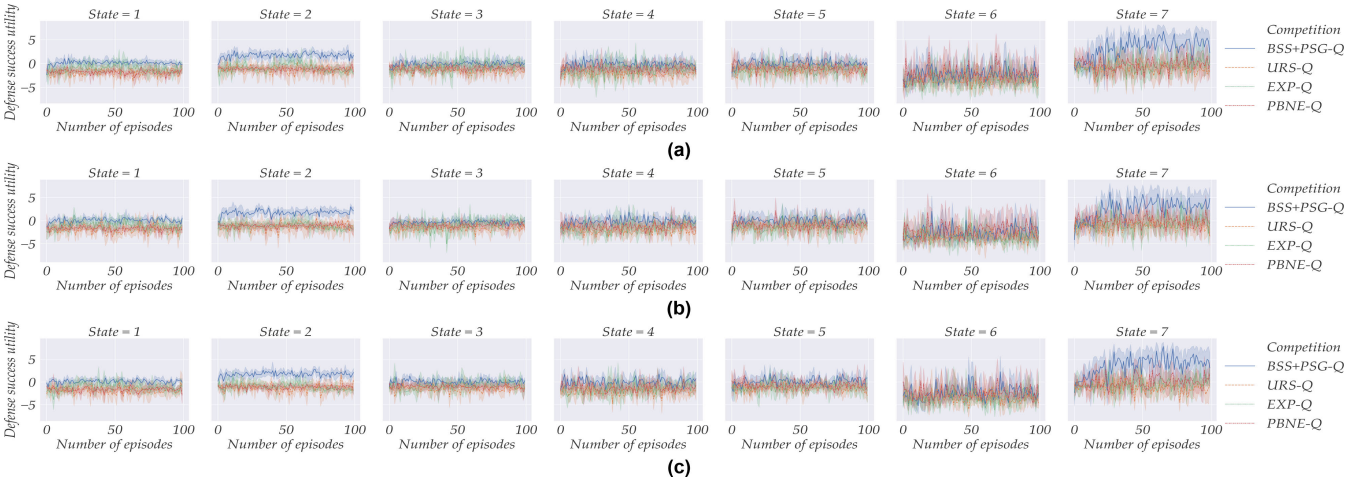

FIGURE 18. Comparison of MTD-based defense success utility outside rugged drone by each microscopic episode. (a) number of microscopic steps=500, (b) number of microscopic steps=600, (c) number of microscopic steps=700.

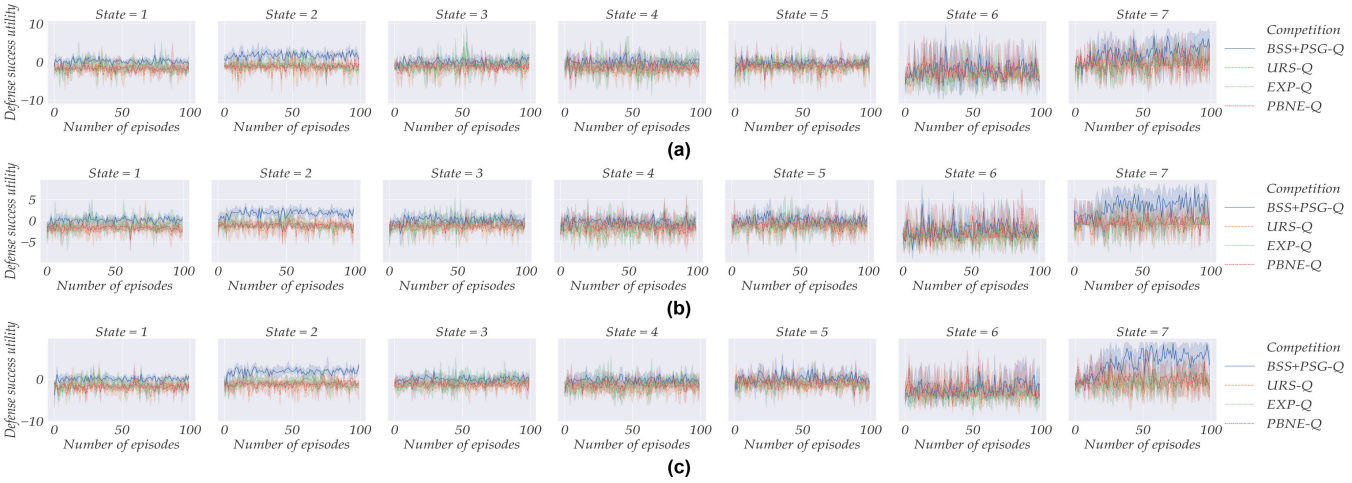

FIGURE 19. Comparison of MTD-based defense success utility outside of rugged drone by each variance coefficient. (a) constant value of coefficient=5, (b) constant value of coefficient=6, (c) constant value of coefficient=7.

engagement does not significantly occur successively in the external wireless environment.

Figure 16 shows that when the variance coefficient factor increased from 5 to 6, and from 6 to 7, the total defense success utility significantly decreased by 26% and 21%, respectively, on average. In addition, when results were subdivided by decision logic, the defense success utility can be observed to decrease by 12% and 10% on average, respectively, in the case of PBNE, by 35% and 31%, on average, respectively, in the cases of BSS and PSG, and by 11% and 9%, 13% and 12%, on average, respectively, in the cases of URS and EXP, respectively. Unlike the attack simulation scenario in Figure 13, which assumes only a single drone as compromised target from a macroscopic perspective, the foregoing tendency appears to quantitatively reflect the difference stemming from an expanded simulation range based on master drones, slave drones, GCS, and ZSP.

V. DISCUSSION AND CONCLUSION

As an active countermeasure to solve the domain limitations of previous MTD studies, this paper proposes the novel concept of the drone-type MTD. In addition, the D3GF framework was formalized for additional comparison and analysis of deceptive defense performance against drone wireless threats based on competitive engagement simulations. Multiple-sum engagement modeling was optimized based on perfect Bayesian Nash equilibrium, stochastic Stackelberg, and partial signal game. Subsequently, based on the formal threat modeling with POMDP, the target vulnerabilities of the drone's internal functional components and communication entities external to the drones were analyzed to establish the relevant wireless encounter sequences. In addition, after conducting a simulation experiment of engagement based on the adapted game decision logics, sensitivity analyses were also performed with quantitative

TABLE 5. Probability matrix of transition and semi-constant reward value with payoff strategy for inside of drone.

State	Probability of Transition
S_0	$[(1,0,0,0,0,0,0,0)]$
S_1	$\begin{bmatrix} (0,1,0,0,0,0,0,0) & (0,1,0,0,0,0,0,0) & (0,1,0,0,0,0,0,0) \\ (0,0.3,0.7,0,0,0,0,0) & (0,0.98,0.02,0,0,0,0,0) & (0,0.35,0.65,0,0,0,0,0) \\ (0,0.35,0.65,0,0,0,0,0) & (0,0.3,0.7,0,0,0,0,0) & (0,0.98,0.02,0,0,0,0,0) \end{bmatrix}$
S_2	$\begin{bmatrix} (0,0,1,0,0,0,0,0) & (0,0,1,0,0,0,0,0) & (0,0,1,0,0,0,0,0) & (0,0,1,0,0,0,0,0) \\ (0,0.15,0.2,0.65,0,0,0,0) & (0,0.7,0.27,0.03,0,0,0,0) & (0,0.15,0.25,0.6,0,0,0,0) & (0,0.15,0.25,0.6,0,0,0,0) \\ (0,0.1,0.2,0.7,0,0,0,0) & (0,0.15,0.3,0.55,0,0,0,0) & (0,0.7,0.27,0.03,0,0,0,0) & (0,0.15,0.3,0.55,0,0,0,0) \\ (0,0.15,0.2,0.65,0,0,0,0) & (0,0.15,0.35,0.5,0,0,0,0) & (0,0.1,0.3,0.6,0,0,0,0) & (0,0.7,0.27,0.03,0,0,0,0) \end{bmatrix}$
S_3	$\begin{bmatrix} (0,0,0,1,0,0,0,0) & (0,0,0,1,0,0,0,0) & \{skipped\} & (0,0,0,1,0,0,0,0) & (0,0,0,1,0,0,0,0) \\ (0,0.05,0.1,0.25,0.6,0,0,0) & (0,0.7,0.2,0.06,0.04,0,0,0) & \{skipped\} & (0,0.05,0.2,0.25,0.5,0,0,0) & (0,0.05,0.2,0.25,0.5,0,0,0) \\ \{skipped\} & \{skipped\} & \{skipped\} & \{skipped\} & \{skipped\} \\ (0,0.05,0.2,0.15,0.6,0,0,0) & (0,0.05,0.15,0.3,0.5,0,0,0) & \{skipped\} & (0,0.65,0.2,0.13,0.02,0,0,0) & (0,0.05,0.2,0.2,0.55,0,0,0) \\ (0,0.05,0.2,0.15,0.6,0,0,0) & (0,0.05,0.15,0.3,0.5,0,0,0) & \{skipped\} & (0,0.05,0.2,0.2,0.55,0,0,0) & (0,0.65,0.2,0.13,0.02,0,0,0) \end{bmatrix}$
S_4	$\begin{bmatrix} (0,0,0,0,1,0,0,0) & (0,0,0,0,1,0,0,0) & (0,0,0,0,1,0,0,0) & (0,0,0,0,1,0,0,0) \\ (0,0.1,0.05,0.05,0.1,0.7,0,0) & (0,0.8,0.1,0.04,0.04,0.02,0,0) & (0,0.05,0.1,0.05,0.2,0.6,0,0) & (0,0.05,0.1,0.05,0.2,0.6,0,0) \\ (0,0.1,0.05,0.05,0.15,0.65,0,0) & (0,0.05,0.1,0.05,0.25,0.55,0,0) & (0,0.78,0.1,0.05,0.05,0.02,0,0) & (0,0.05,0.1,0.05,0.25,0.55,0,0) \\ (0,0.1,0.05,0.1,0.15,0.6,0,0) & (0,0.05,0.1,0.15,0.2,0.5,0,0) & (0,0.05,0.1,0.15,0.2,0.5,0,0) & (0,0.76,0.1,0.06,0.06,0.02,0,0) \end{bmatrix}$
S_5	$\begin{bmatrix} (0,0,0,0,0,1,0,0) & (0,0,0,0,0,1,0,0) & (0,0,0,0,0,1,0,0) \\ (0,0.1,0.05,0.05,0.05,0.05,0.7,0) & (0,0.8,0.05,0.05,0.05,0.03,0.02,0) & (0,0.05,0.05,0.05,0.1,0.1,0.65,0) \\ (0,0.1,0.05,0.05,0.05,0.1,0.65,0) & (0,0.05,0.05,0.05,0.1,0.1,0.65,0) & (0,0.85,0.04,0.04,0.04,0.02,0.01,0) \end{bmatrix}$
S_6	$\begin{bmatrix} (0,0,0,0,0,0,1,0) & (0,0,0,0,0,0,1,0) & (0,0,0,0,0,0,1,0) & (0,0,0,0,0,0,1,0) & (0,0,0,0,0,0,1,0) \\ (0,0.1,0.1,0,0,0,0,0.8) & (0,0.85,0.15,0,0,0,0,0) & (0,0.1,0.1,0.05,0,0,0,0.75) & (0,0.1,0.1,0.025,0,0,0,0.775) & (0,0.1,0.1,0.025,0,0,0,0.775) \\ (0,0.1,0,0.1,0,0,0,0.8) & (0,0.1,0.05,0.1,0,0,0,0.75) & (0,0.85,0,0.15,0,0,0,0) & (0,0.1,0.025,0.1,0,0,0,0.775) & (0,0.1,0.025,0.1,0,0,0,0.775) \\ (0,0.1,0.05,0.05,0,0,0,0.8) & (0,0.1,0.05,0.1,0,0,0,0.75) & (0,0.1,0.05,0.1,0,0,0,0.75) & (0,0.85,0.05,0.1,0,0,0,0) & (0,0.05,0.05,0.15,0,0,0,0.75) \\ (0,0.1,0.05,0.05,0,0,0,0.8) & (0,0.1,0.05,0.1,0,0,0,0.75) & (0,0.1,0.05,0.1,0,0,0,0.75) & (0,0.05,0.05,0.15,0,0,0,0.75) & (0,0.85,0.05,0.1,0,0,0,0) \end{bmatrix}$
S_7	$\begin{bmatrix} (0,0,0,0,0,0,0,1) & (0,0,0,0,0,0,0,1) & (0,0,0,0,0,0,0,1) \\ (0.875,0,0,0,0,0,0.025,0.1) & (0,0.8,0,0,0.1,0,0.05,0.05) & (0.8,0,0,0,0,0,0.05,0.15) \\ (0.875,0,0,0,0,0,0.025,0.1) & (0.8,0,0,0,0,0,0.05,0.15) & (0,0.8,0,0,0,0.1,0.05,0.05) \end{bmatrix}$
State	**Reward Value for Defender**
S_0	$[-200]$
S_1	$\begin{bmatrix} 0 & -3 & -3 \\ -10 & 10 & -3 \\ -10 & -3 & 10 \end{bmatrix}$
S_2	$\begin{bmatrix} 0 & -2 & -1 & -2 \\ -10 & 10 & -1 & -2 \\ -3.9 & -2 & 3.9 & -2 \\ -8.375 & -2 & -1 & 8.375 \end{bmatrix}$
S_3	$\begin{bmatrix} 0 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ -10 & 10 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ -8.375 & -2 & 8.375 & -2 & -2 & -2 & -2 & -2 & -2 & -2 \\ -6.5 & -2 & -2 & 6.5 & -2 & -2 & -2 & -2 & -2 & -2 \\ -10 & -2 & -2 & -2 & 10 & -2 & -2 & -2 & -2 & -2 \\ -10 & -2 & -2 & -2 & -2 & 10 & -2 & -2 & -2 & -2 \\ -8.6 & -2 & -2 & -2 & -2 & -2 & 8.6 & -2 & -2 & -2 \\ -4.9 & -2 & -2 & -2 & -2 & -2 & -2 & 4.9 & -2 & -2 \\ -10 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 10 & -2 \\ -10 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 10 \end{bmatrix}$
S_4	$\begin{bmatrix} 0 & -2 & -2 & -2 \\ -10 & 10 & -2 & -2 \\ -5.1 & -2 & 5.1 & -2 \\ -10 & -2 & -2 & 10 \end{bmatrix}$
S_5	$\begin{bmatrix} 0 & -2 & -2 \\ -10 & 10 & -2 \\ -10 & -2 & 10 \end{bmatrix}$
S_6	$\begin{bmatrix} 0 & -2 & -1 & -1 & -2 \\ -8.75 & 8.75 & -1 & -1 & -2 \\ -5.25 & -2 & 5.25 & -1 & -2 \\ -7.35 & -2 & -1 & 7.35 & -2 \\ -3.65 & -2 & -1 & -1 & 3.65 \end{bmatrix}$
S_7	$\begin{bmatrix} 0 & -5 & -5 \\ -10 & 30 & -5 \\ -10 & -5 & 30 \end{bmatrix}$

metrics for the calculated drone-type MTD defense effectiveness. As a result, compared to conventional security elements, the presented drone-type MTD was demonstrated to ensure robustness of security avoidance for the inside and outside of drones. Furthermore, the defense effects divided according to major indicators such as discount factor, learning rate, exploration rate, number of macroscopic episodes, microscopic steps, and sampling variance coefficient, were calculated.

However, from a threat-to-validity analysis of this study, most results were obtained from limited simulations within a range of internal and external invasion scenarios, which

TABLE 6. Probability matrix of transition and semi-constant reward value with payoff strategy for outside of drone.

State	Probability of Transition
S_0	$[(1,0,0,0,0,0,0,0)]$
S_1	$\begin{bmatrix} (0,1,0,0,0,0,0,0) & (0,1,0,0,0,0,0,0) & (0,1,0,0,0,0,0,0) & (0,1,0,0,0,0,0,0) \\ (0,0.2,0.8,0,0,0,0,0) & (0,0.9,0.1,0,0,0,0,0) & (0,0.35,0.65,0,0,0,0,0) & (0,0.3,0.7,0,0,0,0,0) \\ (0,0.3,0.7,0,0,0,0,0) & (0,0.35,0.65,0,0,0,0,0) & (0,0.95,0.05,0,0,0,0,0) & (0,0.35,0.65,0,0,0,0,0) \\ (0,0.25,0.75,0,0,0,0,0) & (0,0.3,0.7,0,0,0,0,0) & (0,0.3,0.7,0,0,0,0,0) & (0,0.9,0.1,0,0,0,0,0) \end{bmatrix}$
S_2	$\begin{bmatrix} (0,0,1,0,0,0,0,0) & (0,0,1,0,0,0,0,0) & (0,0,1,0,0,0,0,0) \\ (0,0.05,0.25,0.7,0,0,0,0) & (0,0.85,0.14,0.01,0,0,0,0) & (0,0.1,0.3,0.6,0,0,0,0) \\ (0,0.05,0.15,0.8,0,0,0,0) & (0,0.1,0.2,0.7,0,0,0,0) & (0,0.88,0.11,0.01,0,0,0,0) \end{bmatrix}$
S_3	$\begin{bmatrix} (0,0,0,1,0,0,0,0) & (0,0,0,1,0,0,0,0) & (0,0,0,1,0,0,0,0) & (0,0,0,1,0,0,0,0) & (0,0,0,1,0,0,0,0) \\ (0,0.05,0.05,0.1,0.8,0,0,0) & (0,0.9,0.05,0.04,0.01,0,0,0) & (0,0.05,0.1,0.15,0.7,0,0,0) & (0,0.05,0.1,0.15,0.7,0,0,0) & (0,0.05,0.1,0.15,0.7,0,0,0) \\ (0,0.05,0.05,0.15,0.75,0,0,0) & (0,0.05,0.1,0.2,0.65,0,0,0) & (0,0.85,0.1,0.04,0.01,0,0,0) & (0,0.05,0.1,0.2,0.65,0,0,0) & (0,0.05,0.1,0.2,0.65,0,0,0) \\ (0,0.05,0.05,0.15,0.75,0,0,0) & (0,0.05,0.1,0.2,0.65,0,0,0) & (0,0.05,0.1,0.2,0.65,0,0,0) & (0,0.85,0.1,0.04,0.01,0,0,0) & (0,0.05,0.1,0.2,0.65,0,0,0) \\ (0,0.05,0.05,0.15,0.75,0,0,0) & (0,0.05,0.1,0.2,0.65,0,0,0) & (0,0.05,0.1,0.2,0.65,0,0,0) & (0,0.05,0.1,0.2,0.65,0,0,0) & (0,0.85,0.1,0.04,0.01,0,0,0) \end{bmatrix}$
S_4	$\begin{bmatrix} (0,0,0,0,1,0,0,0) & (0,0,0,0,1,0,0,0) & (0,0,0,0,1,0,0,0) & (0,0,0,0,1,0,0,0) & (0,0,0,0,1,0,0,0) \\ (0,0.05,0.05,0.05,0.1,0.75,0,0) & (0,0.85,0.08,0.04,0.025,0.005,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) \\ (0,0.05,0,0.1,0.15,0.7,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) & (0,0.825,0.05,0.075,0.04,0.01,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) \\ (0,0.05,0,0.1,0.15,0.7,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) & (0,0.825,0.05,0.075,0.04,0.01,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) \\ (0,0.05,0,0.1,0.15,0.7,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) & (0,0.05,0.05,0.1,0.15,0.65,0,0) & (0,0.825,0.05,0.075,0.04,0.01,0,0) \end{bmatrix}$
S_5	$\begin{bmatrix} (0,0,0,0,0,1,0,0) & (0,0,0,0,0,1,0,0) & (0,0,0,0,0,1,0,0) & (0,0,0,0,0,1,0,0) & (0,0,0,0,0,1,0,0) \\ (0,0.05,0.05,0.05,0.05,0.05,0.75,0) & (0,0.85,0.05,0.05,0.03,0.01,0.01,0) & (0,0.05,0.05,0.05,0.1,0.1,0.65,0) & (0,0.05,0.05,0.05,0.1,0.1,0.65,0) & (0,0.05,0.05,0.05,0.1,0.1,0.65,0) \\ (0,0.05,0.05,0.05,0.05,0.1,0.7,0) & (0,0.05,0.05,0.05,0.1,0.15,0.6,0) & (0,0.825,0.075,0.05,0.03,0.01,0.01,0) & (0,0.05,0.05,0.05,0.1,0.15,0.6,0) & (0,0.05,0.05,0.05,0.1,0.15,0.6,0) \\ (0,0.05,0.05,0.05,0.05,0.1,0.7,0) & (0,0.05,0.05,0.05,0.1,0.15,0.6,0) & (0,0.05,0.05,0.05,0.1,0.15,0.6,0) & (0,0.825,0.075,0.05,0.03,0.01,0.01,0) & (0,0.05,0.05,0.05,0.1,0.15,0.6,0) \\ (0,0.05,0.05,0.05,0.05,0.1,0.7,0) & (0,0.05,0.05,0.05,0.1,0.15,0.6,0) & (0,0.05,0.05,0.05,0.1,0.15,0.6,0) & (0,0.05,0.05,0.05,0.1,0.15,0.6,0) & (0,0.825,0.075,0.05,0.03,0.01,0.01,0) \end{bmatrix}$
S_6	$\begin{bmatrix} (0,0,0,0,0,0,1,0) & (0,0,0,0,0,0,1,0) & \{skipped\} & (0,0,0,0,0,0,1,0) & (0,0,0,0,0,0,1,0) \\ (0,0.1,0.05,0,0,0,0,0.85) & (0,0.9,0.08,0.015,0,0,0,0.005) & \{skipped\} & (0,0.1,0.05,0.05,0,0,0,0.8) & (0,0.1,0.05,0.05,0,0,0,0.8) \\ \{skipped\} & \{skipped\} & \{skipped\} & \{skipped\} & \{skipped\} \\ (0,0.15,0.05,0,0,0,0,0.8) & (0,0.15,0.05,0.05,0,0,0,0.75) & \{skipped\} & (0,0.95,0.03,0.0175,0,0,0,0.0025) & (0,0.15,0.05,0.05,0,0,0,0.75) \\ (0,0.1,0.05,0,0,0,0,0.85) & (0,0.1,0.05,0.05,0,0,0,0.8) & \{skipped\} & (0,0.1,0.05,0.05,0,0,0,0.8) & (0,0.9,0.08,0.015,0,0,0,0.005) \end{bmatrix}$
S_7	$\begin{bmatrix} (0,0,0,0,0,0,0,1) & (0,0,0,0,0,0,0,1) & (0,0,0,0,0,0,0,1) & (0,0,0,0,0,0,0,1) & (0,0,0,0,0,0,0,1) & (0,0,0,0,0,0,0,1) \\ (0.9,0,0,0,0,0,0,0.1) & (0.05,0.85,0,0,0,0,0,0.1) & (0.8,0,0,0,0,0,0.05,0.15) & (0.8,0,0,0,0,0,0.05,0.15) & (0.8,0,0,0,0,0,0.05,0.15) & (0.8,0,0,0,0,0,0.05,0.15) \\ (0.95,0,0,0,0,0,0,0.05) & (0.85,0,0,0,0,0,0.025,0.125) & (0.025,0.9,0,0,0,0,0,0.075) & (0.85,0,0,0,0,0,0.025,0.125) & (0.85,0,0,0,0,0,0.025,0.125) & (0.85,0,0,0,0,0,0.025,0.125) \\ (0.9,0,0,0,0,0,0,0.1) & (0.8,0,0,0,0,0,0.05,0.15) & (0.8,0,0,0,0,0,0.05,0.15) & (0.05,0.85,0,0,0,0,0,0.1) & (0.8,0,0,0,0,0,0.05,0.15) & (0.8,0,0,0,0,0,0.05,0.15) \\ (0.9,0,0,0,0,0,0,0.1) & (0.8,0,0,0,0,0,0.05,0.15) & (0.8,0,0,0,0,0,0.05,0.15) & (0.8,0,0,0,0,0,0.05,0.15) & (0.05,0.85,0,0,0,0,0,0.1) & (0.8,0,0,0,0,0,0.05,0.15) \\ (0.95,0,0,0,0,0,0,0.05) & (0.85,0,0,0,0,0,0.025,0.125) & (0.85,0,0,0,0,0,0.025,0.125) & (0.85,0,0,0,0,0,0.025,0.125) & (0.85,0,0,0,0,0,0.025,0.125) & (0.05,0.85,0,0,0,0,0,0.1) \end{bmatrix}$

State	Reward Value for Defender
S_0	$[-200]$
S_1	$\begin{bmatrix} 0 & -3 & -3 & -3 \\ -10 & 10 & -3 & -3 \\ -8 & -3 & 8 & -3 \\ -10 & -3 & -3 & 10 \end{bmatrix}$
S_2	$\begin{bmatrix} 0 & -2 & -2 \\ -10 & 10 & -2 \\ -6.5 & -2 & 6.5 \end{bmatrix}$
S_3	$\begin{bmatrix} 0 & -2 & -2 & -2 & -2 \\ -10 & 10 & -2 & -2 & -2 \\ -3.9 & -2 & 3.9 & -2 & -2 \\ -10 & -2 & -2 & 10 & -2 \\ -8 & -2 & -2 & -2 & 8 \end{bmatrix}$
S_4	$\begin{bmatrix} 0 & -3 & -2 & -2 & -3 \\ -10 & 10 & -2 & -2 & -3 \\ -6.5 & -3 & 6.5 & -2 & -3 \\ -10 & -3 & -2 & 10 & -3 \\ -8 & -3 & -2 & -2 & 8 \end{bmatrix}$
S_5	$\begin{bmatrix} 0 & -2 & -1 & -1 & -2 \\ -10 & 10 & -1 & -1 & -2 \\ -5.5 & -2 & 5.5 & -1 & -2 \\ -3.9 & -2 & -1 & 3.9 & -2 \\ -8 & -2 & -1 & -1 & 8 \end{bmatrix}$
S_6	$\begin{bmatrix} 0 & -4 & -4 & -4 & -4 & -4 & -4 & -4 \\ -10 & 10 & -4 & -4 & -4 & -4 & -4 & -4 \\ -8.6 & -4 & 8.6 & -4 & -4 & -4 & -4 & -4 \\ -10 & -4 & -4 & 10 & -4 & -4 & -4 & -4 \\ -10 & -4 & -4 & -4 & 10 & -4 & -4 & -4 \\ -10 & -4 & -4 & -4 & -4 & 10 & -4 & -4 \\ -10 & -4 & -4 & -4 & -4 & -4 & 10 & -4 \\ -10 & -4 & -4 & -4 & -4 & -4 & -4 & 10 \end{bmatrix}$
S_7	$\begin{bmatrix} 0 & -1 & -1 & -1 & -1 & -1 \\ -8.75 & 8.75 & -1 & -1 & -1 & -1 \\ -5.25 & -1 & 5.25 & -1 & -1 & -1 \\ -2.65 & -1 & -1 & 2.65 & -1 & -1 \\ -8.75 & -1 & -1 & -1 & 8.75 & -1 \\ -8.75 & -1 & -1 & -1 & -1 & 8.75 \end{bmatrix}$

were not completely dynamic despite fine-tuning of game metrics. The decision boundaries by actor were likewise limited. Therefore, we expect the introduction of stochastic scalability in POMDP to account for more diverse drone battlefield ranges as required. In addition, because the concept of perfect complete information used to optimize game

decisions by drone actors was also unrealistically assumed to differ from the actual drone's operational security, it is necessary to secure a game solution that does not require such prior knowledge separately. Furthermore, because most internal and external vulnerabilities of drones were abstracted based on threat modeling results from CVE/CVSS-based quantitative scores, they could differ from the unique policies or beliefs related to the actual organizations and personnel operating a drone network. Likewise, practical differences from combat network radios and related datalinks could depend on the range of expose for vulnerability information, all of which should be mitigated. Futhermore, by quantifying the attack-exploration surface of the defender, which could fluctuate depending on whether the drone-type MTD is applied multidimensionally, variability in performance as a result of surface elements must also be analyzed in detail. In addition, most actual attack and defense actors in a wireless communication drone operating environment subjectively process asymmetric information, or perform actions after making incomplete judgments. In this study, subjective decisions were simulated under the premise that actors in uncertain situations have a consistent opinion, which does not fully represent a practical scenario.

Accordingly, all abovementioned limitations will be mitigated by conducting a follow-up study to expand the optimization domain of the drone-type MTD with the hypergame, which is a zero-sum-based unbalanced meta game logic, while additionally integrating the MTD applied to a prototype drone with a drone-type decoy element and AI (artificial intelligence) [55]. Based on the follow-up study, actual drone active protection technology will be combined with the cyber flare type avoidance and cyber camouflage type disarrangement strategies, yielding further advances in actual tactical modernized cyber devices.

APPENDIX–SUPPLEMENTARY DATA

See Tables 5 and 6.

AUTHOR CONTRIBUTIONS

Conceptualization, methodology, and software: Sang Seo; validation: Sang Seo and Donghyeon Kim; formal analysis: Sang Seo and Donghyeon Kim; investigation: Sang Seo, Sunho Lee, Donghyeon Kim, Byeongjin Kim, and Woojin Lee; resources: Sang Seo, Heaeun Moon, Sunho Lee, Donghyeon Kim, Jaeyeon Lee, Byeongjin Kim, and Woojin Lee; data curation: Sang Seo, Heaeun Moon, Sunho Lee, Donghyeon Kim, Jaeyeon Lee, Byeongjin Kim, Woojin Lee, and Donghyeon Kim; writing—original draft preparation: Sang Seo and Donghyeon Kim; writing—review and editing: Sang Seo and Donghyeon Kim; visualization: Sang Seo; supervision: Heaeun Moon, Jaeyeon Lee, and Donghyeon Kim; project administration: Sang Seo, Heaeun Moon, Jaeyeon Lee, and Donghyeon Kim; funding acquisition: Heaeun Moon, Jaeyeon Lee, and Donghyeon Kim. All authors have read and agreed to the published version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

AVAILABILITY OF DATA AND MATERIAL

Please contact the corresponding author (Dohoon Kim) at karmy01@kyonggi.ac.kr

REFERENCES

[1] *Understanding Multi-Domain Operations in NATO*. Accessed: Feb. 3, 2023. [Online]. Available: https://www.jwc.nato.int/application/files/1516/3281/0425/issue37_21.pdf
[2] *Army Modernization Strategy*. Accessed: Feb. 3, 2023. [Online]. Available: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34818-SD_08_STRATEGY_NOTE_2021-02-000-WEB-1.pdf
[3] *Military Drones in Europe*. Accessed: Feb. 3, 2023. [Online]. Available: https://www.sdu.dk/-/media/cws/files/cws_military_drones_in_europe_report.pdf
[4] *Left of Launch: Countering Theater Ballistic Missiles*. Accessed: Feb. 3, 2023. [Online]. Available: https://www.jstor.org/stable/pdf/resrep03498.pdf?refreqid=excelsior%3A9bab317f0419f0c7682a0466acc041ac&ab_segments=&origin=&acceptTC=1s
[5] C. J. Hee, "Toward a secure drone system: Flying with real-time homomorphic authenticated encryption," *IEEE Access*, vol. 6, pp. 24325–24339, Mar. 2018, doi: 10.1109/ACCESS.2018.2819189.
[6] U.S Army. *FM 3-38 Cyber Electromagnetic Activities*. Accessed: Feb. 3, 2023. [Online]. Available: https://irp.fas.org/doddir/army/fm3-38.pdf
[7] N. Saputro, S. Tonyali, A. Aydeger, K. Akkaya, M. A. Rahman, and S. Uluagac, "A review of moving target defense mechanisms for Internet of Things applications," in *Modeling and Design of Secure Internet of Things*, Hoboken, NJ, USA: Wiley, 2020, pp. 563–614, doi: 10.1002/9781119593386.ch24.
[8] J. D. Mireles, E. Ficke, J. Cho, P. Hurley, and S. Xu, "Metrics towards measuring cyber agility," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 12, pp. 3217–3232, Dec. 2019, doi: 10.1109/TIFS.2019.2912551.
[9] L. Igor and A. Kott, "Fundamental concepts of cyber resilience: Introduction and overview," in *Cyber Resilience of Systems and Networks*. Cham, Switzerland: Springer, 2018, pp. 1–25, doi: 10.1007/978-3-319-77492-3_1.
[10] M. Zhu, A. H. Anwar, Z. Wan, J.-H. Cho, C. Kamhoua, and M. P. Singh, "Game-theoretic and machine learning-based approaches for defensive deception: A survey," 2021, pp. 1–37, *arXiv:2101.10121*, doi: 10.48550/arXiv.2101.10121.
[11] D. Fraunholz, S. D. Anton, C. Lipps, D. Reti, D. Krohmer, F. Pohl, M. Tammen, and H. D. Schotten, "Demystifying deception technology: A survey," 2018, pp. 1–25, *arXiv:1804.06196*, doi: 10.48550/arXiv.1804.06196.
[12] J. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim, H. Lim, and F. F. Nelson, "Toward proactive, adaptive defense: A survey on moving target defense," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 709–745, 1st Quart., 2020, doi: 10.1109/COMST.2019.2963791.
[13] P. K. Manadhata and J. M. Wing, "An attack surface metric," *IEEE Trans. Softw. Eng.*, vol. 37, no. 3, pp. 371–386, May 2011, doi: 10.1109/TSE.2010.60.
[14] C. Lei, H.-Q. Zhang, L.-M. Wan, L. Liu, and D.-H. Ma, "Incomplete information Markov game theoretic approach to strategy generation for moving target defense," *Comput. Commun.*, vol. 116, pp. 184–199, Jan. 2018, doi: 10.1016/j.comcom.2017.12.001.
[15] S. Sengupta and S. Kambhampati, "Multi-agent reinforcement learning in Bayesian Stackelberg Markov games for adaptive moving target defense," 2020, *arXiv:2007.10457*, doi: 10.48550/arXiv.2007.10457.
[16] H. Li, W. Shen, and Z. Zheng, "Spatial-temporal moving target defense: A Markov Stackelberg game model," 2020, *arXiv:2002.10390*, doi: 10.48550/arXiv.2002.10390.
[17] S. Wang, H. Shi, Q. Hu, B. Lin, and X. Cheng, "Moving target defense for Internet of Things based on the zero-determinant theory," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 661–668, Jan. 2020, doi: 10.1109/JIOT.2019.2943151.
[18] X. Feng, Z. Zheng, D. Cansever, A. Swami, and P. Mohapatra, "A signaling game model for moving target defense," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Atlanta, GA, USA, May 2017, pp. 1–9, doi: 10.1109/INFOCOM.2017.8057200.

[19] *Lockheed Martin. Gaining the Advantage*. Accessed: Feb. 3, 2023. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-Martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

[20] B. Ly and R. Ly, "Cybersecurity in unmanned aerial vehicles (UAVs)," *J. Cyber Secur. Technol.*, vol. 5, no. 2, pp. 120–137, Apr. 2021, doi: 10.1080/23742917.2020.1846307.

[21] NIST. *Common Vulnerabilities and Exposures (CVE)*. Accessed: Feb. 3, 2023. [Online]. Available: https://nvd.nist.gov/vuln

[22] NIST. *Common Vulnerability Scoring System (CVSS)*. Accessed: Feb. 3, 2023. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss

[23] White House. *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*. Accessed: Feb. 3, 2023. [Online]. Available: https://www.nitrd.gov/pubs/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

[24] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Comput. Surv.*, vol. 48, no. 3, pp. 1–39, Feb. 2016, doi: 10.1145/2835375.

[25] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Comput. Secur.*, vol. 72, pp. 212–233, Jan. 2018, doi: 10.1016/j.cose.2017.09.001.

[26] J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–28, Jul. 2020, doi: 10.1145/3337772.

[27] K. Park, S. Woo, D. Moon, and H. Choi, "Secure cyber deception architecture and decoy injection to mitigate the insider threat," *Symmetry*, vol. 10, no. 1, p. 14, Jan. 2018, doi: 10.3390/sym10010014.

[28] F. Cohen. *The Use of Deception Techniques: Honeypots and Decoys Deception*. Accessed: Feb. 3, 2023. [Online]. Available: http://all.net/journal/deception/Deception_Techniques_.pdf

[29] R. E. Navas, F. Cuppens, N. B. Cuppens, L. Toutain, and G. Z. Papadopoulos, "MTD, where art thou? A systematic review of moving target defense techniques for IoT," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7818–7832, May 2021, doi: 10.1109/JIOT.2020.3040358.

[30] J. Sun and K. Sun, "DESIR: Decoy-enhanced seamless IP randomization," in *Proc. 35th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, San Francisco, CA, USA, Apr. 2016, pp. 1–9, doi: 10.1109/INFOCOM.2016.7524602.

[31] D. Reti, D. Fraunholz, K. Elzer, D. Schneider, and H. D. Schotten, "Evaluating deception and moving target defense with network attack simulation," in *Proc. 9th ACM Workshop Moving Target Defense (MTD)*, New York, NY, USA, 2022, pp. 45–53, doi: 10.1145/3560828.3564006.

[32] Z. Wan, J.-H. Cho, M. Zhu, A. H. Anwar, C. A. Kamhoua, and M. P. Singh, "Foureye: Defensive deception against advanced persistent threats via hypergame theory," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 1, pp. 112–129, Oct. 2021, doi: 10.1109/TNSM.2021.3117698.

[33] P. Madani, N. Vlajic, and I. Maljevic, "Randomized moving target approach for MAC-layer spoofing detection and prevention in IoT systems," *Digit. Threats, Res. Pract.*, vol. 3, no. 4, pp. 1–24, Dec. 2022, doi: 10.1145/3477403.

[34] Q. Zhu and T. Basar, "Game-theoretic approach to feedback-driven multi-stage moving target defense," in *Proc. Int. Conf. Decis. Game Theory Secur.*, FortWorth, TX, USA, Nov. 2013, pp. 246–263, doi: 10.1007/978-3-319-02786-9_15.

[35] L. Ge, W. Yu, D. Shen, G. Chen, K. Pham, E. Blasch, and C. Lu, "Toward effectiveness and agility of network security situational awareness using moving target defense (MTD)," *Proc. SPIE*, vol. 9085, pp. 1–9, Jun. 2014, doi: 10.1117/12.2050782.

[36] S. Neti, A. Somayaji, and M. E. Locasto, "Software diversity: Security, entropy and game theory," in *Proc. USENIX Work. Hot Top. Secur. (HotSec)*, 2012, pp. 1–6.

[37] M. Wright, S. Venkatesan, M. Albanese, and M. P. Wellman, "Moving target defense against DDoS attacks: An empirical game-theoretic analysis," in *Proc. ACM Workshop Moving Target Defense*, 2016, pp. 93–104, doi: 10.1145/2995272.2995279.

[38] K. M. Carter, J. F. Riordan, and H. Okhravi, "A game theoretic approach to strategy determination for dynamic platform defenses," in *Proc. 1st ACM Workshop Moving Target Defense*, Scottsdale, AZ, USA, Nov. 2014, pp. 21–30, doi: 10.1145/2663474.2663478.

[39] R. Colbaugh and K. Glass, "Predictability-oriented defense against adaptive adversaries," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2012, pp. 2721–2727, doi: 10.1109/ICSMC.2012.6378159.

[40] M. M. Hasan and M. A. Rahman, "Protection by detection: A signaling game approach to mitigate co-resident attacks in cloud," in *Proc. IEEE 10th Int. Conf. Cloud Comput. (CLOUD)*, Honolulu, HI, USA, Jun. 2017, pp. 552–559, doi: 10.1109/CLOUD.2017.76.

[41] Q. Zhu, A. Clark, R. Poovendran, and T. Basar, "Deceptive routing games," in *Proc. IEEE 51st IEEE Conf. Decis. Control (CDC)*, Dec. 2012, pp. 2704–2711, doi: 10.1109/CDC.2012.6426515.

[42] S. Sengupta, S. G. Vadlamudi, S. Kambhampati, A. Doupé, Z. Zhao, M. Taguinod, and G. J. Ahn, "A game theoretic approach to strategy generation for moving target defense in web applications," in *Proc. AAMAS*, vol. 1, 2017, pp. 178–186.

[43] S. Sengupta, A. Chowdhary, D. Huang, and S. Kambhampati, "General sum Markov games for strategic detection of advanced persistent threats using moving target defense in cloud networks," in *Decision and Game Theory for Security* Cham, Switzerland: Springer, 2019, pp. 492–512, doi: 10.1007/978-3-030-32430-8_29.

[44] S. Seo and D. Kim, "OSINT-based LPC-MTD and HS-decoy for organizational defensive deception," *Appl. Sci.*, vol. 11, no. 8, pp. 1–34, 2021, doi: 10.3390/app11083402.

[45] S. Seo and D. Kim, "SOD2G: A study on a social-engineering organizational defensive deception game framework through optimization of spatiotemporal MTD and decoy conflict," *Electronics*, vol. 10, no. 23, pp. 1–40, 2021, doi: 10.3390/electronics10233012.

[46] S. Seo and D. Kim, "IoDM: A study on a IoT-based organizational deception modeling with adaptive general-sum game competition," *Electronics*, vol. 11, no. 1623, pp. 1–38, 2022, doi: 10.3390/electronics11101623.

[47] P. K. Manadhata, "Game theoretic approaches to attack surface shifting," in *Moving Target Defense II*. New York, NY, USA: Springer, 2013, pp. 1–13, doi: 10.1007/978-1-4614-5416-8_1.

[48] H. Zhang, K. Zheng, X. Wang, S. Luo, and B. Wu, "Strategy selection for moving target defense in incomplete information game," *Comput., Mater. Continua*, vol. 62, no. 2, pp. 763–786, 2020, doi: 10.32604/cmc.2020.06553.

[49] S. Seo, S. Han, and D. Kim, "D-CEWS: DEVS-based cyber-electronic warfare M&S framework for enhanced communication effectiveness analysis in battlefield," *Sensors*, vol. 22, no. 3147, pp. 1–26, 2022, doi: 10.3390/s22093147.

[50] *MAVLink Developer Guide*. Accessed: Feb. 3, 2023. [Online]. Available: https://mavlink.io/en/

[51] *IEEE 802.11 Wireless Local Area Networks. The Working Group for WLAN Standards*. Accessed: Feb. 3, 2023. [Online]. Available: https://www.ieee802.org/11/

[52] ETSI. *LTE Standard*. Accessed: Feb. 3, 2023. [Online]. Available: https://www.etsi.org/technologies/mobile/4G

[53] B. Ly and R. Ly, "Cybersecurity in unmanned aerial vehicles (UAVs)," *J. Cyber Secur. Technol.*, vol. 5, no. 2, pp. 120–137, Apr. 2021, doi: 10.1080/23742917.2020.1846307.

[54] R. H. Jacobsen and A. Marandi, "Security threats analysis of the unmanned aerial vehicle system," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2021, pp. 316–322, doi: 10.1109/MILCOM52596.2021.9652900.

[55] X. Liang, W. Xiaoyue, L. Xiaozhen, Z. Yanyong, and W. Di, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 4–41, Sep. 2018.

SANG SEO received the B.S. degree in computer science and the M.S. degree in computer science (with specialization in cybersecurity and cyber deception) from Kyonggi University, in 2020 and 2022, respectively. He has been a Technical Research Personnel with the RedAlert Team, NSHC Company Ltd., Seoul, South Korea, since 2022. His research interests include cyber deception, moving target defense (MTD), decoy, and cyber resilience.

HEAEUN MOON received the M.S. degree in information communication engineering from Yeungnam University, in 2002. From 2002 to 2014, he was a Chief Technology Officer with Netman Company Ltd., Seoul, South Korea. He has been a Chief Technology Officer with the RedAlert Team, NSHC Company Ltd., Seoul, since 2014. His research interests include cybersecurity and artificial intelligence.

SUNHO LEE received the B.S. degree in environmental engineering from the Korea National University of Transportation, in 2005. He has been a Principal Research Engineer with the RedAlert Team, NSHC Company Ltd., Seoul, South Korea, since 2005. His research interests include hardware hacking and operation technology (OT) device hacking.

DONGHYEON KIM received the B.S. degree in multimedia engineering from Dongeui University, in 2020. He has been an Assistant Research Engineer with the RedAlert Team, NSHC Company Ltd., Seoul, South Korea, since 2021. His research interests include cybersecurity and computer engineering.

JAEYEON LEE received the B.S. degree in information communication engineering from the Catholic University of Korea, in 2002, and the M.S. degree in information communication engineering from the Gwangju Institute of Science and Technology, in 2004. She is currently a Principal Research Engineer with the Cyber Battlefield Team, Hanwha Systems Company Ltd., Seongnam-si, South Korea. Her research interests include cyber security and intrusion analysis.

BYEONGJIN KIM received the B.S. degree in computer engineering from Kyunghee University, in 2008. He is currently a Senior Research Engineer with the Cyber Battlefield Team, Hanwha Systems Company Ltd., Seongnam-si, South Korea. His research interests include cybersecurity and computer engineering.

WOOJIN LEE received the B.S. degree in computer engineering from Pusan National University, in 2018. He is currently a Research Engineer with the Cyber Battlefield Team, Hanwha Systems Company Ltd., Seongnam-si, South Korea. His research interests include cybersecurity and computer engineering.

DOHOON KIM received the B.S. degree in mathematics and computer science, the M.S. degree in information security and computer science, and the Ph.D. degree in information security and computer science (with specialization in cybersecurity and network security) from Korea University, in 2005, 2007, and 2012, respectively.

From 2012 to 2018, he was a Senior Research Engineer with the Agency for Defense Development (ADD), Daejeon-si, South Korea. He has been an Assistant Professor with the Department of Computer Science, Kyonggi University, Suwon, South Korea, since 2018. His research interests include cybersecurity, botnet, risk analysis, cyber deception, and moving target defense (MTD).