Taxonomy and Simulation of Bio-Analogous Multi-Stage Cyberattacks

Shaher Suleman Slehat
Department of Basic Sciences (Humanities and Natural Sciences), Al-Zaytoonah University of Jordan, Amman, Jordan
s.slehat@zuj.edu.jo

Esraa Abu Elsoud
Cybersecurity and Cloud Computing Department, Faculty of Information Technology, Applied Science Private University, Amman, Jordan
e_abuelsoud@asu.edu.jo

Layla Albdour
Cyber Security Department, Al-Zaytoonah University of Jordan, Amman, Jordan
l.albdour@zuj.edu.jo

Esra'a Alhenawi
Department of Information Systems, Al al-Bayt University, Mafraq, Jordan
esraahenawi@aabu.edu.jo

Malek Mahmoud Barhoush
Cybersecurity Program, IT Department, IT&CS Faculty, Yarmouk University, Irbid, Jordan
malek@yu.edu.jo (corresponding author)

Received: 29 November 2025 | Revised: 18 February 2026, 7 March 2026, and 21 March 2026 | Accepted: 23 March 2026

 DOI: https://doi.org/10.48084/etasr.16605

ABSTRACT

Today, bio-inspired approaches in cybersecurity represent an active research area in the literature, as these approaches offer adaptability, learning, and robustness to face modern, evolving cyber threats. Traditional Intrusion Detection Systems (IDSs) are increasingly proficient at identifying isolated malicious events, yet they remain vulnerable to coordinated, multi-stage deception that mimics biological social structures. The primary gap in current literature is a lack of formal frameworks that map complex predator-prey dynamics, such as distraction-based deception and fission–fusion coordination, to modern network attack vectors. To address this, we propose a novel taxonomy and realistic discrete-event simulation framework for bio-analogous cyberattacks based on two natural archetypes: the Crow, representing sophisticated deception and decoy-based exfiltration, and the Wild Dog, representing decentralized coordination and sequential hunting. Leveraging the OMNeT++/INET framework and an enterprise-inspired network topology, we emulate how biological perseverance and role-division can be mapped to advanced multi-vector intrusions.

Keywords-bio-analogous; Crows; Wild Dogs; Intrusion Detection Systems (IDSs); multi-stage attacks

I. INTRODUCTION

Modern cyberattacks are now coordinated, agile, and stealthy in ways that more closely resemble naturalistic tactics [1]. Today's adversaries use dynamic tactics that can alter in real time, avoid conventional defenses, and remain undetected within systems, in contrast to previous attacks that relied on brute force or predictable techniques. This flexibility presents a significant obstacle to traditional security tools, which are frequently reactive and have a limited effect [2]. There are serious repercussions, including increasing financial losses, extended system outages, and increased difficulty in differentiating between malicious and legitimate activity. Researchers are using models beyond traditional computing to better understand and combat these threats, using animal behavior and natural survival techniques as a guide to create stronger defenses [3].

Researchers have long used biological metaphors like immune systems, evolutionary processes, and swarms to create and enhance adaptive cyber defense techniques [4]. Many algorithms are derived from nature, just like optimized routing choices in networking and cybersecurity, by imitating ants' pathfinding [5]. Ant-colony algorithms are derived from the way real ants find food using the shortest path by leaving pheromones on the path they take while looking for food [6]. The colony gradually "discovers" the most effective path by following the stronger pheromone. In computing, this idea is used to simulate software agents. Each "ant" leaves a digital "pheromone" after exploring various paths within a network. More agents are drawn to the best, shortest, safest, or least crowded routes, which strengthens them. Wireless networks or dynamic environments can take advantage of this algorithm to choose the most effective communication path, which also helps secure these networks.

Many researchers have been inspired by natural phenomena such as ants, swarms, and the immune system to create cybersecurity defense mechanisms [7]. However, there are few studies that examine attacks in the same manner, equating their actions with those of animals that hunt or cooperate to perform tasks. For example, such studies attempt to connect animal behaviors with the steps hackers take in real attacks, like reconnaissance, exploitation, or remaining hidden. Because this connection is missing, defenders are usually reactive rather than proactive.

Without such mapping between attacks and natural phenomena, security teams are unable to model the potential evolution of cyber attackers without learning from nature's most successful attackers, such as swarms and predators.

This study examines two natural archetypes to investigate attacker strategies: wild dogs, which represent coordinated, sequential hunting, and crows, which exhibit sophisticated deception and problem-solving. Crows are intelligent, as they use tools and tricks that hide things. In the cybersecurity world, this is analogous to decoy files, phishing/social engineering, or polymorphic malware that keeps changing so it cannot be detected. They represent a single, clever attacker who takes advantage of weak spots [8].

Wild dogs, which are organized in packs to perform specific tasks, and their ability to surround prey are similar to botnet swarms or insider-assisted campaigns that move across networks in sync, breaking through defenses by timing and dividing up tasks [9].

These species offer different points of view: crows are like the sly, solitary intruder who takes advantage of cognitive blind spots, whereas wild dogs are like the coordinated, multi-vector attack. They cover all kinds of hostile behavior, from sneaking around to swarming. This makes it possible to create more detailed attacker models that are based on biology and match how hackers really work.

This study aims to (i) develop a taxonomy that links cyberattack tactics to animal behaviors, (ii) organize these associations into multi-phase attack models, and (iii) evaluate their detectability and defensive implications. To achieve these objectives, this study combines the domains of cybersecurity and ethology to uncover novel adversarial behaviors and improve threat detection models.

To validate the suggested bio-inspired attack frameworks, OMNeT++, a discrete-event network simulator, was used in this study to facilitate multi-tiered cyberattacks that mimic the coordination and deception of wild dogs and crows.

The Crow scenario demonstrates advanced reconnaissance and misdirection techniques, as the attacker nodes create decoy traffic and obfuscate packets to mask the actual malicious payload. The Wild Dog scenario involves multiple attacker nodes working together in a sequential, role-oriented fashion to overwhelm the target, similar to a synchronized botnet attack.

The primary contributions of this work are as follows:

- Bio-analogous attack taxonomy: We propose a novel taxonomy mapping the social predatory behaviors of Crows (deception) and Wild Dogs (coordination) to multi-stage cyberattack vectors.
- Realistic discrete-event simulation framework: We developed a defense-aware enterprise topology in OMNeT++/INET, utilizing realistic network physics and bottleneck constraints to evaluate attack efficacy.

II. RELATED WORK

Simulation and classification of bio-analogous multi-stage cyberattacks is a significant area of research for many scholars today. It offers a better understanding of complex cyber threats and highlights the importance of defensive systems. There are many research papers in this area. One of the most recent research papers in this direction is the work done by authors in [10], in which they developed a simulation environment that captures multi-stage adversarial behavior, detailing communication patterns and power flows in a power grid. They used attack trees to define attacker strategies and game-theoretic modeling for defender actions. Another work based on attack trees was presented by authors in [11]. In this research, the authors developed a residual cyber-security risk management framework. This framework integrates attack trees that span multiple sub-systems in safety-critical cyber-physical systems.

Authors in [12] developed a system called the "Cyber Incident Simulation System". This system employs attack graphs for threat modeling and synthetic data for attack simulation to assess security, test system performance, and evaluate controls without disrupting production.

Authors in [13] introduced a three-stage cyberattack framework for hybrid hydrogen-electric networks. The proposed framework in the first stage uses a Convolutional Neural Network (CNN) to identify the most vulnerable buses; in the second stage, it deploys a Double Deep Q-Network (DDQN) to improve the attack strategy based on grid response and demand profiles, whereas in the last stage (sustained attack), it maintains high-intensity disruptions while minimizing detection through continuous feedback adaptation.

Authors in [14] adapted a semi-supervised learning approach to propose an Advanced Persistent Threats (APT)

detection framework based on the Shared Nearest Neighbors (SNN) and K-Nearest Neighbors (KNN) algorithms. The proposed framework shows an average detection precision of three APT stages equal to 90.5% by applying it to real-world data from a large-scale enterprise network consisting of 17,684 hosts from the Los Alamos security lab.

Authors in [15] presented a Machine Learning (ML)-based framework for cyberattack detection and classification. This framework starts by detecting attacks efficiently in the first stage and then analyzing the available data to predict the specific attack class in the second stage. They developed an efficient Intrusion Detection System (IDS) focused on detecting attacks in smart grids using a recursive feature elimination method, which not only reduces the number of features but also reduces the number of features captured at the data acquisition stage.

In [16], authors proposed a goal- and effect-based hierarchical multi-stage attack modeling framework. This framework uses the goal and effect model for constructing a unit attack, and the multi-stage configuration of unit attacks achieves the final goal of a cyberattack. Table I summarizes the related works discussed in this section, whereas Table II presents the classification of cyberattack modeling approaches:

- Attack tree approach
- Attack graph approach
- Simulation-based approach
- Cyber kill chain / multi-stage attack modeling
- ML-based approach
- Goal-effect modeling approach

There exist many research papers in the literature concerning specific cyberattack modeling approaches. Authors in [17] conducted a comprehensive survey of automatic attack-tree generation methods, tools, and open challenges. In [18], authors used attack trees within a quantitative risk framework and showed how to compute residual risk after defenses.

Authors in [19] presented graph formalisms and automatic generation pipelines for attack graphs. The authors proposed a fully automatic Large Language Model (LLM)-based framework called AttacKG+ to enhance automated attack-graph construction and reasoning.

Authors in [20] conducted a survey of simulation, including its applications, the types of cyber threats represented, the simulation techniques employed, and the primary objectives of the simulation. In [21], authors deployed a digital-twin simulation for industrial security scenarios to evaluate attack paths without impacting operations.

Bio-inspired optimization techniques have also been explored in related domains. In [22], authors proposed an approach that leverages ant colony optimization to improve information retrieval by jointly exploiting document features and collection-level information. The method enhances relevance scoring and produces a merged result list, demonstrating how swarm intelligence principles can be applied to complex data organization and ranking problems.

TABLE I. SUMMARY OF RELATED WORKS

Work	Advantages	Disadvantages
[10]	Realistic modeling of cyber-physical interactions. Supports multi-stage scenario generation and attacker-defender analysis. Useful for generating validated datasets for IDS/forensics.	Domain-specific to power grids limited generalization. Attack trees may not capture an adaptive behavior as it rigid.
[11]	Supports modeling of complex, multi-subsystem CPS environments. Provides a systematic implementation method. Meets over 75% of ISO/SAE 21434 risk management framework requirements.	Framework complexity increases with CPS system size. Requires detailed system-level knowledge for diagram-to-graph conversion. Initial construction and tuning of attack tree libraries can be time-consuming.
[12]	Efficient in realistic environments as it enables safe, and non-disruptive testing. Attack graphs provide analyzable threat modeling. Support the generation of a synthetic dataset for ML and training.	May abstract low-level physical or timing dynamics. Quality of simulation depends on attack graph accuracy. Limited focus on biologically inspired adaptivity.
[13]	Combines ML with adaptive attack logic-closer to bio-analogous behavior. Models stealthy, sustained disruptions with real-time learning. Focused on emerging hybrid energy systems.	It requires quality training data as it depends on ML. Risk of overfitting or limited generalization to real systems.
[14]	High detection accuracy in real-world data. Effective in detecting multi-stage APTs. Scalable to large enterprise networks.	Depends on availability of labeled/unlabeled data. Limited insight into attacker behavior mechanisms. May not generalize across threat types without tuning.
[15]	Modular detection classification pipeline. Efficient early-stage attack identification. Applicable to various attack types.	Limited handling of multi-stage attack flow. No simulation or attacker modeling involved.
[16]	Provides a structured and systematic representation of cyberattacks. Enables analysis of attacker intent and progress at each stage. Enhances understanding of complex, multi-stage attacks.	May be complex to implement and require detailed domain knowledge. Scalability can be challenging for large-scale attack scenarios. Depends heavily on accurate modeling of goals and effects.

TABLE II. CLASSIFICATION OF CYBERATTACK MODELING APPROACHES IN RECENT RESEARCH

Research work	Modeling approach
[10]	Attack tree + simulation
[11]	Attack tree
[12]	Attack graph + simulation
[13]	Multi-stage attack modeling + reinforcement learning
[14]	Cyber kill chain + semi-supervised learning
[15]	ML-based detection
[16]	Goal-effect modeling + hierarchical multi-stage attack modeling

Based on our literature review, few works fully integrate biologically inspired attack behaviors (e.g., mutation, evolution, immune system interplay, swarm coordination) in multi-stage attack simulations. This gap must be filled to achieve a complete taxonomy and simulation of bio-analogous multi-stage cyberattacks. Although there is no universal replacement for the classical approaches listed above, biologically inspired attack behaviors will bring complementary strengths. Therefore, in this paper, we developed a bio-inspired approach for simulating and modeling cyberattacks by leveraging patterns of animal behavior that closely correspond to real-world attack methods.

The automated generation of attack graphs requires sophisticated retrieval and organization of threat intelligence. This process mirrors the challenges found in scholarly information retrieval, where the exponential growth of literature necessitates advanced indexing and network analysis. As discussed in [23], existing retrieval systems often struggle to meet specific user needs due to a lack of deep structural analysis. To mitigate this, authors in [24] demonstrate that integrating citation network analysis and query expansion can significantly improve search precision and accuracy.

By adopting these principles of network analysis and structured knowledge retrieval, our framework ensures that the Wild Dog and Crow attack graphs are generated with high precision, mapping biological behaviors to technical vulnerabilities through a logically indexed knowledge base.

III. METHODOLOGY

As shown in Figure 1, our approach begins with a formal taxonomy that translates ethological behaviors, such as deception, pack hunting, and ambush, into corresponding cyberattack strategies, ensuring that biological inspiration is grounded in operational cyber realism. After that, each attack is encoded as an attack graph or multi-stage state machine, allowing for the accurate simulation of decision points, dependencies, and progression. We implement realistic traffic and behavioral models by building a scalable network environment with attacker, defender, and decoy nodes using OMNeT++.

For comparison, two main bio-inspired attack scenarios are created: Crow, which is based on deception, and Wild Dog, which is based on coordinated sequential strikes. Defensive mechanisms like signature-based IDSs and ML-driven anomaly detectors are incorporated into the simulation to evaluate detection effectiveness. Through controlled experimentation, we assess key performance metrics, including attack success probability, true/false positive rates, time-to-detection, and computational overhead.

A. Formal Mapping

This section develops a structured mapping between natural animal behaviors and cyberattack tactics. We separate the mapping into two complementary parts: (a) animal behavior: descriptions of the relevant biological traits and survival strategies observed in the species of interest (crows and wild dogs); and (b) cyberattack analogs: how each behavioral trait can be interpreted as a digital adversary technique, the corresponding stage in an attack lifecycle, and measurable signals that can be used for simulation and detection. The mapping provides the foundation for formalizing bio-inspired attack models and for designing detection features in the OMNeT++ experiments.

We first create a mapping between animal behaviors and cyberattack techniques to convert biological strategies into cybersecurity insights. Table III links the behaviors of crows to cyberattacks, whereas Table IV links observed wild dog behaviors to analogous cyberattack strategies. These mappings should be interpreted as conceptual inspirations derived from cooperative hunting dynamics, rather than strict one-to-one representations of biological behavior.

TABLE III. MAPPING OF CROW BEHAVIORS TO CYBERATTACK TACTICS

ID	Observed crow micro-behavior (ethology source)	MITRE ATT&CK mapping	Cyberattack tactic	Observable signal / simulation feature
C1	Deceptive caching: hides food while observed, then re-caches later when alone	T1566.001 + T1071.001	Malware delivery via decoy document; delayed C2 activation	Beaconing spikes during off-hours; delayed cloud access
C2	Tool modification: bends wires to create hooks	T1059.001 + T1218.011	Abuse of legitimate admin tools to construct attack chains	Deep process lineage; unsigned scripts via signed binaries
C3	Future planning and tool storage	T1195.002	Pre-position malicious dependencies in build pipelines	Unexpected package hashes; delayed CI/CD activation
C4	Context-dependent vocalization	T1071.004 + T1005	Multi-channel C2 (DNS + HTTP)	Dual-protocol beaconing; entropy differences
C5	Cache protection via surveillance	T1014 + T1562.001	Environment-aware malware execution	Registry/process checks before payload launch
C6	Opportunistic theft during social interaction	T1056.001 + T1555	Credential harvesting during user sessions	Keystroke anomalies; clipboard access
C7	Use of environmental objects as distractions	T1204.002 + T1566.002	Decoy lures via fake error or update prompts	Unexpected GUI prompts; user-triggered processes
C8	Long-term spatial memory of cache locations	T1530	Gradual exfiltration to multiple cloud services	Repeated small uploads to diverse endpoints
C9	Juvenile learning through play	T1105 + T1106	Testing malicious tools in dev/sandbox environments	Unusual dev-folder writes; silent API calls
C10	Flexible problem-solving in novel tasks	T1053.005 + T1059.003	Adaptive attack logic based on environment	Conditional scripts; system fingerprinting
C11	Food hoarding in safe vs. risky zones	T1566.003 + T1562.006	Payload staging in trusted collaboration services	Writes to SharePoint/Teams; encrypted payloads
C12	Recognition of individual humans	T1598.001	Role-based and behavior-aware targeting	Job-title-based emails; BEC-style requests

TABLE IV. MAPPING OF WILD DOG BEHAVIORS TO CYBERATTACK TACTICS

ID	Observed wild dog micro-behavior (ethology source)	MITRE ATT&CK mapping	Cyberattack tactic	Observable signal / simulation feature
W1	Endurance pursuit behavior: pack members may alternate positions during prolonged chases, helping maintain pursuit over long distances	T1498.002 (application layer DoS) + T1091 (lateral movement)	Rotating attack nodes sustain pressure while evading IP-based blocking, analogous to alternating pursuit participation	Shifting source IPs with consistent payload patterns; stable aggregate traffic rate
W2	Opportunistic spatial spreading: during pursuit, pack members may spread across the landscape, which can incidentally limit escape routes for prey	T1562.001 (impair defenses) + T1570 (lateral tool transfer)	Disable egress controls, backups, and recovery mechanisms to isolate target	Blocked outbound flows; failed backup jobs; disabled logging services
W3	Flexible pursuit participation: individuals may temporarily take different positions during a chase (e.g., leading pursuit or intercepting movement), although roles are not rigidly assigned, and some individuals act as blockers (cutting off escape)	T1059.001 (PowerShell) + T1071.001 (web protocols) + T1003 (OS credential dumping)	Modular malware with specialized components (recon, lateral movement, exfil)	Dynamic role switching across attacker nodes; variation in process and network activity patterns
W4	Pre-hunt vocal coordination: Short-range "hoo" calls used to assemble and synchronize group before departure	T1071.004 (DNS tunneling) + T1001.003 (protocol impersonation)	Low-volume encrypted coordination before main attack burst	Burst of DNS TXT/NULL queries followed by traffic spike
W5	Persistence after temporary loss: Pack resumes chase after briefly losing sight of prey	T1102 (web service) + T1090.003 (multi-hop proxy)	Resume C2 via fallback channels after disconnection or detection	Reconnection via alternate ports/protocols after silence gap
W6	Group size scales with prey size: Larger packs form when targeting larger prey (e.g., wildebeest vs. impala)	T1484 (domain trust discovery) + T1087 (account discovery)	Scale attacker infrastructure based on recon results (e.g., domain admin found)	Increase in number of active attacker nodes following reconnaissance; scaling of network traffic volume and connection attempts
W7	Alloparental care: Non-breeding adults guard den/pups while breeding pair hunts	T1547.001 (registry run keys) + T1543.003 (cron job)	One "guard" node maintains persistence while others conduct active operations	Single node shows autostart artifacts; others show transient activity
W8	Fission-fusion grouping: Subgroups form and merge dynamically based on hunting needs	T1053.005 (scheduled task) + T1029 (scheduled transfer)	Rotate active attackers to reduce per-host footprint and evade detection	Periodic node activation/deactivation; steady aggregate traffic
W9	Reduced vocalization near prey: Dogs become silent during final approach to avoid alerting prey	T1562.006 (indicator blocking) + T1027 (obfuscated files or info)	Disable endpoint telemetry and encrypt exfiltration during final stage	Sudden drop in logs; high-entropy encrypted flows to external IPs
W10	Use of terrain for ambush: Position behind natural cover (bushes, termite mounds) before initiating chase	T1091 (lateral movement) + T1068 (exploitation for privilege escalation)	Hide in low-security network segments (e.g., IoT VLAN), then escalate to core assets	Initial low-visibility activity in isolated network segments, followed by privilege escalation events and lateral movement into critical assets
W11	Post-hunt resting: Pack rests together after successful hunt before next activity cycle	T1029 (scheduled transfer) + T1071.001 (web protocols)	Exfiltrate in bursts followed by extended quiet periods	Data spikes every 60–120s, then >5-min silence
W12	Group decision-making via “sneezes”: Collective hunt initiation requires sufficient participation (measured by sneeze count)	T1071.002 (file transfer) + T1105 (ingress tool transfer)	Distributed trigger: attack launches only after multiple nodes signal readiness	Correlated file transfers across internal hosts before main attack

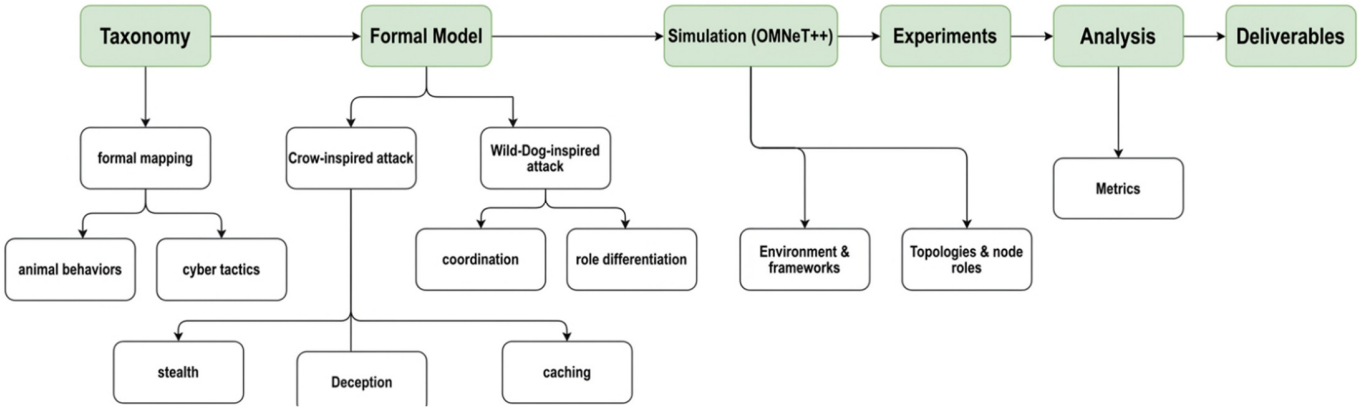

Fig. 1. Research methodology.

B. Simulation

We validate the proposed bio-inspired attack models using the OMNeT++ discrete-event simulator together with the INET framework to provide realistic TCP/IP stacks, hosts, routers, and application traffic. Our methodological pipeline starts with a taxonomy that maps animal behaviors to cyberattack tactics (e.g., crow misdirection → decoy traffic; wild dog coordination → multi-node sequential strikes) and formalizes those archetypes as multi-stage state machines. These formal models are then implemented as modular attacker controllers and compromised host behaviors inside an enterprise network topology. Defender capabilities include signature-based sensors and sliding-window anomaly detectors instrumented at gateway and internal monitoring points. Experiments vary attacker coordination, decoy ratios, and background load; each configuration is repeated multiple times to obtain statistically meaningful measures of attack success, time-to-detect, and detection accuracy. Finally, we export PCAP and per-flow features for offline analysis and release the OMNeT++ project, configuration files, and analysis notebooks to ensure reproducibility.

The simulation environment is implemented in OMNeT++ (with the INET framework). We model two archetypal attacks: Crow (deception + caching) and Wild Dog (coordinated, sequential) as state machines implemented in C++ modules. The enterprise topology includes an Internet gateway, a firewall, a DMZ, and a set of internal hosts. Detectors include a simple signature IDS at the gateway and a sliding-window anomaly detector that computes flow features. For each scenario, we measure attack success probability, time-to-detect, detection precision/recall, and resource overhead. Each experiment is repeated at least 30 times; statistical tests compare our bio-inspired attacks to baseline APT and botnet models.

The simulation scenarios are designed to capture behavioral coordination patterns inspired by biological strategies, rather than reproducing the full operational complexity of real-world malware campaigns. Accordingly, the implemented attacks focus on observable network-level characteristics, such as coordinated traffic bursts, source rotation, staged activity timing, and decoy traffic patterns. Advanced payload-level mechanisms are intentionally abstracted to allow controlled evaluation of behavioral dynamics within the discrete-event simulation environment.

C. Crow-Inspired Cyberattacks

To simulate cyberattacks inspired by the Crow's biological foraging and defense behaviors, we model a dual-layered strategy of deception and intelligent reconnaissance. Unlike standard volumetric attacks, our model distinguishes between "noisy" decoy traffic (the distraction) and stealthy "tool-use" probes (the objective).

- Deception strategy: The crowAttacker node generates high-volume, bursty UDP traffic to saturate the network bottleneck and overwhelm the idsMonitor. This mimics the Crow's behavior of using loud vocalizations to distract potential threats.
- Stealth and tool-use: Under the cover of the decoy noise, the attacker introduces randomized TCP-based malicious patterns. These packets use smaller sizes and irregular intervals to bypass traditional signature-based detection systems while the defender's resources are occupied by the decoy flood.
- Baseline and control: A baseline scenario was established using legitimate background traffic (HTTP/TCP and DNS/UDP) to serve as a control for evaluating latency, throughput, and packet loss metrics.

The INET framework is used to implement the simulation in OMNeT++, utilizing a full TCP/IP stack to ensure realistic congestion control and physical layer behavior. In this framework, each host consists of a comprehensive model of an IPv4/IPv6 host that provides a complete network stack with configurable application, transport, network, and link layers. It supports multiple network interfaces, protocols, and applications that can be customized through parameters, as summarized in Table V.

TABLE V. NODE MODEL COMPONENTS

Layer / category	Module(s)	Research-specific description
Application	app[numApps]	Crow implementation: Configured for multi-stage behavior, including legitimate baseline traffic, noisy UDP decoys, and stealthy TCP probes
Transport	UDP, TCP	Crow implementation: Uses TCP for stealthy "tool-use" reconnaissance and UDP for high-volume "distraction" bursts to test defender response
Network layer	IPv4, IPv6	Crow implementation: Handles realistic routing and ICMP error reporting during bottleneck-induced congestion
Link / bridging	Ethernet, bridging	Crow implementation: Implements a 10 Mbps physical bottleneck with finite DropTail queues to capture realistic packet loss metrics
Physical interfaces	Ethernet	Crow implementation: Standard 802.3 interfaces used for high-fidelity wired organization simulation
Support modules	pcapRecorder	New addition: Vital for capturing raw traffic data at the idsMonitor to calculate detection probability

We evaluated the efficacy of the Crow-inspired deception model within a defense-aware enterprise topology. This architecture transitions from a linear path to a sophisticated environment comprising a multi-application attacker (crowAttacker), a central gateway, and a dedicated idsMonitor to evaluate detection evasion.

- Attacker configuration: The crowAttacker implements a dual-layered traffic strategy. A steady baseline application simulates legitimate user activity (1 pkt/s, 100 B), whereas an aggressive decoy application generates 'crow-like' distraction bursts. The decoy is parameterized with an exponential inter-arrival mean of 0.05 s (approximately 20 pps) and 1500 B MTU-sized packets to intentionally induce queue pressure.

- Network physics and bottlenecks: To ensure physical realism, the gateway-to-targetServer link is configured as a 10 Mbps bottleneck, whereas the internal crowAttacker-to-gateway link operates at 100 Mbps. The gateway utilizes DropTail queuing with finite capacity to realistically model congestion-induced packet loss and buffer exhaustion.
- Defense evaluation: Unlike basic volumetric simulations, this setup specifically measures the detection probability at the idsMonitor. We analyze how the decoy traffic masks stealthy malicious probes by forcing the defender to process high volumes of 'noisy' data.
- Statistical rigor: To ensure results are statistically significant, each scenario was executed with 30 independent iterations (repeat = 30) for a duration of 120 s.

D. Wild Dog–Inspired Cyberattacks

Inspired by wild dogs' cooperative hunting strategies, we designed cyberattack scenarios that mimic their coordination and adaptability.

Table VI shows how different cyberattacks can be modeled based on wild dog hunting behaviors. Each row links a type of attack to the settings used in the OMNeT++ simulations and to the data that can be measured during the experiments. The table helps explain how attackers behave, how the network responds, and what signals can be tracked to detect these behaviors. Connecting biological strategies with technical parameters and measurable outcomes gives a clear picture of how attacks are simulated and how their effects can be observed, making it easier to study, test, and improve detection methods. These behaviors are implemented using the specialized submodules in our OMNeT++ environment: the botnet [6] for high-volume bursts, scouts [4] for reconnaissance, and ambushNodes [3] for dormant-to-strike activation. By converging these flows at the edgeRouter before passing through the coreGateway bottleneck, we can precisely record the measurable signals monitored by the idsMonitor.

IV. RESULTS AND EVALUATION

A. Results and Evaluation

In the Crow scenario, we injected aggressive, bursty UDP decoy traffic from host A to host B while preserving a steady baseline flow for comparison, as presented in Table VIII and in Figure 2. The decoy traffic increased the total packet count by 225% (20 → 65 packets) but produced only a modest increase in measured throughput (+4%), indicating that the network became saturated and packets were queued rather than increasing the delivered payload rate. Average end-to-end delay more than tripled (123,453 ms → 379,601 ms, +207.5%), showing severe queuing and latency due to buffer buildup at the router bottleneck. Interestingly, packet loss dropped from 5% to 0% under the Crow load; this is consistent with packets being held in the router queue (DropTail, capacity = 100 packets) and delivered later rather than being dropped. Overall, the results indicate that the Crow decoy effectively floods the path, increasing queuing delay and degrading timeliness, while not increasing throughput proportionally—a pattern expected when a bottleneck link and finite queuing cause large buffers and long delays under UDP flooding.

TABLE VI. CYBERATTACK BEHAVIORS, OMNET++ SIMULATION PARAMETERS, AND OBSERVABLE SIGNALS

Behavior analogy	**Cyberattack type**	**OMNeT++ simulation parameters**	**Measurable signals / data to record**
Coordinated burst	Synchronized multi-node DDoS attack	Attackers: 6 nodes launch synchronized bursts. Burst duration: 3 s. Send interval during burst: exponential, mean 0.02 s.	Aggregate packet-rate spikes over time. Router queue length / packet-loss spikes. Instantaneous latency increases.
Scout (low-rate probing)	Network reconnaissance / slow probes	Scout nodes: 4 nodes perform reconnaissance. Send interval: exponential, mean 5 s. Packet size: 200 B.	Low-rate background traffic. Rare destination IP/port changes. Destination-entropy analysis.
Ambush (dormant to strike)	Dormant bots with coordinated activation	Ambush nodes: 3 nodes initially dormant. Sleep duration: uniform, 120–300 s. On wake: burst 2 s. Send interval exponential mean 0.03 s.	Long quiescence followed by abrupt rate spikes. Node activation / deactivation timestamps.
Fission–fusion (rotation)	Rotating active subsets for evasion	Total attackers: 13 nodes. Active set size: 5 nodes active at once. Rotation interval: 60 s; duty cycle: 40 s on / 80 s off.	Node duty-cycle traces. Aggregate rate steady; per-node low footprint. Detection false-negative risk metrics.
Distraction + stealth exfiltration	Noisy decoy flow with covert exfiltration	Decoy flow: one high-volume node. Stealth exfiltration: one node sends a packet every 10 s. Concurrency: decoy + stealth simultaneous.	Cross-flow correlation analysis. Small but consistent stealth-flow bytes.

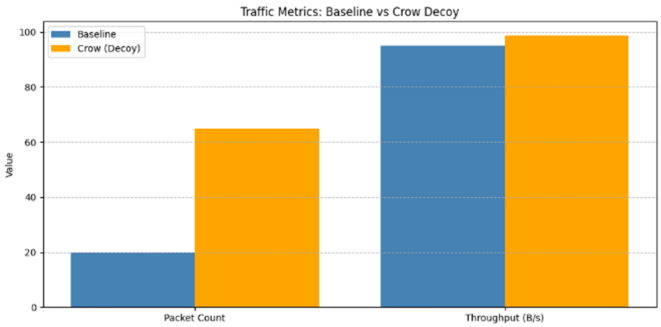

Fig. 2. Baseline vs. Crow decoy.

The simulation results clearly illustrate the impact of Crow decoy attacks on network performance. Figure 3 shows the evolution of the router queue on the bottleneck link, highlighting a stark contrast between baseline and attack scenarios. While the baseline maintains minimal queue

occupancy, increasing decoy aggression (from low to high) causes the queue to fill rapidly, often reaching its maximum capacity of 50 packets, resulting in significant packet drops and confirming severe congestion. Figure 4 presents the Cumulative Distribution Function (CDF) of benign packet delays, providing further insight into the attack's effects on latency. Under the baseline, nearly all packets experience negligible delays, with the CDF rising sharply to nearly zero. In contrast, the low and medium Crow decoy attacks shift the CDF to the right and flatten the curve, indicating a broad distribution of delays and substantial latency for a large fraction of packets. For the medium attack, 50% of packets experience delays up to ~50 ms, with some exceeding 100 ms, and the drop-off at the tail reflects increased packet loss. Together, these figures confirm that the Crow decoy attack significantly disrupts legitimate traffic, demonstrating a successful denial-of-service effect through both congestion and elevated latency.

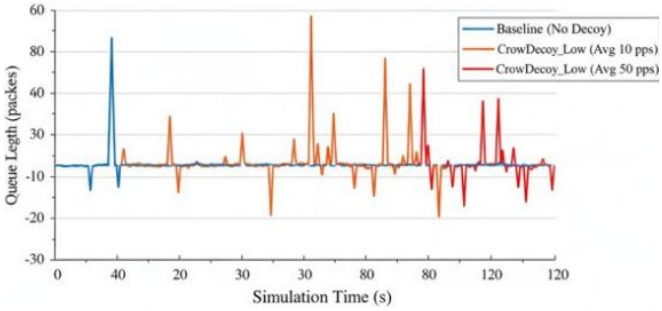

Fig. 3. Router queue length on bottleneck link (router to host B).

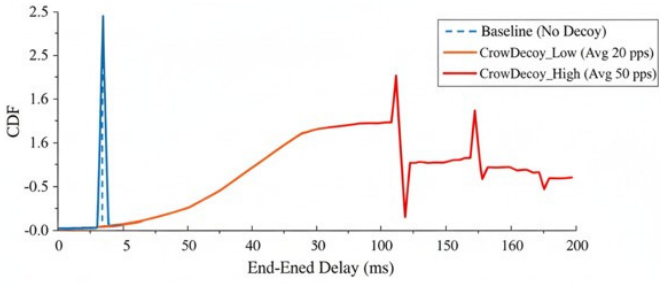

Fig. 4. CDF of benign traffic end-to-end delay (port 1,000).

The Crow's saturation of the router queue is a deception tactic. Its significance lies in creating a "temporal blind spot": by filling the buffer, the attacker causes a lag in IDS processing, which can be exploited for stealthy exfiltration.

B. Wild Dog Scenario

We simulated the Wild Dog attack scenario using OMNeT++ and extracted key network performance features, summarized in Table VII. The features include metrics such as packet count, throughput, average delay, packet loss, queue length, and TCP retransmissions, which collectively provide a comprehensive view of the network's behavior under attack conditions. By analyzing these features, we can quantify the impact of coordinated malicious activity on both the target and intermediary network components.

TABLE VII. FEATURES EXTRACTED FROM OMNET++ FOR THE WILD DOG ATTACK SCENARIO

Feature	Description
packet_count_sent	Number of packets sent by a host or application
packet_count_recv	Number of packets received by the target/application
bytes_sent	Total bytes transmitted by a host/application during the measurement window
throughput_Bps	Average bytes per second received by the target over the window
avg_delay_ms	Mean end-to-end packet delay in milliseconds
jitter_ms	Variation of inter-arrival times in milliseconds
packet_loss_pct	Packet loss percentage = (sent − received) / sent × 100
queue_length_mean	Mean queue occupancy at the switch/router during the window (packets), from queue signals
queue_drops	Number of packets dropped at the switch or queue module (drop counters/signals)
tcp_retransmissions	Number of TCP retransmissions observed for a flow
tcp_goodput_Bps	Successfully delivered TCP bytes per second
time_window_start	Start time of the aggregation window(s)—useful for time-series analysis

Table VIII summarizes the impact of the Wild Dog attack on network performance, comparing baseline traffic to the scenario under attack. The results show dramatic increases in packet count, throughput, delay, packet loss, and jitter, reflecting the disruptive effect of coordinated aggressive behavior in the network. Unlike a pack of wild dogs that overwhelms its prey, attackers in this scenario flood the network, causing congestion, delays, and loss of legitimate traffic.

TABLE VIII. COMPARISON OF BASELINE TRAFFIC AND WILD DOG ATTACK SCENARIO (MEAN VALUES ACROSS 30 RUNS)

Metric	Baseline mean	Wild Dog mean	Change (%)
Packet count	20.0	480.0	+2,300.0
Throughput (B/s)	95.0	420.0	+342.105
Avg delay (ms)	123,453.0	1,200,000.0	+872.110
Packet loss (%)	5.0	70.0	+1,300.0
Jitter (ms)	10.0	200.0	+1,900.0

V. CONCLUSION

Connecting attack behavior with biological behaviors, such as distraction and coordinated aggression, improves the understanding of these attacks' mechanisms and potential impacts.

Crow decoy attacks demonstrate their significance in compromising network performance by rapidly saturating router queues, causing substantial packet loss, and dramatically increasing latency for legitimate traffic. The findings of this study show how behaviors observed in nature can effectively represent complex cyberattack patterns. Both the Crow and Wild Dog simulations showed that when attackers act in a coordinated and adaptive manner, network resources can quickly become congested, leading to significant packet loss and communication delays. These findings emphasize that studying biological strategies, such as group coordination and

distraction, can provide valuable insights into understanding and predicting cyber threats.

In the future, it would be beneficial to integrate the proposed framework with an Intrusion Detection System (IDS). Later, simulation datasets can be extracted to support Machine Learning (ML) techniques for simplifying the detection, classification, and mitigation of such bio-inspired attacks more efficiently, paving the way toward intelligent and adaptive defense systems capable of responding to evolving threats.

DECLARATION OF COMPETING INTERESTS

The authors declare that they have no competing interests.

ACKNOWLEDGMENT

Not applicable to this work.

DATA AVAILABILITY

The data used in this study were generated through simulations using OMNeT++. No external datasets were used. The simulation models and configurations are available from the authors upon reasonable request.

REFERENCES

[1] M. A. I. Mallick and R. Nath, "Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments," *World Scientific News*, vol. 190, no. 1, pp. 1–69, Jan. 2024.

[2] N. R. Choudhury, S. Paul, and S. Ghosh, "Comparative Analysis of Traditional vs. AI-Driven Network Security," in *AI for Large Scale Communication Networks*, R. Kanthavel and R. Dhaya, Eds. Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 107–128, 10.4018/979-8-3693-6552-6.ch006, https://doi.org/10.4018/979-8-3693-6552-6.ch006.

[3] N. Fang, C. Xu, X. Gong, and Z. Wu, "A new human-based offensive defensive optimization algorithm for solving optimization problems," *Scientific Reports*, vol. 15, no. 1, Apr. 2025, Art. no. 12119, https://doi.org/10.1038/s41598-025-96559-6.

[4] P. K. Myakala, C. Bura, and A. K. Jonnalagadda, "Artificial Immune Systems: A Bio-Inspired Paradigm for Computational Intelligence," *Journal of Artificial Intelligence and Big Data*, vol. 5, no. 1, pp. 1–13, Jan. 2025, https://doi.org/10.31586/jaibd.2025.1233.

[5] R. Satheeskumar, V. Premalatha, R. K. Talatoti, S. Vecha, and M. Koteswara Rao, "Next-generation ant-inspired cryptography for secure and resilient decentralized IoT ecosystems," *Iran Journal of Computer Science*, vol. 8, no. 4, pp. 2221–2236, Dec. 2025, https://doi.org/10.1007/s42044-025-00311-2.

[6] C. Blum, "Ant colony optimization: A bibliometric review," *Physics of Life Reviews*, vol. 51, pp. 87–95, Dec. 2024, https://doi.org/10.1016/j.plrev.2024.09.014.

[7] M. Irfan, "Nature-Inspired Techniques in Cybersecurity: Evolving Approaches to Domain Detection and Threat Mitigation," Sept. 2024, https://doi.org/10.13140/RG.2.2.14573.81124.

[8] S. G. Qureshi and S. K. Shandilya, "Novel Hybridized Crow Optimization for Secure Data Transmission in Cyber Networks," in *Advances in Nature-Inspired Cyber Security and Resilience*, S. K. Shandilya, N. Wagner, V. B. Gupta, and A. K. Nagar, Eds. Cham, Switzerland: Springer International Publishing, 2022, pp. 137–156, https://doi.org/10.1007/978-3-030-90708-2_8.

[9] D. Prabakaran, K. R. Senthil, and R. Shyamala, "14 A Novel African Wild Dog Optimization (AWDO) Algorithm for Applications of Artificial Intelligence," in *Math Optimization for Artificial Intelligence: Heuristic and Metaheuristic Methods for Robotics and Machine Learning*, U. Kumar Lilhore, V. Dutt, T. A. Kumar, M. Margala, and K. Raahemifar, Eds. Berlin, Germany: De Gruyter, 2025, pp. 303–316, https://doi.org/10.1515/9783111436180-014.

[10] Ö. Sen *et al.*, "Simulation of multi-stage attack and defense mechanisms in smart grids," *International Journal of Critical Infrastructure Protection*, vol. 48, Mar. 2025, Art. no. 100727, https://doi.org/10.1016/j.ijcip.2024.100727.

[11] A. N. Khan, J. Bryans, G. Sabaliauskaite, and H. Jadidbonab, "Integrated Attack Tree in Residual Risk Management Framework," *Information*, vol. 14, no. 12, Nov. 2023, Art. no. 639, https://doi.org/10.3390/info14120639.

[12] E. Iturbe, J. Arcas, E. Rios, and N. Toledo, "A Multi-layer Approach through Threat Modelling and Attack Simulation for Enhanced Cyber Security Assessment," in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, Vienna, Austria, 2024, pp. 1–8, https://doi.org/10.1145/3664476.3670458.

[13] M. Alhazmi, A. P. Zhao, X. Cheng, and C. Yang, "Multistage adaptive cyberattack in power systems with CNN identification feedback loops," *Scientific Reports*, vol. 15, no. 1, July 2025, Art. no. 25051, https://doi.org/10.1038/s41598-025-10582-1.

[14] A. Zimba, H. Chen, Z. Wang, and M. Chishimba, "Modeling and detection of the multi-stages of Advanced Persistent Threats attacks based on semi-supervised learning and complex networks characteristics," *Future Generation Computer Systems*, vol. 106, pp. 501–517, May 2020, https://doi.org/10.1016/j.future.2020.01.032.

[15] M. M. Alani, L. Mauri, and E. Damiani, "A two-stage cyber attack detection and classification system for smart grids," *Internet of Things*, vol. 24, Dec. 2023, Art. no. 100926, https://doi.org/10.1016/j.iot.2023.100926.

[16] M. K. Ahn, Y. H. Kim, and J.-R. Lee, "Hierarchical Multi-Stage Cyber Attack Scenario Modeling Based on G&E Model for Cyber Risk Simulation Analysis," *Applied Sciences*, vol. 10, no. 4, Feb. 2020, Art. no. 1426, https://doi.org/10.3390/app10041426.

[17] A.-M. Konsta, A. Lluch Lafuente, B. Spiga, and N. Dragoni, "Survey: Automatic generation of attack trees and attack graphs," *Computers & Security*, vol. 137, Feb. 2024, Art. no. 103602, https://doi.org/10.1016/j.cose.2023.103602.

[18] A. Rana, S. Gupta, and B. Gupta, "A comprehensive framework for quantitative risk assessment of organizational networks using FAIR-modified attack trees," *Frontiers in Computer Science*, vol. 6, Feb. 2024, Art. no. 1304288, https://doi.org/10.3389/fcomp.2024.1304288.

[19] V. Kuikka, L. Pykälä, T. Takko, and K. K. Kaski, "Network modelling in analysing cyber-related graphs," *Frontiers in Complex Systems*, vol. 3, Sept. 2025, Art. no. 1620260, https://doi.org/10.3389/fcpxs.2025.1620260.

[20] L. Serena, G. D'Angelo, S. Ferretti, and M. Marzolla, "Simulation in Cybersecurity: Understanding Techniques, Applications, and Goals." arXiv, Aug. 08, 2025, https://doi.org/10.48550/arXiv.2508.06106.

[21] G. Erceylan, A. Akbarzadeh, and V. Gkioulos, "Leveraging digital twins for advanced threat modeling in cyber-physical systems cybersecurity," *International Journal of Information Security*, vol. 24, no. 3, June 2025, Art. no. 151, https://doi.org/10.1007/s10207-025-01043-x.

[22] A. Garba *et al.*, "Utilizing Ant Colony Optimization for Result Merging in Federated Search," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14832–14839, Aug. 2024, https://doi.org/10.48084/etasr.7302.

[23] S. Khalid and S. Wu, "Supporting Scholarly Search by Query Expansion and Citation Analysis," *Engineering, Technology & Applied Science Research*, vol. 10, no. 4, pp. 6102–6108, Aug. 2020, https://doi.org/10.48084/etasr.3655.

[24] S. Khalid, S. Khusro, I. Ullah, and G. Dawson-Amoah, "On The Current State of Scholarly Retrieval Systems," *Engineering, Technology & Applied Science Research*, vol. 9, no. 1, pp. 3863–3870, Feb. 2019, https://doi.org/10.48084/etasr.2448.