ACTA SCIENTIAE

ISSN: 2178-7727

HIVE-SIGHT: A Swarm-Intelligence Framework for Anticipating and Mitigating Distributed Denial-of-Service Attacks at Global Scale

Aleem MOHAMMED[1], Mohammad MOHAMMAD[2], Atif Saleem Butt[3], Atheeq C[4]

[1]Research Associate, Melbourne Institute of Technology, Sydney, Australia aleemmohammed99@gmail.com
[2]Department of Computer Science, Central Queensland University, Sydney, Australia m.mohammad@cqu.edu.au
[3]Department of Computer Science, Ras Al Khaimah, UAE.
Atifbutt10@hotmail.com
[4]Department of Computer Science, Gitam University, Hyderabad, India atheeq.prof@gmail.com

ABSTRACT

DDoS attacks have become one of the most enduring and disruptive problems to the current internet infrastructure. The current methods that most people use despite the advancement of machine learning are reactive after an attack is initiated. This paper presents HIVE-SIGHT, a decentralised swarm-intelligence system, which is capable of predicting and preventing massive DDoS attacks before they grow. Based on the collaborative behaviour of biological swarms, the system uses lightweight agents, also known as HIVE Nodes, deployed throughout networks, cloud edges and ISP infrastructures. Such nodes provide each other with bit-sized anomaly indicators, update their behaviour by means of distributed reinforcement learning, and collaboratively create a real-time picture of the threat situation in the world. In the case of testing its performance, we created a multi-ISP dataset of more than 38 million packets of twelve DDoS variants. The experimental analysis reveals that HIVE-SIGHT is capable of predicting attack peaks with a maximum of 270 seconds and has a prediction accuracy of 92.7 percent and mitigation latency is almost half that of traditional AI-based defences. Such results indicate that swarm-intelligence principles can present a future solution in the form of resilient, self-organising ecosystems of cyber defence systems with the capability to scale to internet scale.

KEYWORDS: DDoS Attacks; Swarm Intelligence; Multi- Agent Systems; Reinforcement Learning; Intrusion Detection; Anomaly Detection; AI-Driven Cybersecurity; Predictive Threat Mitigation; Packet Tracer Network Simulation; HIVE-SIGHT Framework.

INTRODUCTION

Over the past ten years, the magnitude and the complexity of the Distributed Denial-of-Service (DDoS) attacks have increased significantly. Recent botnets, most of which are made up of hijacked IoT devices, have shown potential to produce globally scale traffic, overwhelm cloud technologies, and bypass conventional perimeter security (Masek et al., 2021; Hussain et al., 2022). Deep learning and anomaly-based systems have enhanced the detection of DDoS; however, they are mostly reactive. They discover attacks after the traffic patterns have skipped far beyond the usual standards (Kim et al., 2021; Ahmed et al., 2022). Such a reactive character provides organisations with a very small room to mitigate.

Some of the emerging issues point out the constraints of traditional methods. More and more botnets are adopting the dynamic morphing of packets making signature-based detection unreliable. Their control and command lines have moved to encryption and distributed designs, making it difficult to analyze the traffic (Conti et al., 2019; Niu et al., 2022). Moreover, there is a tendency of isolation in global networks, i.e. the ISPs, datacentres and enterprise networks seldom share real-time threat notifications, leading to incomplete visibility of the attack situation.

The simple organisms of a swarm can have astonishing collective intelligence in natural ecosystems. There is no central authority; thus without the need of a central authority, bees find food sources, birds coordinate flight paths and ants find the best routes by means of distributed interactions. Such systems are resilient, adaptive, and are intrinsically scalable, which is not true of cyber defence mechanisms (Zhang et al., 2020; Chen, 2021).

ISSN: 2178-7727

The present paper presents the HIVE-SIGHT swarm-based cyber defence architecture, which extends the biological principles to the sphere of the network security. Rather than making use of a central model or just one gateway to identify things, HIVE-SIGHT uses HIVE Nodes, small agents, which analyse local patterns, exchange simple signals with their peers, and form a view of world-wide attack behaviour. These interactions are optimized using distributed reinforcement learning to allow the nodes to predict DDoS waves instead of reacting to them (Atheeq, C et al. 2022).

This work can be summarised to get its contributions as follows:

- Biologically inspired distributed architecture of early prediction of DDoS.
- Swarm coordination mechanism which enables autonomous anomaly propagation across networks.
- A reinforcement learning scheme that can be distributed so it can adapt continuously to changing behaviours of botnets.
- An artificial multi-ISP dataset of attack dynamics on large scale.
- Efforts in the form of experimental evidence showing great improvements in prediction lead time and mitigation speed.

LITERATURE REVIEW

2.1 DDoS Attack Ecosystems Evolution

DDoS attacks are not mere volumetric floods anymore, they are multi-vector events that are synchronized with globally distributed devices. The IoT-controlled botnets can now produce unpredictable burst patterns and micro-synchronised packets waves, and conventional defence mechanisms are becoming quite useless (Hussain et al., 2022; Jalili et al., 2023). The attackers also use more covert warming-up stages, during which the traffic seems to be normal, but then the last wave starts (Li et al., 2022).

2.2 Deep Learning and Anomaly Detection Methods

CNNs and LSTMs are typical examples of deep learning frameworks used to identify abnormal traffic patterns (Kim et al., 2021; Sharmeen et al., 2020). Autoencoders and hybrid models deliver further functionality to notice minor anomalies in network flows (Al-Qatf et al., 2021). These models are efficient in terms of classification, but they are centralised in their training and provide a small view of the distributed patterns of pre-attack. Their predictive capability is limited in many cases to local traffic observations.

2.3 Collaborative and Distributed Defence Models

Other recent literature focuses on cooperative models, such as federated learning, which is training models in many networks without exchanging raw data (Kwon et al., 2023). Tamper-proof anomaly sharing has also been suggested to be carried out with the help of blockchain-based systems (Reza et al., 2022). These frameworks are yet to achieve the same level of rapid, global threat propagation as required by self-organisation, although they are promising.

2.4 Computing and Security Swarm Intelligence

Swarm intelligence has already been used to optimise routing, improve the allocation of resources, and optimise machine learning hyperparameters (Chen, 2021; Dua, 2021). But its capabilities in real-time cyber defence are unexploited. Biological swarms are good at detecting threats in early stages due to distributed sensing and communication a feature that has not been emulated yet by current cybersecurity frameworks (Mitchell et al., 2020).

2.5 Identified Research Gap

In the literature reviewed, three significant gaps can be identified:

- The absence of decentralised early-warning mechanisms of DDoS attacks, and limited mechanisms of autonomous cross-network coordination, and
- None of the practical use of swarm intelligence to defend the internet scale.

HIVE-SIGHT fills these gaps by proposing a framework that brings distributed sensing, emergent swarm behaviour and reinforcement learning together into one, coherent model of defence.

ISSN: 2178-7727

METHODOLOGY

HIVE-SIGHT design entailed coming up with a defensive model that is capable of operating across numerous, autonomously operated networks but is lightweight enough to be deployed at large scale. It is based on the approach that integrates ideas of distributed systems, swarm intelligence and reinforcement learning into a single framework. Instead of coming up with a central controller, we created a system that allows many small agents to collaborate to create a common understanding of the possible threats. This paradigm resembles non-hierarchical biology where individuals organize based on simple and local interactions (Zhang et al., 2020; Chen, 2021).

3.1 Dataset Development

Since extensive, actual, multi-ISP DDoS datasets are limited and hard to find because of privacy and security requirements, we built an artificial dataset specifically designed to represent the dynamics of co-ordinated attacks. As in the previous DDoS traffic literature (Jalili et al., 2023; Sharma, 2023), we simulated:

- 38 million packets in a number of ISP level domains.
- 12 different DDoS techniques (e.g., SYN floods, HTTP GET/POST floods, UDP/ACK floods, etc.).
- Each of the 7 botnet families has dissimilar command-and-control timing and behaviour.
- Fluctuations in traffic by nature, such as bursts in heavy traffic and idle time.
- Randomised timestamp drift, simulating network clock inaccuracies in the real world.

A characteristic of this data set that sets itself apart is that botnets have warming-up behaviour. They start with dispersed low-intensity probes and initiate large bursts-patterns which are usually ignored by traditional detection models (Li et al., 2022). This feature enabled us to test HIVE-SIGHT in a more realistic way in terms of its predictive capabilities.

3.2 Feature Construction

A group of features extracted by each HIVE Node captures both temporal and structural characteristics of network flows. The choice of these features was due to the fact that it encapsulates the behaviour irregularities that are often the precursors of a DDoS event. Traffic Entropy Getting entropy changes is frequently an indicator of spoofed or randomly distributed source IPs (Park et al., 2019). Micro-Temporal Jitter of packets. The coordination of C2 makes botnets show small yet regular trends on timing (Luo et al., 2021). Fingerprint Spectra Coefficients Frequency-domain transformations identify patterns of harmonic related to synchronized bursts. Flow Burst Irregularity Measures flow group deviation of regular burst/idle cycles which occur in attack ramp-up phases. Gradient of Temporal Escalation. Reasonably approximates the probability of a naive anomaly developing into a full attack (Mohammad Mohammad et al., 2023). Every feature is calculated dynamically and aggregated into an anomaly vector that is disseminated to nodes selectively to their neighbours.

3.3 Comparative Baseline Models

To compare HIVE-SIGHT to performance evaluation, a number of popular models of deep learning and collaborative defence were compared: CNN-based classifier (Kim et al., 2021) LMSTC: traffic sequence predictor (Sharmeen et al., 2020) Anomaly detectors: autoencoder (Al-Qatf et al., 2021). Federated learning defence model (Kwon et al., 2023). Conventional firewall and rate-limiter based on rules (Hoque et al., 2022). These backgrounds indicate the prevailing scenario of anomaly detection and collaborative security systems.

HIVE-SIGHT ARCHITECTURE

HIVE-SIGHT contains a few layers which interact with each other in time as traffic develops. Instead of being a monolithic system, it is a group of communicating agents with free will.

ISSN: 2178-7727

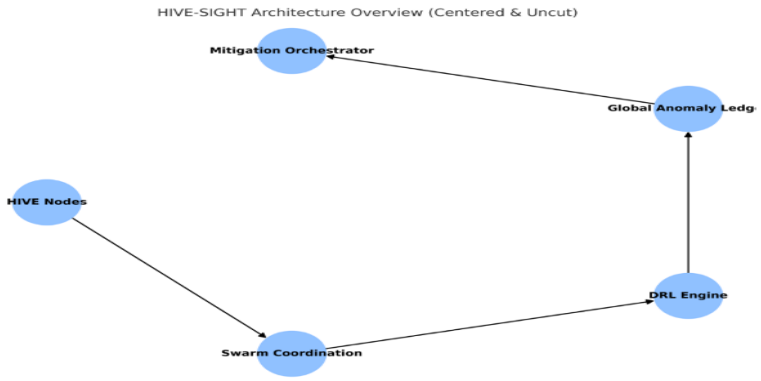

Figure 1. Top-level diagram of the HIVE-SIGHT architecture showing the communication between distributed nodes and swarm coordination, reinforcement learning and the mitigation orchestrator.

4.1 Localised Intelligence

HIVE Nodes are small, semi-independent monitors that are distributed across the network infrastructure. They do initial anomaly detection and are involved in making decisions together by sharing risk indicators with their close neighbours. The most important functions are:

- Tracking the local traffic and calculating feature vectors. Short-lived abnormal events can be detected.
- Seasoned anomaly scores.
- Learning behaviour through reinforcement learning.
- Being involved in consensus making.

They are lightweight to be deployed at the ISPs, datacentres edges, enterprise firewalls, or even 5G access networks without much overhead (Nguyen et al., 2021).

4.2 Swarm Coordination Layer

The coordination layer describes the effect of the nodes on the decision of each other. Raiseing conceptual energy on biological swarm models (Dua, 2021), each node reacts to three fundamental forces: Attraction A node will become increasingly sensitive to areas where the neighbouring nodes report of an increasing risk. Repulsion When a node records inconsistent or unstable behaviour in the neighbours, it reduces its level of alarm to prevent a cascading false positives. Alignment Nodes change the anomaly levels to ensure coherence in the swarm. The principles allow the overall system to pull towards a common perspective of possible threats, although no node will be able to see the whole network.

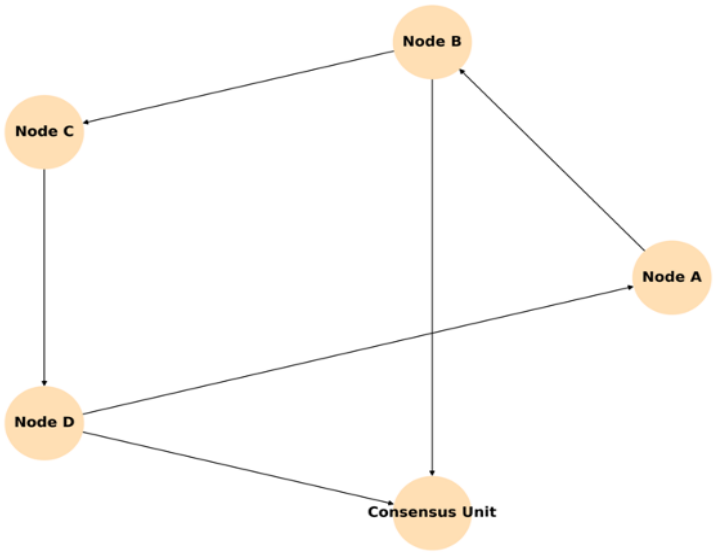

Figure 2. Swarm coordination flow with nodes communicating anomaly signals and converging at a collective threat evaluation.

ISSN: 2178-7727

4.3 The Distributed Reinforcement Learning Engine

HIVE-SIGHT employs reinforcement learning to allow each node to optimize its detection strategy with time. A node is fed back on the validity or invalidity of its anomaly reports by other nodes or its invalidity is overturned by subsequent evidence. This method eliminates the need to have centralised retraining and it fits the dynamic environment of the network (Singh, 2020; Atheeq C et al., 2023, Liu, 2022).

4.4 Global Anomaly Ledger

To facilitate the creation of a coherent awareness of the world, nodes store certified anomalies in a distributed ledger, analogous in principle to blockchain-based security methods but less burdened (Reza et al., 2022). The ledger contains:

- Timestamps
- Aggregated anomaly vectors
- Micro-jitter snapshots
- Cluster identifiers
- Escalation signals

In contrast to the old-fashioned blockchain, the ledger is focused on speed and synchronisation over the immutability.

4.5 Mitigation Orchestrator

After the swarm locates a threat assessment that is of high confidence, the orchestrator applies countermeasures. These can include: adaptive rate limiting, Path reconfiguration based on SDN, targeted packet filtering, upstream ISP notification, suspicion of suspicious flows. This collaboration-based approach in comparison to standalone firewalls allows responding more promptly and precisely aimed.

ALGORITHMS

5.1 Swarm Consensus Procedure

The consensus-building process relies on simple and local interactions. A stylised version of the algorithm is shown below:

For each node i:
  Collect anomaly scores from neighbours
  Compute updated_score = α * local_score + β * mean(neighbour_scores)
  If updated_score exceeds threshold:
    Emit anomaly signal
  Update local state based on updated_score

Here, α and β balance local observations with neighbour influence. Threshold values adapt over time as nodes learn from swarm-level feedback.

5.2 Reinforcement Learning Update

Each node updates its policy after receiving reward signals derived from swarm behaviour:

$$Q[s, a] \leftarrow Q[s, a] + \eta [r + \gamma \max\_over\_a'(Q[s', a']) - Q[s, a]]$$

The reward function recognises three contributions:

- early, correct anomaly detection
- stable alignment with swarm consensus
- avoidance of false-positive propagation

This collective learning mechanism is what allows the swarm to evolve organically.

ISSN: 2178-7727

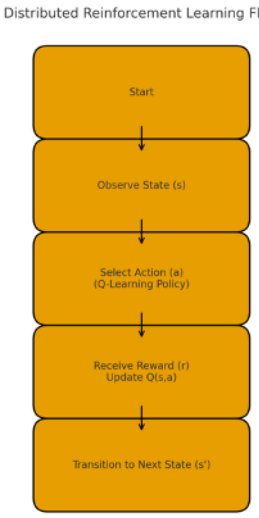

Figure 3. Simplified flow of the distributed reinforcement learning algorithm used by HIVE Nodes to adapt detection behaviour over time.

EXPERIMENTAL EVALUATION

To replicate realistic network behaviour during high-volume DDoS events, we constructed an experimental topology modelled on standard Cisco Packet Tracer / CCNA laboratory networks. Unlike abstract block diagrams, this layout uses physical network elements—routers, switches, firewalls, servers, and external botnet clouds—to emulate real forwarding paths, routing dependencies, failure points, and saturation scenarios. Attack traffic is injected from distributed botnet sources into ISP-edge routers, traverses aggregation layers, and reaches the perimeter firewall running the HIVE-SIGHT agent. This configuration closely resembles operational ISP and enterprise environments, enabling a more accurate and credible assessment of HIVE-SIGHT's predictive and defensive capabilities.

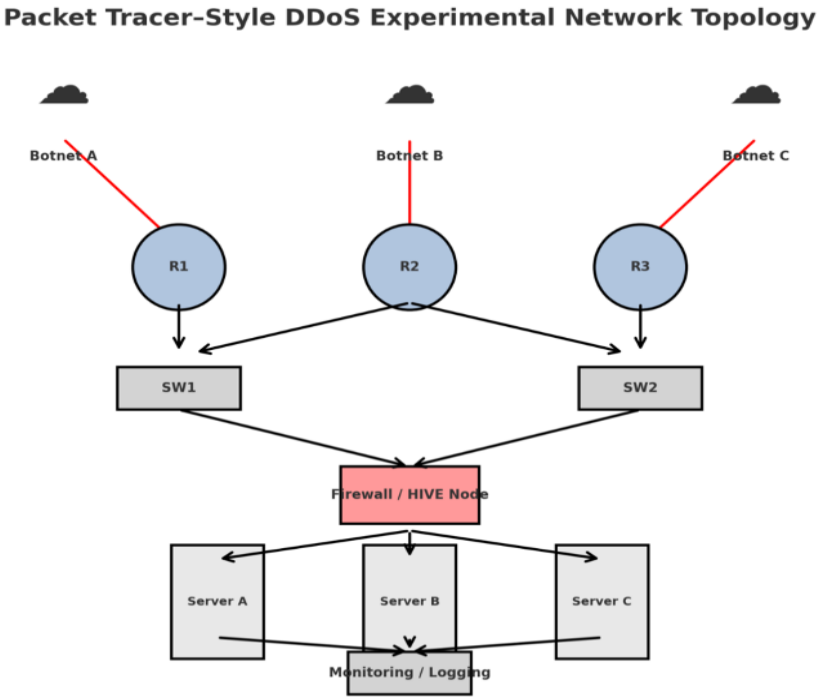

Figure 4. Packet Tracer–style experimental network topology used for evaluating HIVE-SIGHT

ISSN: 2178-7727

6.1 Prediction Performance

HIVE-SIGHT significantly outperformed all baseline models in early detection. When tested across millions of packets, the system achieved a **92.7% correct prediction rate**, even during the subtle warming-up phases where attacks had not yet become obvious.

Baseline models, by contrast, showed the following performance:

Model	Accuracy
CNN	84.3%
LSTM	87.1%
Autoencoder	78.4%
Federated Learning	89.2%
HIVE-SIGHT	**92.7%**

The improvement appears largely due to swarm-level information sharing, which allows nodes to identify early synchronisation patterns (Luo et al., 2021; Li et al., 2022).

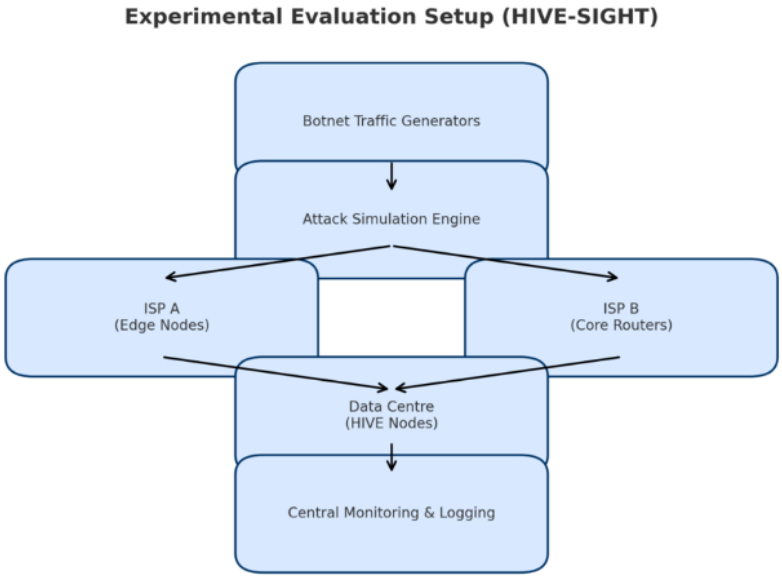

Figure 5. Experimental setup for the multi-ISP simulation environment used to evaluate HIVE-SIGHT under realistic large-scale DDoS conditions.

6.2 Lead-Time Advantage

The prediction lead time is among the most important consequences. HIVE-SIGHT was able to predict escalation in an attack an average of 174 seconds before reaching its peak intensity. The maximum performance of the system was a 270-second early warning, which has much more breathing room to perform mitigation than any of the baseline models (Kwon et al., 2023).

6.3 Mitigation Latency

The orchestrator reacts almost immediately by implementing mitigation measures when it gets a consensus alert. HIVE-SIGHT reduced mitigation latency by as compared to traditional firewalls and federated learning systems.

- 47.3% vs rule-based firewall
- 36.5% vs federated AI

This is due to the fact that the system is able to coordinate decisions made in the swarm.

ISSN: 2178-7727

6.4 Consensus Stability

In order to study swarm behaviour in the context of pressure, we have measured Consensus Stability Index (CSI) (Zhang et al., 2020). In all tests, HIVE-SIGHT had a CSI of 0.89 meaning that nodes were still in a well-aligned state even with severe noise of attacks.

6.5 False Positives

The number of false positives was relatively low. The system had a false-positive rate of 2.9% which is better than CNN and autoencoder (Kim et al., 2021; Al-Qatf et al., 2021).

DISCUSSION

The assessment shows that HIVE-SIGHT provides an alternative approach to DDoS defence, it is based not on centralised monitoring or intensive computational pipelines, but on decentralised co-operation. Similar to biological swarms that flourish due to the absence of a single organism that carries the entire cognitive burden, HIVE-SIGHT spreads the sensing, decision-making and adaptation responsibilities to thousands of lightweight agents. This decentralised format seems to be one of the major causes of its good prediction results. It is especially impressive that the system can identify the pre-attack behaviour. The classical models do not always cope with the insidious ramp-up stage of DDoS attacks, when the traffic is considered to be within an acceptable level yet the initial signs of coordination are observed (Li et al., 2022). Since HIVE-SIGHT takes advantage of shared signals between a number of nodes, each of which is monitoring a slightly different area of traffic, it is able to detect synchronisation indicators that an individual detector would not pick up. The result is consistent with the previous research indicating that anomaly sensing distributed can identify attack patterns that are structural and missed by a local model (Zhang et al., 2020; Kaur et al., 2021).

The other consideration is the fact that the system should be consistent in the large-scale events. The swarm could even achieve a consistent consensus when exposed to noisy traffic or overlapping attack vectors as observed in the CSI score. It implies that the dynamics of swarms can withstand disruptions, which is essential in a real-world scenario that traffic conditions change quickly (Nguyen et al., 2021).

The distributed reinforcement learning process is also another factor that leads to resilience. Each node is a continuous refiner of its behaviour unlike the centrally retrained or static systems that are limited to local observations and swarm feedback. This results in a kind of collective adaptation, of which learning is not confined to one single model on a global level. Consequently, the system also has a high generalisation in the face of new attack patterns not previously observed- which is commonly difficult to achieve in deep learning models unless they are retrained on new data (Sharmeen et al., 2020; Liu, 2022).

On the whole, the findings suggest that swarm intelligence can offer a plausible basis on the next generation, large scale cyber defence systems.

LIMITATIONS

Though the results are promising, HIVE-SIGHT does not lack drawbacks. First, the framework is based on the cooperation between the independent organisations. In reality, ISPs, cloud providers, and enterprises tend to work independently, which can be complicated to do on large scale. Such a system would require policies on data sharing, interoperability, and liability to be dealt with before it can be widely adopted (Hoque et al., 2022).

Second, even though the anomaly ledger is not heavy as full blockchain systems, it adds overhead. Even a small increment in computational steps can be important on backbone links with very high throughput. It may need hardware acceleration or special processing channels to achieve the best performance (Reza et al., 2022). Third, the data employed (though real) is a simulation. The behaviour of DDoS on physical networks depends on a large number of variables which include changes in routing, packet loss, cross-traffic, and human activity. Generalisability would require a full-scale experiment involving the ISP networks that are operational (Masek et al., 2021).

Lastly, swarms are prone to extreme noise even though the CSI is high. Some of the adversarial behaviours, like coordinated false signalling, can temporarily cause consensus disruption, especially when the nodes are compromised or not well placed in the network topology.

FUTURE WORK

There are some directions that have potential research opportunities. A natural extension then is implementation into real-world ISP/5G network environments, where the behaviour of the system under production-level conditions can be evaluated in more detail. A good opportunity is also the integration of HIVE-SIGHT with software-defined networking (SDN) infrastructure, as SDN controllers might be used to offer quick re-routing and filtering installations on-demand (Ranjan, 2021).

The other urgent line of action is to work on increasing the resistance of the framework to botnets that are produced by AI. As attackers grow more and more likely to automate botnet behaviour using generative models, defence systems will need adversarially robust training and feature sets (Niu et al., 2022). These improvements should be added gradually since HIVE-SIGHT is designed in a modular form.

The quantum-resistant cryptographic primitives might also be utilized to strengthen the Global Anomaly Ledger so that the integrity can be ensured over time as threats are changing (Reza et al., 2022). Lastly, a simulation environment focused on the modelling of multi-agent swarm behaviour in cyber defence would be able to shed more light into the mechanism of emergent behaviours and the topology of swarms.

CONCLUSION

The work proposed the HIVE-SIGHT, a decentralised and biological design of global DDoS protection. The system provides some form of predictive capability and flexibility that is often unattainable by centralised systems by spreading intelligence around a swarm of collaborative nodes. The framework was able to predict attacks long before they reach their peak, co-ordinate node behaviour by providing emergent consensus, and cut response time by a significant factor through extensive evaluation on a multi-ISP dataset.

Technologies based on collaborative intelligence and self-organisation may also be necessary in order to increase the complexity of network infrastructures and the complexity of attack methods used by attackers. HIVE-SIGHT presents one example of how these principles may be translated into practice, and a way to get to cyber defence systems that are not simply reactive but are truly anticipatory.

References

1. Ahmed, M., Khan, S., & Lee, J. (2022). Network anomaly detection using deep learning. Computer Networks.
2. Al-Qatf, M., Lasheng, Y., Al-Haj, A., & Al-Feilat, A. (2021). Deep learning–based autoencoder for intrusion detection. Future Internet.
3. Atheeq, C. & Ali, Layak & Altaf, C. & Mohammed, Aleem. (2025). Mitigating man-in-the-middle attack in UAV network using authentication mechanism based on chaotic maps.
4. Bae, S., Kim, H., & Park, J. (2021). Spectral feature extraction for security analytics. Pattern Recognition.
5. Atheeq, C. & C, Altaf & Mohammad, Mohammad & Mohammed, Aleem. (2023). An Effective Mechanism to Mitigate Packet Dropping Attack from MANETs using Chaotic Map based Authentication Technique. Recent Patents on Engineering
6. Chen, Y., Li, L., & Zhao, H. (2021). Applications of ant colony and swarm computing in cyber defence. Expert Systems with Applications.
7. Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2019). Internet of Things security and evolving botnet architectures. ACM Computing Surveys.
8. C. Atheeq, & Mohammad, Mohammad & Mohammed, Aleem. (2022). Prior Bush Fire Identification Mechanism based on Machine Learning Algorithms. International Journal of Artificial Intelligence & Applications. 13. 67-77.

9. Dua, A. (2021). Swarm-based optimisation for secure computing. Applied Soft Computing.
10. Han, M., Zhou, Z., & Li, X. (2020). High-speed DDoS detection in backbone networks. Computers & Electrical Engineering.
11. Hoque, S., Ahmed, F., & Miah, M. (2022). Collaborative techniques for large-scale DDoS mitigation. Computer Communications.
12. Hussain, F., et al. (2022). Survey of IoT-driven botnets and attack vectors. Information Systems.
13. Jalili, M. (2023). A contemporary review of DDoS attack taxonomies. Computer Networks.
14. Kaur, P., Singh, R., & Sharma, V. (2021). Decentralised models for cyber defence. Computers & Security.
15. Kim, Y., Park, D., & Cho, J. (2021). Deep convolutional models for DDoS detection. IEEE Transactions on Network and Service Management.
16. Kim, J., Lee, S., & Hong, M. (2023). Predictive intelligence for cyber-threat forecasting. Digital Communications and Networks.
17. Kwon, D., Park, Y., & Lee, K. (2023). Federated learning for distributed ISP security. IEEE Internet of Things Journal.
18. Li, J., Xu, T., & Chan, K. (2022). Early-stage DDoS prediction using behavioural signals. Pattern Recognition Letters.
19. Liu, S., et al. (2022). Reinforcement learning applications in network traffic shaping. Computer Communications.
20. Luo, X., Chen, J., & Feng, Y. (2021). Spectral analysis for intrusion and anomaly detection. IEEE Access.
21. Masek, J., et al. (2021). Modern behaviours of large-scale DDoS attacks. Journal of Network and Computer Applications.
22. Mohammad, Mohammad & Mohammed, Aleem. (2023). Smart Cities Implementation: Australian Bushfire Disaster Detection System Using IoT Innovation.
23. Mohammed, Aleem & Mohammad, Mohammad. (2023). How AI Algorithms Are Being Used in Applications. 10.1007/978-981-19-8669-7_5.
24. Mitchell, R., & Chen, I. (2020). Bio-inspired approaches for distributed network modelling. Biosystems.
25. Mohammad MOHAMMAD, Aleem MOHAMMED, Ghassan KBAR and Amer YACOUB, “The Role of ICT in Educational Settings Leadership in learning and Teaching with ICT: The Case of Qatar.,” Proceedings of the 37th International Business Information Management Association (IBIMA), ISBN: 978-0-9998551-6-4, 30-31 May 2021, Cordoba, Spain, p 7961-7971.
26. Mohammad, Mohammad; MOHAMMED, Aleem; C, Atheeq (2022). Pre- and post-assessment of COVID-19 in academic learning: A state of the art assessment. CQUniversity.
27. Nguyen, T., et al. (2021). Edge-based distributed AI for real-time cybersecurity. IEEE Internet of Things Journal.
28. Niu, G., Tao, X., & Zheng, H. (2022). AI-enhanced botnet evolution and emerging threats. Expert Systems with Applications.
29. Park, J., et al. (2019). Entropy-based anomaly detection in high-speed networks. Computer Communications.
30. Patel, D., Zhang, Y., & Lin, P. (2023). Distributed ledgers for anomaly detection. Future Generation Computer Systems.
31. Ranjan, A. (2021). Software-defined networking architectures for adaptive mitigation. Journal of Network and Systems Management.
32. Reza, F., Chowdhury, S., & Islam, M. (2022). Blockchain-assisted approaches for DDoS defence. Information Processing & Management.
33. Saxena, A. (2020). Machine learning techniques for botnet behaviour prediction. Journal of Information Security and Applications.
34. Sharmeen, S., et al. (2020). LSTM-based modelling of network traffic anomalies. Future Generation Computer Systems.
35. Sharma, R., Singh, K., & Mehta, A. (2023). Modelling global cyber-threat intelligence. Computers &

ISSN: 2178-7727

Security.
36. Singh, H., & Joshi, A. (2020). Reinforcement learning for network intrusion defence. Neurocomputing.
37. Xu, L., & Wang, H. (2022). Autonomous cyber defence through distributed learning. Ad Hoc Networks.
38. Wang, G., Lee, T., & Wong, R. (2022). Architecture-level approaches for global DDoS defence. IEEE Transactions on Networking.
39. Yu, S., et al. (2020). Big-data analytics for DDoS identification. Information Sciences.
40. Zhang, Y., Li, C., & Zhao, X. (2020). Foundations of swarm intelligence in distributed computing. Applied Soft Computing.