Received: 2 June 2025 | Revised: 2 September 2025 | Accepted: 13 September 2025 | Published online: 16 October 2025

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2026, Vol. 5(1) 133–142
DOI: 10.47852/bonviewJCCE52026303

BON VIEW PUBLISHING

A Study on Zeek IDS Effectiveness for Cybersecurity in Agricultural IoT Networks

Samsul Huda[1,*], Muhammad Bisri Musthafa[2], S. M. Shamim[2], and Yasuyuki Nogami[2]

[1] *Interdisciplinary Education and Research Field, Okayama University, Japan*
[2] *Graduate School of Environmental, Life, Natural Science and Technology, Okayama University, Japan*

Abstract: As agriculture moves toward Agriculture 4.0, which uses Internet of Things (IoT) devices to collect data in real time and monitor things from a distance, these networks are becoming increasingly vulnerable to cyberattacks. A common method used to protect against these kinds of threats is the use of intrusion detection systems (IDS). However, the agricultural environment is often changing and has limited resources, which makes cybersecurity challenging. Several available IDS tools are not designed to work properly in places with few resources, intermittent access, and unpredictable network conditions. This paper investigates the performance of Zeek, an open-source IDS, in identifying potential threats in agricultural IoT networks. We performed both offline and real-time experiments: offline analysis used pcap files from the Stratosphere Laboratory dataset, and real-time evaluation involved simulated live attack scenarios, focusing on unauthorized access attempts and distributed denial-of-service (DDoS) attacks. Zeek's performance was assessed based on CPU and memory utilization, as well as quality of service (QoS) metrics. From the experimental results, we found that Zeek was quite effective in protecting agricultural IoT networks against typical threats. Memory usage remained stable around 5% during offline analysis and under 20% during active attacks. However, CPU usage was more volatile, peaking at 120% during DDoS events. In terms of QoS, the system maintained a good throughput (1,375 kbits/s) with minimal packet loss (0.000186%). Among the attack types that we tested, brute force attacks, which represent attempts at unauthorized access, had the strongest effect on network performance, increasing delay to 2.159 ms and jitter to 0.793 ms. It seems clear that a heavier traffic load during such attacks can interfere with QoS. On the basis of our observation, we recommend practical deployment strategies for agricultural IoT systems that take these limitations into consideration, aiming to keep networks both secure and efficient under pressure.

Keywords: agricultural IoT, Zeek IDS, intrusion detection systems, open-source security tools, Agriculture 4.0, cybersecurity, Raspberry Pi

1. Introduction

The agricultural sector is undergoing a major transformation with the integration of Internet of Things (IoT) technologies, a movement commonly referred to as Agriculture 4.0 [1–3]. In support of this trend, we previously developed an IoT-based application that is designed to monitor plant agricultural systems [4]. This application helps farmers track and manage critical environmental conditions that are essential for optimal plant growth. Our approach contributes to the United Nations Sustainable Development Goal 2 (SDG 2), which seeks to end hunger and promote sustainable agricultural practices [5].

The security problems affecting agricultural IoT networks are shown in Figure 1. These systems are vulnerable from unauthorized users who attempt to compromise critical agricultural infrastructure. They can also interfere in wireless connections between environmental sensors and central monitoring hubs using distributed denial of service (DDoS). The risks in agriculture are especially high because sensor data operate as the direct control mechanism for essential farm operations, including automated irrigation and pesticide application and other vital farm tasks [6–8].

Agricultural IoT networks pose a different security challenge because of their unique operational features. They are frequently working in isolated settings with inadequate IT infrastructure, poor network connectivity, and limited technical capabilities [9, 10]. These networks typically consist of devices with limited resources, such as limited processing power and memory, making traditional security solutions impractical [11].

The compromise of these systems could have serious consequences, including the following [12]:

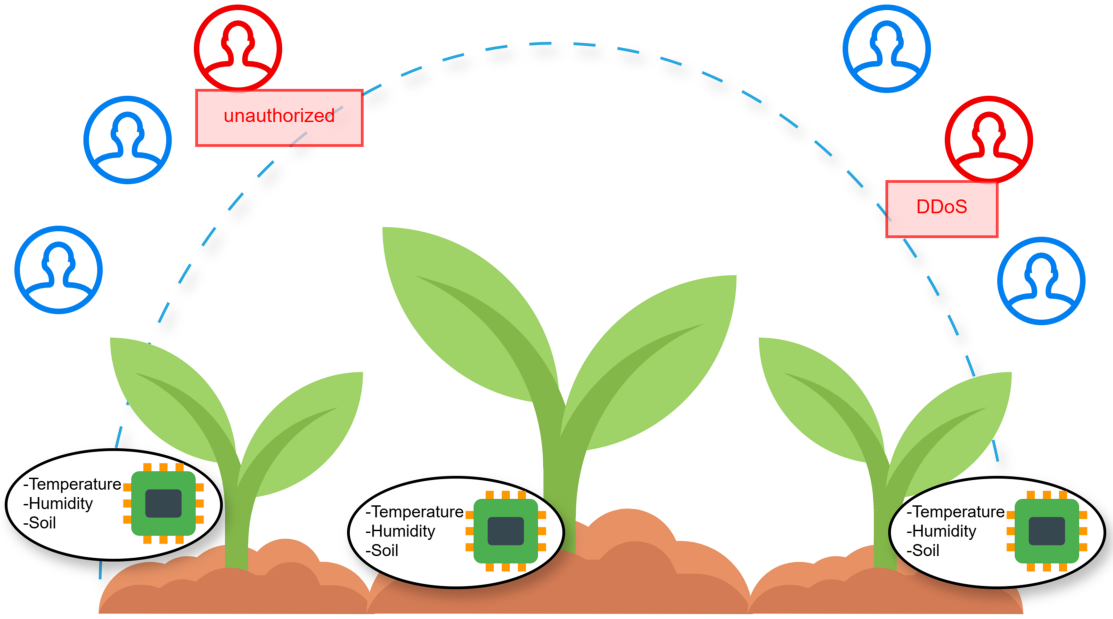
1) Disruption of critical farming operations
2) Unauthorized access to sensitive agricultural data
3) Tampering with automated irrigation or fertilizer systems
4) Economic losses due to reduced yields or damaged equipment.

Theft of agricultural data, including yield predictions, soil composition analyses, and operational patterns, could give competitors unfair advantages or enable market manipulation [13, 14]. Most existing work focuses on securing data transmission, transaction, or authentication protocols [15–18], with limited emphasis on real-time threat detection and system performance in the agricultural case.

Intrusion detection systems (IDS) are promising solutions for monitoring and protecting agricultural IoT networks [19]. IDS functions to detect unauthorized access, unusual activity, and other potential security threats. The protection of sensitive agricultural data through IDS maintains the reliability of smart farming operations. Among the numerous IDS options available, Zeek stands out as a powerful, flexible, and open-source network analysis tool that can be customized to fit specific environments [20]. The effectiveness of Zeek has been proven in conventional IT environments. However, its performance and

*Corresponding author: Samsul Huda, Interdisciplinary Education and Research Field, Okayama University, Japan. Email: shuda@okayama-u.ac.jp

Figure 1
Agricultural IoT network security challenges



suitability for resource-constrained agricultural IoT networks remain largely unexplored.

The research gap is essential because agricultural IoT networks need to maintain strong security monitoring and respect the operational constraints of agricultural activities. The primary difficulty lies in developing intrusion detection methods that do not overwhelm IoT gateway computational capabilities or disrupt essential field operations.

The performance of Zeek IDS in an agricultural IoT environment was thoroughly evaluated in this study. In particular, we focused on Zeek's ability to detect and stop unauthorized access attempts and DDoS attacks while running within the confines of the resource/bandwidth constraints characteristic of many agricultural environments. In particular, in agriculture, these risks can be very real since an interruption in the field or unauthorized access to control systems may affect crop management and livestock monitoring.

In this study, we set up Zeek in a virtual environment to create a safe and controlled environment. For the offline part, we used pcap files from the Stratosphere Laboratory dataset, which included a mix of normal and malicious traffic. To test active attack, we simulated live attack scenarios using different open-source network tools. By analyzing both types of traffic offline and in real time, we obtained clearer results regarding Zeek's performance and resource requirements in various situations. These results help in informing how network security monitoring can be effectively implemented in an agricultural environment.

Our research contributions include the following:

1) A comprehensive performance evaluation of Zeek IDS under resource-constrained agricultural IoT networks, considering both offline analysis and real-time operation.
2) Quantitative analysis of resource utilization (CPU and memory) patterns during normal operations and attack scenarios.
3) Assessment of the impacts of quality of service (QoS) on agricultural network communications, including throughput, packet loss, delay, and jitter.
4) Practical deployment recommendations for implementing Zeek in resource-constrained farming environments.

The remainder of this paper is organized as follows. Section 2 reviews related work on IoT security in agricultural settings, compares open-source IDS solutions, and offers a comparative analysis of current approaches. Section 3 explains experimental details such as the setup of the test environment and performance metrics. Section 4 describes our experimental results from offline and real-time analyses, key performance, and security efficacy. Section 5 provides the discussion of the results and deployment recommendations for agricultural setups. Finally, Section 6 summarizes the paper and outlines future work.

2. Review of IoT Security and Intrusion Detection in Agriculture

The following section reviews multiple relevant studies on IoT security in agriculture and open-source IDS and evaluates existing works against our current experiment.

2.1. IoT security in agriculture

Security concerns in agricultural IoT are very different from those in other domains. Vangala et al. [21] pointed out that agricultural IoT has some unique (aspects-related field) challenges, outdoor deployment, and wide coverage. Weathering is another key challenge. According to Mahlous [22], environmental factors such as humidity, temperature variations, and dust might deteriorate the mechanical properties of the components of security supply chains for farming equipment. Therefore, it is important to work on hardening robust hardware that can survive hard circumstances in the field.

This vulnerability exposes IoT agricultural farms to multiple potential cyber threats. In their study, Elijah et al. [23] highlighted common threats such as unauthorized access, data tampering, and DoS attacks. They emphasized the importance of strong security to secure these systems. Meanwhile, Ali et al. [24] pointed out that one major challenge is the resource-constrained nature of farming devices because several security software tools demand more speed and computational power than these devices can accommodate.

To prevent such attacks, the protection of agricultural IoT systems against unauthorized access requires robust authentication protocols. Fathy and Ali [25] created an IoT-based smart irrigation system that implemented secure communication protocols together with the expeditious cipher algorithm. Although the system protected MQTT protocol communications according to their approach, it lacked essential advanced intrusion detection capabilities to identify and respond to emerging cyber threats effectively.

Similarly, Chaganti et al. [26] proposed a secure IoT-based agricultural monitoring system architecture that employs blockchain technology. They used blockchain's decentralized and immutable features to protect data integrity and prevent unauthorized access. Their main focus was on data security, but they did not address the detection and mitigation of network-based threats that are crucial for complete system protection.

The need for IDS becomes essential because of these limitations to improve agricultural IoT network cybersecurity. IDS operates as a network traffic monitoring system that detects abnormal patterns that could signal unauthorized access or DDoS attacks.

2.2. Intrusion detection system for IoT

IDS has an essential role at IoT deployment level, detecting cyber threats. There are a number of open-source IDS tools, such as Zeek, Snort, and Suricata. These tools allow real-time network traffic monitoring and detection of anomalies and suspicious activities. The integration of IDS into IoT environments enhances security visibility and enables proactive threat mitigation. A comparison of some major open-source IDS according to features essential for agricultural IoT deployments is provided in Table 1 [27–29].

1) Detection approach: Zeek is not a signature-based tool like Snort and Suricata that relies mostly on known threats defined by regular expression patterns. Zeek offers more comprehensive behavioral-based capabilities. The agricultural environment requires systems that can detect abnormal behavior because the known threats in this setting are not well established.
2) Resource requirements: The implementation of agricultural IoT requires resource-constrained devices to perform monitoring and control operations. Snort generally demonstrated lower resource utilization compared to both Zeek and Suricata. Zeek handles memory better than the other two tools. Therefore, it is best suited for environments where memory is more limited than processing power.

Abdulganiyu et al. [30] performed a detailed study of some IDS methods and emphasized the benefits of Zeek IDS, such as its ability to perform deep packet inspection, support for custom scripting, and extensibility. They noted that Zeek IDS is well suited for detecting network-based attacks and can be customized to specific network environments. Aligned with their observations, Nguyen et al. [31] utilized Zeek IDS to detect and mitigate IoT-based anomaly packets in smart home environments with machine learning models. They demonstrated the effectiveness of Zeek IDS in identifying anomalous malicious traffic patterns and implementing countermeasures to protect IoT devices.

Our study fills an important gap in existing literature by offering an empirical performance study of Zeek in the context of agricultural IoT. We measure both resources (CPU and memory) and QoS variables to provide a detailed understanding of network behavior during cyber-attacks targeting agricultural systems. Our study includes both offline analysis using public pcap datasets and real-time evaluation in a representative deployment, highlighting performance differences between these two approaches. We also investigate the operational difficulties of implementing Zeek in limited-resource networks while providing specific guidelines to optimize security performance.

Table 1
Comparative analysis of major open-source IDS

Components	Zeek	Snort	Suricata
Detection	Behavior analysis and protocol validation	Signature-based	Signature-based
Analytics	Strong (statistical anomaly detection)	Limited	Moderate
Customization	High (Zeek scripting)	Moderate (rule)	Moderate (rule)
Performance	Moderate (CPU intensive)	Good	Poor
Community support	Academic and research focus	Large enterprise	Growing enterprise
Agricultural suitability	High	Moderate	Moderate

3. Experimental Methodology

Our study contributes to filling the gap in IDS research by focusing on agricultural IoT networks that are often characterized by spotty internet, constrained level of computing power, and a set of different devices. What makes our work unique is that we focus on how well open-access Zeek IDS performs in these kinds of environments, which are not usually covered in existing research. This section presents our comprehensive experimental approach for evaluating Zeek IDS effectiveness in agricultural IoT networks. We begin by describing the experimental setup, followed by the test scenarios designed to assess both offline and real-time performance. We then outline the performance metrics used to measure resource utilization and network impact.

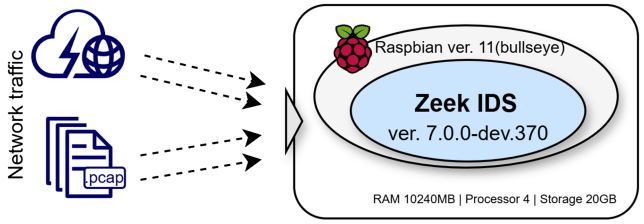
3.1. Experimental setup

Our experiments were conducted in both controlled and isolated conditions. To accomplish this, a virtual setup of Zeek replicated Raspberry Pi system operations through its deployment. VirtualBox on host PC enabled us to create a dependable framework that produced consistent results.[1] This configuration allowed us to compare offline and real time. This virtualized approach eliminated the need for physical Raspberry Pi hardware while maintaining similar performance characteristics. As a result, through this approach, we achieved exact control of experimental conditions, which enhanced the reliability of our performance comparison results.

Figure 2 presents the experimental design implemented in our virtual environment. The setup was designed to support the analysis of both live network traffic and precaptured traffic from pcap files. Zeek IDS was deployed in a virtualized instance of Raspbian 11 (Bullseye), running on a configuration of 4 processor cores, 10,240 MB of RAM,

[1] https://www.virtualbox.org/

Figure 2
Experimental design within virtual environment



and 20 GB of storage. To ensure compatibility and customization, we compiled Zeek version 7 from source. Required dependencies, including libpcap and CMake, were installed and configured prior to deployment.

To avoid any inference by the host system, we set up a virtual machine with a dedicated network interface. This isolation enabled us to separate Zeek traffic analysis from anything else and had a clean, controlled testing environment. With that environment, we can simulate different attack scenarios and network conditions that are typical of agricultural IoT systems, ensuring that the results were both reliable and reproducible. In the next section, we will talk about the various threats that we examined, such as efforts to get in without permission and DDoS attacks.

3.2. Agricultural IoT security scenarios

In this subsection, we present the detailed test scenarios and threat types that we simulated in the virtualized agricultural IoT environment.

3.2.1. Unauthorized access attempts

This scenario simulated unauthorized access attempts targeting the agricultural IoT network. These attempts were designed to test the effectiveness of Zeek IDS in detecting and preventing intrusions. These attacks target sensitive agricultural systems such as central databases containing crop yield data or management platforms controlling farm operations. We focused on the detection of unauthorized access behaviors such as the following:

1) Unusual login patterns: In agricultural IoT, farmers and operators typically log in at specific times to check crops and adjust other operations. Here, we monitored for multiple failed login attempts because these could indicate brute force. Moreover, logins that happened at strange times were noted because they could mean that someone who should not have access was trying to get into important systems.
2) Suspicious IP addresses: Agricultural IoT generally has certain devices and users that access from trusted locations to control operations. During our analysis, we identified login attempts originating from unfamiliar or blacklisted IP addresses. This kind of activity is often a red flag, indicating potential external attackers attempting to infiltrate farm management systems or gain access to sensitive data.
3) Unusual data access requests: In farming operations, access to sensitive data such as crop yield, irrigation schedules, and soil health is typically restricted to specific users or systems. We focused on identifying patterns where large volumes of this critical data were accessed by unauthorized users or from untrusted sources. This kind of activity could mean that someone was trying to steal or change important farming information.

The rules in Zeek for detecting unauthorized access attempts are shown in Figure 3, which focuses on monitoring unusual login patterns, suspicious IP addresses, and atypical data access requests. These detection methods were specifically designed to protect sensitive agricultural systems, ensuring that critical operations, such as irrigation, fertilization, and pest control, remain secure. We monitored these common access patterns to prevent potential data breaches and operational disruptions in agricultural IoT networks.

3.2.2. Distributed denial of service (DDoS) attacks

In addition to unauthorized access, we simulated DDoS attacks targeting agricultural IoT systems to evaluate their resilience under resource-constrained conditions. Our DDoS detection approach focused on identifying sudden spikes in traffic volume and connection attempts, which are typical signs of DDoS attacks that could disrupt agricultural IoT operations. Specifically, we monitored unusual patterns of volumetric attacks, including the following:

1) UDP floods: In agricultural IoT networks, devices such as sensors and controllers rely on consistent communication. We monitored for high traffic volume from UDP packets sent to random ports, which could overwhelm network resources and interfere with the real-time transmission of agricultural data, such as soil moisture levels or weather updates.
2) ICMP floods: Large-scale ping requests (ICMP packets) can flood network devices, consuming bandwidth and causing delays in the communication between IoT devices on farms. This type of attack could disrupt time-sensitive operations such as irrigation or pest control systems that rely on immediate responses.
3) SYN floods: A high volume of SYN requests aimed at initiating TCP connections can overload farm management systems and prevent legitimate users from accessing critical platforms, such as those used for crop management or environmental monitoring.

The rules for detecting these DDoS attack patterns are shown in Figure 4. These simulations were designed to test the ability of Zeek IDS to detect and mitigate threats that could disrupt the operations of agricultural IoT networks. We evaluated Zeek's effectiveness in maintaining the continuity of critical agricultural operations, such as crop monitoring, irrigation, and pest control, even during network stress caused by DDoS attacks by detecting traffic anomalies in real time.

3.3. Performance evaluation

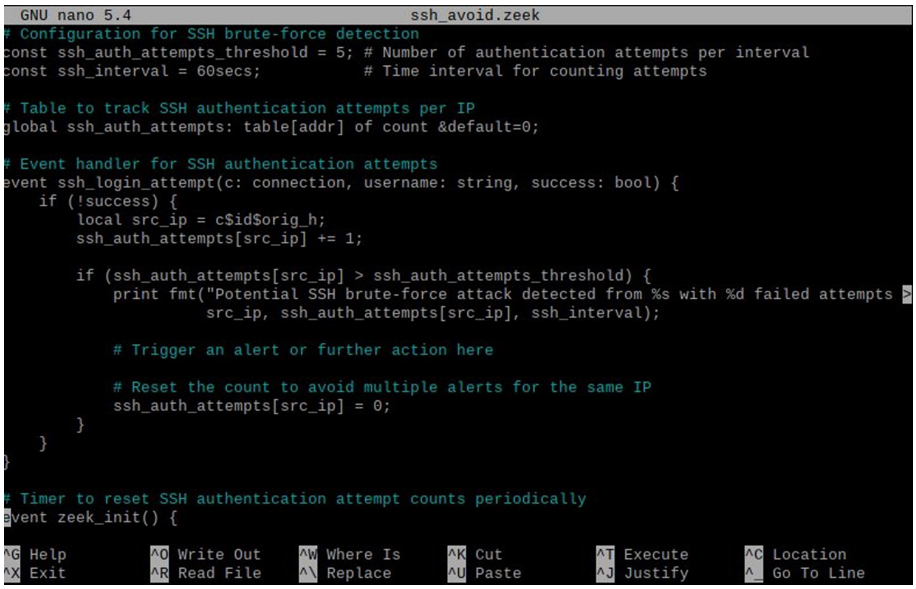
We tested Zeek's behavior in both offline and real-time environments to understand its behavior under different operational conditions. We measured CPU usage, memory consumption, and service quality in both conditions. The same metrics allowed us to directly compare how each mode affected Zeek's efficiency and resource usage.

3.3.1. Offline analysis

The offline analysis used pcap files from the Stratosphere Laboratory dataset. The dataset contains harmless agricultural IoT transmissions together with different attack scenarios. We selected this dataset because it demonstrates network behavior while providing valuable labeled traffic samples that match agricultural IoT requirements.

In the offline scenario, we measured the performance of Zeek by processing pcap files under two different traffic conditions: mixed traffic, which included both normal and malicious activities, and normal traffic, which represented typical agricultural IoT communications. The use of Zeek to analyze these pcap files allowed us to examine network traffic in depth without the constraints of real-time pressure. This way allowed for multi-instance dynamic traffic pattern analysis,

Figure 3
Zeek rule for detecting unauthorized access



detection rule testing in a controlled environment, and detailed analysis of individual events.

During the evaluation, we observed CPU and memory consumption to study Zeek resource consumption under different traffic conditions. We also collected QoS metrics to evaluate performance under normal and attack conditions. These measurements provided us a great deal of information about how effectively and consistently Zeek processes a range of network events when not connected to the internet.

3.3.2. Real-time analysis

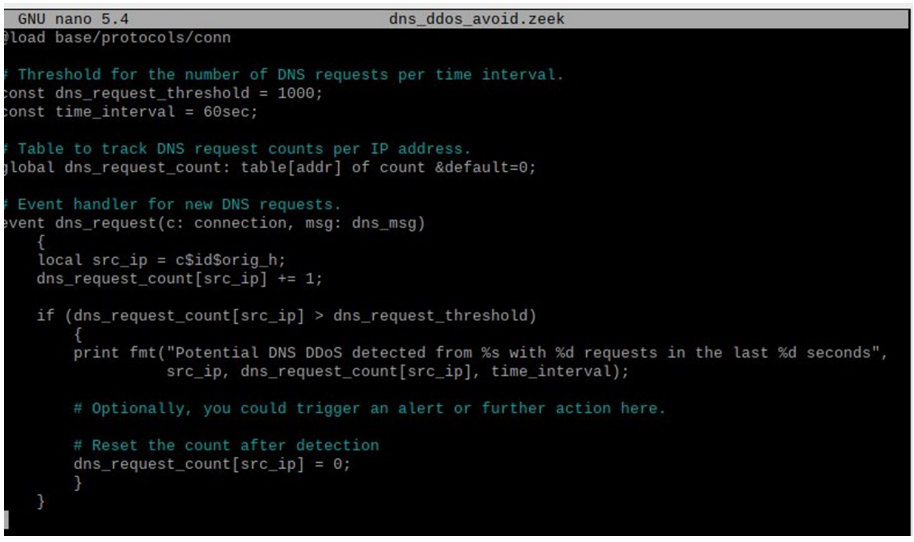
The real-time analysis evaluated Zeek's performance in live network monitoring across three representative scenarios typical of agricultural IoT environments:

1) Normal agricultural IoT traffic: We recorded baseline performance during normal sensor operations that involved regular data exchanges, command and control messages, and standard operational activities.
2) DDoS attack scenario: We evaluated Zeek's performance in detecting and responding to DDoS attacks that target essential IoT infrastructure.
3) Unauthorized access scenario: We evaluated Zeek's ability to identify brute-force authentication attempts that targeted gateway devices.

To replicate the unpredictable and dynamic nature of real-world agricultural networks, a live traffic generation setup was implemented using open-source tools that are capable of producing both legitimate and malicious traffic. Specifically:

1) Hydra was used to simulate unauthorized access through brute-force attacks on SSH logins.

Figure 4
Zeek rule for detecting DDoS attacks



2) Hping3 produced high-volume traffic that simulated different DDoS attack types, including SYN floods, UDP floods, and ICMP floods.

The real-time analysis setup is shown in Figure 5. Three virtual machines were deployed: one running Zeek IDS on Raspbian and two Kali Linux VMs. One Kali VM generates normal, legitimate traffic, and the other simulates attacks as a malicious user. This configuration allows us to create realistic mixed traffic scenarios that combine benign and malicious activities that closely mirror real agricultural IoT network conditions.

We utilized Zeekctl to control Zeek, which allowed us to keep an eye on network traffic all the time and in real time. This configuration allowed us to test how successfully Zeek found and reacted to different kinds of traffic. We kept an eye on CPU and memory use during the tests to see how Zeek used resources when the network was busy. These measurements together give us a clear image of how well and how stable Zeek is in real-time situations.

4. Experimental Results

In this section, we present the experimental results from our evaluation of Zeek IDS in the agricultural IoT environment. This evaluation focuses on resource usage and QoS to determine how Zeek performs under different traffic conditions.

4.1. Offline analysis

4.1.1. CPU and memory usage

Figure 6 and Figure 7 illustrate the pattern of Zeek resource utilization when processing two different offline scenarios: normal agricultural IoT traffic and mixed traffic containing both normal and malicious activities. The initial 40 s of normal traffic shows CPU utilization that ranges between 50% and 120%. After Zeek identifies typical patterns of agricultural IoT communications, the CPU utilization becomes stable. The adaptation period shows how Zeek improves its processing efficiency by learning normal traffic characteristics.

The mixed traffic scenario shows that Zeek requires an initial adaptation period of approximately 20 s before CPU usage stabilizes at 100%–120%. We observed significant periodic drops in CPU usage at the 20 and 90 s marks, which are associated with transitions between different traffic patterns in the dataset. This variability indicates Zeek's dynamic resource allocation based on traffic complexity, with a higher CPU demand during periods containing signs of an attack.

Memory usage stayed at a steady 5% level throughout the entire process in both scenarios. The stable memory usage proves that Zeek can effectively process big historical datasets without memory waste, which makes it appropriate for farming environments with restricted resources and memory.

Figure 5
Real-time analysis setup

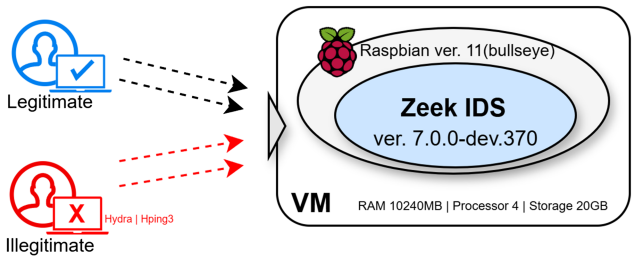
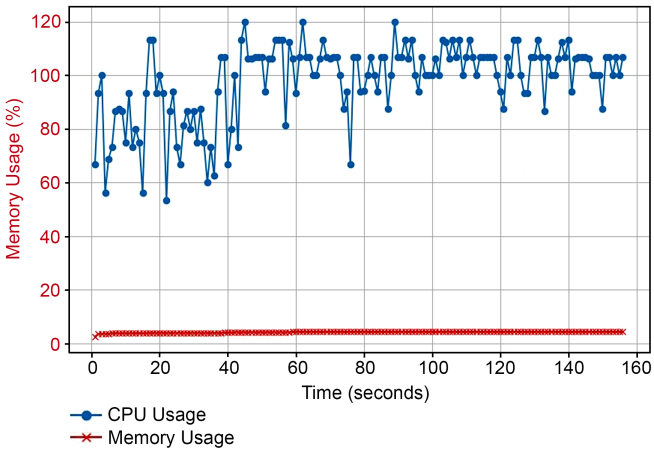


Figure 6
CPU and memory usage during offline analysis of normal traffic



4.1.2. QoS metrics

The QoS measures of our offline analysis are shown in Table 2. During this study, we processed more than 1.4 million packets from a dataset that was 852 MB in size. The throughput was 30.26 kbits/s. Although the packet loss rate of 0.5753% is modest, it still shows that there are some problems with processing vast amounts of historical data. In addition, the delay of 156.24 ms and jitter of 296.32 ms are much higher than what is needed for real-time performance. This means that offline analysis has different performance trade-offs than live monitoring.

The results indicate that Zeek can handle historical agricultural IoT data for security analysis, but performance characteristics need to be considered. The evaluation of old farm data in resource-limited farming environments requires careful consideration of these factors to prevent bottlenecks during review or analysis.

4.2. Real-time analysis

4.2.1. CPU and memory usage

Figure 8, Figure 9, and Figure 10 show the dynamic resource utilization behaviors of Zeek in three real-time cases, including a normal agricultural IoT operation scenario, an unauthorized access detection scenario, and a DDoS attack response scenario.

Figure 7
CPU and memory usage during offline analysis of mixed traffic

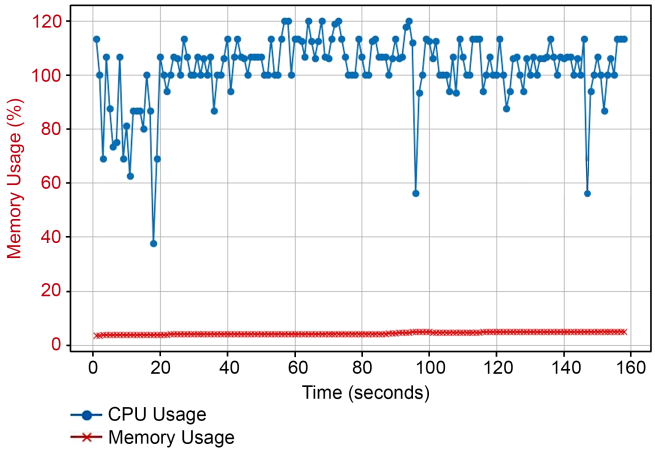


Table 2
QoS results from offline analysis

Metric	Value
Total packets	1,437,980
Capture time	224,83 s
Throughput	30.26 kbits/s
Packet loss	0.5753 %
Delay	156.24 ms
Jitter	296.32 ms

Under normal traffic, Zeek consumes very little resources, remaining below 10% of both CPU and memory while it is being monitored. This low resource utilization demonstrates how well Zeek handles everyday farming operations such as sensor data delivery and network management. Its consistent and low utilization also shows that Zeek is a good choice for gateway devices that do not have a lot of resources, which is often the case in agricultural settings.

When unauthorized access attempts occur, Zeek shows a distinct CPU usage pattern, with spikes of 12%–14%, followed by quiet periods of low activity. These spikes happen each time an authentication attempt is made because Zeek processes and checks the credentials against its detection rules. Throughout this, memory usage stays steady at 6%, suggesting that Zeek handles the authentication process efficiently without overloading memory.

Our results of DDoS attack show how Zeek uses its resources the most. In 30–40 s, when the attack detection algorithms are on, CPU usage goes up to 120%. After the first detection, CPU usage goes down, but it stays high at 10%-–20% because Zeek processes the attack traffic that is still going on. After an attack is detected, memory consumption goes up from 5% to 20% and stays there. This is because of the storage needs for logging data and status information connected to the attack. Memory utilization stays higher even after the attack finishes, unlike CPU usage. This suggests that Zeek maintains an expanded state or cache so that it can quickly respond to any follow-up attacks.

4.2.2. QoS metrics

Table 3 presents the QoS metrics for all real-time scenarios, making it easy to compare how network performance holds up under varying operational conditions.

The DDoS attack scenario shows how Zeek can handle high throughput (1,375 kbits/s) and process more than one million packets

Figure 8
CPU and memory consumption during real-time analysis of normal traffic

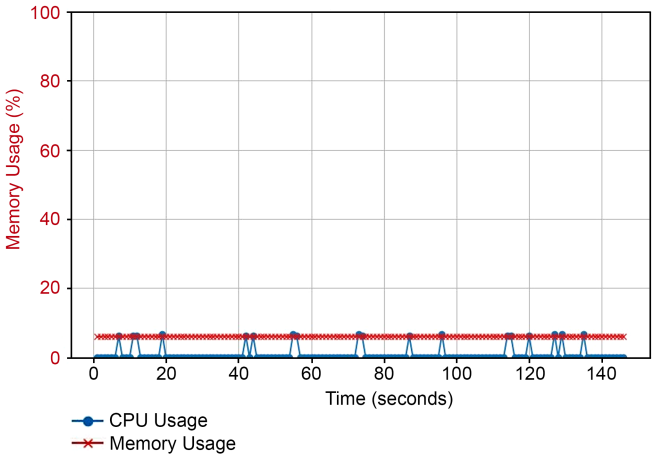
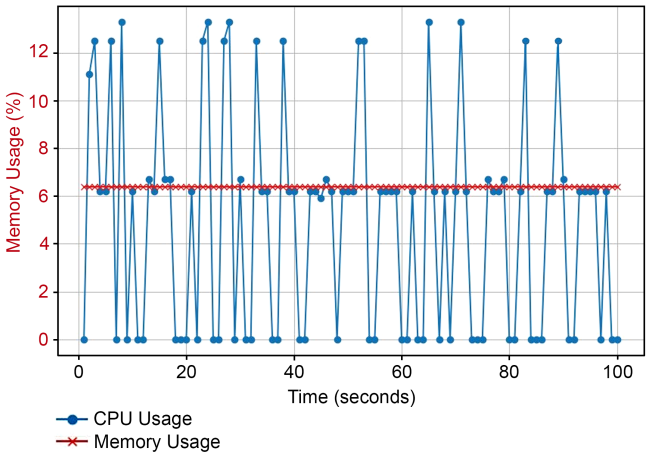


Figure 9
CPU and memory usage during real-time analysis of unauthorized access attempts



with only 0.000186% packet loss. The performance of Zeek is very important for agricultural IoT networks because it ensures data integrity during attacks, which is necessary for agricultural operations to continue. The minimal latency (0.043 ms) and zero jitter show that legitimate agricultural traffic continues to flow efficiently even under attack conditions.

Real-time data show that unauthorized access attempts cause the highest disruption across the network, with delay reaching 2.159 ms and jitter at 0.793 ms. The increased latency is due to the computational overhead of authentication processing and security rule evaluation during login attempts. However, zero packet loss demonstrates Zeek's reliability in maintaining complete traffic visibility during security incidents, ensuring no critical agricultural data are lost.

The system maintains optimal performance through normal traffic monitoring, which shows moderate throughput (246.5 kbits/s), zero packet loss, reasonable delay (1.806 ms), and minimal jitter (0.007 ms) during extended periods. The measured metrics demonstrate that Zeek operates effectively for agricultural IoT monitoring while preserving fundamental network operations.

Such different real-time QoS profiles can serve as special detection signatures, based on which the Zeek IDS rules could be defined to detect some attack attacks in the agricultural IoT scenarios.

Figure 10
CPU and memory usage during real-time analysis of DDoS attacks

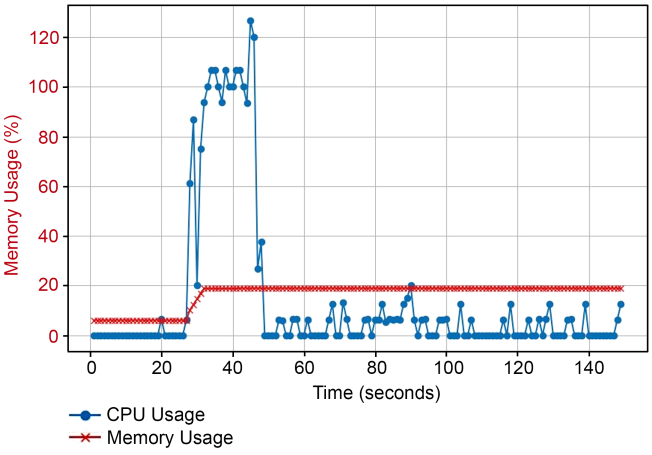


Table 3
QoS results from real-time analysis

Scenario	Total packets	Throughput (kbits/s)	Packet loss (%)	Delay (ms)	Jitter (ms)
DDoS attack	1,072,554	1,375.0	0.000186	0.043	0
Brute force	9,049	401.6	0	2.159	0.793
Normal traffic	45,034	246.5	0	1.806	0.007

5. Discussion and Deployment Recommendations

5.1. Discussion

Our performance analysis illustrates that the behaviour of Zeek differs considerably between offline and real-time monitoring. Real-time monitoring performs better in terms of QoS, with much lower delays. Nevertheless, offline analysis can handle large scale dataset. Therefore, it is more appropriate for in-depth historical analysis.

Data show that real-time monitoring adjusts dynamically to traffic, whereas offline processing maintains stable resource consumption. In both cases, Zeek uses memory efficiently, with usage staying below 20%, which is ideal for devices with limited memory in agriculture.

The CPU usage remains stable until DDoS attacks occur, which cause spikes reaching 120% and potentially overload gateway devices with lower processing power. The discussion in Section 2.2 confirms that CPU usage stands as a major obstacle for Zeek operation in limited-resource settings. The high CPU usage of Zeek during attacks does not result in significant packet loss, which remains crucial for agricultural systems that need uninterrupted sensor data.

The virtualized Pi in VirtualBox provides an effective approximation of physical Raspberry Pi performance, but it does not fully capture the thermal and power constraints encountered in real-world deployments. The devices deployed in outdoor or rural agricultural environments may be exposed to elevated temperatures and limited power availability, which could potentially lead to thermal throttling or degraded performance. These factors could influence the effectiveness of the IDS, especially in real-time scenarios. Future work should include experiments on physical Raspberry Pi hardware under controlled thermal and power conditions to validate and extend the results presented.

5.2. Deployment recommendations for agricultural environments

On the basis of our experimental findings, we present recommendations for the deployment of Zeek IDS in agricultural IoT networks:

1) **Hierarchical deployment.** The recommended deployment model configuration for Zeek resource management should use hierarchical deployment to distribute network resources effectively. The main analysis will be performed by advanced gateway devices that will utilize all capabilities of Zeek. The edge devices will operate with basic filtering and anomaly detection through lightweight agents. The system will experience reduced processing demands. The monitoring station will receive suspicious traffic from the edge for detailed analysis. The system distributes computational tasks similarly to the work by HaddadPajouh et al. [32] while maintaining complete security coverage throughout the system.

   The system can be expanded by adding more gateway devices in areas with high activity or complex operations if the farm is large or has many different areas. Edge devices can be placed in key locations to manage smaller sections of the network. These devices help in sorting data and finding unusual patterns, and their functions can be customized based on the size and diversity of the environment. This keeps the system running smoothly, even as the network expands.
2) **Offline online hybrid analysis.** The system should operate in two modes where light monitoring runs continuously in real time. The system performs detailed traffic analysis of recorded data during periods when resource usage remains low outside peak hours. The proposed method enables the resolution of performance issues that occur when analyzing big datasets offline.
3) **Resource-aware scheduling.** The monitoring intensity of Zeek can be reduced during critical agricultural operations such as coordinated irrigation or harvesting by adopting a dynamic scheduling mechanism when maximum network performance is required. This strategy can help in ensuring that security monitoring does not interfere with time-sensitive agricultural activities.
4) **Resource optimization.** The system should filter packets based on agricultural protocols to reduce data processing needs while maintaining detection performance. The sampling rate needs to be adjusted according to operational needs by increasing monitoring during critical times such as irrigation periods.
5) **Selective script activation.** The Zeek system should be configured to run only the essential detection scripts that align with the farm's threat model while focusing on unauthorized access detection during regular operations. The system can automatically activate additional detection features when a suspicious activity occurs to optimize resource usage during normal operations.

6. Conclusion

In this paper, we analyze the effectiveness of Zeek IDS in securing IoT-based agricultural networks against unauthorized access and DDoS attacks in both offline and real time. Our experimental results show that Zeek can still work with such elements, but the performance is not very satisfactory for both CPU computation and network bandwidth in the attack stage. In contrast, memory stays consistent, and it is processing power not memory that prevents deployment of Zeek in AG networks. The clear performance gains on network level (throughput, packet loss, latency, and jitter) prove the point that secure deployment planning should be considered for an especially resource-constrained edge device. Because of the high CPU utilization that such attacks reveal, we provide deployment suggestions that provide strong security while accounting for the limited resources found in agricultural IoT. Future work will investigate machine learning methods in improving Zeek's detection abilities, especially in identifying sophisticated attack behaviors in agricultural fields.

Acknowledgement

This work is conducted as part of the projects in the Green Innovation Center (GIC), Okayama University, Japan, and we acknowledge their continued support and facilitation.

Funding Support

This work is supported by the budget of Green Innovation Center (GIC) projects at Okayama University, Japan.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

The data that support the findings of this study are openly available in the Stratosphere Laboratory at https://www.stratosphereips.org/datasets-overview, in GitHub at https://github.com/zeek/zeek, https://github.com/vanhauser-thc/thc-hydra, and https://github.com/antirez/hping.

Author Contribution Statement

Samsul Huda: Conceptualization, Formal analysis, Writing – original draft, Writing – review & editing, Visualization, Supervision, Project administration. **Muhammad Bisri Musthafa:** Conceptualization, Methodology, Software, Validation, Investigation, Resources, Data curation, Writing – review & editing, Visualization. **S. M. Shamim:** Conceptualization, Methodology, Software, Validation, Investigation, Resources, Data curation, Writing – review & editing, Visualization. **Yasuyuki Nogami:** Supervision, Funding acquisition.

References

[1] Lezoche, M., Hernandez, J. E., Alemany Díaz, M. D. M. E., Panetto, H., & Kacprzyk, J. (2020). Agri-food 4.0: A survey of the supply chains and technologies for the future agriculture. *Computers in Industry*, *117*, 103187. https://doi.org/10.1016/j.compind.2020.103187

[2] Latino, M. E., Corallo, A., Menegoli, M., & Nuzzo, B. (2023). Agriculture 4.0 as enabler of sustainable agri-food: A proposed taxonomy. *IEEE Transactions on Engineering Management*, *70*(10), 3678–3696. https://doi.org/10.1109/TEM.2021.3101548

[3] Abbasi, R., Martinez, P., & Ahmad, R. (2022). The digitization of agricultural industry — A systematic literature review on agriculture 4.0. *Smart Agricultural Technology*, *2*, 100042. https://doi.org/10.1016/j.atech.2022.100042

[4] Huda, S., Nogami, Y., Akada, T., Rahayu, M., Hossain, M. B., Musthafa, M. B., ..., & Jie, Y. (2023). A proposal of IoT application for plant monitoring system with AWS cloud service. In *2023 International Conference on Smart Applications, Communications and Networking*, 1–5. https://doi.org/10.1109/SmartNets58706.2023.10215620

[5] United Nations. (n.d.). *United Nations sustainable development goals (SDGs)*. https://unric.org/en/united-nations-sustainable-development-goals/

[6] Yang, X., Shu, L., Chen, J., Ferrag, M. A., Wu, J., Nurellari, E., & Huang, K. (2021). A survey on smart agriculture: Development modes, technologies, and security and privacy challenges. *IEEE/CAA Journal of Automatica Sinica*, *8*(2), 273–302. https://doi.org/10.1109/JAS.2020.1003536

[7] Padhy, S., Alowaidi, M., Dash, S., Alshehri, M., Malla, P. P., Routray, S., & Alhumyani, H. (2023). AgriSecure: A fog computing-based security framework for Agriculture 4.0 via blockchain. *Processes*, *11*(3), 757. https://doi.org/10.3390/pr11030757

[8] Irshad, A., Aljaedi, A., Bassfar, Z., Jamal, S. S., Daud, A., Chaudhry, S. A., & Das, A. K. (2024). SAWPS: Secure access control for wearable plant sensors: Reinforcing Agriculture 4.0. *IEEE Sensors Journal*, *24*(18), 29293–29304. https://doi.org/10.1109/JSEN.2024.3402538

[9] Liu, Y., Ma, X., Shu, L., Hancke, G. P., & Abu-Mahfouz, A. M. (2021). From Industry 4.0 to Agriculture 4.0: Current status, enabling technologies, and research challenges. *IEEE Transactions on Industrial Informatics*, *17*(6), 4322–4334. https://doi.org/10.1109/TII.2020.3003910

[10] Sinha, B. B., & Dhanalakshmi, R. (2022). Recent advancements and challenges of Internet of Things in smart agriculture: A survey. *Future Generation Computer Systems*, *126*, 169–184. https://doi.org/10.1016/j.future.2021.08.006

[11] Gupta, M., Abdelsalam, M., Khorsandroo, S., & Mittal, S. (2020). Security and privacy in smart farming: Challenges and opportunities. *IEEE Access*, *8*, 34564–34584. https://doi.org/10.1109/ACCESS.2020.2975142

[12] Xu, J., Gu, B., & Tian, G. (2022). Review of agricultural IoT technology. *Artificial Intelligence in Agriculture*, *6*, 10–22. https://doi.org/10.1016/j.aiia.2022.01.001

[13] Hazrati, M., Dara, R., & Kaur, J. (2022). On-farm data security: Practical recommendations for securing farm data. *Frontiers in Sustainable Food Systems*, *6*, 884187. https://doi.org/10.3389/fsufs.2022.884187

[14] Kang, Y. (2023). Development of large-scale farming based on explainable machine learning for a sustainable rural economy: The case of cyber risk analysis to prevent costly data breaches. *Applied Artificial Intelligence*, *37*(1), e2223862. https://doi.org/10.1080/08839514.2023.2223862

[15] Ramprasath, J., Nishath, M. M., Varunkarthick, S., & Gowtham, G. (2023). Secured data transaction for agriculture harvesting using blockchain technology. In *2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies,* 1–4. https://doi.org/10.1109/ViTECoN58111.2023.10156998

[16] Taji, K., & Ghanimi, F. (2024). Enhancing security and privacy in smart agriculture: A novel homomorphic signcryption system. *Results in Engineering*, *22*, 102310. https://doi.org/10.1016/j.rineng.2024.102310

[17] Huda, S., Nogami, Y., Rahayu, M., Akada, T., Hossain, M. B., Musthafa, M. B., ..., & Jie, Y. (2024). IoT-enabled plant monitoring system with power optimization and secure authentication. *Computers, Materials and Continua*, *81*(2), 3165–3187. https://doi.org/10.32604/cmc.2024.058144

[18] Rahul, R., Venkatesan, R., & Jebaseeli, T. J. (2024). Smart farming with improved security using Ascon encryption and authentication. In *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things*, 365–373. https://doi.org/10.1109/IDCIoT59759.2024.10467361

[19] Huda, S., Musthafa, M. B., & Nogami, Y. (2024). Zeek intrusion detection on Raspberry Pi for IoT-based agriculture monitoring systems: Preliminary investigation. In *2024 IEEE International Symposium on Consumer Technology*, 372–377. https://doi.org/10.1109/ISCT62336.2024.10791229

[20] Mudgal, A., & Bhatia, S. (2022). Experimental-based comparative study on open-source network intrusion detection system. *International Journal of Internet Technology and Secured Transactions*, *12*(5), 462–475. https://doi.org/10.1504/IJITST.2022.125781

[21] Vangala, A., Das, A. K., Chamola, V., Korotaev, V., & Rodrigues, J. J. P. C. (2023). Security in IoT-enabled smart agriculture: Architecture, security solutions and challenges.

Cluster Computing, *26*(2), 879–902. https://doi.org/10.1007/s10586-022-03566-7

[22] Mahlous, A. R. (2024). Security analysis in smart agriculture: Insights from a cyber-physical system application. *Computers, Materials & Continua*, *79*(3), 4781–4803. https://doi.org/10.32604/cmc.2024.050821

[23] Elijah, O., Abdul Rahman, T., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet of Things Journal*, *5*(5), 3758–3773. https://doi.org/10.1109/JIOT.2018.2844296

[24] Ali, I. A., Bukhari, W. A., Adnan, M., Kashif, M. I., Danish, A., & Sikander, A. (2025). Security and privacy in IoT-based smart farming: A review. *Multimedia Tools and Applications*, *84*(16), 15971–16031. https://doi.org/10.1007/s11042-024-19653-3

[25] Fathy, C., & Ali, H. M. (2023). A secure IoT-based irrigation system for precision agriculture using the Expeditious Cipher. *Sensors*, *23*(4), 2091. https://doi.org/10.3390/s23042091

[26] Chaganti, R., Varadarajan, V., Gorantla, V. S., Gadekallu, T. R., & Ravi, V. (2022). Blockchain-based cloud-enabled security monitoring using Internet of Things in smart agriculture. *Future Internet*, *14*(9), 250. https://doi.org/10.3390/fi14090250

[27] Waleed, A., Jamali, A. F., & Masood, A. (2022). Which open-source IDS? Snort, Suricata or Zeek. *Computer Networks*, *213*, 109116. https://doi.org/10.1016/j.comnet.2022.109116

[28] Hu, Q., Yu, S.-Y., & Asghar, M. R. (2020). Analysing performance issues of open-source intrusion detection systems in high-speed networks. *Journal of Information Security and Applications*, *51*, 102426. https://doi.org/10.1016/j.jisa.2019.102426

[29] Boukebous, A. A. E., Fettache, M. I., Bendiab, G., & Shiaeles, S. (2023). A comparative analysis of Snort 3 and Suricata. In *2023 IEEE IAS Global Conference on Emerging Technologies*, 1–6. https://doi.org/10.1109/GlobConET56651.2023.10150141

[30] Abdulganiyu, O. H., Ait Tchakoucht, T., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). *International Journal of Information Security*, *22*(5), 1125–1162. https://doi.org/10.1007/s10207-023-00682-2

[31] Nguyen, T. B., Nguyen, D. D. K., Le Nguyen, B. N., & Le, T. (2023). A machine learning-based anomaly packets detection for smart home. In *Proceedings of the 12th International Symposium on Information and Communication Technology*, 816–823. https://doi.org/10.1145/3628797.3628930

[32] HaddadPajouh, H., Dehghantanha, A., Khayami, R., & Choo, K.-K. R. (2018). A deep recurrent neural network based approach for Internet of Things malware threat hunting. *Future Generation Computer Systems*, *85*, 88–96. https://doi.org/10.1016/j.future.2018.03.007

How to cite: Huda, S., Musthafa, M. B., Shamim, S. M., & Nogami, Y. (2026). A Study on Zeek IDS Effectiveness for Cybersecurity in Agricultural IoT Networks. *Journal of Computational and Cognitive Engineering*, *5*(1), 133–142. https://doi.org/10.47852/bonviewJCCE52026303