2026 IEEE 17th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) | 979-8-3195-2011-1/26/$31.00 ©2026 IEEE | DOI: 10.1109/UEMCON70256.2026.11775586

Cross-Domain Cyber Awareness Using Signal Intelligence Techniques

Srinivas Rahul Sapireddy
College of Engineering
Illinois State University
Normal, IL, USA
ssapire@ilstu.edu

Priyanka siddappa
Miner School of Computer & Information Sciences
University of Massachusetts Lowell
Lowell, MA, USA
Priyanka_Siddappa@student.uml.edu

Hemanth Bandi
Minnesota Supercomputing Institute
University of Minnesota Twin Cities
Twin Cities, MN, USA
bandi045@umn.edu

Sai Anirudh Godavarthi
School of Science and Engineering
University of Missouri-Kansas City
Kansas City, MO, USA
sg2bt@umkc.edu

***Abstract*—This paper introduces a lightweight and training-free cyber awareness framework that models network traffic as a time-varying signal and continuously monitors deviations in behavioral dynamics. Instead of relying on packet-level rules or supervised learning, the proposed approach extracts a baseline-referenced residual signal and analyzes it using interpretable signal-level features, including entropy, residual energy, envelope characteristics, and lag-1 temporal autocorrelation. These features are fused into a robust awareness score that emphasizes sustained behavioral deviation and groups threshold crossings into coherent awareness episodes rather than generating isolated alerts. The framework operates in a streaming manner at one-second resolution and does not require prior training or attack-specific knowledge. The framework is evaluated over a 25-minute experimental interval (1500 s), during which 1,471 sliding windows are analyzed using a 30 s window and 1 s step size. Although 538 windows (36.6%) exceed the awareness threshold, alert activity is consolidated into only three temporally coherent awareness episodes corresponding to scanning, denial-of-service, and data exfiltration behaviors. Feature-level analysis shows that scanning activity is primarily characterized by entropy deviation (peak $|z| = 23.28$), denial-of-service behavior exhibits extreme residual energy and envelope expansion (peak $|z| = 379.54$ and 39.79, respectively), and data exfiltration manifests as sustained entropy-driven structural deviation (peak $|z| = 33.27$). Awareness is triggered at attack onset in all evaluated scenarios due to the streaming, training-free design. These results demonstrate that distinct cyber behaviors map to distinct signal-level signatures, enabling interpretable, real-time cyber awareness that can complement existing intrusion detection systems, particularly in resource-constrained and edge environments.**

***Index Terms*—Cyber situational awareness, network traffic analysis, signal processing, anomaly detection, residual analysis, robust statistics.**

I. Introduction

The increasing scale and complexity of modern networked systems have introduced significant challenges for cyber defense mechanisms. Contemporary networks must contend with a wide range of threats, including reconnaissance activity, high-rate denial-of-service attacks, and low-and-slow data exfiltration. While traditional intrusion detection systems (IDS) are effective at identifying known attack patterns or classifying traffic into predefined categories, they often provide limited visibility into the evolving behavioral state of a network. This has motivated growing interest in cyber awareness approaches that emphasize continuous monitoring, behavioral interpretation, and sustained deviation rather than binary detection outcomes [1], [2].

Many existing cyber defense solutions rely on rule-based inspection, supervised machine learning, or deep neural networks to achieve high detection accuracy [3], [4]. Although these techniques have demonstrated success in controlled settings, they frequently require extensive labeled datasets, periodic retraining, and substantial computational resources. In addition, black-box learning models often lack interpretability, making it difficult for analysts to understand the underlying cause of an alert or distinguish among different forms of abnormal behavior. These limitations become particularly relevant in real-time, resource-constrained, and edge computing environments, where lightweight and explainable solutions are preferred [5].

In contrast, signal intelligence methodologies have long been used in fields such as communications, radar, and electronic warfare to detect and characterize dynamic phenomena by analyzing signal-level properties such as energy, entropy, and temporal structure [6], [7]. From this perspective, network traffic can be modeled as a time-varying signal whose statistical and temporal characteristics reflect underlying behavioral dynamics. Treating traffic in this manner enables the application of interpretable and computationally efficient signal analysis techniques without reliance on packet inspection or training-intensive learning models.

This paper adopts a signal-centric view of network traffic and proposes a lightweight, training-free cyber awareness framework for continuous behavioral monitoring. Network traffic volume is modeled as a time-domain signal, from which a baseline-referenced residual is extracted. Interpretable

979-8-3195-2011-1/26/$31.00 ©2026 IEEE

Authorized licensed use limited to: Milner Library Illinois State University. Downloaded on November 18,2026 at 17:19:39 UTC from IEEE Xplore. Restrictions apply.

signal-level features, including entropy, residual energy, envelope dynamics, and lag-1 temporal autocorrelation, are computed over sliding windows and fused into a robust awareness score. Rather than generating isolated alarms, threshold crossings are aggregated into temporally coherent awareness episodes, providing a higher-level representation of sustained abnormal behavior.

The proposed Cyber Awareness and Response System (CARS) framework is evaluated using both controlled synthetic scenarios and real network traffic from the UNSW-NB15 dataset. The expanded evaluation includes comparisons with raw-traffic robust thresholding, residual-energy-based detection, and Isolation Forest, together with precision, recall, F1-score, false-positive rate, AUROC, AUPRC, detection delay, sensitivity analysis, and computational measurements. Additional experiments examine benign workload changes and persistent low-and-slow behavior to assess false-alert characteristics and baseline adaptation. The results show that distinct traffic behaviors can produce interpretable signal-level signatures while also revealing sensitivity to changing network operating regimes. The framework is therefore positioned as a lightweight behavioral awareness layer that can complement existing intrusion detection systems rather than replace attack-specific classification mechanisms.

The main contributions of this paper are as follows:

- A lightweight, training-free framework that models network traffic as a time-varying signal using causal 30 s windows with a 1 s step for continuous cyber awareness.
- An interpretable awareness score based on entropy, residual energy, envelope dynamics, and lag-1 autocorrelation, with window-level alerts consolidated into coherent awareness episodes.
- Evaluation using controlled synthetic scenarios and real UNSW-NB15 traffic, including three anomaly-detection baselines. The framework requires approximately 0.65–0.80 ms per analysis window, while the long-duration stress test achieves an 8 s detection delay and 98.7–100% alert coverage across the evaluated attack intervals.

II. Related Work

Cyber awareness builds on situation-awareness theory, which emphasizes continuous perception, comprehension, and interpretation of system state in dynamic environments [1]. In cyber systems, this perspective extends beyond isolated alerts toward sustained understanding of evolving network behavior [2].

Most intrusion and anomaly detection research relies on statistical, machine-learning, or deep-learning methods [3], [4]. While effective in many settings, these approaches may require labeled data, retraining, and increased computational complexity, and can offer limited interpretability. Signal-processing methods provide an alternative by modeling network traffic as a time-varying signal and examining energy, entropy, correlation, and temporal structure [6]–[8]. Signal-centric approaches in related domains have also demonstrated the effectiveness of interpretable statistical features for characterizing temporal signal behavior [11], [14].

Network anomaly studies have also examined aggregate feature shifts without payload inspection [9], while benchmark datasets such as UNSW-NB15 support evaluation under mixed benign and malicious traffic [12]. Lightweight statistical thresholding and unsupervised methods such as Isolation Forest provide useful comparison baselines [13]. Building on these directions, the proposed framework combines signal-centric traffic modeling with interpretable indicators to support continuous cyber awareness without supervised attack-specific training.

III. Cyber Awareness via Signal-Centric Traffic Analysis

This section describes a signal-centric cyber awareness framework that treats aggregate network traffic as a time-varying signal and derives awareness from changes in signal structure. A key design goal is interpretability. Each computed indicator is linked to an intuitive traffic property such as burst magnitude, flow diversity, or temporal regularity. Another design goal is robustness under non-stationary conditions, since real networks exhibit workload shifts and transient congestion. For this reason, the framework uses robust normalization and episode formation to emphasize persistent behavioral regimes rather than isolated fluctuations.

Let $x[t]$ denote the measured traffic signal sampled at frequency F_s Hz, where $x[t]$ is the total number of bytes observed during the t-th second. A sliding window of duration T_w seconds is used, corresponding to $W = F_s T_w$ samples, and windows advance by a step size of T_s seconds. The analysis is causal: the window associated with time t contains only the current and preceding samples, $x[t-W+1], \ldots, x[t]$. The timestamp assigned to each feature vector is therefore the end of the analysis window, ensuring that awareness decisions do not depend on future traffic samples.

Direct thresholding on $x[t]$ is unreliable because baseline traffic can drift over time. A baseline model is therefore introduced to separate slowly varying trends from short-term deviations. The baseline $\hat{x}[t]$ is estimated using an exponential moving average. The smoothing coefficient is selected as

$$\alpha = \frac{2}{W+1}, \tag{1}$$

which ties the smoothing rate to the selected window size. The baseline recursion is

$$\hat{x}[t] = \alpha x[t] + (1-\alpha)\hat{x}[t-1]. \tag{2}$$

The residual signal is then defined as

$$r[t] = x[t] - \hat{x}[t]. \tag{3}$$

The residual emphasizes short-term deviations from expected traffic behavior and reduces dependence on absolute traffic scale.

Authorized licensed use limited to: Milner Library Illinois State University. Downloaded on November 18,2026 at 17:19:39 UTC from IEEE Xplore. Restrictions apply.

A smooth deviation magnitude is constructed using an envelope proxy. The absolute residual $|r[t]|$ is passed through the same exponential moving average operator,

$$e[t] = \mathrm{EMA}(|r[t]|). \tag{4}$$

The envelope $e[t]$ behaves as a smoothed amplitude estimate, increasing when deviations persist over multiple samples and remaining comparatively small during nominal variation.

Within a window spanning indices $t_0, \ldots, t_0 + W - 1$, several complementary features are computed. The mean envelope is

$$\mu_e = \frac{1}{W} \sum_{k=0}^{W-1} e[t_0 + k], \tag{5}$$

while the envelope standard deviation is

$$\sigma_e = \sqrt{\frac{1}{W} \sum_{k=0}^{W-1} \left(e[t_0 + k] - \mu_e\right)^2}. \tag{6}$$

The mean envelope captures sustained deviation magnitude, whereas its variation characterizes burstiness.

Signal intensity is measured using residual energy,

$$E_r = \frac{1}{W} \sum_{k=0}^{W-1} r^2[t_0 + k]. \tag{7}$$

This feature emphasizes large residual magnitudes and is particularly responsive to high-volume or strongly deviating traffic behavior.

Traffic diversity is quantified using Shannon entropy. Let c_i denote the number of observations associated with traffic entity i within the analysis window and let $C = \sum_i c_i$. The entropy is

$$H = -\sum_i \left(\frac{c_i}{C}\right) \log_2 \left(\frac{c_i}{C}\right). \tag{8}$$

Higher entropy indicates activity distributed across a larger set of entities, whereas lower entropy indicates more concentrated behavior. This provides structural information that cannot be obtained from traffic volume alone.

Temporal regularity is captured using the lag-1 autocorrelation of the residual. Let $\bar{r}$ denote the residual mean within the window. The lag-1 autocorrelation coefficient is

$$\rho_1 = \frac{\sum_{k=0}^{W-2} (r[t_0 + k] - \bar{r})(r[t_0 + k + 1] - \bar{r})}{\sqrt{\sum_{k=0}^{W-2} (r[t_0 + k] - \bar{r})^2} \sqrt{\sum_{k=0}^{W-2} (r[t_0 + k + 1] - \bar{r})^2}}. \tag{9}$$

This feature captures temporal structure and complements entropy, which characterizes distributional structure across traffic entities.

Because raw feature magnitudes are not directly comparable, each feature is robustly normalized relative to a benign reference distribution. For feature $f[j]$, the normalized value is

$$z_f[j] = \frac{f[j] - \mathrm{median}(\mathcal{R}_f)}{1.4826, \mathrm{MAD}(\mathcal{R}_f) + \epsilon}, \tag{10}$$

where $\mathcal{R}_f$ denotes the available benign reference values for feature f, and ϵ prevents numerical instability. The use of median and MAD provides robustness to heavy-tailed traffic distributions and isolated extreme values. In streaming operation, reference statistics are updated only from nominal observations. During an active awareness episode, reference adaptation is suspended to reduce the possibility that persistent anomalous behavior is gradually incorporated into the normal baseline.

An awareness score is formed by fusing normalized feature magnitudes into a single scalar indicator:

$$S[j] = 0.35|z_{\mu_e}[j]| + 0.25|z_H[j]| + 0.25|z_{E_r}[j]| + 0.15|z_{\rho_1}[j]|. \tag{11}$$

The weights emphasize sustained deviation magnitude and diversity changes while retaining information about intensity and temporal regularity. Absolute values are used because deviations in either direction may indicate behavioral change. The score is robustly normalized to obtain $z_S[j]$, and an alert is generated when

$$\mathcal{A}[j] = \begin{cases} 1, & z_S[j] \geq \tau, \\ 0, & \text{otherwise.} \end{cases} \tag{12}$$

where τ is the awareness threshold.

Single alert windows are not treated as independent incidents. Instead, temporally adjacent alerts are merged into awareness episodes representing sustained anomalous regimes. Let t_j denote the timestamp of the j-th alert window. Adjacent alerts are assigned to the same episode when

$$t_{j+1} \leq t_j + g, \tag{13}$$

where g is the maximum allowable gap. Each episode is summarized using its start time, end time, and duration, providing a compact representation of persistent behavioral change.

Event-level responsiveness is quantified using detection delay. For a known event beginning at t_{start}, the first awareness trigger occurring during or after event onset is

$$t_{\mathrm{trig}} = \min \left\{ t_j \mid \mathcal{A}[j] = 1 \wedge t_j \geq t_{\mathrm{start}} \right\}. \tag{14}$$

The detection delay is

$$D = t_{\mathrm{trig}} - t_{\mathrm{start}}. \tag{15}$$

Smaller values indicate faster awareness after event onset. Temporal consistency is additionally characterized by the overlap between an event interval $[a_s, a_e]$ and an awareness episode $[b_s, b_e]$,

$$\mathrm{Overlap} = \max \left\{ 0, \min(a_e, b_e) - \max(a_s, b_s) \right\}. \tag{16}$$

Overall, the framework converts aggregate traffic into an interpretable awareness signal by combining baseline separation, residual envelope analysis, traffic diversity, residual energy, temporal autocorrelation, and robust reference normalization. The resulting window-level alerts and episode-level summaries support evaluation of behavioral deviation, responsiveness, persistence, and computational efficiency without requiring supervised attack-specific model training.

Authorized licensed use limited to: Milner Library Illinois State University. Downloaded on November 18,2026 at 17:19:39 UTC from IEEE Xplore. Restrictions apply.

IV. Results and Discussion

This section presents experimental results obtained using the proposed Cyber Awareness and Response System (CARS). The evaluation examines awareness generation, temporal consistency, feature dominance, event-level responsiveness, and computational performance. Controlled synthetic experiments are first used to illustrate the behavior of the signal-centric framework, followed by real-network evaluation using UNSW-NB15 and comparisons with representative anomaly-detection baselines.

Synthetic traffic is used to emulate three representative cyber events: scanning, denial-of-service, and data exfiltration. The objective is to examine whether the proposed signal-intelligence framework can convert raw traffic into stable and interpretable awareness signals under controlled conditions.

A. Overall Awareness Monitoring Performance

Table I reports the overall monitoring statistics for the controlled synthetic experiment. The experiment spans 1500 s with a sampling rate of 1 Hz. A sliding window of 30 s and a step size of 1 s result in 1471 evaluated windows.

Using a robust z-score threshold of 3.5, 538 windows exceed the awareness threshold, corresponding to an alert rate of 36.57%. These alerts are not uniformly distributed across the experiment but are concentrated around the three injected behavioral events. Temporally adjacent alert windows are consolidated into three coherent awareness episodes with a combined duration of 538 s, corresponding to 35.87% of the experimental timeline.

These results show that episode formation converts numerous window-level threshold crossings into a smaller number of temporally coherent behavioral intervals. Rather than treating each anomalous window as an independent event, the framework preserves temporal context and provides a more compact representation of sustained network deviations.

B. Awareness Episode Formation

The merged awareness episodes obtained from the controlled synthetic experiment are listed in Table IV. Three distinct episodes are observed, with durations of 130 s, 130 s, and 278 s. Each episode corresponds to a sustained deviation from the baseline traffic behavior.

The first episode aligns with the scanning interval, while the second captures the high-intensity deviation associated with denial-of-service activity. The third episode persists for the longest duration and corresponds to the prolonged data-exfiltration interval.

Temporal merging reduces fragmentation among adjacent alert windows and converts repeated threshold crossings into coherent awareness intervals. This provides a more compact and interpretable representation of sustained behavioral changes for operational monitoring.

TABLE I: Overall Awareness Monitoring Summary

Metric	Value
Total duration (s)	1500
Sampling rate (Hz)	1
Window size (s)	30
Step size (s)	1
Windows evaluated	1471
Alert windows	538
Alert rate (%)	36.57
Awareness episodes	3
Episode duration (%)	35.87

TABLE II: Event-Level Detection Delay and Dominant Features

Event	Start (mm:ss)	Trigger (mm:ss)	Delay (s)	Dominant Feature
SCAN	06:00	06:00	0	Entropy
DDOS	12:00	12:00	0	Residual Energy
EXFIL	18:00	18:00	0	Entropy

TABLE III: Peak Feature Magnitudes During Controlled Cyber Events

Event	$\lvert z_{\text{entropy}}\rvert$	$\lvert z_{\text{env}}\rvert$	$\lvert z_{\text{energy}}\rvert$	$\lvert z_{\text{ac1}}\rvert$
SCAN	23.28	0.83	1.33	1.65
DDOS	7.65	39.79	379.54	3.76
EXFIL	33.27	7.43	19.32	2.84

C. Event-Level Awareness and Detection Delay

Event-level responsiveness in the controlled synthetic experiment is evaluated using detection delay, as shown in Table II. Three cyber events are considered: SCAN, DDOS, and EXFIL.

For all three events, the first awareness trigger occurs at the event onset, corresponding to a detection delay of 0 s under the controlled experimental conditions. The alert fraction within each event interval is 1.0, indicating continuous awareness coverage throughout the injected events. Dominant-feature analysis further illustrates the interpretability of the proposed framework. Entropy provides the strongest response during SCAN and EXFIL, whereas residual energy dominates during the high-intensity DDOS interval.

Table III reports the corresponding peak robust feature magnitudes. SCAN produces a strong entropy deviation with peak $|z| = 23.28$, while DDOS produces substantially larger residual-energy and envelope responses, reaching peak values of 379.54 and 39.79, respectively. EXFIL is characterized primarily by sustained entropy deviation, with a peak $|z|$ of 33.27. These differences illustrate how distinct behavioral regimes produce different signal-level signatures even when they are processed by the same awareness framework.

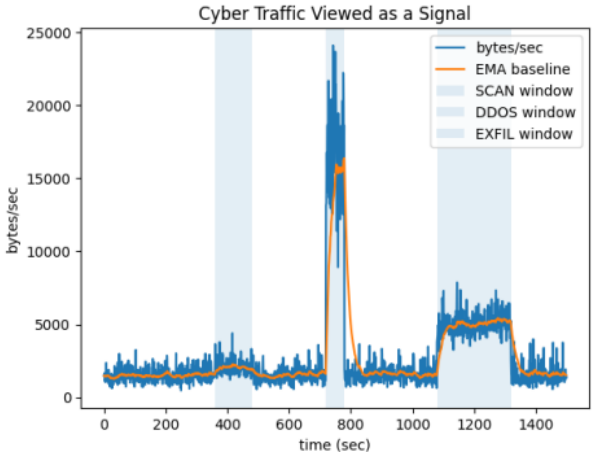
D. Feature Intensity and Peak Behavior

Peak feature magnitudes are summarized in Table III. The responses differ substantially across the three controlled cyber events, illustrating the distinct signal-level signatures captured by the framework.

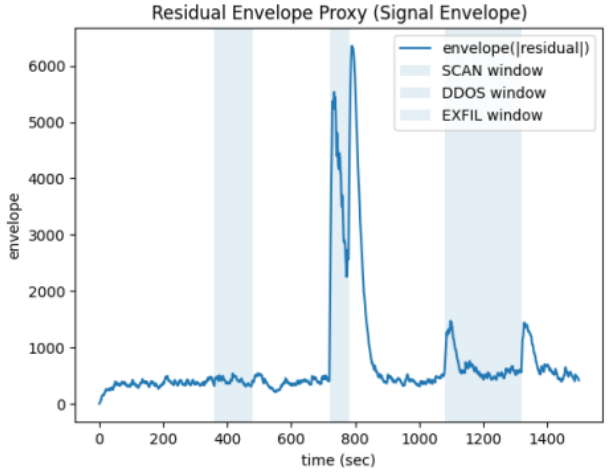
TABLE IV: Merged Awareness Episodes

Episode	Start (s)	End (s)	Duration (s)
1	356	485	130
2	706	835	130
3	1072	1349	278

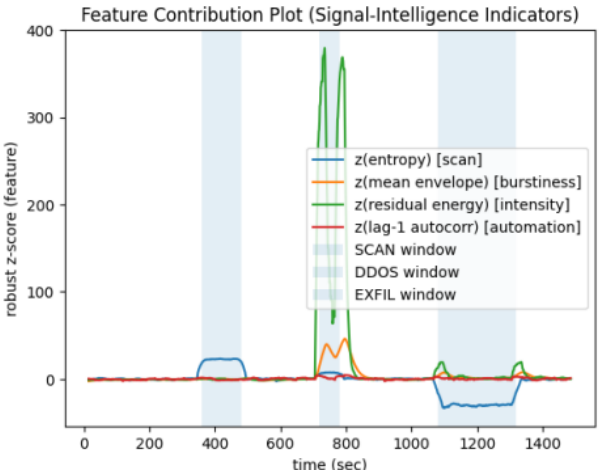
Authorized licensed use limited to: Milner Library Illinois State University. Downloaded on November 18,2026 at 17:19:39 UTC from IEEE Xplore. Restrictions apply.



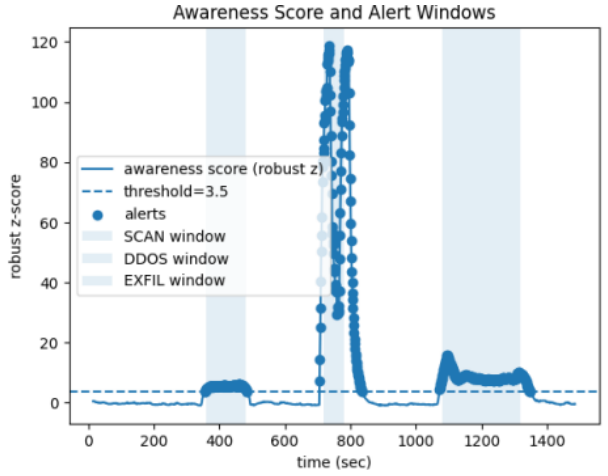
(a) Aggregate cyber traffic with EMA baseline.



(b) Residual envelope highlighting sustained deviations from baseline behavior.



(c) Robust feature contributions from entropy, envelope statistics, residual energy, and temporal autocorrelation.



(d) Composite awareness score with detected alert windows.

Fig. 1: Signal-centric awareness behavior for the controlled synthetic experiment. (a) Aggregate cyber traffic modeled as a time-varying signal with an exponential moving average baseline. (b) Residual envelope capturing sustained deviations from nominal behavior. (c) Robust z-score responses of entropy, envelope statistics, residual energy, and lag-1 autocorrelation. (d) Composite awareness score and alert windows corresponding to sustained behavioral deviations.

The DDOS event produces the strongest residual-energy response, reaching a peak $|z|$ of 379.54, together with a pronounced envelope deviation of 39.79. In contrast, entropy exhibits the strongest response during SCAN and EXFIL, with peak magnitudes of 23.28 and 33.27, respectively. These values indicate substantial departures in traffic-diversity structure relative to the reference behavior.

Lag-1 autocorrelation exhibits smaller normalized deviations than the dominant entropy and energy features across the three events. This suggests that temporal regularity provides complementary information rather than serving as the primary indicator for these particular scenarios.

Figure 2 illustrates the temporal alignment between the injected events and the corresponding awareness episodes. The controlled experiment shows that awareness is maintained across the event intervals while preserving the temporal structure of the detected behavioral changes.

E. Real-Network Evaluation and Robustness Analysis

To complement the controlled synthetic experiment, the proposed framework was evaluated using real network traffic from UNSW-NB15. A benign session was used as a shared reference, while four independent sessions containing benign and attack traffic were evaluated separately. CARS was compared with raw-traffic robust thresholding, residual-energy thresholding, and Isolation Forest. Table V reports macro-averaged performance across the four evaluation sessions.

Authorized licensed use limited to: Milner Library Illinois State University. Downloaded on November 18,2026 at 17:19:39 UTC from IEEE Xplore. Restrictions apply.

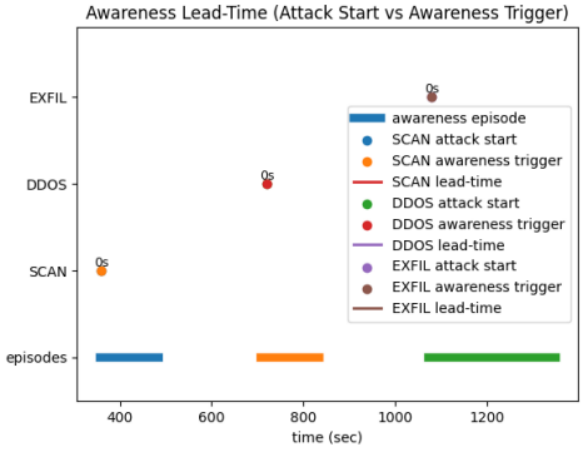


Fig. 2: Event onset, detection delay, and awareness-episode alignment in the controlled synthetic experiment.

The real-network results show substantial variation across traffic sessions, indicating sensitivity to differences between the benign reference and changing operating regimes. CARS therefore provides behavioral awareness rather than definitive attack classification. Nevertheless, the implementation remained computationally lightweight, requiring approximately 0.65–0.80 ms per analysis window, corresponding to roughly 1250–1550 processed windows per second.

Additional robustness experiments examined benign workload changes and persistent anomalous activity. Under ordinary benign traffic, CARS produced a 6.85% false-positive rate, while abrupt backup and flash-crowd conditions generated stronger awareness responses. In the long-duration low-and-slow experiment, the first awareness response occurred after 8 s, with alert coverage of 98.67% during the first 10 min and 100% during the middle and final 10 min intervals. These results demonstrate the value of preserving persistent awareness while also highlighting the need for improved multi-regime reference modeling.

V. Conclusion and Future Work

This paper presented a lightweight, training-free cyber awareness framework that models network traffic as a time-varying signal and combines entropy, residual energy, envelope dynamics, and lag-1 autocorrelation into an interpretable awareness score. Controlled synthetic experiments demonstrated distinct signal-level signatures for scanning, denial-of-service, and data-exfiltration behaviors, while temporal merging consolidated window-level alerts into coherent awareness episodes. Evaluation using UNSW-NB15 and representative anomaly-detection baselines further showed that the framework remains computationally lightweight, requiring approximately 0.65–0.80 ms per analysis window in attack-bearing sessions. In the long-duration low-and-slow experiment, awareness was triggered after 8 s and maintained 98.7–100% alert coverage after reference adaptation was suspended during active awareness episodes.

Real-network experiments also revealed sensitivity to changing network operating regimes and abrupt benign workload variations, indicating that awareness episodes should be interpreted as behavioral deviations rather than definitive attack classifications. Future work will investigate multi-regime reference modeling, context-aware discrimination between benign and malicious anomalies, multi-scale temporal analysis, and integration with automated response mechanisms for closed-loop cyber defense.

TABLE V: Macro-Average Performance on UNSW-NB15

Method	Prec.	Recall	F1	FPR	AUROC	AUPRC
CARS	0.540	0.130	0.180	0.514	0.342	0.628
Raw Traffic	0.479	0.030	0.054	0.262	0.192	0.619
Residual Energy	0.532	0.057	0.096	0.015	0.309	0.650
Isolation Forest	0.527	0.106	0.142	0.506	0.340	0.629

References

[1] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[2] V. Dutt, Y.-S. Ahn, and C. Gonzalez, "Cyber situation awareness: Modeling detection of cyber attacks with instance-based learning theory," *Human Factors*, vol. 55, no. 3, pp. 605–618, 2013.

[3] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[4] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

[5] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[6] R. G. Wiley, *Electronic Intelligence: The Interception of Radar Signals*. Norwood, MA, USA: Artech House, 2006.

[7] A. V. Oppenheim and R. W. Schafer, *Signals and Systems*. Upper Saddle River, NJ, USA: Prentice Hall, 1997.

[8] G. Nychis, V. Sekar, D. G. Andersen, H. Kim, and H. Zhang, "An empirical evaluation of entropy-based traffic anomaly detection," in *Proc. ACM Internet Measurement Conference (IMC)*, 2008.

[9] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing network-wide traffic anomalies," in *Proc. ACM SIGCOMM*, 2004.

[10] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, vol. 41, no. 3, Article 15, 2009.

[11] S. R. Sapireddy and M. Rahman, "Revisiting R: Statistical envelope analysis for lightweight RF modulation classification," in *Proc. 2025 1st Int. Conf. Radio Frequency Communication and Networks (RFCoN)*, pp. 1–6, 2025.

[12] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. 2015 Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, 2015.

[13] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *Proc. 2008 Eighth IEEE International Conference on Data Mining (ICDM)*, pp. 413–422, 2008.

[14] S. R. Sapireddy, G. Surekha, and H. Bandi, "Bin-Based R: Resource-Efficient RF Modulation Classification Using Envelope Statistics," in *Proc. SoutheastCon 2026*, Huntsville, AL, USA, 2026, pp. 1–6, doi: 10.1109/SoutheastCon63549.2026.11476603.

Authorized licensed use limited to: Milner Library Illinois State University. Downloaded on November 18,2026 at 17:19:39 UTC from IEEE Xplore. Restrictions apply.