УДК 004.89

Гуреев Р.Д.
студент
6 курс, факультет
«Прикладной математики, информатики и механики»
Воронежский государственный институт
Россия, г. Воронеж
Дудин В.С.
студент
6 курс, факультет
«Прикладной математики, информатики и механики»
Воронежский государственный институт
Россия, г. Воронеж
Игнатович Д.А.
студент
6 курс, факультет
«Прикладной математики, информатики и механики»
Воронежский государственный институт
Россия, г. Воронеж

ИНТЕЛЛЕКТУАЛЬНАЯ КЛАССИФИКАЦИЯ ПОТОКОВЫХ ДАННЫХ НЕИЗВЕСТНОЙ ПРИРОДЫ В ЗАДАЧАХ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Аннотация: *В современных системах мониторинга безопасности значительная часть телеметрии поступает в виде потоков с неопределённой семантикой и неполной разметкой: события SIEM, сетевые подключения, а также радиотехнические наблюдения. В статье предложен унифицированный подход к представлению «данных неизвестной природы» как потока объектов в пространстве признаков и показано, как выбор*

метода классификации определяется степенью разметки и ресурсными ограничениями. В качестве трёх репрезентативных направлений рассмотрены: supervised-классификация SIEM-событий методами машинного обучения, обнаружение и классификация DDoS-активности на основе агрегированных признаков входящих IP-подключений, а также статистическое распознавание модуляций по IQ-отсчетам SDR-приёмника. Показано, что сочетание интерпретируемых признаков, оконной агрегации и гибридной схемы "оценка риска → классификация" позволяет повышать устойчивость к изменчивости потоков и снижать нагрузку на аналитиков SOC.

Ключевые слова: *компьютерная безопасность, потоковые данные, данные неизвестной природы, классификация, аномалии, DDoS, SIEM, IQ-отсчет.*

INTELLIGENT CLASSIFICATION OF STREAM DATA OF UNKNOWN NATURE IN COMPUTER SECURITY PROBLEMS

Annotation: *In modern security monitoring systems, a large share of telemetry arrives as streams with uncertain semantics and incomplete labels: SIEM events, network connections, and radio observations. This paper proposes a unified view of "unknown-nature data" as a stream of objects embedded into a feature space and shows how the choice of a classification method depends on label availability and resource constraints. Three representative directions are considered: supervised ML classification of SIEM events, detection and classification of DDoS activity based on aggregated features of incoming IP connections, and statistical modulation recognition from SDR IQ samples. The results indicate that combining interpretable features, window-based aggregation, and a hybrid "risk scoring → classification" scheme improves robustness to stream variability and reduces SOC analyst workload..*

Key words: *cybersecurity, streaming data, unknown-nature data, classification, anomalies, DDoS, SIEM, IQ-counting.*

Введение

Современные инфраструктуры генерируют большие объёмы телеметрии: журналы аутентификации, сетевые соединения, действия пользователей, срабатывания средств защиты. В SIEM-контуре это приводит к необходимости централизованного сбора и анализа событий и последующей их приоритизации для SOC-аналитиков [1]. Однако существенная доля таких потоков не имеет однозначной априорной разметки и может меняться во времени, что характерно как для сетевых угроз (включая DDoS), так и для задач радиомониторинга, где тип сигнала/модуляции заранее неизвестен.

Практическая проблема проявляется одинаково в разных разделах: объект наблюдения поступает в поток, но в момент поступления неизвестно, является ли он нормой/атакой (для сетевых подключений и SIEM) либо какой тип сигнала присутствует в эфире (для SDR). Поэтому ключевой задачей становится построение интеллектуальной классификации потоковых данных неизвестной природы с применением методов supervised-обучения при наличии разметки, аномалий/кластеризации при её отсутствии, интерпретируемых правил при ограниченных ресурсах.

Данные неизвестной природы как унифицированный объект анализа

Под данными неизвестной природы в рамках статьи будем понимать поток объектов, для которых:

1. Отсутствует или неполна разметка классов;

2. Свойства распределения меняются во времени (concept drift);

3. Присутствуют шум, неполнота и неоднородность признаков.

Единая модель представления: каждый элемент потока (SIEM-событие, IP-подключение, окно IQ-отсчётов) приводится к вектору признаков $x(t) \in R^d$

и анализируется в рамках оконной агрегации (time window), что особенно важно для атак класса DDoS (эффект проявляется на агрегированном уровне) и для радиосигналов (признаки вычисляются по окну отсчётов).

Унифицированный конвейер обработки потоков

На рисунке 1 представлена обобщённая схема обработки потоковых данных неизвестной природы.

Рисунок 1. Унифицированный конвейер интеллектуальной классификации потоков

В SIEM-задачах поток событий преобразуется в управляемую очередь обработки (игнорировать/наблюдать/эскалировать), что снижает нагрузку triage и риск пропуска критики [1]. В SDR-задаче поток IQ-отсчётов делится на окна, вычисляются статистические признаки, после чего применяется логическая схема принятия решения [5].

Три направления применения унифицированного подхода

Supervised-классификация событий SIEM

В работе по классификации событий ИБ в SIEM-контуре рассмотрены признаки смешанной природы: контекстные поля, временные характеристики (hour, weekday) и индикаторы, извлечённые из поля command (например, признаки инструментов и техник).

Для оценки качества использованы Accuracy, F1_macro и F1_weighted, что корректно отражает проблему дисбаланса классов в SIEM-данных [2].

Таблица 1.

Сравнение моделей классификации событий ИБ

Модель/Метрики	**Accuracy**	**F1_macro**	**F1_weiggted**
Random Forest	1.00000	1.00000	1.00000
LinearSVC	0.99999	0.99976	0.99988
Logistic Regression	0.99701	0.96171	0.99741

Результаты показывают, что Random Forest и LinearSVC дают максимальное качество на исследуемом наборе, а также демонстрируют пригодность для потокового применения; при этом Random Forest выгоден по вычислительным затратам обучения/инференса [3].

Для Logistic Regression отмечены ложноположительные срабатывания (часть NORMAL отнесена к COMPLEX), что практически увеличивает нагрузку на SOC-аналитиков из-за ложных тревог [4].

Вывод для унифицированного конвейера: при наличии разметки и стабильных классов (пусть и дисбалансных) наиболее рациональна supervised-схема с контролем метрик по малым классам и ограничением ложноположительных эскалаций.

Классификация входящих IP-подключений и DDoS в условиях отсутствия разметки

Для входящих IP-подключений (и сетевого трафика в целом) типична ситуация, когда система не знает априори, относится ли объект к норме или атаке [10]. Поэтому в практическом конвейере основными становятся:

1. Обнаружение аномалий (точечные/групповые выбросы);

2. Оценка риска на основе отклонения от статистической нормы и динамики во времени;

3. Адаптация/онлайн-обучение, если распределение меняется;

4. Кластеризация (поиск устойчивых групп поведения).

Для DDoS-атак критично, что отдельное соединение может выглядеть легитимным, а опасность проявляется на агрегированном уровне [9]. Поэтому используются группы признаков:

1. Временные: частота запросов, интервалы, длительность сессий;
2. Объёмные: пакеты/байты;
3. Пространственные: распределение источников, энтропия по IP/географии;
4. Протокольные: флаги TCP, типы запросов HTTP и т.п.

Вывод для унифицированного конвейера: для DDoS практична гибридная схема “аномалия/риск → уточняющая классификация”, где первичный риск-скоринг формируется без разметки, а последующая классификация типа атаки может выполняться по выявленным кластерам (например, SYN/UDP/HTTP-паттерны).

Статистическая классификация радиосигналов по IQ-отсчётам SDR

В задаче радиомониторинга входной поток представляет собой IQ-отсчёты SDR-приёмника, а цель – определить тип модуляции в условиях ограниченных вычислительных ресурсов [6].

В рассмотренном подходе используется интерпретируемый набор статистических признаков, вычисляемых по окнам IQ-данных, и пороговый эвристический классификатор для AM/FM/SSB, а также классы “нет сигнала” и “неопределено”.

Ключевой набор признаков включает: моменты 2-го и 4-го порядка, коэффициент вариации амплитуды CV_A, спектральную плоскостность SF, частоту нулевых пересечений ZCR_A и оценку SNR [5].

Итоговый вектор признаков формируется по окну и подаётся на логическую функцию решения [7]. Отмечается, что такой метод

работоспособен близко к реальному времени и удобен для начального радиомониторинга, не требуя больших обучающих выборок [8].

Типовые решения:

1. При очень малых значениях моментов и низкой вариативности амплитуды и фазы ($CV_a \approx 0$, $SN\hat{R}$ мала) блок отсчётов относится к классу “нет сигнала”;

2. Если амплитуда почти постоянна (CV_a мала), а моменты фазовых производных указывают на выраженную частотную структуру (существенные $\sigma^2(\Delta\varphi)$ и $\kappa(\Delta\varphi)$), сигнал классифицируется как FM;

3. При высокой вариативности амплитуды (CV_a велика) и достаточной мощности сигнала ($SN\hat{R}$ выше порога) принимается решение в пользу AM;

4. При сочетании относительно невысокой вариативности амплитуды, специфических значений моментов по фазе и спектральной плоскостности сигнал относится к классу SSB;

5. При сильно выраженной негауссовости распределения амплитуды и её существенных колебаниях (аномальные значения κ_a, высокое ZCR_a) возможно эвристически выделить группу “QAM/PSK” как индикатор цифровой модуляции;

6. Во всех неоднозначных случаях используется класс “неопределено”.

Вывод для унифицированного конвейера: даже без обучения можно строить качественную первичную классификацию потоков неизвестной природы, если признаки отражают физическую/процессную природу наблюдения и обеспечивают интерпретируемость правил.

Сопоставление: признаки и методы

Ниже приведено практическое сопоставление трёх источников потоковых данных и оптимальных подходов.

Таблица 2.

Соответствие источников данных, признаков и подходов классификации

Источник потока	**Тип объекта**	**Примеры признаков**	**Приоритетный метод**
SIEM	Событие	Контекст, время, индикаторы команд	supervised ML (RF, SVM)
Сетевые подключения	IP/окно трафика	Частота, интервалы, объемы, энтропия, протокол	Аномалии, кластеризация
SDR	Окно IQ	Моменты, CVA, SF, ZCRA, SNR	Правила/эвристики, ML

Заключение

Показано, что три, на первый взгляд, разные области (классификация SIEM-событий, анализ сетевых подключений/DDoS и распознавание модуляции по SDR) объединяются общей постановкой: классификация потоковых данных неизвестной природы при изменчивости распределений и ограниченности априорной разметки. На материалах SIEM-задачи продемонстрирована эффективность supervised-классификаторов с контролем F1_macro и вычислительных затрат, где Random Forest и LinearSVC показывают максимальное качество, а ложноположительные срабатывания критичны с точки зрения нагрузки SOC.

Для задач радиомониторинга показана ценность интерпретируемых статистических признаков и пороговой логики, позволяющих решать задачу при малых ресурсах.

Для сетевого трафика и DDoS обоснована необходимость оконной агрегации и гибридной схемы “аномалия/риск → уточняющая классификация”.

Перспективы дальнейшей работы связаны с построением гибридных систем, где интерпретируемые признаки используются для первичной фильтрации/скоринга, а обучаемые модели – для уточнения класса и адаптации к дрейфу потоков.

Использованные источники:

1. Абденов А. Ж. Анализ, описание и оценка функциональных узлов SI EM-системы: учебное пособие / А. Ж. Абденов, В. А. Трушин, К. Сулайман. – Новосибирск: НГТУ, 2018. – 122 с.

2. Вьюгин В.В. Математические основы машинного обучения и прогно зирования. М.: МЦНМО, 2014. – 432 с

3. Buczak A., Guven E. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection // IEEE Communications Surveys & Tutorials. 2016. Vol. 18, No. 2. P. 1153–1176.

4. Кугаевских А. В. Классические методы машинного обучения: учебное пособие. – СПб.: Университет ИТМО, 2021. – 160 с.

5. Dobre O. A., Abdi A., Bar-Ness Y., Su W. Survey of automatic modulation classification techniques // IET Communications. 2007. Vol. 1, № 2. P. 137-156.

6. Nandi A. K., O’Connor D. Algorithm for automatic modulation recognition // IEE Proceedings – Radar, Sonar and Navigation. 1996. Vol. 143, № 5. P. 261-266.

7. Proakis J. G., Salehi M. Digital Communications. New York: McGraw-Hill, 2008.

8. Kay S. M. Fundamentals of Statistical Signal Processing. Upper Saddle River, NJ: Prentice Hall, 2001.

9. Mirkovic J., Reiher P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms // ACM SIGCOMM Computer Communication Review. – 2004. – Vol. 34, No. 2. – P. 39-53.

10. Zargar S. T., Joshi J., Tipper D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks // IEEE Communications Surveys & Tutorials. – 2013. – Vol. 15, No. 4. – P. 2046–2069.