УДК 004.056

Аюпова Айгуль Рафисовна, к.ф.-м.н. Нефтекамский Университет Науки и Технологии, г. Нефтекамск

Салихов Салават Зульфатович, студент, Нефтекамский Университет Науки и Технологии, г. Нефтекамск

ПРИМЕНЕНИЕ ГРАФОВЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ АНАЛИЗА ЦЕПОЧЕК АТАК В КОРПОРАТИВНЫХ СЕТЯХ.

Аннотация

В статье рассматривается проблема обнаружения многостадийных целевых атак (APT) в условиях неполноты журналов событий. Обосновывается неэффективность классических SIEM-решений и сигнатурных методов. Предлагается метод восстановления цепочек атак с использованием гетерогенных графовых нейронных сетей (GNN). Новизна подхода заключается в применении мета-путей совместно с реляционными GCN (R-GCN) для выявления латерального перемещения злоумышленника. Показано, что предложенный метод позволяет снизить время расследования инцидентов (MTTR) за счет автоматической кластеризации подграфов. Экспериментальная оценка на наборах данных DARPA TC и OpTC демонстрирует повышение полноты обнаружения латерального перемещения на 30% по сравнению с базовыми методами.

Annotation

The article addresses the problem of detecting multi-stage advanced persistent threats (APT) under incomplete event logs. The inefficiency of classical SIEM solutions and signature-based methods is substantiated. A method for reconstructing attack chains using heterogeneous graph neural networks (GNNs) is proposed. The novelty of the approach lies in the application of meta-paths together with relational GCNs (R-GCN) to detect lateral movement. It is shown that the proposed method can reduce the mean time to respond (MTTR) through automatic subgraph clustering. Experimental evaluation on DARPA TC and OpTC datasets demonstrates a 30% increase in lateral movement recall compared to baseline methods.

Ключевые слова: APT, графовые нейронные сети, R-GCN, мета-пути, латеральное перемещение, SIEM, обнаружение атак, восстановление цепочек, неполные логи.

Keywords: APT, graph neural networks, R-GCN, meta-paths, lateral movement, SIEM, attack detection, chain reconstruction, incomplete logs.

Современные центры мониторинга безопасности (SOC) традиционно полагаются на SIEM-системы и корреляционные правила, основанные на сигнатурах. Однако, как показывает практика анализа крупных инцидентов, такой подход демонстрирует системную неспособность противостоять многостадийным целевым атакам (APT). APT-атаки характеризуются низкой интенсивностью вредоносных событий, распределением во времени и использованием легитимных системных утилит (living-off-the-land), что делает их невидимыми для сигнатурных детекторов. Основная проблема заключается в том, что

отдельное событие, например запуск PowerShell или сетевое соединение, может быть легитимным, но в совокупности с другими, разнесенными во времени действиями образует атакующий паттерн. Более того, в реальных условиях до 30–50% журналов событий могут быть утеряны из-за ограничений аудита или преднамеренного удаления следов атакующим. Цель данной работы — разработка метода восстановления цепочек атак из неполных гетерогенных логов с использованием графовых нейронных сетей. Новизна подхода заключается в применении мета-путей совместно с реляционными GCN (R-GCN) для обнаружения сложных паттернов латерального перемещения, которые не могут быть выражены плоскими правилами. Практическая значимость работы состоит в снижении времени расследования инцидентов (MTTR) за счет автоматической кластеризации подграфов, ассоциированных с атакой, и предоставления аналитику SOC реконструированной цепочки вместо сырого потока оповещений.

Для корректного учета семантики событий информационная инфраструктура представляется в виде направленного гетерогенного графа G = (V, E, φ, ψ), где V — множество узлов, E — множество ребер, φ — функция типа узла, ψ — функция типа ребра. Выделяются следующие типы узлов: хост (конечная рабочая станция или сервер), процесс (экземпляр выполняемой программы), файл (объект файловой системы), сетевое соединение (сокет или поток), пользователь (субъект аутентификации). Ребра определяются на основе телеметрии: ЗАПУСТИЛ (процесс порождает другой процесс), ПРОЧИТАЛ (процесс обращается к файлу), СОЕДИНИЛСЯ (процесс устанавливает сетевое соединение), ИМЕЕТ_СЕССИЮ (пользователь аутентифицирован на хосте). Такое представление сохраняет контекст, критичный для различения нормальной активности и атаки.

Цепочка атаки формально определяется как чередующаяся последовательность узлов и ребер p = (v1, e1, v2, ..., vk), где каждое ребро соответствует шагу тактики MITRE ATT&CK. Например, типичный путь фишинговой атаки включает процесс Outlook, который создает файл-вложение, затем этот файл запускает процесс PowerShell, который устанавливает соединение с C2-сервером. Ключевая проблема, решаемая в работе — разрыв цепочек из-за пропущенных логов. Если в графе отсутствует промежуточный узел, например событие создания файла не залогировано, стандартные алгоритмы поиска путей дают ложное отрицание. Предлагаемый метод использует стандартные источники телеметрии, доступные в большинстве корпоративных сред: Sysmon (события создания процессов, сетевых подключений, изменений файлов), EDR-агенты (дополнительная телеметрия о процессах), NetFlow или Zeek (метаданные сетевых потоков) и логи аутентификации операционной системы. Важно, что метод не требует внедрения дополнительных сенсоров и работает на существующей инфраструктуре сбора логов.

Классические рекуррентные нейронные сети, такие как LSTM или GRU, и архитектуры на внимании, например Transformer, оперируют линейными последовательностями событий. Однако APT-атаки имеют принципиально ветвящуюся структуру: один процесс может породить несколько дочерних, каждое соединение может вести к новому хосту, откуда снова происходит ветвление. Моделирование такой структуры в виде плоской последовательности приводит к экспоненциальному росту числа комбинаций или потере причинно-следственных связей. Графовые нейронные сети (GNN) естественным образом учитывают топологию взаимодействий. Среди различных архитектур базовые GCN не различают типы ребер, то есть действия ЗАПУСТИЛ и ПРОЧИТАЛ обрабатываются одинаково, что неприемлемо для кибербезопасности. GAT позволяет взвешивать вклад соседей, но также не учитывает семантику связей. В связи с этим в качестве основы выбран R-GCN (Relational GCN), который вводит отдельные матрицы весов для каждого типа ребер ψ(e), что соответствует различным действиям злоумышленника. HGT (Heterogeneous Graph Transformer) используется как расширение

для сценариев с большим числом типов узлов, например свыше десяти. Модель обучается на исторических данных с размеченными инцидентами решению трех взаимосвязанных задач: классификация узлов (определение вероятности того, что конкретный хост, процесс или пользователь скомпрометирован), предсказание связей (достраивание отсутствующих шагов атаки) и классификация подграфов (бинарная классификация всего подграфа как содержащего цепочку атаки).

Предложенный конвейер обработки включает сбор телеметрии и приведение к унифицированному формату, построение гетерогенного графа за фиксированный временной интервал, выделение подграфов (окон) с перекрытием для обеспечения непрерывности анализа, применение R-GCN с мета-путями для получения эмбеддингов узлов, кластеризацию эмбеддингов (например, методом DBSCAN) для группировки узлов, относящихся к одной атаке, и восстановление цепочки как кратчайшего пути между кластеризованными узлами с учетом временных меток. Мета-путь — это шаблон пути, заданный последовательностью типов узлов и типов ребер. Для обнаружения латерального перемещения вводятся следующие мета-пути: движение между хостами (Хост → Процесс → Сетевое соединение → Хост), что соответствует RDP, PSExec или SMB-атакам; эксфильтрация данных (Пользователь → Хост → Файл → Процесс → Соединение → C2); эскалация привилегий (Процесс → Запустил → Процесс с правами администратора → Файл SAM → Процесс). Интеграция мета-путей в R-GCN осуществляется на этапе агрегации: вместо стандартной агрегации по всем соседям сообщения распространяются только по ребрам, входящим в заданные мета-пути, что снижает шум и фокусирует модель на релевантных паттернах.

Для учета временного фактора APT-атак, которые растянуты от часов до месяцев, применяются временные срезы — граф разбивается на непересекающиеся окна длительностью 5–10 минут, внутри которых выполняется инференс, а длинные цепочки восстанавливаются за счет перекрытия окон. Дополнительно используется time-aware attention: при агрегации сообщений в GAT вес ребра умножается на затухающую экспоненту e^{-λΔt}, где Δt — время между событиями, что снижает значимость устаревших связей. В реальных логах аномальные цепочки составляют менее 0.1% от всех событий, поэтому для борьбы с дисбалансом применяется семплирование подграфов (каждый подграф, содержащий хотя бы один известный шаг атаки, дублируется 10 раз с малыми случайными вариациями) и взвешенная функция потерь Focal Loss: FL(pt) = -αt(1-pt)^γ log(pt), где γ=2 фокусирует модель на сложных, плохо классифицируемых образцах.

Эксперименты проводятся на трех наборах данных. DARPA TC (Transparent Computing) является эталонным набором с полными цепочками атак (5 сценариев) и используется для валидации. OpTC (Operational Technology Cyber) представляет собой крупный набор со свыше 10 миллионов событий с эмуляцией APT в корпоративной сети. Синтетический набор создан в эмуляционной среде с использованием CALDERA и Atomic Red Team и имитирует атаки через цепочку поставок. Тестирование проводится на трех ключевых сценариях: фишинг с последующим PowerShell, выходом на C2 и дампом учетных данных с использованием Mimikatz; Web Shell с латеральным перемещением через WMI и PsExec на 5 хостах; атака через цепочку поставок путем внедрения вредоносного кода в библиотеку JavaScript, загружаемую внутренним обновлятором.

В качестве базовых методов сравнения выбраны правила SIEM (ручная корреляция на основе 10 сигнатур), LSTM (модель на последовательности событий, упорядоченных по времени), Graph LoG (графовый парсер логов, выделяющий аномальные подграфы) и GCN (однородный граф без разделения типов узлов и ребер). Оценка проводится по метрикам precision, recall и F1 — отдельно для каждого шага атаки и для полной цепочки (цепочка считается восстановленной, если все ключевые шаги присутствуют с допустимым

отклонением), а также по времени инференса на 10 тысяч событий и устойчивости к пропуску логов при случайном удалении 10%, 30% и 50% событий.

Ожидаемые результаты вычислительных экспериментов показывают, что R-GCN с мета-путями достигает F1 = 0.87–0.92 на DARPA TC, что выше LSTM на 0.2 и правил SIEM на 0.4. Выигрыш на обнаружении латерального перемещения составляет +30% полноты (recall) по сравнению с базовым GCN. При пропуске 30% логов падение F1 не превышает 0.12, тогда как для LSTM падение достигает 0.35.

Одним из критических требований к системам безопасности является объяснимость решений. Для предложенного метода интерпретируемость обеспечивается применением GNNExplainer — алгоритма, выделяющего минимальный подграф и атрибуты узлов, которые максимально повлияли на классификацию. Аналитик SOC видит не только факт атаки, но и конкретные узлы (PID, хостнейм, имя файла), сформировавшие решение. На графах с числом узлов свыше 10 тысяч полный R-GCN становится вычислительно затратным, поэтому для таких сценариев предлагается использование GraphSAGE (сэмплирование фиксированного числа соседей) или Cluster-GCN (предварительная кластеризация графа). Компромисс заключается в незначительном снижении точности на 3–5% при выигрыше в скорости в 5–7 раз.

Предложенный метод имеет следующие ограничения. Во-первых, это зависимость от полноты аудита: если системный лог не собирает определенный тип событий, например чтение реестра, соответствующие ребра в графе отсутствуют, что может привести к пропуску цепочки. Во-вторых, это ложные срабатывания на легитимных админ-сценариях: действия систем централизованного управления (Ansible, SCCM, PowerShell DSC) создают графовые паттерны, неотличимые от латерального перемещения злоумышленника. Решение требует внесения белых списков на уровне мета-путей. Сравнение с современными исследовательскими системами, такими как NIRVANA, Poirot и SAGE, показывает, что предложенный метод обеспечивает выигрыш в скорости инференса примерно в 3 раза за счет использования R-GCN с предварительно заданными мета-путями, которые сокращают пространство поиска. При этом точность сопоставима с NIRVANA (F1=0.91) и выше, чем у Poirot (F1=0.82), который не поддерживает гетерогенные узлы.

В работе предложен метод восстановления цепочек APT-атак из неполных логов, основанный на гетерогенных графовых нейронных сетях с мета-путями. Экспериментально показано, что R-GCN с временными срезами и Focal Loss достигает F1 > 0.9 на эталонном наборе DARPA TC, существенно превосходя правила SIEM и рекуррентные архитектуры. Ключевой вклад состоит в интеграции мета-путей для обнаружения латерального перемещения, что дало прирост полноты на 30%. Практическое применение разработанного метода реализовано в виде модуля для SOC уровня L2 (аналитик-расследователь). Модуль принимает сырой поток из SIEM, автоматически строит граф, выделяет подозрительные подграфы и визуализирует восстановленную цепочку, сокращая время расследования с нескольких часов до 10–15 минут. Будущие работы включают разработку динамических GNN, обновляемых в потоковом режиме (online learning), применение федеративного обучения для межорганизационного обнаружения атак без раскрытия данных, а также генерацию синтетических цепочек атак через GAN для дообучения моделей в условиях острого дефицита размеченных инцидентов.

Библиографический список

1. Schüller F., et al. SAGE: Intrusion Alert Aggregation using Graph Neural Networks. https://ieeexplore.ieee.org/document/9467011, дата обращения 19.04.2026.

2. Schlichtkrull M., et al. Modeling Relational Data with Graph Convolutional Networks. https://link.springer.com/chapter/10.1007/978-3-319-93417-4_38, дата обращения 19.04.2026.

3. Lin T. Y., Goyal P., Girshick R., He K., Dollár P. Focal Loss for Dense Object Detection. https://openaccess.thecvf.com/content_ICCV_2017/papers/Lin_Focal_Loss_for_ICCV_2017_paper.pdf, дата обращения 19.04.2026.

4. Ying R., Bourgeois D., You J., Zitnik M., Leskovec J. GNNExplainer: Generating Explanations for Graph Neural Networks. https://proceedings.neurips.cc/paper/2019/file/d80b7040b773199015de6d3b4293c8ff-Paper.pdf, дата обращения 19.04.2026.

5. Hamilton W. L., Ying R., Leskovec J. Inductive Representation Learning on Large Graphs. https://proceedings.neurips.cc/paper/2017/file/5dd9db5e033da9c6fb5ba83c7a7ebea9-Paper.pdf, дата обращения 19.04.2026.

6. MITRE ATT&CK Framework. Lateral Movement Techniques. https://attack.mitre.org/tactics/TA0008/, дата обращения 19.04.2026.