Application of OPTICS and ensemble learning for Database Intrusion

Поляков Степан, Грицаенко Александра, Екатерина Степура, Слипченко Вера, Хугаева Дана, Рублева Вита, Тихомирова Алина

Актуальность

- Базы данных — ядро информационных систем
- Хранят критически важные сведения (финансы, клиенты, наука)
- Потери организаций ≈ 5% дохода/год (ACFE, 2016)
- Атаки бывают внешние и внутренние

Проблема

Внешний атакующий	База данных	Внутренний атакующий
уязвимости, слабые пароли		злоупотребление правами

Стандартная защита:

- аутентификация
- контроль доступа
- пароли
- firewall (межсетевые экраны)
- шифрование

НЕДОСТАТОЧНО

Системы DIDS

Ключевые требования:

- высокая точность
- низкий уровень ложных срабатываний
- надежность и скорость
- работа в реальном времени

Существующие подходы

Год	Метод	Описание	Методы
2015	ANFIS (нейро-нечёткие правила), *Brahma & Panigrahi*	Система на основе нейро-нечёткой логики. Строит правила поведения пользователей, транзакции вне правил считаются подозрительными.	ANFIS – Adaptive Neuro-Fuzzy Inference System; Нечёткая логика – работа с неопределённостью; Нейронные сети.
2016	Ассоциативные правила + кластеризация, *Singh et al.*	Используются ассоциативные правила для профиля пользователей и кластеризация для объединения схожих транзакций.	Ассоциативные правила – закономерности вида 'если A, то B'; Кластеризация – группировка объектов по схожести.
2016	PCA + Random Forest, *Ronao & Cho*	PCA уменьшает размерность данных, Random Forest классифицирует транзакции, выявляя аномалии.	PCA – метод главных компонент; Random Forest – ансамбль деревьев решений.

Существующие подходы

Год	Метод	Описание	Методы
2017	CNN + система правил LCS, *Bu & Cho*	Гибридный метод: система правил LCS выделяет аномалии, CNN уточняет классификацию.	CNN – свёрточная нейросеть; LCS – система обучающихся классификаторов.
2018	Квантовые протоколы, *Wei et al.*	Применение квантовой криптографии для защиты транзакций и запросов.	Квантовая криптография – методы защиты на основе квантовой механики.
2018	Контроль доступа по схеме БД, *Yesin et al.*	Использование структуры базы данных для построения правил доступа.	Контроль доступа – система разрешений для пользователей.
2018	Наивный Байес для SQL-запросов, *Jayaprakash & Kandasamy*	Применение Наивного Байеса для классификации SQL-запросов как нормальных или атакующих.	Наивный Байес – вероятностный метод классификации, предполагающий независимость признаков.

Основная проблема

- IDS часто генерирует слишком много тревог
- Эффект базовой частоты (Axelsson, 2000)

Даже редкие атаки -> низкая эффективность IDS, если высокий уровень ложноположительных результатов

Зачем нужен новый подход?

Необходим метод, который:

- сохраняет высокую точность
- уменьшает количество ложных тревог

Предложение авторов:

- кластеризация OPTICS (поиск аномалий)
- ансамблевое обучение (устойчивая классификация)

Обзор используемых методов - Кластеризация с использованием OPTICS

Вход:
ε — радиус окрестности
MinPts — минимальное количество точек, необходимое для образования кластера.

Выход:
Упорядоченная последовательность точек, отражающая структуру кластеризации

Основная идея алгоритма OPTICS: Для каждого объекта k в кластере существует как минимум MinPts объектов в его ε-окрестности.

Ядровая точка – объект, в ε-окрестности которого находится как минимум MinPts объектов (≥ MinPts).

$$cd_{\varepsilon,Minpts}(k) = \begin{cases} undefined & \text{if } |N_\varepsilon(k)| < MinPts \\ Minpts\_distance(k) & \text{otherwise} \end{cases}$$

$$lrd_{MinPts}(k) = 1 \Big/ \frac{\sum_{o \in N_{MinPts}(k)} rd_{\infty,MinPts}(k,o)}{|N_{MinPts}(k)|}$$

$$rd_{\varepsilon,Minpts}(k,q) = \begin{cases} undefined & \text{if } |N_\varepsilon(k)| < MinPts \\ max(cd(q), dist(q,k)) & \text{otherwise} \end{cases}$$

$$OF_{MinPts}(k) = \frac{\sum_{o \in N_{MinPts}(k)} \frac{lrd_{MinPts}(o)}{lrd_{MinPts}(k)}}{|N_{MinPts}(k)|}$$

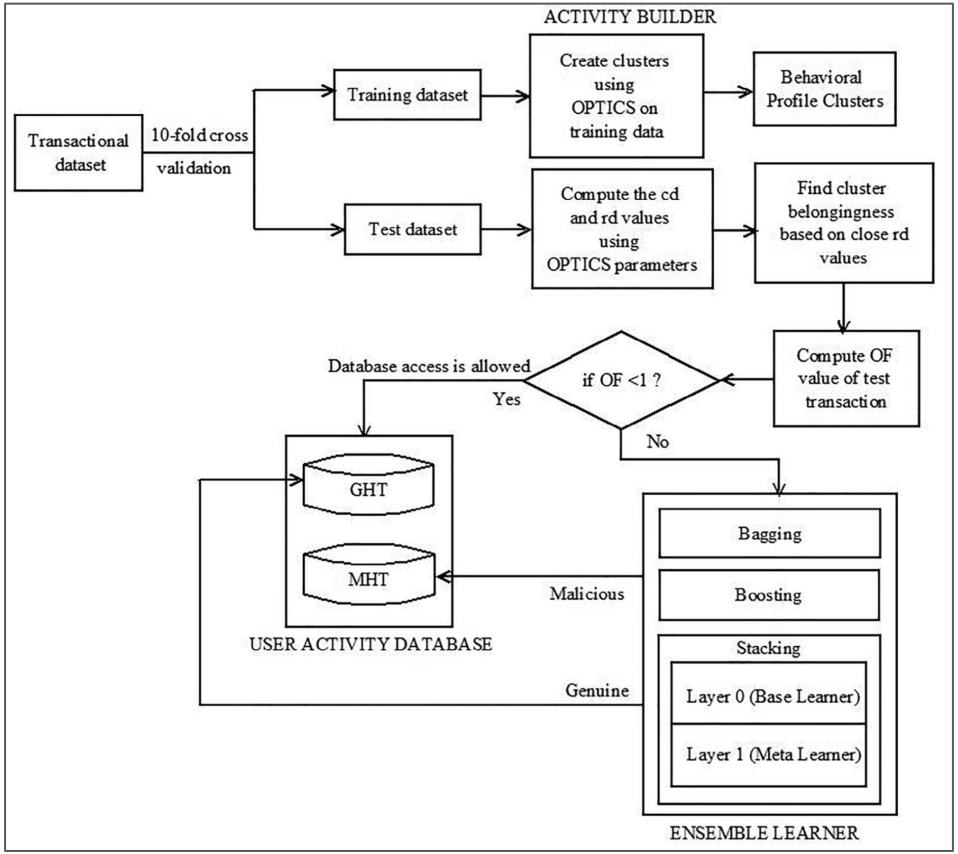
Обзор используемых методов - Ансамблевое обучение

Ансамбль – комбинация или агрегирование нескольких классификаторов. → Снижение риска увеличения числа ложноположительных результатов за счёт выбора удачного сочетания разных классификаторов.

Типы ансамблевых методов:

- ***Bagging*** — метод построения ансамбля, при котором на разных подвыборках обучаются одинаковые базовые модели. Предсказания комбинируются путём усреднения или голосования.
- ***Boosting*** — итеративное построение ансамбля, где каждая следующая модель обучается на ошибках предыдущих. Ошибочно классифицированные объекты получают больший вес. Предсказания объединяются с учётом весов моделей.
- ***Stacking*** — ансамбль, состоящий из разнородных базовых моделей. Их предсказания используются в качестве признаков для обучения метамодели («модели второго уровня»).

Предложенный подход



Activity Builder — модуль построения активности

Построение профилей пользователей базы данных на основе их прошлых транзакций.

Транзакция: $\langle u\_id, transaction\_id, query\_type, table\_list, att\_list, time\_slot, loc, time\_gap \rangle$

Пользователь с u_id = 10:
Q1: SELECT x, y FROM T1 WHERE z = 1
Q2: DELETE FROM T2 WHERE w = 1

query_type = {SELECT, DELETE}
att_list = {z, x, y, w}
table_list = {T1, T2}

transaction_id = 1
query_type {SELECT, DELETE} = {1, 4}
att_list {z, x, y, w} = {40, 23, 12, 6}
table_list {T1, T2} = {3, 6}
loc = 1 (из офиса)
time_slot = 37 (в интервале с 18:00 до 18:30)
time_gap = 21

{10, 1, {1,4}, {3,6}, {40,23,12,6}, 37, 1, 21}

u_id	transaction_id	query_type	table_list	att_list	time_slot	loc	time_gap
1	10	select	3, 1, 14	1, 6, 2, 3	9	1	4
	11	alter	17, 33	29, 30, 31, 32, 25	12	2	1
2	78	update	10, 4	4, 6, 50	33	1	5

User Activity Database — *база активности пользователей*

u_id	transaction_id	query_type	table_list	att_list	time_slot	loc	time_gap	label
1	10	select	3, 1, 14	1, 6, 2, 3	9	1	4	genuine
	11	alter	17, 33	29, 30, 31, 32, 25	12	2	1	genuine
2	78	update	10, 4	4, 6, 50	33	1	5	genuine

(a) Genuine History Table (GHT)

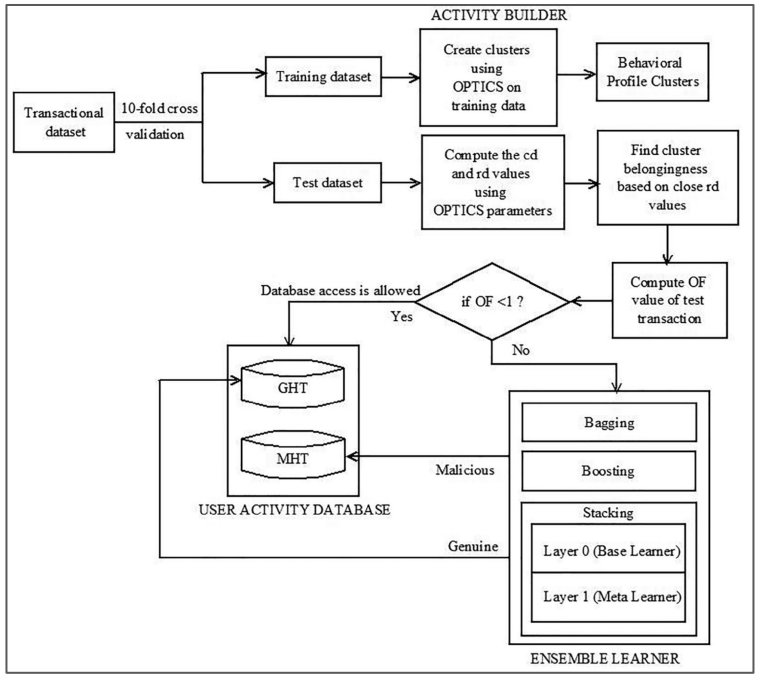
query_type	table_list	att_list	time_slot	loc	time_gap	label
delete	8, 11	16, 24, 5, 16	11	0	2	malicious
alter	55	55, 57, 75, 67	9	2	4	malicious
insert	66	1, 82, 40	27	1	1	malicious

(b) Malicious History Table (MHT)

Activity Builder — модуль построения активности

Базовые классификаторы:

- Наивный Байесовский классификатор (Naïve Bayes)
- Дерево решений (Decision Tree, DT)
- Индукция правил (Rule Induction, RI)
- Метод k-ближайших соседей (k-NN)
- Сети с радиальными базисными функциями (Radial Basis Function Network, RBFN)



Input: $D_u[m][n]$, ε, $MinPts$
Output: Genuine or Fraud

1: $Norm\_D_u[m][n] = normalize\ (D_u[m][n])$ ▷ Data Normalization
2: $[Train[m_1][n], Test\ [m_2][n]] = divide\ (Norm\_D_u[m][n])$ ▷ Train and Test sets are extracted ▷ $m = m_1 + m_2$
3: $Prof_u = OPTICS\_cluster\ (Train[m_1][n_1], \varepsilon, MinPts)$ ▷ Using Eq. (1)- Eq. (2) ▷ $Prof_u$= User Profile of User u
4: $rd[m_2] = OPTICS\_cluster(Test[m_2][n], \varepsilon, MinPts)$ ▷ Generate rd values for Incoming transaction
5: $OF[m_2] = OPTICS\_cluster\ (rd[m_2])$ ▷ Using Eq.4
6: **if** $OF[m_2] < 1$ **then**
7: Output ("Database Access is allowed")
8: Insert_GHT $(Test_x)$ ▷ Insert $Test_x$ in GHT ▷ $Test_x \in Test[m_2][n],\ \ x = 1, \cdots, m_2$
9: **else**
10: goto EL ▷ EL: Ensemble Learner
11: **end if**
Collect History Information D(U_x) about user U_x from User Activity Database
EL:
12: $Bag = Bagging(Test_x, Prof_U)$ ▷ Bag: Bagging model
13: $Boost = Boosting(Test_x, Prof_U)$ ▷ $Boost$: Boosting model
14: $Stack = Stacking(Test_x, Prof_U)$ ▷ $Stack$: Stacking model
15: **if** $(Test_x \in Bag) \| (Test_x \in Boost) \| (Test_x \in Stack)$ **then**
16: Insert_GHT $(Test_x)$ ▷ Insert $Test_x$ in GHT
17: Output ("Genuine")
18: **else**
19: Insert_MHT $(Test_x)$ ▷ Insert $Test_x$ in MHT
20: Output ("Malicious")
21: **end if**

Экспериментальные данные

- Использован симулятор транзакций с тремя модулями:
  - GTGM – генерация нормальных действий.
  - MTGM – моделирование атакующих транзакций.
  - MMPPM – управление частотой и структурой потоков.
- Итоговый объём данных: 41 390 транзакций (нормальные + атакующие).

Настройка OPTICS

- OPTICS применяется для кластеризации транзакций и выделения профилей нормального поведения.
- Для подбора оптимальных параметров исследовались комбинации MinPts и ε.
- Наилучшие результаты получены при MinPts = 10, ε = 0.
- Обеспечили минимальное число ложных тревог.

Performance of OPTICS with Different Parameter Values.

Performance Metrics (in %)	Parameter Values					
	Minpts = 10 $\varepsilon = 0$	Minpts = 10 $\varepsilon = 5$	Minpts = 50 $\varepsilon = 0$	Minpts = 50 $\varepsilon = 5$	Minpts = 100 $\varepsilon = 0$	Minpts = 100 $\varepsilon = 5$
Accuracy	**56.34**	56.24	58.37	58.27	62.58	62.48
Precision	**69.90**	69.80	68.40	68.30	66.43	66.33
F1_Score	**50.73**	50.60	53.63	53.53	62.30	62.20
TPR	**58.79**	58.69	60.12	60.02	64.30	64.20
FPR	**34.73**	35.09	34.94	34.84	37.11	38.46

Сравнение классификаторов и ансамблей

- Проверялись пять алгоритмов: Naïve Bayes, Decision Tree, Rule Induction, k-NN, RBFN.
- При индивидуальном применении модели показывали средние результаты.
- Использование ансамблевых методов (Bagging, Boosting) повысило эффективность:
  - увеличилась точность классификации;
  - снизился уровень ложных тревог.
- Наиболее стабильные показатели зафиксированы у k-NN и RBFN.

Stacking

- Реализована архитектура stacking.
- Этот подход обеспечил наилучшее качество среди всех методов.
- Stacking показал преимущество в точности и устойчивости по сравнению с одиночными классификаторами и другими ансамблями.

Сравнение с существующими подходами

- Проведено сравнение с ANFIS-DIDS и PCA-WRF.
- Новый метод показал преимущество по всем ключевым критериям.
- Дополнительное преимущество — меньшие вычислительные затраты за счёт фильтрации транзакций на этапе OPTICS.

Заключение

- Разработанная система объединяет кластеризацию OPTICS и ансамблевые методы обучения.
- Достоинства подхода:
  - высокая точность обнаружения атак,
  - снижение числа ложных срабатываний,
  - меньшая вычислительная сложность по сравнению с существующими решениями.
- Предложенный метод можно рассматривать как эффективный и перспективный инструмент для построения систем обнаружения вторжений в базы данных.