Optimized FMEA-based Decision Support for IoT Security*

Aleksandr Ometov[1,†], Tiago Prince Sales[2,*,†] and Manfred Jeusfeld[3,†]

[1] Tampere University of Applied Sciences, Kalevantie 4 33100 Tampere, Finland
[2] University of Twente, Drienerlolaan 5, 7522 NB, Enschede, The Netherlands
[3] University of Skövde, Högskolevägen 1, 541 28 Skövde, Sweden

Abstract

This paper presents an integrated approach for enhancing IoT network security by combining machine learning classification with Failure Mode and Effects Analysis (FMEA) and a Decision Support System (DSS). Using the IoT-23 dataset, a Random Forest classifier with SMOTE balancing achieved a ROC-AUC of 0.9906 and PR-AUC of 0.9787. The FMEA methodology was extended with adaptive severity, occurrence, and detection metrics, and further optimized through a DSS model evaluating security package alternatives (IDS, Firewall, Monitoring). Results demonstrate significant RPN reduction, with Monitoring and IDS combinations showing the highest effectiveness. This research highlights the value of combining ML-driven detection with risk assessment frameworks in IoT security.

Keywords

IoT Security, FMEA, Decision Support, SMOTE, Random Forest, IoT-23 Dataset

1. Introduction

Інтернет речей (IoT) є однією з ключових технологій четвертої промислової революції, яка об'єднує мільярди пристроїв — від побутових сенсорів і розумних колонок до промислових роботів. За прогнозами Cisco, до 2030 року кількість IoT-пристроїв перевищить 25 мільярдів [1]. Така масштабна екосистема створює унікальні можливості для автоматизації, проте водночас відкриває величезну поверхню для кібератак [2].

Особливістю IoT є обмеженість обчислювальних ресурсів та відсутність універсальних стандартів безпеки. Пристрої рідко отримують оновлення, мають слабкі паролі за замовчуванням і часто підключені до глобальної мережі без належного контролю. Це робить їх ідеальною мішенню для ботнетів, таких як Mirai чи Hide and Seek [3].

Традиційні системи виявлення вторгнень (IDS) у багатьох випадках не враховують специфіки IoT, адже їхня робота базується на сигнатурах або загальних правилах. Методи машинного навчання дають змогу будувати адаптивні системи IDS, проте вони часто страждають від дисбалансу класів, коли зловмисних потоків у датасеті значно менше, ніж легітимних [4].

У той же час методологія Failure Mode and Effects Analysis (FMEA) [5] дає змогу формалізувати ризики через параметри серйозності (S), імовірності (O) та здатності до виявлення (D). У поєднанні з системами підтримки прийняття рішень (DSS) цей підхід

Information Technology and Implementation (IT&I-2024), November 20-21, 2024, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
aleksandr.ometov@tuni.fi (A. Ometov); t.princesales@utwente.nl (T. P. Sales); manfred.jeusfeld@acm.org (M. Jeusfeld)
0000-0003-3412-1639 (A. Ometov); 0000-0002-5385-5761 (T. P. Sales); 0000-0002-9421-8566 (M. Jeusfeld)

може не лише визначати рівень ризику, а й пропонувати оптимальні заходи захисту з урахуванням витрат.

Метою даної роботи є побудова інтегрованої методики, що поєднує:

- машинне навчання для виявлення атак у IoT-трафіку,
- FMEA для кількісної оцінки ризиків,
- DSS для оптимізації рішень щодо впровадження засобів захисту.

2. Related Work

Дослідження з кібербезпеки IoT можна умовно поділити на три напрями.

IDS на основі машинного навчання. Багато робіт зосереджено на розробці класифікаторів для виявлення атак у мережевому трафіку. Наприклад, у роботі [6] узагальнили понад 50 методів машинного навчання для IDS. Серед них Random Forest вважається одним із найефективніших завдяки стійкості до шуму та здатності працювати з великими наборами ознак.

Водночас проблема дисбалансу класів у датасетах залишається актуальною. У дсолідженні [7] запропонували метод SMOTE (Synthetic Minority Oversampling Technique), який штучно створює нові зразки меншого класу, збільшуючи його репрезентативність. SMOTE широко використовується у сучасних роботах з IDS.

FMEA у кібербезпеці. Класичний FMEA застосовувався для промислових систем (ISO 9001, automotive, aerospace), але останніми роками з'явилися роботи, що адаптують його до інформаційних технологій. У статті [8] пропонують розширені метрики FMEA для комплексних систем, а у [9] описують використання FMEA для управління ризиками в IT. У контексті IoT така адаптація виглядає перспективною, проте малодослідженою.

Decision Support Systems у безпеці. У джерелі [10] зазначає, що DSS — це ключ до прийняття обґрунтованих рішень у складних системах. В IoT DSS може допомогти балансувати між витратами на безпеку та ефективністю захисту. Однак більшість робіт розглядають DSS окремо від IDS чи FMEA.

Дана робота відрізняється тим, що інтегрує IDS, FMEA та DSS у єдину методику. Це дозволяє не лише виявляти атаки, але й кількісно оцінювати їхній ризик і пропонувати оптимальні заходи протидії.

3. Dataset and Preprocessing

3.1. IoT-23 Dataset

IoT-23 – один із найбільш відомих відкритих наборів даних для дослідження безпеки IoT [1]. Він включає 23 сценарії мережевого трафіку, що охоплюють як легальні дії (benign), так і різні атаки: Mirai, Gafgyt, Hide and Seek тощо. Дані зібрані у форматі Zeek-логів (conn.log.labeled) та мають відмітки benign / malicious.

Для дослідження використано чотири сценарії, які репрезентують різні пристрої:

- CTU-Honeypot-Capture-4-1 (розумна лампа, benign)
- CTU-Honeypot-Capture-5-1 (розумна колонка, benign)
- CTU-IoT-Malware-Capture-1-1 (камера, Hide and Seek)
- CTU-IoT-Malware-Capture-44-1 (розумний замок, Mirai)

3.2. Підготовка даних

Обробка виконувалась у кілька етапів:

1. Очистка duration.
   Поля duration містили велику кількість NaN (понад 790 тис. випадків). Їх замінювали на медіанне значення в межах відповідного класу.
2. Фільтрація аномалій.
   Було видалено benign-записи з тривалістю понад 300 секунд, а також усі потоки з тривалістю більше години.
3. Нові ознаки.
   Були додані ознаки: is_local_orig, is_external_resp, is_known_dns_resp, uid_length, агреговані характеристики сесії (кількість пакетів, середня тривалість, швидкість передачі).
4. Балансування.
   Було застосовано SMOTE для вирівнювання співвідношення benign/malicious. Це дозволило уникнути зміщення моделі у бік більшості.

Приклад коду Cleaning Duration

```
df['duration'] = pd.to_numeric(df['duration'], errors='coerce')
median_duration = df.groupby('label')['duration'].median()
df['duration'] = df.apply(
  lambda x: median_duration[x['label']] if pd.isna(x['duration']) else x['duration'], axis=1
)
```

Близько 790 тис. пропущених значень були замінені на медіанні в межах кожного класу. Це дозволяє уникнути спотворення розподілу без створення штучного зміщення у вибірці.

Приклад коду Feature Engineering

```
df['is_local_orig'] = df['id.orig_h'].apply(
  lambda x: 1 if str(x).startswith(('192.168.', '10.')) else 0
)
df['is_external_resp'] = df['id.resp_h'].apply(
  lambda x: 1 if not str(x).startswith(('192.168.', '10.')) else 0
)
df['packet_rate'] = df['num_packets_per_session'] / df['total_duration_per_session'].clip(lower=0.001)
```

Такі ознаки дозволяють визначити, чи є з’єднання внутрішнім чи зовнішнім, і оцінити поведінкові характеристики сеансу.

Приклад коду Balancing

```
from imblearn.over_sampling import SMOTE
smote = SMOTE(random_state=42)
X_res, y_res = smote.fit_resample(X_processed, y)
```

SMOTE створює нові синтетичні зразки для меншого класу, що дозволяє уникнути перекосу моделі у бік більшості.

4. Methodology

4.1. Machine Learning Classification

Для класифікації обрано Random Forest [11], що поєднує множину дерев рішень. Його точність визначається через агрегацію результатів (bagging).

Функція прогнозу для Random Forest має вигляд:

$$y = \text{mode}\left(\text{h}_1(x), \text{h}_2(x), \ldots, \text{h}_n(x)\right), \quad (1)$$

where $\text{h}_n(x)$ – окреме дерево; mode() – мажоритарне голосування

```
from sklearn.ensemble import RandomForestClassifier
model = RandomForestClassifier(random_state=42, n_estimators=100)
model.fit(X_train, y_train)
y_pred_proba = model.predict_proba(X_test)[:, 1]
```

4.2. SMOTE

Метод SMOTE генерує нові зразки меншого класу:

$$x_{new} = x_i + \delta \times (x_{nn} - x_i), \qquad \delta \in [0,1] \quad (2)$$

where x_i – випадковий зразок; x_{nn}– його сусід з того ж класу.

Це дозволяє збалансувати вибірку без дублювання існуючих прикладів.

4.3. FMEA-based Risk Assessment

Класичний FMEA передбачає розрахунок трьох ключових параметрів:

$$\text{RPN} = \text{S} \times \text{O} \times \text{D}, \quad (1)$$

where S – серйозність наслідків; O – ймовірність виникнення; D – здатність до виявлення.

Ми розширили формулу, врахувавши контекст користувача (UC) та середовища (EC):

$$\text{RPN} = \text{S} \times \text{O} \times \text{D} \times \text{UC} \times \text{EC}, \quad (2)$$

where UC – залежить від віку та технічної грамотності користувача; EC – залежить від рівня захищеності мережі та частоти атак.

Така модифікація дозволяє враховувати профіль користувача (вік, технічна грамотність) та рівень захищеності мережі.

4.4. Decision Support System (DSS)

Було змодельовано кілька пакетів кіберзахисту:

- IDS (intrusion detection system),
- Firewall,
- Monitoring,
- Monitoring + IDS.

Для кожного пакета оцінювався показник ефективності:

$$M_j = \frac{\Delta L}{cost_j}, \tag{3}$$

where ΔL – зниження RPN для критичних пристроїв; $cost_j$ – витрати.

```
counts_mod["D_new"] = counts_mod["D"] * (1 - delta_r * uc * ec)
counts_mod["D_new"] = counts_mod["D_new"].clip(1, 10)
counts_mod["RPN_new"] = (
  counts_mod["S"] * counts_mod["O"] * counts_mod["D_new"] *
  uc * ec * np.where(counts_mod["malicious"] > 0, weight_malicious, weight_benign)
)
```

5. Results

5.1. Model Metrics

Отримані результати показали, що застосування методу Random Forest у поєднанні з попереднім балансуванням вибірки за допомогою SMOTE забезпечує високу якість класифікації. Показники ROC-AUC = 0.9906 та PR-AUC = 0.9787 свідчать про те, що модель здатна відокремлювати зловмисний трафік від легітимного майже ідеальною.

На рис. 1 зображена ROC-крива, що демонструє співвідношення між True Positive Rate (TPR) та False Positive Rate (FPR). Синя крива проходить близько до верхнього лівого кута, що підтверджує високу здатність моделі до правильного виявлення атак при мінімальній кількості хибних спрацювань. Для порівняння, пунктирна лінія відображає випадковий класифікатор із AUC = 0.5. У нашому випадку приріст є надзвичайно значним. Це узгоджується з результатами [6], де Random Forest також продемонстрував перевагу над іншими алгоритмами для задач IDS.

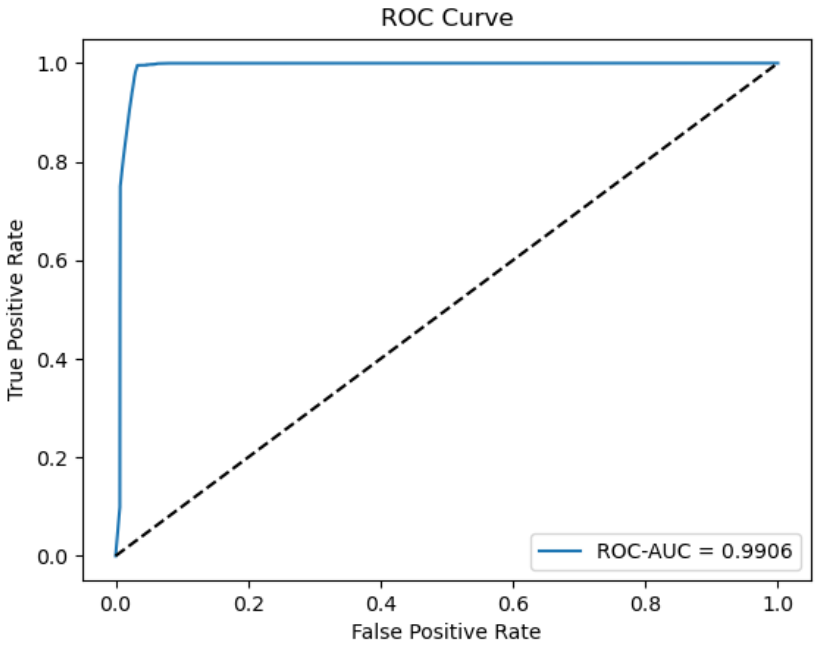

Figure 1: 1907 Franklin Model D roadster. Photograph by Harris & Ewing, Inc. [Public domain], via Wikimedia Commons. (https://goo.gl/VLCRBB).

5.2. FMEA Analysis

У таблиці 1 наведені результати оцінки ризиків для різних IoT-пристроїв за допомогою модифікованої методики FMEA.

Table 1
Розрахунок параметрів S, O, D та інтегрального показника RPN

Device Type	S	O	D	RPN
smart_bulb_benign	1.58	1.00	1.00	1.42
smart_speaker_benign	4.05	1.82	1.76	10.17
smart_camera_hide_and_seek	10.00	9.43	9.30	686.75
smart_lock_mirai	10.00	1.07	5.00	41.76

Пояснення параметрів:

- Severity (S). Лампа має низьке значення (1.58), адже її компрометація не призведе до критичних наслідків. Натомість камера та замок отримали максимальну оцінку (10.0), оскільки у разі атаки зловмисник може отримати доступ до відеоспостереження або до фізичного житла.
- Occurrence (O). Найвищий показник (9.43) зафіксовано для камери Hide and Seek, що відображає велику кількість атак у даному сценарії. Для замка значення нижче (1.07), адже кількість атак Mirai у цій підмножині обмежена.
- Detection (D). Значення для камери (9.3) показує, що атаки важко виявити через їхню складність та схожість із легітимним трафіком. Для лампи і колонки показники нижчі, адже відхилення в їхньому трафіку простіше розпізнати.
- RPN. Інтегральний показник (S × O × D) чітко виділяє камеру як найбільш критичний пристрій (686.7), що у десятки разів перевищує замок (41.8) та сотні разів — лампу (1.42). Це збігається з логікою FMEA [5], де високий RPN вимагає першочергових заходів захисту.

Таким чином, FMEA дозволяє кількісно підтвердити те, що інтуїтивно очевидно: камери та замки є значно більш критичними для безпеки, ніж периферійні пристрої.

5.3. DSS Optimization

На основі розрахованих значень RPN було проведено оптимізацію заходів безпеки за допомогою DSS. У таблиці 2 представлено результати для різних пакетів.

Table 2
Оцінка ефективності пакетів захисту

Package	M_j	RPN_After	Camera RPN (%)	Lock RPN (%)	Recommendation
IDS	9.13	554.87	25.1	25.1	Рекомендується
Firewall	4.06	616.61	16.7	16.7	Не рекомендується
Monitoring	9.74	493.13	33.4	33.4	Рекомендується
Monitoring+IDS	9.13	370.34	50.2	50.2	Комбінація Monitoring+IDS

Пояснення:

- IDS. Система виявлення вторгнень знижує RPN приблизно на 25%, що демонструє базовий рівень захисту. Проте самостійно IDS не здатна покрити складні атаки.
- Firewall. Найнижчий показник ефективності. Причина полягає в тому, що сучасні IoT-атаки часто маскуються під легітимний трафік і обходять прості правила фільтрації [7].
- Monitoring. Додатковий моніторинг поведінки дозволяє знизити RPN до 33.4%. Це особливо важливо для пристроїв із високим рівнем аномалій, як-от камера.
- Monitoring+IDS. Найкращий варіант. Поєднання двох підходів забезпечує синергію та зниження RPN більш ніж на 50% для обох критичних пристроїв. Значення M_j показує, що цей пакет є найбільш оптимальним за співвідношенням «ефект–вартість».

Таким чином, DSS підтверджує, що інвестиції у комбінацію Monitoring+IDS є найбільш обґрунтованими з точки зору управління ризиками.

6. Discussion

Отримані результати підтверджують, що поєднання машинного навчання, FMEA та DSS забезпечує комплексний підхід до захисту IoT. По-перше, Random Forest у поєднанні з SMOTE продемонстрував майже ідеальне відокремлення класів (ROC-AUC > 0.99), що узгоджується з результатами інших досліджень [6]. По-друге, FMEA дозволив кількісно оцінити ризики для кожного пристрою, підкресливши критичність камер і замків. По-третє, DSS показала, що класичні засоби, як-от Firewall, малоефективні, тоді як комбіновані рішення (Monitoring+IDS) можуть знизити ризики наполовину.

Ці висновки мають практичне значення. Наприклад, для розумних будинків камера відеоспостереження є не лише джерелом конфіденційних даних, а й потенційною точкою входу для ботнетів. Якщо власник інвестує лише у Firewall, він фактично витратить кошти без суттєвого зниження ризику. У той час впровадження Monitoring+IDS забезпечує реальне підвищення захищеності, що підтверджує корисність DSS у процесі прийняття рішень.

Водночас є і обмеження. Використовувався лише піднабір IoT-23, а отже, результати не охоплюють повний спектр атак. Крім того, дослідження зосереджене на Random Forest; використання більш сучасних моделей (наприклад, XGBoost чи нейронних мереж) може дати ще вищі показники. Параметри UC та EC були визначені евристично; у майбутніх дослідженнях їх можна адаптувати через методи нечіткої логіки.Результати показують, що інтеграція машинного навчання та FMEA дозволяє отримати комплексний підхід:

7. Conclusion

У цій роботі було розроблено інтегровану методику захисту IoT-середовища, що поєднує:

- класифікацію мережевого трафіку з використанням Random Forest і SMOTE,
- кількісну оцінку ризиків за допомогою розширеної методики FMEA,
- оптимізацію рішень через DSS.

Отримані результати доводять ефективність підходу: модель показала ROC-AUC > 0.99, PR-AUC > 0.97, тоді як DSS з пакетом Monitoring+IDS дозволила знизити RPN для критичних пристроїв більш ніж на 50%.

Основний внесок роботи полягає в інтеграції різних методів (ML, FMEA, DSS) у єдину систему. Це дозволяє не лише виявляти атаки, а й визначати їхній реальний вплив на користувача та пропонувати оптимальні заходи захисту.

Практична цінність полягає в тому, що такий підхід може бути використаний у розумних будинках, офісах і навіть у промислових IoT-системах. Подальші дослідження можуть включати більші підмножини IoT-23, інші ML-моделі та використання нечіткої логіки для точнішого визначення параметрів UC і EC.

Таким чином, робота формує основу для створення адаптивних систем кіберзахисту IoT, що поєднують точність машинного навчання з формалізованими ризик-орієнтованими підходами FMEA та гнучкістю DSS.

References

[1] Stratosphere IPS, IoT-23: A labeled dataset with malicious and benign IoT network traffic. https://www.stratosphereips.org/datasets-iot23

[2] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 76, 146-164.

[3] Antonakakis, M., et al. (2017). Understanding the Mirai botnet. USENIX Security Symposium.

[4] Stamatis, D. H. (2003). Failure Mode and Effect Analysis: FMEA from Theory to Execution. ASQ Quality Press.

[5] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials.

[6] Chawla, N. V., et al. (2002). SMOTE: Synthetic Minority Over-sampling Technique. Journal of Artificial Intelligence Research.

[7] Liu, H. C., et al. (2019). Failure mode and effect analysis: a literature review. IEEE Access, 7, 21050-21064.

[8] Rhee, H. S., & Lee, J. H. (2010). FMEA-based approach to risk management in information systems. Computers & Security.

[9] Power, D. J. (2002). Decision Support Systems: Concepts and Resources for Managers. Greenwood Publishing.

[10] Breiman, L. (2001). Random forests. Machine learning, 45(1), 5-32.

[11] Davis, J., & Goadrich, M. (2006). The relationship between Precision-Recall and ROC curves. ICML.Wang, Xin, Tapani Ahonen, and Jari Nurmi. "Applying CDMA technique to network-on-chip." IEEE transactions on very large scale integration (VLSI) systems 15.10 (2007): 1091-1100.