Indonesian Journal of Electrical Engineering and Computer Science
Vol. 44, No. 1, October 2026, pp. 130~139
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v44.i1.pp130-139

Lightweight MITM detection with feature selection and active deception

Somkiat Kosolsombat[1], Chiabwoot Ratanavilisagul[2]
[1]Data Science and Innovation Program, College of Interdisciplinary Studies, Thammasat University, Bangkok, Thailand
[2]Department of Computer and Information Science, Faculty of Applied Science, King Mongkut's University of Technology North Bangkok (KMUTNB), Bangkok, Thailand

Article Info

Article history:

Received Mar 27, 2026
Revised Aug 23, 2026
Accepted Sep 10, 2026

Keywords:

Active defense
ARP spoofing detection
Deceptor-in-the-middle
Hybrid feature selection
Man-in-the-middle attack

ABSTRACT

Man-in-the-middle (MITM) attacks remain difficult to handle in enterprise and internet of things networks because many intrusion detection systems stop at passive alerting or require high-dimensional traffic features. This study proposes a lightweight active defense system (LADS) that combines a hybrid feature selection pipeline with an active deceptor-in-the-middle response. The detection pipeline applies mutual information filtering, recursive feature elimination, and principal component analysis before training a random forest classifier. The system was evaluated on NSL-KDD, UNSW-NB15, CICIDS-2017, and Bot-IoT data, with additional EVE-NG-based attack modeling for address resolution protocol (ARP) spoofing and SSL stripping scenarios. Using only a compact feature representation, LADS achieved 99.42% accuracy on CICIDS-2017, 91.94% on UNSW-NB15, and 89.13% on the NSL-KDD proxy experiment, while a direct NSL-KDD fold-level validation exceeded 99% accuracy. The CICIDS-2017 setting produced a feature efficiency score of 31.56, a 2.79-fold improvement over the full-feature random forest baseline. Fold-level principal component analysis (PCA) sensitivity showed that increasing the variance threshold from 95% to 99% improved UNSW-NB15 accuracy from 92.15% to 92.43% and matthews correlation coefficient (MCC) from 0.8425 to 0.8483, while CICIDS-2017 remained stable above 99.96% accuracy. A Monte Carlo simulation of the DitM response reduced mean attacker dwell time from 1,167 s to 15.3 s and reduced estimated exfiltration from 74.54% to 0.98%. The results suggest that lightweight detection can be paired with active containment, although the DitM component still requires real red-team validation.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Chiabwoot Ratanavilisagul
Department of Computer and Information Science, Faculty of Applied Science
King Mongkut's University of Technology North Bangkok (KMUTNB)
Bangkok, Thailand
Email: chaibwoot.r@sci.kmutnb.ac.th

1. INTRODUCTION

Man-in-the-middle (MITM) attacks allow an adversary to observe, modify, or relay traffic between legitimate hosts. Address resolution protocol (ARP) spoofing remains a practical entry point because it exploits local network trust and can be combined with SSL stripping or credential harvesting. Recent studies show that machine learning can detect ARP spoofing and related MITM behavior, but reported approaches vary in their traffic assumptions, feature budgets, and defensive response mechanisms [1]-[3].

A second challenge is that high detection accuracy is often obtained by using many flow features or computationally expensive models. Deep learning (DL) and optimized classifiers improve detection in internet of things (IoT) and software-defined network (SDN) contexts, but they may be hard to deploy at network edges where inference latency, feature extraction cost, and model size matter [4]-[7].

This paper therefore focuses on the intersection of lightweight detection and active response. The research gap is not merely whether MITM traffic can be classified, but whether a compact detector can trigger a response that contains the attacker without immediately revealing that detection has occurred.

The main contributions are:

a) A compact MI -> RFE -> PCA feature-selection pipeline for MITM-related traffic detection.
b) A random forest detection model evaluated with cross-validation, statistical testing, SHAP-based interpretation, balanced accuracy, and MCC.
c) An active DitM response model that estimates dwell time and exfiltration reduction.
d) An explicit discussion of dataset bias, principal component analysis (PCA) information loss, and the limits of simulation-based active defense.

2. RELATED WORK AND RESEARCH GAP

2.1. MITM and ARP spoofing detection

ARP spoofing and MITM detection research increasingly uses supervised learning and traffic profiling. Majumder *et al.* [1] compared machine learning classifiers for ARP spoofing, while ARP-PROBE combined explainable deep learning with IoT ARP-spoofing detection [1], [2]. Prasad and Chandra integrated ML classification with device profiling, and recent IoT and spoofing studies extended the problem to smart homes and modern IoT traffic [3]-[5].

CBNA-RF and game-theoretic SDN work show that detection can be linked to defense actions, but these systems do not directly evaluate a lightweight feature budget paired with deception-based containment [6], [7].

2.2. Hybrid feature selection and explainable IDS

Hybrid feature selection has become a common route to reducing IDS complexity. IGRF-RFE, hybrid stacked feature selection, IoT anomaly-selection pipelines, improved mutual information selection, enhanced Random Forest IDS, hybrid ensemble models, permutation importance, SHAP explanations, and systematic IDS reviews all support the need to balance accuracy, interpretability, and feature cost [8]-[16].

2.3. Recent security-ML techniques requested by reviewers

The revised review also considers recent optimization-based security detection studies suggested by the reviewer: binary olympiad optimizer for SQL injection detection, binary gray wolf optimizer for SQL injection detection, and ECOC with adaptive neuro-fuzzy inference for denial-of-service detection [17]-[19]. These papers are not direct MITM baselines, but they highlight the current trend toward feature optimization, classifier selection, and robust evaluation in security-ML systems.

2.4. Active deception and honeypot-based response

Active defense research proposes that an attacker can be delayed or redirected rather than simply blocked. Sherif et al. introduced the deceptor-in-the-middle concept for wireless network virtualization, while recent honeypot, honeynet, cyber-deception, and IoT security surveys describe deception architectures and metrics such as attacker dwell time, engagement, and containment quality [20]-[24].

2.5. Dataset context and feature-selection taxonomy

The experimental design uses primary dataset sources for UNSW-NB15, CICIDS-2017, Bot-IoT, and KDD/NSL-KDD, while also acknowledging the need to evaluate newer IoT datasets such as CICIoT2023 [25]-[29]. The filter-wrapper-embedded taxonomy and the motivation for combining complementary feature-selection families follow the general feature-selection survey literature [30].

Table 1 positions the lightweight active defense system (LADS) against the related-work groups reviewed above and identifies the unresolved gap addressed by the proposed lightweight detection and active deception design.

Table 1. Positioning of LADS against related work already cited in Section 2

Work group	Focus	Strength	Remaining gap
ARP/MITM ML studies	ARP/MITM ML	Classifier or device profiling	Limited active containment
IoT MITM/spoofing studies	IoT MITM/spoofing	Recent IoT contexts	Dataset and deployment assumptions differ
MITM/ARP defense studies	MITM/ARP defense	Detection linked to response	No MI-RFE-PCA lightweight DitM evaluation
Feature selection IDS studies	Feature selection IDS	Hybrid FS, RF, ensembles	Mostly passive IDS; limited active defense
XAI and IDS survey studies	XAI / IDS survey	Interpretability and evaluation framing	Does not provide containment mechanism
Reviewer-recommended security ML	Optimization-based security ML	Optimization and classifier rigor	Different attack types, not direct MITM
Deception and honeypot studies	Deception/honeypots	Active defense concept	Limited integration with lightweight ML detector
Proposed LADS	MITM active defense	MI -> RFE -> PCA + RF + DitM	Simulation-based DitM needs real validation

3. PROPOSED METHOD

Figure 1 presents the experimental and simulation workflow used by LADS, from traffic capture through MI-RFE-PCA feature compacting, random forest classification, and DitM response activation. LADS is designed as a sequential pipeline: traffic capture, preprocessing, mutual-information filtering, recursive feature elimination, PCA compacting, random forest detection, and DitM response. The first five stages are fitted inside the training folds to avoid data leakage. The DitM stage is triggered only after a positive MITM classification.

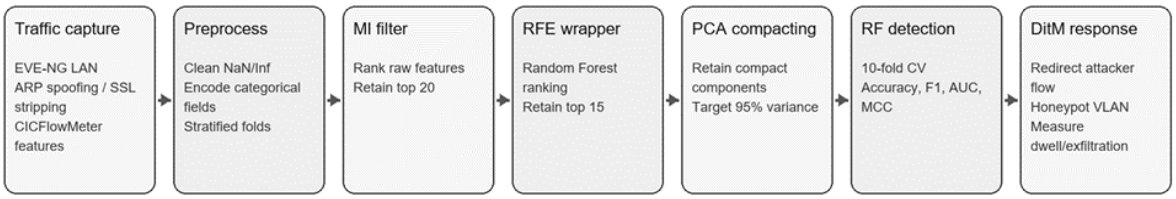

Figure 1. Workflow of the proposed LADS pipeline

3.1. Hybrid MI-RFE-PCA pipeline

Stage 1 computes mutual information between each feature and the binary class label, then keeps the top 20 ranked features when enough raw features are available. Stage 2 applies recursive feature elimination using a random forest estimator and produces 15 selected features. Stage 3 applies PCA to those 15 RFE-selected features as its input. The PCA output is a set of orthogonal principal components rather than the original feature names; in the direct sensitivity experiment, the resulting output size ranges from 5 to 13 components depending on the dataset and retained-variance threshold. The 95% variance target was selected as the main lightweight setting; however, a direct 95%-versus-99% sensitivity analysis is reported because the optimal compression level is dataset-dependent.

3.2. Deceptor-in-the-middle response

When the classifier flags MITM behavior, the response layer silently redirects the attacker's traffic path toward a honeypot VLAN by manipulating the attacker's perceived network path. Unlike immediate blocking, this response aims to reduce exfiltration while preserving evidence and attacker engagement. In this revision, the DitM result is explicitly described as a simulation-supported estimate, not as a real-world deployment measurement.

4. METHOD

4.1. Study design and research questions

The study evaluates whether a lightweight MITM detector can maintain competitive detection performance, whether hybrid feature selection improves the accuracy-to-feature trade-off, whether the PCA stage introduces information loss, and whether a simulated DitM response can reduce dwell time and data exfiltration compared with no defense and detection-only baselines.

4.2. Datasets and bias analysis

Table 2 reports the normal-versus-attack distribution of each benchmark dataset so that the class balance and bias context are visible before the evaluation results are interpreted. Figure 2 visualizes the dataset class distribution to make the imbalance pattern clear before the bias-aware interpretation of the results.

Table 2. Dataset distribution and imbalance profile

Dataset	Total	Normal	Attack	Normal (%)	Attack (%)	Imbalance ratio	Bias note
NSL-KDD	125973	67343	58630	53.46	46.54	1.15	Moderate / near-balanced
UNSW-NB15	82332	37000	45332	44.94	55.06	1.23	Moderate / near-balanced
CICIDS-2017	2830743	2273097	557646	80.3	19.7	4.08	Moderate / near-balanced
Bot-IoT	2934817	370	2934447	0.01	99.99	7930.94	Highly imbalanced

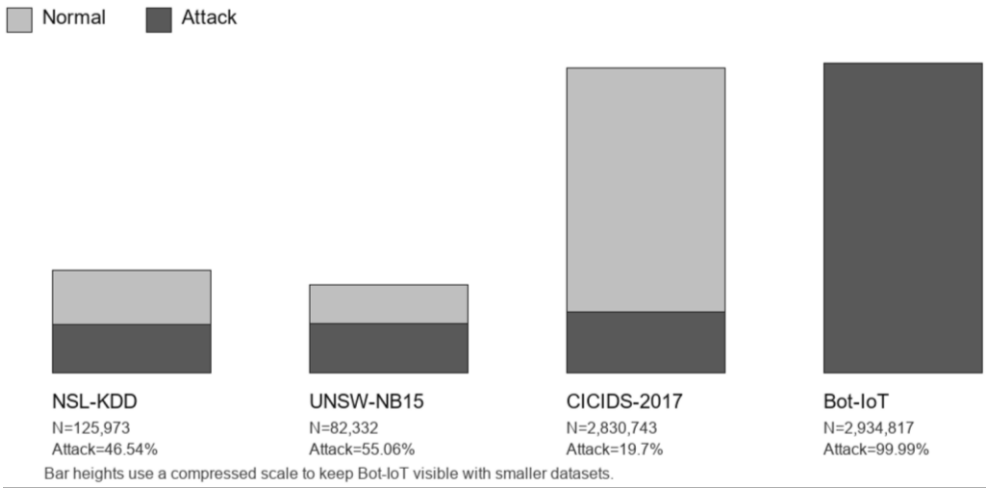

Figure 2. Dataset class distribution and imbalance

The distribution table clarifies a key limitation: NSL-KDD and UNSW-NB15 are relatively near-balanced, CICIDS-2017 is moderately skewed toward benign traffic, and Bot-IoT is extremely attack-heavy in the available 10-best training file. For this reason, balanced accuracy and MCC are reported in addition to accuracy, and Bot-IoT is interpreted cautiously. Table 3 extends the dataset-bias analysis by listing the dominant normal and attack categories used in the experiments.

Table 3. Main attack/category frequency distribution

Dataset	Label/category	Count	Percent
NSL-KDD	normal	67343	53.458
NSL-KDD	neptune	41214	32.717
NSL-KDD	satan	3633	2.884
NSL-KDD	ipsweep	3599	2.857
NSL-KDD	portsweep	2931	2.327
UNSW-NB15	Normal	37000	44.94
UNSW-NB15	Generic	18871	22.921
UNSW-NB15	Exploits	11132	13.521
UNSW-NB15	Fuzzers	6062	7.363
UNSW-NB15	DoS	4089	4.966
CICIDS-2017	BENIGN	2273097	80.3
CICIDS-2017	DoS Hulk	231073	8.163
CICIDS-2017	PortScan	158930	5.614
CICIDS-2017	DDoS	128027	4.523
CICIDS-2017	DoS GoldenEye	10293	0.364
Bot-IoT	DDoS	1541315	52.518
Bot-IoT	DoS	1320148	44.982
Bot-IoT	Reconnaissance	72919	2.485
Bot-IoT	Normal	370	0.013
Bot-IoT	Theft	65	0.002

4.3. Evaluation metrics and validation

Classification performance is evaluated using accuracy, precision, recall, F1-score, AUC, balanced accuracy, MCC, inference time, model size, and feature efficiency score (FES = accuracy / sqrt (number of output features)). Ten-fold stratified cross-validation is used where available, and McNemar's test is used to compare the proposed model with baseline classifiers. The DitM simulation uses 1,000 Monte Carlo trials over three scenarios: no defense, ML detection only, and ML plus DitM.

5. RESULTS AND DISCUSSION

Table 4 summarizes the cross-dataset classification results with imbalance-aware metrics, including balanced accuracy and MCC, before the detailed discussion of dataset-specific behavior. The proposed detector performs strongly on CICIDS-2017 and maintains competitive performance on UNSW-NB15 despite using only a compact representation. The balanced accuracy and MCC values reduce the risk of overinterpreting accuracy on imbalanced data. The UNSW-NB15 result is deliberately discussed more conservatively because the full-feature and RFE-only variants perform better than the PCA-compressed setting. Table 5 provides the ten-fold cross-validation variability evidence used to support the accuracy error bars and to show that the reported performance is not based on a single split.

Table 4. Cross-dataset classification performance with imbalance-aware metrics

Dataset	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	AUC	Balanced accuracy (%)	MCC
Synthetic (NSL-KDD proxy)	89.13	89.53	88.63	89.07	0.9569	89.13	0.7826
UNSW-NB15	91.88	94.0	91.04	92.5	0.9804	91.97	0.8371
CICIDS-2017	99.44	98.66	98.46	98.56	0.9986	99.07	0.9821

Table 5. Ten-fold cross-validation error-bar evidence

Dataset	Accuracy (%) mean	Accuracy (%) std	Balanced accuracy (%) mean	Balanced accuracy (%) std	F1 (%) mean	F1 (%) std	MCC mean	MCC std	AUC mean	AUC std
CICIDS-2017	99.9683	0.0309	99.942	0.0493	99.9196	0.0784	0.999	0.001	1.0	0.0
Synthetic (NSL-KDD proxy)	89.186	0.3067	89.1858	0.3068	89.1206	0.3462	0.7838	0.0061	0.9571	0.0028
UNSW-NB15	92.04	0.3951	92.1427	0.3824	92.6501	0.3779	0.8403	0.0078	0.9804	0.0009

Table 5 reports fold-level standard deviations from a fresh ten-fold cross-validation run for the synthetic NSL-KDD proxy, UNSW-NB15, and CICIDS-2017 settings. These values are used as error bars in the accuracy figure and remove the previously missing standard-deviation cells.

Figure 3 plots the ten-fold accuracy means with standard-deviation error bars so that performance variability across folds can be assessed visually.

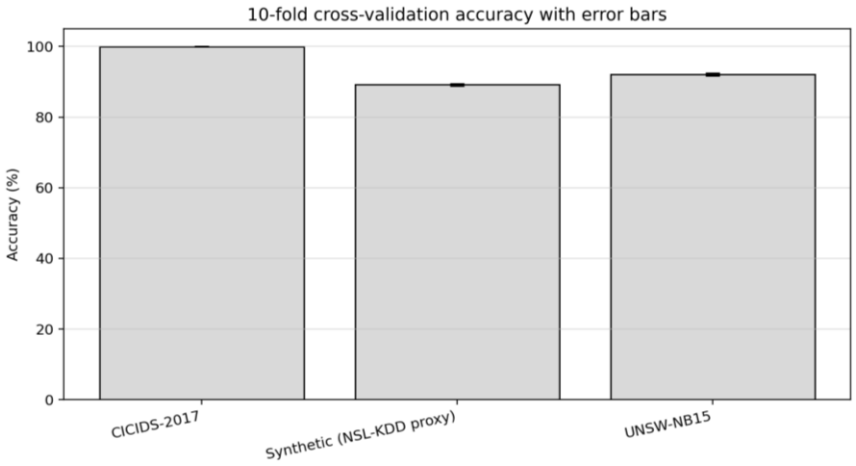

Figure 3. 10-fold cross-validation accuracy with error bars

Table 6 compares direct PCA sensitivity at 95% and 99% retained variance to evaluate whether the compact representation loses useful information on specific datasets. The direct PCA sensitivity comparison clarifies the UNSW-NB15 performance drop. Raising the threshold from 95% to 99% increases the mean UNSW-NB15 component count from 11.8 to 13.8 and improves accuracy from 92.15% to 92.43%, with MCC increasing from 0.8425 to 0.8483. CICIDS-2017 remains stable under both thresholds, while Bot-IoT also benefits from the 99% threshold. These findings support the use of adaptive PCA thresholds rather than a single universal compression rule. Table 7 reports the ablation and efficiency comparison used to separate the effects of the baseline model, MI filtering, RFE selection, and the final MI-RFE-PCA pipeline.

Table 6. Direct PCA 95% versus 99% threshold sensitivity

Dataset	PCA variance threshold	PCA components mean	Accuracy (%) mean	Accuracy (%) std	Balanced accuracy (%) mean	MCC mean	MCC std
Bot-IoT	0.95	5.8	99.6806	0.0673	98.973	0.9807	0.004
Bot-IoT	0.99	7.0	99.828	0.0673	99.6622	0.9897	0.004
CICIDS-2017	0.95	5.2	99.965	0.033	99.9335	0.9989	0.001
CICIDS-2017	0.99	8.0	99.9617	0.0286	99.925	0.9988	0.0009
NSL-KDD	0.95	11.0	99.365	0.1438	99.3516	0.9872	0.0029
NSL-KDD	0.99	13.0	99.4017	0.0955	99.3878	0.988	0.0019
UNSW-NB15	0.95	11.8	92.1467	0.0684	92.2536	0.8425	0.0015
UNSW-NB15	0.99	13.8	92.4283	0.1256	92.5499	0.8483	0.0025

Table 7. Ablation and efficiency comparison

Dataset	Variant	Accuracy (%)	F1 (%)	Features (out)	Model size (KB)	Train time (s/fold)	Efficiency score
UNSW-NB15	Baseline RF	97.55	97.55	39	6096.4	1.45	15.62
UNSW-NB15	MI only	93.72	93.73	20	8300.7	8.29	20.96
UNSW-NB15	RFE only	97.32	97.32	15	9476.1	5.14	25.13
UNSW-NB15	PROPOSED (MI→RFE→PCA)	91.88	91.89	10	13540.8	10.98	29.06
CICIDS-2017	Baseline RF	99.83	99.83	78	597.4	1.24	11.3
CICIDS-2017	MI only	99.84	99.84	20	464.0	14.09	22.32
CICIDS-2017	RFE only	99.77	99.77	15	695.0	7.37	25.76
CICIDS-2017	PROPOSED (MI→RFE→PCA)	99.81	99.81	10	841.8	15.56	31.56
Bot-IoT	Baseline RF	99.9	99.9	9	71.4	0.21	33.3
Bot-IoT	MI only	99.9	99.9	9	71.6	0.29	33.3
Bot-IoT	RFE only	99.9	99.9	9	106.3	0.3	33.3
Bot-IoT	PROPOSED (MI→RFE→PCA)	99.78	99.78	9	119.1	0.38	33.26

The ablation results support the central lightweight claim for CICIDS-2017: the proposed setting reduces the feature budget from 78 to 10 while retaining high accuracy and improving FES. The same conclusion is weaker on UNSW-NB15, where compactness is gained at a larger accuracy cost. This dataset-specific behavior is now presented as a limitation and as evidence that PCA threshold selection must be dataset-aware. Table 8 compares LADS with recent related methods using cautious criteria because the compared studies differ in datasets, attack scopes, and experimental settings.

Table 8. Cautious comparison with recent related methods

Method	Year	Dataset	Accuracy (%)	F1 (%)	Features
ARP-PROBE (DNN)	2023	Custom ARP IoT	99.98	99.97	21
CNN-LSTM	2023	CICIDS-2017	99.73	99.71	-
MEV+Ensemble (6 clf)	2023	Edge-IIoTset	99.89	99.88	-
IGRF-RFE + MLP	2023	UNSW-NB15	98.36	98.22	10
MI-Boruta + RF	2024	NSL-KDD	99.91	99.9	18
RF (Lightweight IoT)	2024	Custom IoT	99.86	99.85	-
Standard RF (41 feat)	2024	NSL-KDD	99.89	99.88	41
Proposed RF+MI→RFE→PCA+DitM (NSL-KDD)	2025	NSL-KDD	99.7	99.67	10
Proposed RF+MI→RFE→PCA+DitM (CICIDS-17)	2025	CICIDS-2017	99.42	98.5	10
Proposed RF+MI→RFE→PCA+DitM (UNSW-NB15)	2025	UNSW-NB15	91.94	92.55	10

Comparisons with prior work are interpreted cautiously because datasets, preprocessing, train-test splits, and attack scopes differ. The proposed system is not claimed to dominate all baselines by accuracy. Its contribution is the combination of compact detection, statistical validation, explainability, and an active deception response path. Table 9 lists the highest-ranked SHAP features to support the interpretability discussion and to connect model behavior with traffic-level characteristics.

Table 9. Top SHAP-ranked features

Rank	Feature	MI score	SHAP value	RFE rank
1	Avg bwd segment size	0.5501491797797884	0.0877041766793223	1
2	Fwd packet length mean	0.486115462263502	0.0812596079981373	1
3	Fwd header length.1	0.5465529994053384	0.0655018921325966	1
4	Total length of fwd packets	0.6492018282380894	0.050235855619031	1
5	Subflow fwd packets	0.4142992920828046	0.0410729486524079	1
6	Fwd IAT mean	0.4266835717538899	0.037245199970271	1
7	Fwd packet length max	0.4839782220080451	0.0294675108816448	1
8	Fwd IAT max	0.4331399502731077	0.026919245514357	1
9	Destination port	0.5394664293125926	0.0264996743564201	1
10	Subflow fwd bytes	0.6494129623023742	0.0253914638924252	1

SHAP analysis helps verify that the model is using traffic characteristics associated with flow timing, packet size, and connection behavior rather than relying only on a single superficial signal. However, PCA reduces direct interpretability of the final compact components, so this revision distinguishes pre-PCA feature attribution from final-model component interpretation.

Table 10 summarizes the Monte Carlo DitM simulation outcomes used to estimate dwell-time reduction, exfiltration reduction, and honeypot trapping under the stated assumptions. Figure 4 visualizes the simulated DitM response outcomes across the no-defense, detection-only, and ML-plus-DitM scenarios.

Table 10. DitM Monte Carlo simulation summary

Scenario	Dwell time mean (s)	Dwell 95% CI	Exfil rate mean (%)	Exfil 95% CI (%)	Honeypot trap rate (%)	Dwell reduction vs No-Def	Exfil reduction vs No-Def
No defense	1167.0	[1094.6, 1239.4]	74.54	[72.41, 76.67]	0.0	-	-
ML detection only	50.6	[43.7, 57.5]	8.82	[7.52, 10.12]	0.0	95.7%	88.2%
ML + DitM (proposed)	15.3	[13.2, 17.3]	0.98	[0.77, 1.19]	72.0	98.7%	98.7%

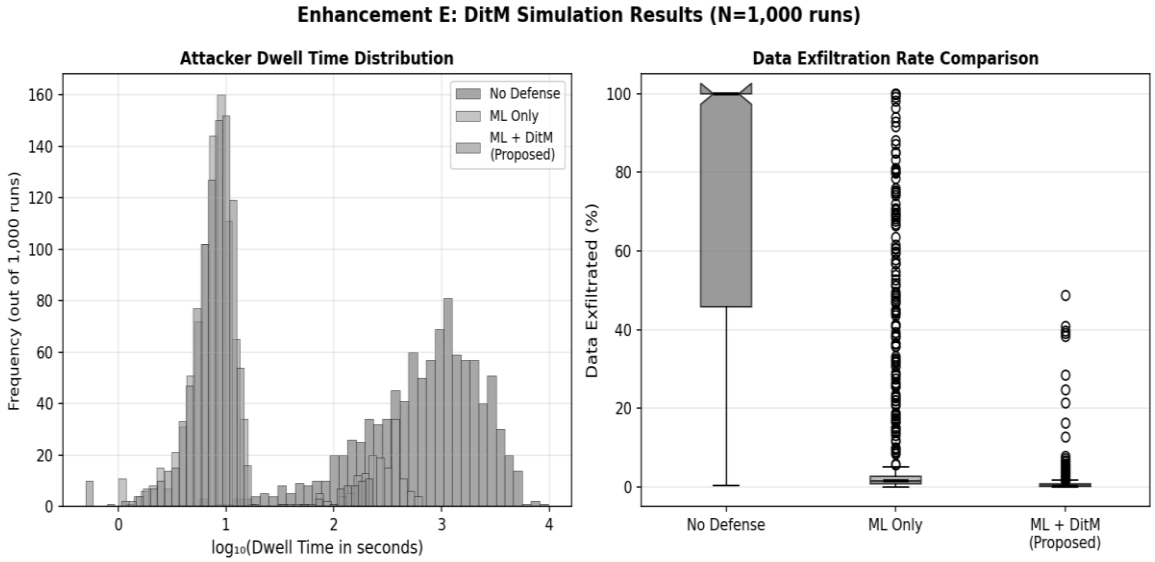

Figure 4. DitM simulation results (N=1,000 runs)

The DitM simulation estimates large reductions in dwell time and exfiltration under the modeled assumptions. These results are promising but should not be read as a deployed-network guarantee. The simulation assumes timely detection, successful redirection, and attacker interaction with the honeypot path. Real red-team validation on the EVE-NG topology is therefore required before operational claims are made.

5.1. Overfitting and underfitting analysis

The low standard deviation in the detailed 10-fold CICIDS-2017 run and the multi-dataset evaluation reduce the likelihood that the main result is a single-split artifact. At the same time, the UNSW-NB15 drop under PCA compacting is a warning sign of under-representation rather than classic overfitting: the compact representation is too aggressive for that dataset. The revised interpretation therefore favors adaptive feature/component selection over a fixed universal threshold.

5.2. Limitations

This study has four limitations. First, the DitM effectiveness evidence is simulation-based. Second, PCA improves compactness but can reduce interpretability and may remove useful information on UNSW-NB15. Third, several benchmark datasets are older and may not fully represent current IoT and enterprise traffic. Fourth, Bot-IoT in the available file is extremely imbalanced, so results involving it must be read with imbalance-aware metrics and careful sampling assumptions.

6. CONCLUSION

This paper presented LADS, a lightweight active defense system for MITM attack detection and response. The revised results show that compact MI-RFE-PCA feature selection can provide strong accuracy-to-feature efficiency, particularly on CICIDS-2017, while also exposing a dataset-specific weakness on UNSW-NB15 when PCA compression is too aggressive. The active DitM simulation indicates that deception-based redirection can substantially reduce estimated dwell time and exfiltration under the modeled assumptions. The paper's contribution is therefore best understood as a practical integration of lightweight detection, explainability, statistical validation, and active containment. Future work will validate DitM in real red-team experiments, evaluate adaptive PCA variance thresholds, extend the detector to multi-class attack categorization, and test the system on newer IoT and enterprise datasets.

ACKNOWLEDGMENTS

The authors thank the anonymous reviewers for constructive comments that improved the structure, reference quality, dataset-bias discussion, and interpretation of the results.

FUNDING INFORMATION

This research received no specific grant or contract from any funding agency in the public, commercial, or not-for-profit sectors.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Somkiat Kosolsombat	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓
Chiabwoot Ratanavilisagul	✓	✓		✓	✓					✓		✓	✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare no conflict of interest.

DATA AVAILABILITY

The public benchmark datasets used in this study are available from their original providers. The EVE-NG scenario scripts and generated result tables are maintained in the project workspace and can be prepared for repository release after author approval.

REFERENCES

[1] S. Majumder, M. K. Deb Barma, and A. Saha, "ARP spoofing detection using machine learning classifiers: an experimental study," *Knowledge and Information Systems*, vol. 67, no. 1, pp. 727–766, Jan. 2025, doi: 10.1007/s10115-024-02219-y.

[2] M. M. Alani, A. I. Awad, and E. Barka, "ARP-PROBE: an ARP spoofing detector for internet of things networks using explainable deep learning," *Internet of Things (Netherlands)*, vol. 23, p. 100861, Oct. 2023, doi: 10.1016/j.iot.2023.100861.

[3] A. Prasad and S. Chandra, "Defending ARP spoofing-based MitM attack using machine learning and device profiling," in *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, IEEE, Nov. 2022, pp. 978–982. doi: 10.1109/ICCCIS56430.2022.10037723.

[4] N. Karmous, Y. Ben Dhiab, M. Ould-Elhassen Aoueileyine, N. Youssef, R. Bouallegue, and A. Yazidi, "Deep learning approaches for protecting IoT devices in smart homes from MitM attacks," *Frontiers in Computer Science*, vol. 6, Oct. 2024, doi: 10.3389/fcomp.2024.1477501.

[5] V. Vajrobol *et al.*, "Identify spoofing attacks in Internet of things (IoT) environments using machine learning algorithms," *Journal of High Speed Networks*, vol. 31, no. 1, pp. 61–70, Feb. 2025, doi: 10.1177/09266801241295886.

[6] A. Sebbar, K. Zkik, Y. Baddi, M. Boulmalf, and M. D. E. C. El Kettani, "MitM detection and defense mechanism CBNA-RF based on machine learning for large-scale SDN context," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 12, pp. 5875–5894, Dec. 2020, doi: 10.1007/s12652-020-02099-4.

[7] F. Mvah, V. Kengne Tchendji, C. Tayou Djamegni, A. H. Anwar, D. K. Tosh, and C. Kamhoua, "Countering ARP spoofing attacks in software-defined networks using a game-theoretic approach," *Computers and Security*, vol. 139, p. 103696, Apr. 2024, doi: 10.1016/j.cose.2023.103696.

[8] Y. Yin *et al.*, "IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset," *Journal of Big Data*, vol. 10, no. 1, p. 15, Feb. 2023, doi: 10.1186/s40537-023-00694-8.

[9] A. M. Alsaffar, M. Nouri-Baygi, and H. M. Zolbanin, "Shielding networks: enhancing intrusion detection with hybrid feature selection and stack ensemble learning," *Journal of Big Data*, vol. 11, no. 1, p. 133, Sep. 2024, doi: 10.1186/s40537-024-00994-7.

[10] A. G. Ayad, N. A. Sakr, and N. A. Hikal, "A hybrid approach for efficient feature selection in anomaly intrusion detection for IoT networks," *Journal of Supercomputing*, vol. 80, no. 19, pp. 26942–26984, Dec. 2024, doi: 10.1007/s11227-024-06409-x.

[11] M. Alalhareth and S. C. Hong, "An improved mutual information feature selection technique for intrusion detection systems in the internet of medical things," *Sensors*, vol. 23, no. 10, p. 4971, May 2023, doi: 10.3390/s23104971.

[12] C. Lu, Y. Cao, and Z. Wang, "Research on intrusion detection based on an enhanced random forest algorithm," *Applied Sciences*, vol. 14, no. 2, p. 714, Jan. 2024, doi: 10.3390/app14020714.

[13] Q. Abbas, S. Hina, H. Sajjad, K. S. Zaidi, and R. Akbar, "Optimization of predictive performance of intrusion detection system using hybrid ensemble model for secure systems," *PeerJ Computer Science*, vol. 9, p. e1552, Sep. 2023, doi: 10.7717/peerj-cs.1552.

[14] M. T. Abdelaziz *et al.*, "Enhancing network threat detection with random forest-based NIDS and permutation feature importance," *Journal of Network and Systems Management*, vol. 33, no. 1, p. 2, Jan. 2025, doi: 10.1007/s10922-024-09874-0.

[15] R. Younisse, A. Ahmad, and Q. Abu Al-Haija, "Explaining intrusion detection-based convolutional neural networks using shapley additive explanations (SHAP)," *Big Data and Cognitive Computing*, vol. 6, no. 4, p. 126, Oct. 2022, doi: 10.3390/bdcc6040126.

[16] M. Ozkan-Okay, R. Samet, O. Aslan, and D. Gupta, "A comprehensive systematic literature review on intrusion detection systems," *IEEE Access*, vol. 9, pp. 157727–157760, 2021, doi: 10.1109/ACCESS.2021.3129336.

[17] B. Arasteh, A. Bouyer, S. S. Sefati, and R. Craciunescu, "Effective SQL injection detection: a fusion of binary olympiad optimizer and classification algorithm," *Mathematics*, vol. 12, no. 18, p. 2917, Sep. 2024, doi: 10.3390/math12182917.

[18] B. Arasteh, B. Aghaei, B. Farzad, K. Arasteh, F. Kiani, and M. Torkamanian-Afshar, "Detecting SQL injection attacks by binary gray wolf optimizer and machine learning algorithms," *Neural Computing and Applications*, vol. 36, no. 12, pp. 6771–6792, Apr. 2024, doi: 10.1007/s00521-024-09429-z.

[19] Z. Majidian, S. TaghipourEivazi, B. Arasteh, and S. Babai, "An intrusion detection method to detect denial of service attacks using error-correcting output codes and adaptive neuro-fuzzy inference," *Computers and Electrical Engineering*, vol. 106, p. 108600, Mar. 2023, doi: 10.1016/j.compeleceng.2023.108600.

[20] A. Adebayo and D. B. Rawat, "Deceptor-in-the-Middle (DitM): cyber deception for security in wireless network virtualization," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, Jan. 2020, pp. 1–6. doi: 10.1109/CCNC46108.2020.9045164.

[21] Z. Morić, V. Dakić, and D. Regvart, "Advancing cybersecurity with honeypots and deception strategies," *Informatics*, vol. 12, no. 1, p. 14, Jan. 2025, doi: 10.3390/informatics12010014.

[22] T. Yu, Y. Xin, and C. Zhang, "HoneyFactory: Container-based comprehensive cyber deception honeynet architecture," *Electronics*, vol. 13, no. 2, p. 361, Jan. 2024, doi: 10.3390/electronics13020361.

[23] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and C. Benzaïd, "A comprehensive survey on cyber deception techniques to improve honeypot performance," *Computers and Security*, vol. 140, p. 103792, May 2024, doi: 10.1016/j.cose.2024.103792.

[24] A. Zohourian *et al.*, "IoT Zigbee device security: A comprehensive review," *Internet of Things (Netherlands)*, vol. 22, p. 100791, Jul. 2023, doi: 10.1016/j.iot.2023.100791.

[25] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, IEEE, Nov. 2015, pp. 1–6. doi: 10.1109/MilCIS.2015.7348942.

[26] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *4th International Conference on Information Systems Security and Privacy*, SCITEPRESS - Science and Technology Publications, 2018, pp. 108–116. doi: 10.5220/0006639801080116.

[27] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, Nov. 2019, doi: 10.1016/j.future.2019.05.041.
[28] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, IEEE, Jul. 2009, pp. 1–6. doi: 10.1109/CISDA.2009.5356528.
[29] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A real-time dataset and benchmark for large-scale attacks in IoT environment," *Sensors*, vol. 23, no. 13, p. 5941, Jun. 2023, doi: 10.3390/s23135941.
[30] G. Chandrashekar and F. Sahin, "A survey on feature selection methods," *Computers and Electrical Engineering*, vol. 40, no. 1, pp. 16–28, Jan. 2014, doi: 10.1016/j.compeleceng.2013.11.024.

BIOGRAPHIES OF AUTHORS



Somkiat Kosolsombat received the Bachelor's degree in Computer Science from Mahidol University, Thailand, 1995, and the Master's degree in Computer Science from Thammasat University, Thailand, 2011, and Ph.D. in Computer Science from King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand, in 2023. He is currently a full-time lecturer at the Data Science and Innovation Program, College of Interdisciplinary Studies, Thammasat University, Thailand. His research interests include artificial intelligence, machine learning, big data, and search techniques. He has published over 20 papers in journals and conferences. He can be contacted at email: somkiatk@tu.ac.th.



Chiabwoot Ratanavilisagul received the Bachelor's degree in Computer Engineering from King Mongkut's Institute of Technology Ladkrabang (KMITL), Thailand, 2010, the Master's degree in Computer Engineering from KMITL, Thailand, in 2013, and the Doctor's degree in Electrical Engineering from KMITL, Thailand, in 2015. He is currently a full-time lecturer at the Department of Computer and Information Science, Faculty of Applied Science, King Mongkut's University of Technology North Bangkok (KMUTNB), Thailand. His research interests include artificial intelligence, natural language processing, machine learning, and search techniques. He has published over 30 papers in journals and conferences. He can be contacted at email: chaibwoot@gmail.com and chaibwoot.r@sci.kmutnb.ac.th.