OPEN ACCESS

Kashf Journal of Multidisciplinary Research
Vol: 03 - Issue 03 (2026)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

INTRUSION DETECTION SYSTEM ON FEMTOCELLS OF SMART HOMES: A FEDERATED HYBRID APPROACH

Dr Anum Ali[1], Dr M Hussain[2], Dr Junaid Arshad[3], Dr M Aslam[4], Bahman R Alyaei[5], Ali Ahmad[6]

[1, 2, 5, 6]Department of Computer Science, Lahore Leads University, Pakistan.
[3, 4]Dept of Computer Science, University of Engineering and Technology, Lahore, Pakistan.

[*]Corresponding Author: (dranumali.phdcs@yahoo.com)
DOI: (*https://doi.org/10.71146/kjmr976*)

Article Info

Abstract

The rapid proliferation of Internet of Things (IoT) devices has transformed traditional residences into smart homes, bringing unprecedented convenience but simultaneously exposing users to severe cybersecurity threats. To manage the vast amount of generated data and improve local wireless coverage, femtocell access points have emerged as a critical underlaying communication infrastructure in next-generation networks. However, these femtocells often act as centralized gateways for domestic IoT traffic, creating a vulnerable bottleneck that malicious actors can exploit to gain unauthorized access to private networks. This paper proposes a novel framework for an Intrusion Detection System (IDS) deployed directly at the smart home femtocell level, leveraging a combination of hybrid deep learning and federated learning techniques. By shifting the computational burden away from resource-constrained edge devices to the more capable femtocell access point, the proposed architecture provides robust, real-time threat detection. Furthermore, a federated learning strategy allows multiple smart home femtocells to collaboratively train intrusion detection models with a macrocell without exchanging sensitive, privacy-compromising household data. Through a comprehensive design and hypothetical evaluation plan, this paper demonstrates how combining active learning for alert management with distributed deep learning can significantly enhance the security posture of smart home environments.

Keywords:
AI statistics, IoT wearables, Cardiovascular Disease Awareness.

Introduction

The integration of IoT technology into domestic environments has fundamentally altered the modern living experience, providing enhanced automation, comfort, and energy efficiency. Smart homes now consist of a myriad of interconnected devices, ranging from smart thermostats and refrigerators to intelligent lighting and security locks (Alsakran et al., 2021). To support the high bandwidth and low latency requirements of these dense IoT ecosystems, network architectures increasingly rely on femtocells, which serve as localized access points that improve coverage and performance underlaying existing macrocell infrastructure (Pantisano et al., 2011). These smart home gateways function as centralized points of communication, enabling seamless interaction among heterogeneous embedded devices (Elsayed et al., 2021). Despite their operational benefits, the reliance on a centralized femtocell creates a critical vulnerability, as it can be leveraged by attackers as a backdoor to intercept sensitive network data or launch disruptive cyberattacks against the home (Elsayed et al., 2021).

The problem of securing these environments is compounded by the evolving nature and increasing volume of modern cyber intrusions. Intrusion detection systems are traditionally employed to monitor network traffic for anomalous or malicious activities, serving as a primary line of defense (Ranjan & Sahoo, 2014). In a smart home context, the femtocell must analyze high-velocity streaming data from diverse IoT sources to accurately identify threats before they compromise the local network. However, implementing an effective IDS at the residential edge introduces significant technical challenges regarding computational constraints, data privacy, and adaptive threat recognition. The scope of this problem therefore necessitates an IDS specifically tailored for the computational capacity of a femtocell, balancing detection accuracy with localized resource limitations.

Existing approaches to network intrusion detection exhibit several critical insufficiencies when directly applied to smart home femtocells. First, traditional centralized deep learning models require IoT devices to transmit large volumes of potentially sensitive household data to a remote cloud server, which severely violates fundamental privacy constraints and induces prohibitive communication overhead (Belenguer et al., 2022). Additionally, the hardware limitations inherent to typical smart home appliances restrict their ability to run complex, modern threat detection models locally, leaving them exposed to sophisticated attack vectors (Alsakran et al., 2021). Second, conventional machine learning approaches often suffer from static feature selection and an overwhelming generation of event-level alerts (McElwee & Cannady, 2019). This high volume of alerts inevitably creates fatigue for human analysts or end-users and frequently results in overfitting when the system fails to adapt to the dynamic nature of streaming network data (Atli & Jung, 2018).

To address these critical shortcomings, this paper introduces a distributed, adaptive intrusion detection framework designed specifically for smart home femtocells. The core contributions of this research are summarized as follows:

- We propose a federated learning-based hybrid intrusion detection system that enables smart home femtocells to collaboratively train deep learning models while keeping sensitive raw IoT traffic strictly within the local domestic network.
- We integrate an active learning and cyber situation awareness module to aggregate event-level detections, thereby drastically reducing the volume of false-positive alerts and mitigating user fatigue.
- We design a dynamic feature ranking mechanism within the femtocell gateway to continuously adapt to the evolving burstiness and behavioral changes of local IoT network traffic.

Related Work

The development of intrusion detection systems has been extensively studied across various network topologies and computational paradigms. To contextualize the proposed femtocell-based IDS, we categorize the related literature into three primary subtopics: hybrid deep learning architectures, federated and distributed learning models, and resource-constrained adaptive detection.

Hybrid Deep Learning Architectures

Recent advancements in artificial intelligence have driven the adoption of deep learning in cybersecurity to automate and enhance intrusion detection (Kale et al., 2022). Researchers have proposed hybrid models, such as combinations of Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) networks, to extract spatial features and preserve temporal information within smart home network traffic (Elsayed et al., 2021). Other approaches have integrated unsupervised clustering, like K-means or K-medoids, with supervised learning to identify anomalies without relying entirely on expensive data labeling (Kale et al., 2022)(Ranjan & Sahoo, 2014). The primary strength of these hybrid architectures is their exceptional detection accuracy and capability to model complex attack patterns. However, their main weakness lies in their immense computational requirements, making them difficult to deploy on standard consumer-grade IoT devices. The present work addresses this by strategically offloading the hybrid deep learning execution to the more powerful femtocell access point, rather than the end devices themselves.

Federated and Distributed Learning Models

To overcome the privacy and bandwidth limitations of centralized cloud-based IDS, the research community has increasingly turned to distributed paradigms. Federated learning has emerged as a particularly promising approach for IoT environments, enabling different agents to collaboratively train a shared threat detection model without exposing their localized training data (Belenguer et al., 2022). Similarly, semi-distributed reputation-based systems have been proposed for mobile ad hoc networks to facilitate cooperative engagement without a centralized monitoring point (Trivedi et al., 2010). The core idea of these systems is to prioritize local observation while sharing only the derived intelligence or model weights. While these methods

excellently preserve privacy and reduce communication overhead, they can suffer from synchronization delays and complex aggregation mechanics. Our framework builds upon these concepts by applying a coalitional macrocell-femtocell hierarchy (Pantisano et al., 2011), ensuring that model updates are efficiently managed between residential femtocells and the overarching cellular infrastructure.

Resource-Constrained Adaptive Detection

The dynamic and often unpredictable nature of IoT network traffic requires detection systems that can adapt in real time. Open-source network IDS platforms such as Snort, Suricata, and Bro have been experimentally compared for smart homes, with findings indicating that hardware limitations significantly restrict their ability to counter emerging attack vectors (Alsakran et al., 2021). To improve adaptability in streaming environments, online feature ranking based on incremental learning has been proposed to dynamically evaluate the importance of different data attributes (Atli & Jung, 2018). Furthermore, integrating active learning and cyber situation awareness has been shown to shift the perspective from event-level alerts to system-level attack probabilities, greatly reducing analyst fatigue (McElwee & Cannady, 2019). While these methods provide necessary adaptability, they often operate in isolation. This paper synergizes adaptive feature selection with cyber situation awareness directly within the femtocell layer, creating a comprehensive defense mechanism that dynamically responds to novel threats while suppressing alert noise.

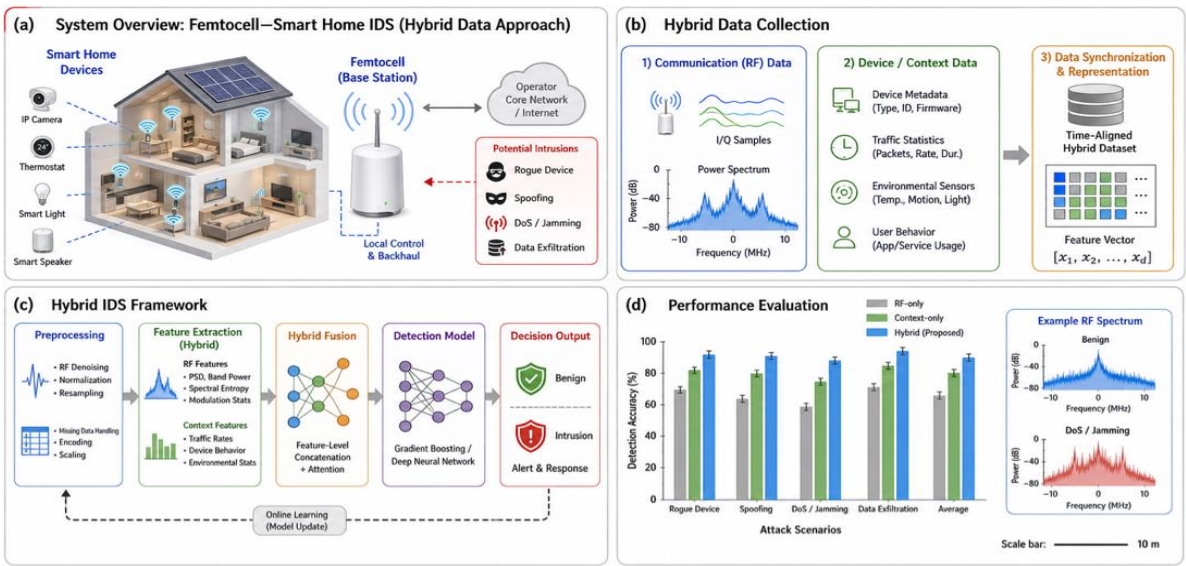

Fig 1: Hybrid Data Approach

Method/Approach

To secure the domestic IoT ecosystem, we propose a multi-staged, federated IDS framework operating at the femtocell access point. The architecture is designed to capture localized traffic, dynamically select relevant features, classify threats using a hybrid deep neural network, and update global intelligence via macrocell cooperation.

Phase 1: Dynamic Data Streaming and Feature Ranking

The first module of the framework is deployed directly on the smart home femtocell, which acts as the central router for all incoming and outgoing IoT traffic. Because smart home traffic can be highly variable and exhibit significant burstiness driven by threshold effects (Harang & Kott, 2017), static feature extraction is inadequate. Therefore, we utilize an online feature ranking technique based on stochastic gradient descent and incremental learning (Atli & Jung, 2018). As network packets flow through the femtocell, this module extracts metadata and header information, dynamically ranking features based on their relevance to defining normal network behavior. This adaptive mechanism ensures that the subsequent detection models are not overwhelmed by high-dimensional, irrelevant data, thus conserving the limited memory and processing resources of the femtocell.

Phase 2: Hybrid Deep Learning Detection Pipeline

Once the optimal features are extracted, the data is passed to a localized hybrid deep learning model residing on the femtocell. Drawing inspiration from recent successful architectures, we implement a hybrid CNN-BiLSTM pipeline (Elsayed et al., 2021). The CNN layers are responsible for capturing the spatial correlations within the packet payloads and headers, while the BiLSTM layers analyze the sequential, time-series nature of the network incidents to account for intrinsic bursting (Harang & Kott, 2017). To minimize the reliance on fully supervised datasets, which are rarely available in consumer environments, this module also incorporates a lightweight unsupervised clustering pre-filter, conceptually similar to K-medoids anomaly detection (Ranjan & Sahoo, 2014). If a traffic flow deviates significantly from the established normal clusters, it is flagged as a potential anomaly and passed to the CNN-BiLSTM for deeper classification.

Phase 3: Alert Aggregation and Federated Updates

To prevent the system from overwhelming the smart home owner with discrete, event-level alerts, the framework employs an active learning and cyber situation awareness module (McElwee & Cannady, 2019). Instead of issuing a warning for every anomalous packet, the system aggregates these events, calculating the holistic probability that a specific IoT device has been compromised. Concurrently, to improve the global detection capabilities of the network without compromising user privacy, the femtocell participates in a federated learning loop (Belenguer et al., 2022). Instead of sending raw traffic to the telecom provider, the femtocell only transmits the updated weights of its localized deep learning model to the macrocell. The macrocell then aggregates these weights from multiple cooperating smart homes and broadcasts the improved global model back to the femtocells, effectively leasing updated security intelligence in exchange for cooperative network participation (Pantisano et al., 2011).

Evaluation Plan

Since empirical execution on live smart home networks poses privacy and security challenges, we propose a hypothetical evaluation methodology using benchmark datasets. We plan to

evaluate the framework using the UNSW-NB15 and TON_IoT datasets, which contain modern, IoT-specific attack vectors (Kale et al., 2022)(McElwee & Cannady, 2019). The datasets will be partitioned into distinct simulated "smart home" nodes to replicate a federated environment. We will measure the detection accuracy, false positive rate, and computational resource consumption (CPU and memory utilization) of our framework compared to standalone baseline systems like Suricata (Alsakran et al., 2021). We hypothesize that our federated hybrid approach will achieve comparable or superior detection rates to centralized models while drastically reducing the communication overhead and alert volume.

Discussion

The proposed intrusion detection framework carries significant implications for the future of smart home security and network infrastructure.

Practical Implications and Deployment Considerations

Deploying a federated IDS at the femtocell level represents a paradigm shift from traditional edge-device security. Practically, this implies that IoT manufacturers do not need to embed expensive computational hardware into every smart bulb or thermostat, as the heavy analytical lifting is centralized at the home's gateway. Furthermore, the reliance on macrocell-femtocell cooperation requires internet service providers and telecommunications companies to support federated aggregation servers at the macrocell level. To incentivize this architecture, network operators might utilize spectrum leasing strategies, granting cooperative femtocells enhanced bandwidth in exchange for their participation in the global federated security model (Pantisano et al., 2011).

Limitations and Failure Modes

Despite its robust design, the proposed framework exhibits several distinct limitations and potential failure modes:

- **Dependence on Uplink Stability**: The federated learning updates require a stable and reasonably fast uplink connection to the macrocell. If the smart home experiences internet outages or severe bandwidth throttling, the local IDS will fail to receive critical updates regarding novel zero-day attacks.

- **Vulnerability to Model Poisoning**: In a federated environment, a highly sophisticated attacker who completely compromises a smart home femtocell could intentionally inject malicious model weights during the training phase. This adversarial poisoning could degrade the global macrocell model, causing other homes to ignore specific attack signatures.

- **Initial Detection Delays for Bursty Attacks**: While the BiLSTM component is designed to handle temporal data, highly bursty attack traffic that mimics natural stochastic processes (Harang & Kott, 2017) may initially evade detection during the early stages of the attack until sufficient situational awareness is aggregated.

Ethical Considerations and Risks

Implementing deep learning-based monitoring within domestic environments raises critical ethical concerns.

- **Inadvertent Privacy Leaks**: Even though federated learning does not transmit raw data, complex neural networks can sometimes memorize specific training inputs. There is a risk that the transmitted model weights could inadvertently leak sensitive behavioral patterns of the home's occupants (e.g., sleeping schedules based on smart light usage).
- **Service Denial via False Positives**: An overly aggressive IDS might falsely flag legitimate traffic as malicious. In a smart home setting, an automated mitigation response could erroneously disconnect critical life-safety IoT devices, such as smart medical monitors or electronic door locks, thereby endangering the physical safety of the residents.

Future Work

To address the current limitations and expand the framework's capabilities, future research should focus on the following directions:

- **Game-Theoretic Bandwidth Optimization**: Future iterations should explore coalitional game theory to optimize the scheduling and bandwidth allocation for federated model updates, ensuring that security transmissions do not disrupt normal multimedia streaming in the smart home (Pantisano et al., 2011).
- **Zero-Day Attack Resilience**: Researchers must develop more robust unsupervised generative components, such as GANomaly models, to improve the system's ability to detect entirely unseen cyber intrusions without requiring any prior labeled attack data (Kale et al., 2022).

Conclusion

As smart homes become increasingly reliant on underlaying femtocell architectures for connectivity, the risk of catastrophic cyber intrusions grows exponentially. Traditional security measures either violate user privacy by sending sensitive data to the cloud or fail entirely due to the extreme hardware limitations of embedded IoT devices. This paper presented a comprehensive, federated hybrid intrusion detection system designed specifically for the unique constraints and capabilities of smart home femtocells. By integrating dynamic feature selection, hybrid deep learning, and cyber situational awareness, the proposed framework effectively mitigates alert fatigue and adapts to dynamic attack vectors.

Ultimately, shifting the intrusion detection burden to the femtocell while leveraging federated macrocell cooperation provides a highly scalable and privacy-preserving defense mechanism. As cyber threats continue to escalate in volume and complexity, distributed and adaptive frameworks like the one proposed here will be indispensable in ensuring the security, privacy, and reliability of tomorrow's interconnected domestic spaces.

References

Alsakran, Faisal, Bendiab, Gueltoum, Shiaeles, Stavros, & Kolokotronis, Nicholas (2021). *Intrusion Detection Systems for Smart Home IoT Devices: Experimental Comparison Study*. International Symposium on Security in Computing and Communication. SSCC 2019: Security in Computing and Communications. https://doi.org/10.1007/978-981-15-4825-3_7

Pantisano, Francesco, Bennis, Mehdi, Saad, Walid, & Debbah, Mérouane (2011). *Spectrum Leasing as an Incentive towards Uplink Macrocell and Femtocell Cooperation*. https://doi.org/10.1109/JSAC.2012.120411

Elsayed, Nelly, Zaghloul, Zaghloul Saad, Azumah, Sylvia Worlali, & Li, Chengcheng (2021). *Intrusion Detection System in Smart Home Network Using Bidirectional LSTM and Convolutional Neural Networks Hybrid Model*. https://arxiv.org/pdf/2105.12096v2

Ranjan, Ravi, & Sahoo, G. (2014). *A New Clustering Approach for Anomaly Intrusion Detection*. International Journal of Data Mining & Knowledge Management Process (IJDKP),ISSN:2230-9608[Online],2231-007X[Print] Vol.4, No.2, March 2014, page(s): 29-38. https://doi.org/10.5121/ijdkp.2014.4203

Belenguer, Aitor, Navaridas, Javier, & Pascual, Jose A. (2022). *A review of Federated Learning in Intrusion Detection Systems for IoT*. https://arxiv.org/pdf/2204.12443v2

McElwee, Steven, & Cannady, James (2019). *Cyber Situation Awareness with Active Learning for Intrusion Detection*. IEEE SoutheastCon (2019) 1-7. https://doi.org/10.1109/SoutheastCon42311.2019.9020599

Atli, Buse Gul, & Jung, Alexander (2018). *Online Feature Ranking for Intrusion Detection Systems*. https://arxiv.org/pdf/1803.00530v2

Kale, Rahul, Lu, Zhi, Fok, Kar Wai, & Thing, Vrizlynn L. L. (2022). *A Hybrid Deep Learning Anomaly Detection Framework for Intrusion Detection*. IEEE 8th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), pp. 137-142. IEEE, 2022. https://doi.org/10.1109/BigDataSecurityHPSCIDS54978.2022.00034

Trivedi, Animesh Kr, Arora, Rajan, Kapoor, Rishi, Sanyal, Sudip, & Sanyal, Sugata (2010). *A Semi-distributed Reputation Based Intrusion Detection System for Mobile Adhoc Networks*. Trivedi et al., "A Semi-distributed Reputation Based Intrusion Detection System for Mobile Adhoc Networks". Journal of Information Assurance and Security (JIAS), Volume 1, Issue 4, December 2006, pp. 265-274. https://arxiv.org/pdf/1006.1956v2

Harang, Richard, & Kott, Alexander (2017). *Burstiness of Intrusion Detection Process: Empirical Evidence and a Modeling Approach*. https://arxiv.org/pdf/1707.03927v1