Advanced International Journal of Multidisciplinary Research

E-ISSN: 2584-0487
editor@aijmr.com

Volume 1, Issue 1, July-August 2023

CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

Distributed Intrusion Detection for Ultra-Mobile 6G Edge Architectures

Adedayo Bello

Cyber Security & Network Engineer
Institution: Signature Bank
Lagos, Nigeria

Abstract:
The advent of sixth generation (6G) of wireless communications network is anticipated to bring an unprecedented level of movement, intelligence, and interconnections through ultra-dense edge computing, artificial intelligence (AI), and heterogeneous access technologies. Unlike generations that have come before it, 6G networks will include ultra-mobile environments where devices such as autonomous vehicles, unmanned aerial vehicles, extended reality platforms and cyber-physical systems are constantly changing network attachment points, while demanding ultra-low latency and high reliability. These characteristics make the network infrastructures considerably more complex when it comes to intrusions and detection. Traditional centralized intrusion detection systems (IDS) are no longer effective in such environments, due to the limited scalability, delayed response, and limited ability to provide contextual awareness.

This research is concerned with distributed intrusion detection as a basic security mechanism for ultra-mobile 6G edge architectures. By decentralizing the logic of detecting these threats, and allowing for cooperative intelligence between edge nodes, distributed intrusion detection systems (D-IDS) are potentially able to offer in-time, scalable, and context-aware protection from new types of cyber threats. The article examines the shifting threat environment of edge environments that 6G will encounter, points to the shortcomings of centralized security concepts using edge environments and proposes a structured model for distributed intrusion detection adapted to ultra-mobile scenarios. Based on new research in edge computing, federated learning and AI secure, the study discusses how distributed IDS architectures help improve resilience and cut detection time and improve threat visibility while maintaining privacy. The article provides a useful and updated basis for future work and practical implementation of intrusion detection mechanisms for next-generation 6G networks.

Keywords: 6G Networks; Distributed Intrusion Detection; Edge Computing; Ultra-Mobile Networks; Federated Learning; AI-Based Security; Network Defense.

1. INTRODUCTION

Wireless communication networks are in a process of transformative evolution with ongoing research and development of wireless communication networks moving beyond the fifth-generation (5G) communication networks to sixth-generation (6G) systems. While 5G focused on enhanced mobile broadband, massive machine type of communication, and ultra-reliable low latency services, 6G is envisioned as a full intelligent ultra-mobile and deeply integrated cyber-physical ecosystem. 6G networks

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

are expected to support extreme data rates, sub-millisecond latency, pervasive artificial intelligence and seamless integration of terrestrial, aerial, and non-terrestrial network components.
A defining characteristic of 6G is the most important role of edge computerization. Computation, storage and intelligence are now all being moved away from centralized cloud infrastructures and towards distributed edge nodes, near the end users and the source of data. This shift in architecture opens up the possibility for real-time offering and context-aware applications as well as some huge security loopholes. Edge nodes are resource limited, geographically dispersed and exposed in dynamic operating conditions, making them vulnerable to a whole range of cyber threats (Alasmary et al., 2022).

Security concern is heightened even more by ultra-mobility, and 6G is distinct in this respect compared to the previous generations. In ultra-mobile environments, devices can often move around the network domains dynamically modifying their connectivity, trust relationships and traffic patterns. Autonomous vehicles, drones, wearable devices, industrial robots are examples of such moves, in which devices communicate with device of several edge nodes, and do so in a very fast time. This constant mobility makes security monitoring difficult and produces the traditional understanding of stable networks topologies and persistent connections (Dang et al., 2022).

Intrusion detection systems (IDS) are a vital part of any cybersecurity structure, their job is to detect any malicious activity that gets past any preventative. Conventional IDS architectures are very much centralised, with aggregated data analysis at a core location on the network. While effective in relatively static enterprise networks, centralized IDS have major limitations in 6G edge environments. There are challenges such as high data volumes, latency-sensitive applications and intermittent connectivity that make centralized monitoring inefficient and in some cases impossible (Abdelwahab et al., 2021).

One of the main limitations of the centralized IDS in ultra-mobile 6G networks is the detection time. Transmitting the monitoring data from distributed edge nodes to a central analyzer makes them suffer from delays and from the requirements of 6G applications to operate as real-time data. In the context of safety, for example autonomous power steering or a remotely operated healthcare system where punctual intrusion detection is mandatory, delay in detecting intrusion can have severe consequences. In addition, centralized systems tend to act as bottlenecks as the number of connected devices and edge nodes increase dramatically.

Another limitation is the lack of contextual awareness of a local context. Centralized IDS usually run on aggregated traffic data thus losing the fine-grained context associated with role of devices, mobility and application behavior. In ultra mobile environment, this local context plays a critical role in classifying whether the mobility induced anomaly is real anomaly or is the malicious activity (Wang et al., 2021). As a consequence, centralized approaches are likely to exhibit a high false-positive rate and a reduced detection accuracy.

To overcome these difficulties, advocates of distributed intrusion detection systems (D-IDS) have become more common research areas. Distributed IDS architecture computes the detection capabilities in a decentralized way across multiple nodes, where each node can conduct its own analysis cooperatively with its peers in order to identify distributed and coordinated attacks. This is a natural fit with the decentralized and intelligent design methodology of 6G networks where edge nodes are expected to work autonomously but work together.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

Distributed intrusion detection has a number of advantages in ultra-mobility 6G edge environments. First, it allows for real-time local detection, hence reducing latency levels by analyzing threats near their source. Second, it provides better scalability and resilience, i.e., detection is not based on one centralised component. Third, by controlled information sharing, distributed IDS can obtain a global situational awareness without an excessive data aggregation and privacy risks (Nguyen et al., 2022).

The growing complexity of AI and machine learning only adds further weight to the argument on distributed intrusion detection. AI-based models at the edge are able to learn the behaviour patterns locally and can adapt to the dynamic environment. Collaborative learning paradigms such as, but not limited to, federated learning, gives privacy to edge nodes by letting them share updates to their models instead of sharing raw data while optimizing the strength of the detection network as a whole (Li et al., 2020). However, they also provide new challenges such as poisoning models and trust management that have to be handled in the design of distributed IDS frameworks.

Despite the interest, distributed intrusion detection for ultra-mobile 6G edge architectures is an emerging research area. Many of the existing studies address edge security or distributed IDS in isolation, without taking the full impact of extreme mobility, AI-native control planes and heterogeneous network components to be expected in 6G systems. There is therefore a need for a comprehensive and up-to-date analysis which synthesizes these dimensions into a coherent security framework.

Research Objectives

The main goal of this research is to look into how distributed intrusion detection can be used to effectively secure ultra-mobile 6G edge architectures. Specifically, the following are the objectives of the article:

- Analyze the cybersecurity issues that are specific to Ultra-mobile 6G edge environments.
- Evaluate the drawback of centralized approaches to intrusion detection in such situations.
- Propose a structured distributed intrusion detection framework to bring closer with 6G design principles;
- Identify enabling technologies, open issues and future studies.

2. LITERATURE REVIEW

2.1 Evolution of Security Requirements 5G to 6G

The progression from 5G to 6G networks has been widely acknowledged as moving from a connection-oriented network architecture to an intelligence and service-focused network architecture. While 5G security frameworks, especially virtualization isolation, network slicing protection, as well as software defined networking (SDN) security, are suggested, these security mechanisms are inadequate for 6G systems complexity and autonomy (Zhang et al., 2019; Dang et al., 2022). Researchers point out that 6G networks will work with deep integration of artificial intelligence, non-terrestrial network and massive intelligence at the edge, which fundamentally redefines the attack surface.

Recent studies believe that security in 6G will and should be proactive, adaptive, and distributed rather than reactive and centralized (Saad et al., 2020; Akyildiz et al., 2020). Ultra-low latency requirements and extreme mobility precludes the use of centralized security monitoring or delayed threat correlation. As a result, intrusion detection will need to be rethought as a native and edge-centric function implemented across the network fabric.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

2.2 Edge Computing and Issues with Security

Edge computing is one of the backbone of 6G architecture, to perform computation and analytics gain close to data sources. While this decentralization makes them better and more scalable, it also presents a cable of serious security issues. Edge nodes often work in an untrusted or semi-trusted environment, are resource limited, and frequently subjected to physical access or tampering (Shi et al., 2016; Roman et al., 2018).

Security research constantly hampers visibility loss as one of the major problems that edge environments face. Centralized monitoring has a hard time maintaining a comprehensive situational awareness based on data processing fragmented across thousands of edge nodes. For the same reason, the dynamic movement of services and workloads over edge locations makes it more challenging to trace and analyze attacks forensically (Alasmary et al., 2022).

These problems have been a stimulus to development of security mechanisms that are native to the edge of the network, such as local intrusion detection and anomaly monitoring. However isolated edge-based detection systems often suffer from a lack of contextual understanding and the ability to detect any coordinated attack that did span as many as several nodes or domains. This limitation highlights the divide for distributed architectures of intrusion detection, based on a combination of local autonomy and collaborative intelligence.

2.3 Intrusion Detection Systems: What Are They and What Are Their Limitations?

Intrusion detection systems are generally classified into signature-based, anomaly-based and hybrid intrusion detection systems. Signature-based IDS use known attack patterns and have low rates of false positives but fail to detect zero-day attacks. Anomaly or behavior-based IDS are designed to identify the detections of deviations from the normal behaviour and are more suited in detecting the novel threats, however they can have high false positive rate (Buczak & Guven, 2016).

Centralized architectures of IDS collect monitoring data at a central point for analysis. While effective in a stable enterprise network, centralized IDS suffer from serious limitations in ultra-mobile environments. The studies point out problems associated with scalability, detection latency and single points of failure, especially in large-scale distributed systems (Mitchell & Chen, 2014). In 6G networks, where multiple devices join and leave the network and connectivity is likely to be intermittent, centralized IDS is no longer practical.

Distributed Intrusion Detection Systems (D-IDS) counter these restrictions by having the detection logic spread to many nodes. An early example of work on D-IDS was that it exhibited enhanced fault tolerance and scalability with cooperative detection agents (Snapp et al. 1991). Recent research revives D-IDS in the context of cloud, IoT, and edge environment with a focus on being suitable for decentralized and dynamic infrastructures (Abdelwahab et al., 2021).

2.4 Distributed Identifier Location Identifier System (IDS) in Edge & IoT Environment

The application of distributed IDS to the edge and IoT environment has attracted much attention in recent years. Researchers take advantage of architectures in which each edge node does local detection, and shares the alerts or summary of its behavior with its peers. This approach allows latency reduction of the detection, and thus allows for early response which is crucial in time-sensitive applications (Mitchell and Chen, 2014; Abdelwahab and others, 2021).

However, the existing distributed IDS solutions frequently make certain assumptions about relatively static network topologies or limited mobility. In contrast, ultra-mobile 6G environments are characterised by continuous changes in node connectivity, trust relationship and service context. Wang et al. (2021)

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

observe that mobility leads to benign anomalies that look like attacks, making detection difficult and producing more false positive results if a proper context is not taken into consideration.
Furthermore, coordination overhead as well as trust management are issues that need to be solved for distributed IDS. Excessive information exchanging may prove to be too much for network resources, whereas not enough information can deteriorate the detection. It is of special importance to highlight the importance of adaptive information sharing and reputation-based trust mechanisms to balance these trade-offs during the last weeks (Nguyen et. al, 2022).

2.5 Intruder Detection using AI on the border.
Artificial intelligence techniques and machine learning techniques have become crucial to the study of intrusion detection in recent years. Deep learning, ensemble models, and reinforcement learning have shown impressive success in identifying complicated and changing attack patterns (Buczak & Guven, 2016). In edge environments, AI-powered IDS can learn the behavior of individual environments and adapt to different situations.
However, taking the model of applications to the edge presents new challenges. Edge nodes in many cases have limited computational resources, and this poses challenges for models since they need to be lightweight and use efficient inference mechanisms (Chen et al., 2020). Additionally, AIs are also sensitive to adversarial attacks, such as data poisoning and evasion techniques, which is especially unsafe in distributed learning contexts (Biggio & Roli, 2018).
Recent research work has stressed the need for robust and explainable AI in security-critical applications, in particular in 6G networks that have potential to directly impact safety and service availability due to automated decision-making (Dang et al., 2022). These considerations restrict further the impetus to implement trust-oriented and collaborative learning mechanisms in distributed IDS frameworks.

2.6 Federated Learning & Collaborative Detection
Federated learning has become one such interesting paradigm for collaborative intrusion detection for distributed environments. In federated IDS architectures, locally observed data is used to train the local detection model at the edge nodes that periodically share updates to the model, instead of raw data. This approach guarantees data privacy, will lower down on communication overhead, and will make it possible to be continuously adapted to the changing threats (Li et al., 2020).
Recent surveys emphasize on the usability of federated learning in IoT and edge security showing superior accuracy and scalability over centralized approaches to training learning models (Nguyen et. al., 2022). In ultra-mobile 6G environments in particular, the problem of federated learning appears to be a strong focal point: As federated machine learning allows for some level of intermittent connectivity, it facilitates decentralized control.
Nevertheless, there are new security challenges in federated learning such as model poisoning, free-riding, and heterogeneous data distributions. For this reason, research has recently moved to secure aggregation, the detection of anomalies at the model-update level and the reputation-based weighting of contributions to reduce these risks (Fung et al., 2020).

2.7 Mobility and Context - Awareness Intrusion Detection
Mobility is a characteristic of 6G networks and holds great implications for intrusion detection. Traditional IDS are sometimes based on static thresholds and fixed behavior profiles, which are insufficient for an environment where normal behavior changes depending on location, time and service context (Wang et al., 2021).

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

Context-aware intrusion detection takes into account other information, such as the mobility patterns and the role of devices and applications, to enhance the accuracy of intrusion detection. Recent studies have argued that 6G network will make room for rich context sensing and the use of digital twins to increase security analytics capability by providing predictive and holistic views of network behavior (Zhang et al., 2023).

Distributed IDS architectures are well suited to make use of such context: local nodes have immediate access to contextual information that may be lost during centralized aggregation. Collaborative sharing of alerts with context-awareness an additional optimizing the ability to detect coordinated and mobility driven attacks.

2.8 Research Deficits and the Motivation

The reviewed literature shows the significant improvement in edge security, distributed intrusion detection and artificial intelligence based defense mechanism. However, several gaps remain. First, most of the current work is either 5G, IoT or static edge scenarios, and does not fully address the extreme mobility and integration of intelligence which will be expected from 6G networks. Second, a lot of distributed IDS proposals are missing the architectural clarity in areas such as coordination, trust management and scale under ultra-mobile conditions.

Moreover, there are hardly any studies that offer a unified framework combining distributed intrusion detection, federated learning and mobility-aware context analysis for 6G edge architectures in particular. This gap provides motivation for the current research which aims to consolidate these dimensions into an integrated and future-ready security framework.

3. RESEARCH METHODOLOGY, SYSTEM MODEL

3.1 Research Methodology

This study uses a design science research (DSR) method, which is commonly applied in information systems and cybersecurity studies to design and analyze new architectures, models and frameworks. Design science is especially suited to this type of research as the goal is not to observe and explain security phenomena but to design and reason about a security artifact - here, the distributed intrusion detection framework designed for ultra-mobile 6G edge architectures.

The methodology is in four structured stages of.

First, the problem identification stage lays the basis of the inadequacy of centralized intrusion detection in ultra-mobile 6G environments based on the above literature review. Second, the requirements definition stage develops design goals based on the characteristics of 6G networks, such as extreme mobility, edge intelligence and decentralized control. Third, artifact design stage is used to create a system model for distributed intrusion detection, including specifications of detection agents, collaboration mechanisms and learning paradigms. Finally, the evaluation stage performs analytical assessment of the proposed model by mapping it against the known classes of attack and mobility scenarios and operational constraints reported in the literature (Akyildiz et al., 2020; Alasmary et al., 2022).

Rather than simulation or tests of the testbeds, which is still limited when it comes to 6G research at an early stage, this work focuses on conceptual rigour and analytical validation. This type of approach is in line with latest 6G security research where architectural feasibility and system logic are determined prior to conducting large-scale empirical evaluation.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

3.2 Design Assumptions and System Requirements

The proposed distributed intrusion detection system (D-IDS) is designed using a set of assumptions that align with the realistic 6G deployment scenarios.

First, the network is composed of the large population of heterogeneous edge nodes such as mobile devices, vehicles, UAVs, sensors, and micro-edge servers. These nodes have very different computational power, energy capacity and the connection stability. Second, the mobility of nodes is assumed to be continuous and multi-dimensional, which includes horizontal mobility among access points, and vertical mobility among network layers and domains.

Third, the system assumes that partial trust is an assumption between participating nodes. While mass collusion is unlikely, individual nodes may be vulnerable to compromise, malfunction or malicious action. Therefore, the intrusion detection framework has to be tolerant about unreliable or adversarial participants. Fourth, the system is based on the availability of basic cryptographic mechanisms for secure communication and identity verification as envisioned in 6G security architectures (Dang et al., 2022).

From these assumptions, a number of important system requirements follow:

- Low-latency detection and near-real-time, edge-ended response.
- Scalability, being able to support thousands / millions of mobile nodes.
- Mobility awareness, Dynamic context adaptation of the detection logic.
- Resilience, Avoiding Single Points of Failure.
- Privacy preservation, minimizing the sharing out of raw data

These requirements are the basis of the proposed distributed IDS model.

3.3 Model of Distributed Intrusion Detection System

The proposed D-IDS model conceptualizing 6G edge environment is a dynamic and decentralized detection environment, comprising of interacting detection agents. Each edge node has a local agent for intrusion detection that is responsible for monitoring and analyzing the behavior of each node.

Local detection is not enough in identifying coordinated/distributed attacks. Therefore, nodes get involved in a collaborative detection layer, where selected information is shared between peers. Importantly, this collaboration does not involve exchanges of raw data, rather intelligence summaries such as alerts, feature abstractions or instructions updates for learning models are exchanged among nodes. This approach has the advantage of reducing communication overhead, and contributes to privacy preservation.

To support the system-wide awareness, the model also has an adaptive coordination mechanism. Coordination entities can be done through regional edge controller, cluster head and/or dynamically elected leaders like in network condition. Unlike rigidity of hierarchical architectures, ostensibly, coordination is opportunistic and adaptive so that detection can continue to be performed, even when the centralized connectivity is degraded or not available at all.

3.4 Learning and The Detection Paradigm

Given the novelty and variability of threats in 6G environments, the design goals that contribute to the proposed D-IDS put emphasis on anomaly-based and behavior-based detection instead of static signature matching. Each node runs lightweight machine learning models that learn normal behavior patterns locally or at each node, and identify deviations from that pattern which is a symptom of an intrusion.

In order to have better performance in detection within the network, the system supports federated and distributed learning. Nodes train local models based on locally observed data and illustrate upwards and downwards the model parameters or gradients as occurs periodically. Aggregation of these updates thus

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

allows the collective model to adapt to incidents of new emerging threats without centralising sensitive data (Li et al., 2020; Nguyen et al., 2022).
Because different attack surfaces are created when collaborating with others, the process for learning here is made trust-aware. Nodes assess the reliability of the update received from consistency, historical behavior and characteristics of anomalies. Updates from suspicious nodes can be down-weighted or discarded minimizing the effect of poisoning attacks. This trust-aware learning paradigm is critical to ultra-mobile environments because the membership of nodes changes frequently.

3.5 Comparative Analysis of the IDS Architectures

In order to clarify the suitability of distributed intrusion detection for ultra-mobile 6G networks, Table 1 compares centralized, isolated edge-based, and distributed IDS architectures with respect to dimensions that are of interest for 6G.

Table 1: Comparison of Intrusion Detection Architectures inUltra-Mobile 6G Environments

Dimension	Centralized IDS	Isolated Edge IDS	Distributed IDS (Proposed)
Detection latency	High	Low	Low
Scalability	Limited	Moderate	High
Mobility handling	Poor	Local only	Cooperative
Resilience	Low	Moderate	High
Context awareness	Delayed	Local	Local + shared
Privacy preservation	Low	High	High
Suitability for 6G	Low	Partial	High

This comparison gives an indication that isolated edge IDS help the latency but lacks the intelligence to work collaboratively to detect the distributed attack. Distributed IDS architectures have the low latency, global awareness, and are especially suitable for ultra-mobile 6G edge environments.

3.6 Summary of Contribution of Methodology

In this section, the methodological basis and system model to study distributed intrusion detection in ultra-mobile 6G edge architectures have been established. By taking a design science approach, and formalizing a decentralized ecosystem for detection, the study gives a clear analytical foundation for the framework introduced in the next section. The model to be proposed has autonomy, collaboration, and adaptive learning as its main characteristics - an essential mix for the guarantee of next-generation mobile networks with extreme dynamism and intelligence.

4. DISTRIBUTED INTRUSION DETECTION FORMAT AND ANALYSIS

4.1 Framework of the Distributed IDS for Ultra-Mobile 6G

Building on the methodology foundation and system model introduced in the previous section, this part presents and analyses a distributed intrusion detection framework that is specifically designed for ultra-mobile 6G edge architectures. The framework operationalizes three foundational principles - local autonomy, collaborative intelligence and adaptive response. These principles correspond to the requirements for security mechanisms that can operate with high levels of cybersecurity in case of extreme mobility, intermittent connectivity, and heterogeneous resource restrictions.
Unlike centralized security systems, which are based on persistent connectivity backhaul and aggregation of all traffic across the globe, the proposed framework considers each edge node to be an intelligent security agent. Detection decisions are drafted near where data is being produced while greater awareness is attained through selected and policy-driven information sharing. This design is consistent with the vision

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

of 6G that intelligence is not located in the centre of the network, but embedded everywhere (Zhang et al., 2023).

4.2 Architectural Components

The proposed framework is divided into four interacting layers, each of which is responsible for a different aspect of intrusion detection and response.

The Local Detection Layer is on individual edge nodes and continuously monitors the activity of individual nodes. This includes features of network traffic, protocols, authentication attempts and system-level events. Detection at this layer relies mainly on anomaly-based and behavior-based techniques, and therefore makes it possible to identify attacks that have not been seen before. Lightweight machine learning models are used for the feasibility of resource-constrained devices. Due to a local detection, the latency time is minimal and the immediate actions of containment could be prompted in case of need.

The Intelligence Sharing Layer provides for cooperation among distributed agents which perform detection. Rather than sending around raw traffic or sensitive data, nodes exchange condensed versions of data since informations for example summaries of alerts, behavioural fingerprint or model updates. Information sharing is adaptive and context aware: the nodes increase collaboration in the case of suspected attack scenarios, and dissolve the communication overhead in the case of normal operation. This layer is important in order to detect coordination attacks which play out in a subtle way at individual nodes but which become visible when the observations are combined.

The Coordination and Aggregation Layer provides synthesis of the intelligence combining to create a larger picture of the situation. Coordination entities can be implemented either as regional edge controllers or cluster leaders and coordinators can be dynamically elected depending on the network conditions. Importantly though, there is no strict hierarchy of coordination: it can adapt to topology changes and to mobility of nodes. This layer helps to correlation of alerts, finding distributed attack campaigning, and sending newer methods of detection.

The Response and Adaptation Layer takes the results of the detection and turns it into action to defend it. Responses may be local, e.g. isolation of a suspicious process, throttling traffic, or collaborative responses, e.g. alert propagation, shared detection model update. Adaptation mechanisms enable the system to fine tuning the thresholds, the re-training of the models and the policies of collaboration as the threats evolve.

4.3 Conceptual Diagram of the Framework

In this paper, a conceptual representation of the distributed intrusion detection framework for ultra-mobile 6G edge environments is presented,

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

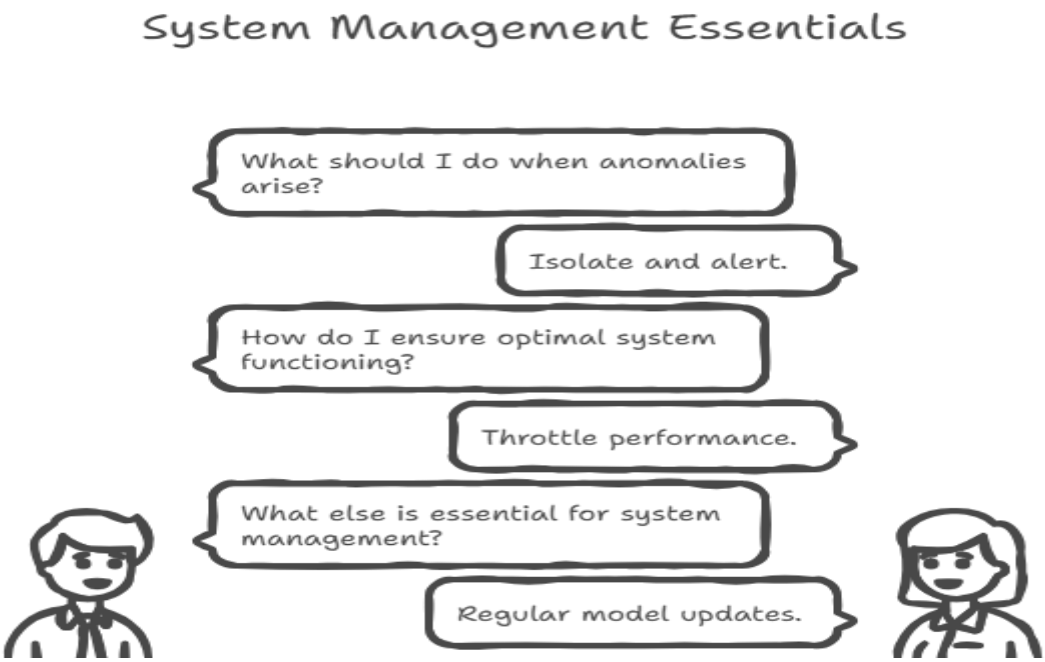

Figure 1. Distributed intrusion detection architecture for ultra-mobile 6G edge architectures.

The decentralized nature of the detection and the two-way flow of intelligence between local nodes and coordination entities is highlighted in the diagram. The framework continues to operate even in the absence of coordination during a limited time keeping baseline security requirements in place under extreme mobility conditions.

4.4 Threat Coverage and Capabilities to Detect

To assess how well the proposed framework meets and addresses some of the main categories of threats pertinent to ultra-mobile 6G edge environments, the main contributions are as follows: The representative threats to the detection mechanisms made possible by the distributed framework are mapped in Table 2.

Table 2. Threats and Detection Capabilities in Distributed 6G IDS

Threat Category	Description	Detection Mechanism
Edge node compromise	Malware injection, privilege escalation	Local behavior analysis and anomaly detection
Mobility-driven malware spread	Rapid propagation via moving nodes	Collaborative alerts and mobility-aware correlation
Distributed reconnaissance	Low-rate, multi-source scanning	Shared intelligence and pattern aggregation
Lateral movement	Cross-edge pivoting attempts	Context-aware detection and alert correlation
Edge-based DDoS	Coordinated traffic floods from edge nodes	Distributed flow analysis and cooperative response

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

Learning model attacks	Model poisoning or manipulation	Trust-aware aggregation and update validation

This mapping shows that distributed intrusion detection goes beyond threat identification in isolated environments to address 6G environment characteristic coordinated and mobility driven and learn-based attacks.

4.5 Analytical Discussion of Benefits of Framework

From an analytical perspective, the proposed framework has some advantages over the centralized and isolated edge-based IDS architectures.

The latency is reduced by performing the detection at the edge, bypassing the need for sending of raw data to analysers in the centralised purification. This is critical to many 6G use cases with decisions that have to be made in the microseconds or sub-milliseconds. Scalability is improved as the detection workload is spread among nodes and there are no bottlenecks and single points of failure.

The framework is also what helps with contextual awareness. Local detectors have the direct access to contextual information such as device role, mobility pattern and service requirements. Used together through collaboration this context allows more accurate detection of complex attack behaviors. Furthermore, resilience is enhanced as the failure/compromise of individual nodes does not inactivate the whole detection system.

But there are trade-offs for such benefits. Distributed detection adds coordination overhead and also involves strong trust management, in order to avoid having false or malicious alerts being propagated. Too much collaboration can result in straining network resources, or too little collaboration can result in less effect on detection. These trade-offs pain a climate information-sharing policy be that important to adapt.

4.6 Performance Considerations and Performance Trade Off

To offer an extended analysis of the framework, Table 3 summarizes the important performance dimensions and corresponding trade-offs in distributed intrusion detection for ultra-mobile 6G networks.

Table 3. Performance Considerations Trading off

Dimension	Benefit	Trade-Off
Detection latency	Near real-time response	Limited global visibility per node
Scalability	Supports massive node counts	Coordination complexity
Communication overhead	Reduced raw data sharing	Need for intelligent summarization
Detection accuracy	Improved through collaboration	Risk of false alert propagation
Privacy	Local data retention	Limited centralized analysis

This table shows that there is a trade-off of performance goals involved in distributed intrusion detection. Adaptive policies as well as trust-aware mechanisms are crucial to ensure the best benefits and the least drawbacks.

4.7 Security, Privacy and Trust Analysis

Security and privacy issues lie at the heart of the acceptability of the proposed framework. By restricting the exchange of information to indicate high level indicators and model updates, the framework helps to limit the exposure of sensitive information. This is in accordance with privacy-preserving principles receiving greater focus in 6G research (Dang et al., 2022).

Trust management remains a very important challenge. In the ultra-mobile environment, nodes often join and leave the network, and some nodes could be compromised. Reputation systems, consistency checks,

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

and anomaly detection at the level of the collaboration layer, may help to identify unreliable participants. Along with this, secure communication channels and trusted execution environments can be used to protect the local detection agents from tampering.

4.8 Summary of Framework Analysis

In summary, in this section we have presented and analyzed a distributed intrusion detection framework that is designed for ultra-mobile 6G edge architectures. Through decentralized detection, collaborative intelligence and adaptive response mechanisms, the framework solves the main issues regarding latency, scalability, mobility, and resilience. The analytical discussion and accompanying tables illustrate how distributed IDS architectures provide a strong and future-ready security foundation for the next generation of mobile networks, and in turn provides insight into the need for careful design of policy and trust management issues.

CONCLUSION AND FUTURE RESEARCH INVESTIGATIONS

The advent of ultra-mobile 6G edge architectures is a significant change in the design, operation, and security of wireless networks. Unlike the environments of previous generations, 6G environments are envisioned to be highly decentralized and intelligence-native ecosystems where massive numbers of heterogeneous devices interact dynamically across domain and space in the terrestrial, aerial and non-terrestrial domains. While these capabilities facilitate the transformative applications that they are used for, they also reveal fundamental limitations in traditional cybersecurity mechanisms - specifically centralized intrusion detection systems which require stable topologies, persistent connectives, and delayed analysis.

In this article, the concept of distributed intrusion detection as a fundamental security paradigm for ultra-mobile 6G edge architectures has been discussed. By bringing together the latest developments in 6G connectivity, edge computing and artificial intelligence-based security, the study has shown that intrusion detection will have to move from centralised security monitoring towards decentralised, cooperative and adaptive defence mechanisms. Distributed intrusion detection systems (D-IDS) address the architecture principles of 6G in an obvious way by performing detection intelligence at the edge of the network and thus responding locally and in real time while facilitating cooperative situation awareness throughout the network.

A number of important insights arise from the analysis. First of all, the ultra-mobility fundamentally changes the requirements of intrusion detection. The rapidity of change of the connectivity, trust boundaries and service context make static detection thresholds and centralized correlative worthless. Distributed IDS architectures meet this challenge by using the local context available at the edge nodes and correlating the local observations in an opportunistic way in order to improve the responsiveness and accuracy. Second, the integration of artificial intelligence (speaking specifically in regards to federated and distributed learning) increases the ability of D-IDS to adapt to evolving threats without centralizing the sensitive data. This is something that is particularly crucial in 6G environments where privacy preservation and scalability are of the utmost importance.

Third, the proposed framework indicates the importance of collaborative intelligence. Many attacks in 6G environments are likely to be low-rate, stealthy and distributed to exploit the mobility and heterogeneity

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

to evade isolated detectors. By allowing for controlled sharing of information and coordinated analysis, distributed intrusion detection systems can detect such patterns more effectively than isolated solutions that are edge based. At the same time, the framework also emphasizes that collaboration should be adaptive and trust-aware so that there is no excessive overhead or exploitation by malicious participants.

From a practical standpoint, the findings imply that working on intrusion detection in 6G should be considered a native network function rather than an external security add-on. Embedding the detection agents within edge nodes and combining them with mobility management, orchestration and AI control planes enables the evolution of security mechanisms along with network intelligence. For network operators, that means a paradigm shift and eventual move towards security architectures with an emphasis on autonomy, resilience and (continuing) learning versus power centric and static rule sets.

Despite all these advantages, there are also challenges with distributed intrusion detection. Coordination overhead, trust management and resource constraints are major concerns. Ultra-mobile environments make a vivid reputation difficult to assess, as well as raise the likelihood for false or misleading information propagation. In addition, lightweight detection models that are deployed at the edge have to compromise between accuracy and computational efficiency. Explicit action to address these trade-offs involves a careful system design and adaptive policies, and continued evaluation on them.

FUTURE RESEARCH DIRECTIONS

Several promising avenues for future research are suggested by this research. First of all, such empirical evaluation of distributed intrusion detection frameworks under realistic 6G scenarios becomes necessary. As 6G testbeds and large-scale simulators come of age, researchers should be testing the accuracy of detection and analyze latency, communication overhead and resilience in various mobility as well as attack conditions. Standardized benchmarks and datasets to ultra-mobile spaces would help with such evaluations enormously.

Second, more work is required in the area of secure and trust-aware collaborative learning. While federated learning has great advantages, there are also some vulnerabilities posed by model poisoning and unreliable participants. In future the authors suggest that robust aggregation techniques, incentive and cross layer trust models should be investigated that can yield collaborative detection processes in highly dynamic networks.

Third, mobility-aware context-aware detection is an important bridge that should beothing on the research. Incorporating predictive mobility models, digital twins and cross-domain context information can improve the ability of distributed IDS to differentiate between benign anomalies induced by mobility cooperembined with real attacks. This has a special mention to safety critical 6G applications such as autonomous transportation and industrial automation.

Finally, issues of ethical, regulatory and governance considerations should be given more attention. With the increasing autonomy, proactivity of distributed systems for intrusion detection come the questions of accountability, transparency, and proportionality of defensive action. Resolving these problems will be critical to ensuring effective and responsible deployment as well as societal trust in the next-generation wireless infrastructures.

FINAL REMARKS

In conclusion, distributed intrusion detection offers a solid and future-proof basis for securing the ultra-mobile 6G edge architectures. Ask D-IDS Founder Andrew H. Cyarney: "By matching that scenario in terms of security mechanisms, by matching that scenario in terms of its intelligence and its connectivity to the decentralized nature and the adaptable nature of 6G networks, you can mitigate some of the threats,

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

as it were, that are emerging; but you can also address the efficacy of performance and scalability requirements that are occurring with respect to the next generation of applications." As 6G conversion from vision to reality, the close combination of distributed intrusion detection from the very first will be the key to create wireless ecosystems not only fast and intelligent, but also secure and trustworthy.

REFERENCES:

2. Abdelwahab, S., Hamdaoui, B., Guizani, M., & Rayes, A. (2021). Distributed intrusion detection in the era of edge computing and Internet of Things. *IEEE Network, 35*(2), 120–126. https://doi.org/10.1109/MNET.011.2000463
3. Akyildiz, I. F., Kak, A., & Nie, S. (2020). 6G and beyond: The future of wireless communications systems. *IEEE Access, 8*, 133995–134030. https://doi.org/10.1109/ACCESS.2020.3010896
4. Alasmary, W., Alhaidari, F., & El Saddik, A. (2022). Security challenges and solutions in edge computing-enabled 6G networks. *IEEE Communications Surveys & Tutorials, 24*(3), 1576–1602. https://doi.org/10.1109/COMST.2022.3162385
5. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition, 84*, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023
6. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
7. Chen, J., Ran, X., & Chen, L. (2020). Edge AI: On-demand acceleration for deep neural network inference via edge computing. *IEEE Wireless Communications, 27*(5), 96–102. https://doi.org/10.1109/MWC.001.1900503
8. Dang, S., Amin, O., Shihada, B., & Alouini, M.-S. (2022). What should 6G be? *Nature Electronics, 3*(1), 20–29. https://doi.org/10.1038/s41928-019-0355-6
9. Fung, C., Yoon, C. J. M., & Beschastnikh, I. (2020). Mitigating sybils in federated learning poisoning. *Proceedings of the IEEE International Workshop on Trusted and Trustworthy Machine Learning*, 1–6.
10. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine, 37*(3), 50–60. https://doi.org/10.1109/MSP.2020.2975749
11. Mitchell, R., & Chen, I.-R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys, 46*(4), Article 55. https://doi.org/10.1145/2542049
12. Nguyen, D. C., Ding, M., Pathirana, P. N., & Seneviratne, A. (2022). Federated learning for Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 23*(3), 1622–1658. https://doi.org/10.1109/COMST.2021.3075439
13. Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems, 78*, 680–698. https://doi.org/10.1016/j.future.2016.11.009
14. Saad, W., Bennis, M., & Chen, M. (2020). A vision of 6G wireless systems: Applications, trends, technologies, and open research problems. *IEEE Network, 34*(3), 134–142. https://doi.org/10.1109/MNET.001.1900287
15. Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-94

E-ISSN: 2584-0487
editor@aijmr.com
Volume 1, Issue 1, July-August 2023
CrossRef DOI: 10.62127/aijmr.2023.v01i01.1200

16. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198
17. Snapp, S. R., Brentano, J., Dias, G. V., Heberlein, L. T., Ho, C., Levitt, K. N., Mukherjee, B., Smaha, S. E., Grance, T., Teal, D. M., & Mansur, D. (1991). DIDS (Distributed Intrusion Detection System) – Motivation, architecture, and an early prototype. *Proceedings of the 14th National Computer Security Conference*, 167–176.
18. Wang, X., Han, Y., Leung, V. C. M., Niyato, D., Yan, X., & Chen, X. (2021). Convergence of edge computing and deep learning: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 22*(2), 869–904. https://doi.org/10.1109/COMST.2020.2970550
19. Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., Karagiannidis, G. K., & Fan, P. (2019). 6G wireless networks: Vision, requirements, architecture, and key technologies. *IEEE Vehicular Technology Magazine, 14*(3), 28–41. https://doi.org/10.1109/MVT.2019.2921208
20. Zhang, Y., Chen, M., Saad, W., Yin, C., & Hong, C. S. (2023). Edge intelligence for 6G networks: Vision, enabling technologies, and applications. *IEEE Journal on Selected Areas in Communications, 41*(1), 6–20. https://doi.org/10.1109/JSAC.2022.3218347