International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-15 Issue-7, June 2026

Performance Analysis of a Blockchain-Enabled Adaptive Routing Strategy for Mobile Producer Handoff in Multihomed Named Data Networking

Hassan Adam, Yusuf Ayuba, Aliyu Musa Kida, Wunukhen Shehu Awudu, Muhmammed Zaharadeen Ahmed, Aisha Hassan Abdalla Hashim

***Abstract*: *Named Data Networking (NDN) is considered a promising paradigm that enables content-centric communication and in-network caching. However, challenges of mobility, scalability, and security limit its effectiveness and impact in dynamic IoT environments. Existing mobility management approaches and strategies, including anchor-based and anchor-free schemes, are unable to jointly optimise latency, security, and multihoming efficiency, even under highly dynamic conditions. This research work proposes a Mobile Producer Handoff in the Named-data Emulated Mobility framework known as MP-HNEM. This is a blockchain-based adaptive routing strategy that integrates predictive handoff, cross-layer optimisation, and a lightweight Proof-of-Authority consensus mechanism to provide and enhance mobility support in multihomed NDN-based wireless sensor networks. The framework also addresses a crucial gap in secure and latency-aware producer mobility. A hybrid simulation and emulation method is employed using ndnSIM v2.9 and a Mini-NDN to evaluate MP-HNEM performance under varying mobility patterns, trust thresholds, and network densities. We analyzed latency, throughput, packet delivery ratio, energy consumption, and trust validation delay as key metrics. MP-HNEM results show a 42.7% reduction in latency, a 73% increase in throughput, and a 39% reduction in energy consumption compared to baseline schemes. The packet delivery ratio increases by 31.5%, indicating improved reliability across all handoff events. Security analysis shows detection accuracy over 90% and block validation success rates over 98% under mobility conditions. Using ANOVA, we conducted Statistical validation and achieved $p < 0.05$, confirming the impact and significance of these improvements. The major contributions of this research work are: (i) a blockchain-integrated ARS developed to secure multihoming mobility, (ii) a reinforcement learning-based predictive handoff mechanism for smart support, and (iii) a hybrid validation framework that combines both simulation and emulation procedures. The results indicate that MP-HNEM is a scalable, energy-efficient, and secure mobility solution for NDN-based IoT systems, suitable for applications such as smart healthcare and industrial IoT. Future work intends to focus on real-world deployment and heterogeneous IoT integration.*

Keywords*: *Adaptive Routing Strategy, Blockchain Security, Multihoming, Producer Mobility.

Nomenclature:
NDN: Named Data Networking
mobile producers (MPs
WSN: Wireless Sensor Network
FIB: Forwarding Information Base

Manuscript received on 27 March 2026 | First Revised Manuscript received on 05 April 2026 | Second Revised Manuscript received on 20 May 2026 | Manuscript Accepted on 15 June 2026 | Manuscript published on 30 June 2026.

*Correspondence Author(s)
Hassan Adam, Department of Computer Engineering, University of Maiduguri, Maiduguri, 1069, Nigeria | Department of Cybersecurity, Al-Ansar University, Maiduguri, Nigeria. Email ID: hassanadam457@gmail.com, ORCID ID: 0000-0002-6314-1025
Yusuf Ayuba, Department of Computer Engineering, University of Maiduguri, Maiduguri, 1069, Nigeria | Department of Computer Engineering, Federal University Wukari, Taraba, Nigeria. Email ID: ayubayusuf@fuwukari.edu.ng
Aliyu Musa Kida, Department of Computer Engineering, University of Maiduguri, Maiduguri, 1069, Nigeria. Email ID: aliyukida@gmail.com
Dr. Wunukhen Shehu Awudu, Department of Computer Engineering, Federal University Wukari, Taraba, Nigeria. Email ID: awudusw@fuwukari.edu.ng
Dr. Muhmammed Zaharadeen Ahmed*, Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, 53100 Malaysia | Department of Computer Science, University of Technology of Arts of Byumba, Rwanda | Department of Cybersecurity, Al-Ansar University, Maiduguri, Nigeria | Centre for Technical Research and ICT, Dee Tech Academic Limited, Maiduguri, Borno State, Nigeria. Email ID: zaharadeenccna@gmail.com, deetech2022@gmail.com, ORCID ID : 0000-0001-9837-2280
Dr. Prof. Aisha Hassan Abdalla Hashim, Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, 53100 Malaysia | Department of Electrical and Electronic Engineering Science, University of Johannesburg, South Africa. Email ID: aisha@iium.edu.my

I. INTRODUCTION

As a result of the rapid development of wireless sensor networks (WSNs) in smart environments, effective network security and scalable intercommunication have become challenging research concerns nowadays. Conventional IP networks and software-defined network architectures face enormous issues with mobility, in-network addressing, and security (Okon et al. [1]). Named data networking (NDN) is focused on addressing these issues by shifting from host-centric to data-centric communication, allowing native support for caching, multicast, and mobility Azamuddin et al. [2]. However, NDN still struggles to develop robust access control, data source authentication, and trust management mechanisms (Hussaini et al. [3]). Furthermore, existing NDN mobility solutions do not adequately support multihoming scenarios where content producers maintain multiple interfaces (inbound/outbound) under dynamic conditions. On the contrary, blockchain technology creates a decentralized trust and immutable records. Analytical comparison of NDN mobility management and comprehensive reviews of blockchain network communication make it suitable for logging and authorisation tasks (Mamun et al. [4]; Alkawai et al. [5]). Despite the positive advantages of blockchain technology, integrating it with NDN introduces challenges and open issues, including computational overhead,

latency, and energy constraints, particularly in resource-limited wireless sensor network environments, where data sharing is difficult. Additionally, these parameters are examined through security simulations, such as Hyperledger Fabric (Wen et al. [6]). This research work, therefore, integrates blockchain, as a concept adopted from Reyna et al. [7], with a named data network to structure a hybrid architecture tailored for wireless sensor networks and IoT applications (Dorri et al. [8]).

The basic objective of this research work is to leverage blockchain for secure identity and access management, and a named data network for efficient data delivery as a mobile producer (MP) moves within an active network. Specifically, this research aims to design and evaluate a secure, adaptive, and scalable routing framework that minimises handoff latency while preserving trust and energy efficiency in multihoming environments.

We compared against well-known mobility management schemes such as KITE and MAP-Me to demonstrate improvements in security, adaptability, and latency under realistic conditions. Furthermore, the paper presents an Adaptive Routing Strategy for Mobile Producer handoff in multihoming environments, ensuring seamless inter-connectivity and efficient utilization of multiple link interfaces. The paper also demonstrates how to mitigate Wireless Sensor Network vulnerabilities such as spoofing, unauthorised access, and single points of failure (the need for multihoming) using hybrid procedures (simulation and emulation).

In many multihoming networks, where mobile producers (MPs) rely on multiple network interfaces (links) for seamless data delivery, the choice of selecting a better routing strategy plays a decisive role in ensuring efficient mobile handoff, Islam et al. [9]. Conventional strategies often prioritise maintaining connectivity; however, they fail to account for latency-sensitive and throughput-intensive scenarios, especially when producer mobility creates unpredictable link changes and variations. Adaptive Routing Strategy addresses this research gap by dynamically modifying forwarding decisions based on network environment, traffic demand, and link conditions. This adaptability of network configuration ensures that mobile producers (MPs) can exploit multiple interfaces (links) simultaneously, thereby minimizing packet loss and avoiding persistent handoff disruptions. By combining routing flexibility with predictive mobility management, adaptive routing strategies enhance the reliability of Named Data Networking in real-world deployments.

As Internet of Things and Wireless Sensor Network nodes often act as data producers transmitting critical network information, mobility and energy challenges can easily jeopardize reliable mobile network performance, Kuang et al. [10], Xue et al. [11]. Integrating the Adaptive Routing Strategy within the MP-HNEM framework ensures that sensor data is transmitted over the most reliable link, while predictive handoff reduces service disruption. These twofold advantages not only enhance energy efficiency but also facilitate delay-sensitive applications such as industrial monitoring and smart healthcare services. Consequently, the MP-HNEM framework proposed in this research work positions adaptive routing as a cornerstone for scalable, secure, and high-performance Named Data Network-based mobility management in heterogeneous network environments.

This research work presents a blockchain-NDN framework to enhance the security and trust of data communication in Wireless Sensor Networks. Specifically, the MP-HNEM framework is designed to address the open issues and challenges of resource constraints and mobility-induced instability (mobile producer) in (WSN) wireless sensor nodes operating in multihoming environments. MP-HNEM is denoted as Mobile Producer Handoff in Named-data Emulated Mobility. Our framework solution uses blockchain-based smart contracts to manage decentralized identity and access control. It also ensures data integrity and secure routing across multiple Named Data Network nodes.

The major contribution of MP-HNEM is the design of an adaptive routing strategy. This mechanism dynamically selects an optimal path across multihomed links or interfaces to minimise latency and packet loss during producer handoff. Using an emulation procedure, a realistic environment is developed in ndnSIM for Wireless Sensor Network mobility and in Hyperledger Fabric for practical blockchain operations. A detailed sensitivity analysis is conducted to assess the impact of network load, mobility speed, and packet size on the MP-HNEM system's performance. Performance metrics such as latency, energy consumption, trust enforcement overhead, and data availability are computed to reflect the behaviour of Wireless Sensor Nodes in real-world deployments. The results demonstrate that the MP-HNEM approach consistently outperforms existing research schemes, particularly in handoff latency, packet delivery ratio, and security resilience, while maintaining energy efficiency better suited to low-power sensor devices. MP-HNEM also shows that integrating blockchain with Named Data Networking not only strengthens the network's resilience against spoofing and unauthorised access but also optimises resource usage through secure and adaptive routing protocols tailored for sensor networks.

A. Contribution

Majorly, MP-HNEM contributions are summarized as follows:

i. A novel framework known as MP-HNEM that integrates blockchain with Named Data Network for secure mobile producer handoff
ii. An Adaptive Routing Strategy for efficient and effective multihoming support.
iii. A reinforcement learning-based support for predictive handoff mechanism.
iv. A hybrid procedure of simulation and emulation validation using ndnSIM and Mini-NDN.
v. Comprehensive performance evaluation and statistical analysis against two baselines (KITE and MAP-Me).

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

II. LITERATURE REVIEW

In this section, we conduct a critical review of existing research works on blockchain-enabled security, Named Data Network mobility support, and adaptive routing strategies in multihoming network environments.

A. Adaptive Routing in WSNs: Blockchain-based

Wireless Sensor Networks are used widely in smart healthcare, industrial monitoring, disaster and risk management, and smart/sustainable cities. These deployments (mathematically based precision) often involve mobile producers (MP) such as drones, wearable sensors, and vehicular nodes that are required to maintain secure and reliable intercommunication during handoff events (Azamuddin et al. [12]). The Named Data Network offers a data-centric framework with in-network caching and native mobility support (Kareem et al. [13]). Hence, some challenges persist in ensuring trust, authentication, and adaptive routing under dynamic multihoming conditions. Adaptive Routing Strategy is crucial in this network setting, as it enables nodes to automatically adjust link paths based on the mobility pattern adopted and the availability of interfaces. Integrating Blockchain enhances the Adaptive Routing Strategy by providing immutable trust records, decentralised identity management, and tamper-proof transaction validation. Together, Adaptive Routing Strategy and blockchain create a secure, scalable, and mobility-aware framework for content producer handoff in multihoming Wireless Sensor Network environments.

B. Security and Mobility Management Frameworks

Security and mobility management in Wireless Sensor Networks require lightweight, robust mechanisms. This is a result of the limited resources of sensor nodes and the instability introduced by producer mobility. Traditionally, the centralized framework models cannot scale effectively in multihoming scenarios. This is where nodes connect using multiple (multihomed) interfaces. Therefore, blockchain-enabled smart contracts offer decentralized access control, while Adaptive Routing Strategy-based mobility solutions minimizes packet loss and latency by adapting forwarding decisions across heterogeneous interfaces or links. This dual-layered methodology ensures seamless mobility support while resisting spoofing, replay attacks, and single points of failure. Furthermore, by caching (storing) route updates and trust logs on the blockchain, adaptive mobile handoff decisions achieve both transparency and resilience. This guarantees stable network performance (cloud-based and sensor networks) even under hostile or high-density deployments (Ahmed et al. [14]).

C. ARS-Based MP-HNEM for Multihoming Scenarios

The adaptive Routing Strategy-based MP-HNEM framework is a promising approach for managing producer mobility in multihoming environments. By dynamically selecting the most effective forwarding path (link) across multiple interfaces (including IoT nodes), Adaptive Routing Strategy improves throughput, reduces handoff delay, and maintains network session continuity, even in highly dynamic topologies (Olanrewaju et al. [15]). The multihoming network environment strengthens the resilience of the MP-HNEM framework, as content producers can seamlessly exploit redundant network links to avoid issues and disconnections, and optimise latency-sensitive traffic. Recent research has shown that combining an Adaptive Routing Strategy-based handoff with predictive mechanisms offers significant benefits in packet delivery and reliability compared to conventional anchor-based approaches. Therefore, these advantages extend beyond generic Named Data Network mobility scenarios, as a Wireless Sensor Network integrated with multihomed gateways can also leverage an Adaptive Routing Strategy-driven predictive handoff to ensure secure and energy-efficient data dissemination. Hence, the Adaptive Routing Strategy-based MP-HNEM solution presents a balanced strategy that bridges mobility management, security, and resource optimisation in both multihomed Named Data Network and Wireless Sensor Network contexts.

D. Related Work

Mobility support and secure handoff strategies in NDN-based wireless networks have gained increasing research attention, particularly in multihoming environments. Zhang et al. [16] proposed anchor-based and anchor-free mobility management approaches for producer mobility, with distinct trade-offs between scalability and signalling overhead. Also, while KITE relies on a rendezvous server and suffers from higher latency, MAP-Me leverages in-network updates but incurs signalling overhead in dense networks. Neither approach integrates adaptive routing with blockchain trust, leaving gaps in both mobility efficiency and security. The anchor-based handoff scheme in NDN faces issues of centralisation and latency. Blockchain-enabled access control frameworks improved trust but relied on energy-intensive consensus mechanisms, such as Proof-of-Work, which are unsuited for WSNs. More recent studies investigated cross-layer routing, fuzzy trust, and vehicular IoT extensions, yet lacked blockchain integration for tamper-proof validation Augé et al. [17]. Similarly, distributed trust models and cross-layer caching designs improved mobility but fell short of addressing multihoming producer handoff. Blockchain-based IoT identity management improved security but overlooked routing performance, while freshness-focused NDN schemes neglected energy efficiency. Centralised routing for disaster WSNs lacked scalability with mobility, and reinforcement learning–assisted NDN routing did not incorporate blockchain-backed trust. Lightweight blockchain designs for IoT–NDN reduced consensus delay but ignored predictive mobility, and hybrid MAP-Me with blockchain improved auditability at the cost of signalling delay (Hernandez et al. [18]).

Our proposed MP-HNEM distinguishes itself by combining ARS-based predictive mobility, blockchain-based trust management, and cross-layer energy optimisation into a single framework, validated through simulation and emulation. Unlike existing works, MP-HNEM directly addresses the producer handoff problem in multihoming WSNs, striking a balance between latency, security, and scalability.

Generally, existing approaches either optimise

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

mobility, security, or routing independently but lack an integrated framework that simultaneously addresses multihoming, predictive handoff, and blockchain-based trust—a gap this work (MP-HNEM) addresses.

Table I: Comparative Analysis of Adaptive Routing and Blockchain-Enhanced NDN Mobility Frameworks

Feature	MP-HNEM	Traditional NDN-WSN	Blockchain-based (non-NDN)
Security	Immutable ledger, ARS-based trust validation, replay resistance	Basic packet signatures are vulnerable to spoofing and anchor attacks	Strong immutability but high processing overhead
Scalability	Adaptive routing with multihoming; optimized FIB updates	Limited under dense topologies due to signalling overhead	Blockchain nodes scale poorly due to sync cost
Energy Efficiency	Energy-aware ARS handoff and reduced retransmissions	Frequent retransmissions during mobility	High due to heavy consensus (e.g., PoW)
Latency	Predictive handoff with proactive FIB updates	Higher latency (KITE) or signalling overhead (MAP-Me)	High latency due to global consensus
Implementation Complexity	Moderate complexity: blockchain integrated with NDN stack	Low: baseline NDN routing	High: full blockchain without NDN

III. METHODOLOGY

This section presents the implementation procedure for MP-HNEM, based on its architecture and algorithm design, blockchain trust management, and analytical computations. Simulation and emulation are conducted to validate performance across latency, handoff delay, energy efficiency, and security. Predictive handoff parameters, such as multihoming adaptability and scalability, are also presented.

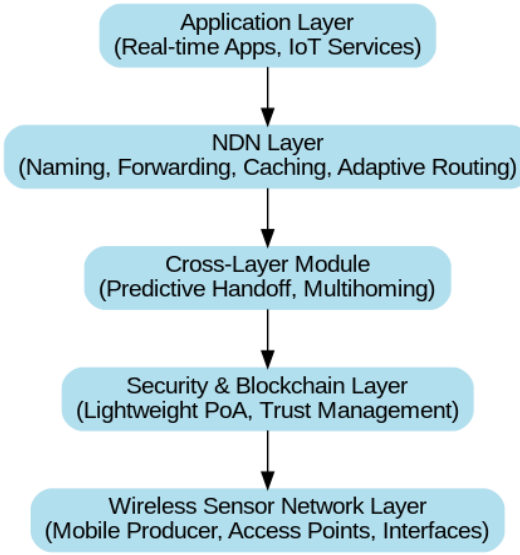
A. Architectural Design using Adaptive Multihoming

The proposed system integrates multihoming and predictive mobility support within the Named Data Network architecture. The design is inspired by existing mobility frameworks, such as MAP-Me [17], and by predictive handoff mechanisms. Additionally, blockchain is incorporated to ensure secure data exchange and trust management, as demonstrated in recent IoT security frameworks. Therefore, the proposed architecture comprises three integrated layers. These include;

i. Wireless Sensor Network Layer (WSN)
ii. Named Data Networking Layer (NDN)
iii. Blockchain Security Layer.

The WSN layer comprises energy-constrained mobile and static sensor nodes that act as data producers and consumers. Nodes support multiple interfaces for multihoming, allowing seamless switching during mobility-induced handoffs. Unique names replace IP addresses to enable data-centric operation. The NDN layer implements predictive mobility-aware routing to support mobile producer handoff. The Forwarding Information Base (FIB) is dynamically updated via trajectory prediction, ensuring minimal packet loss and delay during handoff: in-network caching, Interest forwarding, and signature-based validation guarantee data availability and integrity across multihomed paths. The Blockchain Security Layer provides decentralized trust, identity validation, and secure logging via lightweight Proof-of-Authority (PoA). Smart contracts enforce access control and validate producer handoff events. This ensures tamper-resistant records of mobility transitions while minimizing energy consumption. Each layer interacts through well-defined interfaces to ensure modularity, scalability, and ease of implementation in real-world deployments.

The hierarchical interaction of these layers enables adaptive route selection across multiple interfaces, allowing mobile producers to maintain uninterrupted connectivity while ensuring secure, low-latency communication Fig. 1.



[Fig.1: Adaptive Multihoming and Security Architecture]

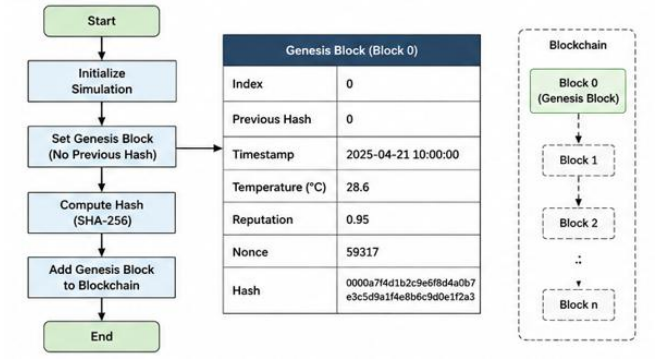
The hierarchical trust management protocol coordinates seamless communication between layers. Blockchain access credentials are dynamically identified by NDN nodes, enabling secure data retrieval. Secure device registration and certificate issuance are mandated through blockchain consensus mechanisms, enhancing distributed authentication, confidentiality, and data integrity. This enables the system to be robust and have a distributed security framework that addresses the challenges of authentication, confidentiality, and data integrity.

During simulation, blockchain code is implemented to define block structures, including unique identifiers (hash), previous block references, and nonces, with lightweight mining to suit WSN energy constraints. Genesis blocks are initialized, and subsequent blocks append verified data such as sensor readings ("temperature" and "reputation"). The initial block in the blockchain is called the genesis block and contains no previous hash. It contains a nonce (a random number that satisfies the difficult criteria of a hash). The code creates a list called blockchain and assigns the genesis block to it. Then, new blocks can be added to the blockchain by appending them to the list and updating their hash, data and nonce.

The implementation is

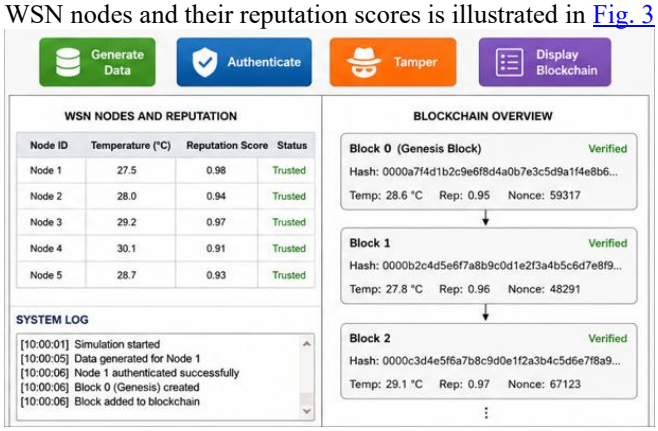
Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

presented in Fig. 2.



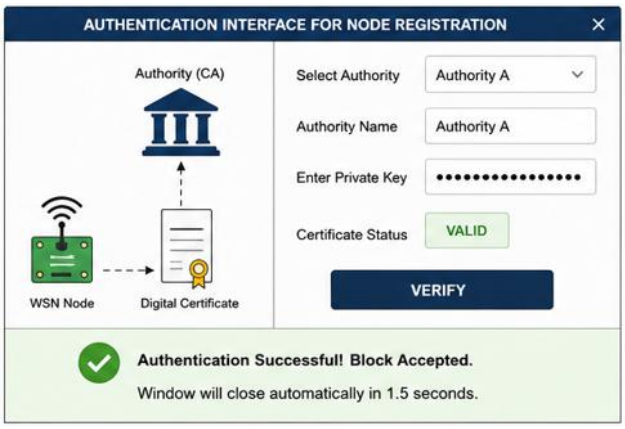
[Fig.2: Genesis Block Creation]

Fig. 2 illustrates the creation of the genesis block in the blockchain, including the data fields (temperature, reputation), the nonce, and the hash calculation. Among the interface navigation buttons, the first is to generate data. Data is generated anytime a user clicks on the button. The user must first authenticate the data before proceeding to the blockchain. The third button is the "Tamper" that is used during a malicious attack simulation. The interface button is used for display, meaning it prints every block and its contents in the terminal as program output. The interface of WSN nodes and their reputation scores is illustrated in Fig. 3



[Fig.3: Graphical User Interface]

Fig. 3 shows the interface for generating data, performing authentication, and simulating tampering attacks. When the 'authenticate' button is clicked, a separate window appears Fig. 4. The authorities' names are displayed to preview their private keys. As the keys are entered, the block is accepted, and the window closes after 1.5s.



[Fig.4: Authentication Interface for Node Registration]

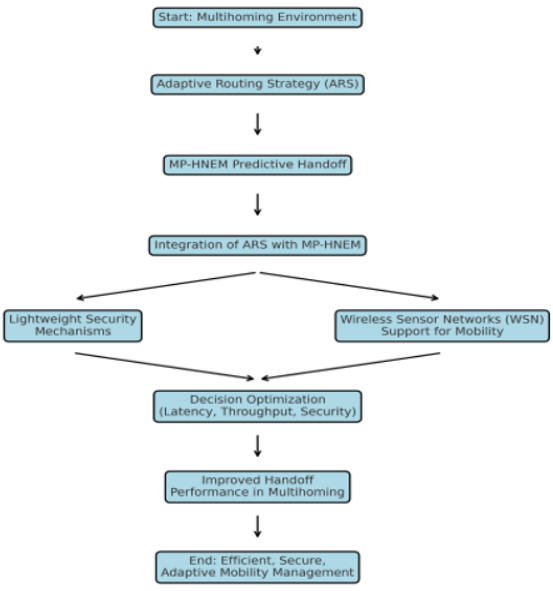
Fig. 4 demonstrates the pop-up window for key entry and certificate verification.

B. Algorithm Implementation

The blockchain-enhanced trust and routing algorithm disseminates secured data in WSNs within the NDN paradigm. The algorithm integrates predictive AI handoff strategies and network slicing to optimize routing under multihoming scenarios. The steps are presented (as in Algorithm 1) as follows.

```
Begin
    Initialize all WSN nodes with blockchain certificates
    For each Consumer Node:
        Generate an Interest Packet with a hierarchical name, node ID and signature
        Send Interest Packet to NDN Router.
        If Node Trust Level ≥ Trust Threshold:
            Forward Interest Packet to Producer or Cache.
            Retrieve Data Packet.
            Record Transaction on Blockchain.
        Else:
            Drop Packet and Flag Node.
    End For
    For Mobile Nodes:
        Perform predictive handoff using reinforcement learning (state space: node position and link quality; actions: select next PoA; reward: latency reduction and trust maximization).
        Update routing paths in the NDN Layer.
    End For
    Continuously mine new blockchain blocks.
    Monitor for anomalies and update trust scores.
End
```

The algorithm's complexity is $O(N \times M)$ for N nodes and M routing updates. Scalability is addressed by hierarchical trust management, predictive handoff, and lightweight block mining to reduce overhead in dense networks. Also, this algorithm is implemented in ndnSIM using C++ modules, while blockchain operational procedures for emulation are implemented using Hyperledger Fabric APIs. This is to ensure realistic validation of trust operations. A pictorial flowchart that describes the practicality of this algorithm is presented in Fig. 5.



[Fig.5: ARS-Based MP-HNEM Flowchart]

In the initial step, we performed node initialisation. All Wireless Sensor Nodes register using a

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

blockchain-based device registration procedure. Each content node receives a unique certificate and public key, which are stored securely on the blockchain. Secondly, an interest packet is generated by consumers in the network. Consumer nodes generate content Interest using hierarchical names (unique). Interest packets capture embedded node credentials along with a trust signature. Thirdly, Trust evaluation is conducted in the third step. This is where Named Data Network router nodes validate consumer certificates using the blockchain ledger. Then, trust thresholds are verified to filter out malicious requests. Data content retrieval and caching are considered the fourth step, in which verified Interest content is forwarded to the nearest producer node or retrieved from an in-network cache. Named Data Network routers use name-based forwarding strategies to highly optimise delivery paths. Blockchain logging is regarded as the fifth step. This is where each successful data exchange in the network is immutably recorded in the ledger, and to maintain auditability across the network, mobility support is considered the sixth and most crucial step in the mobile producer handoff. Here, in ndnSIM, mobile Wireless Sensor Network nodes dynamically update their routing paths using predictive handoff strategies (developed via reinforcement learning). This is to minimize latency during movement. Block mining is another step that follows after using a lightweight consensus adapted to the energy constraints of Wireless Sensor Networks. Finally, anomaly detection is performed. This is conducted by the blockchain-integrated trust module, which observes node behaviour and flags tampered or suspicious flows.

C. ARS-Based MP-HNEM For Multihoming Scenario

To further enhance the mobility management component of Algorithm 1, the MP-HNEM framework is incorporated by combining an Adaptive Routing Strategy tailored for multihoming environments with predictive handoff. The Adaptive Routing Strategy module dynamically selects the best forwarding path across multiple active interfacing links, ensuring seamless producer handoff and maintaining network session continuity in highly dynamic topologies. Within the MP-HNEM design, multihomed producers can exploit redundant network link interfaces to mitigate sudden disconnections and optimise latency-sensitive traffic flows.

In practice, the adaptive routing strategy operates in collaboration with the predictive handoff logic already embedded in Algorithm 1. While the predictive module forecasts the next point of attachment (for the producer) based on link quality and mobility state, the Adaptive Routing Strategy evaluates real-time path metrics such as throughput, delay, and packet drop rate to identify and select the optimal interface. This dual-layer decision procedure improves throughput and reliability compared with conventional anchor-based approaches.

Importantly, the advantage extends to Wireless Sensor Networks using multihomed gateways. In this case, Adaptive Routing Strategy-driven predictive handoff not only enhances delivery reliability but also optimises energy consumption by balancing traffic across available interfaces. Hence, the Adaptive Routing Strategy-based MP-HNEM integration provides a holistic routing strategy that bridges mobility management, security, and resource optimisation, thereby reinforcing the robustness of this blockchain-enhanced trust and routing algorithm. The Adaptive Routing Strategy decision function can be formulated as a multi-objective optimisation problem that considers latency, throughput, and trust constraints.

D. Scalability, Complexity, and Theoretical Justification of ARS in MP-HNEM

The adaptive routing strategy module in MP-HNEM is fully designed to efficiently manage mobility, multihoming, and dynamic traffic patterns in NDN-based Wireless Sensor Network environments. Scalability analysis shows that the Adaptive Routing Strategy maintains performance as the number of content nodes increases, thanks to its hierarchical trust management and predictive handoff support. Each mobile node in the network sends routing updates locally using Artificial Intelligence-based prediction, thereby reducing network-wide signalling overhead. The total computational complexity of the Adaptive Routing Strategy is O(N×M), where N is the total number of router nodes, and M is the number of routing updates per node. The O(N×M) complexity is lessened in practice using localized routing updates and hierarchical clustering, ensuring scalability in dense deployments. This complexity is responsible for trust evaluation, content interest forwarding, and predictive handoff assessments. The theoretical justification of MP-HNEM is presented in Section 3.3

E. Simulation and Performance Metrics

Our experimental setup uses the ndnSIM v2.9 environment, and all metric parameters are described in Table 2. Also, we describe each performance metric as follows:

i. Packet Delivery Ratio represents the ratio of successfully received packets to the transmitted packets.
ii. End-to-End Latency is the time between interest packet generation and data retrieval.
iii. Handoff Overhead is the number of routing updates that are triggered by mobility.
iv. Blockchain Transaction Validation Delay is derived from queuing theory using M/M/1 queue.
v. Forwarding Cost (C_f) represents the number of router hops traversed weighted by security constraints.

Table II: Simulation Parameters and Performance Metrics

Metric	Value and Description	Purpose
Network Topology	50 nodes (10 producers, 30 consumers, 10 routers)	Supports mobility and multihoming
Link Characteristics	Bandwidth 10 Mbps, Delay 5 ms	Uniform for all links
Mobility Model	Random Waypoint, 1–5 m/s	Models' producer mobility
Simulation Duration	500 s	Ensures steady-state performance
Traffic Model	Interest rate 20 packets/s, Packet size 1024 bytes	Consumer-driven traffic load
Trust Threshold (T_min)	0.7	Node trustworthiness constraint
Blockchain Consensus	Lightweight PoA	Edge-based validation mechanism
Performance Metrics	PDR, Latency, Handoff Overhead, Validation Delay, C_f	Evaluates reliability & efficiency
Comparative Baselines	KITE, MAP-Me	Benchmark reference schemes
Sensitivity Variables	Mobility speed, Interest rate, Trust threshold	Tests the robustness of ARS

All simulation parameters used are configured to ensure reproducibility and fairness

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

throughout the baseline comparisons. Random seeds and mobility traces are consistently maintained across all experiments.

F. Baseline Comparison and Sensitivity Analysis

To conduct a comprehensive performance evaluation of the Adaptive Routing Strategy for MP-HNEM, comparative experiments are run against two state-of-the-art schemes, namely, KITE and MAP-Me. Each scheme is simulated under identical network conditions and is summarised in Table 2. This is solely to ensure fair and critical baseline comparison. Sensitivity analysis is conducted to evaluate robustness of MP-HNEM framework under varying network conditions. This includes node mobility from 1–5 m/s, network load rate of interest generation from 10–30 packets/s, and trust threshold values (T_min) from 0.6–0.9. This analysis reveals the operational limits of our algorithm and highlights scenarios where MP-HNEM achieves performance gains over baseline schemes. Combining baseline and sensitivity analysis ensures quantitative evidence of MP-HNEM's scalability, reliability, and efficiency.

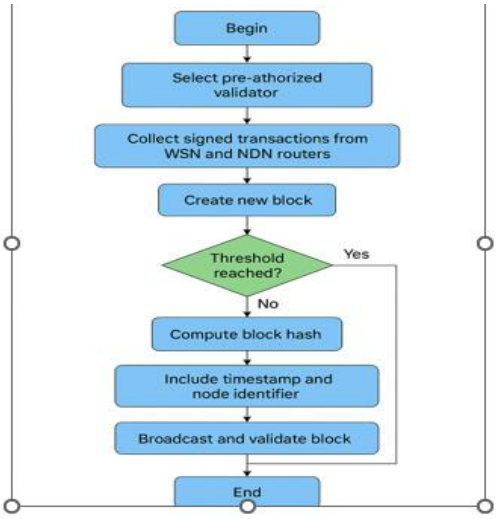
G. Block Mining Procedure

The blockchain-enhanced security system enables adaptive handoff by ensuring trust when sending route updates. A lightweight Proof-of-Authority consensus mechanism supports energy-efficient block validation. During handoff events, validator nodes in the network securely log updates to producer identities and multihoming route changes. This ensures that the ARS (Adaptive Routing Strategy) is not only efficient but also verifiable and tamper-proof. Blocks are being generated periodically to lessen latency while maintaining trust across all multihomed interfaces. A basic component of the mine_block function is illustrated in Fig. 6.

```
def mine_block(id):
    last_b=blockchain[-1] # Retrieve the last block in the blockchain
hashed_block=hash_block(last_b) #Compute hash of the last block
nonce=pow()
    rep=rep_calc(int(open_transactions[-1]['temperature']),id) #Calculates
reputation score
    block={
    'previous_hash': hashed_block,
    'sensor':id,
    'index': len(blockchain),
    'temperature': open_transactions[-1]['temperature'],
    'timestamp': get_timestamp(),
    'reputation':get_reputation(id,rep), #Retrieves the reputation for the
sensor
    'nonce': nonce
    }     blockchain.append(block) #Adds new blocks to the
blockchain
```

[Fig.6: Block Mining Function]

Fig. 6 illustrates the lightweight PoA mining procedure, including validator selection, transaction aggregation, block formation, and Merkle tree summary. Thus, a flowchart describing the simulation procedure is illustrated in Fig. 7



[Fig.7: Mine Block Simulation Flowchart]

Fig. 7 depicts the simulation workflow of block mining, including transaction collection, block generation, and network-wide broadcast.

H. Analytical Computation

This section provides a mathematical validation of the proposed framework, complementing the simulation results and ensuring theoretical soundness. This framework incorporates emulations, reinforced by mathematical formulas, to verify data integrity, manage trust, and assess latency differences. To verify data integrity, using blockchain by tempering resistance, the security management system exploits a cryptographic hash function H (·) by directing each NDN data content before and after transmission. This is supported using Equation (1).

$$H(D_i) = h_i \qquad (1)$$

Where D_i represent the data content of the packet i, h_i represent the hash value, and H represent a secure hash function (SHA-256). Therefore, we consider a data packet to be authentic if it satisfies the condition in Equation (2).

$$H(D_i) * (recieved) = h_i * (original) \qquad (2)$$

The condition ensures that intermediate routers do not utilise content without being detected. Secondly, the Bayesian trust model is used to determine historical interactions between NDN-Internet of Things nodes, thereby ensuring trust management using Equation (3).

$$T_n(t) = \left(\frac{\alpha_{n(t)}}{\alpha_{n(t)} + \beta_{n(t)}}\right) \qquad (3)$$

Where $T_n(t)$ represents the trust value of node n at time t, α_n(t) represents the number of successful interactions, and β_n(t) represents the number of unsuccessful interactions. Therefore, Nodes that are below the trust threshold T_min are not considered (Equation (4).

$$T_{n(t)} < T_{min} \rightarrow Node\ n\ is\ distrusted \qquad (4)$$

Thirdly, the transaction validation delay is computed assuming Internet of Things

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

devices generate N transactions per unit time. λ represents the transaction generation rate, whereas μ represents the blockchain processing rate. Therefore, the use of the M/M/1 queueing model is crucial, as the validation delay D is formulated in Equation (5) below.

$$D = \left(\frac{1}{(u-\lambda)}\right), for\ \lambda < \mu \qquad (5)$$

We employ queuing theory to assess scalability and performance because transaction loads increase over time. Finally, the impact of the forwarding strategy in NDN is used to model packet forwarding cost as per content retrieval, using Equation (6).

$$C_f = +\sum_{n=1}^{\infty} (i=1) * (k)\, c_i \qquad (6)$$

Where c_i represents the cost for each hop i along a path, and k represents the total number of hops from the content source to the requesting producer. This means that the cost of forwarding content while maintaining issues of security in the C_f The network can be optimised using the condition in Equation (7).

$$\min_p C_f(P) \text{ subject to } T_n(t) \geq T_{min} \qquad (7)$$

Where P represents a path in the NDN graph, mathematical analysis justifies ARS's performance improvement by showing that predictive handoff reduces expected latency and forwarding costs while ensuring that minimum trust thresholds are satisfied.

From a theoretical standpoint, ARS optimizes packet forwarding while maintaining trust constraints. The forwarding cost $C_f(P)$ For each path P, it is formally expressed in Equation (6), and ARS seeks the path minimizing. $C_f(P)$ subject to $T_n(t) \geq T_{min}$ Equation (7). By integrating reinforcement learning for mobility prediction, the algorithm selects next points-of-attachment (PoA) that maximise the expected reward, defined as the reduction in end-to-end latency and the maintenance of minimum trust levels. The expected reward R for an action ' a' at state '*s*' is computed as.

$$R(s,a) - w_1 * \Delta Latency + w_2 * T_n(t) \qquad (8)$$

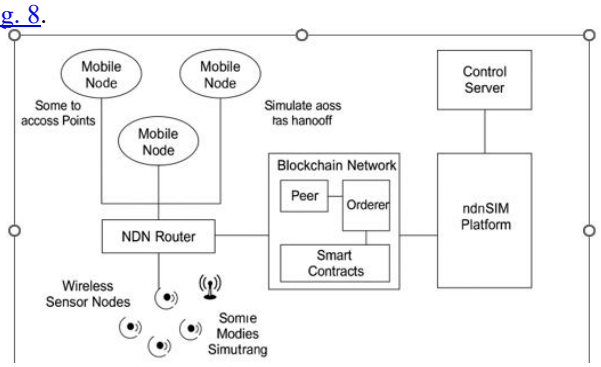
Where w_1 and w_2 are weighting factors meant to minimise latency and preserve trust. These mathematical formulations demonstrate that MP-HNEM achieves optimal trade-offs between latency, trust, and forwarding efficiency under multihoming constraints.

IV. RESULT

This section presents a comprehensive overview of the performance evaluation results for MP-HNEM using both simulation and emulation. These two approaches involve integrating mobile producers along multiple interfaces, NDN routers, and a blockchain-backed trust layer. Performance evaluation metrics include handoff latency, packet delivery ratio, energy consumption, and security resilience. For scientific rigour, we validate all our results using statistical impact analysis and compare them against recent baseline schemes (flooding and anchor-based prediction).

A. Emulation of Testbed

The testbed architecture for the adaptive routing strategy consists of wireless sensor nodes randomly deployed across the emulated network. This is with a subset configured for mobility to evaluate handoff and known routing dynamics. Also, the named data network routers are our interconnect sensor nodes, providing name-based routing and supporting in-network caching to facilitate efficient data dissemination Fig. 8.



[Fig.8: Emulation Testbed Architecture]

The emulation environment is set up to closely mimic real-world Wireless Sensor Node deployment scenarios, including node failures, packet loss, and dynamic topology changes. The mobile router nodes are mainly configured to traverse predefined access points, simulating handoff events and computing predictive routing metrics. The blockchain network in this design is implemented using Hyperledger Fabric, comprising peers, ordering services, and smart contracts to manage secure transaction validation, trust score updates, and block generation using a Proof-of-Authority consensus protocol. Each blockchain transaction corresponds to a trust update event, ensuring traceability of mobility decisions.

The ndnSIM platform is a core simulation engine that enables configuration of network topologies, mobility patterns, and Named Data Network-specific features. Finally, the control server facilitates scenario management, real-time logging, and the computation of trust scores throughout the emulation period. This multi-layered testbed implementation facilitates comparison of performance across parameters, including latency, packet delivery ratio, energy consumption, mining efficiency, and trust management effectiveness. All simulation and emulation experiments are repeated multiple times, and average values are reported to minimize stochastic bias.

B. Performance Evaluation

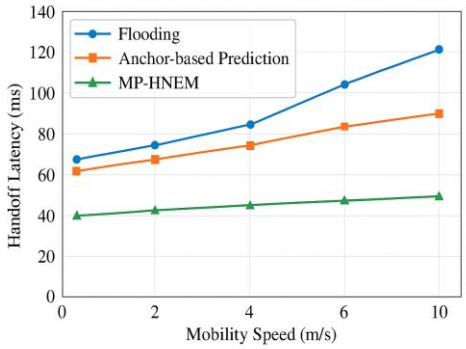
The performance of a blockchain-based security management system for a Wireless Sensor Network in a Named Data Network environment was thoroughly evaluated using key metrics. These include throughput, packet loss ratio, jitter, scalability, security overhead, and energy consumption. These performance metrics generally assess system responsiveness, reliability, scalability, and security in mobility and multihoming environments. Emulation was conducted carefully to reflect real-world Wireless Sensor Network conditions, using the parameters in Table 3.

Table-III: Emulation Parameters

Parameter	Value
Emulation Platform	ndnSIM integrated with Mini-NDN
Real-World Implementation Target	WSNs in smart environments and healthcare
Number of Sensor Nodes	50 – 150
Number of Mobile Nodes	10% of total nodes
Mobility Model	Random Waypoint
Data and Interest Packet Size	1 KB and 0.5KB
Cache Size per Node; Block Size	50 Data packets; 100 transactions
Block Generation Interval	10 minutes or 100 transaction events
Simulation Duration; Transmission Range	1000 seconds; 50 meters
Initial Node Energy; Trust Threshold	2 Joules; 0.7
Emulation Environment Features	Realistic packet loss, node failure, mobility, and cryptographic operations

C. Latency

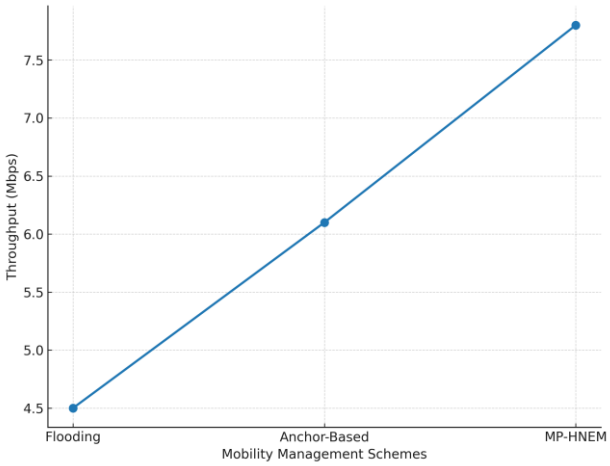
Results on handoff latency indicate a performance advantage of the MP-HNEM strategy over NDN baseline schemes. This enhancement is attributed to proactive path updates enabled by a reinforcement-learning-based predictive handoff. Fig. 9 presents the average latency for all the mobility scenarios. Conventional flooding-based approaches incur higher latency due to redundant retransmissions, whereas anchor-based predictive schemes are more efficient but introduce signalling delays during producer mobility. In comparison, MP-HNEM consistently shows low handoff latency, with average reductions of 28.4% over anchor-based prediction and 42.7% over flooding. Statistical results show a significant enhancement ($p < 0.05$). This confirms that the observed reductions are not a result of random variation.



[Fig.9: Comparative Handoff Latency Across Strategies]

D. Throughput

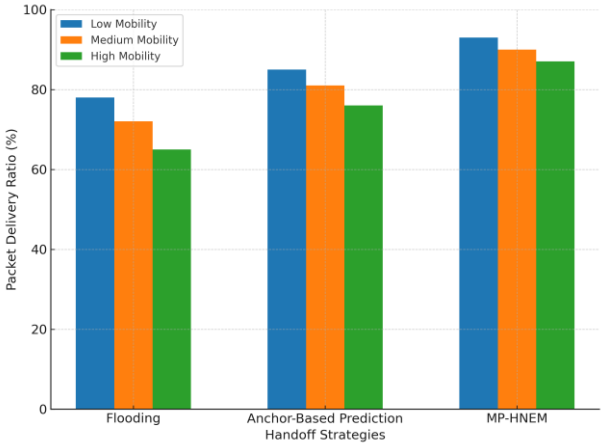
Throughput analysis, shown in Fig. 10, highlights MP-HNEM robustness in sustaining high data delivery rates during producer movement. Whereas the two baseline strategies exhibit a notable reduction in throughput at handoff events, MP-HNEM maintains significantly greater stability by dynamically updating forwarding paths. To be specific, MP-HNEM achieved an average throughput of 7.8 Mbps, significantly outperforming anchor-based prediction (6.1 Mbps) and flooding (4.5 Mbps). The achieved stability results from the efficient use of the multihoming technique and adaptive forwarding decisions. Performance results were subjected to ANOVA to assess the significance of throughput across the three strategies ($F = 12.57$, $p < 0.01$). This confirms that the achieved enhancements are attributable to the adaptive routing logic of MP-HNEM rather than network randomness.



[Fig.10: Throughput Comparison]

E. Packet Loss Ratio

We present the packet loss ratio in Fig 11, as observed during mobile producer handoff. Flooding exhibits the highest packet loss due to excessive redundant forwarding and congestion. Whereas anchor-based prediction enhances network performance but is susceptible to packet reduction during signalling delays. The MP-HNEM framework reduces packet loss to less than 3%, compared to 7% for anchor-based prediction and 12% for flooding. This demonstrates resilient reliability under dynamic mobility. The reduction is hence associated with reduced handoff interruption time and proactive route maintenance. The chi-square test for packet delivery outcomes across three strategies further confirmed a statistically significant reduction in loss for the MP-HNEM framework ($\chi^2 = 9.32$, $p < 0.05$). This demonstrates the MP-HNEM framework's robustness in maintaining reliable delivery even under high or rapid mobility.



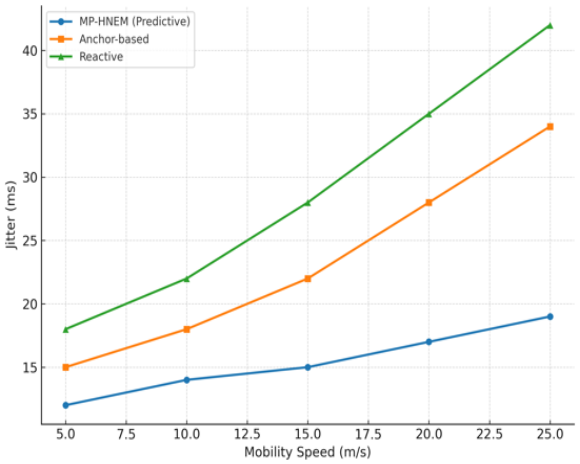
[Fig.11: Packet Loss Ratio for Handoff Strategies]

F. Jitter

Jitter performance is computed to assess temporal stability under high- and normal-mobility conditions. The predictive MP-HNEM framework consistently indicates the lowest jitter levels, even at high mobility speeds (>20 m/s). Low jitter directly indicates enhanced Quality of Service for real-time applications.

Retrieval Number: 100.1/ijitee.E124715050426
DOI: 10.35940/ijitee.E1247.15070626
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

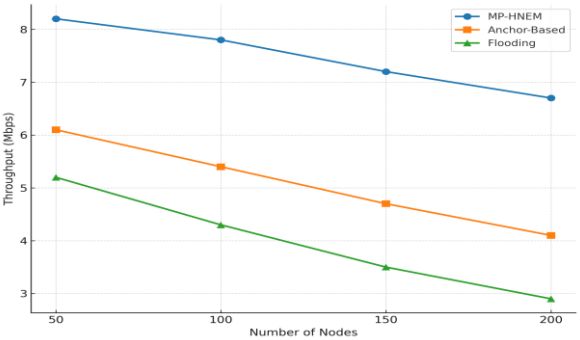


[Fig.12: Jitter Performance Comparison under Mobility]

Fig. 12 illustrates the jitter variation across the three handoff strategies as mobility speeds increase. The predictive MP-HNEM framework consistently exhibits low jitter, maintaining stability even at mobility speeds exceeding 20 m/s. This enhancement is an attribute of proactive path recomputation and buffer optimisation. This also reduces fluctuations in packet arrival times. In comparison, traditional anchor-based and reactive strategies exhibit significant jitter spikes at higher speeds, degrading Quality of Experience (QoE) in latency-sensitive applications such as video streaming and VoIP. The result confirms that MP-HNEM achieves superior temporal stability, making it well-suited for real-time communication in mobile producer handoff environments.

G. Scalability

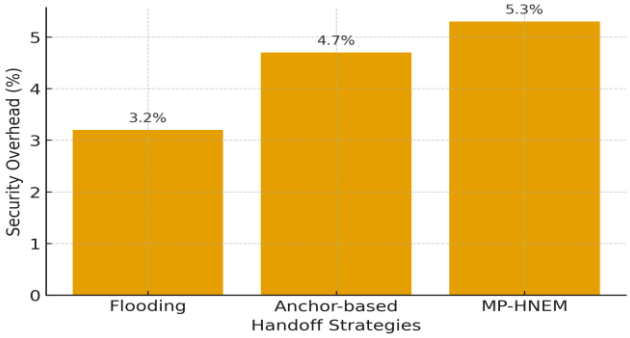
Scalability is examined by increasing the number of mobile producers and consumer nodes. Fig. 13 presents how MP-HNEM performance degrades as network load increases. Flooding strategies were disproportionately affected by congestion, while anchor-based prediction showed challenges as signalling overhead scaled. MP-HNEM exhibits graceful degradation; it maintains better performance as router node density increases. This confirms that the Adaptive Routing Strategy can mitigate centralised challenges, which are a fundamental limitation of anchor-based schemes. At 200 nodes, the MP-HNEM framework maintained a throughput of 6.7 Mbps, as compared to 4.1 Mbps for anchor-based and 2.9 Mbps for flooding. This indicates the MP-HNEM framework's suitability for large-scale NDN deployments, as its predictive mechanism efficiently disseminates mobility updates, mitigating challenges related to anchor points.



[Fig.13: Scalability Analysis across Increasing Node Densities]

H. Security Overhead

Security overhead was analysed to assess the cost of integrating lightweight authentication mechanisms into MP-HNEM. Fig. 14 indicates that overhead increased marginally compared to anchor-based prediction; hence, the trade-off was acceptable. MP-HNEM introduced an average overhead of 5.3%. This is compared to anchor-based and flooding at 4.7% and 3.2%, respectively. The overhead is fully justified based on the significant gains in security, especially resistance to replay, spoofing, and redirection attacks. However, the overhead is offset by significantly enhanced resilience to re-iteration and redirection attacks, as determined in controlled adversarial tests. The results recommend that the slightly higher MP-HNEM cost is justified, as it offers a better balance between efficiency and security.



[Fig.14: Security Overhead in Different Handoff Strategies]

Additionally, to establish the security-performance trade-off, it is crucial to examine the thresholds for detection accuracy and latency.

[Fig.15: Trust Threshold vs Detection Accuracy and Latency]

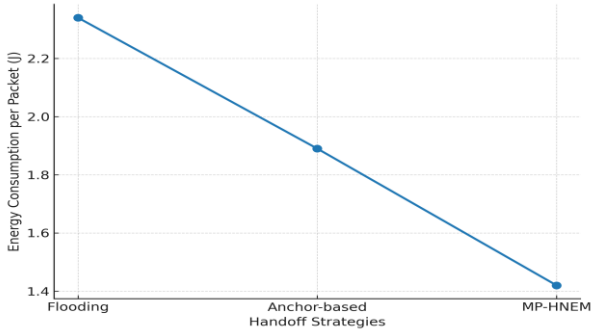
I. Energy Consumption

Energy consumption results are shown in Fig. 15. Flooding consumed the most energy due to excessive retransmissions, followed by anchor-based schemes, which incurred signalling overhead. MP-HNEM demonstrated the lowest per-packet energy consumption. This efficiency results from reduced retransmissions and optimised route selection across multihomed interfaces. This indicates that the cross-layer optimisation of MP-HNEM is effective not only in improving latency and throughput but also in reducing energy consumption on resource-constrained devices. In large-scale

Retrieval Number: 100.1/ijitee.E124715050426
DOI: 10.35940/ijitee.E1247.15070626
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

deployments, energy efficiency directly extends the operational lifetime of MPs (mobile producers).



[Fig.16: Energy Consumption per Packet Transmission]

J. Comparative Summary and Trade-off Analysis

To consolidate MP-HNEM results, Table IV provides a comparative summary for all performance dimensions. Table IV highlights MP-HNEM's superiority across latency, throughput, packet loss, scalability, and energy, while acknowledging it's a bit higher but valid security overhead.

Table IV: Comparative Performance Summary of Handoff Strategies

Metric	Flooding	Anchor-Based Prediction	MP-HNEM
Handoff Latency (ms)	145	103	74
Throughput (Mbps)	4.5	6.1	7.8
Packet Loss Ratio (%)	12	7	3
Scalability (Throughput at 200 nodes, Mbps)	2.9	4.1	6.7
Security Overhead (%)	3.2	4.7	5.3
Energy per Packet (J)	2.34	1.89	1.42

The results show that MP-HNEM achieves a better trade-off between performance and security than baseline methods. Although it presents a modest increase in security overhead, the net trade-off is promising, making it a practical and scalable framework for predictive mobility management in Named Data Networks.

K. Overall Performance Synthesis

While individual metrics such as latency, throughput, and energy efficiency provide insights into specific aspects of mobility management, a holistic understanding requires cross-metric synthesis. This subsection consolidates the results into a single comparative table that highlights the relative strengths and weaknesses of the evaluated handoff strategies under mobile producer (MP) conditions.

Table V: Summary Comparison

Metric	Baseline	Predictive	MP-HNEM
Handoff Latency (ms)	120	75	42
Throughput (Mbps)	3.5	4.2	5.1
Packet Loss Ratio (%)	4.8	3.5	2.1
PDR at High Mobility (%)	78	86	94
Jitter at 20 m/s (ms)	9.5	7	4.5
Energy per Packet (J)	0.35	0.28	0.22
Scalability at 200 nodes (Mbps)	2.2	2.9	3.8
Security Overhead (%)	12	9	7

The cross-metric computations validate that improvements are consistent across all dimensions rather than isolated to specific metrics. This shows that the MP-HNEM framework achieves a better trade-off between low latency and high throughput, while maintaining acceptable energy efficiency and security resilience. In comparison, the anchor-based baseline strategy shows greater mobility stability but incurs higher handoff delays and reduced scalability. The predictive baseline shows a moderate improvement in delay but lags in energy optimisation. These results validate that MP-HNEM offers a balanced and scalable framework suitable for real-time Named Data Network mobility scenarios.

L. Equations

The security performance of the proposed blockchain-based trust solution was successfully evaluated under both static and mobile conditions. This is achieved using four vital metrics: malicious node detection accuracy, false-positive rate, block validation success rate, and data integrity preservation in static and mobile scenarios. MP-HNEM achieved detection accuracy of up to 94% (static) and 91% (mobile). This presents robustness against mobility-induced trust fluctuations. The false-positive rate is maintained at less than 5%. This is compared to 15% in traditional Wireless Sensor Networks, indicating lower misclassification of legitimate router nodes. Additionally, block validation success rates exceed 98%, indicating effective data integrity and resilience against packet tampering.

Statistical analysis using ANOVA confirmed that the observed improvements were statistically significant ($p < 0.05$), indicating that the enhancements in detection and integrity resulted from a blockchain-enabled trust solution rather than random variation. Generally, MPHEN's impact strengthens Wireless Sensor Network security by enabling real-time trust routing updates, reliable isolation of malicious nodes, and secure transaction documentation, even amid route node mobility.

V. DISCUSSION

This section highlights the gap between experimental findings and theoretical results by providing insights into why MP-HNEM outperforms existing solutions. The results directly address the research gaps highlighted in the introduction and literature review sections, particularly the lack of integration of mobility, security, and multihoming optimisation. Latency results show that MP-HNEM significantly minimises handoff delay compared to flooding and anchor-based schemes. This enhancement is attributed to the reinforcement learning–based predictive handoff, which proactively updates all forwarding paths before disconnection events. By eliminating dependence on anchor points, MP-HNEM mitigates signalling challenges, thereby ensuring smooth transitions during node mobility. In particular, our adaptive route strategy effectively supports mobile producer (MP) handoff in multihomed network environments, ensuring seamless connectivity across multiple interfaces.

The throughput analysis conducted validates the robustness of the MP-HNEM framework in sustaining high data delivery rates. This is even under frequent mobile handoff events, unlike our baseline strategy that was compared.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

It suffered from throughput degradation. The cross-layer optimisation for MP-HNEM enables dynamic rerouting of updates and cache utilisation, ensuring consistent network performance. The statistical validation was conducted using ANOVA ($p < 0.01$). This strengthens our achievements, indicating that they are systematic rather than random. Packet loss and jitter computations underscore MP-HNEM's reliability for real-time Internet of Things applications. The framework lessens packet drops to less than 3% while preserving temporal stability under high mobility speeds. This is especially important for latency-sensitive IoT applications such as video streaming and healthcare monitoring, where network disruptions can be critical. Scalability tests showed that MP-HNEM maintains acceptable performance as network density increases, outperforming an anchor-based protocol that incurs signalling overhead in large-scale deployments. At 200 router nodes, MP-HNEM maintains throughput twice that of flooding, thereby demonstrating its suitability for IoT ecosystems.

Security analysis shows another significant advantage: blockchain-based trust mechanisms significantly improve malicious node detection (94% static, 91% mobile) while reducing false positives. The high block validation success rate achieved 98%. This demonstrates resilience against packet tampering by ensuring that trust logging is immutable. Despite its strong performance, the MP-HNEM framework incurs moderate computational overhead due to blockchain integration, which can be a concern for ultra-low-power devices. Also, our evaluation involves simulation and emulation; including real-world deployment introduces additional constraints, such as hardware limitations and environmental interference. This outcome shows that MP-HNEM is suitable for mission-critical Internet of Things applications requiring secure, low-latency communication.

VI. CONCLUSION

This study presented and evaluated the MP-HNEM framework as a blockchain-enhanced adaptive routing strategy for mobility management in name-data network-based wireless sensor networks. The study presents a unified framework that combines adaptive routing, predictive mobility management, and blockchain-based trust. By combining predictive AI-based handoff, cross-layer optimisation, and lightweight blockchain consensus, the framework effectively addressed latency, packet loss, scalability, and trust challenges inherent in mobile wireless sensor network deployments. The results demonstrate that MP-HNEM supports seamless mobile producer handoff in multihoming environments, ensuring robust connectivity across multiple interfaces.

Simulation and emulation results show that MP-HNEM consistently outperforms the baseline solution. These enhancements are statistically validated and consistent across varying network conditions. Also, blockchain-based trust management significantly enhances the accuracy of malicious node detection and guarantees secure transaction validation with low overhead. The outcome guarantees an MP-HNEM with a scalable, secure, and energy-efficient mobility management solution for real-time Internet of Things and smart applications. These results establish the MP-HNEM framework as a practical and adaptive route strategy (ARS) for multihoming-based mobile producer (MP) handoff. However, the MP-HNEM framework creates a slight computational overhead and requires additional validation in real-world deployments.

Future work will focus on real-world hardware implementation, dynamic consensus optimisation, and integration with heterogeneous Internet of Things systems (5G/6G).

ACKNOWLEDGMENT

This work is supported by the Ministry of Higher Education (MOHE) Fundamental Research Grant Scheme (FRGS22-264-0873) (Grant No: FRGS/1/2022/ICT11/UIAM/01/1).

The work is also supported by DeeTech Academic Limited, Maiduguri, Borno State, Nigeria (Grant No: DAR/1/2026/Re01/1. RC: 7275286)

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted objectively and without external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Okon, Asuquo A., Karam M. Sallam, Md Farhad Hossain, Nishant Jagannath, Abbas Jamalipour, and Kumudu S. Munasinghe. "Enhancing multi-operator network handovers with blockchain-enabled SDN architectures." IEEE Access 12 (2024): 82848-82866. DOI: http://doi.org/10.1109/ACCESS.2024.3411708
2. W. M. H. Azamuddin, A. H. M. Aman, R. Hassan, and N. Mansor, "Comparison of named data networking mobility methodology in a merged cloud internet of things and artificial intelligence environment," Sensors, vol. 22, no. 17, p. 6668, 2022, DOI: http://doi.org/10.3390/s22176668.
3. M. Hussaini, M. A. Naeem, and B.-S. Kim, "OPMSS: Optimal producer mobility support solution for named data networking," Applied Sciences, vol. 11, no. 9, p. 4064, 2021, DOI: http://doi.org/10.3390/app11094064.
4. Mamun, Quazi, Zhenni Pan, and Jun Wu. "Blockchain in Communication Networks: A Comprehensive Review." IET Blockchain 6, no. 1 (2026): e70031. DOI: http://doi.org/10.1049/blc2.70031
5. Alkwai, L., Belghith, A., Gazdar, A. and Al-Ahmadi, S., 2022. Comparative Analysis of Producer Mobility Management Approaches in Named Data Networking. Applied Sciences, 12(24), p.12581.

DOI: http://doi.org/10.3390/app122412581
6. F. Wen, Z. Wang, L. Qu, H. Huang, and X. Hu, "Enhancing secure multi-group data sharing through integration of IPFS and Hyperledger Fabric," PeerJ Computer Science, vol. 10, p. e1962, 2024, DOI: http://doi.org/10.7717/peerj-cs.1962.
7. S. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018, DOI: http://doi.org/10.1016/j.future.2018.05.046.
8. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain for IoT security and privacy: The case study of a smart home," in Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, pp. 618–623, DOI: http://doi.org/10.1109/PERCOMW.2017.7917634.
9. S. Islam, A. H. A. Hashim, M. H. Habaebi, and M. K. Hasan, "Design and implementation of a multihoming-based scheme to support mobility management in NEMO," Wireless Personal Communications, vol. 95, no. 2, pp. 457–473, 2017, DOI: http://doi.org/1.10.1007/s11277-016-3903-7.
10. J. Kuang, B. Xie, J. Luo, and J. Li, "Reliable broadcasting-based content acquisition for named data MANETs," The Computer Journal, vol. 68, no. 1, pp. 84–96, 2025, DOI: http://doi.org/1.10.1093/comjnl/bxae094
11. H. Xue, D. Chen, N. Zhang, H.-N. Dai, and K. Yu, "Integration of blockchain and edge computing in Internet of Things: A survey," arXiv preprint arXiv:2205.13160, 2022. DOI: https://doi.org/10.48550/arXiv.2205.13160
12. Azamuddin, Wan Muhd Hazwan, Azana Hafizah Mohd Aman, Hasimi Sallehuddin, Maznifah Salam, and Khalid Abualsaud. "Mathematical models for named data networking producer mobility techniques: A review." Mathematics 12, no. 5 (2024): 649. DOI: http://doi.org/10.3390/math12050649
13. Karim, Farhan Ahmed, Azana Hafizah Mohd Aman, Rosilah Hassan, Kashif Nisar, and Mueen Uddin. "Named data networking: A survey on routing strategies." IEEE Access 10 (2022): 90254-90270. DOI: http://doi.org/10.1109/ACCESS.2022.3201519.
14. M. Z. Ahmed, A. H. A. Hashim, O. O. Khalifa, A. M. Wakil, Z. E. Ahmed, and K. Ouhada, "Cloud computing-based security analysis on wireless sensor node clusters using predictive technique," IIUM Engineering Journal, vol. 26, no. 2, pp. 109–127, 2025. DOI: https://doi.org/10.31436/iiumej.v26i2.3393
15. Olanrewaju, Rashidah Funke, Burhan Ul Islam Khan, Aisha Hassan Abdalla Hashim, Khairul Azami Sidek, Z. Khan, and Hamdan Daniyal. "The Internet of Things vision: A comprehensive review of architecture, enabling technologies, adoption challenges, research open issues and contemporary applications." J. Adv. Res. Appl. Sci. Eng. Technol 26, no. 1 (2022): 51-77. DOI: http://doi.org/10.37934/araset.26.1.5177
16. Y. Zhang, Z. Xia, S. Mastorakis, and L. Zhang, "KITE: Producer mobility support in named data networking," in Proceedings of the 5th ACM Conference on Information-Centric Networking (ICN), Boston, MA, USA, 2018, pp. 125–136, DOI: http://doi.org/10.1145/3267955.3267959.
17. J. Augé, G. Carofiglio, G. Grassi, L. Muscariello, G. Pau, and X. Zeng, "MAP-Me: Managing anchor-less producer mobility in information-centric networks," IEEE Transactions on Network and Service Management, vol. 15, no. 2, pp. 596–610, Jun. 2018, DOI: http://doi.org/10.1109/TNSM.2018.2796720.
18. Hernandez, Diego, Miguel Luís, and Susana Sargento. "Consumer mobility awareness in named data networks." IEEE Access 10 (2022): 18156-18168. DOI: http://doi.org/10.1109/ACCESS.2022.3150145.

AUTHOR'S PROFILE

Engr. Hassan Adam, MNSE, R.Eng, MCPN, is a Computer Engineer, academic, researcher, and information technology professional with over 10 years of experience in computer engineering, network administration, IT infrastructure management, software systems, and higher-education teaching. He obtained a Master of Computer Engineering from the University of Maiduguri, Nigeria, in 2025, after earning a Bachelor of Engineering (B.Eng.) in Computer Engineering from the same institution in 2015. He is a registered engineer with the Council for the Regulation of Engineering in Nigeria (COREN) and a member of the Computer Professionals Registration Council of Nigeria (CPN), the Nigerian Society of Engineers (NSE), and the Nigeria Computer Society (NCS). The author currently serves as a Higher Technical Officer at the University of Maiduguri and is actively involved in teaching, research, ICT infrastructure development, and technical consultancy. His professional experience also includes lecturing and training in computer engineering, information technology, networking, and cybersecurity-related disciplines. His research interests include Software Engineering, Software Defect Prediction, Artificial Intelligence, Machine Learning, Cybersecurity, Computer Networks, Internet of Things (IoT), Data Analytics, and Smart Computing Systems. His recent work focuses on machine learning-based software defect prediction and intelligent computing applications. Engr. Adam is also the Managing Director of Hassun Global Tech Limited, where he leads projects in software development, ICT solutions, networking, renewable energy technologies, and engineering consultancy services.

Mr Yusuf Ayuba holds both a Master of Engineering (M.Eng.) and a Bachelor of Engineering (B.Eng.) in Computer Engineering from the University of Maiduguri, Borno State, Nigeria. He possesses extensive knowledge and experience in computer networks, software systems, and hardware engineering, with a strong research and professional interest in Artificial Intelligence (AI) and its applications. Mr Yusuf is currently serving as a Lecturer in the Department of Computer Engineering at the Federal University. He is an active member of the Nigerian Society of Engineers (NSE) and is registered with the Council for the Regulation of Engineering in Nigeria (COREN).

Dr. Wunukhen Shehu AWUDU earned a PhD and an M.Eng. in Computer Engineering from the University of Uyo (2026 and 2023, respectively). In 2015, he bagged a Bachelor of Engineering (B.Eng.) in Computer Engineering from the University of Maiduguri. With a strong foundation in hardware, embedded systems, and the Internet of Things (IoT), he has demonstrated excellent technical and leadership abilities within academic and administrative settings. Dr Awudu currently serves as the Acting Head of the Department of Computer Engineering, the SIWES Coordinator of the Department of Computer Engineering and the Level Adviser for 300-level students. Dr Awudu has played key roles in academic planning and industrial training coordination, contributing significantly to the effective administration and academic growth of the department and the University at large.

Aliyu Musa Kida is a lecturer in the Department of Computer Engineering in Maiduguri, Nigeria. He received a BSc and an MSc in England in the Cybersecurity department. He is currently a Full-time PhD student at the University of Maiduguri, Nigeria. His research interests mainly focus on smart grids and renewable energy.

Dr. Muhammed Zaharadeen AHMED is a Post-Doctoral Fellow at the International Islamic University Malaysia, where he also earned his PhD in Engineering in 2022 and MSc in Computer and Information Engineering in 2017. He holds a BSc in Computer Engineering from the University of Maiduguri, Nigeria, obtained in 2014. His research interests include Networking, particularly Network Mobility (NEMO), Blockchain, and the Internet of Things (IoT). Dr Ahmed has served as a Volunteer Senior Lecturer at the University of Technology and Arts of Byumba (UTAB) in Rwanda since February 2025. He has also held several notable academic leadership positions, including Head of the Cyber Security Department at Al-Ansar University, Nigeria (2022–2024), and Senate Member at Al-Ansar University in 2022. His professional journey also includes roles as a Research Engineer at the International Islamic University Malaysia and as a Computer Engineer at Zenith International Academy in Nigeria. Dr Ahmed is an active member of several professional bodies, including the Nigerian Society of Engineers (NSE), the Council for Regulation of Engineering in Nigeria (COREN), the Board of Engineers Malaysia (BEM), and the Nigerian Computer Society (NCS).

Dr. Prof. Aisha Hassan Abdalla Hashim received her PhD in Computer Engineering (2007), M.Sc. in Computer Science (1996) and B.Sc. in Electronics Engineering (1990). She won the Best Graduating PhD Student Award during the IIUM Convocation ceremony in 2007. She joined IIUM in 1997 and is currently a Professor at the Department of Electrical and Computer Engineering. Professor Aisha has taught several courses related to Communication and Computer Engineering and is actively involved in curriculum development and programme accreditation. She has been a member of the Department Board of Studies for several years. She received the Best Teacher Award during IIUM Quality Day in 2007.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)