[1]Zubair Ahmed Khan

[2]Dr. Asha Ambhaikar

Identity Based Authentication Scheme (IAS) for Securing WSN Based Internet of Things

Journal of Electrical Systems

Abstract: - The growing number of connected devices in IoT networks has raised security concerns. These networks face unique challenges, including limited resources, lack of standardized security protocols, and diverse devices and applications. Identity-based authentication is needed to address these threats and limitations. Implementing a multi-factor authentication system can enhance security and protect sensitive information from unauthorized access. The proposed Identity Based Authentication (IAS) scheme is implemented using the NS-2 simulator to address security challenges in IoT networks. Each node is assigned a unique identity for authentication, ensuring only authorized access and preventing security breaches. The IAS scheme enhances IoT network security by verifying node identities. Two scenarios are considered to evaluate the scalability and interoperability of the IAS scheme. The first scenario involves a random environment, assessing performance in real-world settings with varying device densities and network conditions. The second scenario involves a cluster-based environment, providing insights into the scheme's functionality and efficiency. By examining both scenarios, this research aims to provide a comprehensive understanding of how the authentication scheme performs in different deployment scenarios. The findings highlight the importance of selecting the appropriate authentication scheme based on the specific network environment and requirements. The superiority of the IAS authentication scheme suggests its potential for widespread adoption and implementation in various network scenarios over other authentication schemes.

Keywords: Internet of Things (IoT), Network security, Identity Based Authentication (IAS) scheme, NS-2 simulator, Random environment, Cluster-based environment

I. INTRODUCTION

The seeds of WSN-based IoT networks were sown in the 1990s with the emergence of micro-electromechanical systems (MEMS), enabling miniaturized, low-cost sensors [1]. Early deployments focused on military and industrial applications, with networks monitoring battlefield environments or factory machinery [2]. The early 2000s saw the rise of ubiquitous computing and radio frequency identification (RFID), pushing the boundaries of wireless connectivity [3]. This, coupled with advancements in sensor technology and communication protocols, paved the way for WSNs to enter consumer markets. By the mid-2000s, the term "Internet of Things (IoT)" gained traction, envisioning a connected world where physical objects communicate and share data. WSNs became a crucial building block, enabling real-time data collection from diverse environments [4,5].The late 2000s witnessed an explosion in WSN-based IoT applications, from environmental monitoring to smart cities and industrial automation [6]. This rapid growth fueled research and development in areas like energy efficiency, security, and scalability [7].

Today, WSN-based IoT networks are ubiquitous, driving advancements in fields like healthcare, agriculture, and disaster management. Looking ahead, the future lies in integrating artificial intelligence and edge computing at the network edge, further blurring the lines between the physical and digital worlds [8].

The burgeoning world of WSN-based IoT networks, brimming with transformative potential, harbors a dark underbelly: rampant security vulnerabilities. Like fragile fortresses in a turbulent digital landscape, these networks require robust security measures to shield their sensitive data and critical infrastructure from a multitude of threats.Unique vulnerabilities: WSN nodes, often resource-constrained with limited processing power and memory, are susceptible to lightweight attacks that exploit their inherent weaknesses [9]. From personal health information to industrial secrets, WSNs collect and transmit a vast array of sensitive data. Breaches can have devastating consequences, impacting privacy, safety, and financial stability [10]. Network complexity: The sheer

[1] PhD. Research Scholar, Department of CSE, Kalinga University, Raipur, Chhattisgarh

Email: zubairashrafi786@hotmail.com

[2]Professor, Department of CSE & IT Kalinga University, Chhattisgarh, India

Email: asha.ambhaikar@kalingauniversity.ac.in

number and diverse nature of connected devices in an IoT ecosystem create a complex attack surface, making it challenging to implement comprehensive security solutions [11].

Malicious actors can intercept data transmissions, steal sensitive information, or manipulate data to disrupt critical operations [12]. Hackers can infiltrate and hijack nodes, disrupting network communication or launching denial-of-service attacks that cripple the entire network [13]. The physical accessibility of WSN nodes makes them vulnerable to physical attacks that can damage or destroy them, compromising data integrity and network functionality [14]. Implementing robust encryption protocols ensures data confidentiality and integrity during transmission and storage [15]. Employing secure authentication and authorization mechanisms verifies the identity of devices and users, preventing unauthorized access [16,17].

The remainder of this paper is organized as follows: Section 2 presents a literature survey on the relevant proposed research topics. Section 3 describes the proposed methodology for the research work, including the modules, routing protocols, and performance parameters considered. Section 4 describes the analysis of the simulation experiments' results, and the paper is concluded in Section 5.

Contributions in this paper

- To boost wireless IoT security, IAS needs innovative key management that minimizes reliance on central servers and leakage risks. Lightweight cryptography should be integrated for performance, and resilience against new threats like spoofing and jamming must be analyzed and enhanced. This will solidify the security of both communication and infrastructure in the IoT ecosystem.
- Lean IAS protocols minimize resource drain on battery life and processing, optimizing for resource-constrained IoT devices.Scalable and adaptable protocols handle diverse deployments and adapt to individual environments. Interoperability and standardization allow seamless communication across platforms and applications, boosting overall efficiency.
- Validate IAS performance, security, and privacy through real-world testing and open-source contributions. Formalize security guarantees and benchmark against existing solutions to demonstrate IAS's edge. Identify open challenges and future directions to guide the evolution of IAS for wireless IoT.

II. RELATED WORK

The article [18] highlights the importance of implementing security measures in WiMAX-based IoT systems due to their vulnerability to various attacks. The proposed Optimized Privacy Information Exchange Schema aims to address these vulnerabilities and improve the functionality and performance of the traditional system, with validation from the Scyther tool. The paper [19] presents a deep learning-based intrusion detection system for the IoT environment, specifically targeting DDoS attacks. The proposed model combines different types of deep neural networks to leverage their unique properties and achieve high performance. The evaluation results show that the model outperforms other machine learning and deep learning models in terms of various performance metrics. The study in [20] highlights the importance of addressing version attacks in RPL-based IoT networks, particularly in a mobile environment, as these attacks can lead to network instability and denial of service. The research provides a performance metric-based analysis to understand the impact of version attacks on packet delivery, delay, and power consumption, emphasizing the need for preventive measures to maintain the stability of mobile networks in IoT applications.

The paper [21] highlights the significance of IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) in driving the growth of the Internet of Things (IoT) market. It discusses the challenges of energy-efficient routing in 6LoWPAN and the security concerns associated with the Routing Protocol for Low-power and Lossy Networks (RPL). The paper proposes a lightweight Challenge-Response Authentication-based technique called CRA-RPL to secure RPL against DDAO attacks, which has been successfully implemented and validated in experimental settings. The paper [22] highlights the increasing utilization of Wireless Sensor Networks (WSN) and the corresponding rise in attacks on these networks. The use of learning models in WSN, specifically for attack detection, has shown to yield highly accurate results compared to classical detection methods. The study focuses on three network layer attacks and evaluates the performance of various machine learning and deep learning models using a large dataset. The paper [23] highlights the importance of addressing the security concerns in the Metaverse, particularly in relation to the detection of wormhole attacks. The study aims to investigate the impact and characteristics of these attacks in mobile cloud and Metaverse environments, and proposes a novel defense mechanism design to combat them.The paper [24] highlights the rise of smart vehicles and the corresponding increase in cyber threats, emphasizing the need for ensuring the security of these vehicles and their associated equipment. The paper aims to examine detection methods for various networks and analyzes recently published studies in the field, evaluating datasets, simulations/implementations, and key evaluation criteria. It also discusses the challenges and future research opportunities in detecting intrusions, anomalies, and attacks in smart vehicles.

The paper [25] highlights the importance of addressing security and privacy concerns in Smart Home Systems (SHSs) through the use of Machine Learning (ML)-based Intrusion Detection Systems (IDS). The study specifically focuses on the energy consumption of on-device ML algorithms for IoT intrusion detection applications and finds that deploying the Decision Tree (DT) algorithm on-device offers superior results in terms of training time, inference time, and power consumption. The technique known as Pelican Optimization Algorithm with Federated Learning Driven Attack Detection and Classification (POAFL-DDC), proposed in the paper [27], presents a versatile and efficient approach to identify attacks within the realm of the Internet of Things (IoT). By utilizing decentralized on-device data and federating training cycles on a Deep Learning (DL) model, this technique outperforms other models and addresses the limitations of machine learning (ML) approaches in the IoT. The paper [28] highlights the challenges of detecting attacks in Wireless Sensor Networks (WSNs) and introduces the Proportional Overlapping Score-Based Minkowski K-Means Clustering (POS-MKC) technique as a solution. This technique improves attack detection accuracy, reduces computational complexity, and enhances packet delivery ratio in WSN healthcare applications.

III. MATERIALS AND METHODS

To begin, the researcher has gathered a wide range of research articles from reputable sources that discuss authentication schemes and security in wireless-based IoT systems which were discussed in previous chapter 2. These articles had been selected based on their relevance to the topic and their publication date, ensuring that the most recent research is included in the analysis. Once the articles have been collected, the researcher carefully read and analyzed each article to understand the different authentication schemes and security measures that have been implemented in wireless-based IoT systems. This research seeks to make a valuable contribution to the field of network security by presenting a novel Identity-Based Authentication Scheme (IAS). The research delves into the complexities of identity-based authentication, investigates the integration of this scheme into NS-2, and evaluates its effectiveness through a series of simulations.

Identity-Based Authentication Scheme (IAS) offers a novel approach to secure communication in wireless networks, particularly resource-constrained environments like the Internet of Things (IoT). Instead of relying on traditional Public-Key Infrastructure (PKI) with its complex key management, IAS leverages the unique identities of devices themselves as their cryptographic keys. Figure 1 shows the flowchart diagram for proposed IAS scheme.

Here's how IAS works, step-by-step:

1. Identity as the Key: Each node, say a sensor node in an IoT network, has a unique identifier (ID), termed as Node ID. This ID serves as the device's public key for encryption and decryption. The other information is not retrieved from the routing table list of nodes within the network.

2. Trust Recommendation: Nodes can also leverage recommendations from other nodes they trust. This allows them to gain insights into the trustworthiness of nodes they haven't interacted with directly. Recommendations can be explicit (e.g., messages, node is trustworthy or not) or implicit (e.g., routing decisions).

3. Digital Signing with Hash: Firstly, the message that needs to be transmitted is subjected to a secure hash function, such a*a. It is important to note that the size or format of the message does not affect the generation of this hash digest. After the hash digest is created, the sender employs their private key to encrypt it, resulting in the formation of the digital signature. The digital signature, along with the original message, is then transmitted to the intended receiver. On the receiver's end, the verification process takes place. The receiver obtains the sender's public key through a trusted channel. Using this public key, the receiver decrypts the digital signature, thereby recreating the original hash digest. In order to ensure the authenticity of the message, the receiver independently hashes the received message using the same hash function that was used by the sender. Finally, the receiver compares the recreated hash digest from the signature with the independently generated hash digest. The confirmation of a match between these two indicates that the message remains unaltered and can be considered genuine. This procedure of hash authentication offers a dependable method for ensuring the integrity of digitally transmitted messages, such as verifying the authenticity of "Digital Signature and Hash Function".

4. Lightweight Encryption: Encryption involves the process of transforming data by utilizing a mathematical algorithm and a secret key. This transformation ensures that the original data, also known as plain text, becomes incomprehensible to unauthorized individuals. It can be likened to securing valuable items within a locked treasure chest, as only those possessing the key can access its contents. Following the encryption process, the scrambled data, referred to as ciphertext, is then transmitted across a wireless network. Even if an unauthorized party intercepts this transmission, they will only encounter nonsensical and unintelligible information without the corresponding key.

Decryption, on the other hand, involves the receiving node utilizing its own secret key to verify and unlock the ciphertext. This step can be compared to using the correct key to open the aforementioned treasure chest, granting access to its concealed contents. Once the ciphertext is successfully decrypted, the data is transformed back into its original form, known as plain text. At this stage, the receiving node can comprehend and utilize the information contained within the data, enabling further analysis or application of the received data.

5. Neighbor Communication: Once authenticated, devices can communicate securely using their established identities and cryptographic keys. This enables secure data exchange and protects against unauthorized access and eavesdropping.

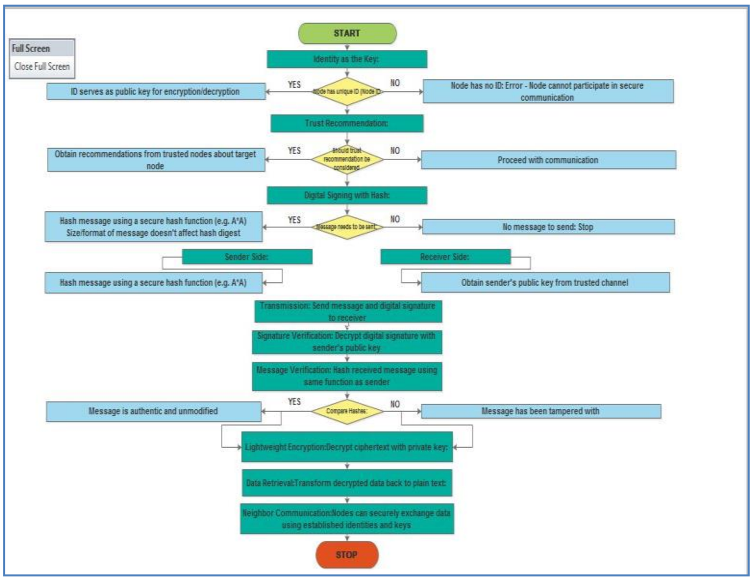

Full Screen
Close Full Screen
START
Identity as the Key:
YES
Node has unique ID (Node ID)
NO
ID serves as public key for encryption/decryption
Node has no ID: Error - Node cannot participate in secure communication
Trust Recommendation:
YES
Should trust recommendation be considered
NO
Obtain recommendations from trusted nodes about target node
Proceed with communication
Digital Signing with Hash:
YES
Message needs to be sent
NO
Hash message using a secure hash function (e.g. A*A) Size/format of message doesn't affect hash digest
No message to send: Stop
Sender Side:
Receiver Side:
Hash message using a secure hash function (e.g. A*A)
Obtain sender's public key from trusted channel
Transmission: Send message and digital signature to receiver
Signature Verification: Decrypt digital signature with sender's public key
Message Verification: Hash received message using same function as sender
YES
Compare Hashes:
NO
Message is authentic and unmodified
Message has been tampered with
Lightweight Encryption:Decrypt ciphertext with private key:
Data Retrieval:Transform decrypted data back to plain text:
Neighbor Communication:Nodes can securely exchange data using established identities and keys
STOP

Figure 1: Flowchart Diagram for IAS Scheme

IAS Pseudo Code Algorithm

```
1.    Identity as the Key:
      Node ID = unique_identifier()
      if Node ID is None:
      Error: Node cannot participate in secure communication
      else:
      Public Key = Node ID
      Go to Step 2
2.    Trust Recommendation:
      Trust_Score = 0
      if trust_recommendation_needed:
         Trust_Score += sum(trust_recommendations)
```

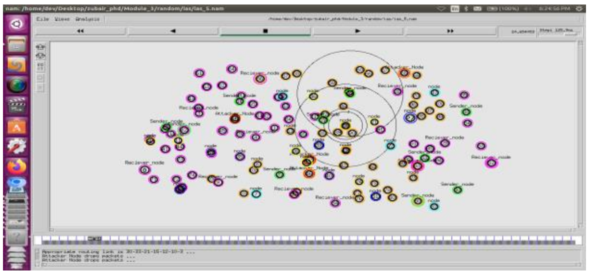
```
        Go to Step 3
    else:
        Trust_Score = 1
        Go to Step 3
3.  Digital Signing with Hash:
    if message is not None:
        Hash_Digest = hash_function(message)
        Digital_Signature = encrypt(Hash_Digest, Private_Key)
        Go to Step 4a
    else:
        Stop
4a. Sender Side:
    if Digital_Signature is None:
        Error: Cannot send secure message
    else:
        Send(message, Digital_Signature)
    Go to Step 4b
4b. Receiver Side:
    if sender_public_key is None:
        Error: Cannot verify sender's identity
    else:
        Decrypted_Hash = decrypt(Digital_Signature, sender_public_key)
        Received_Hash = hash_function(message)
        Go to Step 5
5.  Signature Verification:
    if Decrypted_Hash == Received_Hash:
        Message_Authentic = True
        Go to Step 6
    else:
        Error: Message integrity compromised
6.  Lightweight Encryption:
    if message is None:
        Error: Message content cannot be accessed
    else:
        Decrypted_Data = decrypt(message, Private_Key)
        Go to Step 7
7.  Data Retrieval:
    if Decrypted_Data is None:
        Error: Message content corrupted
    else:
        Plaintext = Decrypted_Data
        Go to Neighbor Communication
8.  Neighbor Communication:
    if Trust_Score * Security_Threshold >= Secure_Communication_Threshold:
        Secure_Connection = True
        Communicate(Plaintext)
    else:
    Error: Secure connection cannot be maintained
    End
```

IV. RESULTS AND DISCUSSION

In the specific context of this research work, an Identity-based Authentication Scheme (IAS) has been developed and successfully integrated into NS 2. However, it is important to note that the process of integrating the IAS involves several intricate steps, therefore, a comprehensive overview of the process and relevant snapshots has been provided for reference. It is crucial for individuals undertaking this task to possess the necessary skills and understanding to effectively implement the proposed scheme. This includes proficiency in C++ programming, knowledge of wireless sensor networks, and a deep understanding of authentication protocols and schemes. Following table 1 shows the simulation parameters and their values in NS-2 while figure 2 and 3 shows the NAM snapshot for random and cluster zone topologies respectively.

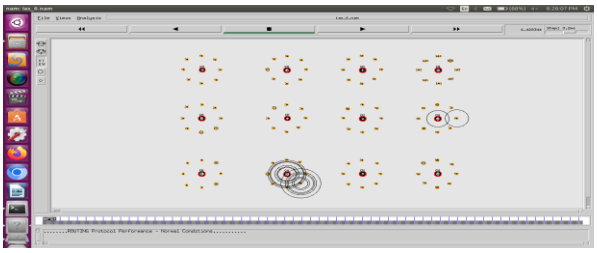
Table 1: Simulation Parameters for Module I and Module II

SN	Simulation Parameters	Values
1	No of Nodes and Topolgy	Random topology: 40 to 160 nodes Cluster Zone topology :20 to 240 nodes
2	Authentication Schemes	IDS, RSS, Digital Signature and IAS authentication scheme for Both
3	Data Payload (UDP)	512 Bytes for Both Modules
4	Transmission Range of Node	250 meters
5	Propagation Model	Two Ray Ground
6	Performance Parameters	PDR, PLR, Throughput, Delay, RO, NRL, No of retransmissions, forwa
7	Simulation time & Area	700 seconds and 1000m x 1000m



```
Appropriate routing link is 30-33-21-18-12-10-2 ...
Attacker Node drops packets ...
Attacker Node drops packets ...
```

Figure 2: NAM Snapshot for Random Topology



```
.........ROUTING Protocol Performance - Normal Conditions...........
```

Figure 3: NAM Snapshot for Cluster Zones

A. Results for Random Topology

The graph in Figure 4 (a) shows that the IAS authentication scheme has a consistently higher packet delivery ratio compared to other schemes, indicating its effectiveness in ensuring successful packet delivery in a random topology scenario. This could be due to factors such as the robustness of the authentication mechanism, efficient communication protocols, or effective handling of node movements.

In conclusion, the graph in Figure 4(b) shows that the IAS authentication scheme outperforms the other three schemes in terms of packet loss ratio (PLR). The IAS scheme consistently exhibits a significantly lower PLR value, indicating its superiority in maintaining packet integrity during transmission. This suggests that the IAS scheme is more reliable and efficient in data transmission, resulting in reduced network congestion.

The graph in Figure 4(c) demonstrates that the end-to-end delay in a random topology is not consistent and can vary due to factors such as the movement of nodes. Additionally, the IAS authentication scheme shows a notably better performance in reducing the delay compared to other schemes.

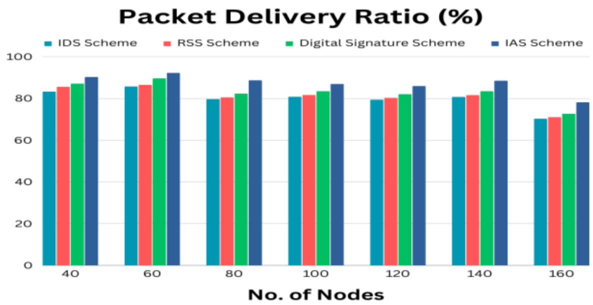
The throughput graph in Figure 4(d) demonstrates how the performance of four authentication schemes changes with an increasing number of nodes in a random topology. The graph shows that the throughput consistently increases as the number of nodes increases, indicating a more robust network. Furthermore, the IAS authentication scheme exhibits significantly higher throughput values compared to the other schemes, suggesting its efficiency in data transmission and processing. Overall, the comparison of the authentication schemes in the graph highlights the superior performance of the IAS scheme in terms of throughput.

The graph in Figure 4(e) finds that as the number of nodes in a network increases, the routing overhead also increases. The IAS authentication scheme consistently had the lowest routing overhead value, indicating its efficiency compared to the other authentication schemes.

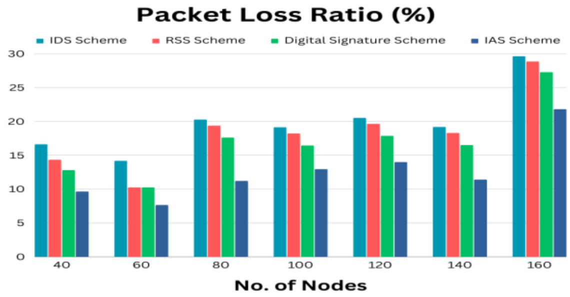
The graph in Figure 4(f) finds that the Improved Authentication Scheme (IAS) demonstrates a significant improvement in the normalized routing load (NRL) compared to the other three authentication schemes. This suggests that the IAS scheme is more efficient in terms of routing overhead, resulting in a lower NRL. This improvement can lead to advantages such as minimizing network congestion, reducing energy consumption, and improving overall network performance.

The graph in Figure 4(g) shows that as the number of nodes increases, the forwarding counts also increase, indicating a consistent upward trend. The IAS scheme stands out as the most efficient authentication scheme, consistently exhibiting superior forwarding counts compared to the other three schemes. The other three schemes show limitations or inefficiencies in forwarding data packets, especially in larger networks.

The graph in Figure 4(h) demonstrates that as the number of nodes increases, the number of retransmissions also increases for all four authentication schemes. However, the IAS scheme stands out as being more efficient in handling network complexities and minimizing the need for retransmissions compared to the other three schemes.



(a)



(b)

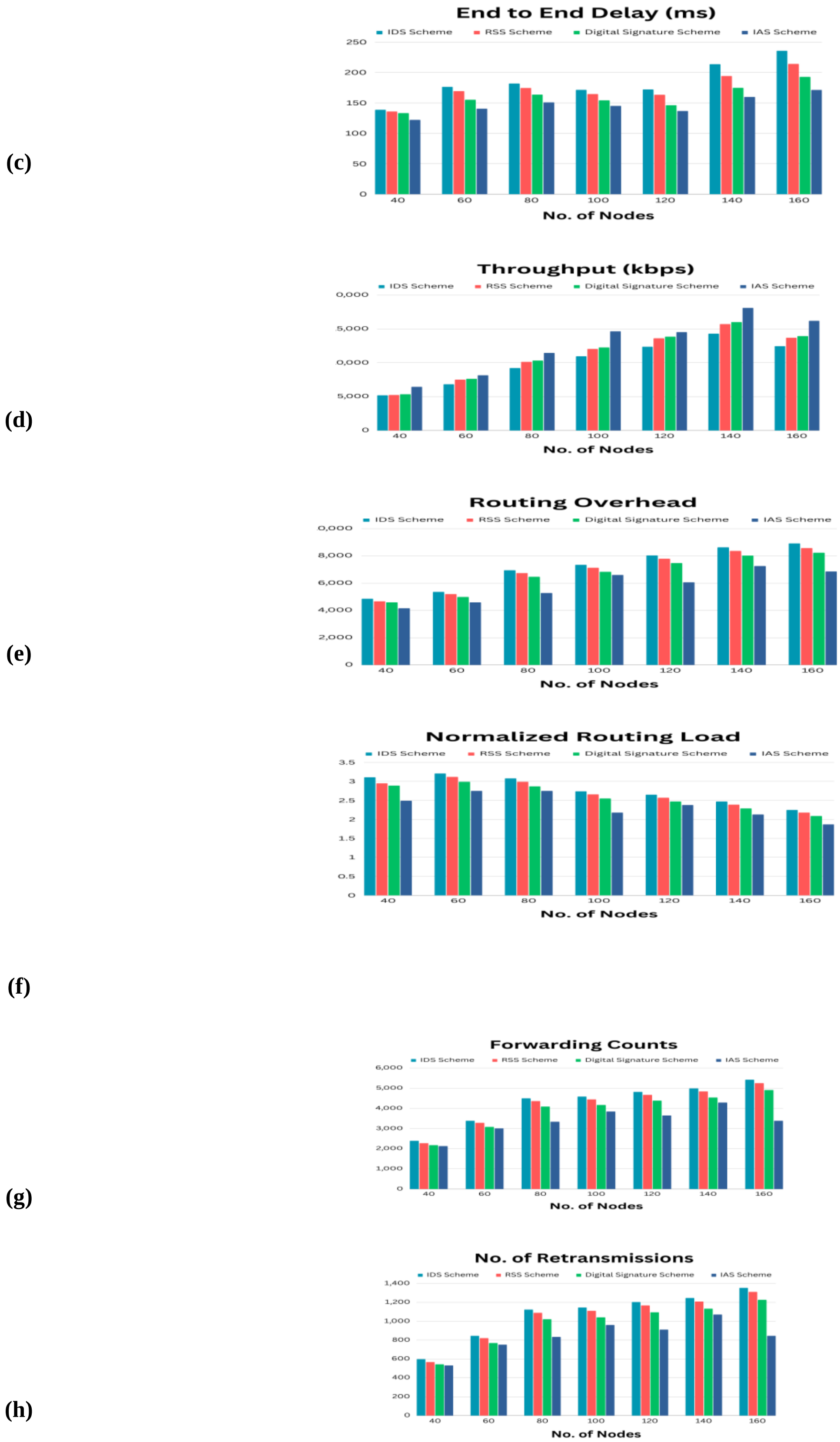


Figure 4 (a) to (h): Results of Performance Parameters - Random Topology

B. Results for Cluster Zones

The graph in Figure 5(a) shows that the packet delivery ratio remains consistent across all scenarios for the four authentication schemes due to the uniform arrangement and static nature of nodes within clusters. Furthermore, the graph highlights that the proposed IAS scheme outperforms the other three schemes in terms of packet delivery ratio, achieving a higher rate of successful packet delivery. Overall, the graph provides valuable insights into the performance of different authentication schemes in terms of packet delivery ratio.

The graph in Figure 5(b) demonstrates that as the number of cluster zones and nodes increase, the packet loss ratio (PLR) becomes more inconsistent across all four authentication schemes. However, the proposed IAS scheme consistently exhibits a lower plr compared to the other schemes, indicating its superior efficiency and robustness in handling scenarios with higher complexity.

The graph in Figure 5(c) shows that the end-to-end delay is affected by the number of cluster zones in different authentication schemes. For scenarios with low node numbers and uniform distribution, the end-to-end delay remains consistent across all schemes. However, as the number of clusters and nodes increase, the performance of the schemes varies. The proposed IAS scheme demonstrates better efficiency in handling increased complexity and larger numbers of nodes and clusters, maintaining a lower end-to-end delay and making it a promising choice for authentication in such scenarios.

The graph in Figure 5(d) shows that the proposed Intelligent Authentication Scheme (IAS) has better throughput compared to three other authentication schemes when the number of nodes and clusters increases, indicating that the IAS scheme is more efficient in handling network complexity and allowing for higher throughput.

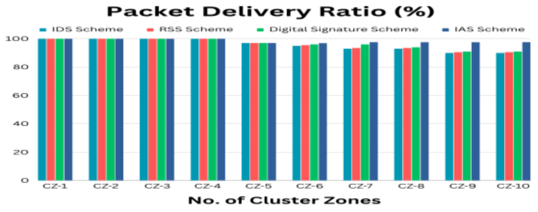
The graph in Figure 5(e) that the routing overhead is not significantly affected by the number of cluster zones in scenarios with a low number of nodes. However, as the number of clusters and nodes increase, the routing overhead also increases for all authentication schemes, indicating a challenge in scalability. Additionally, the proposed IAS scheme demonstrates better routing overhead compared to the other three schemes, suggesting its efficiency in minimizing routing overhead in scenarios with a larger number of cluster zones and nodes.

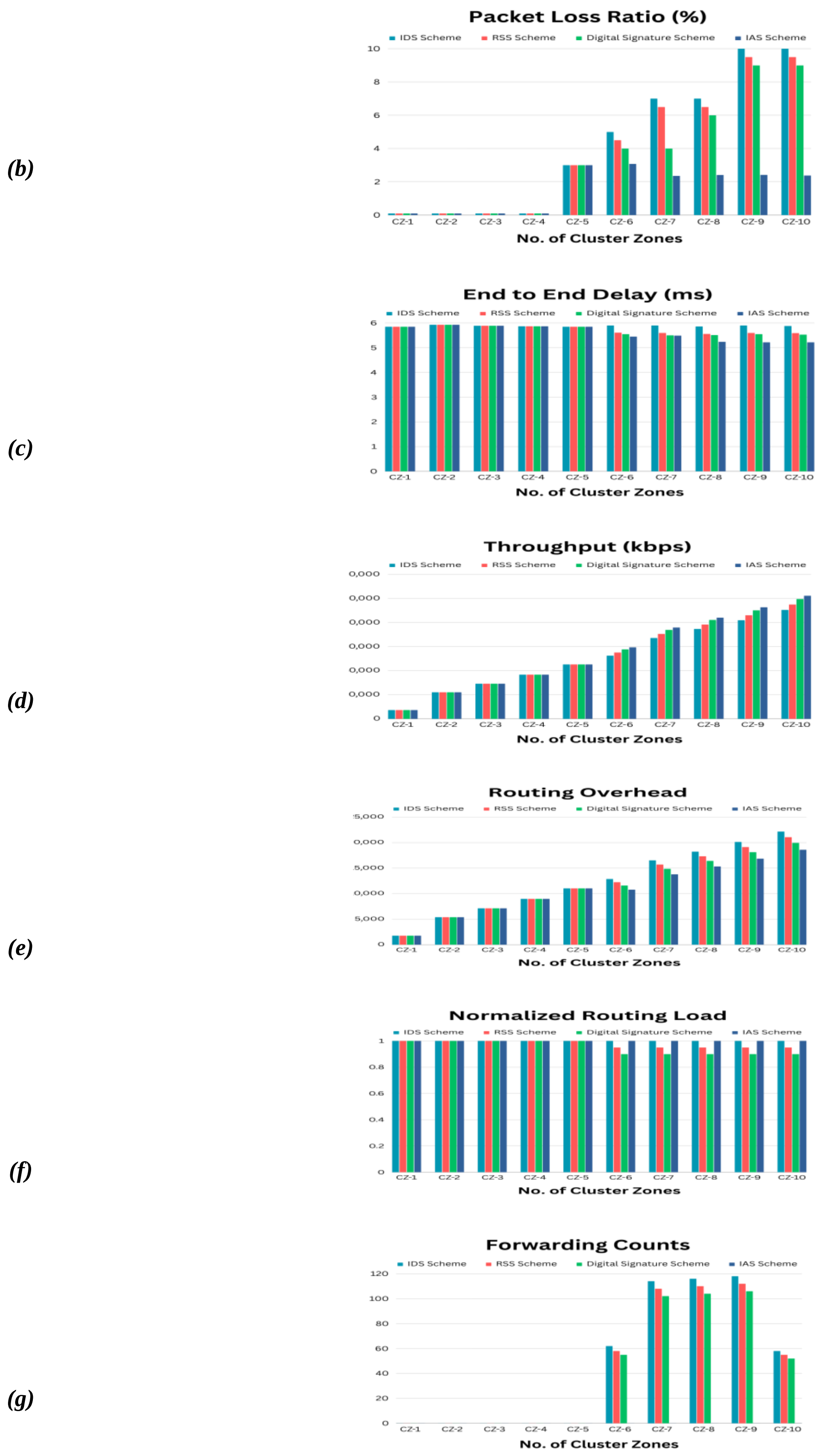
The graph in Figure 5(f) demonstrates that the performance of authentication schemes in a wireless sensor network is influenced by the complexity of the network, with the routing load varying differently for different schemes as the number of clusters and nodes increase. Additionally, the proposed Improved Authentication Scheme (IAS) proves to be more efficient in terms of the amount of routing load it imposes on the network compared to the other schemes.

The graph in Figure 5(g) demonstrates that the performance of authentication schemes is not greatly affected by the number of nodes or clusters in scenarios with a lower number of nodes and evenly distributed clusters. However, as the number of nodes and clusters increase, the forwarding counts vary significantly, indicating that scalability becomes a crucial factor. Additionally, the proposed IAS scheme outperforms the other authentication schemes in terms of forwarding counts, suggesting that its intelligent algorithms and techniques optimize the authentication process and reduce overall message forwarding.

The graph in Figure 5(h) shows that the number of retransmissions is affected by the number of cluster zones in different authentication schemes. For scenarios with fewer nodes and a static cluster formation, the number of retransmissions remains consistent across all schemes. However, as the complexity increases with more clusters and nodes, the number of retransmissions varies significantly among the schemes. The graph also demonstrates that the proposed IAS scheme performs better than the other three schemes in terms of retransmissions, indicating its efficiency and reliability in handling increased complexity.

(a)




(b)
Packet Loss Ratio (%)
IDS Scheme
RSS Scheme
Digital Signature Scheme
IAS Scheme
10
8
6
4
2
0
CZ-1
CZ-2
CZ-3
CZ-4
CZ-5
CZ-6
CZ-7
CZ-8
CZ-9
CZ-10
No. of Cluster Zones
(c)
End to End Delay (ms)
IDS Scheme
RSS Scheme
Digital Signature Scheme
IAS Scheme
6
5
4
3
2
1
0
CZ-1
CZ-2
CZ-3
CZ-4
CZ-5
CZ-6
CZ-7
CZ-8
CZ-9
CZ-10
No. of Cluster Zones
(d)
Throughput (kbps)
IDS Scheme
RSS Scheme
Digital Signature Scheme
IAS Scheme
0,000
0,000
0,000
0,000
0,000
0,000
0
CZ-1
CZ-2
CZ-3
CZ-4
CZ-5
CZ-6
CZ-7
CZ-8
CZ-9
CZ-10
No. of Cluster Zones
(e)
Routing Overhead
IDS Scheme
RSS Scheme
Digital Signature Scheme
IAS Scheme
:5,000
0,000
5,000
0,000
5,000
0
CZ-1
CZ-2
CZ-3
CZ-4
CZ-5
CZ-6
CZ-7
CZ-8
CZ-9
CZ-10
No. of Cluster Zones
(f)
Normalized Routing Load
IDS Scheme
RSS Scheme
Digital Signature Scheme
IAS Scheme
1
0.8
0.6
0.4
0.2
0
CZ-1
CZ-2
CZ-3
CZ-4
CZ-5
CZ-6
CZ-7
CZ-8
CZ-9
CZ-10
No. of Cluster Zones
(g)
Forwarding Counts
IDS Scheme
RSS Scheme
Digital Signature Scheme
IAS Scheme
120
100
80
60
40
20
0
CZ-1
CZ-2
CZ-3
CZ-4
CZ-5
CZ-6
CZ-7
CZ-8
CZ-9
CZ-10
No. of Cluster Zones

(h)

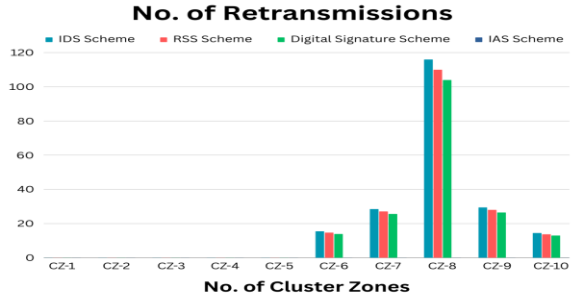


Figure 5 (a) to (h): Results of Performance Parameters- Cluster Zones

V. CONCLUSION

In this research study, the focus is on examining and comparing four different authentication schemes: the IAS scheme, RSS scheme, Digital signature authentication scheme, and the proposed IAS scheme. These authentication schemes are evaluated and compared based on their performance in two different network topologies. The first network topology chosen for analysis is a random topology. In this topology, the number of nodes gradually increases up to 160, and the nodes have the freedom to move in any direction without any restrictions. This topology represents a dynamic and unpredictable network environment. The second network topology is a cluster topology. In this topology, both the number of nodes and the number of clusters increase, but the nodes remain static and are arranged uniformly. This topology represents a more structured and organized network environment.

After conducting the analysis and evaluating the results for both network topologies, it is concluded that the proposed IAS authentication scheme outperforms the other three authentication schemes. The IAS scheme demonstrates superior performance in terms of efficiency, security, and reliability compared to the RSS scheme, Digital signature authentication scheme, and the proposed IAS scheme.The research study provides valuable insights into the effectiveness and suitability of different authentication schemes in different network topologies. The findings highlight the importance of selecting the appropriate authentication scheme based on the specific network environment and requirements. The superiority of the IAS authentication scheme suggests its potential for widespread adoption and implementation in various network scenarios.

REFERENCES

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. Computer Networks, 38(4), 393-422.

[2] Estrin, D., Römer, K., Balakrishnan, M., & Culler, D. (2004). Motes: An infrastructure for wireless sensor networks. IEEE Communications Magazine, 43(5), 36-42.

[3] Weiser, M. (1991). The computer for the 21st century. Scientific American, 265(3), 99-108.

[4] Ashton, K. (2009). That 'internet of things' thing. RFID Journal, 11(7), 22-23.

[5] Akyildiz, I. F., & Malekian, M. (2011). Wireless sensor networks: A survey. Computer Networks, 55(15), 2788-3004.

[6] Gubbi, J., Buyya, R., Marri, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements and future directions. Future Generation Computer Systems, 29(7), 1645-1666.

[7] Pahlavan, K., Krishnamurthy, P., & Cho, J. H. (2014). Networking for the Internet of Things: Challenges and opportunities. IEEE Communications Magazine, 52(4), 96-104.

[8] Tan, L., & Wang, N. (2020). Future of edge computing and cloud computing: A survey. Future Generation Computer Systems, 107, 846-858.

[9] Dogarapu, R., & Mathur, S. (2013). Security vulnerabilities of wireless sensor networks and its possible solutions. International Journal of Computer Applications, 69(5), 37-42.

[10] Khan, M. A., & Salahuddin, S. (2015). Security issues in wireless sensor networks (WSNs): A survey. Sensors, 15(7), 17167-17210.

[11] Sureshkumar, R., & Saraswathi, T. (2017). Security challenges in Internet of Things (IoT) and blockchain technology as a promising solution. In Proceedings of the 2nd International Conference on Inventive Technologies and Applications (ICITA) (pp. 364-369). IEEE.

[12] Lu, R., & Lin, X. (2012). Survey of wireless sensor network security encapsulation. International Journal of Distributed Sensor Networks, 8(7), 934-943.

[13] Kim, H. C., Park, S. H., & Lee, I. (2017). Security architecture for denial-of-service attacks in wireless sensor networks. Sensors, 17(8), 1939.

[14] Zhang, Y., Li, J., & Lin, C. (2015). Security enhancement for wireless sensor networks based on tamper detection mechanisms. Security and Communication Networks, 8(1), 145-153.

[15] Mavroudis, I., & Leligoudis, G. (2011). Lightweight data encryption for WSNs: A survey. In Proceedings of the 2011 IEEE International Conference on Communications (ICC) (pp. 1-5). IEEE.

[16] Park, J. H., & Kang, H. (2016). An efficient and secure authentication scheme for wireless sensor networks based on lightweight hash function. Sensors, 16(10), 1653.

[17] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279.

[18] Premkumar Chithaluru, Aman Singh, Jagjit Singh Dhatterwal, Ali Hassan Sodhro, Marwan Ali Albahar, Anca Jurcut, Ahmed Alkhayyat, An Optimized Privacy Information Exchange Schema for Explainable AI Empowered WiMAX-based IoT networks, Future Generation Computer Systems, Volume 148, 2023, Pages 225-239, ISSN 0167-739X, https://doi.org/10.1016/j.future.2023.06.003. (https://www.sciencedirect.com/science/article/pii/S0167739X23002170)

[19] A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane and I. B. Dhaou, "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model," in IEEE Access, vol. 11, pp. 119862-119875, 2023, doi: 10.1109/ACCESS.2023.3327620.

[20] Girish Sharma, Jyoti Grover, Abhishek Verma, Performance evaluation of mobile RPL-based IoT networks under version number attack, Computer Communications, Volume 197, 2023, Pages 12-22, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2022.10.014. (https://www.sciencedirect.com/science/article/pii/S0140366422004029)

[21] Shefali Goel, Abhishek Verma, Vinod Kumar Jain, CRA-RPL: A Novel Lightweight challenge-Response authentication-based technique for securing RPL against dropped DAO attacks, Computers & Security, Volume 132, 2023,103346,ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103346. (https://www.sciencedirect.com/science/article/pii/S0167404823002560)t

[22] M. Dener, C. Okur, S. Al and A. Orman, "WSN-BFSF: A New Dataset for Attacks Detection in Wireless Sensor Networks," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2023.3292209.

[23] Shu-Yu Kuo, Fan-Hsun Tseng, Yao-Hsin Chou, Metaverse intrusion detection of wormhole attacks based on a novel statistical mechanism, Future Generation Computer Systems, Volume 143, 2023, Pages 179-190, ISSN 0167-739X, https://doi.org/10.1016/j.future.2023.01.017.

(https://www.sciencedirect.com/science/article/pii/S0167739X23000249)

[24] Samira Tahajomi Banafshehvaragh, Amir Masoud Rahmani, Intrusion, anomaly, and attack detection in smart vehicles, Microprocessors and Microsystems, Volume 96, 2023, 104726, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2022.104726. (https://www.sciencedirect.com/science/article/pii/S0141933122002563)

[25] Nazli Tekin, Abbas Acar, Ahmet Aris, A. Selcuk Uluagac, Vehbi Cagri Gungor, Energy consumption of on-device machine learning models for IoT intrusion detection, Internet of Things, Volume 21, 2023, 100670, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2022.100670. (https://www.sciencedirect.com/science/article/pii/S2542660522001512