

Comprehensive performance and security evaluation of a group ring based authentication protocol for mobile agent systems

Mohammad Asim *

Anil Kumar Sagar †

Department of Computer Science & Engineering

Sharda University

Greater Noida 201310

Uttar Pradesh

India

Abstract

Mobile agent is a small program that can be moved from one platform to another and run a given task. In distributed computing environment the demand of mobile agents is exponentially increasing due to automaticity. But security of mobile agents is remains a critical challenge in malicious networks. In this paper proposed a Secure Key Authentication Scheme based on the discrete logarithm problem in group ring structure to enhance the authentication of mobile agents. The proposed method is based on the hardness of discrete logarithm problem and algebraic structure of group rings which provides security model against impersonation replay and man in the middle attacks. With the synchronization of efficient cryptographic operations proposed method ensures secure key generation, authentication and verification while maintaining computational feasibility. After the analysis of proposed method performance with existing similar authentication methods in terms of computational cost, security strength and communication overhead costs. Analysis of the outcomes of proposed method shows that the authentication time is less and security is more in proposed Authentication Scheme Based on discrete logarithm problem in Group Ring which makes it suitable solution in mobile agent based systems in distributed and cloud environments. A secure key validation is based on discrete logarithm problem with a group ring. In method, mobile agents can be securely authenticated by providing data of a secret without revealing it, which is appropriate for distributed and dynamic situations, such as multi agent systems.

Subject Classification: 94A60, 94A62.

Keywords: Mobile agent security, Authentication, Group rings, Discrete logarithm problem, Data integrity, Mobile agents, Distributed environment.

* E-mail: er.mohdasim@gmail.com (Corresponding Author)

† E-mail: aksagar22@gmail.com

1. Introduction

A mobile agent is an autonomous software entity that can roam different forms of malicious networks and perform specific actions on the host computer system. In contrast to the mobile agents of Conventional client-server models which carry their code along with their execution state, they are able to work asynchronously and more efficiently in the distributed environment. Mobile agents are popular in many applications including network management, ecommerce and distributed computing, because they can reduce bandwidth, they can be more scalable and they can be able to perform things dynamically. But security of mobile agents like unauthorized access, malicious hosts and data integrity threats are still important problems and it is required to have robust security mechanisms to protect mobile agents in malicious environments. The working of mobile agents to execute the assigned task is shown in Figure 1.

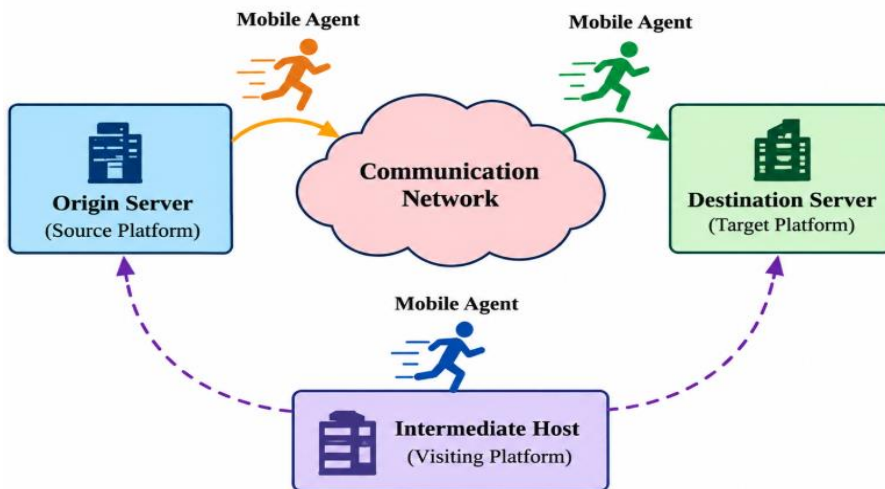


Figure 1
Mobile Agent Architecture

1.1 Mobile Agent Lifecycle and Mobility Operations

The Figure 2 depicts a mobile agent's lifecycle and mobility operations in a distributed computing system. The mobile agent A1 is first created in the Source Node (Agent Server) with the necessary code and data and with the desired execution state. The agent then moves to the Destination Node (Agent Host) to execute the tasks it was assigned to and can then come back to the source node with returned results. This also means that important lifecycle operations such as suspension, resumption, self-copying, and replication are also included in the figure. The operations show the capability of mobile agents and underlines the importance of securing the movement and execution of agents by using authentication, data integrity, and secure communication [1].

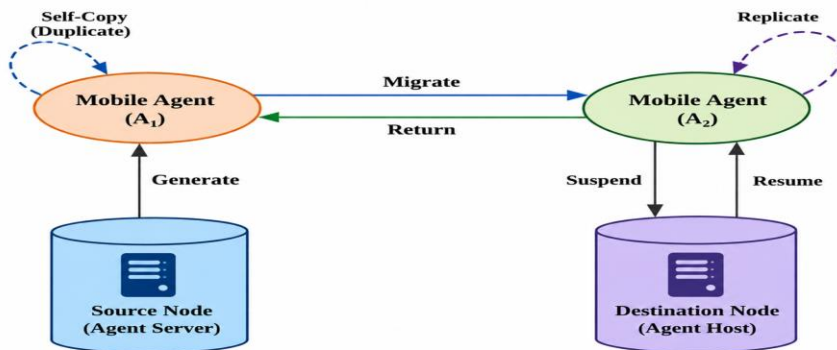


Figure 2
Mobile Agent Lifecycle Workflow

1.2 Applications of Mobile Agents

Mobile agents are autonomous programs that can be transferred from distributed computing platforms, process data and perform tasks without the need for constant human interaction. Mobile agents have been used in various applications because of their mobility, flexibility and autonomous decision making. They can be used in network management to monitor network traffic, identify anomalies, and optimize resource allocation by dynamically migrating between network nodes. In e-commerce, the autonomous behaviour of mobile agents can be used to carry out secure online transactions, conduct price comparisons, and offer personalized recommendations by interacting with various e-commerce platforms. In distributed information retrieval, they can search and retrieve relevant information from multiple sources to lower network bandwidth usage, and enhance the efficiency of searching relevant information. Mobile agents can also perform tasks in mobile cloud computing, such as resource management, security monitoring, and ensuring task reliability. They enable IoT devices to communicate with each other, to gather data, and to make decisions independently. Mobile agents also play a role in cyber security in intrusion detection and identification of attacks and protecting critical infrastructure. Moreover, in e-governance, mobile agents can facilitate effective and secure government services, such as tax filing, document verification, and digital identity management.

1.3 Mobile Agent Security Issue

Mobile agents can be the target of many security concerns, such as threats to their confidentiality, integrity, availability, and authenticity, in a distributed and potentially hostile environment. The integrity and confidentiality of data can be compromised by malicious hosts by changing the code of mobile agents or by interfering with the execution of them [2]. A rogue mobile agent can take advantage of the vulnerabilities in the host system to steal sensitive information, propagate malware, or cause host system functionality to be disrupted by a

propagate malware, or cause host system functionality to be disrupted by a denial-of-service (DoS) attack. Sensitive data passed in an agent migration could be vulnerable to eavesdropping and data theft by unauthorized parties. Violations of integrity and code modification are changes that are made to an agent's code and/or execution state without permission that could lead to undesirable or damaging behavior. DoS attacks can consume computational, memory or network resources of host systems, causing their services to be disrupted [3]. Weak authentication mechanisms that enable a malicious entity to impersonate or hijack a legitimate mobile agent and have access to certain resources is also a problem. Replay attacks are reruns of previously captured legitimate messages in order to gain unauthorized access or disrupt valid transactions [4]. Lastly, repudiation attacks arise when a malicious agent or host asserts that it did not carry out a specific action, making accountability, trust, and non-repudiation difficult in mobile-agent operations [5].

1.4 Mitigation Strategies

To strengthen mobile agent security [6], the following countermeasures come into play:

Encryption and Secure Communication—Ensuring data confidentiality with cryptographic schemes such as AES, RSA, and Homomorphic Encryption [7].

Authentication and Authorization—Employing means of authentication via digital signatures, biometrics, or role-based access control to thwart unauthorized access.

Code Integrity Verification—Confirming non-tampering with the agent's code by using hash functions and digital certificates.

Trust-Based Mechanisms—Instituting reputational and trust scoring systems to identify malicious hosts and agents, hence curbing their operations [8].

Sandboxing and Execution Control—Allowing mobile agents to operate within isolated confines, thereby barring the agents from causing any damage to the host system [9].

1.5. Discrete Logarithm Problem in Group Rings

The use of Discrete Logarithm Problem (DLP) in group rings offers a promising cryptographic basis for the improvement of security in a mobile-agent system in a distributed and potentially hostile environment. Mobile agents are autonomous programs which move from one platform to another in the network to carry out a specific task in platforms like e-commerce, healthcare, cloud computing, and Internet of Things (IoT). Their capabilities and performance on the potentially untrusted hosts, however, are vulnerable to security issues such as agent impersonation, agent duplication, replay attack, and man-in-the-middle attack. The proposed approach is based on the difficulty of computing the discrete logarithm in a group-ring structure and used to enhance authentication and integrity of the communication between mobile agents. The main goal for designing the scheme is to provide a good trade-off between security and

computational efficiency to be used in real time mobile-agent applications in distributed/Cloud computing architecture.

2. Related Works

Security has been an emerging research field for the security of mobile agents, because of the widespread use of distributed and heterogeneous computing environments. Mobile agents are autonomous entities that move and perform operations on possibly untrusted platforms, making them susceptible to numerous attacks, including impersonation, unauthorized access, modification of the code, attack of replaying messages, and leaking data. Accordingly, several protocols and security mechanisms have been suggested for the secure authentication, key management, data integrity and security, and maliciously entities protection. In order to solve the security issues in the distributed, cloud and IoT environments, several existing studies have studied different techniques such as polynomial interpolation, secret sharing, key exchange, public-key cryptography, artificial intelligence and hybrid combinatorial designs. Kumar et al. [10] presented a secure mobile-agent migration mechanism using Lagrange interpolation and Fast Fourier Transformation (FFT). They use a double polynomial based authentication mechanism to enhance the security of mobile-agent migration. The study also uses the Blowfish symmetric encryption algorithm to protect sensitive patient information. A secret key is generated and verified by polynomial techniques and data is encrypted by the mechanism providing confidentiality during its transmission. The authors claimed the improved performance in key generation and reconstruction compared to the conventional CRT-based approach and Euler-based approach. This paper shows the need to use efficient cryptographic operations, along with authentication mechanisms, for securing mobile agents during migration.

Xu et al. [11] proposed an efficient secret sharing scheme based on Linear Homogeneous Recurrence (LHR) relations. The scheme proposed distributes multiple secrets into selected terms in an LHR sequence, and then recovers the secrets in recovery phase. Using a global threshold is more efficient in computation and less complex than using the traditional compartmented secret sharing methods. The scheme is based on Shamir's threshold secret-sharing principle to ensure security, and offers multiple secret-sharing and updating mechanisms. While the emphasis is on secret sharing and not on mobile-agent authentication, the distribution of multiple secrets is an important concern of secure distributed systems.

Wang and Wu [12] worked on how to get a consistent and high rendering performance of Java AWT/Swing applets on different platforms. Their work focuses on performance consistency on heterogeneous platforms and emphasizes platform independence when running programs. While this study does not explicitly address the security for the mobile agent, the aspect of having to execute the agent in a consistent manner across multiple platforms is pertinent to mobile-agent systems, where agents can run on a variety of different platforms and need to be executed in a consistent way.

For cloud-based intelligent machine-learning applications, especially in health-monitoring systems, Almuzaini et al. [13] introduced a key aggregation cryptosystem and double encryption mechanism. They take a data security approach using cryptographic key management and multi-layered encryption. CloudSim was used to evaluate the experimental results, which showed better performance than traditional methods. The study focuses on efficient key-management and encryption mechanisms in the cloud environment and highlights their significance for the protection of mobile agents and their sensitive information when executed in a distributed environment.

Verma, Jain, and Pal [14] suggested a Chinese Remainder Theorem (CRT) based hybrid verifiable secret sharing scheme. They provide a way to distribute several secrets among shareholders that are set in different hierarchical levels. Secret reconstruction may be done at the same level or at different levels; with higher level participants helping lower level participants as needed. The proposed method is based on a one-way hash function to reduce the computational complexity and gives protection against dishonest dealers and malicious shareholders. In addition, a dealer-leakage-resilience mechanism is added to make sure that valid shares do not disclose secret information. It was implemented with cryptographic libraries and its security analysis showed its suitability for verifiable secret sharing. These mechanisms can be of interest for distributed authentication systems where secure secret distribution and verification is critical.

Kuang et al. [15] presented a Homomorphic Polynomial Public Key Cryptography system for quantum secure digital signature. They are designed using the concepts of modular arithmetic and multivariate polynomial structures and are designed to resist known-message, chosen-message, and key-only attacks. The idea of the scheme is to hide the generator element, while its goal is to increase resistance to attacks involving solutions to discrete logarithm problems using quantum computing. The relevance of this work to the current research is evident in the fact that it shows the potential of applying polynomial and number-theoretic structures in the design of cryptographic mechanisms that offer increased security from the new computational attacks.

Alluhaybi et al. [16] have given a thorough survey of the agent-based software technology in the field of cybersecurity. They studied the security threats, security controls, attacks and challenges to agent based systems. Specific attention was paid to agent code and data protection, agent state and itinerary protection and mutual protection of mobile agents and host-platforms. The research revealed several issues such as resistance to complex attacks, security testing, security compliance to cybersecurity, and creation of self-protective, self-communicating agents. The results highlight the importance of strong authentication and integrity schemes that can secure mobile agents in an environment where they may be subject to an intruder.

Jagannathan and Parvees [17] proposed a study on security-break prediction with Artificial Neural Networks (ANNs). Their approach uses machine-learning techniques and security-related parameters to improve the

identification and prediction of potential security breaches. If suspicious activity is detected, the system can start taking appropriate security measures and prevent any further unauthorised access to the network. The study is not about mobile-agent authentication, but rather on predicting security breaches; it shows how intelligent techniques are important and are being used to identify and mitigate cybersecurity threats. These methods can be used together with cryptographic methods in distributed systems to offer extra threat detection.

Hindumathi and Bhaskari [18] have proposed hybrid combinatorial design based session-key distribution in IoT network. They are based on lightweight cryptographic methods coupled with combinatorial structures to enhance the distribution of session keys, connectivity, scalability and attack resistance. The proposed method proved to be more beneficial as compared to the existing hybrid combinatorial methods. The study is applicable to the mobile-agent environment as both the IoT and mobile-agent environment has distributed nodes, dynamic communication and requires efficient key-management mechanism. The focus on scalability and lightweight security mechanisms is particularly beneficial in distributed environments with limited resources.

Gowda et al. [19] studied secure networked image transmission with the help of public-key cryptography and identity authentication. Their work focuses on cryptographic authentication for ensuring the security of information sent in networked environments, and how using public key methods along with identity verification can enhance the security of the information sent. This is applicable to the mobile-agent environment, where it is crucial to ensure the integrity of information while migrating agents and data to and from one machine to another, and to verify that they are legitimate.

Mandal et al. [20] suggested an evolutionary multi-authentication cryptographic-key framework for secure data access control. The research is geared towards enhancing authentication and cryptographic key management to ensure that only authorized users can access the protected resources. Multi-layered authentication and key management are related to the needs for security in mobile-agent systems, especially in distributed systems where agents communicate with multiple possibly untrusted hosts.

Asim and Sagar [21] proposed an approach for securing mobile-agent environments from a cyber security point of view, which centered around the classification of malicious agents. They investigate the problems created by potentially dangerous agents in distributed environments, and focus on detecting malicious activity. The proposed approach helps enhance the security and reliability of mobile-agent systems by guaranteeing the effective detection and classification of threats.

For improving the security of a mobile-agent, Asim and Sagar [22] suggested a multilevel secret-sharing mechanism that uses a threshold with a variable value, called the Chinese Remainder Theorem (CRT). The scheme offers flexible secret distribution and reconstruction and provides flexibility to adjust the threshold as per security needs. Their work shows how the secret

sharing schemes based on CRTs could be applied to enhance the authentication and mobile agent protection in distributed systems.

In Asim and Sagar [23], gave an in-depth study of the various key technologies which can be used to enhance security in a mobile-agent system and compared the various approaches using several performance parameters. Their research points out the necessity to consider security, computational efficiency, communication overhead, and scalability features when designing mobile-agent security mechanisms. A comparative study serves as a basis for creating effective authentication methods, which are appropriate for distributed and resource-limited environments.

3. A Group Ring Based Authentication Scheme for Mobile Agents Using the Discrete Logarithm Problem

To maintain the integrity and confidentiality of a distributed system, secure authentication of mobile agents is a fundamental requirement. Classic authentication schemes are generally based on centralized authorities involving either symmetric or asymmetric cryptography, thereby posing certain scalability problems as well as computational inefficiencies. To actualize a focus over these issues, Figure 3 shows a Secure Key Authentication method based on the Discrete Logarithm Problem on the Group Ring has been proposed as Authentication Framework, Efficient Key Authentication and Security Analysis and Performance Evaluation.

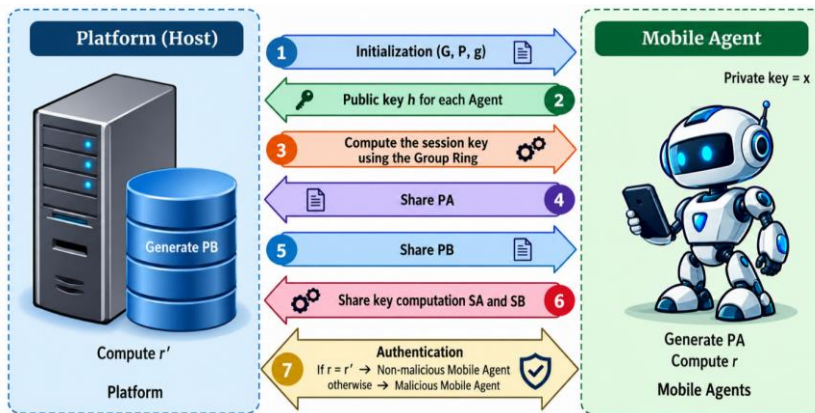


Figure 3
Secure Mobile Agent Authentication Flow

Group Ring Structure

The group ring is an algebraic structure to combine both group and ring which is useful in information security models. Such as a ring structure is denoted by $R[G]$, where G is a group

Operations in Group Rings as Addition and Multiplication: The ring coefficients multiply according to ring properties.

Discrete Logarithm Problem (DLP) in Group Rings

Given a base g , an element h , and a prime p , the problem is to find x in

$$H = g^x \pmod{p}$$

Finding x is computationally difficult, ensuring secure cryptographic systems.

DLP Extended to Group Rings

In group rings, the problem is posed exactly as:

$$H = g^x \text{ in } R[G]$$

Because these group ring structures may be non-commutative, usual attacks (index calculus, for example) are not so reliable.

This makes it more secure for a cryptographic protocol to be designed on a group ring since it is very hard to solve the $g^x = h$ problem.

On the contrary, by correlating group rings with the Discrete Logarithm Problem, the security of mobile agents could have been improved to a great extent by securing authentication, encrypted communication, and resisting attacks in distributed environments.

So, proposed methods ensure secure authentication, by means of the Discrete Logarithm Problem in Mobile Agent security. Table 1 presents the system model and mathematical notations that are used in the rest of the proposed authentication scheme: the underlying cyclic group, the group ring, cryptographic keys, the hash function, the authentication signature and the message.

Table 1
System Model and Notations

G	A cyclic group of prime order p .
Z_p	A finite field of integers modulo p .
$R[G]$	A Group Ring constructed over G with coefficients in Z_p
g	A generator of G
x	Private key of the user (randomly chosen from Z_p)
h	Public key associated with x
$H(\cdot)$	A secure cryptographic hash function.
σ	Authentication signature.
M	Message.

Algorithm 1: System Initialization

Choose a cyclic group G and of prime number p .

Select a generator $g \in G$

Construct the **Group Ring** $R[G]$ over G with coefficients in Z_p .

Define a cryptographic hash function $H: \{0,1\}^* \rightarrow Z_p$.

Generate a **private key** $x \in Z_p^*$

Compute the **public key**: $h = g^x \in G$

Publish (G, g, h, p, H) while keeping x secret.

Algorithm 2: Secret Key Creation in Group Ring

Choose a random ephemeral secret $r \in Z_p$.

Compute the ephemeral public key: $R = g^r$

Compute the session key using the Group Ring: $K = (R \cdot h)^r \bmod p$

Algorithm 3: Authentication Protocol**Step 1: Key Exchange**

User A selects a random ephemeral key $K_A \in Z_p^*$

$$P_A = g^{K_A} \bmod p$$

User B selects a random ephemeral key $K_B \in Z_p^*$

$$P_B = g^{K_B} \bmod p$$

Exchange P_A and P_B

Step 2: Shared Key Computation

User A computes: $S_A = (P_B)^x \bmod p$

User B computes: $S_B = (P_A)^x \bmod p$

Since both computations are equal: $S_A = S_B = g^{K_A K_B} \bmod p$ This shared key is used for authentication.

Algorithm 4: Signature Generation

Compute: $c' = H(M || r)$

Compute: $r' = g \sigma \cdot h c' \bmod p$

Verify if: $r' = r$

If the equation holds, the signature is valid, else reject.

The Secure Key Authentication Scheme is proposed for countering the security issues of mobile agent authentication through the utilization of the Discrete Logarithm Problem (DLP) in Group Ring, which has the following constituents:

The proposed authentication framework is designed to enhance the security of mobile agent systems through a combination of group-ring-based cryptographic operations and the discrete logarithm problem. Each mobile agent is assigned a unique cryptographic key generated using the underlying algebraic structure, making unauthorized key recovery computationally difficult. The authentication process follows a challenge-response mechanism in which the mobile agent proves its legitimacy without revealing sensitive secret information. A secure communication channel is established between the mobile agent and the host system to protect transmitted information from eavesdropping and unauthorized modification. The proposed scheme also incorporates mechanisms to mitigate replay attacks by using fresh authentication parameters during communication. Furthermore, the algebraic properties of the group ring strengthen the scheme against impersonation and man-in-the-middle attacks. The computational hardness of the discrete logarithm problem provides an

additional layer of protection against unauthorized access and key recovery. Compared with conventional asymmetric authentication techniques, the proposed approach aims to reduce computational overhead during key generation and verification. This makes the scheme suitable for mobile agents operating in resource-constrained distributed environments. Experimental evaluation indicates that the proposed authentication mechanism provides improved security and computational performance compared with selected conventional approaches. Therefore, the framework offers a scalable and efficient solution for secure real-time communication and authentication in mobile agent environments.

4. Experimental Results and Analysis

4.1 *Experimental Results*

The proposed DLP-GA (Discrete Logarithm–Group Ring Authentication) protocol was implemented in Python to examine its authentication behavior and performance in terms of execution time, communication overhead, and scalability. For the experimental evaluation, the prime modulus was selected as $p = 3241690071$, providing a considerably larger parameter space than the previously employed value of 104729. The generator was chosen as $g = 5$. Each mobile agent was assigned a randomly generated private key x , from which its corresponding public key h was derived using the proposed group-ring-based cryptographic construction. During authentication, the server generates a fresh random challenge r , which is transmitted to the concerned mobile agent. The agent then produces a response z using its secret key and the received challenge. The server independently calculates the expected response and compares it with the received value to determine whether the requesting agent is legitimate.

4.2 *Authentication Verification*

To validate the authentication procedure, three mobile agents were tested independently. Each agent possessed a distinct private-public key pair. After receiving a randomly generated challenge from the server, the corresponding agent calculated its authentication response. The server subsequently recomputed the expected response using the registered authentication parameters. Successful authentication was established when the response generated by the agent was identical to the value obtained by the server.

For Agent 1, the server generated the challenge $r = 112233445$, and the agent generated the response $z = 287453102218$. The server obtained the same response during verification, resulting in successful authentication.

For Agent 2, a challenge of $r = 998877665$ was generated. The agent calculated $z = 15673211845$, which was subsequently matched by the server during verification. Hence, Agent 2 was successfully authenticated.

For Agent 3, the challenge value was $r = 776655443$, and the resulting response was $z = 30122678901$. The server generated an identical verification value, confirming the authenticity of Agent 3.

4.3 Analysis of Authentication Results

The experimental authentication results indicate that the proposed DLP-GA mechanism can correctly verify legitimate mobile agents without transmitting their private keys over the communication channel.

Figure 4 evaluates the variation in authentication time as the population of mobile agents increases. The proposed DLP-GA mechanism is compared with RSA-AUTH for different numbers of participating agents. The horizontal axis represents the number of mobile agents, whereas the vertical axis denotes the authentication time in seconds.

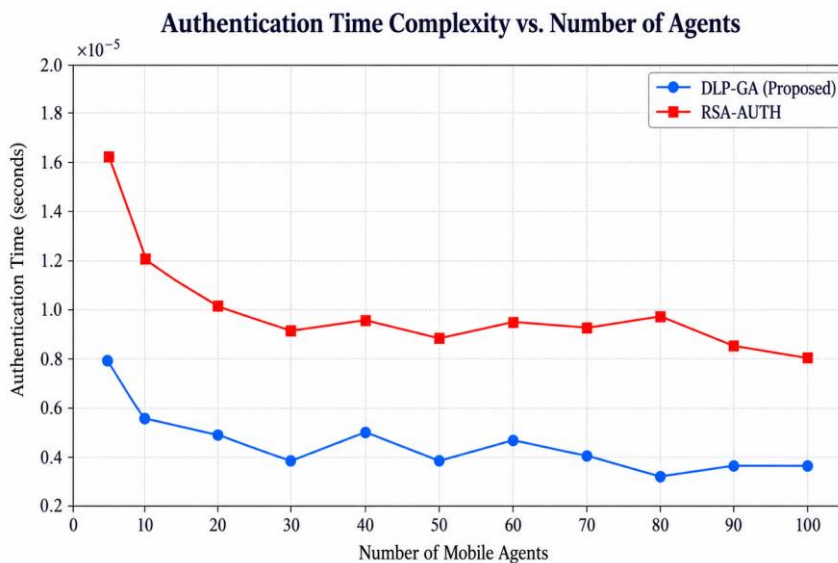


Figure 4
Time complexity vs Number of mobile agents

4.4 Authentication Schemes Comparison

Figure 5 provides a direct comparison of the authentication time of DLP-GA and RSA-AUTH for agent populations of 10, 50, 100, 250, 500, and 1000. The measured values are expressed in seconds using a 10^{-5} scale.

For 10 mobile agents, DLP-GA requires approximately 0.8×10^{-5} seconds, whereas RSA-AUTH requires approximately 2.1×10^{-5} seconds. At 50 agents, the corresponding values are approximately 0.6×10^{-5} and 1.9×10^{-5} seconds. When the population reaches 1000 agents, DLP-GA requires approximately 1.3×10^{-5} seconds, compared with approximately 5.5×10^{-5} seconds for RSA-AUTH.

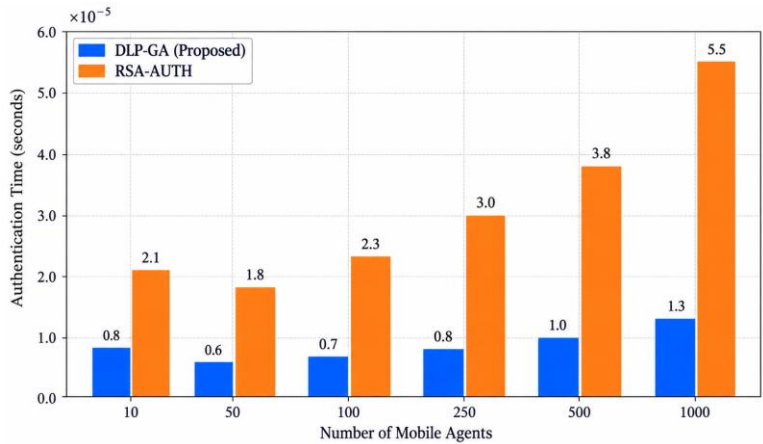


Figure 5
Time complexity vs Number of mobile agents

4.5 Communication Overhead

Figure 6 evaluates the communication requirements of four authentication approaches: DLP-GA, RSA-AUTH, ECC-AUTH, and Lattice-Based Authentication. The comparison is based on the total number of transmitted bits for an experimental population of 500 mobile agents.

The proposed DLP-GA scheme generates a total communication overhead of approximately 452,000 bits. RSA-AUTH requires approximately 2,048,000 bits, whereas ECC-AUTH requires approximately 256,000 bits. The Lattice-Based Authentication approach produces approximately 1,024,000 bits of communication overhead.

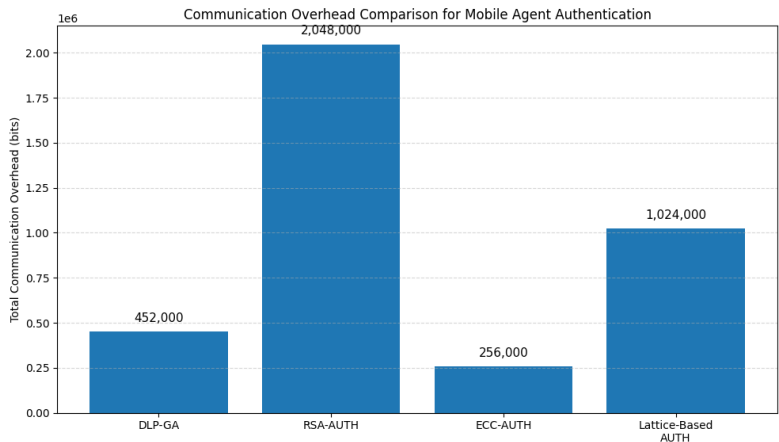


Figure 6
Communication Overhead for mobile agent authentication

4.6 Comparison with Other Authentication Schemes

Table 2
Comparison of the proposed DLP-GA scheme with existing authentication techniques

Authentication Method	Authentication Time (ms)	Overhead (bits)	Scalability
DLP-GA (Proposed)	0.9	896	High
RSA-AUTH	5.8	2048	Moderate
ECC-AUTH	0.6	256	High
Lattice-Based AUTH	7.9	4096	Low
Biometric Hashing	0.4	128	Very High

Table 2 provides an overall comparison of the proposed DLP-GA method with RSA-AUTH, ECC-AUTH, Lattice-Based Authentication, and Biometric Hashing. The proposed scheme requires 0.9 ms for authentication, which is substantially lower than RSA-AUTH (5.8 ms) and Lattice-Based Authentication (7.9 ms). Although ECC-AUTH and Biometric Hashing provide lower authentication times of 0.6 ms and 0.4 ms, respectively, DLP-GA maintains a favorable balance between authentication efficiency and communication overhead.

The communication overhead of DLP-GA is 896 bits, which is significantly lower than RSA-AUTH (2048 bits) and Lattice-Based Authentication (4096 bits). Although ECC-AUTH and Biometric Hashing require lower overhead, the proposed DLP-GA scheme provides high scalability, making it appropriate for distributed environments involving a large number of mobile agents.

5. Conclusion and Future Scope:

The proposed Discrete Logarithm Problem-Based Group Authentication (DLP-GA) scheme provides secure and efficient authentication for mobile agents in distributed environments. The experimental results demonstrate successful agent verification with comparatively low authentication time and communication overhead. The scheme also provides a suitable balance between security, computational efficiency, and scalability. Hence, DLP-GA can be considered a promising approach for protecting mobile-agent communication and data integrity.

Future Scope

Future work can focus on extending DLP-GA to large-scale and heterogeneous mobile-agent networks. The scheme can be further evaluated against advanced attacks, including adaptive impersonation, replay, and man-in-the-middle attacks. Integration with blockchain, IoT, and cloud environments can also be explored for decentralized authentication. Further optimization of group-ring operations may reduce computational and communication overhead for resource-constrained devices.

References

- [1] G. Geetha and C. Jayakumar, "Data security in free roaming mobile agents," *Commun. Comput. Inf. Sci.*, vol. 196, pp. 472–482 (2011), doi: 10.1007/978-3-642-22540-6_45.
- [2] E. Sultanik, D. Artz, G. Anderson, M. Kam, W. Regli, M. Peysakhov, J. Sevy, N. Belov, N. Morizio, and A. Mroczkowski, "Secure mobile agents on ad hoc wireless networks," in *Proc. 15th Innovative Applications of Artificial Intelligence Conf. (IAAI-03)*. Acapulco, Mexico: AAAI Press (2003), pp. 129–136.
- [3] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things (Netherlands)*, vol. 7, p. 100059 (2019), doi: 10.1016/j.iot.2019.100059.
- [4] D. Shehada, C. Y. Yeun, M. J. Zemerly, M. Al Qutayri, Y. Al Hammadi, E. Damiani, and J. Hu, "BROSMAP: A novel broadcast based secure mobile agent protocol for distributed service applications," *Secur. Commun. Netw.*, vol. 2017, pp. 13–15 (2017), doi: 10.1155/2017/3606424.
- [5] H. Lee, J. Alves-Foss, and W. S. Harrison, "The use of encrypted functions for mobile agent security," in *Proc. 37th Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)* (2004), doi: 10.1109/HICSS.2004.1265700.
- [6] P. Kumar, N. Singhal, and D. Pandey, "Euler totient function and Fermat Euler theorem based an optimized key management scheme for securing mobile agents migration," *Int. J. Inf. Technol.*, vol. 14, no. 2, pp. 657–665 (2022), doi: 10.1007/s41870-021-00838-0.
- [7] S. Vinothkumar and J. Amutharaj, "Hybrid cryptosystem based healthcare data sharing with access control policy in cloud environment," *Int. J. Inf. Technol.*, vol. 16, no. 5, pp. 3349–3357 (2024), doi: 10.1007/s41870-024-01911-0.
- [8] M. Kaur and S. Saxena, "A review of security techniques for mobile agents," in *Proc. IEEE Int. Conf. Comput. Commun. Autom. (ICCCA)*, pp. 807–812 (2017), doi: 10.1109/CCAA.2017.8229906.
- [9] P. Bagga and R. Hans, "Mobile agents system security: A systematic survey," *ACM Comput. Surv.*, vol. 50, no. 5, Art. no. 65, pp. 1–45 (2017), doi: 10.1145/3095797.
- [10] P. Kumar, N. Singhal, D. Pandey, and A. Vatsa, "Secure mobile agent migration using Lagrange interpolation and fast Fourier transform-

- tion," *Int. J. Comput. Netw. Inf. Secur.*, vol. 15, no. 4, pp. 72–83 (2023), doi: 10.5815/ijcnis.2023.04.07.
- [11] G. Xu, J. Yuan, G. Xu, and Z. Dang, "An efficient compartmented secret sharing scheme based on linear homogeneous recurrence relations," *Secur. Commun. Netw.*, vol. 2021, Art. no. 5566179 (2021), doi: 10.1155/2021/5566179.
 - [12] Y.-H. Wang and I.-C. Wu, "Achieving high and consistent rendering performance of Java AWT/Swing on multiple platforms," *Softw. Pract. Exp.*, vol. 39, no. 7, pp. 701–736 (2009), doi: 10.1002/spe.920.
 - [13] K. K. Almuzaini, A. K. Sinhal, R. Ranjan, V. Goel, R. Shrivastava, and A. Halifa, "Key aggregation cryptosystem and double encryption method for cloud-based intelligent machine learning techniques-based health monitoring systems," *Comput. Intell. Neurosci.*, vol. 2022, Art. no. 3767912 (2022), doi: 10.1155/2022/3767912.
 - [14] O. P. Verma, N. Jain, and S. K. Pal, "A hybrid-based verifiable secret sharing scheme using Chinese remainder theorem," *Arab. J. Sci. Eng.*, vol. 45, no. 4, pp. 2395–2406 (2020), doi: 10.1007/s13369-019-03992-7.
 - [15] R. Kuang, M. Perepechaenko, M. Sayed, and D. Lou, "Homomorphic polynomial public key cryptography for quantum-secure digital signature," arXiv:2311.08967 (2023), doi: 10.48550/arXiv.2311.08967.
 - [16] B. Alluhaybi, M. S. Alrahhhal, A. Alzhrani, and V. Thayananthan, "A survey: Agent-based software technology under the eyes of cyber security, security controls, attacks and challenges," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 8, pp. 211–230 (2019), doi: 10.14569/IJACSA.2019.0100828.
 - [17] J. Jagannathan and M. Y. Mohamed Parvees, "Security breach prediction using artificial neural networks," *Meas. Sensors*, vol. 24, Art. no. 100448 (2022), doi: 10.1016/j.measen.2022.100448.
 - [18] G. V. Hindumathi and D. L. Bhaskari, "The hybrid combinatorial design-based session key distribution method for IoT networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 8, pp. 384–393 (2022), doi: 10.14569/IJACSA.2022.0130846.
 - [19] V. Dankan Gowda, P. S. V. V. S. R. Kumar, J. Latha, C. Selvakumar, and R. Shekhar, "Securing networked image transmission using public-key cryptography and identity authentication," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 3, pp. 779–791 (2023), doi: 10.47974/JDM-SC-1754.

- [20] S. K. Mandal, R. Singh, N. Chandu, D. Mehta, S. K. Henge, D. Kothapeta, C. K. Hinge, and A. Sharma, "Evolutionary multi-authentication cryptographic key implications for secure data access control," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-B, pp. 1865–1874 (2025), doi: 10.47974/JDMSC-2363.
- [21] M. Asim and A. K. Sagar, "Secure mobile agent environments: A cybersecurity approach for malicious agent classification," *EDPACS*, pp. 1–7 (2026), doi: 10.1080/07366981.2026.2679179.
- [22] M. Asim and A. K. Sagar, "Mobile agent security using multilevel secret sharing with changeable threshold based on Chinese remainder theorem," *J. Mobile Multimedia*, vol. 21, nos. 3–4, pp. 521–534 (2025), doi: 10.13052/jmm1550-4646.213411.
- [23] M. Asim and A. K. Sagar, "Key technologies for security with different performance parameters in mobile agent system," in *Proc. 1st Int. Conf. Advanced Comput. Emerging Technol. (ACET)* (2024), doi: 10.1109/ACET61898.2024.10730506.

Received January, 2026