SECURING THE DYNAMIC PATH: EMPOWERING ON-DEMAND ROUTING WITH AN ID-BASED AGGREGATE SIGNATURE SCHEME

Daxing WANG *

Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection. A number of schemes have been proposed to protect privacy in ad hoc networks. However, adversaries can readily fabricate or alter routing messages to compromise the integrity of the routing protocol. An aggregate signature mechanism enables the compression of n individual signatures—each generated by a different signer on a distinct message—into one consolidated signature. As a result, the verification process, which would normally require checking n separate equations, is streamlined into a single operation. This property makes aggregate signatures particularly suitable for resource-constrained environments such as Mobile Ad hoc Networks (MANETs). We present a novel identity-based aggregate signature (IBAS) scheme that requires only a constant number of pairing operations, independent of the number of signatures aggregated. In contrast to existing IBAS constructions, our approach significantly enhances both communication efficiency and verification speed. Furthermore, we demonstrate the practical applicability of our scheme by integrating it into an authenticated routing protocol, through which we simulate a secure and efficient routing mechanism for ad-hoc networks.

Keywords: Identity-based cryptography; Aggregate signature; Bilinear pairings; on-demand routing protocol

1. Introduction

Over the last twenty years, the field of mobile communications has undergone rapid and widespread development. Within this domain, Mobile Ad hoc Networks (MANETs) have drawn considerable interest from researchers and practitioners alike, largely because of their diverse range of applications [1]. A MANET is composed of mobile devices that interact wirelessly, operating without reliance on any pre-established infrastructure—such as access points or centralized base stations. In such networks, every participating device is responsible for executing core networking operations, including packet forwarding, routing, and overall network management. This stands in contrast to

* Anhui Provincial Philosophy and Social Sciences Key Laboratory of Digital Technology and Rural Revitalization, Chuzhou University, Chuzhou 239000, China. e-mail: daxingwang@chzu.edu.cn

traditional wired networks, where specialized hardware like routers handles these tasks. As a result of their self-organized and decentralized nature, ad hoc networks are inherently more susceptible to a variety of security risks. Accordingly, ensuring robust security has become a fundamental requirement for their reliable operation.

Among the various routing protocols designed for MANETs and mesh architectures, the Ad hoc On-demand Distance Vector (AODV) protocol [2] is widely recognized and frequently implemented. Nevertheless, developing a secure and dependable variant of AODV remains an ongoing challenge, as noted in [3]. The AODV routing protocol, as a typical on-demand routing protocol, has many excellent properties and is currently the most widely used routing protocol. However, the AODV routing protocol is also vulnerable to various attacks. The black hole attack is a relatively common type of attack [4]. During the route discovery process, it deceives the source node by self-promoting routing, claiming to have a route to the destination node and absorbing packets destined for the target node, forming a data black hole and seriously affecting the performance of the mobile network. Securing ad hoc networks has thus gained prominence, leading to numerous routing protocols designed to counter various attack models. For instance, Hu et al. introduced the Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [5], building upon the Destination Sequences Distance Vector (DSUV) [6] protocol. An on-demand secure routing method, Artificial TCP, was also proposed to enhance DSR. Two protocols, SAODV [8] and ARAN [9], were developed to address security flaws in AODV. Zapata et al. created Secure AODV (SAODV) to protect AODV routing messages, integrating digital signatures for authenticating non-mutable fields and hash chains for securing mutable ones. Sanzgiri et al. devised Authenticated Routing for Ad hoc Networks (ARAN), wherein each node holds a certificate from a trusted authority, and security is maintained via hop-by-hop signatures. The concept of aggregate signature was first introduced by Boneh et al. in their seminal work [10]. This cryptographic primitive is designed to combine n distinct signatures—each generated by n potentially different signers on n different messages—into a single compact signature. The resulting aggregate signature retains the same level of authenticity and non-repudiation as the original n individual signatures, thereby providing a powerful mechanism for signature consolidation.

At its core, aggregate signature is a form of digital signature that supports the compression of multiple signatures from various signers on different messages into one unified signature. This technology is especially valuable in applications where verification efficiency and data compactness are critical. For instance, in blockchain systems, aggregating signatures can significantly reduce the size of transaction data, enhancing scalability and throughput. Similarly, in the Internet of Things (IoT), where numerous devices frequently transmit signed data, signature

aggregation helps minimize communication overhead and energy consumption. In cloud computing environments, it allows efficient verification of bulk-signed documents or logs, streamlining audit processes and resource usage [11].

The fundamental objective behind aggregate signatures is to lower the costs associated with storing and transmitting signature data, without compromising the security guarantees or integrity of the original messages. By merging multiple signatures into one, the scheme reduces the computational burden during verification and decreases bandwidth requirements, making it particularly suitable for large-scale and resource-constrained systems.

A graphical representation of the process of aggregating multiple signatures into a single signature is provided in Fig. 1, illustrating the flow from individual signatures to the final aggregated form.

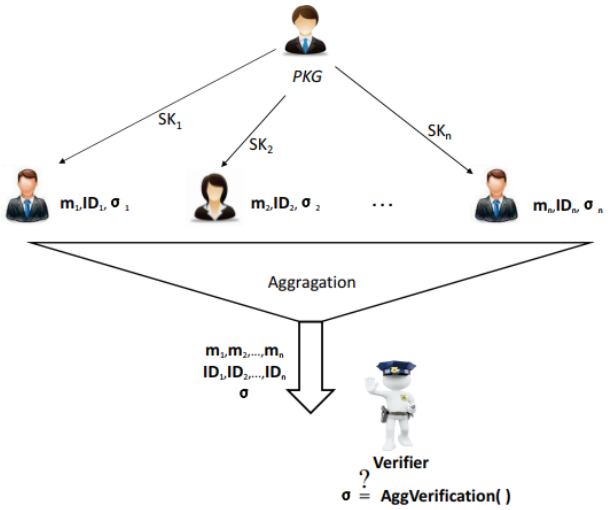

Fig.1. The process of aggregate signatures

A common method for constructing Identity-Based Signature (IBS) schemes relies on a generic transformation that turns any conventional standard signature (SS) scheme into an IBS. In this method, a standard signature is augmented by attaching a certificate that includes the signer's public key. This certification-based methodology is widely recognized and often regarded as part of cryptographic folklore. Bellare et al. [12] rigorously formalized this concept, proposing a generalized and provably secure methodology that enables the construction of identity-based signature (IBS) schemes from any existent secure standard signature (SS) system. Subsequently, Galindo et al. [13] extended the framework introduced by Bellare et al. to devise a more versatile IBS architecture capable of accommodating enhanced functionalities. A notable outcome of their work is a universal technique for building identity-based aggregate signature (IBAS) systems from conventional signatures that permit fixed-length aggregation

[14]. However, a major drawback of this IBAS approach is that the size of the resulting signature increases in direct proportion to the number of participating signers, denoted as n, since the aggregate signature must be accompanied by n public keys. Furthermore, the practical applicability of this approach is constrained by the fact that very few standard signature schemes natively support constant-length aggregation—primarily the BLS short signature scheme, whose aggregate signature mechanism is described in [15–17]. When using the BLS scheme within the Galindo et al. framework, the resulting IBAS requires O(n) pairing operations during verification.

In use cases where identity-based signatures from multiple signers need to be verified in batch over extended periods, verification efficiency and operational flexibility are often more critical than communication overhead. It is well known that pairing operations are the most computationally expensive component in pairing-based cryptosystems. Although significant research has been conducted to analyze and optimize pairing computations, they remain time-intensive in practice. Therefore, to develop cryptosystems suitable for real-world deployment, it is essential to minimize the number of pairing operations [18–20].

In this work, we introduce a new IBS construction that serves as the foundation for an IBAS scheme requiring only a constant number of pairing operations—independent of the number of signers. Our IBAS approach eliminates the need for additional communication rounds or strict synchronization for randomness aggregation, although it does not produce compact signatures. The remainder of the paper is structured as follows: Section II provides background on aggregate signatures. Section III introduces our new IBAS scheme and offers a comparative analysis with existing systems. Section IV presents a secure authenticated routing protocol based on the proposed scheme. Finally, Section V offers concluding remarks.

2. Related Background

2.1 Formal Definitions and Underlying Computational Assumptions

Let G_1 be a cyclic additive group of order q, G_2 a cyclic multiplicative group of the same order. A bilinear paring $e: G_1 \to G_2$ is said to be admissible if it satisfies the following:

(1) Bilinearity: For all $P, Q \in G_1$ and $a, b \in Z_q^*$, we have

$$e(aP, bQ) = e(P, Q)^{ab}$$

(2) Non-degeneracy: There exists a point $P \in G_1$ such that $e(P, P) \neq 1$. That is, the pairing does not trivially map all inputs to the identity in G_2.

(3) Efficient Computability: The value $e(P, Q)$ can be computed in polynomial time for any $P, Q \in G_1$.

Such pairings are typically instantiated using the Weil or Tate pairings over suitably chosen supersingular elliptic curves, with appropriate modifications to ensure non-degeneracy and efficiency.

Within this framework, we consider two classical hardness assumptions:

(1) Computation Diffie-Hellman Problem (CDH): Given $(P, aP, bP) \in G_1^3$ for randomly chosen $a, b \in Z_q^*$, the task is to compute abP.

(2) Bilinear Diffie-Hellman Problem (BDH): Given $(P, aP, bP, cP) \in G_1^4$, compute $e(P,P)^{abc} \in G_2$.

These assumptions form the security foundation for many identity-based and pairing-based cryptosystems.

2.2 Algorithmic Structure of Identity-Based Aggregate Signature Schemes Components of IBAS schemes

An Identity-Based Aggregate Signature (IBAS) scheme extends a standard Identity-Based Signature (IBS) scheme by allowing multiple signatures from different users to be compactly aggregated into one. Formally, an IBAS consists of the following algorithms:

(1) $Setup(\lambda)$: A probabilistic algorithm that takes a security parameter λ and returns public system parameters params and a master secret key msk. This algorithm is run by a trusted Private Key Generator (PKG).

(2) $Extract(ID, msk)$: A key issuance algorithm that, given an identity ID and the master secret, outputs a corresponding private key d_{ID}. This step ensures users derive their keys from their identities.

(3) $Sign(d_{ID}, m)$: A probabilistic algorithm that generates a signature σ on a message m using the private key d_{ID}.

(4) $Verify(ID, m, \sigma)$: A verification algorithm that accepts a message-signature pair (m, σ) and identity ID and returns 1 (accept) or 0 (reject).

(5) $Agg(\{(ID_i, m_i, \sigma_i)\}_{i=1}^n)$: An aggregation algorithm that combines n signatures from n distinct users on (possibly) distinct messages into a single aggregate signature Σ.

(6) $AVerify(\{(ID_i, m_i, \sigma_i)\}_{i=1}^n, \Sigma)$: An aggregate verification algorithm that checks whether Σ is a valid aggregate signature for the given set of identity-message pairs.

From a theoretical perspective, the security of such a scheme generally relies on the difficulty of the BDH or CDH problems in the underlying groups, and is often proved in the random oracle model under chosen-message attacks.

From a practical standpoint, IBAS schemes significantly reduce communication and storage overhead in systems requiring batch signature

verification—such as blockchain transactions, vehicular ad-hoc networks (VANETs), and large-scale authenticated data aggregation in IoT systems. The ability to verify many signatures at once without compromising security makes IBAS particularly attractive in resource-constrained environments.

3. Algorithm efficient ID-based Aggregate Signature Scheme

3.1. Proposed ID-based aggregate signature scheme: IBAS

We now present a novel IBS scheme that serves as the foundation for an efficient IBAS approach.

Setup. With security parameter $k \in Z$, the algorithm proceeds as follows:

(1) Generate a prime q, groups G_1, G_2 of order q, a generator P in G_1 and an admissible pairing $e: G_1 \times G_2 \to G_2$.

(2) Select a random $s \in Z_q^*$ and set $P_{pub} = sP$.

(3) Choose cryptographic hash functions $H_1: \{0,1\}^* \to G_1$ and $H_2: \{0,1\}^* \to Z_q$. The system parameters are

$$Params = (q, G_1, G_2, e, P, P_{pub}, H_1, H_2).$$

Extract. For a given string $ID \in \{0,1\}^*$,

(1) Compute $Q_{ID} = H_1(ID) \in G_1$.

(2) The private key is $S_{ID} = s \cdot Q_{ID}$.

Sign. Given a private key S_{ID} and a message $M \in \{0,1\}^*$,

(1) Choose $r \in_R Z_q^*$ and compute $U = r \cdot P \in G_1$.

(2) Compute $h = H_2(ID, M, U) \in Z_q$, and $V = S_{ID} + h \cdot r \cdot P_{pub} \in G_1$. The signature on m is $\sigma = (U, V)$.

Verify. For a signature $\sigma = (U, V)$ on m for identity ID:

(1) Compute $Q_{ID} = H_1(ID) \in G_1$ and $h = H_2(ID, M, U) \in Z_q$.

(2) Check whether $e(V, P) = e(Q_{ID} + h \cdot U, P_{pub})$, If the equality holds, accept; otherwise, reject.

Agg. Let $S \subseteq A$ be a subset of users. Each user $A_i \in S$ computes a signature (U_i, V_i) on a message M_i. The aggregate signature is

$$\Sigma = (U_1, \cdots, U_k, V = \sum_{i=1}^{k} V_i)$$

AVerify. Given an aggregate signature $\sigma = (U_1, \mathrm{L}\ , U_k, V)$ as above,

(1) Compute $Q_i = H_1(ID_i)$ and $h_i = H_2(ID_i, m_i, U_i)$, $i = 1, \mathrm{L}\ , k$.

(2) Verify $e(V, P) = e(\sum_{i=1}^{k} (Q_i + h_i \cdot U_i), P_{pub})$, Accept if valid; otherwise, reject.

3.2. Implementation and Comparison

This section outlines the implementation of our IBAS approach and evaluates its performance, followed by a proposal for enhancing efficiency in common application settings. The construction of our SAS method relies on Pairing-Based Cryptography (PBC). For 80-bit security, elliptic curve cryptosystems necessitate a minimum key size of 160 bits, whereas discrete logarithm systems call for at least 1024 bits. Accordingly, we adopted an MNT curve with embedding degree 6—near the ideal ratio of 1024/160 ≈ 6.4—to fulfill this requirement. Under this configuration, the group G must be no smaller than 171 bits, and G_1 requires at least 1024 bits to maintain discrete logarithm security. We utilized a 175-bit MNT curve produced through the parameter generation tool within the PBC library.

Performance assessments were conducted on a laptop equipped with a Pentium Dual-Core E6500 processor running at 2.93 GHz. Using the PBC library, a single pairing operation takes 13.0 ms, while exponentiation in G_1 and G_2 requires 1.55 ms and 18.3 ms, respectively. In a scenario with 100 participants (indexed 1 through 100) in the sequential aggregate signature process, the setup phase completes in approximately 0.159 seconds, involving The computational cost includes three exponentiation operations in the group G_1 and five within G_2. Each user's key generation requires about 0.185 seconds, entailing six exponentiations in G_2 and one pairing operation.

The aggregate signing process involves validating the prior aggregate signature and incorporating the new signature. Execution time increases with the user's position in the sequence, with nearly 98% of the effort dedicated to verification—specifically, $4\ell + 14$ exponentiations in G_2, where ℓ is defined as the number of prior signers. For instance, the 50th user would spend 2.421 seconds on verification and only 0.065 seconds to append its signature.

To boost verification performance, preprocessing of exponentiations in G_2 can be employed. This approach assumes users retain public keys of previous participants. In use cases with infrequent user changes—such as routing or certificate chains—public keys can be preprocessed after the initial aggregation. Offline precomputation of public parameters and verification elements is also feasible. With preprocessing, verification time can be cut to just 30% of the original. Lastly, we provide a computational efficiency comparison between our scheme and those in references [14, 19, 20], focusing on costly operations like exponentiations and bilinear pairings. The results are summarized in Fig. 2, where P denotes pairing and SM refers to scalar multiplication.

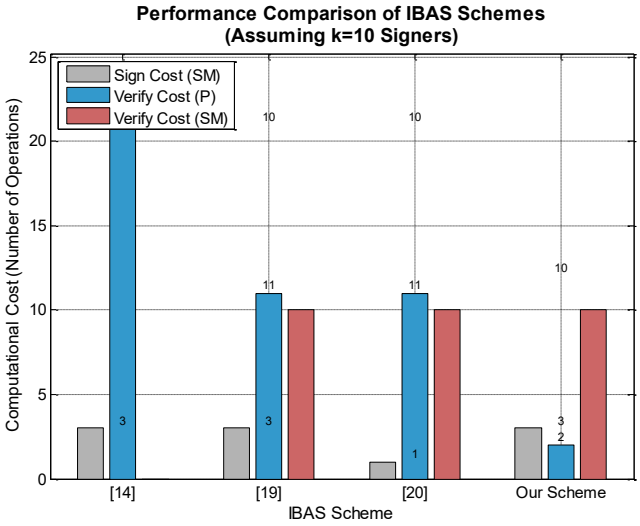

Fig.2. Efficiency Analysis of Different Schemes

4. Application to the on-demand Routing Protocol in MANET

4.1. The Principle of the AODV Routing Protocol

(1) Route Discovery

When a source node sends a data packet to a destination node, if the source node does not have a route to the destination node, it enters the route discovery phase. The source node broadcasts a Route Request (RREQ) message to its neighboring nodes. Upon receiving the RREQ, a neighboring node first establishes a reverse route and then determines whether it is the destination node. Upon determining that a neighboring node is indeed the target destination, the node promptly issues a Route Reply (RREP) packet in response and establishes a forward route along the return path. If not, The node proceeds to propagate the RREQ across its adjacent nodes until the target node is located. Upon acquisition of the RREP by the originating node, it indicates that the route discovery process has been completed.

The route discovery process is shown in Fig. 3. Source node S broadcasts RREQ to neighboring nodes A, B, and C. Nodes A, B, and C, upon determining that they are not the destination node, continue to broadcast the RREQ. Among them, node B's next hop is node C, but C has already received the same RREQ, so it directly discards the request from B. Therefore, the paths that ultimately reach the destination node D are: S—A—F—D and S—A—E—D. Since the RREQ of the path S—A—E—D reaches the destination node first, this path is selected to establish the route.

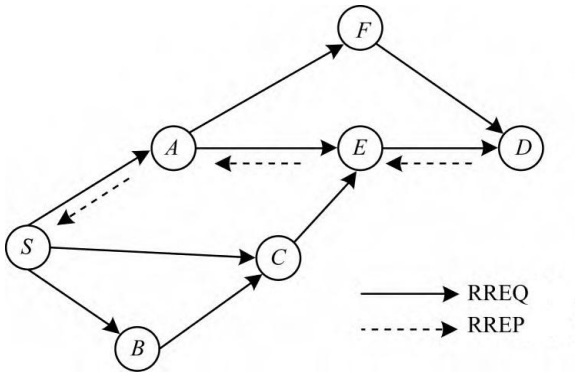

Fig.3 Process of routing discovery

(2) Route Maintenance

Route maintenance can be divided into proactive maintenance and reactive maintenance. Proactive maintenance involves periodically sending HELLO messages to neighboring nodes to detect active routing links. Upon receipt of a HELLO message, an adjacent node refreshes the validity duration entry associated with the originating node within its routing table. Nodes that exceed their lifetime are periodically removed, and destination node information with a next hop of a failed node is packaged into a Route Error Message (RRER) and broadcast. Reactive maintenance occurs as data packets are being forwarded when a node discovers that the route to the destination node has failed or receives an unreachable message from the link layer. In such cases, the node constructs an RRER and broadcasts it, while also entering local recovery or re-initiating route discovery.

The route maintenance process is shown in Fig. 4. When node E detects a link failure between E and D, it forwards an RRER to its neighboring nodes. Node A, upon receiving the RRER, adds all routing information related to the failed path in its routing table to the RRER and continues to forward it to its neighboring nodes until all nodes related to the broken path are notified. Since nodes F, C, and B do not have routes related to the broken link, node C discards the RRER forwarded by E, while nodes F and B do not receive the RRER. Node S receives the RRER from A, and if S still needs to send data packets to D, it re-enters the route discovery phase.

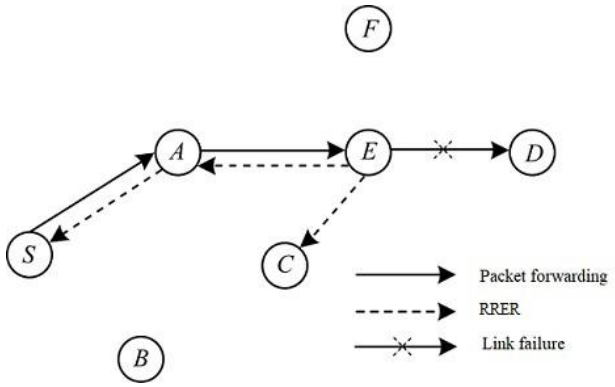

Fig.4 Process of routing maintenance

It can be seen that the AODV protocol establishes minimum-hop routes through flooding control packets. Since it is not sensitive to local area information, it is prone to establishing routes with fewer hops but lower energy and poor link quality, leading to unstable topology formation that is easily broken. This can also cause broadcast storms, thereby reducing the network's lifespan.

4.2. Implementation of routing protocols

In this section, we introduce an on-demand security routing mechanism structured around three main stages: initial setup, the discovery of routes, and ongoing route upkeep. Its protection mechanisms rely on the previously described ID-based aggregate signature technique. For convenience, we abbreviate our proposed protocol as SAR (Secure Aggregate signature-based Routing). The protocol begins with Route Request (RREQ) Propagation, which operates identically to the standard AODV protocol. The source node S floods the network with an RREQ packet. Intermediate nodes create reverse path entries and rebroadcast the request toward the destination.

Next, the Route Reply (RREP) Generation and Aggregation phase is initiated. Upon receiving the RREQ, the destination node D generates a Route Reply (RREP). As the RREP traverses back along the reverse path toward the source S, each intermediate node authenticates the packet and contributes its signature to an aggregate signature structure. Specifically, node D computes an individual signature σ_D on the RREP message m (containing routing information) using its private key S_D via the Sign algorithm, setting the initial aggregate signature to σ_agg = σ_D. It then unicasts the RREP to the next hop (node C).

When an intermediate node (e.g., node C) receives the RREP, it first verifies the current aggregate signature σ_agg using the AVerify algorithm and the public keys (identities) of all nodes already included in the signature. If verification fails, the packet is discarded. If successful, node C computes its own

individual signature σ_C on message m, then aggregates it with the received signature by computing σ_agg' = Agg(σ_agg, σ_C). Node C updates the packet with the new aggregate signature and forwards it to the next hop (node B). This process repeats iteratively for each node along the reverse path (e.g., node B, then node A).

Finally, during Source Verification, The RREP packet is successfully delivered to the source node S containing the final aggregate signature σ_agg, which combines signatures from all nodes along the path (D, C, B, and A). Rather than verifying each signature individually, S performs a single aggregate verification operation (AVerify) using the identities of all nodes in the route. If the verification is successful, the route is deemed authenticated and trustworthy. This process is illustrated in Fig. 5.

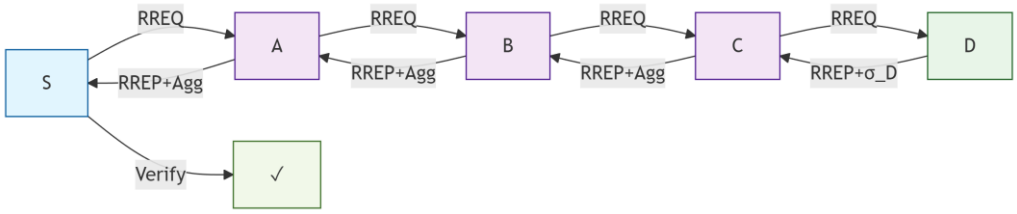

Fig.5 The SAR Route Discovery Process

We employed NS2 simulations to assess the performance of SAR and SAODV in a non-adversarial environment. All nodes were assumed to be loosely time-synchronized, incorporating a fixed synchronization discrepancy. Node movements followed the random waypoint model with a maximum velocity of 20 m/s. In this model, the Pause Time denotes the duration a node remains stationary after reaching a destination before moving to the next waypoint. By varying the Pause Time, we simulate networks with different levels of mobility: longer pause times correspond to more stable topologies, while shorter pause times reflect highly dynamic environments. The simulation area measured 1500 m by 300 m and contained 50 nodes. The upper bound of traversal delay through the network was configured to 0.1 seconds, and each node had a communication radius of 250 meters. A total of 15 node pairs maintained communication, with each source transmitting constant bit rate (CBR) traffic consisting of 64-byte packets at a rate of 4 packets per second. The available link bandwidth was 1 Mbps. Hash, MAC, and key sizes were each set to 80 bits, while signatures were 1024 bits in length. The TESLA interval was 1 second with a synchronization error of 0.1 seconds. Signature generation and verification times were set to 10 ms and 1 ms, respectively; hash computation times were not included.

Every node was assigned a unique hash derived from its identity. We conducted a comparative analysis between SAR and SAODV under identical

network conditions and parameter sets. To ensure a fair comparison, both caching (SAODV1) and non-caching (SAODV2) variants of SAODV were evaluated. The assessment included the following performance indicators: packet delivery ratio, routing overhead (measured in both packet count and byte volume), and end-to-end packet delay.

Results, averaged over 60 simulation runs with distinct mobility patterns for each pause time, are depicted in Figs. 6 and Figs. 7. Error bars represent 95% confidence intervals. SAR exhibited a maximum decrease of 1% in delivery ratio across all pause times, indicating superior performance over both SAODV implementations.

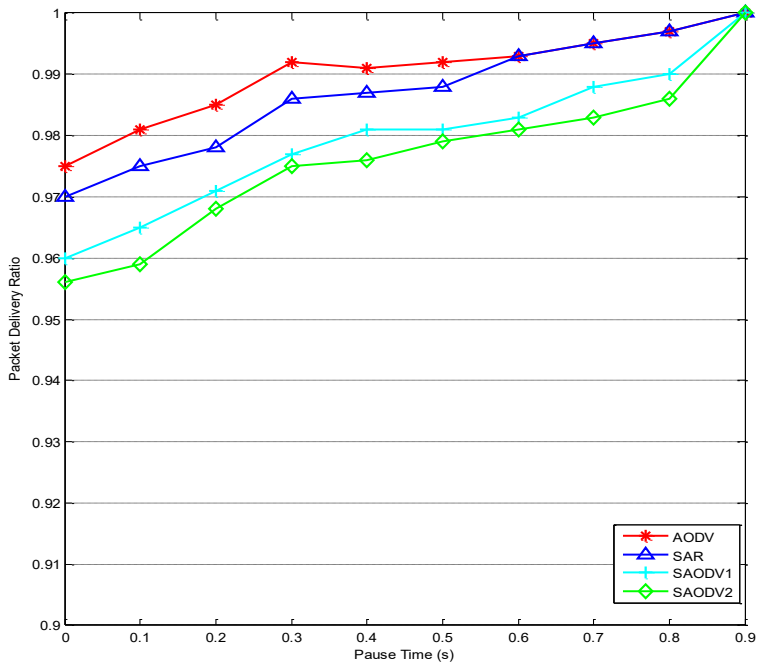

Fig.6. Performance comparison: Packet Delivery Ratio

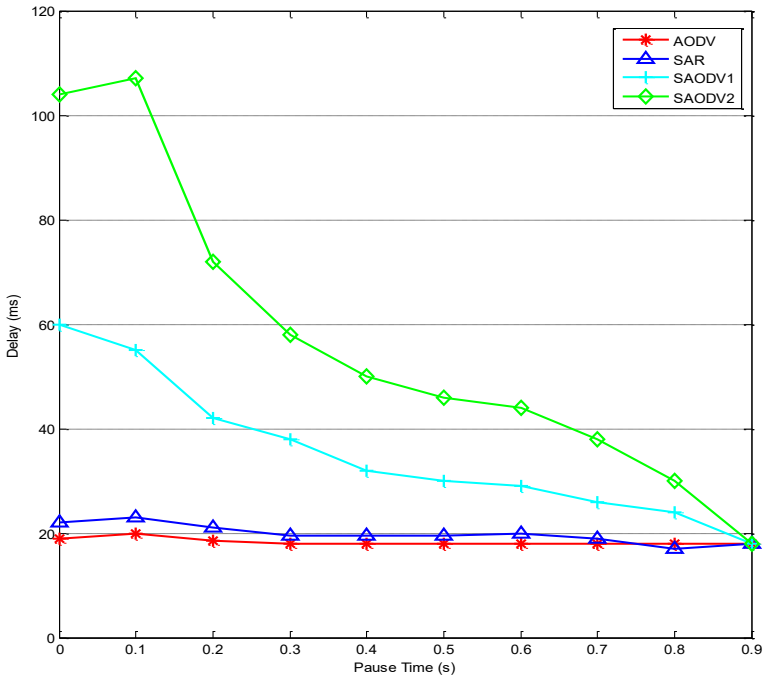

Fig.7. Performance comparison: Packet Delivery Delay

The cached version of SAODV showed improved delivery ratio compared to the non-cached variant. In terms of packet count, SAR's routing overhead was comparable to that of AODV, though approximately double in byte volume. Notably, SAODV incurred about four times the routing overhead bytes compared to SAR. The average packet delay in SAR saw a minor rise due to additional communication demands, whereas SAODV experienced significantly larger increases—approximately threefold with caching and fivefold without. Across all evaluated metrics, SAR demonstrated better overall performance than both forms of SAODV.

4.3 Comparative Analysis of Signature Operations and Performance with SAODV

Although the SAR protocol introduces a hop-by-hop aggregate signature mechanism in the RREP phase, requiring each intermediate node to perform one signing and one aggregate verification operation—which may appear to involve more per-node operations compared to SAODV (where each node verifies only one signature)—SAR demonstrates significant advantages in terms of system-level overhead and scalability. In SAODV, each node must independently verify the signatures of all nodes along the path, resulting in a

linear increase in verification operations with path length, and each verification involves computationally expensive bilinear pairing operations. In contrast, the aggregate verification process in SAR requires only a constant number of pairing operations, independent of the path length, thereby substantially reducing verification latency and computational load in long-path or multi-hop scenarios. Furthermore, by compressing multiple individual signatures into a single fixed-length signature through signature aggregation, SAR significantly reduces the size of routing packets, lowering bandwidth consumption and transmission delay. Thus, despite slightly more per-hop signature operations, SAR's overall optimization in verification efficiency and communication overhead enables it to achieve superior end-to-end performance in dynamic and resource-constrained MANET environments.

Nevertheless, SAR still faces some practical constraints. First, it demands that nodes possess adequate computational power to execute pairing-based operations, which could be challenging for highly resource-limited devices. Second, the initialization phase depends on a trusted Private Key Generator (PKG), creating a potential central trust and setup overhead. Third, even though aggregate verification is efficient, per-hop signing still introduces computational latency that may affect performance in highly dynamic networks with frequent route changes. These limitations suggest that SAR is best suited for networks where nodes have moderate processing capabilities and routes remain relatively stable. Future work may focus on reducing the computational cost of signing and exploring adaptive signing strategies.

5. Conclusions

In this paper, we have proposed a novel identity-based aggregate signature (IBAS) scheme that significantly improves both communication efficiency and verification performance in resource-constrained environments such as MANETs. Unlike existing IBAS constructions, our scheme requires only a constant number of pairing operations during verification, regardless of the number of signatures aggregated. This is achieved through a carefully designed IBS structure that supports efficient aggregation without compromising security.

We have demonstrated the practicality of our scheme by integrating it into an authenticated on-demand routing protocol, referred to as SAR (Secure Aggregate signature-based Routing). Through extensive simulations in NS2, Under the same network environment, we evaluated and compared the performance of SAR and SAODV. The results indicate that SAR achieves a comparable packet delivery ratio while substantially reducing routing overhead and end-to-end delay. Specifically, SAR incurs only half the byte overhead of

SAODV and exhibits significantly lower latency, making it more suitable for dynamic and resource-limited ad hoc networks.

The security of our IBAS scheme is based on the hardness of the Bilinear Diffie-Hellman (BDH) problem, and its efficiency is validated through both theoretical analysis and practical implementation. The scheme is particularly advantageous in scenarios requiring batch verification of multiple signatures, such as in vehicular ad hoc networks (VANETs), IoT systems, and other large-scale distributed networks.

Subsequent efforts will concentrate on reducing the computational cost of the signing operation. Extending the scheme to support more advanced cryptographic properties (such as forward security or revocability), and exploring its application in other types of wireless networks beyond MANETs.

Acknowledgments

The author expresses sincere gratitude to the Editor-in-chief and the referees for their insightful comments and suggestions that have significantly enhanced the quality of our paper. This work was supported by the Open Fund Project of Anhui Provincial Philosophy and Social Sciences Key Laboratory of Digital Technology and Rural Revitalization in Chuzhou University (ZSKF202502), the Scientific Research Project of the Education Department of Anhui Province (2025AHGXZK30459), the Research Team on Innovative Application of Big Data and Financial Technology of Chuzhou University.

R E F E R E N C E S

[1] *Cho J.H., Swami A, Chen I.R.,* A Survey on Trust Management for Mobile Ad Hoc Networks. IEEE Communications Surveys & Tutorials, 2010, **2**(4): 562-583. DOI:10.1109/SURV.2011.092110.00088.

[2] *C. Perkins, E. Belding-Royer, and S. Das,* Ad hoc on-demand distance vector (AODV) routing, 2003. IETF RFC 3561.W.-K. Chen, Linear Networks and Systems (Book style). Belmont, CA: Wadsworth, pp. 123–135. DOI： 10.1109/MCSA.1999.749281.

[3] *Ahmed N., Mohammadani K., Bashir A.K. et al.,* Secure and Reliable Routing in the Internet of Vehicles Network: AODV-RL with BHA Attack Defense. Computer Modeling in Engineering & Sciences, 2024, **139**(4): 633-659. DOI:10.32604/cmes.2023.031342.

[4] *Gupta S., Singla S., Sharma P*., Enhanced Security in MANETs Using AODV Protocol. Journal of The Institution of Engineers (India): Series B, 2025, **106**(1):327-338. DOI:10.1007/s40031-024-01103-1.

[5] *Hu Y.C., Johnson D.B., Perrig A*., SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks, 2003, **1**(1):175-192. DOI: 10.1016/S1570-8705(03)00019-2.

[6] *C. Perkins and P. Bhagwat,* Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In Proceedings of the SIGCOMM Conference on Communications Architectures, Protocols and Applications, pp. 234-244. DOI:10.1145/190314.190336.

[7] *Hu Y.*, Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. Wireless Networks, 2002, **11**(1-2). DOI:10.1145/570645.570648.

[8] *M.G. Zapata and N. Asokan,* Securing ad hoc routing protocols. In Proceedings of ACM Workshop on Wireless Security (WiSe), pp. 1-10. DOI:10.1145/570681.570682.

[9] *K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M.,* Belding-Royer. A secure routing protocol for ad hoc networks. In Proceedings of the 10th IEEE International Conference on Network Protocols, pp. 78-87. DOI:10.1109/ICNP.2002.1181388.

[10] *D. Boneh, C. Gentry, B. Lynn,* Aggregate and verifiably encrypted signatures form billinear maps. Proceedings of Advances in Cryptology-Eurocrypt'2003, Warsaw, pp.416–432. DOI: 10.1007/3-540-39200-9_26

[11] *Tomar A., Tripathi S, Arivarasan K. A.,* Blockchain-Based Certificateless Aggregate Signature Scheme for Fog-Enabled Smart Grid Environment. IEEE Transactions on Green Communications and Networking, 2023, **7**(4):1892-1905. DOI:10.1109/tgcn.2023.3265608.

[12] *Bellare, M., Namprempre, C., Neven, G.,* Security proofs for identity-based identification and signature schemes. In: Advances in Cryptology: Eurocrypt'04, LNCS 3027. Springer-Verlag, pp.268–286. DOI: 10.1007/978-3-540-24676-8_16

[13] *Galindo, D., Herranz, J., Kiltz,* On the generic construction of identity-based signatures with additional properties. In: Advances in Cryptology: Asiacrypt'06, LNCS 4284. Springer-Verlag, pp.179–193. DOI: 10.1007/11935230_12

[14] *LIANG Y. F, LIU Y N.,* Analysis and improvement of an efficient certificateless aggregate signature with conditional privacy preservation in VANETs. IEEE Systems Journal, 2023, **17**(1): 664–672. DOI: 10.1109/JSYST.2022.3180221

[15] *Tang F., Huang D.,* A BLS Signature Scheme from Multilinear Maps. Int. J. Netw. Secur. 2020, **22**:728-735.DOI:10.6633/IJNS.202009_22(5).02.

[16] *ALI I., CHEN Y., ULLAH N. et al.,* An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs. IEEE Transactions on Vehicular Technology, 2021, **70**(2): 1278–1291. DOI: 10.1109/TVT.2021.3050399

[17] *Shi H., Chen Z., Cheng Y. et al.,* PB-Raft: A Byzantine fault tolerance consensus algorithm based on weighted PageRank and BLS threshold signature. Peer-to-Peer Networking and Applications, 2025, **18**(1):1-16. DOI: 10.1007/s12083-024-01876-8.

[18] *Xu R., Zhou Y., Yang Q. et al.,* An efficient and secure certificateless aggregate signature scheme. Journal of Systems Architecture, 2024, 147. DOI:10.1016/j.sysarc.2023.103030.

[19] *XIONG W.J., WANG R.M, WANG Y.J. et al.,* A conditional privacy-preserving batch authentication scheme based on certificateless aggregate signature for VANETs. Journal of Cryptologic Research, 2023, **10**(3): 462–475. DOI: 10.13868/j.cnki.jcr.000605

[20] *Rastegari P.,* Authentication in VANETs with Conditional Privacy-Preserving Property Using Certificateless Aggregate Signature Schemes. International Journal of Mathematical Sciences and Computing (IJMSC), 2024, **10**(4):12. DOI:10.5815/ijmsc.2024.04.05.

[21] *Fotiadis G., Konstantinou E.,* On the Efficient Generation of Generalized MNT Elliptic Curves. Springer Berlin Heidelberg, 2013. DOI: 10.1007/978-3-642-40663-8_15.