International Journal of Safety and Security Engineering
Vol. 15, No. 10, October, 2025, pp. 2043-2054
Journal homepage: http://iieta.org/journals/ijsse

Toward Reliable Key Distribution in Wireless Ad Hoc Networks: A Software-Based Comparative Analysis of Key Management Schemes

Ahlem Nasri[1*], Abdelhabib Bourouis[1], Mohammed El Amine Fekair[2], Kenza Gasmi[1], Asma Saighi[3]

[1] Department of Mathematics and Computer Science, Research Laboratory on Computer Science's Complex Systems (ReLa (CS)[2]), University of Oum El Bouaghi, Oum El Bouaghi 04000, Algeria
[2] Department of Mathematics and Computer Science, University of Ghardaia, Ghardaïa 47000, Algeria
[3] Department of Mathematics and Computer Science, Artificial Intelligence and Autonomous Things Laboratory, University of Oum El Bouaghi, Oum El Bouaghi 04000, Algeria

Corresponding Author Email: nasri.ahlem@univ-oeb.dz

https://doi.org/10.18280/ijsse.151007

Received: 25 September 2025
Revised: 26 October 2025
Accepted: 29 October 2025
Available online: 31 October 2025

Keywords:
WANETs, KMSs, MANET security, threshold cryptography, distributed public key generator, simulation framework, OMNeT++

ABSTRACT

Wireless Ad Hoc Networks (WANETs) face critical security challenges due to their decentralized nature, and Key Management Schemes (KMSs) play a central role in ensuring confidentiality, integrity, and authentication. Although numerous KMSs have been proposed to address these challenges, their rigorous empirical evaluation remains fragmented in the literature. Many existing studies rely on qualitative comparisons or simulations under simplified and static scenarios, which fail to capture the complexities of dynamic environments. To bridge this gap, this study introduces a flexible and automated simulation framework designed for the systematic and comparative evaluation of multiple KMSs under diverse and dynamic network conditions. The evaluation framework implemented in OMNeT++/INET environment offers extensive user-configurable parameters—covering network topology, traffic patterns, node mobility, and KMS-specific settings. It integrates a comprehensive set of performance and security metrics, such as Secure Connectivity Achievement (SCA) and Key Freshness (KF). We conducted experiments under two complementary scenarios. The first is a basic scenario commonly used in prior works. The second is a realistic scenario that reflects larger and highly mobile networks. The evaluation of two representative KMS approaches—a Threshold-based KMS and a distributed identity-based system—demonstrated that variations in network size and conditions directly influenced the observed outcomes, with some configurations showing sharp performance degradation driven by synchronization failures and protocol-mobility mismatches. These findings highlight the necessity of generic and adaptable evaluation tools, thereby enabling researchers and practitioners the ability to tailor assessments to specific deployment contexts and better inform the selection of suitable KMS for real-world WANETs.

1. INTRODUCTION

Wireless Ad Hoc Networks (WANETs) represent a paradigm shift in wireless communication, enabling fully decentralized, infrastructure-free networking that is critical for emergency response, military operations, and remote sensing applications [1]. However, the inherent openness and high mobility of subclasses such as Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), and Flying Ad Hoc Networks (FANETs) expose them to critical security threats—including eavesdropping, spoofing, and node compromise—thereby necessitating robust mechanisms for secure communication [2].

A fundamental component of WANETs security is the Key Management Scheme (KMS), which serves as a foundation for authentication, key distribution, and secure data transmission [3]. Unlike conventional networks with centralized authorities, WANETs require distributed or hierarchical key management strategies to accommodate dynamic topologies and frequent node mobility. An effective KMS must ensure that only legitimate participants gain access to cryptographic keys while mitigating risks associated with node compromise and unauthorized access. Due to the inherently adversarial nature of open wireless environments, designing a KMS that balances efficiency, scalability, and resilience remains a pressing research challenge [4].

Despite substantial theoretical progress, key management persists as a major bottleneck in real-world deployments. The absence of a fixed infrastructure complicates trust establishment, while resource constraints (e.g., limited bandwidth, energy, and computational power) limit the feasibility of computationally intensive cryptographic schemes. Additionally, WANETs are highly susceptible to a spectrum of cyber threats—including node compromise, Sybil attacks, and man-in-the-middle exploits—that can undermine network integrity [5]. Compounded by vulnerabilities such as

malicious packet drops that cripple routing, these threats underscore the critical need for secure communication channels—a need that only a robust KMS can provide. This is the major challenge highlighted in recent MANET security analyses [6].

A key obstacle to practical deployment is the methodological gap between theoretical design and realistic validation. While significant cryptographic advances exist, most studies focus on static or idealized settings and rarely consider dynamic adversarial conditions [7-11]. Moreover, KMS performance is highly sensitive to environmental parameters such as routing protocols, mobility models, and physical constraints. As a result, a scheme that performs well in one context may fail in another. This strong context-dependence challenges the assumption of a single universally optimal solution and underscores the need for flexible, generalized evaluation frameworks capable of benchmarking multiple KMSs across diverse, customizable scenarios [12-14].

Furthermore, the resilience of these frameworks against active adversarial behavior remains inadequately assessed. The lack of evaluation under realistic and dynamic attack conditions limits the practical relevance of existing results, complicates evidence-based decision-making, and ultimately constrains the adoption of KMS in practice [15-18].

To address these interconnected gaps in evaluation rigor and adversarial testing, this study presents an innovative, modular, and extensible simulation-based framework designed to rigorously test KMSs' resilience in realistic MANET environments. Unlike Ad Hoc scripting approaches common in simulators such as OMNeT++, our framework formalizes KMS evaluation as a reusable methodological process rather than a one-off experimental setup. As a key extension, we incorporated and evaluated identity-based schemes. Specifically, we integrate two fundamentally distinct KMS archetypes: a threshold-based [12, 13] and a distributed identity-based KMS [14]. To our knowledge, this work presents the first simulation-based comparative analysis of these two KMSs categories within a unified and controlled evaluation environment tailored for MANETs.

The key contributions of this work are as follows:

(1) The design and implementation of a generic, modular, and extensible simulation framework that enables seamless integration of new protocols, attack models, and evaluation metrics, moving beyond Ad Hoc scripting.

(2) The integration of identity-based KMS into the evaluation framework, addressing a class of schemes not previously covered in comparative studies.

(3) The introduction of two novel evaluation metrics specifically designed for MANET environments: Key Freshness (KF), which quantifies the system's ability to maintain cryptographic key validity over time, and Secure Connectivity Achievement (SCA), which measures the proportion of node pairs capable of establishing secure communication links.

(4) Enhanced simulation flexibility that allows users to customize network scenarios and adversarial conditions, supporting a wide range of operational environments.

(5) The provision of actionable evaluation outcomes to guide deployment decisions in dynamic and resource-constrained network settings.

The remainder of this paper is organized as follows: Section 2 reviews related work, analyzing existing KMSs and evaluation tools to crystallize the identified research gaps. Section 3 provides the necessary background on WANETs and KMS principles. Section 4 details the architecture and components of the proposed evaluation framework. Section 5 presents a case study on the comparative evaluation of the two integrated KMSs, describing the experimental setup and methodology. Section 6 discusses the obtained results and their implications. Finally, Section 7 concludes the paper with key findings and outlines future research directions.

2. RELATED WORK

The evolution of KMS for WANETs has produced a rich diversity of schemes and evaluation tools. However, a critical analysis reveals persistent methodological gaps that limit their practical applicability. To systematically contextualize these gaps, Table 1 synthesizes the main contributions, inherent limitations, and the specific manner in which the proposed framework addresses these shortcomings for a representative selection of prior work across schemes and evaluation tools.

Table 1. Summary of recent KMSs and their evaluation limitations

Reference	Contribution	Limitation	Our Framework
		A. KMSs	
Msolli et al. [16]	Pre-distribution with hashed keys for connectivity & capture resistance.	No attack simulation; omits latency, overhead, and scalability.	Integrates attack modules (e.g., node compromise) and measures latency, overhead, and scalability.
Nafi et al. [17]	Certificateless signcryption for MANETs with low communication cost.	Static models lack attack resilience, energy, and variable density tests.	Uses dynamic mobility models, measures energy, tests under variable density & adversarial conditions.
Yuan et al. [18]	Pairing-free identity-based scheme for WSNs (low computation).	Theoretical focus; no benchmarking or realistic simulation.	Provides empirical, simulation-based benchmarking in realistic MANET scenarios.
Zhang and Liu [19]	Lattice-based scheme for post-quantum security in WSNs.	Focus on correctness only; no empirical/dynamic analysis.	Evaluates beyond correctness, using dynamic network simulations and security/performance metrics.
Sadi et al. [20]	Trust-clustering group key agreement using ECC.	Lacks comparative benchmarking & varied condition testing.	Enables direct comparative analysis of multiple KMS under customizable network conditions.
Janani et al. [21]	genetic algorithm-based optimization for three KMSs.	Limited scope (3 schemes); no baseline or attack resilience.	Supports extensible integration of many schemes, includes baselines and adversarial testing.

Sowmyadevi and Shanmugapriya [22]	Unsupervised ML for key management in WSNs.	Weak baselines; no attack scenarios; inconsistent conditions.	Ensures consistent experimental conditions and integrates concrete attack scenarios (e.g., Sybil).
Naresh et al. [23]	Blockchain-based hierarchical group key management.	No attack simulation; blockchain overhead not quantified.	Incorporates adversarial behavior simulation and measures protocol-specific overheads.
Jain and Singh [24]	Hybrid hierarchical scheme (symmetric/asymmetric).	Static WSN focus; no mobility validation.	Designed for dynamic topologies (MANETs), validating schemes under high mobility.
		B. Evaluation tools & methodologies	
Jurnečka et al. [25]	Automated KMS simulation in OMNeT++/MiXiM.	Deprecated framework (MiXiM); hard to port.	Built on a modern, maintained simulation backbone for sustainable evaluation.
Al-Haija et al. [26]	Simulator for probabilistic KMSs (VB.NET).	Platform-specific; limited to probabilistic schemes.	Modular and language-agnostic, supporting diverse KMS types (probabilistic, deterministic, identity-based).
Roman et al. [27]	Web tool for KMS selection.	Static, non-simulated; WSN-specific.	Provides a dynamic simulation environment adaptable to MANETs, VANETs, and FANETs.
Ragab-Hassen and Lounes [28]	Markov models for hierarchical KMS analysis.	Qualitative only; no quantitative/empirical testing.	Couples' formal insights with quantitative, empirical simulation results.
Ruan et al. [29] and Na et al. [30]	AHP-based comparison of 43 KMSs.	Subjective weighting; no dynamic scenario simulation.	Employs objective, scenario-driven benchmarking with configurable, reproducible metrics.
Kazienko and Albuquerque [31] and Kazienko et al. [32]	Lightweight KMS implementation on TinyOS motes.	Hardware-specific; not generalizable.	Offers a generalized simulation environment, decoupled from specific hardware.
Prantl et al. [33]	Group encryption evaluation in IoT testbed.	IoT-specific; lacks adversarial modeling.	Generalizable to various Ad Hoc networks with built-in adversarial modeling.

Table 1 synthesizes three recurrent and interconnected gaps in the literature:

(1) The isolation between scheme design and rigorous evaluation, where cryptographic innovations are rarely tested under dynamic, adversarial conditions;

(2) The rigidity of evaluation tools, which are often scheme-specific, platform-dependent, or lack adversarial depth;

(3) The absence of holistic metrics that capture both performance and security dimensions, like key validity over time (freshness) and SCA.

The proposed evaluation framework is designed explicitly to bridge these gaps. It advances beyond isolated evaluations by providing a unified, modular platform capable of integrating diverse KMS types—demonstrated here with threshold and identity-based schemes. It replaces rigid, ad-hoc tools with a configurable and reproducible methodological process. Most importantly, it introduces novel security-centric metrics (KF, SCA) alongside traditional performance indicators, enabling a multi-dimensional assessment that aligns evaluation more closely with the operational realities of MANETs. This integrated approach directly addresses the deficiencies cataloged in prior work, positioning our contribution as a step toward standardized and actionable KMS evaluation.

3. BACKGROUND

3.1 WANETs

WANETs are decentralized communication systems that operate without fixed infrastructure, resulting in highly dynamic topologies due to node mobility and energy constraints. This paradigm includes several subtypes, such as MANETs, VANETs, Wireless Sensor Networks (WSNs), and FANETs. Each is tailored to specific application domains.

WANETs are characterized by a set of inherent features that pose significant security challenges:

- Decentralized architecture: The absence of centralized control requires all network functions, including security, to be distributed among participating nodes.
- Dynamic topologies: Frequent node mobility leads to continuous changes in network structure, complicating routing and trust establishment.
- Limited resources: Energy, processing, and storage constraints restrict the use of computationally intensive cryptographic mechanisms.
- Open wireless medium: The broadcast nature of wireless communication increases vulnerability to eavesdropping, spoofing, and malicious data injection.
- Multi-hop communication: Data forwarding through intermediate nodes introduces risks of node misbehavior or compromise along transmission paths.
- Device and context heterogeneity: Nodes vary in capabilities and operate in diverse environments with differing mobility and communication ranges.

These characteristics collectively render WANETs highly susceptible to security threats, underscoring the need for robust and adaptive KMSs that can operate effectively under such constraints. Consequently, it is essential to develop evaluation frameworks that can capture these operational nuances. Such frameworks are needed to assess KMS performance and resilience in realistic scenarios.

3.2 KMSs

A KMS forms the foundation of secure communication in WANETs, overseeing the full cryptographic key lifecycle—

generation, distribution, storage, update, and revocation—to ensure confidentiality, integrity, and authentication.

KMS can be categorized along several design dimensions:

• Architecture: Centralized (relying on a trusted authority)/ distributed (shared responsibility among nodes).

• Deployment mode: Pre-distributed (keys installed before deployment) / dynamic (keys generated on-demand).

• Cryptographic paradigm: Symmetric (efficient but challenging for key distribution) / asymmetric (scalable but computationally intensive).

• Scope: Individual (node-to-node) / group-based (supporting multicast or broadcast).

• Trust model: Schemes that integrate trust mechanisms / those that operate independently.

• Key update policy: Static / dynamic key refresh mechanisms.

The key lifecycle, generally comprising generation, distribution, storage, update, and revocation phases, provides a structured basis for evaluating KMS robustness, scalability, and adaptability.

3.3 Selected KMS and their link to evaluation metrics

This study focuses on two fundamentally distinct KMS paradigms—threshold-based and distributed identity-based schemes—selected for their contrasting architectural principles and operational behaviors. Evaluating their effectiveness in dynamic, adversarial MANETs requires metrics that capture both security health and network utility. To this end, we introduce two novel, context-aware metrics:

• KF: Measures the temporal validity and current usability of cryptographic keys across the network. A high KF indicates that keys are recent and have not been compromised or expired, which is critical for preventing replay attacks and ensuring forward secrecy.

$$\mathrm{KF} = \frac{\text{Number of up-to-date keys}}{\text{Total number of keys}} \quad (1)$$

• SCA: Quantifies the proportion of node pairs that can successfully establish an authenticated and encrypted communication link at a given time. SCA reflects the practical security coverage and operational capacity of the network under a given KMS.

$$\mathrm{SCA} = \frac{\text{Number of securely connected node pairs}}{\text{Total number of node pairs}} \quad (2)$$

The architectural design of each KMS directly shapes its performance against these metrics:

• Threshold-based KMS employs a distributed t-of-n secret sharing mechanism, enhancing fault tolerance by requiring a quorum of nodes to perform key operations. This architecture introduces strong dependencies on node availability, network synchronization, and resistance to partial compromise. In highly dynamic or adversarial MANET environments, delays or failures in quorum formation can directly degrade KF, as key updates may be delayed or incomplete. Consequently, in dynamic MANETs, delays in quorum formation can degrade KF and subsequently impact SCA.

• Distributed identity-based KMS also follows a distributed model but derives public keys directly from node identities, decentralizing the Private Key Generator (PKG) functionality. Its resilience depends on the availability and consistency of PKG-share nodes rather than quorum formation. This design can offer more asynchronous and locality-aware key management. Therefore, under network fragmentation, KF may suffer in isolated domains, affecting SCA.

This explicit link between KMS architecture and measurable outcomes forms the core of our comparative analysis. The proposed evaluation framework is designed to quantify these relationships under realistic MANET conditions.

4. PROPOSED EVALUATION FRAMEWORK

To address the limitations of traditional evaluation practices for KMS in WANETs, this work proposes a comprehensive and extensible simulation-based framework. Its primary objective is to enable realistic, flexible, and security-aware assessments of diverse KMS architectures. These assessments are conducted under dynamic topologies and adversarial conditions that are representative of WANET environments.

4.1 Framework architecture

The framework's architecture, illustrated in Figure 1, is built around four core modules that orchestrate the evaluation workflow from scenario configuration to result analysis.

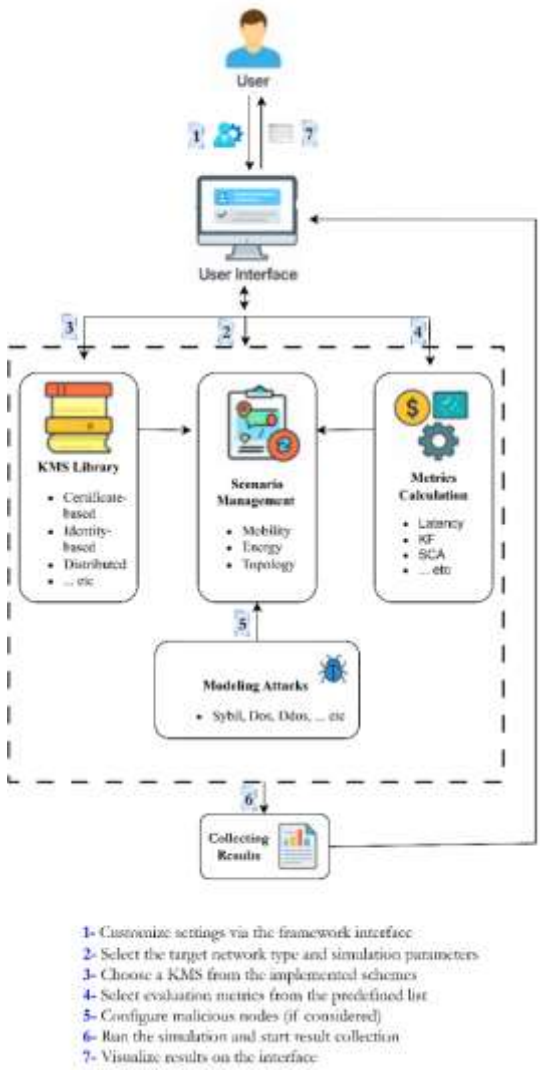

Figure 1. Overall architecture of the proposed framework

(1) Network configuration module: This component initializes and configures the network environment. It supports various WANET types (e.g., MANETs, VANETs, WSNs) through customizable parameters including topology, node density, mobility models, and energy constraints, allowing the definition of realistic deployment scenarios.

(2) KMS module: This module enables the seamless integration and instantiation of different KMS categories via pluggable components. It includes native support for identity-based approaches, specifically the threshold-based and Distributed identity-based KMS implemented in this study. Each scheme is adapted to the underlying network model.

(3) Attack simulation module: This component models and injects malicious behaviors to test KMS resilience. It supports the simulation of WANET-specific attacks (e.g., node compromise, Sybil attacks). Its internal layered architecture, detailed in Figure 2, ensures a systematic workflow from attack specification to impact analysis.

(4) Metrics calculation module: Dedicated to computing evaluation metrics, this module currently incorporates 10 predefined metrics covering performance, scalability, and security. It is fully extensible, allowing researchers to integrate custom metrics. Results are collected automatically in a structured format for comparative analysis.

The user interacts with the framework through a dedicated interface to select the network type, customize simulation parameters, choose the KMS for evaluation, and specify the metrics to be computed. Upon execution, the framework orchestrates the interactions among all modules, integrates attack models when required, and compiles the final evaluation results.

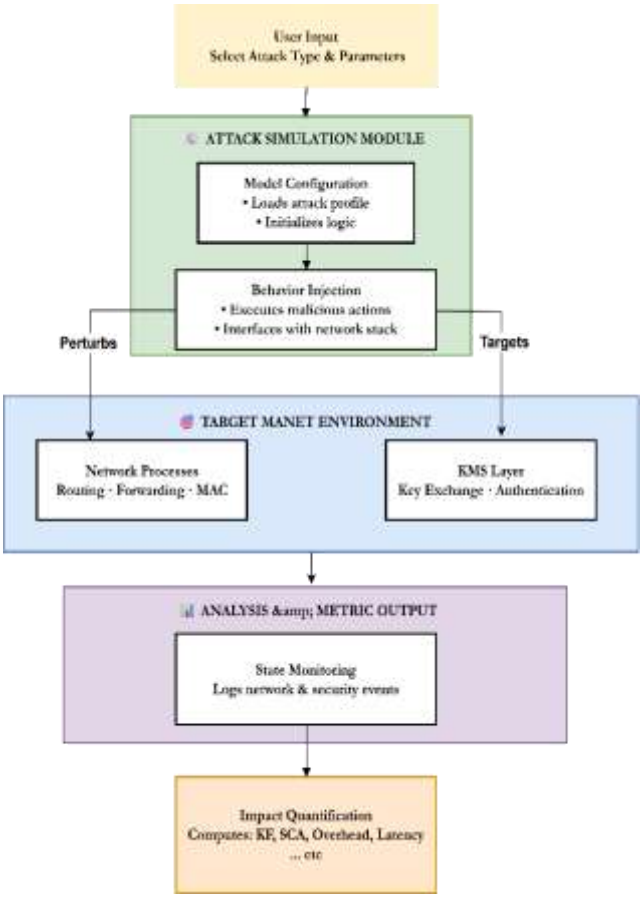

Figure 2. Operational architecture of the attack simulation module

5. CASE STUDY: COMPARATIVE EVALUATION OF IDENTITY-BASED KMS

This section presents a case study applying the proposed framework to evaluate the two identity-based KMS paradigms introduced in Section 3.3: the threshold-based KMS [12, 13] and the distributed identity-based KMS [14]. We first describe the experimental setup designed to assess their performance and robustness under varying network conditions, followed by the presentation and analysis of the results.

5.1 Experimental setup

To evaluate the effectiveness and robustness of the proposed evaluation framework and ensure a fair and reproducible assessment of the selected KMS approaches, we designed a comprehensive experimental setup using the OMNeT++ simulator and the INET framework. We conducted the evaluation under two complementary conditions: a basic scenario, derived from study [34], which reflects conventional configurations frequently employed in prior studies, and a realistic scenario that incorporates parameters more closely resembling actual MANET deployments. We adopted both scenarios for the following reason. Basic configurations provide a common benchmark and facilitate comparability with existing work. However, they often overlook the complexities inherent in real-world environments.

As most of the previous evaluations of KMS have been performed under such simplified settings, their reported results may not fully capture the challenges posed by dynamic topologies, resource constraints, and unpredictable mobility patterns. By complementing the basic scenario with a more realistic one, this study seeks to bridge this gap. This approach aims to yield a more reliable understanding of how KMS schemes would perform in operational networks.

The basic scenario was designed according to commonly adopted practices in MANET simulation studies [34], serving as a reference point for comparative evaluation. In this scenario, the transmission rate was fixed at 6 Mbps. We used the Free Space Path Loss propagation model, and performance metrics were collected every 10 s. The simulation parameters are summarized in Table 2.

Table 2. Parameters of the basic scenario

Parameter	Value
Number of nodes	25/35/50
Simulation area	500 m × 500 m
Node mobility model	Random waypoint
Pause time	2 s
Speed	1-10m/s
Transmission range	250M with the propagation model: RealisticRadioMedium
MAC protocol	IEEE 802.11
Simulation duration	200 s
Routing protocol	AODV
Traffic type	CBR 4 packets/s, 512 octets
Energy model	SimpleEpEnergyConsumer

To reflect conditions closer to real MANET deployments, we designed a more demanding, realistic scenario, as summarized in Table 3. This configuration uses FreeSpacePathLoss as the propagation model. For rate control, we employed *Minstrel*, which adapts across three rates: 6, 12, and 24 Mbps. This configuration introduces a larger number

of nodes, extended simulation duration, and more diverse traffic patterns, while also accounting for energy consumption and mobility variations.

Table 3. Parameters of the realistic scenario

Parameter	Value
Number of nodes	75/100/125/150
Simulation area	1000 m × 1000 m
Node mobility model	GaussMarkovMobility
Pause time	5–10 s
Speed	1–20 m/s
Transmission range	250M with the propagation model: RealisticRadioMedium
MAC protocol	IEEE 802.11
Simulation duration	600 s
Routing protocol	AODV
Traffic type	CBR 4 packets/s, 512 octets
Energy model	StateBasedEpEnergyConsumer

In addition to the simulation scenarios, the evaluation incorporates configuration parameters for the two selected KMS: ThreIdBasedCrypto and IdBasedCryptoSystem. For the threshold-based KMS, parameters were scaled proportionally to network size. The number of INITIAL Nodes (i.e., the number of nodes initially holding partial Master Secret Key shares) ranged from 5 to 30, and the threshold value (K) ranged from 3 to 18, corresponding to network sizes from 25 to 150 nodes. This scaling maintains cryptographic principles of security and fault tolerance. Timers for master and session keys were set to 5 seconds. In contrast, the distributed KMS employed a fixed configuration with five Virtual Private Key Generator (VPKG) servers, and timers of 2 and 5 seconds for client-originator and key response phases, respectively. These configurations ensured realistic operation while enabling fair comparative evaluation under consistent constraints.

Performance measurement was carried out at fixed time intervals of 10 seconds during the simulation rather than at the end only, to capture the dynamic evolution of the metrics.

This interval-based monitoring enabled a more accurate evaluation of how each KMS maintains secure connectivity and freshness of keys under highly mobile conditions. Each experiment was repeated with 10 different random seeds (min value = 0 and max value = 9), and the final results are averaged to ensure statistical reliability.

In total, combining the two KMSs with the basic and realistic scenarios yields 14 distinct experimental settings. The outcomes are presented as comparative figures, illustrating the evolution of the metrics across different network sizes and configurations.

6. RESULTS AND DISCUSSION

6.1 Performance assessment of the threshold-based scheme

This section presents the results of evaluating the Threshold KMS with respect to two key performance metrics: KF and SCA. The evaluation was conducted under two distinct experimental settings: a basic scenario and a realistic scenario. The comprehensive results are summarized in Figure 3.

Figures 3(a) and (b) depict the KF performance for the basic and realistic scenarios, respectively. Figures 3(c) and (d) present the SCA results for the basic and realistic scenarios, respectively.

6.1.1 KF evaluation

The *KF* results for the threshold-based KMS under basic conditions (Figure 3(a)) demonstrated near-perfect performance for smaller network sizes. For 25 and 35 nodes, *KF* maintains a stable value of 1.0 throughout the simulation, indicating flawless key update mechanisms in controlled environments. The 50-node configuration showed a slight degradation to ≈ 0.95 after initialization but stabilizes at this high level, suggesting minor scalability limitations even in ideal conditions.

The Threshold mechanism, while theoretically sound, fails to adapt to the asynchronous nature of large-scale MANETs, where dynamic topology changes hinder node coordination.

The transition to realistic conditions (Figure 3(b)), however, reveals critical scalability limitations beyond 50 nodes. Initial key acquisition is successful in the first period. After that, *KF* drops significantly in the second period. It then stabilizes at approximately 20% for all larger network sizes: 75, 100, 125, and 150 nodes. Network congestion, caused by nearly simultaneous key renewal requests, explains this degradation, leading to packet collisions and transmission delays. The results indicate that approximately a set of 50 nodes represents a practical communication Threshold for the given area (1000 m × 1000 m) and radio range of 250 M, beyond which general network performance becomes severely degraded.

This pronounced performance degradation originates from the scheme's fundamental dependency on timely responses from multiple INITIAL nodes. Under realistic mobility patterns, increased network contention, and multi-hop communication delays, this requirement becomes statistically improbable.

These results are not implementation-specific but stem directly from the design assumptions of threshold-based key management, which presuppose bounded delays and coordinated participation among multiple authorities.

The observed collapse of *KF* under realistic conditions can be further explained by the inherent mismatch between the Threshold-based KMS's synchronous coordination requirement and the dynamic, asynchronous nature of MANETs. Each key renewal relies on receiving timely responses from multiple INITIAL nodes within a strict window. The probability of meeting this requirement decreases sharply as network size increases. Once the network exceeds a critical density, the joint probability of receiving the required number of responses within the timeout window collapses, leading to a sharp rather than gradual performance drop. Our measurements indicate that packet loss rates rise from approximately 5% in the basic scenario to 40% in the realistic scenario—an eightfold increase—while transmission delays frequently exceed the protocol's configured timeouts. This non-linear degradation, where each additional node disproportionately raises the risk of coordination failure, explains why *KF* stabilizes around 20% for networks larger than 50 nodes.

6.1.2 SCA evaluation

The SCA metric shows excellent performance in basic conditions (Figure 3(c)), rapidly increasing to values above 0.95 for all network sizes. The 25 and 35-node configurations achieve near-perfect connectivity (SCA ≈ 0.96%–0.97%), while the 50-node setup shows marginally lower but still high values (SCA ≈ 0.80%). This indicates that the threshold-based scheme effectively establishes secure pathways when network conditions are stable and predictable, validating its design

principles for small-scale deployments. Under realistic conditions (Figure 3(d)), SCA performance varies significantly across network sizes. While initial connectivity establishment occurs, the maintenance of secure links becomes challenging as the network size increases. The results show inconsistent patterns with frequent fluctuations, reflecting the scheme's struggle to sustain secure connections amidst node mobility and communication uncertainties. This behavior highlights the protocol's sensitivity to network dynamics—secure connections that are established may not persist due to KF issues or route breakdowns. These behaviors are not incidental but stem directly from the tight coupling between key management and routing stability inherent in threshold-based security schemes.

The instability observed in SCA under realistic conditions can be traced to a cascade of coordination failures inherent to the Threshold mechanism. Establishing a secure connection requires both fresh keys and stable routing paths. In the realistic scenario, high node mobility combined with reactive AODV routing causes frequent route breaks, often occurring faster than the Threshold protocol can complete its key renewal coordination. This temporal mismatch results in situations where keys are valid but routes are disrupted, or conversely, routes exist, but keys are outdated. In addition, the intense control traffic generated during key renewal phases—accounting for nearly 70% of total network traffic—saturates the network, significantly extending route discovery delays beyond the protocol's tolerances and further compromising secure connectivity.

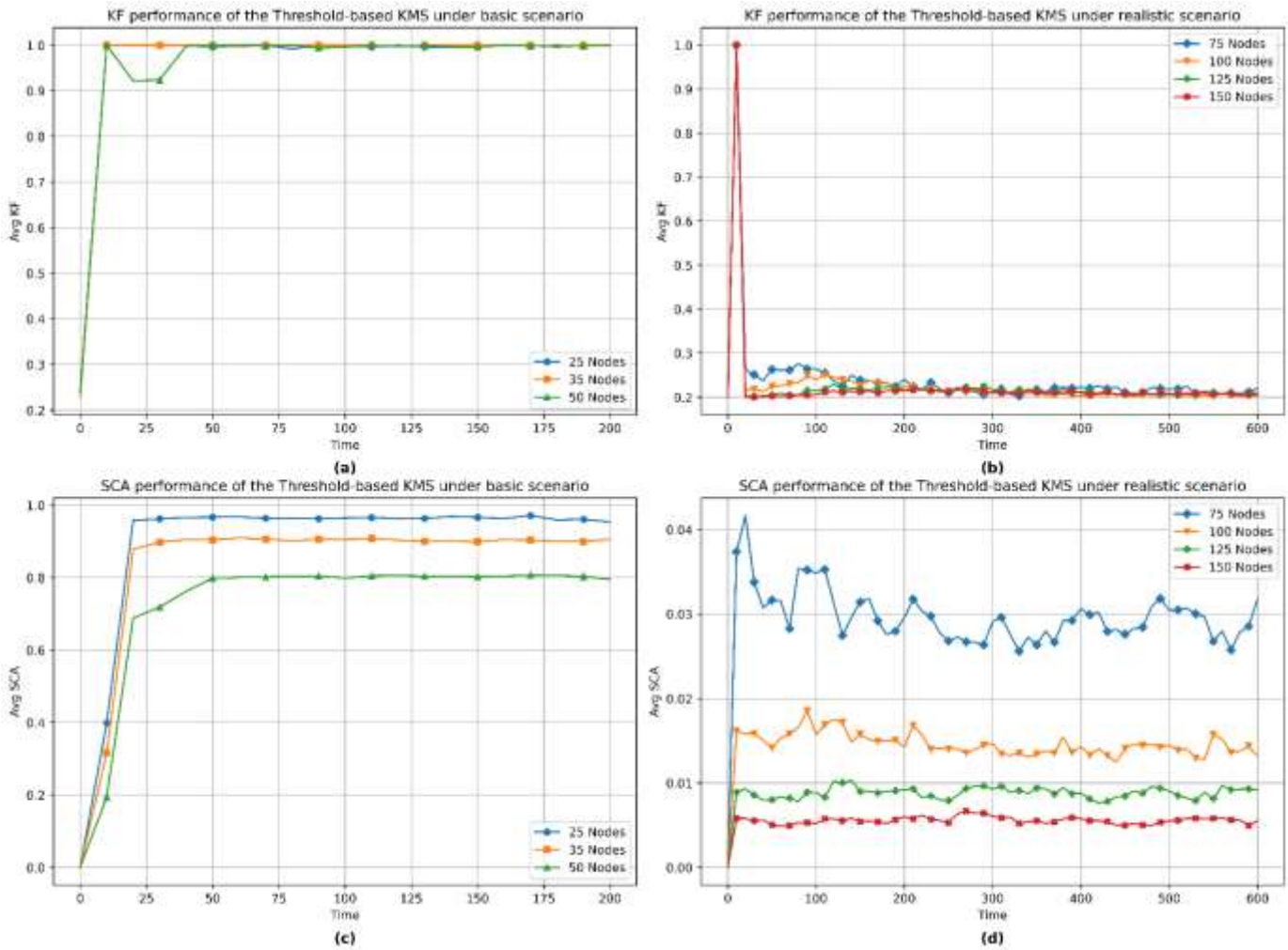

Figure 3. Comparative performance analysis of the threshold-based KMS for (a-b) KF and (c-d) SCA under basic conditions with 25, 35, and 50 nodes and realistic scenarios with 75, 100, 125, and 150 nodes

6.2 Performance assessment of the distributed identity-based scheme

This section presents the results of evaluating the Distributed Identity-based KMS with respect to two key performance metrics: KF and SCA. The evaluation was conducted under two distinct experimental settings: a basic scenario and a realistic scenario. The comprehensive results are summarized in Figure 4.

Figures 4(a) and (b) depict the KF performance for the basic and realistic scenarios, respectively. Figures 4(c) and (d) present the SCA results for the basic and realistic scenarios, respectively.

6.2.1 KF evaluation

The distributed scheme exhibited different KF characteristics (Figure 4(a)) compared to the Threshold approach. While achieving good overall performance, KF values show more variability during initial phases before stabilizing. This pattern reflects the scheme's decentralized nature, where key management responsibilities are distributed across all nodes rather than concentrated on specific originator

nodes. The absence of a single point of failure contributes to more resilient key maintenance, though at the cost of higher coordination overhead during establishment phases.

Remarkably, the distributed scheme demonstrates better scalability under realistic conditions (Figure 4(b)). KF values, while lower than in basic scenarios, maintain more stable levels (approximately 0.4–0.6 across different network sizes) compared to the threshold-based scheme's collapse. This resilience stems from the architecture's inherent fault tolerance—the failure of individual nodes has less impact on overall key management since responsibilities are shared across the network. This consistent performance is robust to variations in network parameters because it arises directly from the architectural principles of distributed key management, which favor local interactions, redundancy, and asynchronous operation. This robustness is further reinforced by its lightweight communication model: Unlike the threshold scheme, which generates a surge of control messages as network size grows, the distributed approach restricts each node's interactions to a limited set of local servers. This reduction in concurrent messaging minimizes collisions and MAC-layer delays. Moreover, its asynchronous operation enables nodes to maintain partial KF by relying on locally available servers, preventing the complete performance collapse seen in the Threshold scheme when critical nodes are temporarily unreachable.

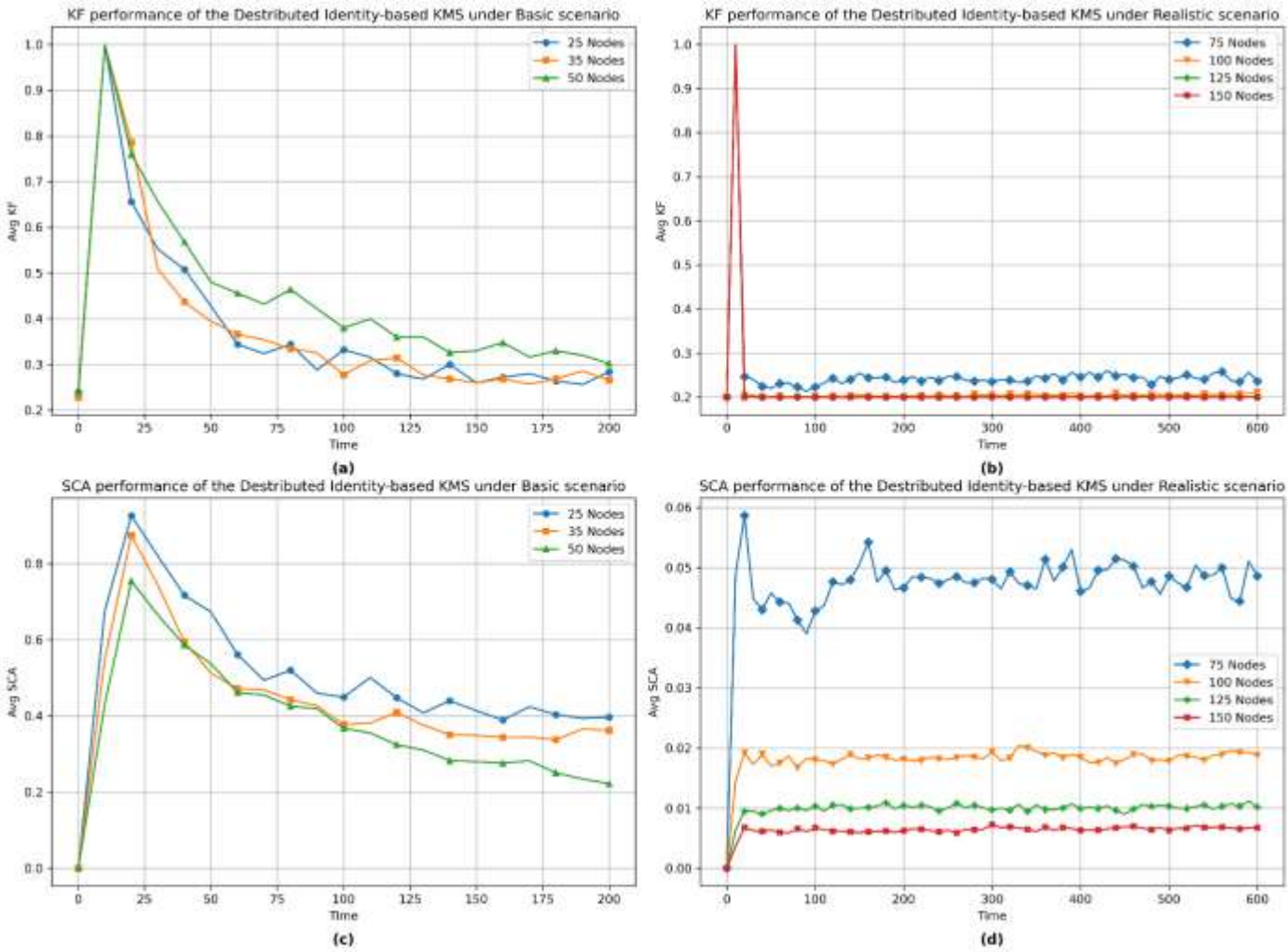

Figure 4. Comparative performance analysis of the distributed identity-based KMS for (a-b) KF and (c-d) SCA under basic conditions with 25, 35, and 50 nodes and realistic scenarios with 75, 100, 125, and 150 nodes

6.2.2 SCA evaluation

The distributed scheme achieved high SCA values (Figure 4(c)) comparable to the Threshold approach in basic conditions. However, the convergence to optimal values occurs more gradually, reflecting the additional coordination required in fully decentralized key establishment. Once stabilized, the scheme maintains consistent, secure connectivity, demonstrating its viability for small to medium-sized networks. Under realistic conditions (Figure 4(d)), the distributed scheme exhibits a significant decrease in absolute *SCA* performance (dropping to approximately 0.02–0.04) compared to the basic scenario. However, it demonstrates far more gradual decline in performance than the Threshold approach. Crucially, while SCA values are much lower, they remain stable over time and show no further degradation as the network scales from 75 to 150 nodes. The scheme's ability to maintain secure connectivity despite KF challenges highlights its robustness—even when individual keys may not be perfectly fresh, the distributed nature of key management allows alternative pathways to be established, preserving overall network security functionality. This resilience originates from the scheme's decentralized and redundant architecture, where node failures have localized rather than network-wide impact. Consequently, SCA degrades gracefully—a direct outcome of its design emphasis on redundancy and local decision-making. As a result, a client

node retains a high probability of finding at least one valid local server to establish a secure connection. This intrinsic robustness through architectural diversity explains why overall secure connectivity remains functional even under high mobility and increased packet loss conditions.

6.3 Comparison of distributed identity-based and threshold-based KMS using KF and SCA metrics

As illustrated in Figure 5, the threshold-based KMS demonstrates superior KF and SCA in basic scenarios, particularly for smaller network sizes (25–50 nodes). Its centralized coordination mechanism proves highly effective under stable conditions with minimal mobility and contention. However, this performance advantage reverses completely under realistic conditions, where the scheme exhibits severe degradation, with KF collapsing to 0.2–0.3 and SCA becoming inconsistent for larger network sizes (75–150 nodes).

Conversely, the distributed identity-based scheme shows more balanced performance across both scenarios. While slightly less efficient in basic conditions, it demonstrates remarkable resilience in realistic environments, maintaining functional *KF* levels (0.4–0.6) and stable *SCA* despite increased network dynamics. The comparison of performance between the two schemes highlights a crucial insight: a KMS that performs optimally in controlled settings may prove inadequate in practical deployments, and vice versa. This performance reversal is a direct manifestation of a fundamental design divergence. The threshold-based KMS is engineered for an idealized environment—synchronous, low contention, and predictable—where its centralized coordination operates efficiently. In the real-world context of MANETs, characterized by variable delays, high network contention, and dynamic topology, this same coordination becomes a critical point of failure. In contrast, the distributed scheme is designed to be delay-tolerant and locally fault-resilient, trading minor efficiency under calm conditions for significantly greater robustness under dynamic and unpredictable scenarios. This analysis confirms that KMS effectiveness is strongly context-dependent, reinforcing the need for evaluation under both basic and realistic network conditions.

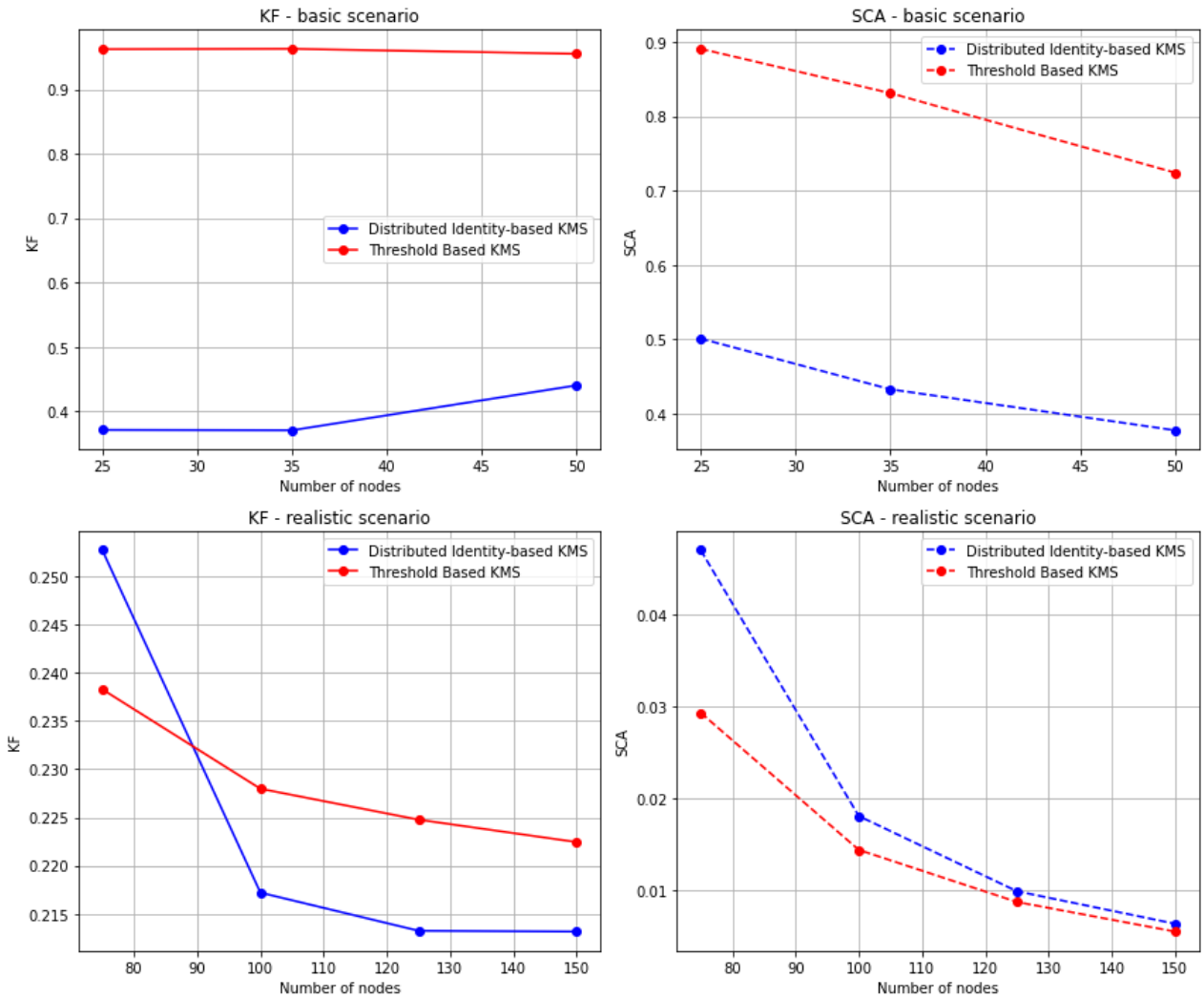

Figure 5. Comparative performance evaluation of distributed identity-based and threshold-based KMS under basic and realistic scenarios

Although the present study focuses on simulation-based performance metrics, the observed results are consistent with the theoretical cost models of the evaluated KMS. In particular, the severe degradation of the threshold-based KMS under realistic conditions aligns with its theoretical reliance on synchronized responses from multiple authorities, as described in reference [12], which implies increasing communication and coordination costs with network scale.

Conversely, the distributed identity-based scheme exhibits behavior consistent with its theoretical design assumptions, favoring local operations and reduced coordination overhead. A formal quantitative comparison between analytical complexity models and empirical metrics such as latency and message overhead are identified as an important extension of this work.

The comprehensive evaluation of both KMSs reveals a critical finding: KMS performance is inherently context-dependent, varying significantly between basic and realistic scenarios. This fundamental observation validates the core premise of our study—that evaluation under diverse conditions is essential for meaningful scheme assessment.

7. CONCLUSIONS

This study introduced a flexible and extensible simulation-based framework for the evaluation of KMS in WANETs. By applying the framework to two representative schemes—a threshold-based KMS and a distributed identity-based KMS—we demonstrated that their performance varies substantially across different simulation conditions. Specifically, while one scheme may appear effective under simplified settings, its performance may degrade significantly in more realistic environments, and vice versa. These findings confirm that evaluation outcomes are highly dependent on contextual parameters such as network size, mobility, and communication conditions.

The analysis yields three principal findings. First, no single KMS can be considered universally optimal across all deployment scenarios. Second, static and narrowly defined evaluation settings are insufficient to capture the complex dynamics of real-world environments. Third, there is a pressing need for a generic and customizable evaluation framework that allows users to configure scenarios according to their operational requirements. Such a framework not only enables fairer comparisons between schemes but also empowers researchers and practitioners to select the most appropriate KMS depending on trade-offs between security, efficiency, and scalability.

Table 4. Decision matrix for MANET KMS selection

Feature	Threshold-Based KMS	Distributed Identity-Based KMS
Best network size	Small (≤ 50 nodes)	Medium to large (> 50 nodes)
Mobility tolerance	Low (Requires stable routes)	High (Delay-tolerant)
Security priority	High control (Centralized trust)	High availability (Fault-tolerant)
Overhead type	Burst traffic (Congestion-prone)	Constant background traffic

This work provides a customizable and adversary-aware testbed. Thus, it contributes to bridging a critical gap in the literature. It also offers a foundation for building more robust, scalable, and context-aware key management solutions for wireless Ad Hoc systems.

The comparative analysis conducted through the proposed evaluation framework underscores its unique capability to capture context-dependent performance variations that are often overlooked in conventional evaluations. For instance, the threshold-based KMS performed optimally only under basic conditions, while the distributed identity-based approach demonstrated superior resilience in dynamic environments, albeit with higher initial overhead. These insights would not have been apparent without the flexible evaluation environment proposed in this study. Thus, the proposed evaluation framework not only facilitates a more truthful assessment of KMS suitability but also empowers stakeholders to make informed decisions tailored to specific operational contexts.

To further support practitioners, we provide actionable guidance by means of a decision matrix that consolidates the main results of this study. Table 4 summarizes the decision Matrix for MANET security evaluation and selection.

While the proposed simulation-based framework provides a flexible and extensible environment for evaluating KMS in WANETs, several limitations must be highlighted:

• Limited KMS categories: The current experimental evaluation covers only two representative KMS Categories: A threshold-based KMS and a distributed identity-based scheme. Consequently, the generalizability of findings to other KMS types remains to be validated.

• Simplified realistic scenario: Although the "realistic" scenario incorporates larger network sizes, heterogeneous mobility models, and extended simulation durations, it still relies on simplified representations of node mobility, traffic patterns, and wireless propagation. In addition, the current experimental setup does not yet explicitly model compromised or malicious nodes, and therefore does not evaluate KMS behavior under active adversarial presence. As such, results may not capture all nuances of real-world deployments.

• Partial metric coverage: The current study focuses primarily on KF and SCA. While the framework architecture supports comprehensive metrics (energy, latency, etc.), this specific case study prioritized KF and SCA to isolate the impact of mobility on security availability. Expanding metric coverage will provide a more comprehensive assessment of KMS performance.

• Framework computational overhead and scalability: The present study does not explicitly profile to ensure its feasibility for large-scale evaluations. Beyond MANETs, the framework shows strong potential for adaptation to related wireless domains: for VANETs, integration with realistic mobility models and latency-critical metrics; for FANETs, energy-aware evaluation under strict power constraints; and for IoT, support for lightweight protocols and massive heterogeneous deployments. Finally, we envision the integration of machine learning techniques for adaptive parameter tuning, enabling the framework to not only evaluate but also predict KMS behavior under evolving network conditions.

These limitations naturally point to several promising avenues for future work. First, the framework will be extended to incorporate additional KMS categories—such as pre-distribution, blockchain-based, and post-quantum schemes—to validate its generality beyond the two paradigms studied here. Second, to address the simplified realism of current scenarios, future iterations will integrate explicit adversarial models—including Sybil attacks, denial-of-service, and insider threats—alongside more refined mobility, traffic, and propagation patterns. Third, metric coverage will be expanded to include energy efficiency, latency under congestion, robustness against specific attacks, and quality-of-service impact, providing a more holistic assessment of KMS performance. Furthermore, the computational overhead and scalability of the framework itself will be systematically

profiled to ensure its feasibility for large-scale evaluations. Beyond MANETs, the framework shows strong potential for adaptation to related wireless domains: for VANETs, integration with realistic mobility models (e.g., via SUMO) and latency-critical metrics; for FANETs, energy-aware evaluation under strict power constraints; and for IoT, support for lightweight protocols and massive heterogeneous deployments. Finally, we envision the integration of machine learning techniques for adaptive parameter tuning, enabling the framework to not only evaluate but also predict KMS behavior under evolving network conditions.

FUNDING

This work is fully funded by the General Direction of Scientific Research and Technological Development (DGRSDT) of the Algerian Ministry of Higher Education and Scientific Research (MERS) (https://dgrsdt.dz/en).

REFERENCES

[1] Salehi Shahraki, A., Lauer, H., Grobler, M., Sakzad, A., Rudolph, C. (2023). Access control, key management, and trust for emerging wireless body area networks. Sensors, 23(24): 9856. https://doi.org/10.3390/s23249856

[2] Conti, M., Giordano, S. (2014). Mobile Ad Hoc networking: Milestones, challenges, and new research directions. IEEE Communications Magazine, 52(1): 85-96. https://doi.org/10.1109/MCOM.2014.6710069

[3] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E. (2002). SPINS: Security protocols for sensor networks. Wireless Networks, 8: 521-534. https://doi.org/10.1023/A:1016598314198

[4] Mansour, I., Chalhoub, G., Lafourcade, P. (2015). Key management in wireless sensor networks. Journal of Sensor and Actuator Networks, 4(3): 251-273. https://doi.org/10.3390/jsan4030251

[5] Pan, J., Cai, L., Shen, X.S. (2007). Promoting identity-based key management in wireless Ad Hoc networks. In Wireless Network Security, pp. 83-102. https://doi.org/10.1007/978-0-387-33112-6_4

[6] Mohammad, A.A.K., Verma, P., Batta, K.B., Bankapalli, J., Nizamuddin, M.K., Abdul, A.M. (2025). Mitigating malicious and unintentional packet drops in mobile Ad Hoc networks. International Journal of Safety & Security Engineering, 15(5): 1035-1048. https://doi.org/10.18280/ijsse.150517

[7] Zhou, L., Haas, Z.J. (1999). Securing Ad Hoc networks. IEEE Network, 13(6): 24-30. https://doi.org/10.1109/65.806983

[8] Huang, D., Misra, S., Verma, M., Xue, G. (2011). PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs. IEEE Transactions on Intelligent Transportation Systems, 12(3): 736-746. https://doi.org/10.1109/TITS.2011.2156790

[9] Raya, M., Hubaux, J.P. (2005). The security of vehicular Ad Hoc networks. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, USA, pp. 11-21. https://doi.org/10.1145/1102219.1102223

[10] Du, W., Deng, J., Han, Y.S., Varshney, P.K., Katz, J., Khalili, A. (2005). A pairwise key predistribution scheme for wireless sensor networks. ACM Transactions on Information and System Security, 8(2): 228-258. https://doi.org/10.1145/948109.948118

[11] Xue, X., Liu, S. (2018). Matching sensor ontologies through compact evolutionary tabu search algorithm. In International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, Melbourne, NSW, Australia, pp. 115-124. https://doi.org/10.1007/978-3-030-05345-1_9

[12] Deng, H., Agrawal, D.P. (2004). TIDS: Threshold and identity-based security scheme for wireless Ad Hoc networks. Ad Hoc Networks, 2(3): 291-307. https://doi.org/10.1016/j.adhoc.2004.03.005

[13] Deng, H., Mukherjee, A., Agrawal, D.P. (2004). Threshold and identity-based key management and authentication for wireless Ad Hoc networks. In International Conference on Information Technology: Coding and Computing, Las Vegas, NV, USA, pp. 107-111. https://doi.org/10.1109/ITCC.2004.1286434

[14] Lv, X., Li, H., Wang, B. (2011). Identity-based key distribution for mobile Ad Hoc networks. Frontiers of Computer Science in China, 5(4): 442-447. https://doi.org/10.1007/s11704-011-0197-5

[15] Abdallah, A.A., Abdallah, M.S., Aslan, H., Abdallah, M.A.A., Cho, Y.I., Abdallah, M.S. (2024). Enhancing mobile Ad Hoc network security: An anomaly detection approach using support vector machine for black-hole attack detection. International Journal of Safety & Security Engineering, 14(4): 1015-1028. https://doi.org/10.18280/ijsse.140401

[16] Msolli, A., Ajmi, N., Helali, A., Gassoumi, A., Maaref, H., Mghaieth, R. (2023). New key management scheme based on pool-hash for WSN and IoT. Journal of Information Security and Applications, 73: 103415. https://doi.org/10.1016/j.jisa.2022.103415

[17] Nafi, M., Bouzefrane, S., Omar, M. (2020). Matrix-based key management scheme for IoT networks. Ad Hoc Networks, 97: 102003. https://doi.org/10.1016/j.adhoc.2019.102003

[18] Yuan, E., Wang, L., Cheng, S., Ao, N., Guo, Q. (2020). A key management scheme based on pairing-free identity based digital signature algorithm for heterogeneous wireless sensor networks. Sensors, 20(6): 1543. https://doi.org/10.3390/s20061543

[19] Zhang, J., Liu, Q. (2023). New key management scheme lattice-based for clustered wireless sensor networks. PLOS One, 18(8): e0290323. https://doi.org/10.1371/journal.pone.0290323

[20] Sadi, M., Amad, M., Badache, N. (2020). Improving performance overhead of a trust-clustering key management protocol in Ad Hoc networks. International Journal of Electronic Security and Digital Forensics, 12(2): 214-228. https://doi.org/10.1504/IJESDF.2020.106319

[21] Janani, V.S., Manikandan, M.S.K. (2015). Genetic-IDGKA: Genetic ID-based group key agreement protocol for large MANETs. Journal of Discrete Mathematical Sciences and Cryptography, 18(3): 313-333. https://doi.org/10.1080/09720529.2015.1023535

[22] Sowmyadevi, D., Shanmugapriya, I. (2023). Unsupervised machine learning based key management in wireless sensor networks. Measurement: Sensors, 28:

100847. https://doi.org/10.1016/j.measen.2023.100847
[23] Naresh, V.S., Allavarpu, V.D., Reddi, S., Murty, P.S.R., Raju, N.L., Mohan, R.J. (2022). A provably secure sharding based blockchain smart contract centric hierarchical group key agreement for large wireless ad-hoc networks. Concurrency and Computation: Practice and Experience, 34(3): e6553. https://doi.org/10.1002/cpe.6553
[24] Jain, K., Singh, A. (2024). IHKM: An improved hierarchical key management scheme for wireless sensor network. Telecommunication Systems, 87(1): 151-166. https://doi.org/10.1007/s11235-024-01182-x
[25] Jurnečka, F., Stehlík, M., Matyáš, V. (2014). Evaluation of key management schemes in wireless sensor networks. In International Workshop on Security and Trust Management, Wroclaw, Poland, pp. 198-203. https://doi.org/10.1007/978-3-319-11851-2_16
[26] Al-Haija, Q.A., Shwehdi, M.H., Banat, M. (2013). Evaluation metrics for wireless sensor network security: algorithms review and software tool. Journal of Computer Science, 9(5): 635-645. https://doi.org/10.3844/jcssp.2013.635.645
[27] Roman, R., Lopez, J., Alcaraz, C., Chen, H.H. (2011). SenseKey—Simplifying the selection of key management schemes for sensor networks. In 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications, Biopolis, Singapore, pp. 789-794. https://doi.org/10.1109/WAINA.2011.78
[28] Ragab-Hassen, H., Lounes, E. (2017). A key management scheme evaluation using Markov processes. International Journal of Information Security, 16(3): 271-280. https://doi.org/10.1007/s10207-016-0323-3
[29] Ruan, N., Ren, Y., Hori, Y., Sakurai, K. (2011). Performance analysis of key management schemes in wireless sensor network using analytic hierarchy process. In 2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, China, pp. 1739-1744. https://doi.org/10.1109/TrustCom.2011.243
[30] Na, R., Ren, Y., Hori, Y., Sakurai, K. (2011). A generic evaluation method for key management schemes in wireless sensor network. In Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication, Seoul Korea, pp. 1-9. https://doi.org/10.1145/1968613.1968680
[31] Kazienko, J.F., Albuquerque, C.V.N. (2010). Authentication, Key Distribution and Secure Storage in Wireless Sensor Networks. In Proceedings of the XXXVI Latin American Computing Conference (CLEI 2010), Asunción, Paraguay, pp. 1-14. (In Portuguese). https://clei.org/proceedings_data/CLEI2010/CLEI2010/03_Seguridad/1.2.7_83CLEIJuliano_Paper.pdf.
[32] Kazienko, J.F., Ribeiro, I.G., Moraes, I.M., Albuquerque, C.V. (2011). Practical evaluation of a secure key-distribution and storage scheme for wireless sensor networks using TinyOS. CLEI Electronic Journal, 14(1): 8. https://doi.org/10.19153/cleiej.14.1.8
[33] Prantl, T., Ten, P., Iffländer, L., Dmitrenko, A., Kounev, S., Krupitzer, C. (2020). Evaluating the performance of a state-of-the-art group-oriented encryption scheme for dynamic groups in an IoT scenario. In Proceedings of the 2020 28th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Nice, France, pp. 1-8. https://doi.org/10.1109/MASCOTS50786.2020.9285948
[34] Kurkowski, S., Camp, T., Colagrosso, M. (2005). MANET simulation studies: The incredibles. ACM SIGMOBILE Mobile Computing and Communications Review, 9(4): 50-61. https://doi.org/10.1145/1096166.1096174

NOMENCLATURE

WANETs	Wireless Ad Hoc Networks
MANETs	Mobile Ad Hoc Networks
VANETs	Vehicular Ad Hoc Networks
WSNs	Wireless Sensor Networks
FANETs	Flying Ad Hoc Networks
KMS	Key Management Scheme
TIDS	Threshold and Identity-Based Security Scheme
OMNeT++	Discrete Event Simulator for Communication Networks
KF	Key Freshness
SCA	Secure Connectivity Achievement
CBR	Constant Bit Rate
MAC	Medium Access Control
VPKG	Virtual Private Key Generator (Server)
CO	Communication Overhead
PC	Power Consumption
RNCA	Resilience Against Node Capture
PM	Performance Metric
CS	Composite Scalability
MSK	Master Secret Key
MPK	Master Public Key