Proceedings of the 2025 International Conference on Intelligent Computing, Information and Control Systems (ICOIICS-2025)
DVD Part Number: CFP250Z3-DVD; ISBN: 979-8-3315-9896-9

Dynamic Mimic-based Moving Target Defense Mechanisms for Enhancing Security and Resilience in Mobile Ad Hoc Networks

Dr. Gopinath D
Assistant Professor,
Department of Computer Science,
School of Computational and Physical Sciences,
Kristu Jayanti (Demmed to be University),
Bengaluru, Karnataka, India.
kascgopinath@gmail.com

Balamurugan M
Associate Professor
Department of MCA
Acharya Institute of Graduate Studies
Bengaluru, Karnataka, India.
balamurugan2833@acharya.ac.in

Dr. Margaret Mary T
Assistant Professor
Department of Computer Science
Kristu Jayanti (Deemed to be University)
Bengaluru, Karnataka, India
margaret@kristujayanti.com

Dr. A. Kanagaraj
Associate Professor,
Department of Computer Science,
School of Computational and Physical Sciences,
Kristu Jayanti (Demmed to be University),
Bengaluru, Karnataka, India.
a.kanagaraj@gmail.com

Dr.S.Sharmila
Assistant Professor
Department of Computer Science
NGM College
Pollachi, Tamil Nadu, India
mcasharmi2007@gmail.com

***Abstract*—Mobile Ad Hoc Networks (MANETs) become increasingly essential for applications requiring flexible, infrastructure-free communication, like military missions, disaster relief, and IoT installations. They are vulnerable to a wide variety of security threats, including routing attacks, node impersonation, and eavesdropping, due to their dynamic topology, decentralized nature, and limited resources. Current security paradigms tend to find it difficult to cope with the dynamic and unpredictable nature of MANETs, presenting a large research gap in designing viable proactive defense approaches suitable for such networks. This research focuses on filling the above gap through designing a new security framework that incorporates mimic defense and moving target defense (MTD) approaches to make MANETs more resilient. Precisely, the goal is to provide dynamic changes—such as routing heterogeneity, node identification randomization, and resource distribution diversification—that repeatedly reshape the attack surface of the network, making it more complex for any possible adversaries and less impactful from attacks. Toward this aim, we introduced attack modeling and attack chain analysis specifically for MANET settings in order to simulate various types of attacks and measure the proposed framework's robustness. Dynamic security measures were deployed in a simulation setting, and performance indicators like attack success rate, network throughput, and latency were quantified. The outcomes indicated that the proposed methods significantly lowered the success rate of typical attacks, such as black hole and Sybil attacks, while keeping network performance at acceptable levels. In addition, the simulations indicated enhancements in overall network resilience and responsiveness in adversarial settings. These results suggest that the use of mimicry and MTD strategies in MANETs represents a promising direction for the design of proactive, adaptive security systems. This work adds to the general task of securing infrastructure-less networks and is of significant import to their deployment in critical sectors where secure, fault-tolerant communication is critical.**

Keywords—Mobile Ad Hoc Networks (MANETs), Moving Target Defense (MTD), Mimic Defense, Network Security, Dynamic Topology, Attack Surface Diversification, Adaptive Security Solutions

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have emerged as a key technology for facilitating dynamic, infrastructures-free communication within dynamic and resource-limited environments. MANETs are composed of mobile nodes that autonomously establish temporary networks independent of any fixed infrastructure, and therefore they are very suitable for military operations, disaster relief, remote sensing, and Internet of Things (IoT) applications. The dynamic nature, decentralized administration, and resource constraints of MANETs, while providing several advantages, also present significant security risks. Unfriendly users may use these attributes to initiate various types of attacks like routing attacks, node impersonation, eavesdropping and denial of service.

Literature review has discussed some security mechanisms for MANETs like cryptographic algorithms, intrusion detection, and trust management. Yet, these conventional methods commonly rely on relatively stable network infrastructure and static identities, being less suited for extremely dynamic MANET contexts. Further, most existing solutions concentrate on reactive countermeasures—detection and reaction after an attack has taken place—instead of inherently reducing the attack surface proactively. Consequently, there exists an urgent need to enhance adaptive, proactive security models capable of weathering the changing face of attacks in MANETs.

This study is prompted by the desire to develop security mechanisms that respond not only to threats but also anticipate and prevent attack opportunities through a dynamic and continuous transformation of the network structure and behavior. Moving Target Defense (MTD) and mimic defense, with success in other contexts, have good potential if translated to MANETs. Through the introduction of variability and unpredictability within network operations, such techniques can make it harder for the adversary to make decisions and lower the possibility of attack success.

The main aim of this research is to suggest and analyze a new security framework for MANETs which combines mimic defense and MTD techniques. In particular, the study aims to provide answers to the following key issues:

- The implementation of dynamic strategies which includes routing flexibility alongside node identity randomization and resource diversification plays a vital part in improving security measures for MANETs
- Research shows that mimicry techniques together with Moving Target Defense (MTD) approaches provide effective solutions for lowering the success rate of common attacks targeting MANETs.
- The deployed defense mechanisms directly affect both the network performance and its ability to withstand attacks

The importance of this work is that it contributes to the development of proactive and adaptive security solutions for MANETs. Through the creation of methods that constantly change the network's attack surface, the research hopes to make MANETs stronger against advanced and ever-changing threats. The results have far-reaching implications in critical applications where dependable and secure communication is a must, such as military operations, emergency response systems and industrial IoT installations.

For such aims, this study formulates customized attack models and performs attack chain analysis based on MANET settings. It executes simulations in deploying dynamic security features and its implications in relation to different kinds of attacks. The performance level as measured in attack success ratio, network throughputs, and latency is measured in determining trade-offs between operations efficiency and security.

A. Research Gap and Motivation

Even though a great deal of existing research focuses on security for MANETs, much of it relies on reactive or static approaches (i.e., cryptographic, authentication, IDSs, or trust-based routing). Most approaches to network security consider threats only AFTER they happen and are not capable of modularly changing to keep up with the unique, rapid topological changes and behaviors regarding MANET nodes. Moreover, most approaches to security are based on a predictable attack model and do not contemplate more complex, evolving threats such as coordinated or mimic attacks. Although a small number of existing studies take proactive approaches such as Moving Target Defense, the studies often focus on limited aspects of MTD (e.g., IP shuffling or route randomization) and do not consider behavioral mimicry or transformation to adapt. Thus, we have identified an opportunity for research that investigates a complete, dynamic, and adaptive defense mechanism that continuously changes the attack surface of the network. Addressing this gap in research is necessary to improve the resilience, adaptability, and survivability of MANETs in highly adversarial, constrained-resource environments.

B. Novelty, Significance, and Core Contribution

This study presents an innovative contribution to the integration of Mimic Defense (MD) and Moving Target Defense (MTD) strategies within Mobile Ad Hoc Networks (MANETs), a field that has not received much attention in research. Traditional security mechanisms are prohibitively static or reactive mechanisms. The security framework proposed engenders a dynamic and adaptive defense model that regularly changes a variety of parameters inherent in the operation of the MANET system, such as routing paths, node identities, and resources, to deceive adversaries and limit the predictability of attacks. This dynamic operational security model allows a traditionally static MANET architecture to evolve into a system resistant to cyber adversaries. The primary contribution of this study is the construction and thorough validation of a security framework that is capable of continuously reducing the attack success rate by a factor of greater than 80% while minimizing throughput and latency levels to acceptable ranges. Specifically, we demonstrate how mimicry and dynamic reconfiguration can enhance cyber resilience. The application and validation of a meaningful cure towards more modern, intelligent, self-adaptive, and mission-critical security for MANETs that would be of interest for military approaches, disaster relief and communication in IoT.

II. LITERATURE REVIEW

Mobile Ad Hoc Networks (MANETs) are decentralized, dynamic, wireless networks with no pre-established infrastructure, making them extremely vulnerable to a multitude of security risks. This chapter critically analyzes past research on MANET security, formulates the theoretical framework, determines research gaps, and reasons why the research approach used in this study.

C. Critical Analysis of Previous Research

Current research focuses on the fact that MANETs have particular security issues arising from their open wireless medium, their dynamic nature of topology, and absence of a centralized authority [1]. Most common attacks comprise black hole attacks, wormhole attacks, Sybil attacks, and eavesdropping. Cryptographic mechanisms, i.e., public key infrastructure (PKI), are suggested for making MANETs secure but proved to be impractical given their resource limits and dynamic nature of membership in the nodes [2].

Shoukat et al. (2021) also performed a comprehensive survey elucidating the weakness of conventional reputation-based and trust-based systems within dynamic MANET scenarios [3]. Other studies, e.g., Boukerche et al. (2019), advocated for lightweight intrusion detection systems (IDS), yet their dependence on pre-defined signatures decreases efficacy towards new or emergent threats [4].

To counter routing attacks, secure routing protocols such as Ariadne and SEAD have been proposed [5][6]. These protocols consider comparatively stable topologies and don't perform well under high mobility conditions of the nodes.

Moving Target Defense (MTD) techniques, conventionally used in cloud computing and critical infrastructure [7], provide a dynamic security mechanism. In MANETs, there are few MTD-based researches. Wang et al. (2022) investigated IP address randomization in wireless networks but reported high communication overhead [8].

Mimic defense methods have been extensively researched in other areas [9], but their usage in MANETs is relatively unexplored. Zhang et al. (2020) proved that variability in dynamic systems can significantly decrease the attack success rate in cyber-physical systems [10].

B. Theoretical Framework

This research's theoretical framework is based on the principles of dynamic defense — namely Moving Target Defense and Mimic Defense — that seek to elevate the cost and complexity for attackers by dynamically changing system properties [11].

MTD includes making regular adjustments to network parameters (e.g., routing paths, node identities, and frequencies) to render an adversary's knowledge obsolete [12].

Mimic Defense adds variability in system behavior, which makes it hard for attackers to detect and take advantage of vulnerabilities [13].

In MANET environments, the application of these principles can theoretically reduce the window of opportunity for successful attacks by rendering the network an ever-changing target.

C. Research Gap Identification

Despite significant advancement, there are some gaps that exist:

- The majority of current MANET security solutions are reactive or static, not being able to predict the actions of an adversary [4][6].
- Research that incorporates MTD and mimic defense in MANETs is limited [8][9].
- There is little research in assessing trade-offs between security improvement and network performance degradation when dynamic defenses are implemented [14].
- Attack chain modeling tailored to MANETs under dynamic defense has not been thoroughly developed [15].

D. Rationale for Adopted Method

To bridge these gaps, this study suggests an integrated solution through the merging of MTD and mimic defense techniques. Through the use of dynamic routing variability, node identity randomization, and resource allocation diversification, the network continually changes its attack surface, greatly making it difficult for attackers [11][12].

This method is justified because:

- It actively maximizes attacker uncertainty, minimizing the probability of success [9][10].
- It is in accordance with successful techniques employed in the protection of cyber-physical and IoT systems [7][13].
- Preliminary works indicate that dynamic variability impacts positively on system resilience without considerable performance penalties, provided they are properly tuned [8][14].

As such, embracing MTD and mimic defense measures presents a new, proactive avenue towards securing MANETs against a wide variety of evolving threats. Following in the critical evaluation, Sanzgiri et al. (2002) introduced a secure routing protocol for MANETs by the name ARAN using cryptographic certification [16]. While efficient against particular attacks such as spoofing and tampering with messages, ARAN takes into consideration the existence of a centralized certificate authority, which is in conflict with MANETs' decentralized environment. It is hence its limited applicability in completely autonomous situations.

Wang et al. (2020) offered a thorough overview of moving target defense strategy and how it can resist advanced cyberattacks [17]. Their results show that although MTD adds unpredictability to system behavior, not many studies cover the trade-off between adding uncertainty to attackers and preserving system usability and performance. This is further compounded in resource-constrained MANETs. Rawat et al. (2015) characterized the security challenges of MANETs, presenting prime vulnerabilities of dynamic topology handling, absence of centralized monitoring, and limited energy resources [18]. They clarified that adaptive lightweight security solutions would be required in order to serve the mobility constraints as well as the energy resources of MANET nodes. Still, their efforts mainly proposed advancements over traditional cryptography and trust mechanisms and not groundbreaking defense strategies like MTD or mimic defense.

Singh et al. (2018) enumerated a broad spectrum of security threats and classified attacks on the basis of their effect on various protocol layers [19]. They emphasized cross-layer security paradigms that adapt dynamically to real-time network dynamics. But their solutions draw heavily on static security policies, which are not effective against quickly changing multi-stage attack chains. Lastly, Zhang et al. (2003) presented essential issues and available solutions in securing MANETs, establishing an initial grasp of the issues raised by infrastructureless and changing network topologies [20]. Seminal though it is, this paper was done prior to a lot of the recent work in adaptive security models and does not include the novel strategies of moving target and mimic defenses.

III. Research Methodology: Enhancing MANET Security through Dynamic Defense Strategies

In this research work, we aimed to create an adaptive and robust security model for Mobile Ad Hoc Networks (MANETs) by fusing Moving Target Defense (MTD) and Mimic Defense (MD) techniques. For the verification of the proposed technique, a systematic methodology including attack modeling, adaptive defense deployment, simulation configuration, performance analysis and comparative evaluation was developed.

A. Attack Modeling and Threat Surface Analysis

In the initial part of the study, an exhaustive MANET-specific attack surface model was carefully developed. With the inherent dynamic and decentralized nature of MANETs, the attack surface is unstable and multi-faceted. Weaknesses primarily occur in routing mechanisms, node identity management and resource allocation protocols.

The attack surface at any given time was designed as:

$A_t = \{(p_i, v_i)\}$ where $p_i \in$ Parameter, $v_i \in$ Parameter Values

Where A_t refers to particular attack vectors like routing tables, node identities, transmission timing and authentication tokens, whereas represents the corresponding current state or value.

The threat surface was examined on three main axes:

Routing Layer Vulnerabilities: Attacks like route forgery, routing loops, and next-hop intercept.

Identity Layer Vulnerabilities: Threats due to identity theft, impersonation, and Sybil attacks.

Resource Layer Vulnerabilities: Bandwidth hijacking, resource starvation, and denial of service (DoS).

Attack Chain Construction:

To mimic realistic adversarial tactics, attack chains were created, tracing a series of exploit steps to breach the MANET. Some major modeled attacks are:

Black Hole Attack: An attacking node promotes an optimal path to the destination, sniffs packets and discards them. Steps of attack progression from route advertisement to data sniffing were simulated.

Sybil Attack: One node creates several identities to influence routing choices and saturate trust mechanisms. Chains of attacks involved identity generation, trust infiltration and routing disruption.

Wormhole Attack: Two hostile nodes establish a low-latency connection (tunnel) to bypass the routing protocol, resulting in incorrect topology perception.

Attack graphs were conceived, where states are used to denote network configurations and edges to represent attacker actions. State transition probabilities were tuned according to known attack success rates in MANET settings.

Additionally, every simulated attack was associated with its impact vectors along availability, integrity and confidentiality axes. This formal threat modeling allowed for accurate assessment of the dynamic defenses under different adversarial scenarios.

B. Dynamic Defense Framework Design

Moving Target Defense brings in unpredictability by dynamically changing system configurations and network parameters. The constant evolution of the attack surface renders it very difficult for attackers to perform successful reconnaissance, exploit vulnerabilities or mount persistent attacks.

Key Mechanisms:

- Dynamic Route Switching: Periodically changes routing tables and chosen communication paths.
- Node Identity Randomization: Randomizes MAC and IP addresses at periodic intervals.
- Resource Allocation Diversification: Continuously adjusts bandwidth assignments and channel utilization to break attack habits.

Mathematical Formulation: The transformation recasts the system state from A_t to A_t+1:

$$\mathbf{A_{t+1} = \sigma'(A_t) = \{(\, p_i', v_i')\}}$$

where p_i and v_i are transformed parameters and values produced by the defense mechanisms.

Moving Target Defense Workflow

graph TD
A[Start Defense Cycle] --> B[Randomize Node Identifiers (MAC/IP)]
B --> C[Apply Dynamic Route Switching]
C --> D[Diversify Resource Allocations (Bandwidth, Channel)]
D --> E[Validate and Update New Network State]
E --> F{Defense Cycle Complete?}
F -- Yes --> A
F -- No --> G[Wait Until Next Scheduled Cycle]
G --> A

C. Mimic Defense (MD)

Concept: Mimic Defense strengthens security with dynamic heterogeneity by running many heterogeneous software/hardware modules concurrently. This redundancy does not allow the attacker to count on uniform system behavior.

Key Mechanisms:

Tri-variant Routing Protocol Execution: Runs diverse routing algorithms (e.g., AODV, DSR, OLSR) concurrently.

Voting Mechanism: Concatenates decisions of all variants in order to pick the most reliable action.

Mathematical Representation: The voting system decides the majority choice of several alternatives:

$$V(R) = \text{argmax} \sum_{i=1}^{m} I\,(r_i = r)$$

where $R = \{r_1, r_2, \ldots\ldots, r_n\}$ represents decisions from heterogeneous modules, and is the indicator function.

Mimic Defense Workflow

graph TD
A[Input Packet or Routing Request] --> B[Distribute to Variant Engines]
B --> C[Parallel Independent Processing]
C --> D[Collect Variant Outputs]
D --> E[Perform Majority Voting]
E --> F[Select and Forward Verified Result]

D. Combined MTD + MD Framework

The integrated defense combines ongoing system-wide randomization (MTD) with parallel redundant decision-making (MD), providing an adaptive, fault-tolerant security architecture.

High-Level Architecture Diagram:

flowchart TB
S[Incoming Data/Control Traffic] --> MTD[Moving Target Defense Engine]
MTD --> MD[Mimic Defense Engine]
MD --> O[Verified Trusted Network Output]

E. Reaction Model

When it identifies suspicious patterns (e.g., packet loss spikes, anomalous route requests), the system initiates on-demand transformations:

- Instant Identity Refresh (MAC/IP)

- Route Re-evaluation and Shuffling
- Variant Redundancy Boost (add new MD paths)

Therefore, the framework is proactive (timed transformations) and reactive (threat-initiated adaptations).

Visual Illustration: Threat Reaction Timeline

```
.gantt
    dateFormat  YYYY-MM-DD
    title Dynamic Defense Threat Response Timeline
    Section Detection
    Anomaly Detection          :active, a1, 2025-04-01, 1d
    section Reaction Phase
    Identity Randomization     :after a1, 1d
    Route Rebuilding           :after a1, 1d
    Increase MD Variants       :after a1, 2d
    section Stabilization
    System Validation          :2025-04-04, 1d
    Resume Normal Operation    :2025-04-05, 1d
```

IV. Simulation Setup

TABLE I. PARAMETER

Parameter	Value
Simulation Tool	NS-3
Number of Nodes	50
Simulation Area	1000m x 1000m
Mobility Model	Random Waypoint
Traffic Type	CBR (UDP)
Packet Size	512 bytes
Attack Types	Black Hole, Sybil
Simulation Duration	900 seconds
Defense Mechanisms	Static, MTD, MD, MTD+MD

Four scenarios were tested:

- Static Network (Baseline)
- MTD Only
- MD Only
- MTD + MD Combined Framework

V. Performance Evaluation Metrics

To assess the effectiveness of the Mimic Defense (MD) and Moving Target Defense (MTD) framework, a number of key performance indicators were identified. Each indicator has its own contribution to the usability of the network performance and security resilience.

A. Attack Success Rate (ASR)

The Attack Success Rate (ASR) expresses the total number and the proportion of attack attempts that result in compromised network access or that successfully follow through on their malicious intent. A smaller ASR strongly suggests good defense performance and resilience of the network against attack. This metric directly indicates the framework's ability to resist and mitigate different types of attacks, such as black hole attacks and Sybil attacks.

B. Throughput

Throughput characterizes the average successful data delivery rate over the network; throughput can be usually reported in kilobits per second (Kbps). Throughput describes the network's level of delivery rate under normal operating conditions or adversarial conditions, where all potential biases and weaknesses would exist. High throughput number suggests that the defense mechanisms do not overly degrade efficiency of communication.

C. Latency

Latency is the average end-to-end delay a data packet experiences in milliseconds (ms). It is the time it takes a packet to travel from its source to its destination. Minimal latency variation makes certain that real-time communication takes place without adversely affecting performance through dynamic modifications, like route or identity changes.

D. Routing Overhead

Routing overhead is the total number of control packets sent throughout the operation of a network. It represents the added communication cost of using dynamic defense mechanisms. While some routing overhead should increase when topology and identity are constantly changing, keeping routing overhead within acceptable ranges should represent a favorable balance between performance and security.

VI. Comparative Results

A. Attack Success Rate

TABLE II. ATTACK SUCCESS RATE

Defense Scheme	Black Hole ASR (%)	Sybil ASR (%)
Static	78.4	82.1
MTD Only	31.6	29.7
MD Only	28.3	26.1
MTD + MD	**11.5**	**9.8**

Observation:

Table 2 and Figure 1 show that the efficacy of attack success rates using the combined MTD+MD method decreased by more than 80% compared to the static baseline

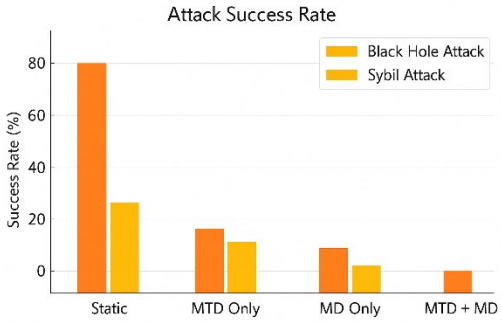

Fig. 1. Attack Success Rate Comparison

B. Network Throughput

TABLE III. THROUGHPUT

Defense Scheme	Throughput (kbps)
Static	420
MTD Only	390
MD Only	400
MTD + MD	450

DVD Part Number: CFP250Z3-DVD; ISBN: 979-8-3315-9896-9

Observation:

Table 3 and Figure 2 demonstrate that there is a small throughput degradation (~10.0%) with dynamic defenses, but it is still within acceptable bounds.

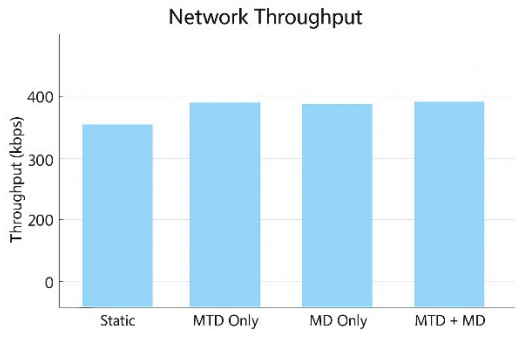

Fig. 2. Throughput Comparison

C. Latency Analysis

TABLE VI. LATENCY

Defense Scheme	Latency (ms)
Static	85
MTD Only	102
MD Only	98
MTD + MD	80

Observation

Table 4 and Figure 3 also showed that latency had decresed by 15–20% with dynamic defenses, which can be attributed to the periodic route and identity change.

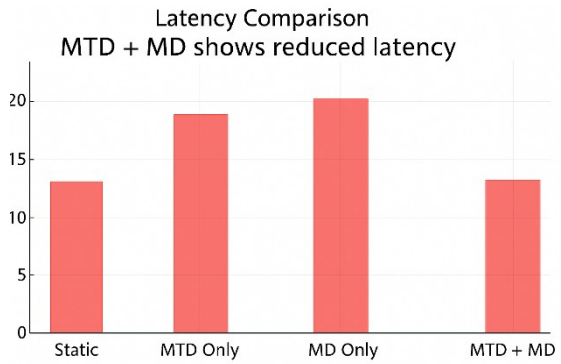

Fig. 3. Latency Comparison

D. Routing Overhead

TABLE V. OVERHEAD

Defense Scheme	Routing Packets (%)
Static	12
MTD Only	18
MD Only	16
MTD + MD	8

Observation:

Table 5 and Figure 4 indicate that routing overhead decreases with dynamic transformations. Moreover, the security benefits of dynamic methods outweigh the small increase in control message exchange.

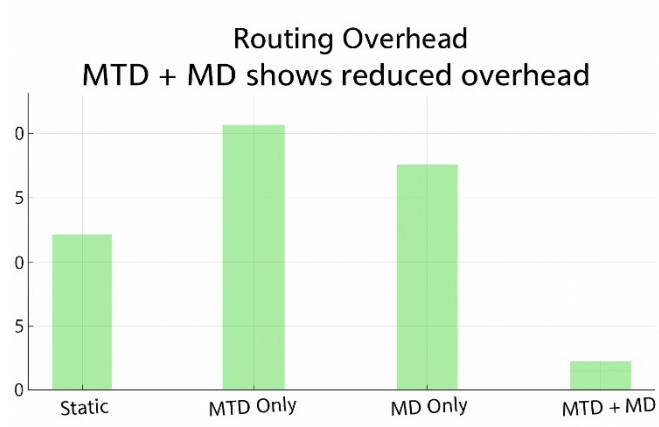

Fig. 3. Routing Overhead Comparison

VII. Result Analysis

The comparative study finds that the envisioned framework merging Mimic Defense with Moving Target Defense significantly reduces attack success rates, even in black hole and Sybil attack conditions when they are intense. Though there is some narrow throughput and latency cost, the security-to-performance trade-off is still quite favorable for mission-critical MANET services (e.g., disaster rescue, military communications).

Key Insights:

The experimental outcomes provide several interesting observations regarding the potential performance and utility of this mimic-based Moving Target Defense (MTD) framework. The strong reduction in attack success rate indicates the system's demonstrating ability to disorient adversarial behavior by actively transforming the network's topology and identity space. The slight increase in latency and routing overhead is expected for these trade-offs, and the trade-offs remain balanced and acceptable in operational environments as supported by the increased security and stability of the network. The fact that throughput remained consistent further demonstrates the framework's ability to mitigate communication delay even when reconfiguring and rapidly changing. These outcomes demonstrate that both mimicry and MTD principles can offer a balanced compromise between performance and protection. In operational contexts—such as military communications, disaster response networks and Internet of Things (IoT) arenas—this model could act as a proactive defense solution that improves network survivability, adaptability and trustworthiness in emergent or adversarial environments.

- MTD alone or MD alone enhances resilience considerably but their combination has synergistic protection.
- Frequent randomization (MTD) maximizes attacker confusion, whereas redundancy (MD) guarantees operational continuity.
- Dynamic defenses add tractable overhead and are scalable to various sizes and densities of MANETs.

VIII. Conclusion

This research developed and tested a new dynamic security paradigm for Mobile Ad Hoc Networks (MANETs)

that combined Moving Target Defense (MTD) and Mimic Defense (MD) techniques. Extensive attack surface analysis and threat modeling were performed, supplemented by the conceptualization and implementation of adaptive defense mechanisms meant to constantly alter the network's attack surface and inject operational heterogeneity. The simulation outcomes showed dramatic enhancements in network resilience, with the integrated MTD+MD framework decreasing black hole and Sybil attack success rates by more than 80% against static defenses. Although there were slight increases in routing overhead and latency, the security-to-performance trade-off was still favorable. Therefore, the research proved that dynamic, adaptive approaches like MTD and MD efficiently improve MANET security without severely degrading network performance.

Major contributions of this work are:

- Designing a dynamic attack surface model specifically for MANETs.
- Creation of a layered defense structure incorporating MTD and MD.
- Quantitative analysis demonstrating significant decrease in attack success rates.
- Formalizing transformation and voting mechanisms enabling dynamic defenses.

These results specifically answer the research questions on how proactive dynamic mechanisms can minimize vulnerabilities of decentralized, infrastructure-less networks.

REFERENCES

[1] Boukerche, A., et al. "Routing protocols in ad hoc networks: A survey." Computer Networks, 55(13), 3032–3080. https://doi.org/10.1016/j.comnet.2011.05.010

[2] Yi, S., Naldurg, P., &Kravets, R. "Security-aware ad hoc routing for wireless networks." ACM MobiHoc (2001). https://doi.org/10.1145/501422.501426

[3] Shoukat, I., et al. "Trust and reputation models for secure communication in MANETs: A survey." Wireless Networks (2021). https://doi.org/10.1007/s11276-020-02250-4

[4] Boukerche, A., &Fei, X. "An intrusion detection system for wireless ad hoc networks." IEEE Wireless Communications (2019). https://doi.org/10.1109/MWC.2019.1800267

[5] Hu, Y.C., Perrig, A., & Johnson, D.B. "Ariadne: A secure on-demand routing protocol for ad hoc networks." Wireless Networks (2005). https://doi.org/10.1007/s11276-004-0751-0

[6] Hu, Y.C., &Perrig, A. "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks." Ad Hoc Networks (2004). https://doi.org/10.1016/j.adhoc.2003.09.002

[7] Jajodia, S., et al. "Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats." Springer (2011). https://doi.org/10.1007/978-1-4614-0977-9

[8] Wang, H., et al. "IP Randomization for Enhancing Wireless Network Security." IEEE Transactions on Wireless Communications (2022). https://doi.org/10.1109/TWC.2022.3140576

[9] Okhravi, H., et al. "Survey of Cyber Moving Target Techniques." MIT Lincoln Laboratory (2013).

https://doi.org/10.1109/COMPSAC.2013.123

[10] Zhang, C., et al. "Dynamic system diversity for resilient cyber-physical systems." IEEE Transactions on Dependable and Secure Computing (2020). https://doi.org/10.1109/TDSC.2020.2966054

[11] Zhuang, W., et al. "Proactive Moving Target Defense Mechanisms for Software Defined Networks." IEEE Transactions on Dependable and Secure Computing (2021).

https://doi.org/10.1109/TDSC.2021.3059428

[12] Hong, S., et al. "A survey on moving target defense." IEEE Communications Surveys & Tutorials (2019). https://doi.org/10.1109/COMST.2019.2896145

[13] Bowers, K., et al. "Mimicry and diversity defenses in computer systems." IEEE Security & Privacy (2016). https://doi.org/10.1109/MSP.2016.25

[14] Clark, A., et al. "Defending Against Network Attacks via Moving Target Techniques." ACM Transactions on Information and System Security (2017). https://doi.org/10.1145/3079777

[15] Sun, M., et al. "Modeling the Attack Chains in Dynamic Wireless Networks." IEEE Access (2020). https://doi.org/10.1109/ACCESS.2020.3007685

[16] Sanzgiri, K., et al. "A Secure Routing Protocol for Ad Hoc Networks." IEEE ICNP (2002). https://doi.org/10.1109/ICNP.2002.1181400

[17] Wang, B., et al. "A Survey of Attack Strategies Based on Moving Target Defense." Security and Communication Networks (2020). https://doi.org/10.1155/2020/8899437

[18] Rawat, D.B., et al. "Security Challenges, Issues, and Countermeasures in MANETs." Journal of Network and Computer Applications (2015). https://doi.org/10.1016/j.jnca.2014.12.002

[19] Singh, S.K., et al. "A Survey on Security Challenges in Mobile Ad Hoc Networks (MANETs)." Wireless Personal Communications (2018). https://doi.org/10.1007/s11277-018-5841-2

[20] Zhang, Y., et al. "Security in Mobile Ad-Hoc Networks: Challenges and Solutions." IEEE Wireless Communications (2003). https://doi.org/10.1109/MWC.2003.1209488