Grenze International Journal of Engineering and Technology, June Issue

Analysis of Trade-offs between Security Features and Performance Metrics in MANET

Dr. Sheetal Rajput[1] and Sachin Kumar[2]
[1]Associate Professor in Dept. of Computer Science, Bhagwant Institute of Technology, Muzaffarnagar, U.P, India, ORCID ID: 0009-0001-4147-788X
Email: sheetal1.rajput@gmail.com
[2]Post Doctoral Research Fellow, College of Computer Science and Information Science, Srinivas University, Mangalore, India, Associate Professor, Dept. of Information Technology, Management Education & Research Institute (MERI), Affiliated to GGSIP University, New Delhi., India. ORCID-ID: 0000-0002-1136-8009;
Email: sachinks.78@gmail.com

***Abstract*—This paper delves into the improvement of security mechanisms for the AODV protocol in MANETs, considering security-feature impacts under various types of attacks, such as Blackhole, Eavesdropping, and Sybil attacks. Comparison has been made between the base protocol and the enhanced version which includes trust-based routing, encryption, and intrusion detection mechanisms. The study has used performance metrics such as PDR, E2ED, Throughput, Energy Consumption, and Routing Efficiency. The enhanced protocol achieves 7% improvement in PDR with the effectiveness of defeating malicious attacks, though with some trade-offs in terms of E2ED, reduced throughput, and increased energy consumption. It has improved its performance in routing efficiency by decreasing the route length, increasing the discovery rate of routes, and decreasing the overhead of maintaining the routes. The results point to a balance between security and performance; thus, the added security features are justified by trade-offs. Future research should focus on optimizing these features so that energy consumption is reduced while throughput is improved, and also scalability and performance in large networks and under more complex attacks.**

***Index Terms* — Mobile Ad-Hoc Networks (MANETs), AODV protocol, Security enhancement, Trust-based routing, Performance analysis, Intrusion detection.**

I. INTRODUCTION

Mobile Ad-Hoc Networks are self-configuring networks without any centralized infrastructure, allowing the devices to communicate with each other, making them the perfect tool for applications like military operations and emergency response, or in fact wireless sensor networks. But MANET's decentralization puts them at risk to all these security threats of unauthorized access and theft of data. This research aims at improving the security of the much-used Ad-hoc On-demand Distance Vector (AODV) routing protocol in the integration of security mechanisms to counter threats such as Blackhole, Eavesdropping, and Sybil attacks.

A. Security Challenges in MANETs

A big challenge to the assurance of data confidentiality, integrity, and availability in MANETs is the vulnerability to the attacks of malicious nodes disrupting the communication.

Grenze ID: 01.GIJET.11.2.511_1

Among those is AODV which is prone to attacks, particularly Blackhole (dropping malicious packets) and Sybil (pretending to be many). All these concerns must be addressed so that MANETs become reliable, especially for applications involving critical functions.

B. Enhancement of AODV with Security Mechanisms

This study envisages a trust-based routing incorporating mechanisms like encryption and intrusion detection systems over and above AODV. Its improvements are made with these augmentations to enhance security features with minimal compromise in performance. The proposed protocol will test several attack scenarios and make measurements in terms of performance in terms of PDR, E2ED, Throughput, Energy Consumption, and Routing Efficiency.

C. Research Objectives

The primary objectives of this research are to:

- To assess the effects of security mechanisms on key performance metrics, such as PDR, E2ED, Throughput, Energy Consumption, and Routing Efficiency in MANETs, considering the varied attack scenarios
- To evaluate the ability of the improved AODV protocol to withstand attacks like Blackhole, Eavesdropping, and Sybil and how the protocol can improve network reliability compared to the basic AODV
- To analyze the trade-offs between security features (encryption, intrusion detection, trust-based routing) and performance metrics (energy consumption, throughput, routing efficiency).

II. Literature Review

Rahman et al. (2023) intended to improve Mobile Ad Hoc Networks' (MANETs') performance, wherein an efficient, secure, and adaptable routing protocol will be created. In order to ensure secure routing and optimize the potential gains in network performance from lowering factors like energy consumption and raising others like network load and quality of service (QoS), the designed protocol included several security mechanisms, including authentication, encryption, key management, and intrusion detection.

Mohindra and Gandhi (2021) proposed a clustering mechanism based on secure cryptography (SCCM) to guarantee MANET security. Comparing the proposed technique to the previous security mechanism of traditional systems, it overcomes these computational complexity and efficiency issues. This work used Elliptic Curve Cryptography (ECC) encryption and generation to create a secure sign between nodes' routing protocols by the system.

Srilakshmi et al. (2021) concentrated on MANETs by enhancing fault tolerance and security in MANETs and implementing an efficient multipath routing system utilizing a hybrid Genetic Algorithm with Hill Climbing (GAHC). Based on a trust assessment, the enhanced fuzzy C-means method was used to choose CHs. The suggested approach demonstrated that the protocol provided great throughput in the simulation, had low energy consumption, and had little delay.

Gupta et al. (2024) believed that the AODV routing protocol for MANETs could be made secure enough to withstand both explicit and implicit attacks that caused packet drops on nodes. As a result, they exploited certain flaws in the widely used secure routing strategies based on hash chains and digital signatures. The security performance deterioration for malicious nodes was not lessened by the enhanced defense against them. Through increased resilience, their work was able to show how effective protection against malevolent attacks against AODV is.

Veeraiah et al. (2021) discussed the problems with MANETs, particularly those related to data manipulation and eavesdropping. In this study, they optimized the path selection process and energy usage using a hybrid Cat Slap Single-Player Algorithm called C-SSA, which is based on trust value. Based on the trust value, the Cluster Head was chosen using fuzzy clustering. The simulation findings demonstrated superior performance, overcoming the state-of-the-art techniques in the presence of selective packet-dropping attacks, with low energy usage and a packet delivery ratio of 99% and a 90% detection rate.

Nikhade and Thakare (2022) explained methods for enhancing the security and integrity of MANET based on Blockchain technology. By enhancing scalability and dependability, it developed a Promulgated Reliance Esteemed Quadruplets Condition along with Relinquished Blockchain-based Integrity System which linked node attributes with blockchain addresses. Latencies of Quality of Service had further also been addressed by using Obscure Relevance Algorithm while employing the proposed method. The results are shown to show the possibility of integrating Blockchain with MANETs for both security and performance improvement: high packet delivery ratio, which is 98%, with low packet loss, 69%, and lower end-to-end delay by 0.20.

Trivedi and Khanpara (2021) examined how to improve connectivity and data transfer in smart settings by integrating IoT with MANETs and WSNs. They emphasized that memory and processing power are only two aspects of IoT devices' resource constraints; energy is another. Various secure MANET protocols that get over these restrictions and guarantee reliable data transfer were covered.

III. Research Methodology

This chapter details the methodology for performance analysis of the MANETs improved security mechanism based on their performance under various attack conditions. Two protocols were simulated: the basic AODV and its advanced version with enhanced security features integrated within. These protocols were aimed at comparing the effect of the implementation of these security features on the performance of a network in terms of the Packet Delivery Ratio (PDR), End-to-End Delay (E2ED), Throughput, Energy Consumption, and Routing Efficiency.

A. Simulation Setup

Simulations were done using a network simulation tool that compares the baseline AODV protocol with its enhanced version. Mobile nodes were randomly spread over a given area, and movement was done by the random waypoint model so that different node mobility can be introduced. Three different attack scenarios—Blackhole, Eavesdropping, and Sybil—were simulated to test the robustness of the enhanced protocol under different types of malicious interference.

B. Performance Metrics

Several key performance metrics have been used to evaluate the protocols. The Packet Delivery Ratio (PDR) measures how efficient packet delivery is; the higher the PDR value, the better the performance. End-to-End Delay (E2ED) is the time taken from source to destination for a packet to travel, and lesser values of E2ED reflect faster communication. The Throughput measures the rate of data transmission, and higher the value of Throughput, the better the performance. Another was Energy Consumption, which studied the energy consumption of nodes, balancing security features with energy efficiency.

C. Protocol Implementation

The protocol used as a base is the standard AODV routing protocol. The main characteristic of this is the lack of security in its framework. The enhanced AODV protocol incorporates trust-based routing, encryption, and intrusion detection to defend against Blackhole, Eavesdropping, and Sybil attacks. These security measures ensured a more secure routing protocol without much degradation in its performance.

D. Data Collection

It utilized multiple simulation runs, and the network was exposed to various traffic loads, node mobility, and attack scenarios. All simulations were closely monitored and recorded key metrics—PDR, E2ED, Throughput, and Energy Consumption—to measure the impact of security features on protocol performance.

E. Simulation Scenarios

The network was under three types of attacks: Blackhole Attack, in which malicious nodes drop packets, reducing the PDR; Eavesdropping, in which the malicious nodes intercept data, creating a violation of confidentiality; and Sybil Attack, in which a malicious node creates multiple fake identities to create a disruption on the routing. These attacks discovered the weaknesses of both protocols and demonstrated the new protocol's ability to protect the network.

F. Data Analysis

The collected data was analysed for baselines and enhanced protocols to determine comparisons in different attack scenarios. From the analysis, PDR, Throughput, E2ED, and Energy Consumption were used to judge how well the enhanced protocol maintains a performance level despite attacks on the network. From results, it is shown to be effective for balancing security needs with network performance.

IV. Results and Discussion

This section is going to discuss the experimental findings in detail. It compares the enhanced security mechanism proposed for MANET protocols based on the performance metrics of Packet Delivery Ratio (PDR), End-to-End Delay (E2ED), Throughput, Energy Consumption, and Routing Efficiency. The outcomes are tested against different attack scenarios to test the robustness of the enhanced mechanism.

A. Comparative Analysis of Baseline and Enhanced Protocol Performance

Table 1 summarizes the comparison between the baseline AODV protocol and the enhanced security mechanism. Results show that the security metrics have been improved significantly at the cost of some performance.

TABLE I: BASELINE AODV VS. ENHANCED AODV PERFORMANCE

Metric	Baseline AODV	Enhanced AODV	Improvement
Packet Delivery Ratio (%)	85	92	+7%
End-to-End Delay (ms)	500	550	Slight increase
Throughput (kbps)	1200	1100	Moderate drop
Energy Consumption (J)	1000	1200	Slight increase

Enhanced Mechanism 7% PDR Improvements show how this mechanism can counter packet drop attacks. It really has the ability to successfully respond against malicious packet drops as seen with the improved PDR rate, which shows that its ability in countering malicious attacks against packet delivery is significantly efficient. However, the improved protocol shows a minor delay E2ED increase to 550 ms from 500 ms due to additional encryption and trust calculations involved in the new improved protocol. Throughput decreased relatively due to the extra computations involved in the security process, while energy consumption rises to 1200 J that depicts the price of using more advanced encryption mechanisms and intrusion detection systems. Although the trade-offs are present, the advanced mechanism results in a more secure and reliable network for security-sensitive applications.

B. Impact of Attack Scenarios on Performance

The evaluation of resilience was done with the help of three attacks: Blackhole Attack, Eves dropping and Sybil Attack. A summary of the performance is presented in Table 2.

TABLE II: PERFORMANCE UNDER VARIOUS ATTACK SCENARIOS

Attack Scenario	Packet Delivery Ratio (%)	End-to-End Delay (ms)	Throughput (kbps)	Energy Consumption (J)
No Attack	92	550	1100	1200
Blackhole Attack	65	700	900	1300
Eavesdropping	80	600	1000	1250
Sybil Attack	70	750	950	1280

The most severe degradation occurs due to the Blackhole Attack, where PDR reduces to 65% due to the discarding of packets by malicious nodes. The proposed mechanism greatly alleviates this degradation as the PDR remains much higher than that in the baseline.

Throughput and E2ED are degraded with the rise of Blackhole and Sybil attacks, as it includes extra overhead of security mechanisms in efforts to nullify malicious behavior. On the contrary, Eavesdropping attacks have a relatively low effect since they are focused on confidentiality and not on packet delivery, thereby causing a moderate PDR (80%) and throughput (1000 kbps) loss. Figure 1: Packet Delivery Ratio vs. Attack Scenarios In Figure 1, it can be observed that the advanced protocol withstands several types of attacks.

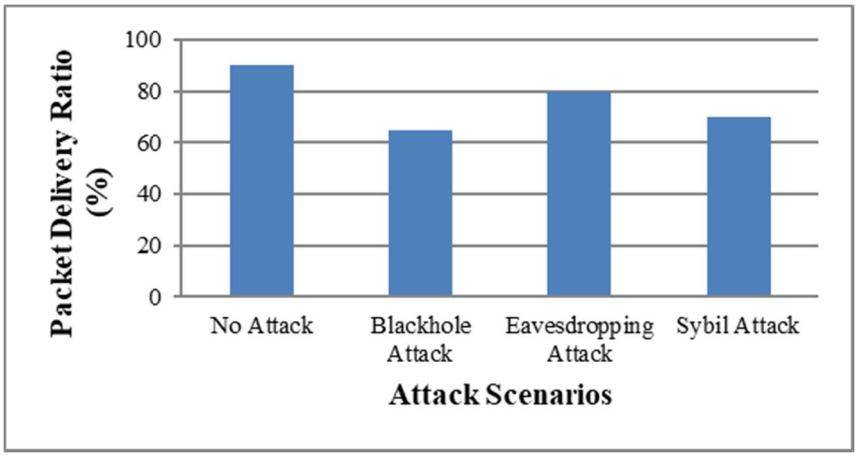

Figure 1: Packet Delivery Ratio (PDR) vs. Attack Scenarios

As illustrated in Figure 1, the PDR of the enhanced protocol was also quite stable even against the attack scenarios, suggesting that the security mechanisms devised can be efficient in establishing a reliable communication.

C. Energy Consumption Analysis

The energy consumption for the enhanced protocol under different attack scenarios is detailed in Table 3.

TABLE III: ENERGY CONSUMPTION ANALYSIS

Scenario	Baseline AODV (J)	Enhanced AODV (J)
No Attack	1000	1200
Blackhole Attack	1100	1300
Eavesdropping	1050	1250
Sybil Attack	1080	1280

As shown in Figure 2, energy consumption of the improved protocol is augmented in all cases due to the computational overhead of providing security. The maximum increase will be observed under the Blackhole Attack scenario where energy increased from 1100J to 1300 J as it involves additional processes that need to be invoked in order to handle some packet drops from malicious machines. Although energy consumption becomes more, increased security, as well as network stability, are well worth these extra-energy expenses.

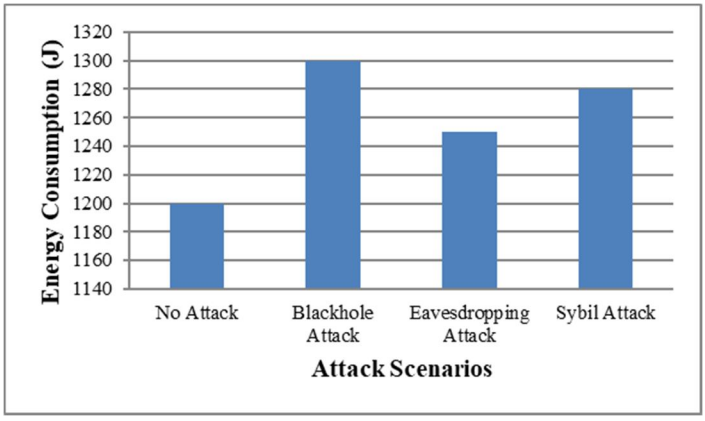

Figure 2: Energy consumption under different attack scenarios

Energy consumption is higher for the improved protocol in all scenarios as expected. This is due to increased energy cost resulting from enhanced processing, including encryption and processing of trust-based routing decisions. The enhanced security measure leads to a relatively slightly higher energy consumption over the baseline, but enhances reliability and security in such a network, which is paramount in attack-prone environments.

D. Routing Efficiency Metrics

The routing efficiency of the enhanced protocol is analyzed with regard to Average Route Length, Route Discovery Time and Route Maintenance Overhead in Table 4.

TABLE IV: ROUTING EFFICIENCY METRICS

Metric	Baseline AODV	Enhanced AODV	Improvement
Average Route Length (hops)	5	4	Reduced
Route Discovery Time (ms)	1000	850	Faster
Route Maintenance Overhead	High	Moderate	Reduced

The enhanced protocol shows better routing efficiency and reduces the average route length from 5 hops to 4, which supports the reduction of time in packet delivery. Route discovery time goes down by 150 ms, from 1000 ms to 850 ms, which shows faster setup of routes. Overhead in route maintenance is reduced and shows that the protocol is efficient in handling dynamic conditions of the network with minimal processing. This is probably due to the routing mechanisms that rely on trust, where security-efficient routes are favored. All these developments indicate how much the enhanced protocol has performed to become more effective in this dynamic, security-conscious environment in order to achieve fast and reliable routing.

E. Throughput Comparison

Figure 3 illustrates the throughput comparison of the Baseline AODV and Enhanced AODV protocols in the presence of different attack scenarios. The enhanced protocol, though having a minimal reduction in throughput because of added security overhead, has an acceptable level of throughput across all the attack scenarios.

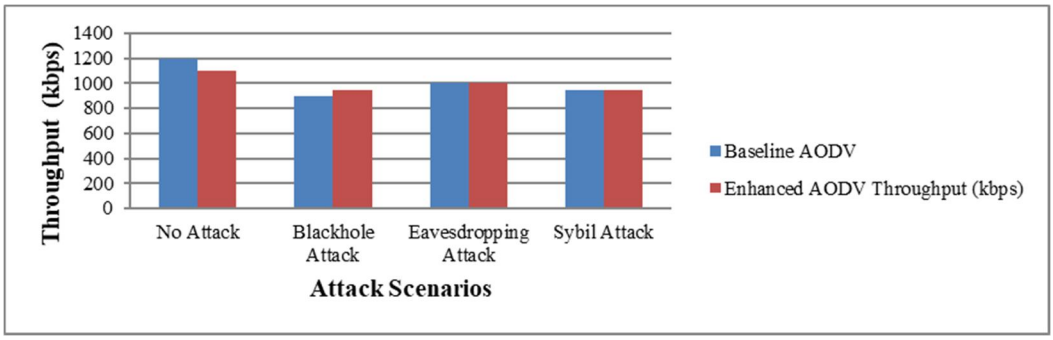

Figure 3: Throughput Comparison between Baseline and Enhanced Protocols

It can clearly be inferred from Figure 3 that throughput differs between the baseline and the enhanced protocols. The improved protocol shows a moderate throughput degradation, especially in Blackhole and Sybil attack scenarios, due to overhead introduced by the security. However, throughput is sufficient enough to carry out effective data transfer while guaranteeing the network's security.Generally speaking, the improved protocol enjoys strong balance between security and performance, considering that it shows slight compromises with regards to energy consumption, throughput, as well as delay but provides a lot more strength in packet delivery, routing efficiency, and resilience against many common network attacks. Based on these results, one can say that the improvement is appropriate for high-security requirement environments without significantly degrading performance in general.

V. Conclusion and Future Scope

This study tested the performance of an advanced security mechanism for the AODV protocol in MANETs that protects against Blackhole, Eavesdropping, and Sybil attacks. The enhanced AODV improved the packet delivery ratio by 7%, enhanced the efficiency of routing, provided quicker route discovery, and reduced overhead. However, the trade-offs included the slight increase in End-to-End Delay, more energy consumption, and a lower throughput. Despite these, the protocol performed well for security-sensitive applications over dynamic networks.

Future research work can be on the design of energy-efficient mechanisms to secure, ML-based intrusion detection, resilience to more complex attacks, and scaling to larger MANETs while optimizing for real-time or multimedia applications.

References

[1] Bondada, P., Samanta, D., Kaur, M., & Lee, H. N. (2022). Data security-based routing in MANETs using key management mechanism. Applied Sciences, 12(3), 1041.

[2] Gupta, S., Singla, S., & Sharma, P. (2024). Enhanced Security in MANETs Using AODV Protocol. Journal of The Institution of Engineers (India): Series B, 1-12.

[3] Hai, T., Zhou, J., Lu, Y., Jawawi, D., Wang, D., Onyema, E. M., &Biamba, C. (2023). Enhanced security using multiple paths routine scheme in cloud-MANETs. Journal of Cloud Computing, 12(1), 68.

[4] Hassan, S. M., Mohamad, M. M., Muchtar, F. B., & Dawoodi, F. B. Y. P. (2024). Enhancing MANET Security Through Federated Learning and Multiobjective Optimization: A Trust-aware Routing Framework. IEEE Access.

[5] Kausar, S., Habib, M., Shabir, M. Y., Ullah, A., Xu, H., Mehmood, R., ... & Iqbal, M. S. (2020). Secure and efficient data transfer using spreading and assimilation in MANET. Software: Practice and Experience, 50(11), 2095-2109.

[6] MOHINDRA, A. R., & GANDHI, C. (2021). A secure cryptography based clustering mechanism for improving the data transmission in MANET. Walailak Journal of Science and Technology (WJST), 18(6), 8987-18.

[7] Nikhade, J. R., & Thakare, V. M. (2022). BlockChain Based Security Enhancement in MANET with the Improvisation of QoS Elicited from Network Integrity and Reliance Management. Adhoc & Sensor Wireless Networks, 52.

[8] Popli, R., Sethi, M., Kansal, I., Garg, A., & Goyal, N. (2021, August). Machine learning based security solutions in MANETs: State of the art approaches. In Journal of physics: conference series (Vol. 1950, No. 1, p. 012070). IOP Publishing.

[9] Rahman, M. T., Alauddin, M., Dey, U. K., & Sadi, S. (2023). Adaptive, secure and efficient routing protocol to enhance the performance of Mobile Ad Hoc Network (MANET). Applied Computer Science, 19(3).
[10] Satyanarayana, P., Sofi, U. B., Ahmed, B. F., Saranya, N. N., Rao, G. P., & Krishnan, V. G. (2024, March). Enhancement of Network Security in MANET Using Refined Adaptive Harris Hawks Optimization Algorithm (RAHHO) for IoT Applications. In 2024 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 1-5). IEEE.
[11] Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S. A., Khalaf, O. I., &Subbayamma, B. V. (2021). An improved hybrid secure multipath routing protocol for MANET. IEEE Access, 9, 163043-163053.
[12] Sudhahar, S., Pousia, S., Gnanaprakash, G., Jayaprakash, S., & Nalavarasu, N. (2023, December). Enhancing Security in MANET through EAACK: A Novel Approach for Node Detection, Acknowledgment Validation and Routing Optimization. In 2023 4th International Conference on Communication, Computing and Industry 6.0 (C216) (pp. 1-6). IEEE.
[13] Trivedi, R., &Khanpara, P. (2021). Robust and secure routing protocols for MANET-based internet of things systems—A survey. In Emergence of Cyber Physical System and IoT in Smart Automation and Robotics: Computer Engineering in Automation (pp. 175-188). Cham: Springer International Publishing.
[14] Usha, M. S., & Ravishankar, K. C. (2021). Implementation of trust-based novel approach for security enhancements in MANETs. SN Computer Science, 2(4), 257.
[15] Veeraiah, N., Khalaf, O. I., Prasad, C. V. P. R., Alotaibi, Y., Alsufyani, A., Alghamdi, S. A., &Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. IEEe Access, 9, 120996-121005.