UDC 004.7

DOI: 10.18372/2073-4751.81.20137

Stoliar A.L.,
orcid.org/0000-0002-7669-1202,
e-mail: stoliarannanau@gmail.com,
Kudrenko S.O.,
orcid.org/0000-0002-0759-3908,
e-mail: stanislava@i.ua

SECURITY MECHANISMS FOR AODV AND E-AODV PROTOCOLS AGAINST BLACK HOLE AND GRAY TUNNEL ATTACKS

State University «Kyiv Aviation Institute»

Introduction

Mobile ad hoc networks (MANETs) have gained significant attention in recent years due to their ability to support flexible, infrastructure-free communication across a wide range of applications – from emergency response and battlefield communication to IoT-based smart environments. These networks consist of self-organizing mobile nodes that cooperate to form temporary network topologies and route data dynamically based on current conditions.

Among the numerous routing protocols developed for MANETs, the Ad hoc On-Demand Distance Vector (AODV) protocol has emerged as one of the most prominent due to its reactive nature, low overhead, and scalability. However, its design assumptions about node cooperation and trust make it particularly susceptible to various types of attacks. To address some of these vulnerabilities, an enhanced version, E-AODV, was introduced, incorporating additional mechanisms to detect and mitigate malicious behavior.

Despite these improvements, MANETs remain vulnerable to sophisticated routing attacks, such as black hole and gray tunnel attacks. In a black hole attack, a malicious node falsely advertises optimal routes and subsequently drops all intercepted packets, effectively disrupting the communication flow. In a gray tunnel attack, the malicious node selectively drops packets, making the attack harder to detect and potentially more damaging over time.

Such threats not only compromise data integrity and availability but also undermine the overall reliability of the network. Hence, ensuring secure and trustworthy routing in MANETs remains a critical challenge.

This paper presents a detailed analysis of the behavior of AODV and E-AODV protocols under black hole and gray tunnel attacks. Through simulated scenarios, we investigate the extent of vulnerabilities and propose a set of protective mechanisms aimed at detecting abnormal routing behavior and mitigating its impact. The effectiveness of these mechanisms is evaluated based on several performance indicators, including packet delivery ratio, end-to-end delay, and throughput.

Principles of AODV and E-AODV

The Ad hoc On-Demand Distance Vector (AODV) protocol is a widely used reactive routing protocol in mobile ad hoc networks (MANETs). It creates routes only when they are needed, which minimizes routing overhead and conserves network resources. When a source node needs to send data to a destination for which it has no route, it broadcasts a Route Request (RREQ) packet. This RREQ propagates through the network until it reaches the destination or an intermediate node with a fresh route. Then, a Route Reply (RREP) is unicast back to the source. AODV uses sequence numbers to ensure the freshness of routing information and to prevent routing loops. Once the route is established, data packets are forwarded along the selected path. If a link break occurs, a Route Error (RERR) message is generated to inform upstream nodes to invalidate the broken route.

Although efficient, AODV is vulnerable to various security threats due to the lack

of built-in authentication or trust verification. For instance, a malicious node can respond with a falsified RREP, attracting data packets and dropping them, resulting in a black hole attack.

To address these vulnerabilities, the Enhanced AODV (E-AODV) protocol introduces several security-oriented improvements. E-AODV maintains the reactive nature of AODV but adds mechanisms to detect and avoid malicious nodes. It incorporates trust evaluation for neighboring nodes, where trust metrics are updated based on routing behavior. Nodes that frequently cause route failures or act abnormally are assigned lower trust values. E-AODV also filters suspicious routes by analyzing the timing and frequency of RREP messages, thereby detecting anomalies such as premature or overly frequent replies. Additionally, it introduces reverse path verification, ensuring the integrity of the routing path by confirming that intermediate nodes are genuinely part of the established route.

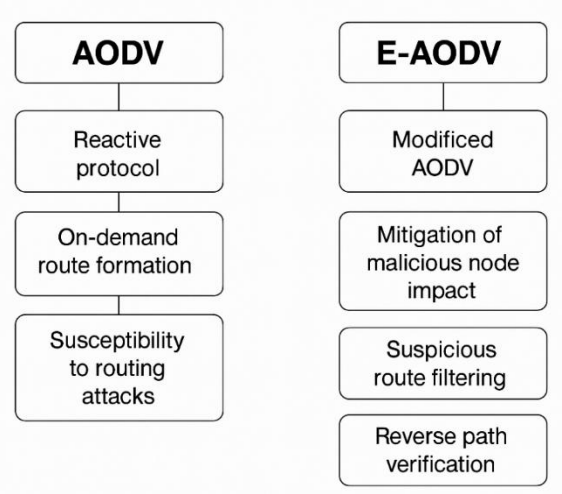

Fig. 1. Comparetion of AODV, E-AODV

Through these (Fig.1) enhancements, E-AODV improves the robustness of routing in hostile or unpredictable network environments, providing a more secure foundation for reliable communication in MANETs.

Mobile ad hoc networks (MANETs) rely heavily on routing protocols such as AODV (Ad hoc On-Demand Distance Vector) and its enhanced version E-AODV to dynamically establish paths between mobile nodes without fixed infrastructure. These protocols, especially AODV, are reactive – meaning routes are discovered only when needed – and they operate based on the assumption of mutual trust between nodes. This fundamental assumption creates a significant vulnerability that is often exploited by routing-layer attacks, such as the black hole and gray tunnel attacks.

In AODV, when a node wants to initiate communication but lacks a route to the destination, it broadcasts a Route Request (RREQ). A malicious node can respond immediately with a forged Route Reply (RREP), claiming to have the shortest path. Because AODV prioritizes replies with the highest sequence numbers and the shortest path, the malicious node is quickly selected as part of the active route. This enables a black hole attack, where the malicious node drops all data packets after attracting the traffic, thereby causing a denial of service. Since AODV does not perform verification of the responding node or the proposed route, it is particularly susceptible to this form of attack.

The gray tunnel attack is more deceptive. In this scenario, a malicious node also responds with a forged RREP and becomes part of the route, but instead of dropping all packets, it selectively drops them–perhaps based on packet content, source address, or timing. This behavior allows the node to appear normal while still disrupting communication, making detection difficult using simple packet delivery metrics. Since AODV lacks continuous route validation or acknowledgment mechanisms, it is ill-equipped to detect such selective interference.

E-AODV was developed to improve upon AODV's limitations, particularly its vulnerability to these attacks. E-AODV integrates several enhancements such as trust evaluation, route reply timing analysis, and reverse route verification. When a node receives multiple RREPs, E-AODV not only considers the shortest path and highest sequence number but also checks for consistency in the reply timing and the behavioral history of the sending node. If a node has been previously identified as suspicious due to dropped packets or abrupt route changes, its replies can be ignored or deprioritized. Some

versions of E-AODV implement a trust score, which is dynamically updated based on past forwarding behavior. This allows nodes to make routing decisions based not only on topology but also on behavioral patterns, increasing resistance to black hole and gray tunnel attacks.

Despite these improvements, gray tunnel attacks still pose a challenge, as even E-AODV's enhancements may not detect them without external acknowledgment or behavioral analysis. To address this, researchers are increasingly integrating machine learning-based anomaly detection, acknowledgment-based methods (e.g., TWOACK, AACK), and cross-layer detection with E-AODV. These hybrid models enable the network to correlate routing behavior with metrics like packet loss, latency, or signal quality, allowing more accurate differentiation between malicious drops and natural disruptions.

In summary, AODV is highly vulnerable to both black hole and gray tunnel attacks due to its trust-based, lightweight design. E-AODV mitigates some of these vulnerabilities by incorporating additional route validation and behavioral monitoring, but further integration with intelligent detection mechanisms is necessary to defend against more sophisticated, selective attacks. Enhancing E-AODV with such adaptive mechanisms continues to be a critical direction for ensuring secure and resilient routing in MANETs.

Simulation of Attack Scenarios and Defense Mechanisms

To evaluate the effectiveness of AODV and E-AODV protocols under security threats, we conducted simulation-based modeling of attack scenarios and integrated defense mechanisms. The goal of the simulation is to assess protocol resilience under black hole and gray tunnel attacks and to observe the behavior of enhanced routing under proposed protective features.

Simulation Environment

The simulation was implemented using a lightweight custom Python-based framework built on the networkx library, which enables dynamic construction of ad hoc topologies. Nodes are represented as vertices in a directed graph, and communication links include attributes such as delay and packet loss probability. This setup provides flexibility for injecting malicious behavior and measuring its impact under controlled parameters.

To assess scalability and protocol behavior across different network sizes, simulations were conducted using several node counts: 10, 25, 50, and 100 nodes. This range allows comparison between small-scale, mid-size, and large-scale MANET environments.

- 10 nodes: A minimal setup to illustrate basic attack impact and defense reactions.
- 25 nodes: Represents a small MANET, such as a localized IoT deployment or tactical team.
- 50 nodes: A standard testbed size for performance benchmarking.
- 100 nodes: A large-scale network scenario simulating high-density mobile environments.

For each configuration, 100 random packet transmissions were simulated between randomly selected source-destination pairs.

Other simulation parameters:

- Topology: Random graph (Erdős–Rényi model)
- Packet generation rate: 100 transmissions per simulation
- Delay range per link: 1–5 ms
- Packet loss probability per link: 0–10%

Attack Modeling

Two attack models were implemented. Black hole attack: A designated malicious node intercepts Route Request (RREQ) messages and immediately responds with forged Route Reply (RREP) messages claiming optimal routes. Once selected for forwarding, the node drops all data packets, simulating a denial of service. Gray tunnel attack: A malicious node selectively forwards some data packets while silently dropping others. The selection is probabilistic (e.g., drops 50% of traffic), making it harder to detect.

Defense Mechanism Integration

To simulate E-AODV, the following adaptive mechanisms were introduced into the baseline AODV logic:

- Trust evaluation: Nodes record successful vs. failed forwarding behavior of neighbors. Nodes with a trust score below a threshold are avoided in route selection.
- Route reply timing analysis: Rapid or frequent RREP responses trigger suspicion flags, especially if inconsistencies arise in sequence numbers or hop counts.
- Gray behavior detection: For each forwarding node, a packet forwarding ratio is calculated over time. If it falls below an acceptable threshold while still forwarding some traffic, gray tunnel behavior is inferred.

Evaluation Metrics

To objectively assess protocol performance under attack and protection scenarios, the following criteria were used:

- Packet Delivery Ratio (PDR) – indicates overall success of data delivery:

$$PDR = \frac{Received\ Packets}{Sent\ Packets}.$$

- Average end-to-end delay – reflects the responsiveness and efficiency of routing:

$$Delay = \frac{\sum(t_{arrival} - t_{sent})}{Received\ Packets}.$$

- Packet loss rate – measures the disruptive impact of attacks or route failures:

$$PLR = \frac{Sent\ Packets - Received\ Packets}{Sent\ Packets} \times 100\%.$$

- Routing Overhead: Quantifies the control message burden imposed by route discovery and maintenance mechanisms.

By evaluating these metrics across multiple network sizes, the robustness and adaptability of each protocol under varied conditions can be thoroughly assessed.

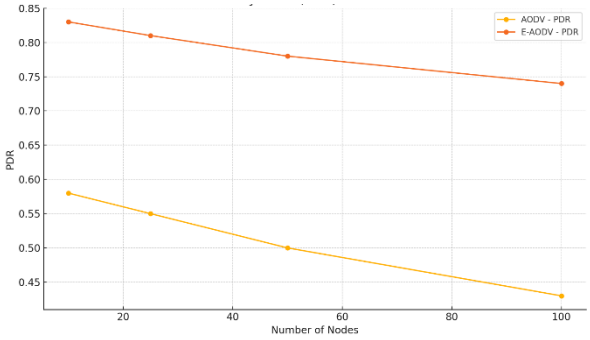

Fig. 2. Packet Delivery Ratio (PDR) vs Number of Nodes

The simulation results clearly demonstrate the performance differences between AODV and its enhanced counterpart, E-AODV, when exposed to black hole and gray tunnel attacks across various network scales.

As illustrated in Fig. 2, the Packet Delivery Ratio (PDR) for the standard AODV protocol decreases significantly as the number of nodes increases–from 0.58 with 10 nodes to just 0.43 at 100 nodes. This degradation reflects AODV's vulnerability to malicious behavior in dense network environments. The more nodes present, the higher the probability that a malicious node will be selected as a part of the routing path due to the lack of verification mechanisms in AODV. In contrast, E-AODV consistently maintains higher delivery rates across all scenarios, starting at 0.83 and remaining above 0.74 even in the 100-node simulation. This improvement results from its integrated trust evaluation and behavioral filtering mechanisms, which successfully prevent malicious nodes from intercepting critical paths.

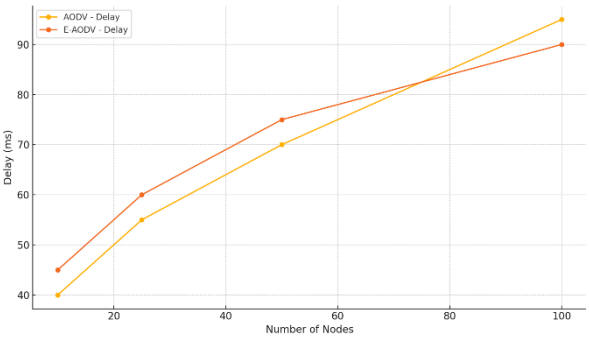

Fig. 3 Average End-to-End Delay vs Number of Nodes

Fig. 3 highlights the trend in average end-to-end delay. For AODV, delay grows sharply with node count, increasing from 40 ms at 10 nodes to 95 ms at 100 nodes. This growth is caused by frequent route discoveries, increased interference, and route failures in the presence of undetected attacks. E-AODV, while initially showing slightly higher delay due to its additional control operations (such as trust calculations and response filtering), demonstrates better scalability and path stability as network size increases. The delay grows more gradually, showing that E-AODV routes are less

frequently disrupted and more efficient over time despite the increased control overhead.

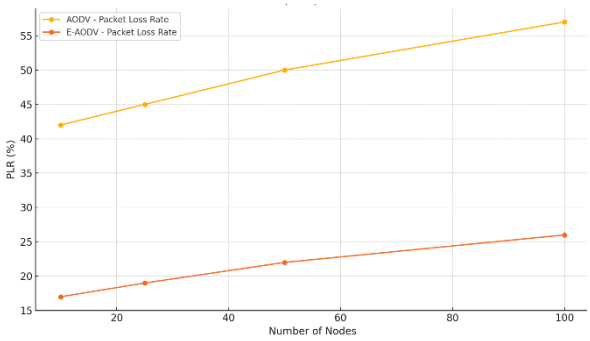

Fig. 4. Packet Loss Rate (PLR) vs Number of Nodes

Packet loss patterns are presented in Fig. 4. AODV suffers from rising Packet Loss Rate (PLR) as the network expands–from 42% at 10 nodes to 57% at 100 nodes–confirming that black hole and gray tunnel attacks have more severe consequences in larger networks. The loss of control over routing decisions and lack of detection mechanisms result in significant data drops. In contrast, E-AODV maintains a comparatively low and stable PLR: only 17% at 10 nodes and 26% at 100 nodes. This confirms the effectiveness of its security enhancements, particularly in filtering untrustworthy nodes and reinforcing valid route construction.

Collectively, the results (Figures 1–3) validate the hypothesis that E-AODV, through the incorporation of adaptive trust and detection mechanisms, significantly enhances routing robustness, delivery success, and resistance to attack-induced disruption across a range of MANET configurations. While the improvements come at the cost of increased routing overhead and slightly higher delays under benign conditions, the gains in packet delivery and resilience make E-AODV a superior choice in environments where security threats are present and network reliability is critical.

Conclusion

This study presented a comprehensive evaluation of the AODV and E-AODV routing protocols under two prominent routing-layer threats in MANETs: black hole and gray tunnel attacks. Through systematic simulation experiments using a custom Python-based environment, we modeled both the malicious behavior and the defense mechanisms and evaluated protocol performance under varying network sizes (10, 25, 50, and 100 nodes).

The results demonstrate that the standard AODV protocol, while efficient in benign conditions, becomes increasingly vulnerable in the presence of malicious nodes. As the network scale grows, its lack of built-in security leads to sharp declines in packet delivery ratio (PDR), increased average end-to-end delay, and higher packet loss rate (PLR). The black hole attack, in particular, shows immediate and severe impact, while the gray tunnel attack introduces subtle, harder-to-detect disruptions that accumulate over time and degrade routing efficiency.

E-AODV, on the other hand, incorporates adaptive trust-based mechanisms, route reply analysis, and selective path filtering to detect and avoid potentially malicious nodes. These enhancements enable the protocol to maintain significantly higher delivery ratios and lower packet loss rates across all tested configurations. Although E-AODV incurs slightly higher end-to-end delay due to its monitoring and trust computations, this trade-off is acceptable given the improved security and resilience outcomes.

Importantly, the scalability of E-AODV was validated by its consistent performance as the number of nodes increased. Even in large-scale networks, it successfully mitigated the disruptive effects of routing attacks through early detection and adaptive route selection. The protocol's modular design also allows for future integration of more advanced detection methods, such as machine learning or cross-layer analysis.

In conclusion, E-AODV presents a viable and effective improvement over the traditional AODV protocol for securing routing in MANETs. Its ability to dynamically evaluate node behavior and respond to emerging threats makes it especially suitable for deployment in hostile or mission-critical environments, such as battlefield networks, emergency response systems, and decentralized IoT frameworks. Future work may focus on further optimizing its trust models and

reducing the overhead introduced by its security extensions.

References

1. Perkins C. E., Belding-Royer E. M., Das S. R. RFC 3561. Ad hoc On-Demand Distance Vector (AODV) Routing. DOI: 10.17487/RFC3561.

2. Tamilselvan L., Sankaranarayanan V. Prevention of black hole attack in MANET. *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)* : proceedings, Sydney, NSW, Australia, 27–30 August 2007 / IEEE. 2007. P. 21–21. DOI: 10.1109/AUSWIRELESS.2007.61.

3. Deng H., Li W., Agrawal D. P. Routing security in wireless ad hoc networks. *IEEE Communications Magazine*. 2002. Vol. 40, iss. 10. P. 70–75. DOI: 10.1109/MCOM.2002.1039859.

4. Shree S. N., Sagar, R. V. A review on gray hole attack in MANET. *International Journal of Computer Applications*. 2017. Vol. 159, iss. 2. P. 1–4. DOI: 10.5120/ijca2017912922.

5. Rathi S., Sharma P. Analysis of Gray-Hole Attack in MANET using AODV. *International Journal of Computer Applications*. 2016. Vol. 139, iss. 12. P. 13–17. DOI: 10.5120/ijca2016908890.

6. Balakrishnan K., Deng H., Varshney P. K. TWOACK: Preventing selfishness in mobile ad hoc networks. *IEEE Wireless Communications and Networking Conference, 2005* : proceedings, New Orleans, LA, USA, 13–17 March 2005 / IEEE. 2005. P. 2137– 2142. DOI: 10.1109/WCNC.2005.1424848.

7. Zhang Y., Lee W. Intrusion detection in wireless ad-hoc networks. *MobiCom '00: 6th annual international conference on Mobile computing and networking* : proceedings, Boston, MA, USA, 2000 / New York, 2000. P. 275–283. DOI: 10.1145/345910.34595.

8. Balakrishnan K., Jing W., Varshney P. K. Trust-based adaptive on-demand ad hoc routing protocol. *Journal of Communications and Networks*. 2005. Vol. 7, iss. 3. P. 287–295. DOI: 10.1109/JCN.2005.6312738.

9. Mishra, A., Nadkarni, K., & Patcha, A. Intrusion detection in wireless ad hoc networks. *IEEE Wireless Communications*. 2004. Vol. 11, iss. 1. P. 48–60. DOI: 10.1109/MWC.2004.1269711.

10. Rafiee M., Javidan R. Hybrid Intrusion Detection System for MANETs Based on AODV. *International Journal of Network Security & Its Applications (IJNSA)*. Vol. 201911, iss. 1. P. 15–27. DOI: 10.5121/ijnsa.2019.11102.

Stoliar A.L., Kudrenko S.O.

SECURITY MECHANISMS FOR AODV AND E-AODV PROTOCOLS AGAINST BLACK HOLE AND GRAY TUNNEL ATTACKS

This paper investigates the security vulnerabilities of the AODV (Ad hoc On-Demand Distance Vector) and E-AODV (Enhanced AODV) routing protocols in mobile ad hoc networks (MANETs), focusing on two common attack types: black hole and gray tunnel attacks. A comprehensive analysis is conducted to examine how these attacks affect routing reliability, packet delivery, and network performance. E-AODV is evaluated as an improved protocol incorporating adaptive trust mechanisms, response timing analysis, and behavioral monitoring to mitigate malicious node interference. A simulation framework is implemented using a Python-based environment, where various network sizes (10–100 nodes) are tested. Key performance indicators such as Packet Delivery Ratio (PDR), End-to-End Delay, and Packet Loss Rate (PLR) are used to compare protocol behavior. Results show that E-AODV significantly enhances resilience to attack-induced disruption, outperforming standard AODV in both delivery efficiency and security reliability across diverse MANET topologies.

***Keywords**: AODV; E-AODV; MANET; black hole attack; gray tunnel attack; secure routing; trust-based mechanism; intrusion detection; packet loss; routing protocol security; simulation analysis; ad hoc network security.*

Столяр А.Л., Кудренко С.О.

МЕХАНІЗМИ БЕЗПЕКИ ДЛЯ ПРОТОКОЛІВ AODV ТА E-AODV ВІД АТАК ЧОРНИХ ДІР ТА СІРОГО ТУНЕЛЮ

У цій статті досліджуються вразливості протоколів маршрутизації AODV (Ad hoc On-Demand Distance Vector) та E-AODV (Enhanced AODV) у мобільних ad hoc мережах (MANET), зосереджуючись на двох поширених типах атак: атаках чорних дір та сірого тунелю. Проведено комплексний аналіз, щоб дослідити, як ці атаки впливають на надійність маршрутизації, доставку пакетів та продуктивність мережі. E-AODV оцінюється як покращений протокол, що включає адаптивні механізми довіри, аналіз часу відгуку та моніторинг поведінки для зменшення втручання зловмисних вузлів. Модельну структуру реалізовано за допомогою середовища на основі Python, де тестуються мережі різних розмірів (10–100 вузлів). Для порівняння поведінки протоколів використовуються ключові показники ефективності, такі як коефіцієнт доставки пакетів (PDR), наскрізна затримка та коефіцієнт втрати пакетів (PLR). Результати показують, що E-AODV значно підвищує стійкість до збоїв, спричинених атаками, перевершуючи стандартний AODV як за ефективністю доставки, так і за надійністю безпеки в різних топологіях MANET.

***Ключові слова**: AODV; E-AODV; MANET; атака чорної діри; атака сірого тунелю; безпечна маршрутизація; механізм на основі довіри; виявлення вторгнень; втрата пакетів; безпека протоколу маршрутизації; симуляційний аналіз; безпека ad hoc мережі.*