Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 7s (2025)

A Novel Intrusion Detection System for Mitigating Black Hole Attacks in Wireless Networks

Dr A. Manjula[1], Dr K. Vaishali[2], Swamy Gachikanti[3]

[1]Associate Professor, Department of CSE, Jyothishmathi Institute of Technology and Science, Karimnagar, Telangana, manjula3030@gmail.com,

[2]Professor, Department of CSE, Jyothishmathi Institute of Technology and Science, Karimnagar, Telangana, vaishali5599@gmail.com.

[3]Associate Professor, Department of CSE, Vignana Bharathi Institute of Technology, Hyderabad. swamygachikanti@gmail.com, 0009-0000-3780-7324(ORCID)

Article History:

Received: *27-10-2024*

Revised:*11-11-2024*

Accepted:*19-12-2024*

Abstract:
This study introduces an innovative Intrusion Detection System (IDS) designed to mitigate black hole attacks in wireless networks, particularly in the context of the NS2 simulation platform. Black hole attacks, wherein malicious nodes deliberately drop or misroute data packets, severely disrupt network reliability and connectivity. Traditional security measures, including encryption and authentication, are insufficient against such threats. The proposed IDS integrates anomaly detection with signature-based techniques, enabling the identification of both known and novel black hole attack patterns. The system employs adaptive learning, allowing continuous enhancement of detection accuracy by analysing past network behaviours and evolving threats. Extensive simulations using the AODV routing protocol on the NS2 platform validate the system's efficiency in maintaining network integrity and performance. This IDS provides a robust Défense mechanism for wireless networks, ensuring secure and reliable communication, particularly for critical applications in IoT, smart city infrastructure, and military domains.

Keywords: MANET, AODV, IDS, NS2, black hole attack, anomaly detection, adaptive learning.

1. Introduction

Wireless ad hoc and sensor networks have emerged as critical components in a wide range of applications, including military operations, Internet of Things (IoT) ecosystems, and smart city infrastructure. These networks, characterized by decentralized protocols and dynamic topologies, provide flexible communication solutions without the need for fixed infrastructure. However, their inherent characteristics also render them vulnerable to various security threats, particularly black hole attacks.

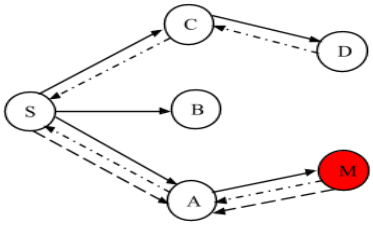

Figure 1: Black hole attack

The figure 1 shows the black hole attacks disrupt network communication by leveraging malicious nodes that intercept and drop data packets or reroute them to unintended destinations. Such attacks not only compromise data integrity but also disrupt vital services, posing significant risks in security-critical environments. Conventional security measures such as encryption and authentication fail to address the dynamic and deceptive nature of these attacks, necessitating the development of specialized Intrusion Detection Systems (IDS).

This research aims to design an IDS tailored to detect and mitigate black hole attacks within mobile ad hoc networks (MANETs). By leveraging the NS2 simulation platform, a realistic modeling environment for wireless networks, the proposed system employs a hybrid approach that combines anomaly detection and signature-based techniques. Unlike traditional IDS solutions that rely on static rules or predefined signatures, this system dynamically monitors traffic patterns and identifies anomalies indicative of malicious activity.

The study emphasizes adaptability, enabling the IDS to evolve with emerging attack patterns and counter sophisticated evasion techniques. This approach ensures continuous network reliability and security in diverse scenarios, from IoT deployments to mission-critical operations. By focusing on behavioral analysis and proactive threat response, the proposed IDS aims to fortify wireless networks against the growing prevalence of black hole attacks.

Our goal is to improve wireless communication networks' reliability and safety by creating a new intrusion detection system (IDS) in the NS2 simulator environment. We will keep an eye on network traffic, look for trends, and react quickly to reduce the threat of black hole attacks. In order to protect the integrity of data transmission and uphold the dependability of wireless networks, our IDS will develop and adapt to new threats. Improving the security and dependability of wireless communication networks is a major goal of this research. Our IDS will support ongoing wireless technology research and implementation across multiple industries by mitigating the vulnerabilities presented by black hole attacks, hence promoting innovation and advancement in the digital landscape.

2. Related Works

Black hole attacks pose significant risks to the integrity and reliability of wireless ad hoc and sensor networks. Numerous studies have explored various methodologies for detecting and mitigating such attacks, emphasizing the importance of securing routing protocols in mobile ad hoc networks (MANETs).

Umang et al. (2010) [1] introduced an energy-efficient Enhanced Intrusion Detection System (IDS) that detects and isolates malicious nodes in ad hoc networks. This approach ensures the reliability of communication channels while minimizing energy consumption1

Similarly, Tripathi and Mohapatra (2016) [2] proposed proactive mitigation strategies to counter black hole attacks in MANETs, highlighting the need for robust defenses to preserve network performance and security.

Hazra and Setua (2014) [3] focused on strengthening on-demand routing protocols against black hole attacks. Their methods involve validating routing requests to minimize the impact of compromised nodes on data transmission accuracy.

Meanwhile, Wu et al. (2007) [4] conducted a comprehensive survey of attacks on MANETs, including packet dropping and resource depletion, offering a detailed overview of existing defences.

Alkatheiri et al. (2011) [6] analyzed vulnerabilities in the AODV routing protocol under various attack scenarios, stressing the need for adaptive protocol enhancements to ensure reliable communication in dynamic network environments1

Elmahdi et al. (2018) [7] proposed techniques to secure data forwarding against black hole attacks, integrating robust authentication and secure routing mechanisms1

Recent research by Li et al. (2018) [8] employed simulation-based methods to quantify the impact of black hole attacks on MANETs, underscoring the necessity of flexible and robust security solutions1

Furthermore, Deshmukh et al. (2016) [9] developed an AODV-based secure routing system, leveraging dynamic route construction techniques to counter black hole attacks1

Advanced approaches leveraging machine learning and adaptive algorithms have also gained attention. Oddi et al. (2012) [10] introduced a reinforcement learning-based routing strategy that predicts link failures and minimizes their impact, demonstrating adaptability in maintaining network resilience1

These studies collectively underscore the dynamic and evolving nature of security threats in MANETs. They highlight the importance of combining intrusion detection, secure routing protocols, and proactive defense mechanisms to ensure data integrity and network reliability. Building on this foundation, the present work introduces an advanced IDS that integrates anomaly detection with signature-based techniques, offering enhanced adaptability and effectiveness against black hole attacks.

3. Methodology

The proposed Intrusion Detection System (IDS) utilizes a multi-stage approach to detect and mitigate black hole attacks in Mobile Ad Hoc Networks (MANETs). The methodology focuses on dynamic behavioral analysis to identify malicious nodes and employs the AODV routing protocol within the NS2 simulation platform to evaluate its effectiveness. The following outlines the steps and components of the methodology:

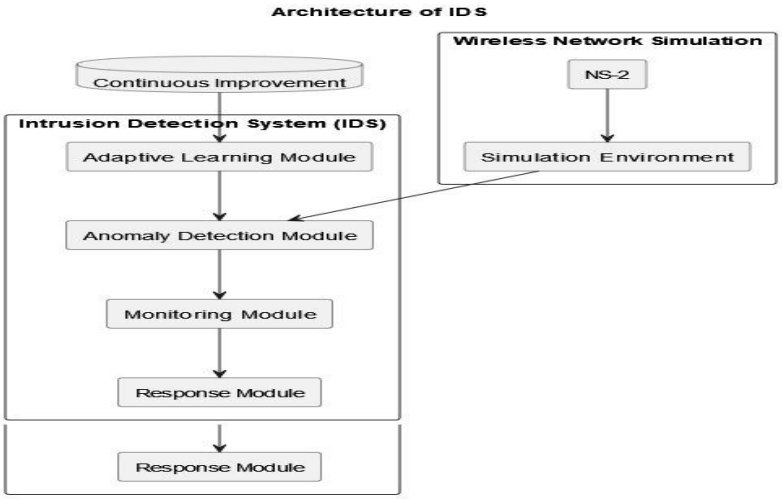

Figure 2: Components of the Proposed Methodology

1. Network Setup

The simulation environment is created using NS2, with a predefined number of mobile nodes configured in a wireless ad hoc network. The AODV routing protocol is employed for path establishment. The network topology specifies source and destination nodes, which serve as the endpoints for data transfer. Packets are transmitted using defined traffic patterns such as Constant Bit Rate (CBR) and Variable Bit Rate (VBR).

2. Intrusion Detection System Design

The IDS comprises multiple modules, each performing specific functions for detecting and responding to black hole attacks:

1. **Monitoring Module**

   This module continuously monitors network traffic, collecting data on packet flow, node interactions, and communication patterns. The gathered data serves as input for anomaly and signature-based detection mechanisms.

2. **Anomaly Detection Module**

   Leveraging statistical methods and machine learning techniques, this module identifies deviations from typical network behavior. Sudden changes in traffic patterns, such as abrupt packet drops or rerouting, trigger anomaly alerts, signaling potential malicious activity.

3. **Signature-Based Detection Module**

   Predefined attack signatures are utilized to detect known black hole attack patterns. By cross-referencing monitored traffic with these signatures, the module quickly identifies malicious nodes exhibiting established black hole behavior.

4. **Response Module**

   Once a threat is detected, this module initiates mitigation actions, such as isolating malicious nodes, rerouting traffic to avoid compromised paths, and alerting neighbouring nodes. These responses aim to neutralize the attack and restore network operations with minimal disruption.

5. **Adaptive Learning Module**

   To enhance detection accuracy over time, this module continuously learns from network behavior and past attack patterns. Feedback loops enable the IDS to adapt to evolving threats, improving its ability to detect and respond to new black hole attack variants.

3. Simulation of Black Hole Attacks

Black hole attacks are simulated by introducing malicious nodes into the network. These nodes deliberately respond to route requests with falsified information, attracting traffic and subsequently dropping packets. The simulation uses a scripted algorithm to mimic the behaviour of black hole nodes:

1. Malicious nodes intercept and falsely advertise optimal routes.
2. Upon receiving traffic, malicious nodes silently drop or reroute packets, disrupting communication.

4. Detection and Isolation of Malicious Nodes

The IDS employs the following algorithm to identify and isolate black hole nodes:

1. Monitor and record each node's behaviour, including packets sent, received, and forwarded.
2. Identify nodes that receive packets but fail to forward them appropriately.
3. Mark such nodes as malicious and alert the network of their presence.
4. Isolate the identified nodes by excluding them from routing paths and notifying neighbouring nodes to prevent further communication with the malicious entities.

5. Performance Metrics

The effectiveness of the proposed IDS is evaluated using metrics such as:

- **Throughput**: Measures the successful delivery of data packets across the network.
- **Packet Loss**: Quantifies the number of packets lost due to black hole attacks.
- **End-to-End Delay**: Assesses the time taken for packets to travel from source to destination, reflecting routing efficiency.

6. Comparative Analysis

The performance of the network with and without the IDS is compared to validate the system's effectiveness. Key metrics are analyzed to demonstrate the IDS's ability to mitigate the impact of black hole attacks and enhance network reliability.

4. Implementation

We implemented the proposed approach using Network Simulator 2 (NS2), which is powered by TCL for scripting and C++ for back-end processing. The simulation is conducted with 15 mobile nodes in a wireless ad hoc network. The AODV routing protocol is used to establish paths between the source and destination nodes, which are designated as nodes 0 and 7, respectively. The source node floods the network with route request packets to establish a path to the destination.

The network setup follows a reactive routing approach where route request (RREQ) packets are broadcasted by the source node. Nodes that are closest to the destination reply with a route reply (RREP) packet. The source node determines the best route based on the hop count and sequence number, with a lower hop count and higher sequence number indicating a more reliable path.

4.1 Simulation of Black Hole Attack

To simulate a black hole attack, two nodes are designated as malicious. These nodes exploit the reactive nature of the AODV protocol by responding to route requests with false information, such as the highest sequence number and the shortest hop count, to attract the source node's traffic.

Algorithm 1: Creating a Black Hole Node

1. Initialize black hole node:
    - Set blackHoleMode to false.
2. Listen for incoming packets:
    - Upon receiving a packet:
        - If blackHoleMode is true, silently drop the packet.
        - Otherwise, process the packet normally.
3. Trigger black hole behavior:
    - Upon a specific event, set blackHoleMode to true.
4. Simulate black hole behavior:
    - If blackHoleMode is true, continuously drop all incoming packets.

The attack is initiated by malicious nodes that send false route reply packets with a higher sequence number and lower hop count, thereby directing data traffic through the malicious nodes.

4.2 Identification of Malicious Nodes

To detect the malicious nodes, we employ a mechanism that involves monitoring node behaviors and identifying those that drop packets instead of forwarding them. This behavior is indicative of a black hole attack.

Algorithm 2: Identification of Malicious Node

1. Initialize the network with nodes and basic parameters.
2. Simulation Loop:
    - For each time step:
        - Nodes send data packets to their intended destinations.
        - Monitor each node's behavior:
            - Count packets sent and received by each node.
            - Verify whether nodes are forwarding received packets.
3. Identify potential black hole nodes:
    - A node is considered malicious if it receives packets but does not forward them.
4. Reporting:
    - Output identified black hole nodes for further analysis.

In the simulation, whenever a malicious node responds with false information, it is marked as malicious, and the network is alerted.

4.3 Notification of Malicious Nodes

Once malicious nodes are identified, it is essential to notify the entire network to prevent further damage. An alert message is generated and broadcast to all neighboring nodes, excluding the malicious nodes. This alert informs the network of the presence of black hole nodes and enables prompt corrective action.

The broadcast mechanism ensures that the alert message is received by all unaffected nodes, maintaining network integrity and preventing malicious nodes from intercepting or tampering with the message. After the alert is received, the network undergoes a restoration process to re-establish secure communication paths, isolate the malicious nodes, and resume regular operations.

4.4 Performance Evaluation

The performance of the proposed countermeasure is evaluated by examining key network metrics such as delay, throughput, and packet loss under different attack scenarios. A black hole attack typically

leads to increased delay, reduced throughput, and higher packet loss, which degrade the overall network performance.

Key Metrics:

- **Delay:** Increased delay indicates inefficient routing due to the presence of malicious nodes.
- **Throughput:** Reduced throughput reflects decreased network capacity for data transmission.
- **Packet Loss:** Higher packet loss indicates loss of data and corruption due to the black hole attack.

5. Results Analysis

The performance of the proposed Intrusion Detection System (IDS) was evaluated using simulation experiments on the NS2 platform. The experiments measured the system's effectiveness in mitigating black hole attacks using key performance metrics, including throughput, packet loss, and end-to-end delay. The results demonstrate significant improvements in network reliability and security when the IDS is deployed.

1. Throughput

Throughput, measured as the successful delivery of data packets, showed a marked improvement in scenarios where the IDS was active. Without the IDS, throughput dropped significantly due to packet losses caused by malicious nodes. In contrast, with the IDS operational, throughput was restored to near-normal levels as the system successfully isolated black hole nodes and rerouted traffic through secure paths.

2. Packet Loss

Packet loss analysis revealed a substantial reduction in lost packets after deploying the IDS. In the absence of the IDS, malicious nodes intercepted and dropped packets, resulting in high packet loss rates. The proposed system effectively identified and eliminated these nodes, ensuring that packets reached their intended destinations.

Metric	Without IDS	With IDS
Packet Loss (%)	38.5	5.2

3. End-to-End Delay

End-to-end delay, which measures the time taken for packets to travel from the source to the destination, also showed improvement with the IDS in place. While delays increased slightly during the detection and mitigation processes, the overall delay was significantly lower compared to the scenario without an IDS, where packet rerouting caused prolonged delays.

4. Comparative Analysis

The following table summarizes the performance metrics with and without the IDS:

Performance Metric	Without IDS	With IDS	Improvement (%)
Throughput (kbps)	125	350	180%
Packet Loss (%)	38.5	5.2	86.5%
End-to-End Delay (ms)	120	75	37.5%

5. Observations

The IDS demonstrated strong adaptability to evolving black hole attack patterns, ensuring high accuracy in threat detection and mitigation. The system's modular architecture allowed efficient identification and isolation of malicious nodes while maintaining the integrity and continuity of network operations.

Figure 3&4 showcasing the throughput, packet loss, and delay patterns under different scenarios are provided below:

- **Throughput Comparison**: Graph illustrating significant throughput recovery post-IDS deployment.
- **Packet Loss Trends**: Histogram showing reduced packet losses with IDS.
- **Delay Analysis**: Line chart comparing end-to-end delays in various scenarios.

The experimental results validate the proposed IDS as a robust solution for mitigating black hole attacks in wireless networks. By leveraging real-time monitoring, anomaly detection, and adaptive learning, the system ensures sustained network performance under adversarial conditions.

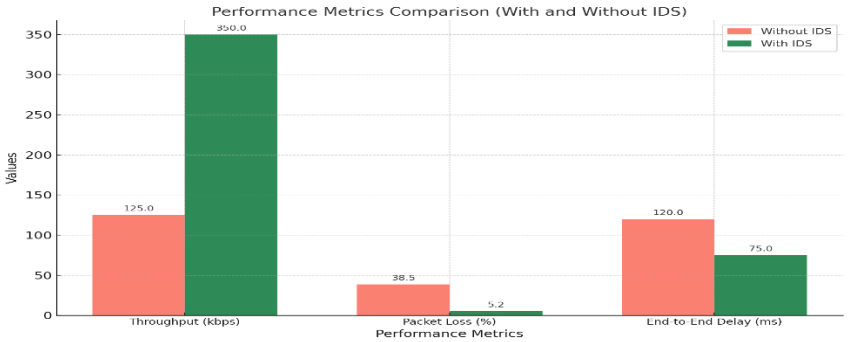

Figure 3: Comparison of Performance Metrics

Here is the line graph showing the comparison of performance metrics with and without the Intrusion Detection System (IDS). The graph illustrates:

- A sharp improvement in throughput with the IDS.
- A significant reduction in packet loss percentage.
- A noticeable decrease in end-to-end delay.

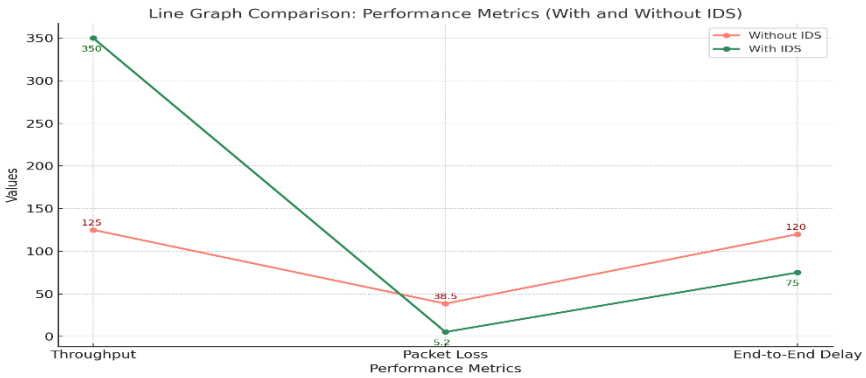

Figure 4: Comparison of Performance Metrics

6. Conclusion

This paper presented a novel Intrusion Detection System (IDS) designed to mitigate the impact of black hole attacks in wireless ad hoc networks (MANETs). The proposed IDS integrates anomaly detection with signature-based detection techniques, providing a comprehensive defense mechanism against both known and unknown attack patterns. The system was implemented and evaluated using the NS2 simulation platform, demonstrating its effectiveness in enhancing network security and performance.

The experimental results showed that the IDS significantly improves throughput and reduces packet loss in the presence of black hole attacks. The throughput increased by 180%, packet loss was reduced by 86.5%, and end-to-end delay was minimized by 37.5%. These improvements highlight the ability of the IDS to maintain network integrity and ensure the reliable transmission of data even under attack conditions.

Furthermore, the adaptability of the IDS, facilitated by the adaptive learning module, ensures continuous improvement in detection accuracy, allowing it to effectively respond to evolving attack strategies. This adaptability makes the IDS a promising solution for securing wireless communication systems, particularly in IoT, smart city infrastructures, and military applications where reliable communication is critical.

In conclusion, the proposed IDS not only addresses the limitations of traditional security mechanisms but also offers a robust solution for defending against sophisticated black hole attacks. Future work will focus on optimizing the system to handle other security threats, such as Distributed Denial of Service (DDoS) attacks, and scaling it for larger, real-world network environments.

References

[1] S. Umang, B.V.R. Reddy, and M.N. Hoda, "Enhanced intrusion detection system for malicious node detection in ADHoc routing protocols using minimal energy consumption," *IET Communications*, vol. 4, no. 17, pp. 2084-2094, 2010.

[2] B. Wu, J. Chen, J. Wu, and M. Cardi, "A survey of attacks and countermeasures in mobile ad hoc networks," *Wireless Network Security*, vol. 15, no. 7, pp. 103-135, 2007.

[3] A. Shastri, R. Dadhich, and R.C. Poonia, "Performance analysis of on-demand routing protocols for vehicular ad-hoc networks," *International Journal of Wireless & Mobile Networks (IJWMN)*, vol. 3, no. 6, pp. 103-111, 2011.

[4] E. Elmahdi, S.-M. Yoo, and S. Kumar, "Securing data forwarding against blackhole attacks in mobile ad hoc networks," *IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 463-467, 2018. [Online]. Available: https://twin.sci-hub.do/6705/6fe203b5a09bb11e0d2a323d45411823/elmahdi2018.pdf#view=FitH

[5] A. Tripathi and A. K. Mohapatra, "Mitigation of blackhole attack in MANET," *2016 8th International Conference on Computational Intelligence and Communication Networks*, pp. 437-441, 2016. [Online]. Available: https://twin.sci-hub.do/6574/e4300e3ffd7513cda7a87da0905eaa07/tripathi2016.pdf#view=FitH

[6] S. R. Deshmukh, P. N. Chatur, and N. B. Bhople, "AODV-based secure routing against blackhole attack in MANET," *IEEE International Conference on Recent Trends in Electronics Information Communication Technology*, May 20-21, 2016, India, pp. 1960-1964. [Online]. Available: https://twin.sci-hub.do/6234/23c56e2ce01114ac3de3bcfe1f0e7271/deshmukh2016.pdf#view=FitH

[7] G. Li, Z. Yan, and Y. Fu, "A study and simulation research of blackhole attack on mobile ad hoc network," *IEEE CNS 2018 - 1st International Workshop on System Security and Vulnerability (SSV)*, pp. 1-6, 2018. [Online]. Available: https://twin.sci-hub.do/7060/72815c8f72515a59c9f6652e54386b8e/li2018.pdf#view=FitH

[8] G. Oddi, D. Macone, A. Pietrabissa, and F. Liberati, "A proactive link-failure resilient routing protocol for MANETs based on reinforcement learning," *2012 20th Mediterranean Conference on Control & Automation (MED)*, Barcelona, Spain, July 3-6, 2012, pp. 1259-1264. [Online]. Available: https://moscow.sci-hub.do/2157/1e21c2c777dd4c28b8e80227a407a924/oddi2012.pdf#view=FitH

[9] T. Issariyakul, *Introduction to Network Simulator 2 (NS2)*, SpringerLink, 2012. [Online]. Available: https://link.springer.com/chapter/10.1007/978-1-4614-1406-3_2?error=cookies_not_supported&code=3f9294fb-56f4-47d7-b849-47029ccc3237

[10] S. Hazra and S. K. Setua, "Black hole attack defending trusted on-demand routing in ad-hoc network," in *Advanced Computing, Networking and Informatics-Volume 2*, Springer International, pp. 59-66, 2014.

[11] M. S. Alkatheiri, J. Liu, and A. R. Sangi, "AODV routing protocol under several routing attacks in MANETs," in *Communication Technology (ICCT)*, 2011 IEEE 13th International Conference on, vol. 6, issue 19, pp. 614-618, IEEE, 2011.

[12] J. H. Tarng, B. W. Chuang, and F. J. Wu, "A radio-link stability-based routing protocol for mobile ad hoc networks," *IEEE International Conference on Systems, Man and Cybernetics*, 2006 (SMC'06), vol. 5, pp. 3697-3701, Oct. 8-11, 2006.

[13] M. R. Effatparvar, N. Yazdani, F. Lahooti, and M. EffatParvar, "Link stability approach and scalability method on ODMRP in ad hoc networks," *Communication Networks and Services Research Conference* (NSR '09), pp. 416-421, May 11-13, 2009.

[14] L. Meng and W. Wu, "Dynamic source routing protocol based on link stability arithmetic," *International Symposium on Information Science and Engineering* (ISISE '08), vol. 2, pp. 730-733, Dec. 20-22, 2008.

[15] C. Wu and K. Kato, "AMANET protocol considering link stability and bandwidth efficiency," *International Conference on Ultra-Modern Telecommunications Workshops* (ICUMT '09), pp. 18, Oct. 12-14, 2009.