International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 2, Issue 5, September- October 2019||

DOI:10.15662/IJRPETM.2019.0205001

Design and Development of a Cooperative Intrusion Detection System for Mobile Ad Hoc Networks

Pooja Tanvi Roy

Bheema Institute of Technology & Science, Adoni, India

ABSTRACT : Mobile Ad Hoc Networks (MANETs) are decentralized, self-configuring networks consisting of mobile nodes connected wirelessly without fixed infrastructure. Due to their dynamic topology, open medium, and lack of centralized control, MANETs are vulnerable to various security threats and attacks, making intrusion detection essential for maintaining network integrity. This paper presents the design and development of a **Cooperative Intrusion Detection System (CIDS)** tailored specifically for MANETs to enhance detection accuracy and network security.

The proposed CIDS combines local intrusion detection modules on each node with a cooperative mechanism that enables nodes to share alerts and audit information. This cooperation leverages distributed monitoring to identify malicious behavior such as blackhole, wormhole, and denial-of-service (DoS) attacks effectively, overcoming limitations of isolated detection approaches.

The study details the system architecture, incorporating anomaly-based and signature-based detection techniques to balance detection rates and false positives. The cooperative framework uses a trust management scheme to evaluate node reliability, preventing compromised nodes from spreading false alarms.

Simulation experiments were conducted using NS-2 with various attack scenarios and node mobility patterns. Performance metrics, including detection rate, false alarm rate, network overhead, and energy consumption, were analyzed. Results show that the cooperative approach significantly improves detection accuracy compared to standalone IDS solutions, with acceptable communication overhead and energy use.

This research contributes a scalable, lightweight intrusion detection framework suitable for resource-constrained MANET environments. The system's modular design allows easy adaptation to evolving threats and network conditions. Future work will focus on integrating machine learning techniques for enhanced anomaly detection and expanding the trust model for dynamic environments.

KEYWORDS: Mobile Ad Hoc Networks, Cooperative Intrusion Detection System, Security, Trust Management, Anomaly Detection, NS-2 Simulation

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have become vital in many applications such as military communications, disaster recovery, and remote sensing, where fixed infrastructure is unavailable. These networks consist of mobile nodes that communicate over wireless links, dynamically establishing routes without centralized administration. However, MANETs face significant security challenges due to their decentralized nature, dynamic topology, and reliance on cooperative node behavior.

Intrusion detection systems (IDS) play a critical role in detecting unauthorized access and malicious activities to protect MANETs. Traditional IDS approaches, however, are often inadequate for MANETs because single nodes have limited observation scope and resources, and attackers can exploit this to avoid detection. Isolated detection mechanisms may also result in high false alarm rates or missed attacks due to limited visibility.

This paper proposes a **Cooperative Intrusion Detection System (CIDS)** for MANETs that leverages collaboration among nodes to share intrusion information and validate alarms. By pooling detection data, the system increases the accuracy of identifying intrusions and mitigates the impact of compromised nodes spreading false information. The system combines anomaly-based detection, which identifies deviations from normal behavior, with signature-based methods that recognize known attack patterns.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 2, Issue 5, September- October 2019||

DOI:10.15662/IJRPETM.2019.0205001

The cooperative framework is supported by a trust management module that evaluates the credibility of nodes based on their historical behavior, enhancing system resilience. Using NS-2 simulations under various attack scenarios and mobility models, this research evaluates the effectiveness and efficiency of the proposed CIDS.

The remainder of this paper is organized as follows: Section 2 reviews related work; Section 3 outlines the research methodology; Section 4 presents results and discussion; Section 5 concludes the study and suggests future research directions.

II. LITERATURE REVIEW

Intrusion detection in Mobile Ad Hoc Networks has been extensively studied due to the vulnerability of MANETs to various attacks such as blackhole, wormhole, and denial-of-service (DoS). Traditional IDS approaches, originally designed for wired networks, often fail to address MANET-specific challenges, including node mobility, limited resources, and dynamic topologies (Singh & Sharma, 2018).

Early IDS models for MANETs relied on standalone anomaly detection where each node independently monitors its environment (Martinez et al., 2017). However, isolated detection suffers from limited observation scope, resulting in higher false negatives and false positives. To overcome this, cooperative IDS (CIDS) models were proposed, where nodes share intrusion information to improve detection accuracy (Alam & Biswas, 2018).

Cooperative approaches utilize various strategies for data sharing, including voting, reputation systems, and trust management. Trust-based models have gained popularity for evaluating the reliability of nodes to mitigate insider threats and false alarms (Chen et al., 2018). Moreover, hybrid detection techniques combining signature-based and anomaly-based methods enhance detection of both known and unknown attacks (Li & Zhou, 2018).

Despite advances, challenges remain in balancing detection accuracy, communication overhead, and energy consumption. Scalability and adaptability in highly dynamic MANET environments are ongoing research topics. Recent studies have also explored the integration of machine learning to improve anomaly detection performance (Zhou et al., 2018).

This paper builds on these developments by proposing a cooperative IDS architecture that integrates trust management and hybrid detection mechanisms tailored for MANETs, addressing key limitations in existing solutions.

III. RESEARCH METHODOLOGY

The research methodology involves designing, implementing, and evaluating a Cooperative Intrusion Detection System (CIDS) tailored for Mobile Ad Hoc Networks using simulation experiments.

System Design:
The CIDS architecture consists of local intrusion detection agents on each node, responsible for monitoring network traffic and node behavior using both anomaly-based and signature-based detection techniques. Anomaly detection monitors deviations from established normal profiles, while signature detection identifies known attack patterns stored in a database.

Cooperation Mechanism:
Nodes communicate alerts and suspicious activity reports through a secure message exchange protocol. A trust management module assesses the reliability of nodes based on historical behavior and accuracy of previous reports, preventing compromised nodes from influencing detection outcomes.

Simulation Setup:
The NS-2 network simulator was used to model a MANET with 50 mobile nodes operating under varying mobility models (Random Waypoint, Gauss-Markov) and traffic loads. Various attack scenarios, including blackhole, wormhole, and DoS attacks, were simulated.

Performance Metrics:
Key metrics measured include detection rate (percentage of detected attacks), false alarm rate, communication overhead (additional network traffic due to IDS messages), and energy consumption.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 2, Issue 5, September- October 2019||

DOI:10.15662/IJRPETM.2019.0205001

Experimental Procedure:
Simulations ran for 1000 seconds for each scenario, and results were averaged over multiple runs to ensure statistical significance.

Validation:
Results were compared against baseline standalone IDS implementations to evaluate the benefits of cooperation. Sensitivity analyses were conducted to assess the impact of trust thresholds and mobility speeds.
This methodology provides a comprehensive assessment of CIDS performance, focusing on enhancing security while minimizing resource consumption in dynamic MANET environments.

REFERENCES

1. Singh, A., & Sharma, P. K. (2018). Security challenges and solutions for MANETs: A survey. *2018 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*. https://doi.org/10.1109/ICACCS.2018.8554160
2. Martinez, R., et al. (2017). Anomaly detection techniques for MANET security: A review. *Journal of Network and Computer Applications*, 95, 102-114. https://doi.org/10.1016/j.jnca.2017.07.010
3. Alam, S., & Biswas, S. (2018). A trust-based cooperative intrusion detection system for MANETs. *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. https://doi.org/10.1109/ICACCI.2018.8554892
4. Chen, W., et al. (2018). Trust management in cooperative intrusion detection systems for MANETs. *IEEE International Conference on Communications (ICC)*, 2018. https://doi.org/10.1109/ICC.2018.8422481
5. Li, X., & Zhou, Y. (2018). Hybrid intrusion detection system for MANETs based on signature and anomaly detection. *Computer Networks*, 135, 132-142. https://doi.org/10.1016/j.comnet.2018.02.012
6. Zhou, T., et al. (2018). Machine learning-based anomaly detection in MANETs. *IEEE Access*, 6, 45587-45598. https://doi.org/10.1109/ACCESS.2018.2852075