A CERTAIN INVESTIGATIONS ON PACKET DROPPING ATTACK DETECTION ON MOBILE ADHOC NETWORK ENVIRONMENT

Dr Niyaz Hussain A M J[1], Dr Chitra M[2], Dr Rajeev R[3], Dr Vigneshkumar K[4],

[1] Associate Professor, Department of Information Technology, Hindusthan College of Arts and Science (Autonomous), City Campus: Nava India, Coimbatore - 641028, Tamilnadu, India.

[2] Professor, Department of Computer Science and Engineering, Hindusthan Institute of Technology (Autonomous), Valley Campus: Pollachi Highway, Coimbatore - 641032, Tamilnadu, India.

[3] Assistant Professor, Department of CS & IT, JAIN (Deemed to be University), Kochi Kerala.

[4] Assistant Professor, Department of Computer Applications (MCA), Hindusthan College of Engineering and Technology (Autonomous), Valley Campus: Pollachi Highway, Coimbatore - 641032, Tamilnadu, India.

Corresponding author mail id: amj.niyaz@gmail.com

ABSTRACT

Various Intrusion Detection Systems (IDS) are critical for securing Mobile Ad hoc Networks (MANET), comprising self-organized, battery-equipped mobile nodes widely utilized in military and private sectors. Security remains a significant concern due to the network's vulnerability to attacks. The primary goal of IDS is to distinguish normal and suspicious activities within the network. Malevolent nodes might flood the system with excessive traffic, threatening to disrupt it. To counter these threats, numerous research endeavors by different experts have been presented.

The first study introduces a novel intrusion detection system based on Cat Swarm Optimization (CSO) for detecting packet dropping attacks in MANETs. This system considers historical and neighboring node information for optimizing failure node discovery and enhancing provenance data transmission security. It utilizes Side Channel Monitoring (SCM) to detect malicious data forwarding nodes' packet drop attacks, identifying selfish nodes and packet drop behaviors.

In a second approach, the Secondary Server-based Distributed and Cooperative Intrusion Detection System (SS-DC-IDS) is proposed to detect packet dropping attacks. The system employs an animal migration algorithm for secondary server selection based on fitness values like energy and bandwidth. Clustering and hybrid

side channel monitoring aid in collecting attack features and differentiating between mobility-related node failure and IDS attacks.

The third method, the Node Failure-aware Packet Drop Attack Detection Method (NF-PDADM), incorporates mobility factors and distinguishes node failure scenarios. It enhances route path stability and employs an improved animal migration algorithm for secondary server selection, considering energy, bandwidth, and distance to the primary server. NS2 simulations demonstrate that NF-PDADM outperforms existing methods in terms of latency, packet loss, delivery ratio, energy consumption, end-to-end delay, false positive rates, and attack probability.

NF-PDADM exhibits significantly lower latency, packet loss, energy consumption, end-to-end delay, and false positive rates compared to SS-DC-IDS and LC-IDS. Moreover, it displays higher delivery ratio and attack probability compared to these systems, demonstrating its superiority in securing MANETs.

1. INTRODUCTION

Wireless ad hoc networks consist of computing devices interconnected wirelessly via radio frequency, devoid of a fixed infrastructure or centralized control [1]. These networks find application across various domains, from military operations and emergency disaster relief to community networking and interactions among attendees or students during lectures [2]. A packet drop attack (gray hole) characterizes a denial-of-service (DoS) strategy where a router selectively relays or drops data packets intended for a specific network destination at specific intervals, such as after every n number of packets or every t number of seconds [3]. The primary objective of this research is to establish a framework for accurate and reliable detection of packet drop attacks. This involves considering node failures and the diverse range of intruders present within the network.

2. LITERATURE SURVEY

Merlin et al [4] introduced a pioneering Trust-Based Energy-Aware Routing (TEAR) mechanism designed for Mobile Ad hoc Networks (MANETs. A key feature of the TEAR mechanism involves mitigating Black Holes (BHs) by dynamically generating multiple detection routes for swift BH detection, ultimately enhancing data route security by establishing nodal trust. Patel et al [5] conducted an analysis of packet drop attacks and their impact on the route discovery time of AODV as well as throughput. Their

modifications to the AODV routing protocol aimed to identify such nodes, illustrating enhancements in the observed parameters. Singh et al [6] presented work emphasizing trust-based computing to counter the consequences of Black Hole, Wormhole, and Collaborative Black Hole attacks. Shah et al [7] proposed the Secure-BEFORE routing strategy to ensure optimal route estimation by computing trust values and hop counts using dummy packets within the network at the 1-hop level. Ahamad et al [8] proposed an efficient step-by-step technique affirming the detectability and defense against such attacks with minimal resource consumption and effort.

3. PROBLEM DEFINITIONS

Several research techniques have been previously introduced for detecting and preventing packet dropping attacks in mobile ad hoc networks. However, these research endeavors exhibit various issues that could potentially degrade the overall network performance. These concerns are as follows: "The existing system struggles to accurately differentiate between attack behavior and node mobility, learning network behaviors proves to be a more challenging task in the current system, the existing system predominantly concentrates on packet dropping attacks, yet real-world scenarios commonly involve Distributed Denial of Service (DDoS) attacks, injecting malicious traffic to disrupt the system."

4. OBJECTIVE OF THE RESEARCH

The primary aim of the research work is to present a framework enabling accurate and dependable detection of packet dropping and intrusion attacks occurring within the network. The objectives of this research work are outlined as follows:

- To introduce a packet dropping attack detection framework considering the presence of selfish nodes.
- To implement a reduced computation overhead packet dropping attack detection framework by selecting the secondary server.
- To develop a packet dropping attack detection framework addressing node failures and various intruders.

5. CONTRIBUTION OF THE RESEARCH

The research work's overall contribution is delineated as follows:

- Introduction of the Distributed and Cooperative Intrusion Detection System (DC-IDS) for accurate identification of packet dropping attacks.
- Implementation of the Secondary Server based Distributed and Cooperative Intrusion Detection System (SS-DC-IDS) to reduce computation overhead in intrusion detection.
- Introduction of the Node Failure aware Packet Dropping Attack Detection Method (NF-PDADM), considering the presence of node failures and intruders.

This comprehensive contribution of the research work is illustrated in Figure 1.

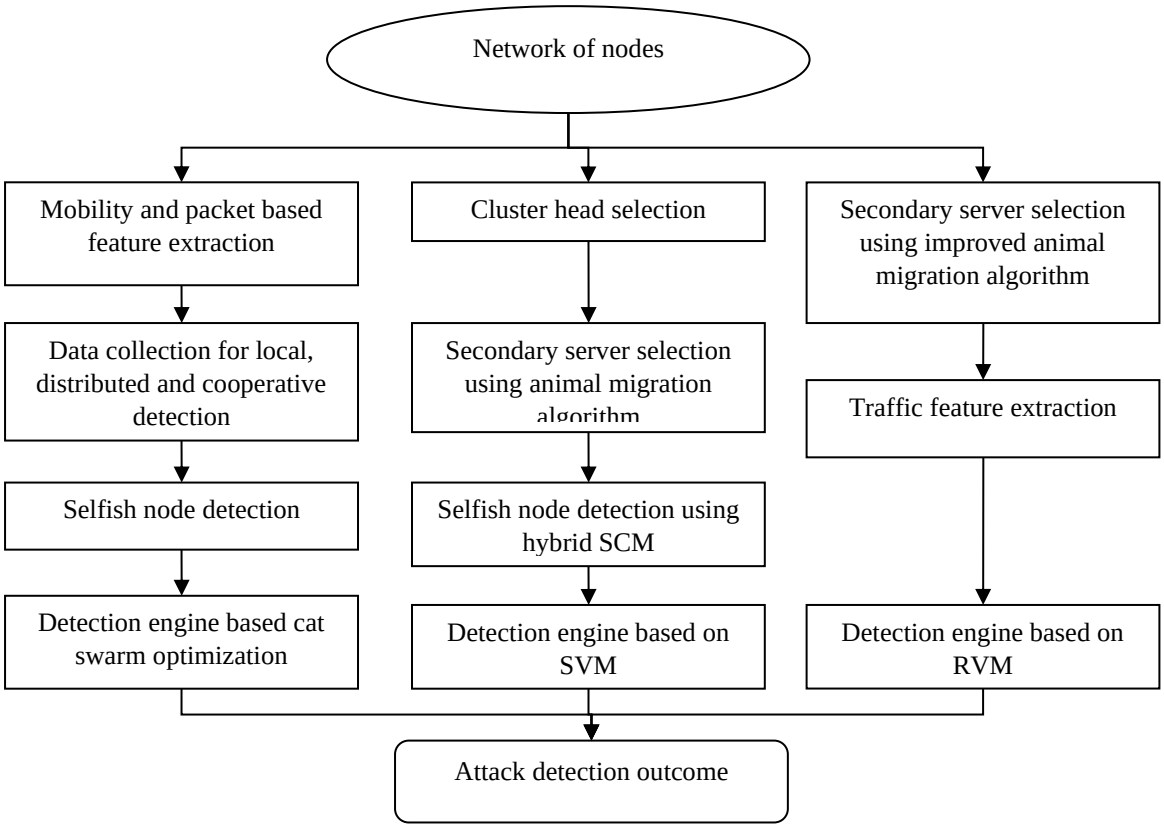


Figure 1. Overall processing flow of the research work

5.1. DISTRIBUTED AND COOPERATIVE INTRUSION DETECTION SYSTEM

The initial research introduced an innovative intrusion detection system employing a swarm optimization approach for mobile ad hoc networks. This system, utilizing Cat Swarm Optimization (CSO), aims to detect potential attacks, specifically focusing on identifying packet dropping attacks within these networks. Moreover, it optimizes the discovery of failed nodes by considering historical node data and neighboring node information. Before utilizing swarm optimization to assess sensor node trustworthiness and enhance the security of provenance data transmission, an extension to the secure provenance scheme is introduced. This extension incorporates Side Channel Monitoring (SCM), enabling the identification of packet

drop attacks orchestrated by malicious data forwarding nodes. The system effectively identifies the presence of selfish nodes and behaviors related to packet drops.

5.2. SECONDARY SERVER BASED DISTRIBUTED AND COOPERATIVE INTRUSION DETECTION SYSTEM

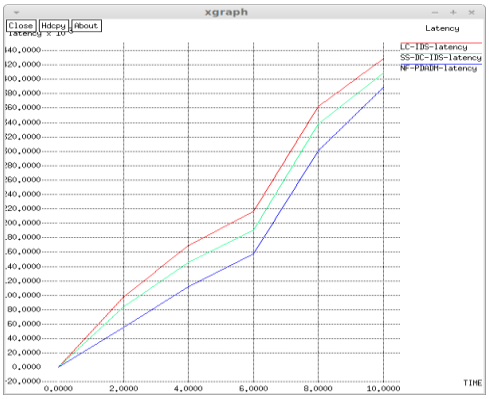
The second research initiative introduces the Secondary Server based Distributed and Cooperative Intrusion Detection System (SS-DC-IDS) specifically designed for detecting packet dropping attacks. Initially, the research focuses on the selection of the secondary server to improve intrusion attack detection and alleviate the computation burden on the primary server. The selection process involves using an animal migration algorithm, considering fitness values such as energy and bandwidth. The expansive network environment is segmented into smaller organizational units using a clustering algorithm, with each cluster appointing a cluster head. These heads collect attack features from their respective cluster members by monitoring their data transmission behaviors, employing hybrid side channel monitoring techniques. Before data transmission, these gathered features are relayed to the secondary server. The secondary server then processes this information using a Modified Support Vector Machine algorithm to determine the existence of intrusion attacks.

5.3. NODE FAILURE AWARE PACKET DROPPING ATTACK DETECTION METHOD

The third research effort introduces the Node Failure aware Packet Drop Attack Detection Method (NF-PDADM) designed for detecting packet dropping attacks. In this research, the impact of mobility factors is taken into account. Node failure, such as packet dropping attacks, can occur due to two scenarios: the presence of Intrusion Detection System (IDS) attackers or node movement. To differentiate between node failure resulting from node mobility and an IDS attack, a network learning mechanism based on packet transfers is employed, facilitated by neighborhood communication. Notably, mitigating node failure is achieved by providing necessary resources rather than re-establishing an alternative route path. The selection of the secondary server in this scenario utilizes an enhanced animal migration algorithm, considering objectives such as energy, bandwidth, and distance to the primary server.

6. RESULTS AND DISCUSSION

In this section, the NS-2 simulator is used to evaluate the performance of the proposed NF-PDADM. This simulation model network consisting of 100 nodes placed randomly within a 100 × 100 meters area.



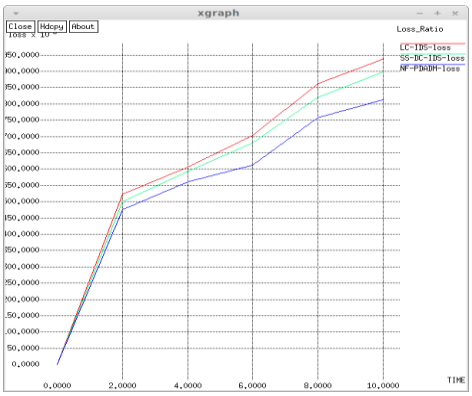
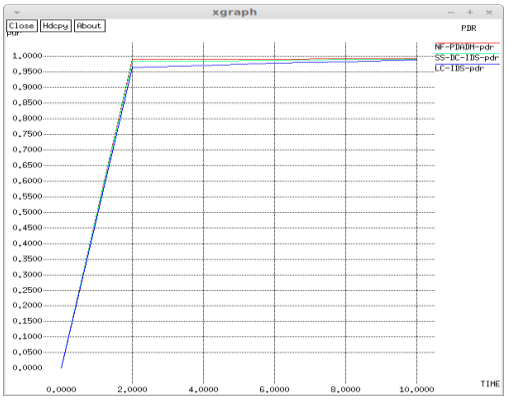


Figure 2 Mean packet latency Figure 3 Comparison of packet loss in different trust model



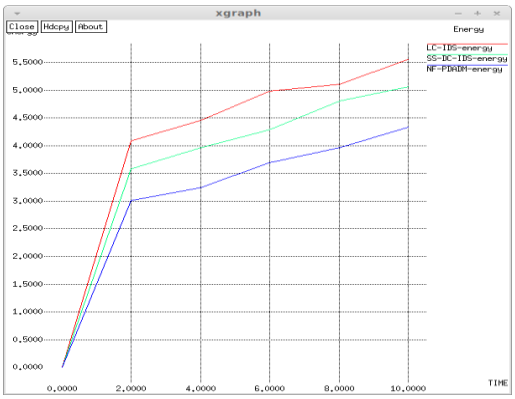
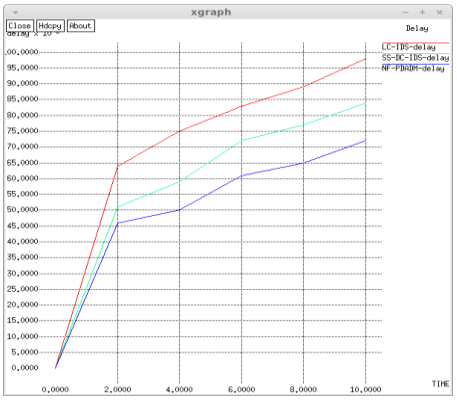


Figure 4 packet delivery ratio for different trust system Figure 5 energy consumption of different trust system



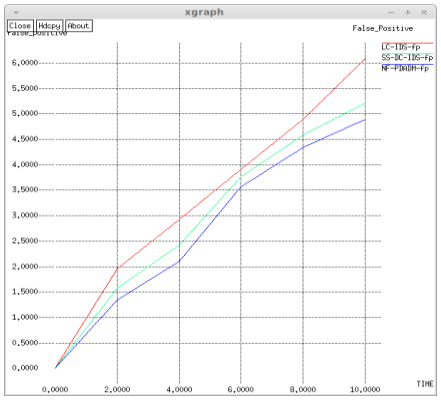


Figure 6 End-to-end delay comparisons Figure 7. False positive rate

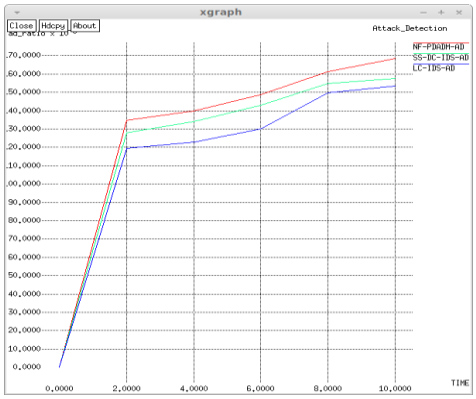


Figure 8. Attack probability comparison

From this comparison shown in the above figures it can be proved that the proposed method NF-PDADM tends to have better performance than the previous methodologies with accurate detection of attacker nodes.

7. CONCLUSION AND FUTURE WORK

The primary research concern in this study centers on packet dropping attacks. The first research work presents a novel intrusion detection system utilizing swarm optimization in binary form, specifically targeting packet dropping attacks in mobile ad hoc networks. In the second research endeavor, the initial focus lies on selecting a secondary server to bolster intrusion attack detection and alleviate the computational burden on the primary server. The secondary server learns attack information through a Modified Support Vector Machine algorithm, determining the presence of intrusion attacks. The third research work considers mobility factors, addressing node failures and packet dropping attacks, which may manifest in two scenarios: the presence of Intrusion Detection System (IDS) attackers or node movement.

The research work's overall analysis is conducted within the NS2 simulation environment, affirming that the proposed research technique outperforms existing methods. Numerical analysis establishes that the proposed Node Failure aware Packet Drop Attack Detection Method (NF-PDADM) achieves a 5.04% higher attack probability than SS-DC-IDS and an 11.5% higher attack probability than LC-IDS.

Future work will center on suggesting and testing further enhancements for metaheuristic approaches to feature selection problems, particularly within intrusion detection systems. The aim is to fine-tune network feature parameters to enhance intrusion detection rates. Additionally, the next steps involve experimenting

with the system using real-world network data, which can be generated and collected through various attack simulation tools encompassing a wide array of recently introduced attack definitions.

8. REFERENCES

1. Rajesh, M., & Gnanasekar, J. M. (2017). Path observation based physical routing protocol for wireless ad hoc networks. *Wireless Personal Communications*, *97*(1), 1267-1289.

2. Bujari, A., Calafate, C. T., Cano, J. C., Manzoni, P., Palazzi, C. E., & Ronzani, D. (2017). Flying ad-hoc network application scenarios and mobility models. *International Journal of Distributed Sensor Networks*, *13*(10), 1550147717738192.

3. Jiang, D., Li, W., & Lv, H. (2017). An energy-efficient cooperative multicast routing in multi-hop wireless networks for smart medical applications. *Neurocomputing*, *220*, 160-169.

4. Merlin, R. T., & Ravi, R. (2019). Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET. *Wireless Personal Communications*, *104*(4), 1599-1636.

5. Patel, K. S., & Shah, J. S. (2016). Study the effect of packet drop attack in AODV routing and MANET and detection of such node in MANET. In *Proceedings of International Conference on ICT for Sustainable Development* (pp. 135-142). Springer, Singapore.

6. Singh, U., Samvatsar, M., Sharma, A., & Jain, A. K. (2016, March). Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol. In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)* (pp. 1-6). IEEE.

7. Shah, R., Subramaniam, S., & Lekala Dasarathan, D. B. (2016). Mitigating Malicious Attacks Using Trust Based Secure-BEFORE Routing Strategy in Mobile Ad Hoc Networks. *Journal of computing and information technology*, *24*(3), 237-252.

8. Ahamad, T. (2016). Detection and defense against packet drop attack in MANET. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *7*(2), 2016.

9. Niyaz Hussain A M J and Dr. G Maria Priscilla. “A Comparative Survey on Traffic Analysis for Mobile AdHoc Network (MANET) Routing Protocol with Soft Computing Techniques.” IJARSE: International Journal of Advance Research in Science and Engineering, ISSN: 2319-8354, Volume-6 Issue-12, December 2017.

10. Niyaz Hussain A M J and Dr. G Maria Priscilla. "A Survey on Various Kinds of Anomalies Detection Techniques in the Mobile Adhoc Network Environment." Int. JS Res. CSE & IT 3.3 (2018): 1538-1541.

11. Niyaz Hussain A M J and Dr. G Maria Priscilla. “An Accurate Identification of Packet Dropping Attacks using Cat Swarm Optimization (CSO) to Ensure Better Intrusion Detection in Manet Environment.” International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-12, October 2020

12. Niyaz Hussain A M J and Dr. G Maria Priscilla. " Secondary Server Based Packet Dropping Attack Detection using Modified Support Vector Machine.” International Journal of Advanced Research in Engineering and Technology (IJARET) Volume 11, Issue 11, November 2020, pp. 356-372.

13. Hussain, AMJ Niyaz, and M. Priscilla. “Packet Drop Attack Detection Framework with the Concern of Node Failures and Intruders Presence.”, Solid State Technology, ISSN: 0038-111X, Volume: 63 Issue: 6, Publication Year: 2020