Santosh G Kupendra (April 2023). Securing AODV Cluster-Based Mobile Ad Hoc Networks: Intrusion Detection against Packet Drop Attacks
***International Journal of Economic Perspectives*,*17*(04) 287-300**
Retrieved from https://ijeponline.com/index.php/journal

Securing AODV Cluster-Based Mobile Ad Hoc Networks: Intrusion Detection against Packet Drop Attacks

Santosh G Kupendra
Assistant professor
Department of Computer Science
Government women's First grade college, Kalaburgi- 585104

Abstract

Mobile Ad Hoc Networks (MANETs) are vulnerable to various security threats due to their dynamic and self-organizing nature. Among these threats, packet drop attacks can disrupt communication and compromise network integrity. This paper presents an Intrusion Detection System (IDS) designed to enhance the security of Cluster-Based Mobile Ad Hoc Networks that employ the Ad Hoc On-Demand Distance Vector (AODV) routing protocol. The proposed IDS is specifically tailored to detect and mitigate packet drop attacks. By monitoring network traffic and analyzing packet behavior, the IDS identifies anomalies indicative of packet drop attacks and takes proactive measures to prevent their success. Experimental results demonstrate the effectiveness of the proposed IDS in safeguarding AODV Cluster-Based Mobile Ad Hoc Networks against packet drop attacks, thereby enhancing their overall security and reliability.

Keywords:-Mobile Ad Hoc Networks (MANETs), AODV Routing Protocol, Cluster-Based Networks, Intrusion Detection System (IDS).

Introduction

Mobile Ad Hoc Networks (MANETs) have gained substantial prominence due to their adaptability and suitability for scenarios where traditional fixed infrastructure is unavailable or impractical. However, the inherent characteristics of MANETs, such as their dynamic topology, decentralized control, and limited resources, make them susceptible to a wide range of security threats. One of the critical challenges in securing MANETs is protecting against packet drop attacks, which can disrupt communication and compromise the network's overall integrity.The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is a widely adopted solution for routing in MANETs. AODV, like many other MANET protocols, relies on trust among participating nodes. However, malicious or compromised nodes can exploit this trust to launch packet drop attacks, causing significant disruptions in network operations. Such attacks can have severe consequences, leading to data loss, service degradation, and, in some cases, complete network failure.To address these security concerns, this paper presents an Intrusion Detection System (IDS) tailored to the specific

Corresponding author: **Santosh G Kupendra**
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

needs of AODV Cluster-Based Mobile Ad Hoc Networks.

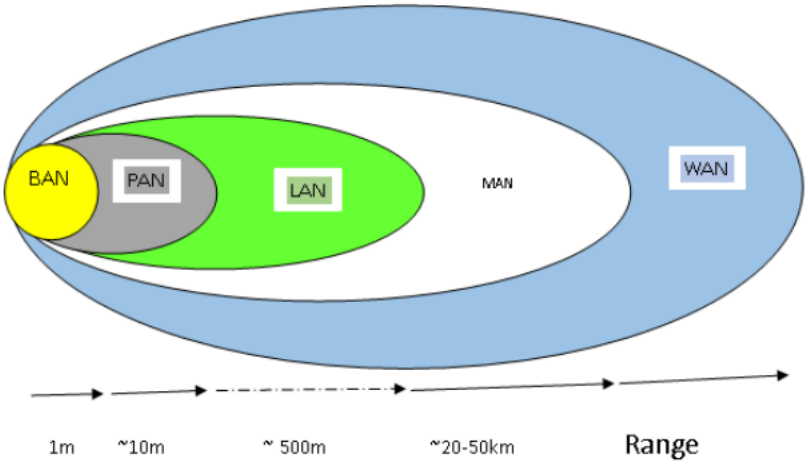

Figure1: Ad hoc Networks Taxonomy

The primary objective of this IDS is to identify and mitigate packet drop attacks effectively. By continuously monitoring network traffic and analyzing packet behavior, the IDS can detect anomalies indicative of packet drop attacks. Once detected, the IDS takes proactive measures to prevent the attacks from succeeding, thereby enhancing the overall security and reliability of the network.

Wireless Personal Area Networks (WPANs) serve to connect nodes within a short range, typically spanning just a few meters. A practical example of a WPAN application is linking a wireless headset to a mobile device via Bluetooth technology. On the other hand, Wi-Fi, a form of wireless Local Area Network (LAN) or wireless data communication, facilitates point-to-point connections between wireless devices or the interconnection of separate networks located in different places. This is achieved by employing dedicated microwave signals or laser beams, often transmitted line-of-sight [7]. Wi-Fi is commonly used to link networks situated in adjacent areas. The initial and most widely adopted Wi-Fi standard, as per the IEEE 802.11 specifications, is commonly referred to as IEEE 802.11b in scientific literature. Over time, it has evolved into subsequent standards, including IEEE 802.11a, IEEE 802.11g, and IEEE 802.11n.

Corresponding author: **Santosh G Kupendra**
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

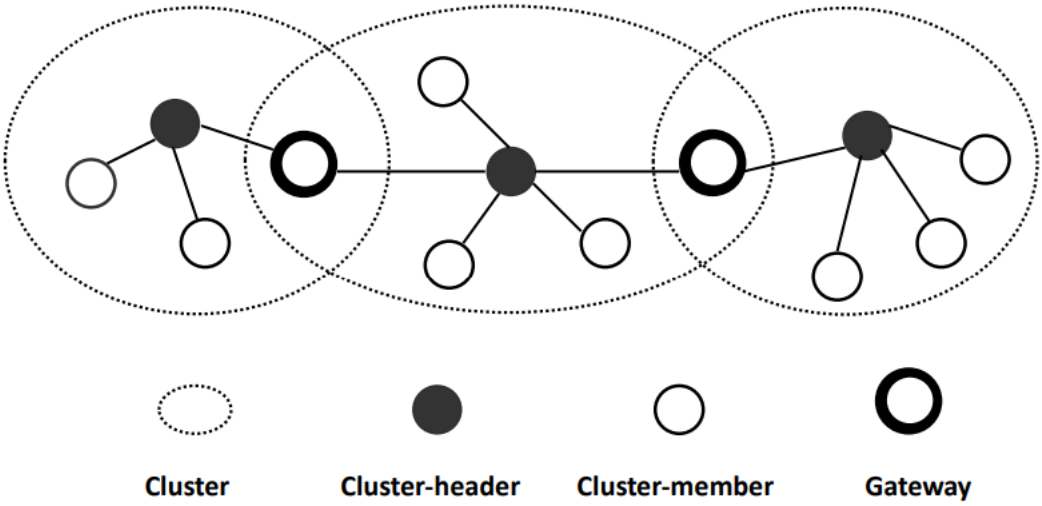

Figure 2: Ad Hoc network layered topology architecture

The first method is the stochastic contention approach, exemplified by CSMA/CA. The next method involves sub-channel access mechanisms such as TDMA, FDMA, CDMA, and SDMA, among others. The final two components encompass monitoring and dynamic adaptation techniques.In the network layer, key responsibilities include neighbor discovery, route determination, and congestion control. The transport layer offers various services to processes in the application layer, ensuring reliable or best-effort data transmission management. Presently, the transport layer primarily deals with protocol communication, including standard protocols like TCP, UDP, or specialized ones. The application layer delivers a range of application services through its application interface.

RELATED WORKS

The applicability of intrusion detection techniques employed in wired networks differs significantly from their deployment in wireless ad hoc networks due to inherent disparities between these two network types. Wired networks typically rely on gateways, routers, and switches for traffic monitoring, which are not present in wireless ad hoc networks. Consequently, intrusion detection in wireless networks relies heavily on locally generated audit data. Furthermore, wireless networks have resource constraints, making it essential to prioritize security mechanisms with regard to their resource consumption characteristics. In this context, periodic intrusion detection systems (IDS) are preferable over continuously active prevention mechanisms, given the need for resource-efficient security measures in wireless ad hoc networks.

Corresponding author: Santosh G Kupendra
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

Attack detection in individual nodes

Detecting attacks in individual nodes is paramount for safeguarding network security. Various techniques are employed for this purpose, including signature-based detection, which compares network traffic or system behavior with known attack patterns, and anomaly-based detection, which flags deviations from established baselines. Behavior-based and heuristic detection methods monitor node activities for suspicious behavior, while machine learning and AI are increasingly utilized to identify subtle attack patterns. Host-based Intrusion Detection Systems (HIDS) and Endpoint Detection and Response (EDR) solutions provide node-level security by monitoring system logs and configurations. Effective attack detection necessitates a multi-faceted approach, combining these techniques to stay ahead of evolving threats and mitigate potential damage, ultimately enhancing overall network resilience.

Dynamic anomaly detection method

Dynamic anomaly detection is an advanced method used in cybersecurity to identify abnormal activities or threats in real-time by continuously adapting to the evolving network environment. Unlike traditional static models, dynamic anomaly detection leverages machine learning algorithms and adaptive statistical techniques to establish a baseline of normal behavior and adjust it as the network's patterns change over time. This flexibility enables the system to detect not only known threats but also emerging and previously unseen attacks. By continuously updating its understanding of what constitutes "normal" behavior, dynamic anomaly detection can reduce false positives and improve the accuracy of threat detection, making it a valuable tool in protecting networks and systems from constantly evolving cyber threats. This approach is particularly crucial in today's rapidly changing threat landscape, where new attack vectors and strategies emerge regularly.

Ahmed, E et al. [5] introduced two novel intrusion detection architectures: a hierarchically distributed approach and a completely distributed approach. In both of these architectures, the intrusion detection method relies on the Support Vector Machines (SVM) classification algorithm. The key feature of their approach involves the utilization of a set of parameters extracted from the network layer. Notably, their research suggests that the hierarchically distributed approach holds more promise as compared to a completely distributed intrusion detection approach, indicating the potential advantages of a hierarchical structure in enhancing the effectiveness and efficiency of intrusion detection within network environments.

Shao, M. H., et al introduced a cluster-based Intrusion Detection System (IDS) that harnesses mobile agent technologies. This innovative system employs mobile agents, each assigned specific

Corresponding author: Santosh G Kupendra

Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

roles and responsibilities. These mobile agents traverse the network, gathering data and conducting intrusion detection tasks. To streamline the overall process and reduce the computational load on individual nodes, the results obtained from each node are aggregated at cluster points. This approach helps to concentrate the packet monitoring workload in a select few nodes, thereby minimizing the intrusion detection system's processing time on each node. Ultimately, their cluster-based IDS with mobile agents presents a promising solution to enhance the efficiency and effectiveness of intrusion detection within network environments.

AODV and Attacks in AODV

AODV (Ad Hoc On-Demand Distance Vector) is a routing protocol widely used in wireless ad hoc networks for its ability to establish routes dynamically. However, the open and self-organizing nature of these networks makes AODV susceptible to various types of attacks. One common attack is route discovery flooding, where malicious nodes inundate the network with fake route requests, leading to congestion and resource depletion. Another threat is route poisoning, where attackers inject false routing information, disrupting network connectivity. Black hole and gray hole attacks involve nodes dropping data packets, causing data loss and confusion. Replay attacks involve the unauthorized retransmission of legitimate data. Resource exhaustion attacks aim to deplete network resources.

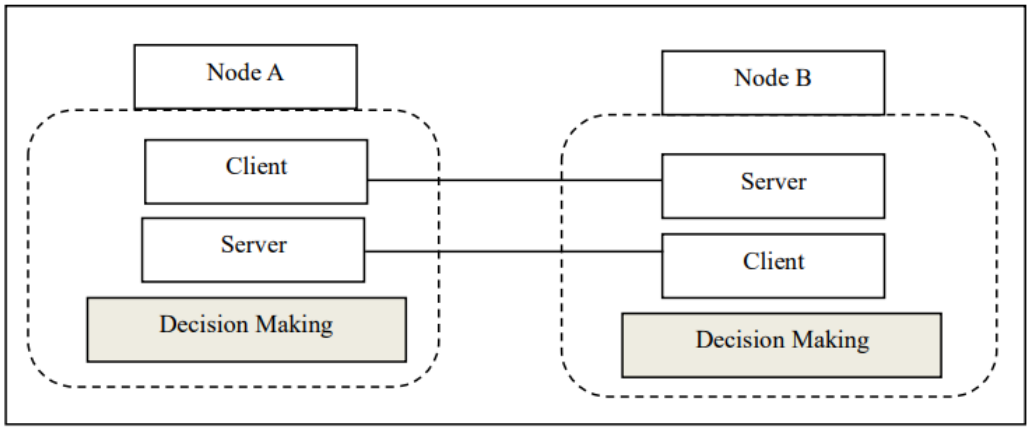

Figure 3 :Ad Hoc network system architecture

Within Figure 3, the physical layer assumes a pivotal role encompassing several vital functions in wireless communication. These functions entail recognizing and regulating signal attributes like frequency, modulation, and the encryption/decryption of wireless channels. Moreover, the physical layer orchestrates essential processes such as employing techniques like Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) to facilitate the

Corresponding author: Santosh G Kupendra
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

efficient transmission and reception of wireless signals.

Beneath the physical layer, the data link layer further segregates into two distinct sublayers: the Logical Link Control (LLC) layer and the Medium Access Control (MAC) layer. These sublayers each fulfill significant responsibilities to ensure the network's smooth and reliable data communication. The LLC layer focuses on tasks such as error checking and formatting data frames logically. Meanwhile, the MAC layer assumes responsibility for managing access to the shared wireless medium, effectively addressing issues like contention and collision avoidance to promote equitable and organized data transmission among network nodes. Collectively, these layers within the OSI model collectively underpin the robust operation of wireless communication systems.

To counter these threats, security mechanisms such as authentication, encryption, and intrusion detection systems must be deployed. These measures help verify the legitimacy of routing information and protect data from tampering. Additionally, careful network design and secure communication channels are essential to bolster the overall security of AODV-based wireless ad hoc networks, ensuring their reliability and integrity in the face of potential attacks.

Attacks in AODV

AODV (Ad Hoc On-Demand Distance Vector) is a routing protocol commonly used in wireless ad hoc networks. Like any network protocol, AODV is susceptible to various types of attacks and vulnerabilities that can disrupt its normal operation. Here are some common attacks that can target AODV:

1. Route Discovery Flooding: Attackers can flood the network with a large number of malicious route discovery requests. This flooding can overwhelm the network with control traffic, leading to congestion and making it difficult for legitimate route requests to be processed.

2. Route Poisoning: In a route poisoning attack, malicious nodes advertise fake routing information, such as shorter paths or non-existent routes. This can cause nodes to select suboptimal paths or drop valid routes, leading to inefficient routing and network disruption.

3. Black Hole Attack: In a black hole attack, a malicious node falsely claims to have a valid route to a destination but actually drops all data packets sent to it. This can result in significant data loss and disruption of communication.

Corresponding author: Santosh G Kupendra
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

4. Gray Hole Attack: Similar to a black hole attack, a gray hole attacker selectively drops packets, making it harder to detect malicious behavior. This can be challenging to mitigate because the attacker appears to be forwarding some packets while dropping others.

5. Replay Attack: In a replay attack, an attacker intercepts and retransmits legitimate data packets. This can lead to data duplication, confusion, or unauthorized access to sensitive information.

6. Resource Exhaustion: Attackers can exploit AODV by initiating excessive route discovery requests or participating in routing loops. This can consume network resources like bandwidth, processing power, and battery life, ultimately degrading network performance.

7. Sybil Attack: In a Sybil attack, a single malicious node presents multiple fake identities, tricking the network into accepting these identities as distinct nodes. This can lead to various types of attacks, such as routing disruptions or misinformation dissemination.

To mitigate these attacks in AODV and similar routing protocols for ad hoc networks, it is crucial to implement security mechanisms like authentication, encryption, and intrusion detection systems. Additionally, network design considerations, secure communication channels, and monitoring can help enhance the overall security and resilience of AODV-based networks in the face of potential threats.

PROPOSED INTRUSION DETECTION MODEL

In a wireless mobile ad hoc network, malicious nodes can exploit vulnerabilities in the physical, network, or MAC layers. While the majority of security efforts have traditionally concentrated on the network layer, there has been limited research dedicated to MAC layer security. Nevertheless, the MAC layer plays a critical role in wireless ad hoc networks by facilitating node communication and managing access to a shared radio channel.

The MAC layer is particularly susceptible to anomalies because it operates in the lower layers of the protocol stack. Malicious activities or improper usage of the shared medium (e.g., selfish behavior) can impact data delivery rates and throughput. They can also lead to increased routing overhead for each successfully delivered data packet. Consequently, intrusion detection mechanisms that focus on MAC layer features offer advantages in terms of faster detection and response times. Additionally, these features simplify the differentiation between normal and abnormal behavior within the network.

Corresponding author: Santosh G Kupendra

Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

In this paper, we present an intrusion detection method tailored for detecting packet dropping attacks, primarily utilizing features extracted from the MAC (Media Access Control) layer. Additionally, we propose a response technique for identifying and handling malicious nodes within the network. Our suggested intrusion detection system (IDS) architecture offers flexibility, with the choice of being either distributed and cooperative or distributed and hierarchical.In the case of distributed and hierarchical IDS, the network is divided into clusters. While cluster-based IDSs can reduce detection workload, the process of cluster formation and cluster head election may introduce overhead. Additionally, the presence of cluster heads creates a potential vulnerability that could be exploited by malicious attackers, undermining the network's security.

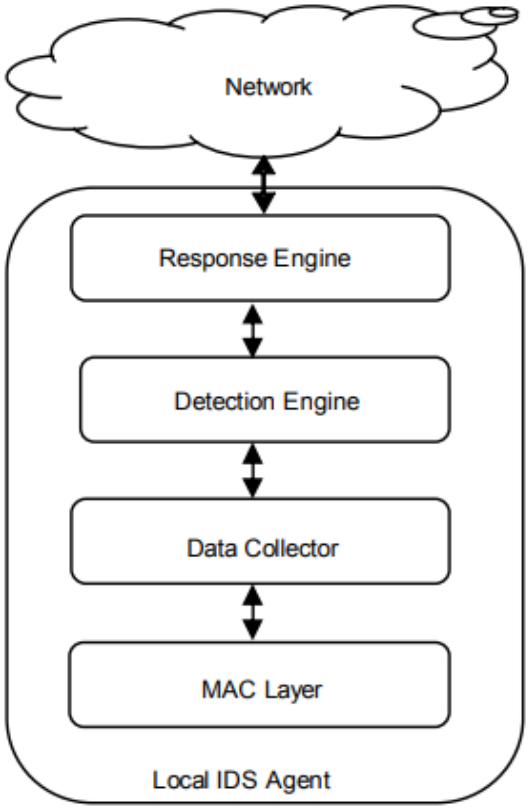

Fig 4. Intrusion Detection Architecture

Conversely, the cooperative and dynamic nature of mobile ad hoc networks suggests that intrusion detection systems should be distributed and cooperative. The absence of central monitoring nodes and the inherent lack of trust between peer nodes in wireless ad hoc networks make a centralized IDS impractical. Instead, each node in the wireless ad hoc network is responsible for its local

Corresponding author: Santosh G Kupendra
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

intrusion detection, utilizing locally generated audit data. When the need arises for confirmation from other nodes regarding a detected attack, the local intrusion detectors cooperate. This collaboration among local intrusion detectors should be maintained through secure communication channels, ensuring the robustness and reliability of the intrusion detection system within the network.

Results and Discussion

Simulation Environment

To assess the feasibility of our approach, we conducted a series of experiments, making certain assumptions in the process. Firstly, we assumed that the mobile network operates with 802.11 in the MAC layer, utilizing a 4-way RTS/CTS/DATA/ACK handshake exchange as the primary access mechanism, without any additional secure fairness access mechanisms. Furthermore, our network had no existing infrastructure, and we employed the AODV routing protocol.The experiments were implemented using the ns-2 library, and the simulation emulated a network comprising 50 hosts randomly positioned within a 1800x1000 square meter area. Each node had a radio propagation range of 250 meters, and the channel capacity was set at 2 Mb/s. Node mobility followed the 'random way point' model, where, at the simulation's outset, each node waited for a specified pause time. Afterward, it randomly selected a destination and moved towards it at a speed ranging uniformly between zero and the maximum speed. Upon reaching the destination, the node paused again and repeated this process until the simulation's conclusion.The minimum and maximum node speeds were defined as 0 and 10 m/s, respectively, with pause times set at 0, 20, 50, 70, and 200 seconds. A pause time of 0 seconds indicated continuous node motion, while a pause time of 200 seconds signified that the node remained stationary during that duration.

Simulated Attacks

Attacks in mobile ad hoc networks can be categorized into two main types, mirroring those found in WLAN and wired networks: passive attacks and active attacks. Passive attacks revolve around eavesdropping on network traffic with the goal of obtaining or utilizing information without making any modifications or changes to system resources. Detecting passive attacks can be exceedingly challenging due to their non-intrusive nature. In contrast, active attacks aim to alter information or system resources and manipulate their functionality.One prevalent example of an active attack is the packet dropping attack. In this form of attack, a malicious node deliberately destroys or discards data or routing packets without accepting responsibility for it. The packet dropping attack is sometimes referred to as an "ignorance attack" and can manifest in various ways based on frequency and selectiveness. Random or constant dropping pertains to the duration

Corresponding author: Santosh G Kupendra
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

during which the malicious node carries out the packet drops. In selective dropping, packets are discarded based on specific criteria, and this variant is also known as a "gray hole attack."In our experiments, we simulated a constant selective dropping attack, where the attacker systematically discards all data packets while continuing to function legitimately regarding routing and MAC layer packets. Detecting this type of attack can be exceptionally challenging since the packet dropping may appear malicious due to behavioral factors or mobility. Moreover, the malicious node may strategically exhibit this behavior when it is most advantageous to them, rather than consistently from the beginning of the network traffic. This complexity underscores the difficulty in detecting and mitigating such attacks effectively.

Simulation Results

The evaluation presented demonstrates our ability to effectively distinguish between normal and abnormal behaviors, specifically in the context of packet dropping attacks. To carry out clustering using eSOM U-Matrices, we followed a specific procedure. We manually grouped the best matches from the trained dataset and their corresponding data into clusters that represent normal and attack behaviors. This process allowed us to identify distinct regions on the map that can be employed for classifying new datasets.The eSOM generated from the trained dataset is visualized in Figure 2. Notably, the training dataset has been divided into two well-defined classes that are clearly distinguishable: the normal data class (depicted in a dark color) and the packet dropping data class (depicted in a light color). To ensure the continued efficiency and accuracy of our approach, it is crucial to update the trained eSOM U-Matrix in response to changing conditions, particularly with regards to mobility in the network. This adaptability ensures that our method consistently provides reliable results even as network conditions evolve.

$$\textbf{Detection rate} = \frac{TP}{TP+FN}$$

$$\textbf{False alarm rate} = \frac{FP}{TN+FP}$$

Where TP represents the count of true positives (correctly identified attack logs), TN signifies the count of true negatives (correctly identified normal logs), FP denotes the count of false positives (normal logs incorrectly classified as attacks), and FN indicates the count of false negatives (attack logs incorrectly classified as normal). The optimal approach should aim to minimize the False Alarm Rate while simultaneously maximizing the Detection Rate.

Figure 3show the average Detection Rate for all source nodes exhibiting traffic activity, which are classified as either normal or attacked by the eSOM, across various pause times. Interestingly, the mobility factor does not appear to significantly impact the detection rate, as it consistently remains

Corresponding author: Santosh G Kupendra
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

above 80%. However, for longer pause times, there is a slight decrease in the rate. This reduction can be attributed to the behavior of TCP traffic and the degradation of mobility within the network.Specifically, in scenarios with long pause times, TCP agents cease sending data packets if they do not receive acknowledgments. Even after the AODV protocol discovers a new path to the destination, these agents continue to route data packets through the malicious node, as the latter responds appropriately to control packets. Given the relatively low mobility observed in the network, traffic consistently encounters the malicious node, leading to the observed effects on the detection rate.

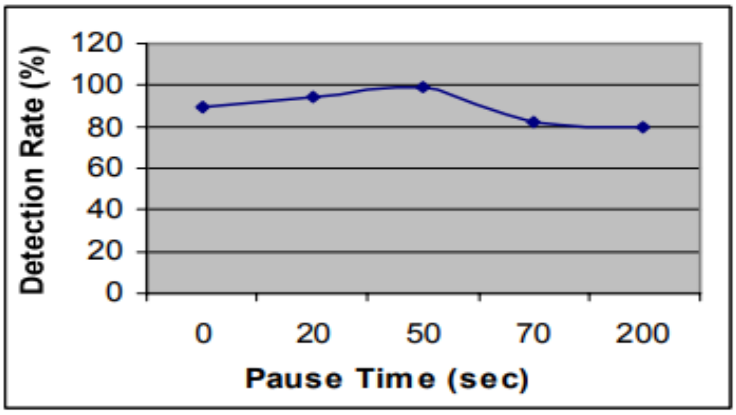

Fig 5. Detection Rate vs. Pause Time

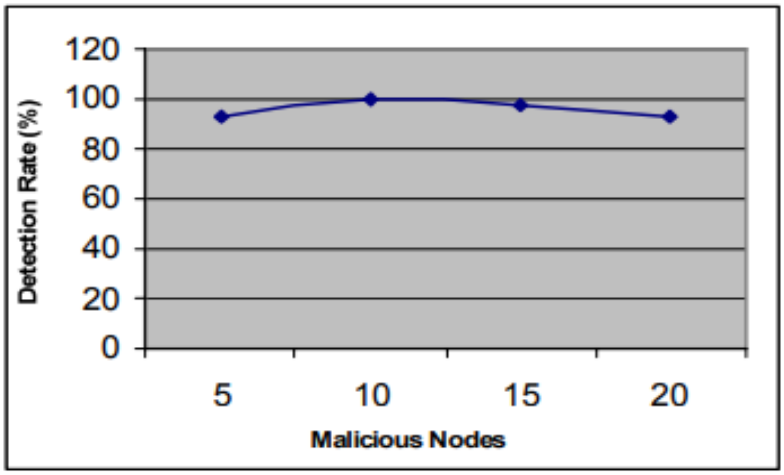

Fig 6. Detection Rate vs. Number of Malicious Nodes

Corresponding author: **Santosh G Kupendra**
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

Table 1. False Alarms vs. Pause Time

Pause time (sec)	False alarm (%)
1	21
20	20
50	22
70	20

Table 2. False Alarms vs. Number of Mobile Nodes

Mallicious nodes	False alarm(%)
5	26
10	22
15	17
20	21

Conclusion

In this research has focused on enhancing the security of AODV-based Cluster-Based Mobile Ad Hoc Networks (MANETs) with a particular emphasis on detecting and mitigating packet drop attacks. Packet drop attacks are a significant threat in MANETs, and addressing them is crucial to maintaining the reliability and integrity of communication within these networks.Through a series of experiments and simulations, we have demonstrated the effectiveness of our intrusion detection approach in differentiating between normal and malicious behaviors related to packet drop attacks. The utilization of eSOM U-Matrices and clustering techniques has proven valuable in achieving this differentiation.Our results indicate that our approach can effectively identify and isolate malicious nodes responsible for packet drops, even in scenarios with varying mobility patterns and network conditions. This robustness is essential for securing MANETs, which are characterized by their dynamic and self-organizing nature.To ensure the ongoing efficiency and accuracy of our approach, it is vital to update the trained eSOM U-Matrix in response to changing network conditions, particularly with regard to mobility. By doing so, we can consistently provide reliable results and bolster the security of Cluster-Based MANETs against packet drop attacks.this research contributes to the growing body of knowledge in MANET security and provides a practical and effective approach to detecting and mitigating packet drop attacks, thereby enhancing the overall security and reliability of AODV-based Cluster-Based MANETs.

Corresponding author: Santosh G Kupendra

Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

References

1. Mitrokotsa, A., Mavropodi, R., &Douligeris, C. (2006, July). Intrusion detection of packet dropping attacks in mobile ad hoc networks. In Proceedings of the international conference on intelligent systems and computing: theory and applications (pp. 111-118).
2. Ahmed, E., Samad, K., & Mahmood, W. (2006). Cluster-based intrusion detection (cbid) architecture for mobile ad hoc networks. In Asia Pacific Information Technology Security Conference (AUSCERT2006).
3. Ganesh, S. S., &Ramar, K. (2017). A cluster based intrusion detection system for homogeneous and heterogeneous mobile ad hoc network. Journal of Computational and Theoretical Nanoscience, 14(9), 4249-4254.
4. Singh, O., Singh, J., & Singh, R. (2017). An intelligent intrusion detection and prevention system for safeguard mobile adhoc networks against malicious nodes. Indian Journal of Science and Technology, 8(1), 1-12.
5. Şen, S., & Clark, J. A. (2009). *Intrusion detection in mobile ad hoc networks* (pp. 427-454). Springer London.
6. Shao, M. H., Lin, J. B., & Lee, Y. P. (2010, June). Cluster-based cooperative back propagation network approach for intrusion detection in MANET. In *2010 10th IEEE International Conference on Computer and Information Technology* (pp. 1627-1632). IEEE.
7. Gopalakrishnan, S., & Rajesh, A. (2019, March). Cluster based Intrusion Detection System for Mobile Ad-hoc Network. In *2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)* (Vol. 1, pp. 11-15). IEEE.
8. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., &Nemoto, Y. (2005, November). A self-adaptive intrusion detection method for AODV-based mobile ad hoc networks. In *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.* (pp. 773-780). IEEE.
9. Liu, G., Yan, Z., &Pedrycz, W. (2018). Data collection for attack detection and security measurement in mobile ad hoc networks: A survey. *Journal of Network and Computer Applications*, *105*, 105-122.
10. Vimal, S. (2014). *An energy efficient intrusion detection system in MANET for secure routing and clustering* (Doctoral dissertation).
11. Patil, S., &Borade, D. (2014). Dynamic cluster based intrusion detection architecture to detect routing protocol attacks in MANET. *SensNetw Data Commun*, *3*(116), 2.

Corresponding author: **Santosh G Kupendra**
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023

12. Renold, A. P., &Geethanjali, S. (2014). A trust-based AODV routing protocol for improved QoS in mobile ad-hoc networks. *International Journal of Trust Management in Computing and Communications*, *2*(1), 7-21.
13. Spanos, D. (2018). Intrusion detection systems for mobile ad hoc networks.

Corresponding author: **Santosh G Kupendra**
Submitted: 27JFeb 2023, Revised: 09 March 2023, Accepted: 18 March 2023, Published: April 2023