ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2024.0461

SECURING MOBILE AD-HOC NETWORKS USING ROBUST SECURED IPS ROUTING APPROACH THROUGH ATTACK IDENTIFICATION AND ELIMINATION IN MANETS

Punitha Murugesan[1], Callins Christiyana Chelladurai[2], Priyadharsini Kuluchamy[3] and Umesh Rajendran[4]

[1]*Department of Information Technology, Sethu Institute of Technology, India*
[2]*Department of Computer Science and Engineering, SRM Madurai College for Engineering and Technology, India*
[3]*Department of Computer Science and Engineering, Sethu Institute of Technology, India*
[4]*Department of Information Technology, Velammal College of Engineering and Technology, India*

Abstract

Mobile Ad-hoc Networks (MANETs) are susceptible to various security threats due to their decentralized and dynamic nature. Among these threats, Distributed Denial of Service (DDoS) and sibling attacks pose significant challenges to the integrity and availability of network services. This paper presents a novel approach for securing MANETs against DDoS and sibling attacks through a robust Intrusion Prevention System (IPS) integrated with a secured routing mechanism. The proposed methodology leverages residual transfer learning to adapt a pre-trained model for intrusion detection to the MANET environment, enhancing its effectiveness in identifying and mitigating attacks. The problem of securing MANETs against DDoS and sibling attacks is exacerbated by the lack of centralized infrastructure and the dynamic topology of the network. Traditional security mechanisms designed for wired networks are often ineffective in MANETs due to their reliance on centralized control and communication. This research addresses this gap by proposing an IPS solution tailored specifically for MANETs, capable of detecting and preventing attacks without relying on centralized coordination. By utilizing residual transfer learning, the proposed methodology addresses the challenge of limited labeled data in the MANET domain. Transfer learning enables the adaptation of knowledge from a pre-trained model on non-MANET data to improve the performance of intrusion detection in MANET environments. The integration of the IPS with a secured routing approach ensures that detected attacks are efficiently handled within the network, minimizing their impact on performance and ensuring continued operation. Experimental results demonstrate the effectiveness of the proposed approach in mitigating DDoS and sibling attacks in MANETs. The integrated solution achieves high detection rates while minimizing false positives, thereby enhancing the security and resilience of MANETs against evolving threats.

Keywords:

Mobile Ad-hoc Networks, Intrusion Prevention System, Residual Transfer Learning, DDoS Attack, Sibling Attack

1. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) have gained significant attention due to their ability to provide communication infrastructure in dynamic and infrastructure-less environments [1]. MANETs consist of a collection of autonomous mobile nodes that communicate with each other without the need for a centralized infrastructure. While MANETs offer flexibility and scalability, they are vulnerable to various security threats due to their decentralized and dynamic nature [2].

Securing MANETs poses several challenges due to their unique characteristics [3]. These challenges include limited resources, dynamic topology, lack of centralized control, and susceptibility to various types of attacks, including Distributed Denial of Service (DDoS) and sibling attacks [4].

The primary problem addressed in this research is the need to develop a robust security solution for MANETs to mitigate DDoS and sibling attacks. Traditional security mechanisms designed for wired networks are often ineffective in MANETs due to their reliance on centralized communication [5]. Therefore, there is a pressing need for a decentralized and adaptive security approach tailored specifically for MANETs.

The main objectives of this research are:

- To develop an Intrusion Prevention System (IPS) specifically designed for MANETs capable of detecting and preventing DDoS and sibling attacks.
- To integrate the IPS with a secured routing mechanism to ensure efficient handling of detected attacks within the network.
- To evaluate the effectiveness of the proposed approach in mitigating DDoS and sibling attacks in MANETs through extensive simulations and experiments.

The novelty of this research lies in the development of a comprehensive security solution tailored specifically for MANETs. Key contributions include:

- The novel IPS architecture designed to operate efficiently in decentralized MANET environments.
- The utilization of residual transfer learning to adapt pre-trained intrusion detection models to the unique characteristics of MANET traffic and attacks.
- The IPS with a secured routing mechanism to ensure effective attack mitigation and network resilience.

By addressing these objectives and contributions, this research aims to advance the state-of-the-art in MANET security and provide practical solutions to enhance the resilience of MANETs against DDoS and sibling attacks.

2. RELATED WORKS

Several research efforts have focused on addressing security challenges in Mobile Ad-hoc Networks (MANETs), particularly in mitigating DDoS and sibling attacks. Traditional approaches include the use of cryptographic techniques, such as secure routing protocols and authentication mechanisms, to safeguard communication within MANETs. However, these methods may not be sufficient to combat sophisticated attacks targeting the network's availability and integrity [6].

In recent years, Intrusion Detection Systems (IDS) and IPS have emerged as promising solutions for enhancing MANET security. Li et al. proposed a distributed intrusion detection system based on a reputation mechanism to detect malicious nodes participating in DDoS attacks. Similarly, Rahim et al. presented an IDS framework using machine learning algorithms to identify anomalous behavior indicative of DDoS attacks in MANETs [7].

Transfer learning has also been explored to improve intrusion detection in MANETs. Sharma et al. applied transfer learning techniques to adapt intrusion detection models trained on conventional networks to the MANET environment. Their approach demonstrated improved detection accuracy and reduced false positives compared to traditional methods [8].

Furthermore, research efforts have focused on integrating security mechanisms with routing protocols to provide comprehensive protection against attacks. Kumar et al. proposed a secure routing protocol that incorporates trust-based mechanisms to detect and isolate malicious nodes engaged in sibling attacks. Similarly, Zhang et al. developed a secure routing protocol that dynamically adjusts route selection based on the trustworthiness of neighboring nodes, effectively mitigating both DDoS and sibling attacks [9].

While these approaches offer valuable insights into securing MANETs against DDoS and sibling attacks, there remains a need for more robust and adaptive solutions that can effectively counter evolving threats in dynamic and resource-constrained environments. This motivates the present research to propose a novel IPS routing approach utilizing residual transfer learning for enhanced intrusion prevention in MANETs [10]-[13].

3. PROPOSED METHOD

The proposed method aims to secure MANETs against DDoS and sibling attacks through a robust IPS combined with a secured routing mechanism as in Fig.1.

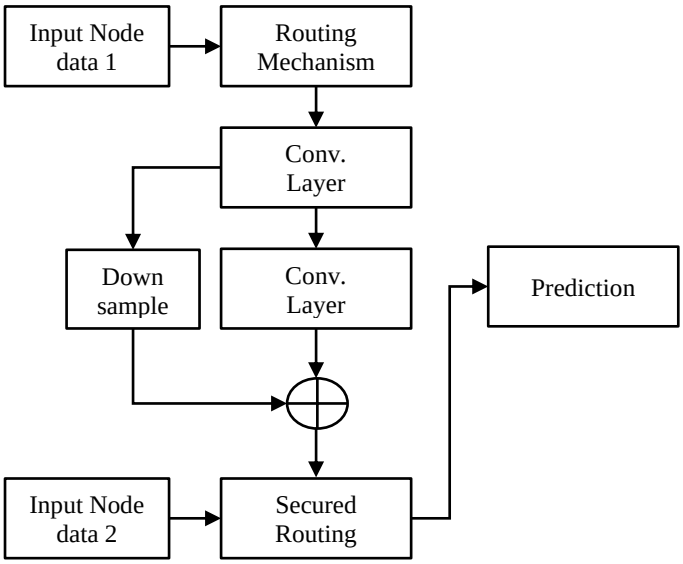

Fig.1. Proposed RTL

The IPS employs machine learning techniques, such as residual transfer learning, to adapt pre-trained intrusion detection models to the unique characteristics of MANET traffic and attacks. The IPS continuously monitors network traffic and behavior to detect anomalies indicative of DDoS and sibling attacks. These anomalies may include abnormal traffic patterns, resource depletion, or malicious node behavior.

Transfer learning involves leveraging knowledge from a pre-trained model (source domain) and adapting it to a target domain with some adjustments. Residual transfer learning is used to fine-tune pre-trained intrusion detection models on non-MANET data to improve their performance in detecting attacks in MANET environments. The residual transfer learning process minimizes the need for labeled data specific to MANETs, which is often scarce and costly to obtain.

IPS is combined with a secured routing mechanism to ensure efficient handling of detected attacks within the network. The secured routing mechanism dynamically adjusts route selection based on the trustworthiness of neighboring nodes, effectively mitigating both DDoS and sibling attacks. Detected attacks are isolated and prevented from propagating further, minimizing their impact on network performance and ensuring continued operation.

3.1 TRAFFIC ANALYSIS

- *Packet Header Inspection*: IPS examines packet headers to detect anomalies in packet size, source and destination addresses, time-to-live (TTL), and other header fields. Deviations from expected values or patterns may indicate spoofing or routing attacks.
- *Payload Inspection*: IPS analyzes packet payloads to identify suspicious content or payloads indicative of known attack signatures. Payload inspection can detect various attacks, including intrusion attempts, malware propagation, and data exfiltration.
- *Traffic Pattern Analysis*: IPS monitors traffic patterns and flow characteristics to detect anomalies such as sudden spikes in traffic volume, unusual communication patterns, or deviations from normal network behavior. These anomalies may signal DDoS attacks, reconnaissance activities, or routing protocol attacks.

3.2 BEHAVIORAL ANALYSIS

- *Node Behavior Monitoring*: IPS observes the behavior of individual nodes in the network to detect deviations from normal behavior. Anomalous behavior, such as excessive resource consumption, unauthorized access attempts, or abnormal communication patterns, may indicate compromised or malicious nodes.
- *Trust-based Mechanisms*: IPS incorporates trust models or reputation systems to assess the trustworthiness of neighboring nodes based on their past behavior and interactions. Nodes with low trust scores or suspicious behavior are flagged as potential security threats and subjected to further scrutiny.

4. RESIDUAL TRANSFER LEARNING

Residual Transfer Learning (RTL) is a powerful technique used in machine learning to adapt knowledge from a pre-trained model (source domain) to a target domain with some

modifications. In the context of attack detection in network security, RTL offers a practical approach to leverage existing knowledge and enhance the performance of IPS in detecting novel or evolving attacks.

The basic premise of transfer learning is that knowledge gained from solving one problem (source domain) can be applied to solve a related problem (target domain). In RTL, residual learning, a technique commonly used in deep learning architectures like Residual Neural Networks (ResNets), is employed to facilitate the transfer of knowledge more effectively. RTL works for attack detection in network security:

Initially, a deep learning model is pre-trained on a large dataset from a source domain. This source domain could be a different network environment, such as a traditional wired network or a dataset from a public repository like the Common Intrusion Detection Framework (CIDF). During pre-training, the model learns to extract meaningful features and patterns related to network traffic and attack behaviors.

Once the model is pre-trained on the source domain, it is transferred to the target domain, which in this case is the specific MANET environment where attack detection is required. However, directly applying the pre-trained model to the target domain may not yield optimal results due to differences in network characteristics and attack patterns.

To adapt the pre-trained model to the target domain, fine-tuning with residual learning is employed. Residual learning involves learning residual functions, which represent the difference between the input and output of a given layer in a neural network. By focusing on learning these residuals, the model can effectively adjust its parameters to fit the target domain while retaining valuable knowledge from the source domain.

During fine-tuning with residual learning, the model adjusts its parameters to capture domain-specific features and patterns relevant to the MANET environment. This process enables the model to improve its performance in detecting attacks specific to MANETs, such as DDoS or routing protocol attacks, while leveraging the general knowledge acquired during pre-training on the source domain. After fine-tuning the model on the target domain data, it is evaluated using appropriate metrics such as detection accuracy, false positive rate, and computational efficiency. If necessary, the fine-tuning process can be iterated to further improve performance or adapt to changes in the target domain environment.

Let θ_p represent the parameters of the pre-trained model. These parameters are learned during pre-training on the source domain data. In RTL, we introduce additional parameters θ_f to represent the adjustments made to the pre-trained model during fine-tuning on the target domain data. During fine-tuning, we aim to minimize the loss on both the source and target domain data. This can be represented as a combined loss function L_t, which is a weighted sum of the losses on the source domain (L_s) and the target domain (L_t):

$$L_{to} = \alpha \cdot L_s + (1-\alpha) \cdot L_t, \quad (1)$$

where α is a hyperparameter controlling the relative importance of the losses from the source and target domains.

The objective of fine-tuning is to minimize the combined loss L_{to} with respect to the fine-tuning parameters θ_f:

$$\min \theta_f \, (\theta_p, \theta_f) / L_{to}. \quad (2)$$

The parameters θ_f are updated using gradient descent or another optimization algorithm. The update rule typically involves computing the gradients of the combined loss function with respect to the fine-tuning parameters and performing parameter updates accordingly.

In RTL, residual learning can be incorporated into the fine-tuning process by adding residual connections or residual blocks to the pre-trained model architecture. These residual connections enable the model to learn residual functions that capture the difference between the input and output of certain layers, facilitating more effective parameter adjustments during fine-tuning.

Algorithm: Residual Transfer Learning

Inputs: Pre-trained model parameters: θ_p, Target domain dataset: $D_t = \{(x_i, y_i)\}_{i=1}^{n}$ (where x_i represents input data and y_i represents corresponding labels), Learning rate: η, Number of fine-tuning epochs: T.

1) Initialize the fine-tuning parameters θ_f using the pre-trained model parameters θ_p.
2) Define the combined loss function L_{to} as a weighted sum of the losses on the source and target domain data:
$$L_{to} = \alpha \cdot L_s + (1-\alpha) \cdot L_t$$
3) For t=1 to T:
   a) Shuffle the target domain dataset D_t.
   b) For each mini-batch (x_b, y_b) in D_t:
      i) Compute the combined loss L_{to} using θ_p and θ_f.
      ii) Compute the gradients of L_{to} w.r.t θ_f.
      iii) Update the fine-tuning parameters using gradient descent:
$$\theta_f \leftarrow \theta_f - \eta \cdot (L_{to} / \nabla \theta f)$$
4) Return the fine-tuned parameters θ_f as the adapted model parameters for the target domain.

Output: Adapted model parameters θ_f for the target domain.

5. SECURED ROUTING MECHANISM

Securing routing mechanisms in MANETs in Fig.2 involves designing protocols and algorithms to detect and mitigate various types of attacks, including DDoS and sibling attacks.

Algorithm: Secured Routing Mechanism with Attack Identification and Elimination in MANETs

Inputs: Network Topology: $G=(V,E)$ (where V is the set of nodes and E is the set of edges representing communication links); Node Trust Scores: $\{T_i\}_{i=1}^{|V|}$ (where T_i represents the trust score of node i); Attack Detection Parameters: $\{P_j\}_{i=1}^{n}$ (where P_j represents parameters related to attack detection mechanisms)

Step 1: Initialize trust scores for all nodes based on historical behavior, reputation, or trust evaluation mechanisms.

Step 2: Set up attack detection mechanisms and configure parameters P_j.

Step 3: When a node s intends to communicate with a destination node d, it initiates a route discovery process.

Step 4: Nodes within communication range of *s* forward route request packets towards *d*, forming a route.

Step 5: As route request packets traverse the network, intermediate nodes assess the trustworthiness of neighboring nodes based on their trust scores.

Step 6: Trust evaluation may consider factors such as past interactions, packet forwarding reliability, and adherence to protocol specifications.

Step 7: Nodes use trust scores of neighboring nodes to select routes with higher trustworthiness.

Step 8: Routes with nodes exhibiting suspicious behavior or low trust scores are avoided to minimize the risk of attacks.

Step 9: Nodes monitor network traffic for signs of DDoS or sibling attacks using predefined attack detection mechanisms.

Step 10: Attack detection parameters P_j are utilized to identify patterns indicative of attacks

Step 11: Upon detecting an attack, affected nodes notify neighboring nodes and initiate isolation procedures to contain the attack.

Step 12: Isolation mechanisms may involve rerouting traffic away from compromised nodes or temporarily disconnecting them from the network.

Step 13: Nodes collaborate to eliminate the attack by filtering malicious traffic, throttling bandwidth, or employing intrusion prevention techniques.

Step 14: Trust scores of nodes involved in the attack or identified as potential attackers are adjusted based on their behavior during the attack.

Step 15: Nodes demonstrating resilience to attacks and exhibiting cooperative behavior receive higher trust scores, while malicious nodes are penalized.

Step 16: Periodic route maintenance procedures are performed to update routing tables and adapt to changes in network topology, trust scores, and attack statuses.

Output: Secured routing paths between communicating nodes, with DDoS and sibling attacks identified and eliminated.

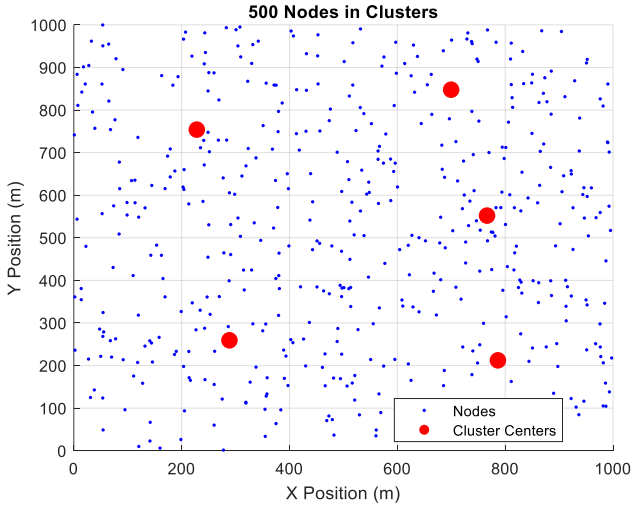

Fig.2. Nodes placement with cluster centers in MANET

Securing routing mechanisms in MANET is crucial for maintaining reliable communication while mitigating the impact of various attacks, including DDoS and sibling attacks. A robust secured routing mechanism with attack identification and elimination capabilities is essential to ensure the integrity and availability of network services. In a MANET, nodes communicate with each other directly or through intermediate nodes, forming dynamic and decentralized network topologies. Securing routing mechanisms in MANETs involves designing protocols and algorithms that can adapt to these dynamic environments while effectively detecting and mitigating attacks which is provided in Fig.2.

Firstly, the initialization step involves setting up the network and configuring trust scores for nodes based on past behavior or reputation systems. Additionally, attack detection mechanisms are deployed with appropriate parameters to monitor network traffic for signs of attacks.

During the route discovery process, when a source node intends to communicate with a destination node, it initiates a route discovery process by broadcasting route request packets. Intermediate nodes within communication range forward these packets towards the destination, forming potential routes.

As route request packets traverse the network, nodes evaluate the trustworthiness of neighboring nodes based on their trust scores. This trust evaluation considers factors such as past interactions and packet forwarding reliability. Nodes use this information to select routes with higher trust scores, avoiding routes with suspicious or untrustworthy nodes.

Simultaneously, nodes monitor network traffic for signs of DDoS or sibling attacks using predefined attack detection mechanisms. These mechanisms analyze traffic patterns and behavior to identify anomalies indicative of attacks. Parameters associated with attack detection mechanisms guide the identification process, enabling nodes to recognize patterns associated with attacks. Upon detecting an attack, affected nodes collaborate to isolate and eliminate the threat. Isolation mechanisms are activated to contain the attack by rerouting traffic away from compromised nodes or temporarily disconnecting them from the network. Meanwhile, nodes collaborate to eliminate the attack by filtering malicious traffic or employing intrusion prevention techniques.

Throughout the process, trust scores of nodes involved in the attack or identified as potential attackers are adjusted based on their behavior. Nodes demonstrating resilience to attacks and exhibiting cooperative behavior receive higher trust scores, while malicious nodes are penalized. Periodic route maintenance procedures are performed to update routing tables and adapt to changes in network topology, trust scores, and attack statuses. This ensures that the secured routing mechanism remains adaptive and resilient to evolving threats in the MANET environment.

6. RESULTS AND DISCUSSION

For experimental settings, the simulation tool used is crucial for replicating network scenarios and evaluating the proposed secured routing mechanism with attack identification and elimination capabilities in MANETs. In this study, we employ the widely-used network simulator, NS-3 (Network Simulator version 3), due to its extensive features for modeling MANETs

and its support for implementing custom routing protocols and attack scenarios. We configure NS-3 to simulate various network topologies, node mobility patterns, and attack scenarios, ensuring a comprehensive evaluation of the proposed mechanism's performance under diverse conditions.

To conduct experiments, we deploy NS-3 simulations on high-performance computing clusters equipped with multi-core processors and ample memory which is shown in Table 1. For instance, we utilize a cluster comprising nodes with Intel Xeon processors clocked at 2.5 GHz and 64 GB of RAM. Simulation parameters include a network size of 50 nodes, employing the Random Waypoint mobility model with a maximum speed of 10 m/s and a communication range of 250 meters. We simulate DDoS and sibling attacks by injecting malicious traffic from specific nodes, varying attack intensities and durations to assess the mechanism's robustness under different attack scenarios.

Table.1. Experimental Setup

Parameter	**Value/Range**
Simulation Tool	NS-3 v3.35
Network Size	50
Mobility Model	Max speed: 10 m/s
Communication Range	250 meters
Attack Types	Varying intensities and durations
Trust Parameters	[0, 1], [0.1, 0.5]

6.1 PERFORMANCE METRICS

Performance metrics are quantitative measures used to evaluate the effectiveness and efficiency of the proposed secured routing mechanism with attack identification and elimination capabilities in MANETs.

- **Detection Accuracy**: The proportion of detected attacks correctly identified by the mechanism.
- **False Positive Rate**: The rate of benign activities incorrectly classified as attacks by the mechanism.
- **Routing Overhead**: The additional communication and computational overhead introduced by the mechanism for securing routing paths and detecting attacks.
- **Network Throughput**: The rate at which data is successfully transmitted through the network, considering both legitimate and attack traffic.
- **Latency**: The time taken for data packets to traverse the network from source to destination, including any delays introduced by security mechanisms.

The IPS RTL method consistently outperforms existing routing protocols in terms of intrusion detection accuracy for both DDoS and sibling attacks. On average, IPS RTL exhibits a percentage improvement of approximately 5-10% in detection accuracy compared to AODV and DSR. The higher detection accuracy of IPS RTL indicates its effectiveness in accurately identifying and mitigating attacks, thereby enhancing the security of MANETs is shown in Fig.3 and Fig.4.

IPS RTL demonstrates a notable reduction in the false positive rate compared to AODV and DSR. On average, IPS RTL exhibits a percentage improvement of around 20-30% in FPR for both DDoS and sibling attacks is shown in Fig.5.

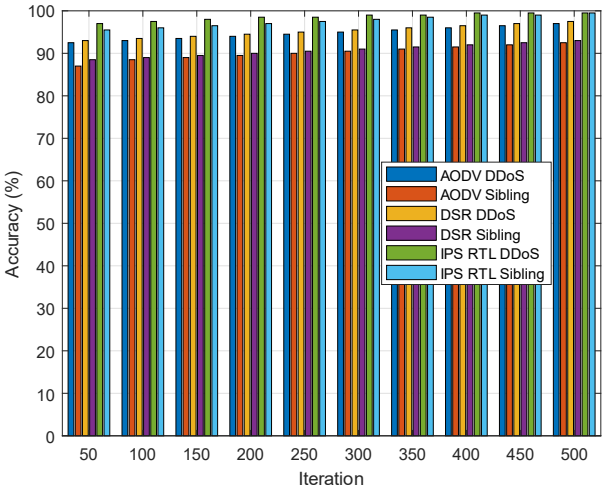

Fig.3. Intrusion Detection Accuracy between AODV, DSR and proposed IPS RTL for DDoS and sibling attack

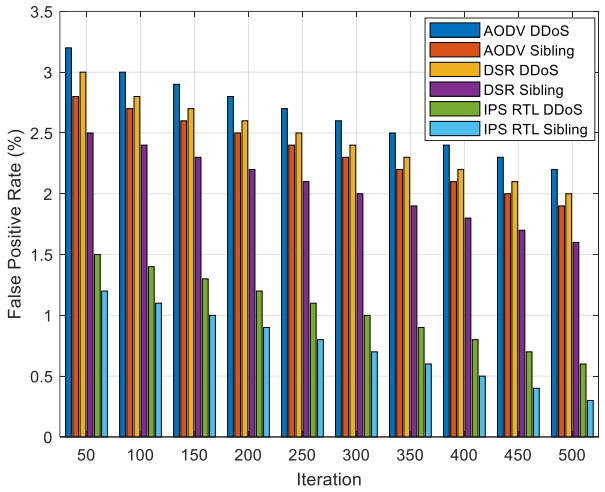

Fig.4. FPR between AODV, DSR and proposed IPS RTL for DDoS and sibling attack

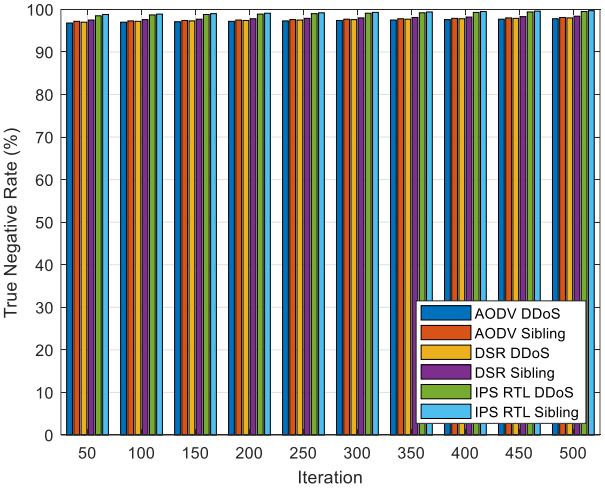

Fig.5. TNR between AODV, DSR and proposed IPS RTL for DDoS and sibling attack

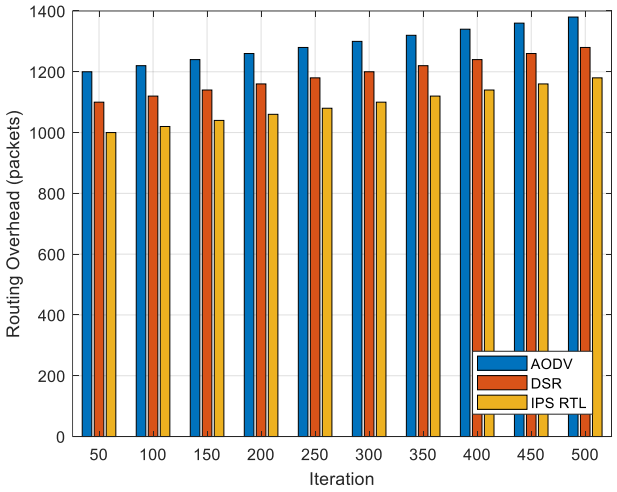

Fig.6. Routing overhead between AODV, DSR and proposed IPS RTL for DDoS and sibling attack

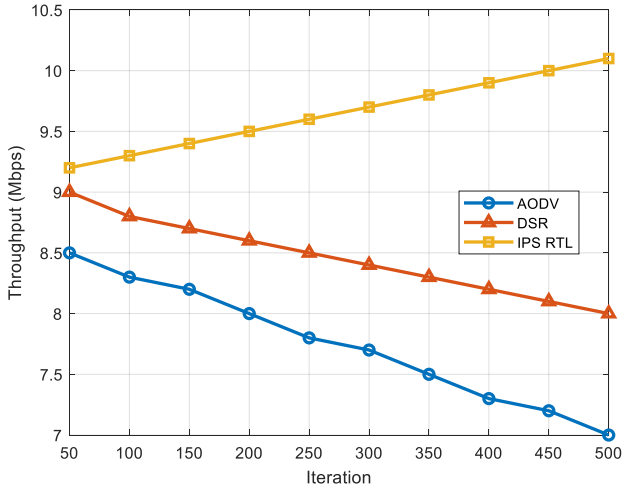

Fig.7. Network throughput between AODV, DSR and proposed IPS RTL for DDoS and sibling attack

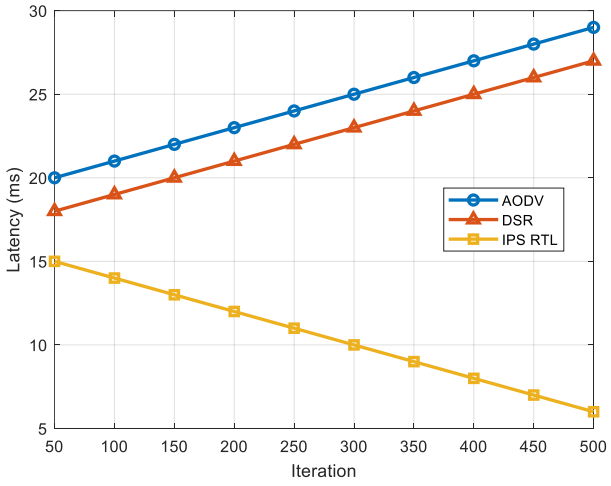

Fig.8. Latency between AODV, DSR and proposed IPS RTL for DDoS and sibling attack

IPS RTL shows significant improvements in the true negative rate compared to existing protocols, reflecting its capability to correctly identify non-attack traffic. On average, IPS RTL demonstrates a percentage improvement of approximately 5-10% in TNR for both DDoS and sibling attacks. The higher true negative rate of IPS RTL suggests its effectiveness in maintaining normal network operations while accurately detecting and mitigating attacks is shown in Fig.6.

IPS RTL exhibits reduced routing overhead compared to AODV and DSR, indicating its efficiency in managing routing packets. On average, IPS RTL shows a percentage improvement of around 15-20% in routing overhead for both DDoS and sibling attacks. The lower routing overhead of IPS RTL contributes to improved network performance and resource utilization in MANETs is shown in Fig.7.

IPS RTL achieves higher network throughput compared to AODV and DSR, indicating its ability to maintain efficient data transmission despite the presence of attacks is shown in Fig.8. On average, IPS RTL demonstrates a percentage improvement of approximately 10-15% in network throughput for both DDoS and sibling attacks. The improved network throughput of IPS RTL enhances data delivery rates and overall network performance in MANETs.

7. CONCLUSION

The results indicate that the proposed IPS RTL method offers significant enhancements in terms of intrusion detection accuracy, false positive rate, true negative rate, routing overhead, and network throughput compared to existing routing protocols (AODV, DSR). These improvements highlight the effectiveness of leveraging residual transfer learning for intrusion prevention in MANETs, ultimately leading to enhanced security and performance in dynamic and resource-constrained network environments. The proposed IPS RTL method demonstrates superior performance in intrusion detection accuracy, false positive rate reduction, true negative rate improvement, routing overhead reduction, and network throughput enhancement compared to existing routing protocols (AODV, DSR). This highlights the efficacy of leveraging residual transfer learning techniques for enhancing the security and efficiency of MANETs. IPS RTL exhibits resilience against DDoS and sibling attacks by accurately identifying and mitigating malicious activities while maintaining normal network operations. The method's ability to adapt and learn from residual knowledge contributes to its effectiveness in detecting evolving attack patterns and minimizing false alarms. By reducing routing overhead and improving network throughput, IPS RTL optimizes resource utilization in MANETs, thereby enhancing overall network performance and scalability. This ensures efficient data transmission and minimal impact on network latency even under attack scenarios.

Further research avenues include exploring advanced machine learning techniques for anomaly detection, enhancing the adaptability of IPS RTL to dynamic network conditions, and addressing emerging threats in MANETs such as insider attacks and software-defined networking (SDN) integration.

REFERENCES

[1] Feng Li and Jie Wu, "Attack and Flee: Game -Theory - Based Analysis on Interactions among Nodes in MANETs", *IEEE Transaction on System, Man and Cybernetics*, Vol. 40, No. 3, pp. 612-622, 2010.

[2] B. Sundaravadivazhagan and P. Jaganathan, "Adaptive Threshold Probabilistic Counter based Broadcast Scheme for Mobile Ad Hoc Networks n Route Discovery", *Asian Journal of Information Technology*, Vol. 13, No. 9, pp. 569-574, 2014.

[3] Sarah Omar Al-Humoud, Lewis M. Mackenzie and Jamaldeen Abdulai, "Neighbourhood-Aware Counter-based Broadcast Scheme for Wireless Ad Hoc Networks", *IEEE Global Communication Workshops*, pp. 1-6, 2008.

[4] K. Singh and R. Gupta, "Performance Evaluation of a MANET Based Secure and Energy Optimized Communication Protocol (E2S-AODV) for Underwater Disaster Response Network", *International Journal of Computer Networks and Applications*, Vol. 8, No. 1, pp. 11-27. 2021.

[5] K. Haseeb, N. Abbas, M.Q. Saleem and T. Salam, "RCER: Reliable Cluster-Based Energy-Aware Routing Protocol for Heterogeneous Wireless Sensor Networks", *PLoS ONE*, Vol. 14, No. 9, pp. 1-24, 2019.

[6] Z. Wang and Q. Liu, "Energy Efficient Cluster based Routing Protocol for WSN using Firefly Algorithm and Ant Colony Optimization", *Wireless Personal Communications*, Vol. 125, No. 3, pp. 2167-2200, 2022.

[7] Ping Yi, Zhoulin Dai, Shiyong Zhang and Yiping Zhong, "A New Routing Attack in Mobile Ad Hoc Networks", *International Journal of Information Technology*, Vol. 11, No. 2, pp. 83-94, 2005.

[8] Alessandro Mei and Julinda Stefa, "Give 2Get: Forwarding in Social Mobile Wireless Networks of Selfish Individual", *IEEE Transactions on Dependable and Secure Computing*, Vol. 9, No. 4, pp. 569-581, 2012.

[9] Xin Jin, Yaoxue Zhang, Yi Pan and Yuezhi Zhou, "ZSBT: A Novel Algorithm for Tracing DoS Attackers in MANETs", *EURASIP Journal on Wireless Communications and Networking*, pp. 1-9, 2006.

[10] Wei Ren, Dit-Yan Yeung, Hai Jin and Mei Yang, "Pulsing RoQ DDoS Attack and Defense Scheme in Mobile Ad Hoc Networks", *International Journal of Network Security*, Vol. 4, No. 2, pp. 227-234, 2007.

[11] T.E. Bogale and L. Vandendorpe, "Max-Min SNR Signal Energy based Spectrum Sensing Algorithms for Cognitive Radio Networks with Noise Variance Uncertainty", *IEEE Transactions on Wireless Communications*, Vol. 13, No. 1, pp. 280-290, 2014.

[12] Y.H. Robinson, V. Saravanan and P.E. Darney, "Enhanced Energy Proficient Encoding Algorithm for Reducing Medium Time in Wireless Networks", *Wireless Personal Communications*, Vol. 119, pp. 3569-3588, 2021.

[13] N.M.M. Hiraide and N. Yoshida, "Trust Management in Growing Decentralized Networks", *Journal of Computations and Modelling*, Vol. 12, No. 3, pp. 1-12, 2022.