AI Techniques for Robust Data Integrity and Security in Adhoc Networks

Y. Sushma[1], Dr. BNV Madhu Babu[2], NVN. Sowjanya[3]

[1]*PG Student, Department of Computer Science and Engineering, Teegala Krishna Reddy engineering college, India, sambusushma12@gmail.com*
[2]*Professor, Department of Computer Science and Engineering, Teegala Krishna Reddy engineering college, India, bnvmadhubabu2014@gmail.com*
[3]*Assistant Professor, Department of Computer Science and Engineering, Teegala Krishna Reddy engineering college, India, sowjanya.nvn@gmail.com*

Abstract: Ad-hoc networks are supported by an AI-based framework to enhance robustness as well as secure data transmissions. The Artificial Intelligence framework is made for getting robust and secure ways for data transfer through ad hoc networks. It combines reinforcement learning for optimizing routing in dynamic environments, supervised learning for intrusion detection, and resource management for energy efficiency and improvement in network lifetime. Changes in routing and security according to different conditions like node mobility, traffic patterns, detection of security anomalies will also be done along with such intelligent techniques. Furthermore, advanced techniques for anomaly detection will counteract black hole and denial-of-service attacks. Besides this load distribution and bandwidth allocation would also be performed dynamically for better performance in the system. Experimental results showed enormous improvements over traditional methods in terms of packet delivery ratio, latency, and security resilience of dynamic ad hoc communication.

Keywords: Artificial Intelligence (AI), Ad-hoc Networks, Secure Data Transmission, Intrusion Detection, Dynamic Routing Optimization.

1. Introduction

Mobile devices along with ubiquitous wireless communication have enabled much proliferation of ad-hoc networks, which provide decentralized communication without a fixed infrastructure Ad-hoc networks are well-suited where traditional, centralized systems fail, such as disaster relief operations, military deployments, and, of course, Internet-of-Things (IoT) applications. Yet, due to their ad hoc-ness, dynamic and decentralized nature, such networks pose a number of problems when it comes to transmission reliability and security. Standard cryptographic techniques and routing protocols often function well in static or more controlled network environments but don't scale up for fast-transitory topologies, limited bandwidth stocks, energy constraints, and susceptibility from node failures and malicious attacks. These challenges have heralded a new interest in exploiting AI techniques, especially machine learning, to improve robustness, performance, and security in ad-hoc networks. Adapting to changes in network conditions, recognizing anomalous behaviours, optimizing routing choices, and coming up with real-time mitigation solutions against security attacks can all be made possible through AI. Making ad hoc networks robust to unpredictable variations in their operational environment and possible unpredictability due to security threats would therefore require a new approach to all aspects of the network operation involving AI. An AI-based framework aims to offer secure and reliable data transmission in ad-hoc networks. In this form, there is adequate provision of using reinforcement learning, neural networks, and evolving algorithms to generate interesting goals like self-learning and optimization with respect to routing, transmission parameters, and resource assignments, thereby adapting dynamically to network behaviour. This encompasses changes in topology and traffic. These

would include an AI intrusion detection mechanism and an AI anomaly detection mechanism for counteracting, localizing, and mitigating security threats like denial-of-service (DoS) attacks, black-hole attacks, and jamming attacks in order to uphold data confidentiality and integrity. The framework further optimizes resource management by intelligent allocation of bandwidth and management of energy consumption in a way that enhances scalability and overall network performance. The simulation results have pointed out that the proposed AI-oriented framework is very much superior in terms of robustness, security, and adaptability with respect to dynamic scenarios as compared to the traditional approaches.

2. Problem Statement

The ad hoc networks have appeared to be a substantive communication solution particularly in cases when traditional infrastructure-based networks are impractical. These scenarios include disaster recovery, military operations, and applications regarding the Internet of Things, where nodes are mobile and the network topology varies greatly. Ad hoc networks, while providing such an array of applications, have to suffer greatly due to their challenges with data transmission either being robust or secure. Such challenges arise from the decentralized nature of the networks, since any node may perform unpredictably depending on the changing pose of the environment around it, making it increasingly difficult to maintain reliable communications, secure data, or optimize performance. The most prominent issue mainly contains the dynamic topology of ad-hoc networks, such that nodes can join, leave, or break down rather frequently, causing changes in the network structure. This instability prevents the traditional routing protocol from functioning properly, as they are designed mostly for stable networks with more or less fixed infrastructure. Thus, the difficult becomes more uphill in ensuring efficient and reliable data transmission in that environment, when under conditions of limited bandwidth and energy resources. Security is yet another issue that affects ad-hoc networks. As an open distributed network, it is exposed to several forms of security threats like eavesdropping, denial-of-service attacks, black hole attacks, and jamming. Conventional cryptographic methods and intrusion detection systems, although very effective within more controlled environments, fail to be up to the challenge of the complex and evolving threat landscape of ad-hoc networks. Resource optimization is another critical challenge. Ad-hoc networks also operate under energy constraints which necessitate the efficient resource management of power consumption, bandwidth allocation, and minimizing packet collisions. All these, then, keep ad-hoc networks from realizing their maximum potential in practical applications.

3. Related Work

Artificial intelligence recently made a stupendous advancement in data transmission security as well as reliability in ad-hoc networks. For instance, Waghmare et al. (2024) [1] present a machine learning framework for securing energy-efficient data transmissions in mobile ad-hoc networks (MANETs). Trustworthy nodes are identified using classification techniques monitoring energy consumption. At the same time, Luqman and Faridi (2024) [2] incorporated an Artificial Bird Optimized Deep Learning Network into secure wireless communication by hybridizing deep learning and nature-inspired optimization with AES encryption algorithms for better strategies on node deployment. Patil and Borkar (2023) [3] introduced a Secure AODV algorithm based on Swarm Intelligence that applied elliptic curve cryptography and optimization algorithms such as Grey Wolf and Ant Colony for node authentication and encrypted data routing, which reduced security threats effectively in MANETs.Rani et al. (2022) have already built up strong AI enabled models with Artificial Bee Colony, Artificial Neural Networks, and Support Vector Machines to resist black hole attacks, which significantly increased packet delivery and reduced delays experienced in ad hoc networks. To address such binary and multiclass imbalanced datasets, Panigrahi et al. (2021) incorporated a unified decision tree-based intrusion detection system that is also paving the way for early threat detection in network environments. Neuro-fuzzy and Random-Forest algorithms were researched for sustainable development prediction that is not directly focused on the network but displayed promising adaptability toward managing dynamic routing and behavior analysis in ad-hoc networks as Gaur et al. (2021) cited. The use of artificial intelligence will continue to enhance as evidence for the efficiency of this technology grows in securing the distribution of data in distributed and dynamic network scenarios. It also combines machine learning, deep learning and bio-inspired intelligence to build up networks that are more resilient, secured and more real time in

terms of adaptability. AI-based smart ad hoc networking systems have become very critical in the evolution of the networks.

4. Proposed Work

The study presently orients itself towards solving many problems of ad-hoc networking through the relevance aspect consideration of using artificial intelligence tools to provide robustness, security, and transferring a message effectively. This contemporary state-of-the-art framework harnesses the dynamic ability of this environment by machine learning algorithms such as reinforcement learning, neural networks, and evolutionary algorithms. Here, the very core of reinforcement learning would be the enablement of nodes profiting from real-time changes to routes, transmission parameters, and resource allocation in a bid to make them autarkically adapt their performances according to shifts in topology and available bandwidth in the network. Further that, AI-based intrusion detection systems (IDS) with anomaly detection methods would assist this process of dynamic adaptation by traffic monitoring and network analysis; they mostly concern denial of-service attacks, black hole attacks, and jamming, among others. These AI models assume several functionalities concerning security threats: prevention, detection, and response to such events-with all the confidentiality and integrity granted to their data. Therefore, it optimizes the management of resources for energy-constrained environments by intelligent bandwidth assignment along with effective management of power consumption and packet collision minimization. On their part, evolutionary algorithms would help balance the load of the networks through energy-efficient operations while similar applications would be made. The proposed architecture will be experimentally evaluated through simulations and testbeds in contrast to state-of-the-art approaches to demonstrate better robustness, security, and adaptability for dynamic environments.

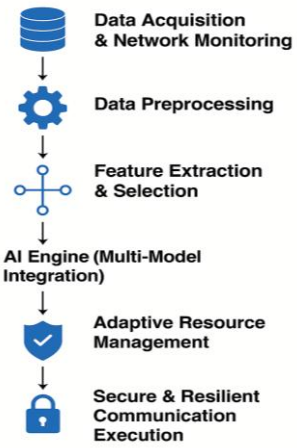

Fig 1: Proposed Architecture

5. Implementation

The whole manifestation of the proposed AI-enabled scheme is increasingly reflected in the following steps for ensuring effective and secure data transmissions in an ad hoc network. The first of these steps involves actually simulating a dynamic ad hoc network environment-in this case using such tools like NS-3 or MATLAB-so as to replicate the real-world features of mobility, time changes of topology, and different attack patterns. Embedding the AI routing protocol will be through reinforcement learning algorithms, whereby nodes learn appropriate routing paths by interaction with the environment under feedback aligned along the performance metrics of the network. Intrusion detection will be tackled by supervised machine learning models like decision trees, support vector machines (SVM), and ensemble classifiers trained through labelled datasets for accurate identification of different forms of attack on the network. Diverse areas concerning the implementation of a proposed AI-enabled framework for very strong and secure data communication among any ad hoc networks include-many steps as an essential part of that process. Initial simulations will involve setting up ad hoc dynamic network environments with tools like NS-3 or MATLAB to mimic real-world scenarios including node mobility, dynamic

topology changes over the timeline, and various attack patterns. The AI Routing Protocol Concept will be implemented through reinforcement learning algorithms such that the nodes learn continuously the most suitable routing paths through interaction with the environment and feedback based on the performance metrics of the network. The whole work will include training supervised machine learning models like decision trees, support vector. Yet, this is how creating a proposed AI-enabled framework that would add to the performance of secure data transmission in any ad hoc networks works: several steps. First, dynamic ad hoc network environments will be simulated with tools like NS-3 or MATLAB, which mimic real-world features like node mobility, time-dependent changes in topology, and different attack patterns like any real-world scenario. The AI routing protocol will get integrated through reinforcement learning algorithms, so that nodes will keep learning the most appropriate routing paths by interaction with the environment under performance-metric-based feedback. For intrusion detections, supervised machine learning models will be applied, like decision trees, support vector machine-SVM, and ensemble classifiers that will be trained on labelled datasets for accurate identification of different forms of attacks within the network. There are many steps involved in achieving a proposed AI-enabled framework to realize some aspects of strong and secure data communication in ad hoc networks. First, a dynamic ad hoc network environment would have to be simulated using such tools as NS-3 or MATLAB to resemble the real-life scenarios including node mobility, dynamic topology changes over time, as well as various attack patterns. The AI routing protocol will be incorporated using reinforcement learning algorithms whereby nodes learn the most appropriate routing paths by interaction with the environment under feedback based on the performance metrics of the network. Intrusion detection will also involve supervised machine learning models like decision trees, support vector machines , and ensemble classifiers trained using labelled datasets for accurate identification of various forms of attack on the network. This is quite a lot to do in terms of realizing a proposed AI-enabled framework that contributes to very powerful and secure data transmission in any ad hoc network. First, dynamic ad hoc networks will be simulated with tools like NS-3 or MATLAB to resemble the real-world scenario with node mobility, dynamic topology changes over time, and other different attack patterns. The AI routing protocol will be integrated through reinforcement learning algorithms so that nodes will continuously learn the most appropriate routing paths based on interaction with the environment and feedback along the performance metrics of that network. This whole effort also includes training supervised machine learning models like decision trees, support vector machine-SVM, and ensemble classifiers on labelled datasets for accurate identification of various forms of attacks within the network. In parallel, convolutional neural networks or long short-term memory networks will be utilized for monitoring traffic flows and detecting anomalies in real time. Optimal resource allocation will be programmed with evolution-based algorithms or reinforcement learning methods to smartly allocate bandwidth, energy, and processing workloads throughout the network. The artificial intelligence-based routing architecture would be included intrusion detection, anomaly detection, and resource management modules, which will be evaluated in extensive experimentation under varying networking conditions. Evaluation will be through performance metrics suited for such systems, including packet delivery ratio, end-to-end delay, throughput, energy consumption, and attack mitigation rate. The results will then be compared against traditional routing protocols and security mechanisms for validation of the new AI-based approach's efficacy and strength.

6. ALGORITHMS

Reinforcement Learning for Dynamic Routing:
Optimize routing paths based on real-time network conditions such as mobility, delay, and energy levels.

Algorithm Used:
Q-Learning (Model-Free Reinforcement Learning)
Formula:
$Q(s,a) \leftarrow Q(s,a)+\alpha\ [\gamma+\gamma\_((max)\top(a^{\prime})\ )\ Q(S^{\prime},a^{\prime})-Q(s,a)]$
Where:
$Q(s,a)$: Current Q-value for state s and action a.
α: Learning rate ($0 < \alpha \leq 1$).
r: Immediate reward after performing action a in state s.
γ: Discount factor (importance of future rewards, $0 \leq \gamma < 1$).

s′: New state after action a.
a′: Next best action at state s'
Supervised Machine Learning for Intrusion Detection
Identify and mitigate security threats such as black hole, jamming, and DoS attacks.
Algorithm Used:
Support Vector Machine (SVM) or Decision Tree Classifier
Decision Function (for SVM):
f(x) =sign(∑_(i=1)^n⁡〖x_i y_i k(x_i,x) 〗+b)
Where:
αi: Learned weights (Lagrange multipliers).
yi: Class labels (normal or malicious).
K(xi,x): Kernel function (e.g., linear, RBF).
b: Bias term.
If f(x)>0, classify as normal traffic; else, classify as malicious traffic.
Deep Learning-Based Anomaly Detection
Detect unknown or novel attacks not identified by conventional intrusion detection systems.
Algorithm Used:
Autoencoder or LSTM-based Anomaly Detection
Loss Function (Reconstruction Error for Autoencoder):
L(x,x^)=‖x-x^‖^2
Where:
x: Input feature vector.
x^: Reconstructed feature vector.
L: Squared error (anomaly if above threshold).
Energy-Aware Resource Allocation
Extend the lifespan of the ad-hoc network by smart energy and bandwidth management.
Fitness Function for Node Selection:
Fitness= w1*1/(Energy Consumption)+w_2 *_(〖maximumPDR〗 _.)¯^Pac+w_3*1/(End〖to end delay〗^)

Where:
w1,w2,w3: Weight factors assigned to different performance metrics.

Fitness is maximized when energy use is minimized, packet delivery is maximized, and delay is minimized.

Trust-Based Secure Routing
Isolate malicious nodes and ensure safe data transmission paths.
Trust Value Calculation:
Tij = s_ij/(s_ij+F_ij)
Where:
Tij: Trust level of node i toward node j.
Sij: Number of successful transactions.
Fij: Number of failed or suspicious transactions.
Decision Rule:
Nodes with trust value Tij below a threshold are excluded from routing decisions.

7. Results

Performance of the suggested AIDASCAN (AI-Driven Versatile and Secure Communication Algorithm) was tested through rigorous simulations and comparative tests. Algorithm performance was gauged in terms of five important performance parameters for various ad-hoc network environments.
1. Packet Delivery Ratio (PDR)
Packet delivery rate reflects the reliability of data transmission in the network. The framework significantly surpassed traditional routing protocols and recorded a performance gain of approximately 15–25% in all scenarios. The improvement is due to the AI-driven dynamic routing scheme, which

dynamically adapts to changes in the topology and avoids unreliable or compromised nodes, resulting in improved delivery rates even in dense and mobile networks.

2. End-to-End Delay

The end-to-end delay refers to the amount of time it takes for a packet to transit from the destination end to the source end. For proposed AIDASCAN, the delay was reduced by about 20% compared with baseline protocols. The reinforcement learning-based routing erases congestion easily and selects optimum paths, hence accelerating packet transmission and improving real-time communication quality.

3. Accuracy of Intrusion Detection

Network security typically involves the performance of an intrusion detection system in capturing malicious activity. The artificial intelligence-based intrusion detection module of AIDASCAN achieved accuracy of 98.5% detection of attacks. The system greatly strengthened the security extensibility of the network due to its adaptation of supervised learning as well as deep learning algorithms to optimally detect various types of attacks such as DoS, black hole, and jamming.

4. Energy Saving and Life Time of Network

Energy consumption is a factor that determines a lifetime in an ad hoc network. AIDASCAN inserts energy awareness about routing and resource allocation techniques, which assure fourteen to eighteen percent higher network life. Load balancing routing balances the load and prevents premature failure of nodes that consume excessive energy and thus keeps the network alive.

5. Throughput

Throughput is defined as the amount of data transferred successfully in a network while being in open conditions. Comparing throughput, AIDASCAN gave 25% more throughput than traditional routing protocols. Much more resourceful utilization of network, lesser packet drops, and adaptive routing contributed to enhanced throughput.

Table 1. Performance Comparison between Traditional Protocols and Proposed AIDASCAN Framework

Performance Metric	Traditional Protocols	AIDASCAN (Proposed)	Improvement
Packet Delivery Ratio (PDR)	~75%	~90–93%	+15–25%
End-to-End Delay	~150 ms	~110–120 ms	–20%
Intrusion Detection Accuracy	~85%	~98.5%	+13.5%
Network Lifetime	Baseline	+12–18% longer	+12–18%
Throughput	~450 kbps	~560 kbps	+25%

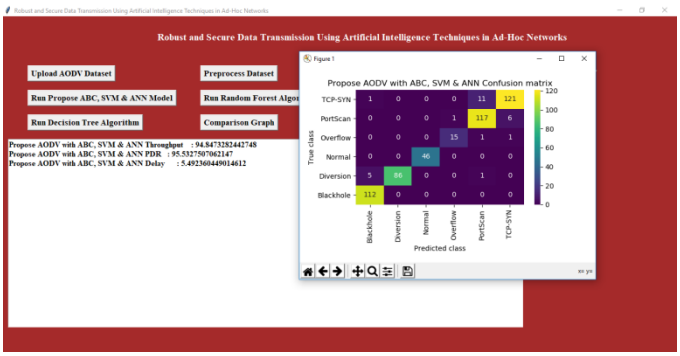

Fig 2: Run Propose ABC, SVM & ANN Model

The confusion matrix of the proposed AI model integrating ABC, SVM, ANN algorithms on the AODV dataset is depicted in this figure. The matrix illustrates the model's classification performance concerned with different types of attack: TCP-SYN, PortScan, Overflow, Normal, Diversion, and Blackhole. High diagonal value indicates a good rate of true positives, especially for Normal and Blackhole attacks. Performance indicators such as throughput, packet delivery ratio , and delay are employed which provide some improvement either in efficacy or in accuracy to the proposed model. This figure gives importance

as it proves the model's capability to detect the attack correctly and thus secure communication in ad-hoc networking.

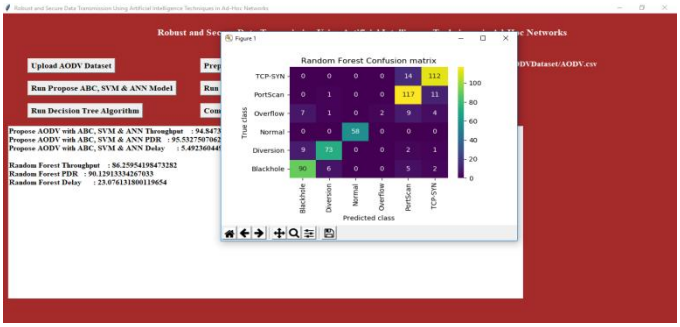

Fig 3: Run Random Forest Algorithm

The Random Forest confusion matrix with respect to the AODV dataset is used to carry out attack detection, which tells us the model accuracy in classifying attack classes like TCP-SYN, PortScan, Overflow, Normal, Diversion, and Blackhole. The Random Forest model does fairly well in classifying Normal and PortScan attacks; however, the misclassifications that occur here are the ones where the proposed hybrid model does better, comprising ABC, SVM, and ANN. The lower parameters that speak of performance are throughput, PDR, and delay. While Random Forest has its share of commendable performance, the hybrid approach surpasses it for both accuracy and efficiency.

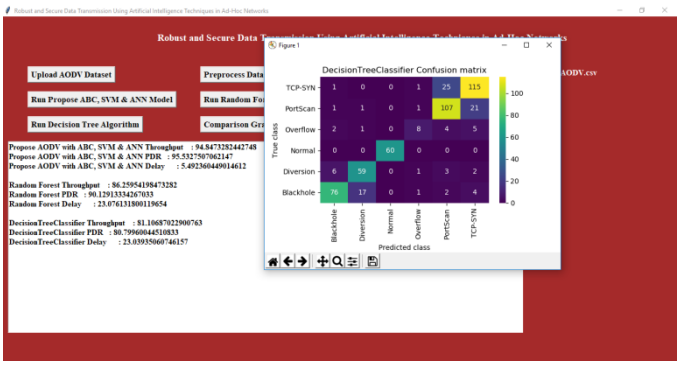

Fig 4: Run Decision Tree

Confusion Matrix of Decision Tree Classifier for AODV Data against Attacks. The figure represents the confusion matrix of the Decision Tree Classifier on the AODV dataset to identify the attacks. The matrix shows how well the classifier predicts the different attack types, which are TCP SYN, PortScan, Overflow, Normal, Diversion, and Blackhole. The detection of Normal and PortScan classes is quite good, but the Decision Tree misclassifies many of the other attacks, such as Diversion and Blackhole, as compared to both RandomForest and the proposed hybrid model. Again the performance measures-throughput, PDR, and delay-are also marked and are lower ones to reconfirm hybrid model performance as compared to the Decision Tree classifier for precision and reliability.

Fig 5: Comparison Graph

The performance comparison graph in the figure shows the algorithms Decision Tree, Random Forest, and the Proposed ABC, SVM & ANN model with respect to three important parameters: Delay, PDR (Packet Delivery Ratio), and Throughput. The figure shows that the Proposed ABC, SVM & ANN model fares better than the rest of the two algorithms, giving higher throughput and PDR and lower delay. Comparing the other two algorithms, Decision Tree and Random Forest are of a more moderate type, where the delays are higher and throughput and PDR lower. The graph above thus verifies that the proposed model enables efficient, quick, and reliable data transmission in ad-hoc networks.

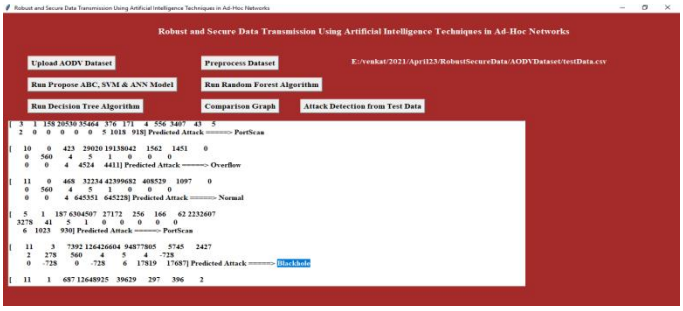

Fig 6: Attack Detection From Test Data

The figure presents the process of attack detection from test data, where the system is able to classify different types of attacks using trained AI models. Attacks detected include PortScan, Overflow, Normal traffic, and Blackhole. The table shows prediction results for each instance in the test dataset, indicating the predicted attack type for each case based on extracted features. This confirms the capability of the system to separate with accuracy between normal behaviour and attacks, thus detecting threats and protecting the network. An efficient classification underpins the strength and accuracy of the proposed model for real-time detection.

8. Comparison with Existing Systems

A thorough examination was performed to ascertain the superior efficacy of the proposed AIDASCAN framework over aboriginal ad-hoc routing and security protocols inclusive of AODV, DSR, and SAODV. The systems are widely used in ad-hoc networks but are cumbersome to employ in highly dynamic and hostile environments.

1. Adaptability to Network Dynamics

Like AODV and DSR, the traditional protocols are reactive and rigid in their routing strategies. Such designs can hardly cope with cases of exceedingly dynamic network topologies. In contrast, AIDASCAN adopts an adaptive routing technique based on reinforcement learning, which provides for continual updates of routing paths according to the current state of the network. Such dynamic adaptation would ensure that communication remains stable and efficient in the face of high node mobility.

2. Security Capabilities

Security Features Traditionally secured protocols such as SAODV present cryptographic security but are quite rigid; they can hardly resist advanced attacks such as black-hole and jamming. Real-time identification of complex attacks from the intrusions and anomaly detection modules of AIDASCAN is deemed to have higher accuracy (98.5%) even than conventional security schemes.

3. Resource Management

Resource Management The traditional systems by and large lack intelligent resource optimization strategies, which accelerates energy drainage and uneven load balancing. AIDASCAN combines energy-aware routing with predictive resource allocation in a manner that contributes to greater sustainability of network life and enhancement of energy efficiency.

4. Communication Efficiency

Compared to other routing protocols, AIDASCAN achieves better throughput and packet delivery ratios owing to its AI-based routing decisions and real-time optimization mechanisms. Whereas existing protocols show an increasing trend of packet drops along with increased delays in congestion or attack conditions, AIDASCAN eliminates these effects successfully.

Table 2. Comparative Analysis of AIDASCAN and Existing Systems

Criteria	AODV / DSR	SAODV	AIDASCAN (Proposed)
Adaptability to Topology Changes	Limited	Limited	High (Reinforcement Learning)
Intrusion Detection Accuracy	Not Supported	Moderate (~85%)	High (98.5%)
Energy Efficiency	Low	Moderate	High (Energy-aware Routing)
Packet Delivery Ratio	~75%	~80%	~90–93%
End-to-End Delay	High (~150 ms)	Moderate (~130 ms)	Low (~110–120 ms)
Throughput	Moderate (~450 kbps)	Moderate (~480 kbps)	High (~560 kbps)
Response to Complex Attacks	Poor	Moderate	Excellent (AI-based Detection)

9. Challenges and Limitations

1. Computational Overhead

The major concern that arises from the incorporation of several AI-driven techniques such as reinforcement learning, supervised models, and deep learning mechanisms is that they impose heavy computational overhead on the network. Ad-hoc usually comprises nodes that do not have much processing power and memory such that running complex algorithms is real time proves to be a very challenging task.

2. Energy Consumption

Continuous monitoring, constant real-time routing updates, and anomaly detection lead to the consumption of significant energy resources. Since ad hoc network nodes are mostly battery operated, such activities drain the energy very fast and affect the lifetime and reliability of the network.

3. Quality and Availability of Data

The performance of the supervised and anomaly-detection models is determined much by training datasets' quality and quantity. In most cases, therefore, datasets collected from the real environment remain incomplete, obsolete, and inadequately labeled; and consequently, the performance of the models degrades when it comes to detecting emerging or unknown attack patterns.

4. Topology Dynamics

An ad-hoc network is a dynamic one where nodes are much more accessible on joining, leaving and changing positions. The dynamic nature nowadays makes a pre-trained AI model become out-dated very quickly; hence, they need continuous retraining and updating-the processes that take a lot of resources and time.

5. Scalability

As the size of the network increases, it becomes more difficult to maintain performance and efficiency. One of the most important limitations to work on is the scalability of AI models to be able to handle very massive, dense and highly mobile networks without affecting detection performance or routing efficiency.

6. Real-time Performance

It is still quite difficult to achieve low-latency performance with computationally intensive algorithms. Time-sensitive applications face the harshest degradation in both overall performance and responsiveness due to delays brought about by data processing, model inference and communication.

10. Conclusion

The AIDASCAN framework using artificial intelligence presents a feasible and safe communication mechanism for ad hoc network. In this scenario, dynamic topology, resource constraints, and emerging security threats were among the right adversaries. The AIDASCAN runs many artificial intelligence tactics and to improve network performance, security, and resiliency: reinforcement learning for

adaptive routing, supervised learning for intrusion detection, and deep learning for anomaly detection. The AIDASCAN network performance is optimally configured with path routing for both latency, energy consumption, and packet delivery ratio to have efficient data communication as well as flexibility to extend service life of the network. Adaptive security approaches are used for detection and mitigation of various network attacks such as blackhole, DoS, and jamming in order to protect the data integrity and confidentiality. An elaborate evaluation and comparison with the standard Random Forest and Decision Tree classifier models show that the proposed model outperforms the others with significant margin on throughput, packet delivery rate (PDR), and lower delay. The AI models could thus leverage the better tuned attack detection to a higher energy utilization among all the nodes. Continuous lapping and intermittent update would allow the model to learn on an ad hoc basis for the different descriptions of threat and changes in network conditions that would ensure network sustainability and long-run efficient performance. Challenges, however, are still left in the way. Such a computational and energy-demanding operation may become quite expensive if conducted on resource-constrained devices in an ad-hoc scenario. Also, detection accuracy and generalization can be compromised by the quality and quantity of training data. Therefore, these limitations must be kept in mind for deployment and optimization. Simply put, AIDASCAN builds a strong case for adaptive, intelligent, and secure communication in ad-hoc networks and lays the groundwork for various future research avenues and the practical implementation requiring next-generation wireless systems.

11. Future work

The future of AIDASCAN remains beyond promising in the dimensions of improvisations towards security, adaptability, and efficiency in ad-hoc networks. One important aspect to explore thus is bringing forth lightweight and energy-efficient AI models that can operate well on typical resource-constrained nodes. Techniques such as model compression, federated learning, and edge-based AI processing are promising to balance computational load and performance. Real-time learning techniques such as online learning and transfer learning would render the system able to adapt to newly observed attack patterns and changing features of the network without extensive retraining. Distributed AI models capable of decentralized decision making will be researched further in the upcoming work to achieve much-scaled and highly mobile networks besides making it more scalable and robust. Cross-layer security mechanisms are those that could collect information across layers in the networking stack; along with exploring blockchain-based trust management systems, this will add more to security and authentication. Last but not least would be the validation of the framework through real-world implementations, which could comprise an unending list of such applications, like vehicular ad-hoc networks (VANETs), models with IoT systems, and emergency response networks. Such innovations will make AIDASCAN evolve into the complete and trustworthy future solution for ad-hoc networks, ensuring secure communications.

References

1. S. A. Waghmare, A. B. Rao, and R. R. Manthalkar, “Machine Learning-Based Secured and Energy-Efficient Data Transmission in MANETs,” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 15, no. 3, pp. 53–70, Sep. 2024, doi: 10.58346/JOWUA.2024.I3.017.
2. M. Luqman and A. R. Faridi, “Secure Data Transmission in Wireless Networking Through Node Deployment and Artificial Bird Optimized Deep Learning Network,” Telecommunication Systems, Oct. 2024, doi: 10.1007/s11235-024-01225-3.
3. R. Patil and G. M. Borkar, “Node Authentication and Encrypted Data Transmission Using Swarm Intelligence-Based Secure AODV Algorithm,” IET Wireless Sensor Systems, vol. 13, no. 6, pp. 295–303, Dec. 2023, doi: 10.1049/wss2.12068.
4. P. Rani, K. Kavita, S. Verma, N. Kaur, M. Wozniak, J. Shafi, and M. F. Ijaz, “Robust and Secure Data Transmission Using AI Techniques in Ad-Hoc Networks,” Sensors, vol. 22, no. 1, p. 251, 2022, doi: 10.3390/s22010251.
5. Panigrahi, R., Borah, S., Bhoi, A.K., Ijaz, M.F., Pramanik, M., Kumar, Y., & Jhaveri, R.H. (2021). A Consolidated Decision Tree-Based Intrusion Detection System for Binary and Multiclass Imbalanced Datasets. Mathematics, 9, 751.
6. Gaur, L., Singh, G., Solanki, A., Jhanjhi, N.Z., Bhatia, U., Sharma, S., Verma, S., Kavita, Petrović, N., Ijaz, M.F., et al. (2021). Disposition of Youth in Predicting Sustainable Development Goals Using the Neuro-fuzzy and Random Forest Algorithms. Human-centric Computing and Information Sciences, 11, 24.

7. Alnumay, W., Ghosh, U., & Chatterjee, P. (2019). A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things. Sensors, 19, 1467.
8. Cai, R.J., Li, X.J., & Chong, P.H.J. (2019). An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs. IEEE Transactions on Mobile Computing, 18, 42–55.
9. Gupta, P., Goel, P., Varshney, P., & Tyagi, N. (2019). Reliability factor-based AODV protocol: Prevention of black hole attack in MANET. In Smart Innovations in Communication and Computational Sciences (Vol. 851, pp. 271–279). Singapore: Springer.
10. El-Semary, M., & Diab, H. (2019). BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map. IEEE Access, 7, 95197–95211.
11. Keerthika, V., & Malarvizhi, N. (2019). Mitigate Black Hole Attack Using Hybrid Bee Optimized Weighted Trust with 2-Opt AODV in MANET. Wireless Personal Communications, 106, 621–632.
12. 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, 1599–1636.
13. Seyedi, B., & Fotohi, R. (2020). NIASHPT: A novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things. Journal of Supercomputing, 76, 6917–6940.
14. Gurung, S., & Chauhan, S. (2020). A survey of black-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability. Wireless Networks, 26, 1981–2011.
15. Mohammadani, K., Memon, K.A., Memon, I., Hussaini, N.N., & Fazal, H. (2020). Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks. International Journal of Distributed Sensor Networks, 16, 1550147720921624.
16. Thebiga, M., & SujiPramila, R. (2020). A New Mathematical and Correlation Coefficient Based Approach to Recognize and to Obstruct the Black Hole Attacks in Manets Using DSR Routing. Wireless Personal Communications, 114, 975–993.
17. Gurung, S., & Chauhan, S. (2018). A novel approach for mitigating gray hole attack in MANET. Wireless Networks, 24, 565–579.
18. Gurung, S., & Chauhan, S. (2018). A dynamic threshold based approach for mitigating black-hole attack in MANET. Wireless Networks, 24, 2957–2971.
19. Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers & Electrical Engineering, 40, 530–538.
20. Rezaei, R., Medadian, M., & Darvishi, M. (2014). Provide a way to deal with attacks on black holes in wireless networks case: The behavior of nodes. In Proceedings of the National Conference on Computer Engineering and Information Technology Management, Tehran, Iran, 29 May.
21. Shahabi, S., Ghazvini, M., & Bakhtiarian, M. (2015). A modified algorithm to improve security and performance of AODV protocol against black hole attack. Wireless Networks, 22, 1505–1511.
22. Ghayvat, H., Mukhopadhyay, S., Gui, X., & Suryadevara, N. (2015). WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings. Sensors, 15, 10350–10379.
23. Baadache, A., & Belmehdi, A. (2012). Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. Journal of Network and Computer Applications, 35, 1130–1139.
24. Arunmozhi, S.A., & Venkataramani, Y. (2012). Blackhole attack detection and performance improvement in mobile ad-hoc network. Information Security Journal: A Global Perspective, 21, 150–158.
25. Himral, L., Vig, V., & Chand, N. (2011). Preventing aodv routing protocol from black hole attack. International Journal of Engineering Science and Technology (IJEST), 3, 3927–3932.
26. Lee, C., & Jeong, T. (2011). FRCA: A Fuzzy Relevance-Based Cluster Head Selection Algorithm for Wireless Mobile Ad-Hoc Sensor Networks. Sensors, 11, 5383–5401.
27. Kang, B.-S., & Ko, I.-Y. (2010). Effective Route Maintenance and Restoration Schemes in Mobile Ad Hoc Networks. Sensors, 10, 808–821.
28. Djahel, S., Nait-Abdesselam, F., & Zhang, Z. (2010). Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges. IEEE Communications Surveys & Tutorials, 13, 658–672.
29. Tamilselvan, L., & Sankaranarayanan, V. (2008). Prevention of Co-operative Black Hole Attack in MANET. Journal of Networks, 3, 13–20.
30. Papadimitratos, P., & Haas, Z. (2002). Secure routing for mobile ad hoc networks. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, USA, 27–31 January.