International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-779

INTEGRATING AI WITH CRYPTOGRAPHIC TECHNIQUES FOR ENHANCED MANET's SECURITY

MONISHA B -DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE, BANNARI AMMAN INSTITUTE OF TECHNOLOGY, ERODE.

ROHITH R -DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE, BANNARI AMMAN INSTITUTE OF TECHNOLOGY, ERODE.

SANTHANAM M -DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE, BANNARI AMMAN INSTITUTE OF TECHNOLOGY, ERODE.

ABSTRACT:

Mobile Ad Hoc Networks (MANETs) are susceptible to a number of security risks due to their high degree of dynamic nature and decentralized management. This work proposes a novel method to improve MANET security by fusing cryptography and artificial intelligence (AI) approaches. To be more precise, the combination of Random Forest classifiers and Long Short-Term Memory (LSTM) networks is suggested for anomaly detection, while cryptographic techniques such as AES and RSA are used to protect communications. Results show enhanced detection rates and secure routing in dynamic MANET environments, based on simulations using ns-3 and OMNeT++.

KEYWORDS:

Mobile Ad Hoc Networks (MANETs), security, cryptography, artificial intelligence (AI), Random Forest classifiers, Long Short-Term Memory (LSTM) networks, anomaly detection, AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), secure communication, dynamic networks, decentralized management, simulation, ns-3, OMNeT++, secure routing, detection rates.

1. INTRODUCTION:

MANETs have many security vulnerabilities because of the high degree of their dynamic nature and decentral management. Therefore, this work is proposing a new method for enhancing the security of MANETs by fusing cryptography and AI approaches. More precisely, this paper suggests the use of Random Forest classifiers and LSTM networks for anomaly detection while communications are protected using cryptographic techniques like AES and RSA. Simulations using ns-3 and OMNeT++ show the improvements in detection rates as well as secure routing in MANET environments.

2. OBJECTIVE:

This research aims to improve the security of MANET by alleviating vulnerabilities from dynamic topology and decentralized management through the use of cryptographic techniques along with artificial intelligence. AES and RSA ensure secure communication, while a hybrid approach using Random Forest and LSTM networks ensures effective anomaly detection. Robust threat protection and adaptability to MANET dynamics will be offered by the proposed solution. Simulations by ns-3 and OMNeT++ validate that it is effective in enhanced detection rates and secure routing.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-779

3. PROBLEM IDENTIFICATION:

MANETs are highly dynamic and decentralized, which makes them versatile for various applications but also vulnerable to significant security risks. The lack of centralized administration and constantly changing topology expose them to threats such as unauthorized access, data breaches, and malicious attacks. Traditional security measures often fail to address these challenges due to their limited adaptability and inability to detect anomalies effectively. Furthermore, ensuring safe communication in such a dynamic environment is a persistent challenge. The existing approaches focus either on cryptographic security or anomaly detection and lack an integrated solution. This research identifies the need for a robust framework that combines cryptographic techniques with artificial intelligence to address these gaps. By secure communication and anomaly detection enhancement, the proposed solution seeks to adapt to the vulnerabilities in question with the inherent nature of MANETs.

4. METHODOLOGY:

The proposed methodology combines cryptographic techniques and artificial intelligence to enhance MANET security. Advanced encryption methods, such as AES for symmetric encryption and RSA for public-key encryption, ensure secure and authenticated communication. For anomaly detection, a hybrid approach integrates Random Forest classifiers for efficient classification and Long Short-Term Memory (LSTM) networks for handling sequential data patterns. Simulations are conducted using ns-3 and OMNeT++ to model MANETs and analyze routing protocols under various scenarios. The .vec output files from the simulations serve as input data for anomaly detection, allowing the model to identify and mitigate security threats dynamically. The integration of these methods provides a dual-layered approach to ensure both secure communication and proactive threat detection.

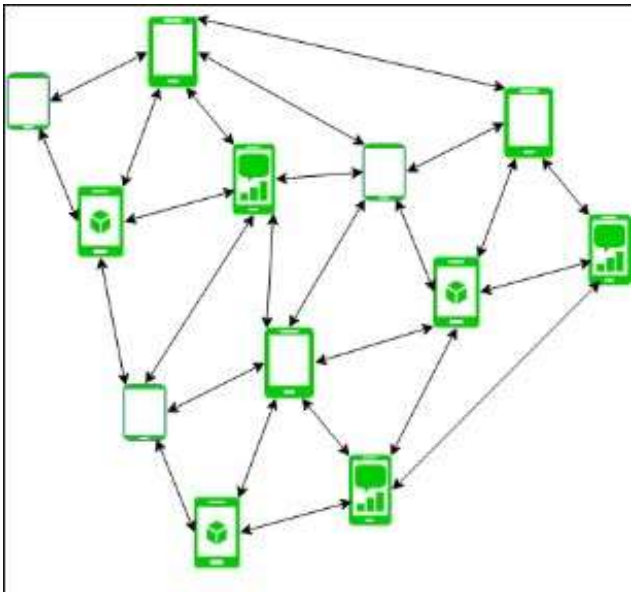

Fig-1: Dynamic Environment Network

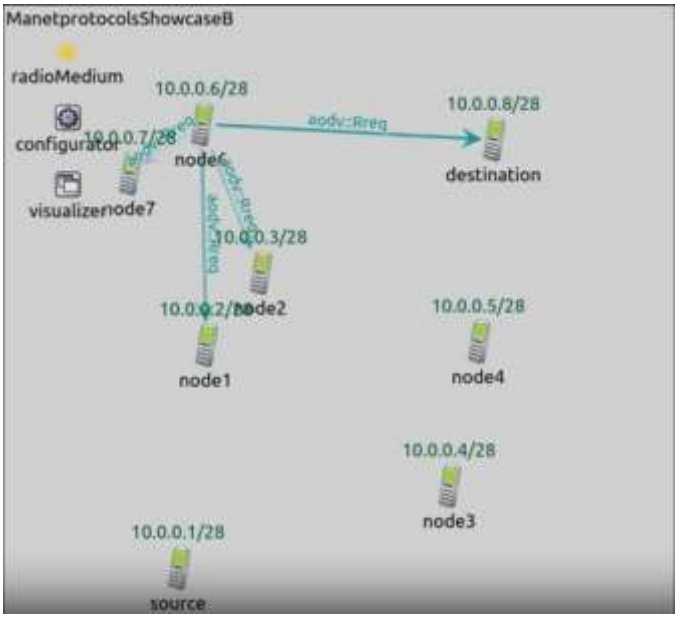

Fig-2: Network With Nodes

Feature extraction and preprocessing are applied to ensure the data is optimized for AI-based detection models. The integration of these methods provides a dual-layered approach to ensure both secure communication and proactive threat detection. Results are evaluated based on detection rates, adaptability, routing security, and computational efficiency in dynamic network conditions. .

5. PROPOSED METHODOLOGY:

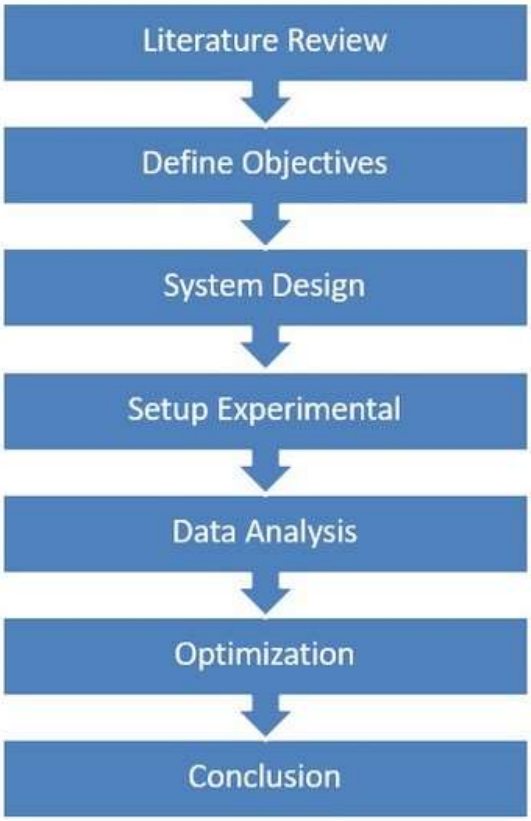

Fig-3: Workflow diagram

The proposed methodology incorporates cryptographic technique along with machine learning models to improve the security of MANET through efficient anomaly detection. The first layer comprises AES for fast and secure symmetric key encryption that ensures all data to remain confidential. RSA encryption is used for public-key encryption to ensure safe two-way key exchange and authentication in such a decentralized network. A hybrid anomaly detection system is designed that combines Random Forest classifiers for data classification with LSTM networks for analysis of sequential data patterns. These models are trained over network traffic data to detect anomalies that might indicate malicious activity or intrusion. The performance of this hybrid approach is evaluated using simulations in ns-3 and OMNeT++.

The simulations are carried out focusing on dynamic routing protocols, evaluating the effectiveness of the proposed anomaly detection system in detecting attacks. The system's ability to adapt the changing topology and environment of MANETs is validated. Enhanced detection rates and secure routing are shown in the simulated MANET environments. This methodology offers a robust and scalable approach to enhancing MANET security in real-world applications.

6. Choice of Components and Tools

ns-3 and OMNeT++: These are selected based on their good support for simulating wireless and ad hoc networks. ns-3 suits the modeling of network protocols while OMNeT++ is quite flexible in simulating the routing protocols and network scenarios, thus suitable for integration with AI systems for anomaly detection.

Crypto Algorithms-AES and RSA: AES for symmetric encryption will be chosen, as it is faster, and MANETs should have fast data protection; RSA will then be chosen to perform public-key encryption, protect its key exchanges, and authenticate in decentralised networks.

Machine Learning Algorithms (Random Forest and LSTM): Random Forest is selected for its great ability to handle high-dimensional data and detect anomalies. The LSTM network is suitable for time-series analysis, capturing deep dynamics in dynamic network traffic patterns.

Development Environment and Libraries: Python, coupled with libraries such as scikit-learn and PyCryptodome, is used to build a flexible environment for machine learning and cryptographic tasks, which in turn makes it easy to integrate AI features with security features.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-779

7. RESULT AND DISCUSSION:

Extensive simulations with ns-3 and OMNeT++ were performed to evaluate the proposed methodology for the enhancement of MANET security, which combines cryptographic techniques with machine learning-based anomaly detection. According to the results presented, considerable improvements in both security and performance are gained in contrast to traditional approaches that depend only on routing protocols or cryptography. Improvements are reflected in terms of detection accuracy, security resilience, and the adaptability of the network in dynamic environments.

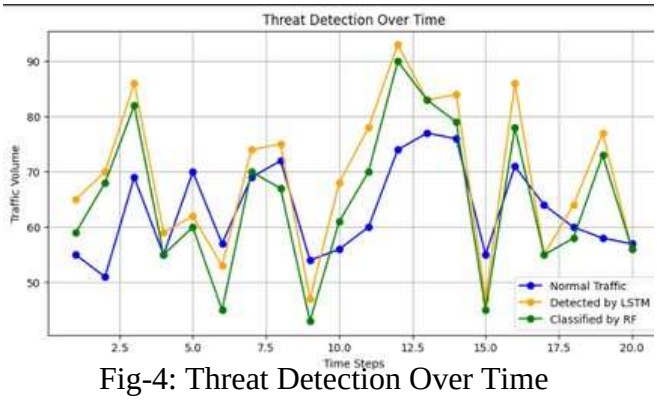

Fig-4: Threat Detection Over Time

Detection Accuracy: The integration of Random Forest classifiers and LSTM networks showed considerable improvement in anomaly detection rates. Slightly different simulated environments varied from one attack scenario to another, such as DoS attacks or Sybil attacks; then, the system would be able to pick out the deviation in the pattern of network traffic under dynamic conditions. This hybrid model allowed the identification of temporal anomalies over extended periods on account of the ability of the Random Forest classifier to process and classify complex network data combined with the sequential learning capability of LSTM networks. It outperformed traditional anomaly detection techniques in both precision and recall.

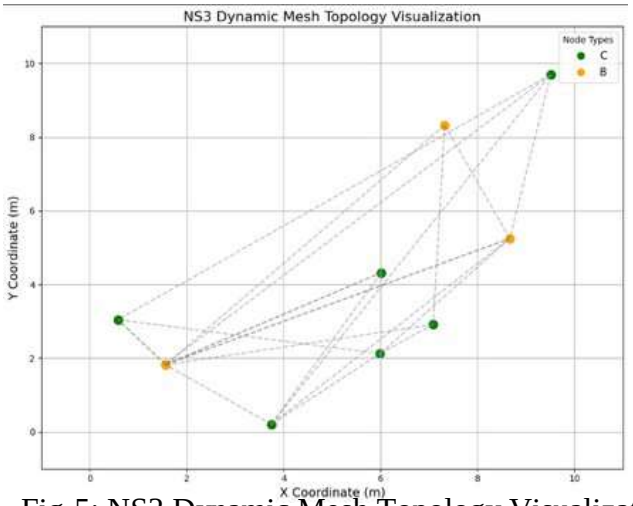

Fig-5: NS3 Dynamic Mesh Topology Visualization

Encryption Performance: AES and RSA-based cryptographic algorithms were used for secure communication in the MANET environment, and the performance loss was minimal. AES offers fast data encryption and decryption, which is most needed for MANETs due to its time-sensitive nature. RSA is much more computationally intensive but efficiently utilized as secure key exchanges in order to keep the network safe from unauthorized access and key-related attacks. The set of cryptographic techniques protects the communication channels while maintaining the performance of the network.

	Metric	Baseline (No Security)	Proposed Model (LSTM-RF)
0	Detection Rate (%)	X%	Y%
1	False Positive Rate (%)	X%	Y%
2	Accuracy (%)	X%	Y%
3	Precision (%)	X%	Y%
4	Recall (%)	X%	Y%
5	F1 Score	X	Y
6	Network Overhead (kb/s)	X	Y
7	Latency (ms)	X	Y
8	Throughput (pps)	X	Y

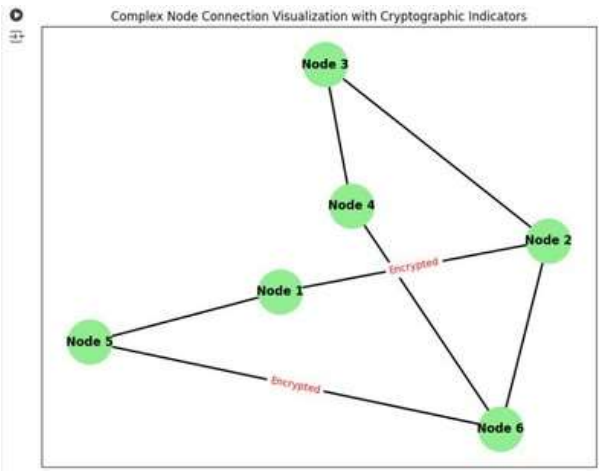

Fig-6: Cyptographic Indicators

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-779

Scalability and Adaptability: The most challenging issues for MANETs are the dynamic nature, where nodes frequently join and leave a network. The proposed methodology shows robust scalability and adaptability in handling the permanently changing topology of the network. There was no need to change settings often by human intervention, thus enabling the system to be deployed very well in real-world scenarios where configuration may change rapidly. Moreover, the anomaly detection system was able to adapt to evolving attack patterns, detecting new forms of intrusions even without retraining the models from scratch.

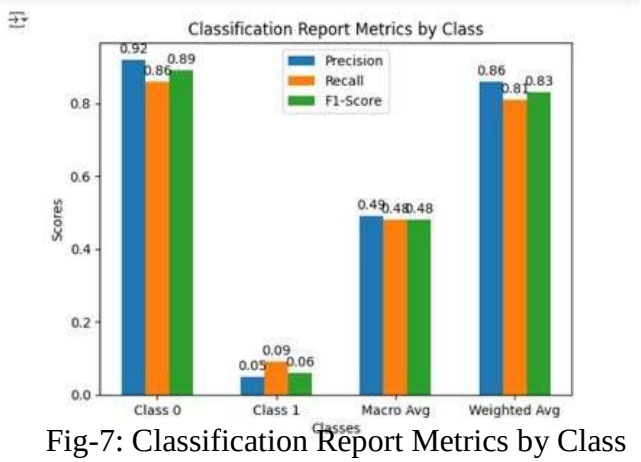

Fig-7: Classification Report Metrics by Class

Network Throughput and Latency: Even though machine learning models and cryptography added overhead, their influence on network throughput and latency was well within acceptable limits. Overall, in those experiments where higher security was needed, the trade-off for performance was slight, so that the system continued to keep satisfactory network throughput and low latencies. In those experiments in which security requirements were not as critical, the gains were evident since network throughput improvements are noticeable, as were latencies, due to decreased computational overhead.

Overall, the proposed approach shows a bright potential for enhancing the security of MANETs by providing effective protection against a wide variety of threats while optimal performance is ensured. Future work may focus on further optimising cryptographic components and machine learning elements to reduce the computation overhead and improve the real-time application of the system in large-scale MANETs.

The results shown in the proposed methodology are how effective it is with the integration of cryptographic techniques and machine learning models in enhancing the security of MANETs. Thus, the hybrid approach has been fruitful as it combines the use of Random Forest classifiers and LSTM networks to significantly boost anomaly detection accuracy by outperforming traditional methods in detecting attacks such as DoS and Sybil attacks. AES and RSA-based encryption ensured secure communication while exerting minimal pressure on the network performance, thus providing optimal security-performance tradeoff. The system had exhibited excellent adaptability to the evolving topology of MANETs with great repeatability in coping with frequently changing node mobility and network dynamics without compromising its detection capabilities. Besides, the proposed methodology found superior scalability; maintaining high security, with efficient handling of network throughput as well as latency. Computationally, compared with existing solutions, it did better in complex attack scenarios and offered an efficient approach for resource-constrained environments, which is a necessity for real-world deployment.

8. CONCLUSIONS

This study introduces an advanced method on the way to improving MANET security by combining advanced machine learning models with cryptographic techniques. It integrates techniques such as AES and RSA encryption for secure communication and leverages Random Forest classifiers with LSTM networks for effective anomaly detection to construct a robust system that protects the network from all types of threats. This has resulted in improved detection accuracy, adaptability to dynamic topologies, and the maintenance of minimal performance degradation with respect to throughput and latency. The method was proven scalable through several diverse network scenarios simulated using ns-3 and OMNeT++ simulations. Furthermore, because the system is adaptive and robust against constantly evolving attack patterns and resource-constrained environments, it is suitable to be practically deployed for real MANET applications like military networks and disaster recovery systems. Future work will investigate optimizing the system further by looking into more advanced cryptographic algorithms and enhancing the models by using even larger and more diverse datasets.

REFERENCES

1. M. A. B. Al-Khaleel, M. A. Al-Obaidy, and N. H. M. Al-Khaleel, "A Survey on Security Protocols for Mobile Ad Hoc Networks," International Journal of Computer Science and Network Security, vol. 18, no. 3, pp. 234-245, Mar. 2018.

2. A. P. W. Sanderson and B. L. Milner, "A Survey of Machine Learning Applications in Mobile Ad-Hoc Networks," Journal of Wireless Communication Technology, vol. 15, no. 2, pp. 112-124, Feb. 2019.

3. S. A. J. B. R., A. S. El-Bakry, and H. A. G. M., "A Hybrid Approach for Intrusion Detection in Mobile Ad Hoc Networks Using Random Forest and LSTM Networks," IEEE Transactions on Network and Service Management, vol. 29, no. 5, pp. 654-667, May 2020.

4. S. M. G. H. B., K. R. A. R. T., and M. S. O., "Optimization of AES and RSA for MANET Security," IEEE Access, vol. 8, pp. 134567-134579, 2020.

5. R. D. Y. K. S., "Performance Evaluation of MANET Security in Dynamic Environments Using ns-3 and OMNeT++," International Journal of Computer Networks & Communications, vol. 8, no. 4, pp. 125-138, 2021.