iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VII **Month of publication:** July 2025

DOI: https://doi.org/10.22214/ijraset.2025.73441

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Malicious Node Detection in MANETs using Trust Based Approach

Dr. K. Suresh Babu[1], K. Sai Charan[2]
[1]*Professor of CSE, JNTUH University College of Engineering, Science and Technology*
[2]*M.Tech CFIS II year, JNTUH University College of Engineering, Science and Technology*

Abstract: ***Mobile Ad-hoc Networks (MANETs) are decentralized wireless networks. The characteristics of MANETs are dynamic topology and a lack of fixed infrastructure. These features make them highly flexible and expose them to significant security vulnerabilities. To overcome these vulnerabilities, our energy composite trust model calculates a trust score for each node based on its packet forwarding behaviour and energy consumption. It also incorporates a direct mechanism for identifying flooding attacks by monitoring packet traffic rates. The proposed system was implemented and evaluated using the NS-3 simulator. Simulation results in NS-3 demonstrate that the proposed method effectively isolates malicious nodes.***
Keywords: MANET, Trust Evaluation, Malicious Node Detection, Energy Trust, Forwarding Trust, NS-3, AODV, Intrusion Detection

I. INTRODUCTION

Mobile ad-hoc networks (MANETs) are decentralized wireless networks consisting of mobile devices, known as nodes, that communicate with each other without relying on a fixed infrastructure. The characteristics of a MANET are dynamic topology, an open wireless network, and a lack of centralized control, which makes it highly vulnerable to malicious attacks.

Nodes in a MANET are expected to cooperate by forwarding packets for each other. Malicious nodes can exploit this open environment to launch attacks, such as packet dropping, resource depletion, and Denial-of-Service (DoS), severely affecting network performance and reliability. This paper presents a trust-based intrusion detection system that monitors energy usage, forwarding behaviour, and Threshold-based detection of network flooding to identify and isolate malicious nodes. By combining these trust metrics, our model can accurately identify and isolate malicious nodes, enhancing the MANET's security.

II. RELATED WORK

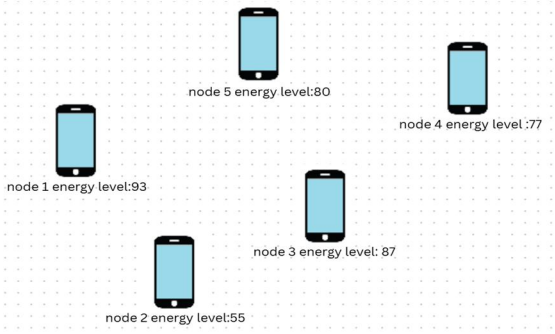
Several trust-based methods have been suggested for MANETs. Some models depend exclusively on packet forwarding behaviour, whereas others consider watchdog techniques or third-party monitoring.

Other research has targeted specific attack vectors, some models are concerned with only data-plane trust, evaluating nodes in terms of packet delivery ratios. They resist simple dropping attacks, but cannot detect more covert attacks such as resource depletion. Some studies have also investigated energy-aware trust, where nodes with high energy drainage are viewed as less reliable for routing. However, these systems may not detect a selfish node that conserves its energy by refusing to forward packets.

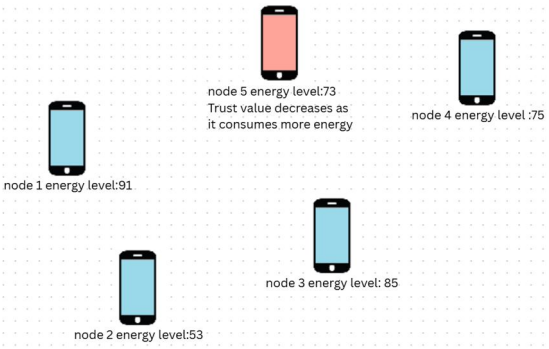
Our approach integrates forwarding trust and energy trust for comprehensive detection and flooding detection in each node.

III. ENERGY COMPOSITE TRUST MODEL

The energy-based composite trust model monitors each node's energy consumption, and when a node's energy consumption is greater than that of the normal nodes in a network, the node's trust value that consumes more energy decreases.

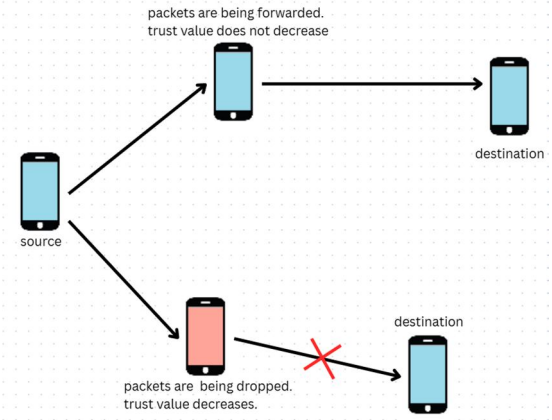


After some time, the energy levels are,

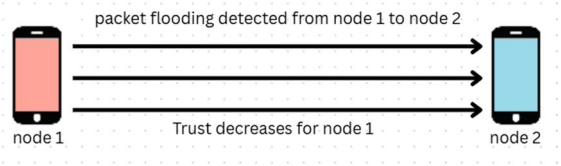


In the above diagram, node 5 consumed more energy than the other nodes.

This model also monitors packet forwarding and packet dropping of a node, and when a node drops packets or does not forward packets, then the trust value of that node decreases.



This model also detects a flooding attack from a node and decreases the node's trust value, causing the flooding attack.



The trust model is built upon three trust metrics, they are: Energy Trust, Forwarding Trust, and a mechanism for Flooding Attack Detection.

A. Forwarding Trust (F_{trust})

This metric is calculated as the ratio of packets successfully forwarded to the total packets received for forwarding (forwarded plus dropped packets).

$$F_{trust} = \frac{P_{fwd}}{P_{fwd} + P_{drop}}$$

P_{fwd} is the count of packets forwarded.

P_{drop} is the count of packets dropped.

F_{trust} is the forwarding trust value of the node.

A cooperative node has a forwarding trust value of 1.0, which will become lower if a node drops packets.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

B. Energy Trust (E_{trust})

This metric evaluates a node's energy consumption behaviour to detect energy drain over time. The idea is that nodes that consume energy at a normal or expected rate are considered more trustworthy, while those with abnormally high consumption (which may indicate malicious or selfish behaviour) are penalized.

If the consumption rate is less than or equal to normal, then energy trust is equal to 1.

$$E_{trust} = 1$$

If the node's energy consumption rate (C) is higher than a "normal" rate (N), a penalty is applied.

$$\text{Penalty} = \min\left(0.5, \frac{C-N}{N} * 0.5\right)$$

$$E_{trust} = E_{trust} * (1 - \text{Penalty})$$

The penalty can reduce the energy trust by up to 50%.

The formula for consumption rate(C) is

$$C = \frac{X[i] - \text{remaining}}{Y - Z[i]}$$

X[i] is last recorded remaining energy for node i, where i is number of nodes.

Remaining is the current remaining energy of the node.

Y is the current time in simulation.

Z[i] is the last time the energy was checked for node i.

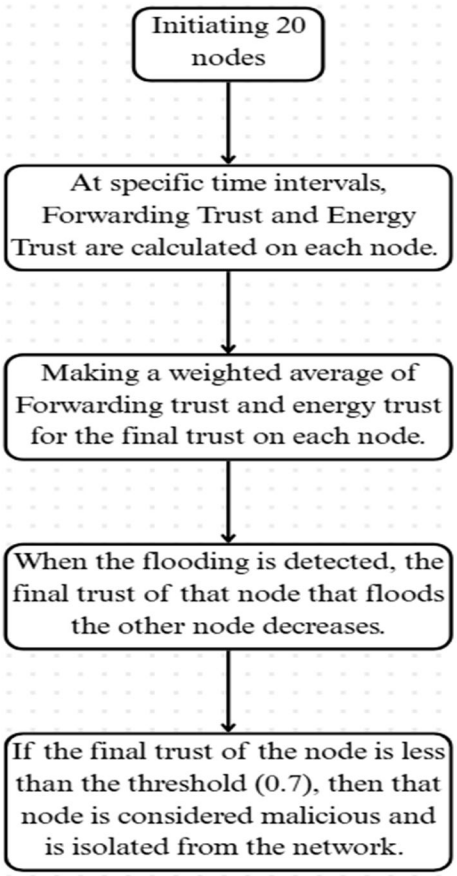
C. Combined trust Calculation

The final trust score is a weighted average of the forwarding and energy trust metrics.

$$\text{Final trust} = (\alpha * E_{trust}) + (ß * F_{trust})$$

Where α = 0.7 and ß = 0.3, these values are used in the simulation.

D. Process Flow



E. Flooding Attack Detection

A separate threshold-based detection mechanism is implemented to counter high-volume denial-of-service attacks. Each node monitors the rate of incoming packets from its neighbors. A flooding attack is detected if the number of packets received from a specific source exceeds a predefined flood threshold within a short time window. Upon detection, the trust score of the offending node is immediately and significantly penalized, accelerating its isolation.

F. Node isolation Mechanism

The combined trust score is initialized to 1. A node is malicious if its combined trust score is less than the minimum trust threshold, set as 0.7 in our simulation. A malicious node is isolated by terminating all its applications, disabling its network devices, and setting its network interfaces down, removing it from its neighbours' routing tables.

G. Simulation Setup

The simulation is performed on NS-3.43 with 20 mobile nodes distributed across a 500 x 500 meter field. Node mobility is according to the Random Walk 2D model for the simulation of dynamic movement. The AODV (Ad hoc On-Demand Distance Vector) routing protocol supports the communication of the nodes. Nodes are given an initial energy value of 100 Joules. Node 5 is set as the malicious node and shows packet-dropping behavior with a 70% probability. A flooding detection algorithm is used. In this simulation, the malicious node sends more than 500 packets in 2 seconds, which is identified as probable flooding. The simulation is executed for 30 seconds, and in that time, trust assessment is conducted, and nodes below the threshold of isolation level of 0.7 are labeled as malicious and deleted from the network.

IV. RESULTS AND ANALYSIS

The effectiveness of our trust model was evaluated by observing the trust score of the malicious node over the simulation time and confirming its eventual isolation.

In the NetAnim visualization tool. Initially, normal nodes were colored green, and the malicious node (Node 5) was yellow. As the simulation progressed, we can see that the nodes are moving, and Node 5 began dropping packets and launching its attacks, its trust score, as reported in the simulation logs, steadily declined. Upon crossing the isolation threshold, Node 5's color changed to red, signifying it had been successfully identified and removed from network participation.

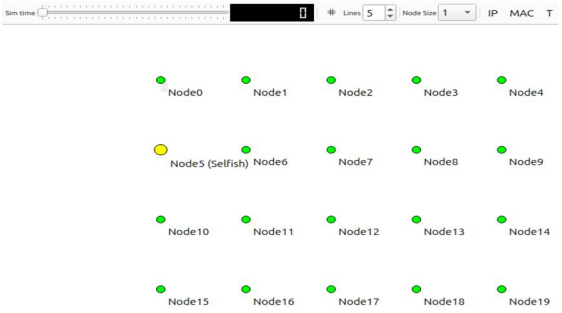


Figure 1 - simulation at 0 seconds

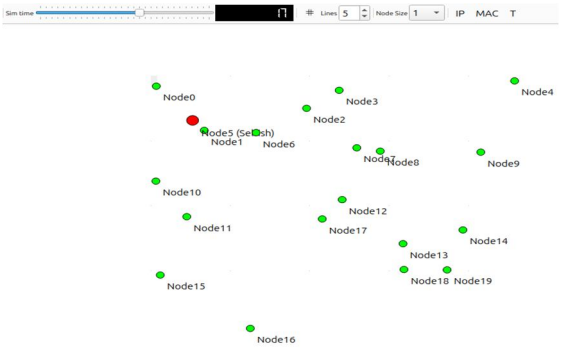


Figure 2 - at 17th second, the selfish node became red

The simulation logs provide a clear quantitative view of the trust evaluation.

The trust scores of all normal, cooperative nodes remained consistently high throughout the simulation, as their forwarding and energy consumption patterns were normal.

The trust score of Node 5 showed a sharp decline. The initial packet dropping lowered its Forward trust. The flooding attack at the 10-second mark caused a direct, sharp penalty to its combined trust score. The combination of these factors and its high energy consumption, reducing its energy trust, pushed its overall trust score below the 0.7 threshold. The logs confirmed its isolation shortly after its malicious behavior became persistent.

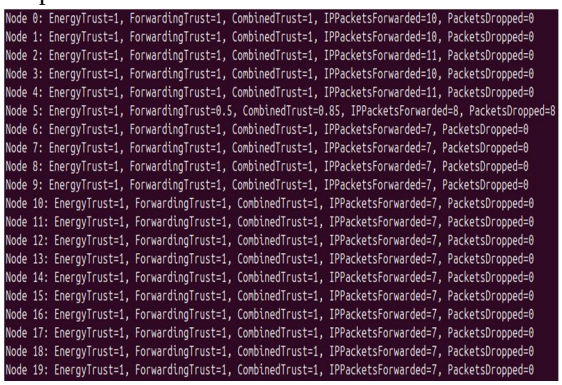


Figure 3 - forward trust is decreasing

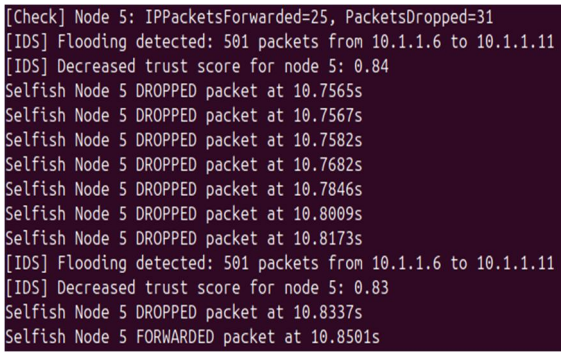


Figure 4 – flooding is detected, and the trust score is decreasing

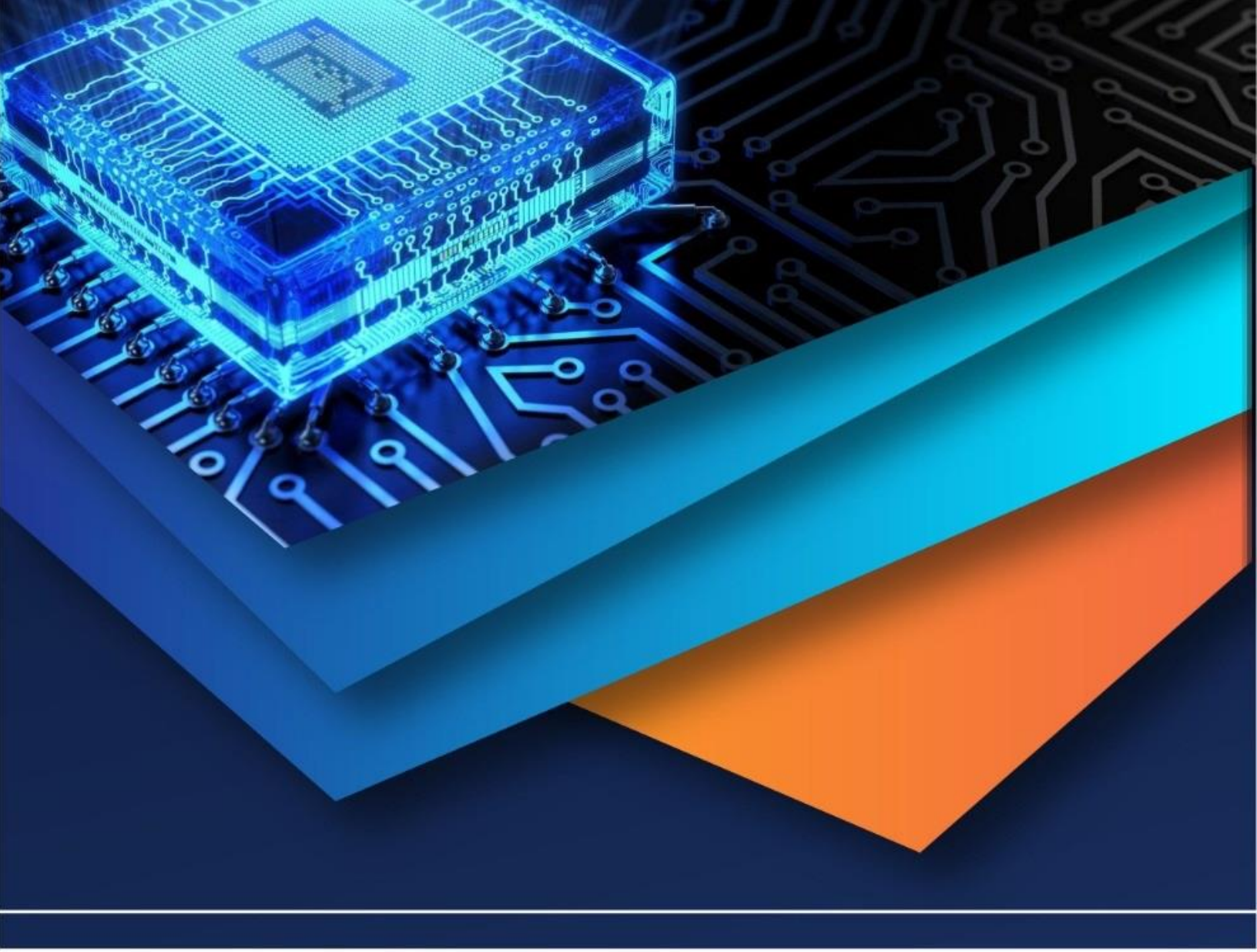
Figure 5 - energy trust decreased and, the node is removed

V. CONCLUSION

This paper presented a trust model that uses forwarding behaviour and energy consumption for trust metrics and integrates a specific flood detection mechanism that decreases the malicious node's trust. The NS-3 simulation results confirmed that the system can successfully identify a node performing simultaneous packet dropping, energy drain, and flooding attacks, and isolate it from the network to protect other nodes.

REFERENCES

[1] Govindan, K., & Mohapatra, P. (2011). Trust computations and trust dynamics in mobile adhoc networks: A survey. IEEE Communications Surveys & Tutorials, 14(2), 279-298.
[2] Ponnusamy, M., Senthilkumar, A., & Manikandan, R. (2021). Detection of selfish nodes through reputation model in mobile adhoc network-MANET. Turkish Journal of Computer and Mathematics Education, 12(9), 2404-2410.
[3] Sen, J. (2010, July). A distributed trust and reputation framework for mobile ad hoc networks. In International Conference on Network Security and Applications (pp. 538-547). Berlin, Heidelberg: Springer Berlin Heidelberg.
[4] Aravindh, S., Vinoth, R. S., & Vijayan, R. (2013). A trust based approach for detection and isolation of malicious nodes in manet. International Journal of Engineering and Technology (IJET), 5(1), 193-199.
[5] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265).
[6] Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. IEEE Communications magazine, 40(10), 70-75.
[7] Veeraiah, N., Khalaf, O. I., Prasad, C. V. P. R., Alotaibi, Y., Alsufyani, A., Alghamdi, S. A., & Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. IEEe Access, 9, 120996-121005.
[8] Kukreja, D., Dhurandher, S. K., & Reddy, B. R. (2018). Power aware malicious nodes detection for securing MANETs against packet forwarding misbehavior attack. Journal of Ambient Intelligence and Humanized Computing, 9(4), 941-956.
[9] Shan, A., Fan, X., Wu, C., Zhang, X., & Fan, S. (2021). Quantitative study on the impact of energy consumption based dynamic selfishness in MANETs. Sensors, 21(3), 716.
[10] Riley, G. F., & Henderson, T. R. (2010). The ns-3 network simulator. In Modeling and tools for network simulation (pp. 15-34). Berlin, Heidelberg: Springer Berlin Heidelberg.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY