ISSN: 2584-0495 Vol. 2, Issue 4, pp. 706-713

International Journal of Microsystems and IoT

ISSN :(Online) Journal homepage: https://www.ijmit.org

EIGRP-Based Hybrid Routing Approach for MANETs

Chitra D, Divya K, Vijay Nath

Cite as: Chitra, D., Divya, K., & Nath, V. (2024). EIGRP-Based Hybrid Routing Approach for MANETs. International Journal of Microsystems and IoT, 2(4), 706-713. https://doi.org/10.5281/zenodo.11208955

Published online: 22 April 2024.

DOI: https://doi.org/10.5281/zenodo.11208955

International Journal of Microsystems and IoT
Vol. 2, Issue 4, pp. 706-713; DOI: https://doi.org/10.5281/zenodo.11208955

EIGRP-Based Hybrid Routing Approach for MANETs

Chitra D [1], Divya.K [2] and Vijay Nath[3]

[1]Department of Electronics and Communication Engineering, Mahendra Engineering College, Namakkal, Tamilnadu, India
[2]Department of Electronics, IHRD College of Applied Science, Payyannur, Kerala, India
[3] Department of Electronics and Communication Engineering, Birla Institute of Technology, Mesra, Ranchi, India

ABSTRACT
In a MANET (mobile ad-hoc network), several mobile nodes are wirelessly linked to each other, but there is no central network infrastructure. The topological changes that occur often, the efficient use of the energy resources that are available, the associated routing overheads, and susceptibility to assaults are the main challenges encountered in the design of routing protocols for MANETs. This article presents a more secure and efficient routing method that makes use of modified EAACK when used with hybrid EIGRP. EIGRP uses the DUAL, an enhanced distance vector protocol, to establish the optimal route between source and destination. Using the modified EAACK scheme, this method successfully addresses several of the shortcomings of standard intrusion detection systems. S-ACK is unable to tell the difference between a legitimate node and a malicious one. When looking for malicious nodes, P2P ACK is superior to S-ACK. In this technique, the P2P ACK acknowledgment packets of the modified EAACK are signed and verified using the RSA algorithm. To improve MANET security, the suggested approach makes use of a modified version of the RSA public key cryptography technology. This suggested method improves overall performance by raising security standards, cutting down on routing overhead, and speeding up packet delivery.

KEYWORDS
EAACK; MANET; Intrusion detection systems; Misbehaving nodes; P2P ACK.

1. INTRODUCTION

A MANET is a group of wireless mobile devices that act independently of one another. Multiple routing requirements are typically required by the MANET. As a result, creating routing protocols for MANETS is extremely difficult. As mobile nodes join and exit the network, its topology frequently shifts. The fact that mobile devices rely on battery power is a significant challenge for wireless ad hoc networks. It takes a long time to recharge or replace batteries when they run out. To lower the energy consumption for packet delivery, it is necessary to make effective use of the energy resources that are currently available. Because of their wireless links and flexible, dynamic topologies, MANETs are more vulnerable to security breaches. There is the possibility for both malicious nodes inside the network and external to the network to develop. Simultaneously, in a wired network, security attacks are stopped by the system's components like switches, routers, and firewalls, which identify and examine node behavior. Strong intrusion detection techniques and other security measures, like digital signatures and encryption, are required to give extra security to prevent unauthorized access.

The many routing issues in MANET fall into the class of NP-hardness. In the year of 1990s, several routing protocols, including DSDV ("Destination Sequenced Distance Vector"), DSR ("Dynamic Source Routing"), and AODV ("Ad Hoc On-Demand Distance Vector"), were suggested for MANETs. These protocols are developed for simple routing tasks. However, self-organized MANETs have other requirements, including low packet latency, a high packet delivery ratio, flexibility in responding to changes in network architecture, efficient use of resources, and encrypted communication.

This approach aims to create a safer as well as optimized routing process for MANETs. This system assures that only authorized nodes may share information. It is based on the EIGRP ("Enhanced Interior Gateway Routing Protocol"), a hybrid vector routing protocol which uses a DUAL ("Diffused Update Algorithm") and encryption based EAACK (Enhanced Adaptive Acknowledgement). To evenly distribute data traffic throughout a network, multipath routing uses load balancing techniques like load sharing and multiple communication channels to provide several paths to the source nodes. The acknowledgment packet type of EIGRP in this work uses an improved EAACK method. To improve the security features, the RSA encryption algorithm is applied.

2. MAJOR RELATED WORKS

MANETs are flexible wireless networks that may be set up in a variety of locations, such as LANs, MANs, military environments, and disaster relief areas. If the mobile nodes in a SI is a method of computational intelligence, and a system of SI is built from a collection of basic agents which communicate and collaborate with one another, and their immediate surroundings decentralized. SDS (Stochastic Diffusion Search) [3], PSO (Particle Swarm Optimization) [4], and ACO (Ant Colony Optimization) [5] are some of the well-known metaheuristics that are used in the SI discipline. Maintaining and optimizing routing in dynamic and self-organizing networks like MANETs is a prime application for ACO algorithms. Nithya et al. [6] provide a method based on Ant Colony Routing Optimization that takes into consideration security concerns. In addition to improving the SNR and the packet delivery ratio, this fuzzy Ant Colony Optimization approach also helps to decrease packet loss.

Veeraiah et al. [7] proposed the Cat Slap Single-Player Algorithm (C-SSA) for a more secure and effective MANET. It employs multi-hop routing based on a fuzzy technique for choosing Cluster Heads (CHs). To choose the best route, it considered the nodes' connectivity, throughput, and time delay. However, throughput rather than overall efficiency was the focus of this approach. Mallikarjuna and Patil [8] introduced an AODV protocol that makes use of the hash function and a location updating method. Packet losses are kept to a minimum with this strategy. Selfish nodes may be avoided with the use of a hash function that regularly updates its position. According to Halhalli et al. [9], Atom Whale optimization is the foundation of a reliable routing system. The trust attributes of the mobile nodes—like frequency of successful cooperation, average encounter rate, and forwarding rate integrity factor—are what this technique depends on. The method combines the techniques.

for Whale Optimization and Atom Search Optimization. “Another trust-based, energy-effective multipath routing approach for MANETs is offered by Alappatt and Pratap [10]”. This approach removes any potentially vulnerable nodes after determining which multipath is the most secure based on direct and indirect trust levels of the nodes.

For MANETs specifically, there is a new intrusion detection mechanism known as EAACK. Based on the DSR protocol, a new acknowledgment-based system (NEWACK) was introduced in [11]. An intrusion detection system known as A3ACKs (Adaptive Three Acknowledgments) has been proposed in [12] to solve 3 main problems with the watchdog method: mutual attacks, receiver collisions, and limited transmission power. In [13], researchers created a dependable and reasonable opportunistic routing system for MANETs named ORGMA that makes use of gradient forwarding. It was chosen to use the Gradient Forwarding technique, in which the receivers choose the optimum path after receiving only one packet from the sender. The Hybrid Enhanced Adaptive MANET can be relied on and work cohesively, the network will succeed. Inspired by biological systems, scientists have developed a plethora of decentralized meta-heuristics [1]. In their study of cellular robotic systems, Beny and Wang [2] applied the theory of SI (Swarm Intelligence) to AI.

Acknowledgement (HEAACK) [14] discussed establishes a secure network while lowering the data utilization rate and network overhead. It does this by using cryptographic algorithms like RSA and Triple DES.
The several present MANET routing methods have been discussed Table 1.

3. PROPOSED METHODOLOGY

To boost the MANET's productivity and safety, this research proposes a novel EIGRP hybrid approach based on EAACK and encryption methods. In the first phase, the EIGRP protocol may be used to construct a whole network. Here, the EIGRP protocol chooses the way based on the available bandwidth and compiles a list of route delay information to minimize latency. In this hybrid protocol, a proactive protocol may make use of Interior Gateway Routing to expedite packet delivery or communication along a predetermined route. Therefore, the EIGRP routing protocol lessens the burden of routing. To increase the network's security, a modified EAACK scheme is integrated with the EIGRP network architecture.

In this case, a better EAACK is employed to increase the detection rates of malicious activity. In this case, EAACK uses P2P ACK rather than S- ACK. The RSA public key exchange technique is used in the proposed system to lessen the necessity for pre-distributed keys. The keys used to encrypt packets using a public key are generated via the RSA method.
The RSA technique's keys are used to decode packets during the acknowledgment phase of P2P ACK. The P2P ACK confirmation packet should “be sent from the first node to the second node on the route. If the 2nd node waits to transmit the P2P ACK to the 1st node while the encrypted packets are being decrypted, the 1st node may recognize the 2nd node as a malicious node and report this to the source node”. This P2P ACK procedure may be performed at each successive node throughout the network to identify spoofed confirmations that cause packet loss.

Very little packet loss is anticipated with this suggested system's higher PDR, lower overhead, excellent energy efficiency, and enhanced security.
The stages of the proposed method are as follows.
A. Network construction by utilizing “the EIGRP hybrid protocol.
B. Utilization of modified scheme of EAACK
C. Encryption utilizing the algorithm” of RSA.

A) Network construction using the EIGRP hybrid protocol

The dynamic routing protocol EIGRP, a hybrid vector routing protocol, is used in the recommended design. The ideal path from the source to destination is chosen using the EIGRP. It exchanges information quickly and efficiently while finding a different route. This method of multipath routing helps to

distribute traffic around the network by using available resources at each node. Multichannel communication and resource sharing among nodes provide the basis for the chosen route. Each node's queue size, remaining energy, energy use per packet, and available bandwidth are all reported during the route request. The cost function at the final node is determined using the data gathered, and the best routes are then selected using the new cost function.

The EIGRP provides the following:

A system that uses neighbor detection and maintenance to only transmit non-periodic incremental updates.

A method for figuring out which loop-free pathways to consider as potential successors.

A method for removing incorrect routes from the network's topology tables.

A strategy for locating long-lost locations by scouring the areas around them.

Non-periodic incremental routing updates are used by EIGRP to disseminate routing information throughout the network; these updates contain information about the route that has changed. Routing table changes in EIGRP are broadcast to all nodes in the network via neighbor relationships. When two nodes exchange HELLO packets over a shared connection, they are considered neighbors. EIGRP broadcasts HELLO packets every 5 seconds over high-bandwidth connections. The maximum number of neighbors that may be supported by EIGRP is not specified. The device's capability will determine the actual number of neighbors.

Instead of depending just on “the routing table, which contains all the data it requires to operate, EIGRP produces a topology table by which it adds routes. Metrics like the minimum bandwidth on a path to a destination as observed by an upstream neighbor, path loading, path reliability, total time delay, MTU (minimum path maximum transmission unit), route source, feasible distance, etc. are all contained in the topology table and can be used to generate a set of vectors and distances to each of the reachable nodes.

B) The modified EAACK scheme

Numerous problems in conventional intrusion detection systems, including transmission power restriction, receiver collision, false misbehavior reports, and ambiguous collisions, may be fixed by using the modified EAACK technique. The three most crucial components of an EAACK, in addition to the data field, are acknowledgement (ACK), secure acknowledgment (S-ACK), and misbehavior report authentication (MRA).

Instead of using S-ACK, the suggested EIGRP hybrid protocol uses P2P ACK in EAACK. Inaccurately identifying a malicious node is a major limitation of S-ACK. Therefore, to effectively identify the offending nodes, we use the P2P ACK rather than the S-ACK. To identify malicious nodes, the proposed EAACK system uses a pair of nodes in each P2P ACK procedure. Each node in P2P ACK decrypts messages using the encrypted public key.

P2P acknowledgment between two successive nodes requires each node to independently decode messages using RSA public key cryptography within a certain amount of time. If a delay occurs in the decryption and acknowledgment process for two consecutive nodes, the node that experienced the delay is labeled as malicious. For every pair of adjacent nodes in a network, the same procedure is repeated. The suggested system detects this kind of misbehavior node by reporting the source node in the network a delay in packet delivery with acknowledgment. P2P is depicted in figure 1.

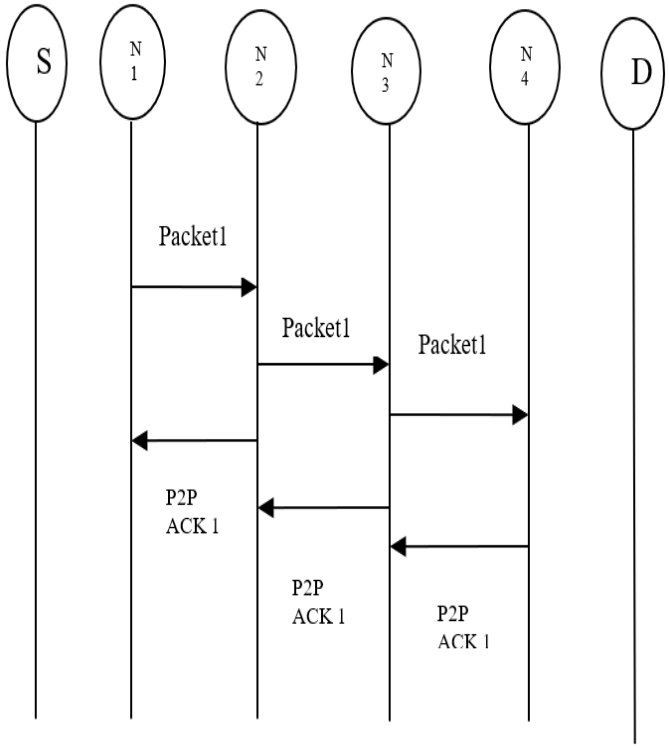

Fig. 1 P2P ACK

Let's say we have four nodes, N1, N2, N3, and N4. At nodes N1 and N2, N2 and N3, and N3 and N4, the P2P ACK is performed. In the case that node N2 fails to transmit the P2P ACK acknowledgment packet to node N1 within the specified time frame, node N1 generates a misbehavior report for node N2 and sends it to the source node. The suggested system can instantaneously determine the time difference between any two nodes in a chain, such as N1 and N2. If N3 does not acknowledge N2's P2P ACK within the allotted period, N3 is flagged as a false node. In a similar vein, if node N4 is late in transmitting the P2P ACK acknowledgment packet to node N3, it will be deemed a misbehaving node as well as the source node will get a complaint about it. As a result, it identifies malicious nodes in the network and performs a thorough security audit of the final confirmation.

C) Encryption using the RSA algorithm

This approach uses the RSA technique to produce and disperse keys for validating and signing P2P ACK acknowledgment packets of modified EAACK. This proposed method improves MANET security by using a modified version of the RSA public key cryptography technology.

Table. 1 Comparing different MANET routing methods.

	Aim	Approach used	Energy consumption	Packet Delivery Ratio	Bandwidth utilization	Intrusion detection means	Delay
[15]	To reduce the energy consumption and to improve the network's lifetime	AODV Elephant Herding Optimization technique	Low energy consumption at constant low mobility speed	Better PDR at constant low mobility speed	Good bandwidth utilization in low mobility speed	Backup routes are provided without considering the attackers	Delay will occur
[16]	To detect malicious nodes and aims to control the congestion	A trust-based multipath approach is used for improving the QoS and to detect the presence of attackers	Better energy utilization only with low mobility nodes	PDR decreases when congestion is present	Poor bandwidth utilization	Not focused on intruder detection measures	Delay will occur in case of congestion.
[17]	To design an analysis a novel mobility and obstacle-aware algorithm	DeCasteljau algorithm with Bezier curves for obstacle avoidance with a high-speed mobility prediction concept	Reduced energy consumption compared with existing AODV protocols	Alternate paths are listed and provides better PDR by selecting reliable and efficient routes	Reduced network overhead and provides good bandwidth utilization	Obstacles in the route are avoided. Need to focus on attacks	Reduced delay
[18]	Aims in an improved secure multipath routing	A hybrid GA-Hill Climbing algorithm is used to pick the optimal route in multipath	Low energy consumption	High detection rate results in good PDR	Not evaluated	Security measures to prevent selective packet-dropping attacks	Small delay time
[19]	To improve energy efficiency and communication latency	BFOA to optimize routing with fuzzy cluster head selection based on the trust values	The route is selected to minimize the energy consumption	Better PDR	Good bandwidth utilization	Intruder detection is based on the threshold value	
[20]	To improve the node energy utilization and bandwidth utilization	Adaptively control the network congestion and achieve load balancing with cloud MANET services.	Depends on the status of congestion	Not evaluated	Bandwidth utilization is poor in case of higher data rate	Need to focus on security measures.	Improved delay
[21]	An adaptive N-channel routing approach to improve energy utilization, and bandwidth utilization with load balancing.	Routes are selected based on the cost function considering the residual energy, energy consumption per packet, queue length and bandwidth capacity	Low energy consumption	Good PDR with low packet drop rate	Good bandwidth utilization with load balancing	Need to focus	Low delay values
[22]	Aims to prolong nodes' clustered time and enhance consistency between cluster relationships with improved energy utilization	Uses a randomly centralized CH selection that works in an event driven on-demand manner reducing the frequent cluster head handovers	Ensures high energy efficiency	Good PDR	Good bandwidth utilization	Malicious nodes can be avoided based on the cluster relationships	Low delay

This enables two users to securely share a key that is required for both the acknowledgment process and further message encryption.
The RSA algorithm is used to encrypt the public key for safety, and it also helps the P2P ACK technique identify fake nodes. The RSA creates unique keys at random, and we use public key cryptography to send and receive session keys in a secure and un-hackable manner [23]-[25].
RSA public key cryptography is one of the most important and helpful applications of public-key cryptography. This is how the RSA algorithm produces keys:

- Two different prime numbers a and b are selected
- $n = a \times b$ is computed
- $\varphi(n) = \varphi(a)\varphi(b) = (a-1)(b-1)$ is calculated, where φ is totient function of Euler.
- An integer e is selected such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$, e and $\varphi(n)$ can be co-prime.
- d is determined as $d \equiv e^{-1} (\text{mod } \varphi(n))$; d can be the modular multiplicative inverse of e in the form of $(\text{mod } \varphi(n))$

A message M and a cipher C are considered here. Let n = 2048 bit and a & b are 1024 bit.
To encrypt the public key, the following given equation is used:

$$\text{Encryption: } M^e \equiv C \ (\text{mod } N) \qquad (1)$$

The following equation is used to decrypt the encrypted.

$$\text{Decryption: } C^d \equiv M \ (\text{mod } N) \qquad (2)$$

The P2P ACK procedure in our proposed system encrypts and decrypts messages using the following procedures.

Choose the public key.
We may securely deliver the public key to the chosen recipient using RSA public key cryptography.
Use the encryption algorithm RSA for the public key.
To obtain a public key permit, they must decrypt the communication using their private key.

4 RESULTS

To calculate the efficacy of the suggested and current approaches, this section provides a range of experimental network characteristics against which to compare their results. The proposed technique is tested using a variety of indicators and compared to industry standards. On a virtual machine (VM) workstation, the simulation is performed by utilizing Network Simulator 2 (NS2), JDK 1.8, and Ubuntu 9.10 operating systems. Table 1 summarizes common choices used when simulating networks.

To get this outcome, three distinct percentage-level steps were used in the simulation.

Step 1: Different nodes run P2P ACK and the findings are comparing to those of previously established techniques like Watchdog and TWOACK. At this point, the sending node can dispatch data packets accompanied by P2P ACK to the receiving node and watch for an acknowledgment packet bearing the same header.
Step 2: The suggested IDS is evaluated, and if successful, the reporting node will notify the reporting node via P2P ACK that a misbehaving node has been identified.
Step 3: To prevent packet loss, Misbehavior nodes are removed when forged acknowledgment has been found.

The PDR, RO, and time delay of the suggested system are calculated and compared to those of the existing methods TWOACK and BFOA. Table. 2 shows Network Simulation Parameters.

Table. 2 Network Simulation Parameters

Network parameters	Values
Area of Simulation	750m x 750m
Number of nodes	60
Packet size in byte	500
Simulation time (s)	110
Traffic	CBR
CBR Sessions	12

Packet Delivery Ratio (PDR)

The proportion of packets supplied by a node that were successfully transmitted by that node is called the node's PDR.

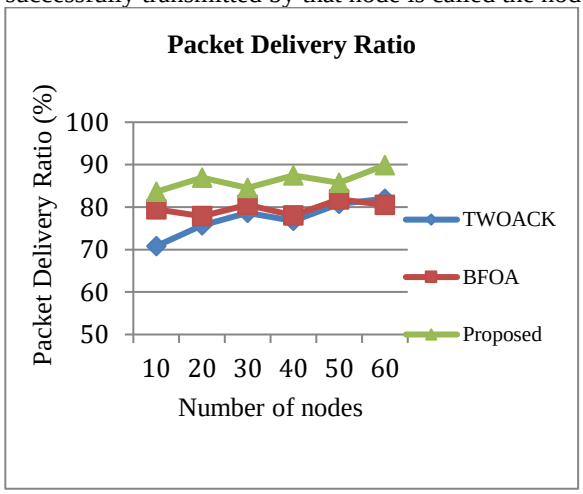

Fig. 2 PDR

Fig 2 demonstrates that this suggested system's PDR is greater than that of the current TWOACK and Watchdog methods. Misbehaving nodes lower the PDR during packet transmission. With the efficient detection of misbehavior nodes, the PDR decreases. The suggested system can identify the faked acknowledgment within the specified period, ensuring that all packets reach their destination. The packets are successfully transmitted to the receiving node.

Routing Overhead (RO)

The ratio of routing-related transmissions, like RREP, RREQ,

ACK, RERR, MRA, and P2P-ACK, is known as RO.

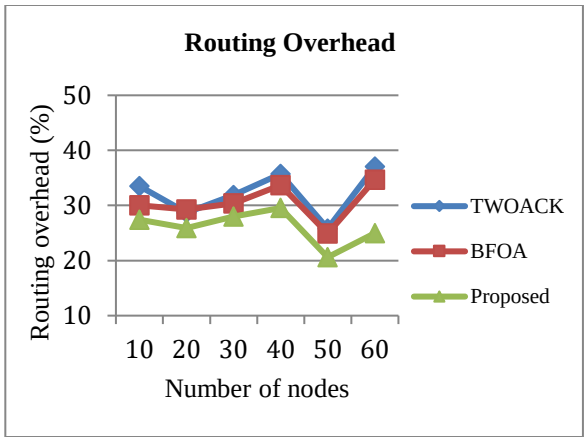

Fig. 3 Routing Overhead

Figure 3 depicts a comparison of routing overhead. It shows that the suggested system requires less overhead for routing than current approaches. The routing overhead in the proposed

Various stages of the simulation process are shown in Figure 4, Figure 5, Figure 6, Figure 7, Figure 8, and Figure 9.

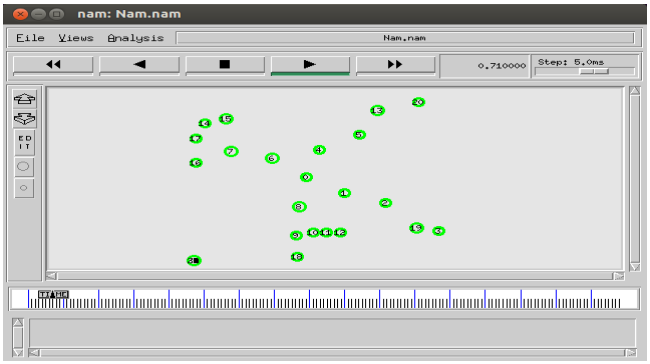

Fig. 4 Mobile nodes initialization

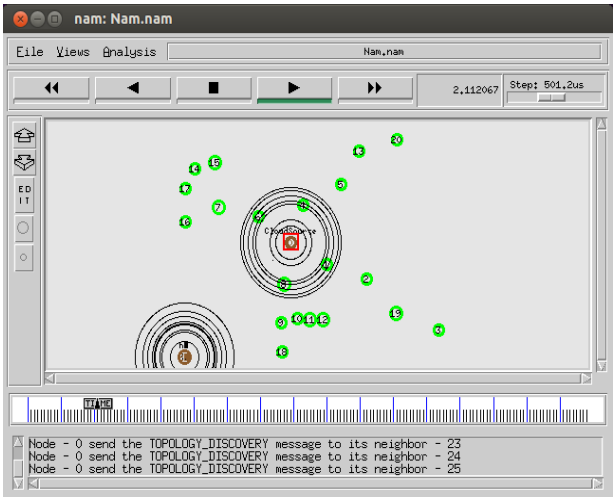

Fig. 5 Path discovery

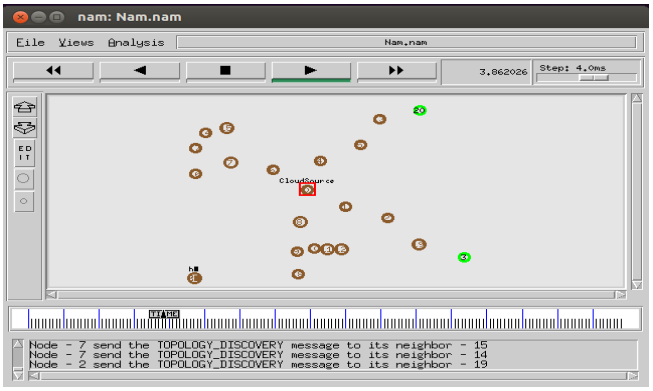

Fig. 6 Neighbors Identification

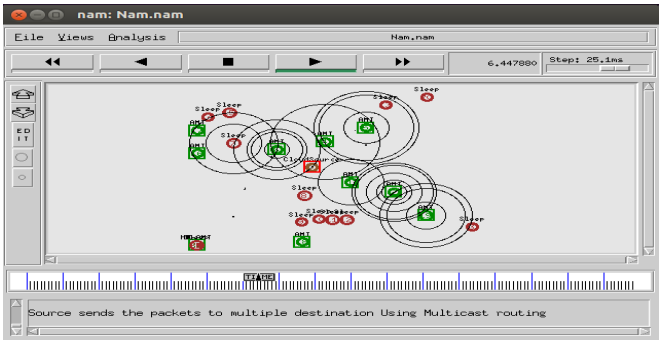

Fig. 7 Multicast routing

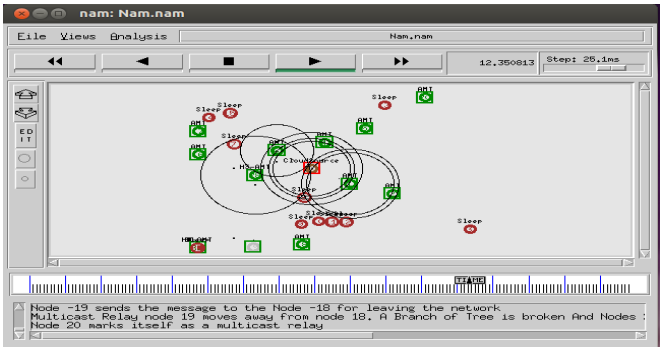

Fig. 8 Nodes Leaving the Network

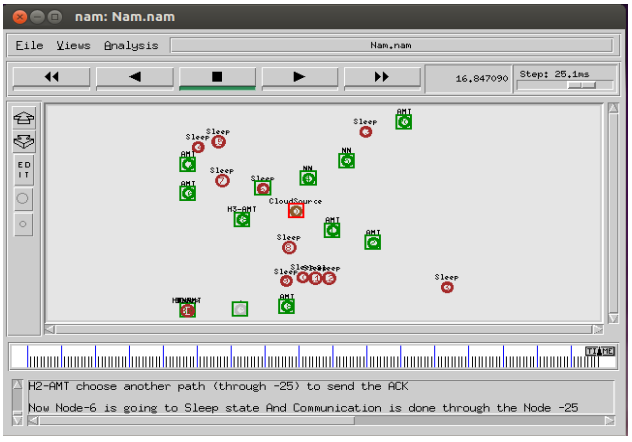

Fig. 9 Selection of Alternate Paths

5 CONCLUSION

In the event of malicious nodes, packet transmission is more dependable and quicker with this secure and efficient routing method. The DUAL, which operates effectively on precise network metrics, has been utilized by the EIGRP to calculate the optimal path. EIGRP guarantees lower network resource consumption and quick convergence time for topology variations. EIGRP reduces routing overhead by sending just the changes that are required at any given moment. Secure packet transmission is ensured by the effective detection of malicious nodes and forged acknowledgments through the use of modified EAACK in conjunction with RSA encryption techniques. We can conclude from the results that the recommended approach has improved PDR, RO, and packet delay.

REFERENCES

1. F. Dressler and O. B. Akan. (2010). ''A survey on bio-inspired networking,'' Comput. Netw., vol. 54, no. 6, pp. 881–900, . https://doi.org/10.1016/j.comnet.2009.10.024
2. G. Beni and J. Wang. (1993). ''Swarm intelligence in cellular robotic systems,'' in Robots Biological Systems: Towards a New Bionics? Berlin, Germany: Springer, 1993, pp. 703–712 https://doi.org/10.1007/978-3-642-58069-7_38
3. C. E. Perkins and P. Bhagwat. (1994). ''Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers,'' ACM SIGCOMM Comput. Commun. Rev., vol. 24, no. 4, pp. 234–244, https://doi.org/10.1145/190809.190336
4. C. Perkins, E. Belding-Royer, and S. Das. (2003). ''Ad hoc on-demand distance vector (AODV) routing,'' IETF, Fremont, CA, USA, Tech. Rep. rfc3561. Accessed: Oct. 26, 2017. [Online]. Available: https://tools.ietf.org/html/rfc3561
5. D. Johnson, D. Maltz, and J. Broch. (2001). "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks," in Ad Hoc Networking, C. E. Perkins, Ed. Boston, MA: Addison-Wesley Longman Publishing Co., Inc., pp. 139–172. https://doi.org/10.1007/978-3-540-45546-9_5
6. R. Nithya, K. Amudha, A. S. Musthafa, D. K. Sharma, E. H. Ramirez-Asis, P. Velayutham, V. Subramaniyaswamy, and S. Sengan. (2022). ''An optimized fuzzy based ant colony algorithm for 5G-MANET,'' CMC-Comput., Materials and Continua, vol. 70, no. 1, pp. 1069–1087, https://doi.org/10.32604/cmc.2022.019221
7. N. Veeraiah, O. I. Khalaf, C. V. Prasad, Y. Alotaibi, A. Alsufyani, S. A. Alghamdi, and N. Alsufyani. (2021). ''Trust aware secure energy-efficient hybrid protocol for MANET,'' IEEE Access, vol. 9, pp. 120996–121005, https://doi.org/10.1109/access.2021.3108807
8. A. Mallikarjuna and V. C. Patil. (2021). ''PUSR: Position update secure routing protocol for MANET,'' Int. J. Intell. Eng. Syst., vol. 14, no. 1, pp. 93–102, https://doi.org/10.22266/ijies2021.0228.10
9. S. R. Halhalli, S. R. Sugave, and B. N. Jagdale. (2021). Optimisation driven-based secure routing in MANET using atom whale optimization algorithm,'' Int. J. Commun. Netw. Distrib. Syst., vol. 27, no. 1, p. 77. http://dx.doi.org/10.1504/IJCNDS.2021.116484
10. V. Alappatt and J. P. P. M. (2021). ''Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E,'' Int. J. Comput. Netw. Appl., vol. 8, no. 4, p. 400, https://www.ijcna.org/Manuscripts/IJCNA-2021-O-30.pdf
11. Vahid Heydari. (2012). "A new acknowledgment-based scheme against malicious nodes and collusion attack in MANETs", IEEE 14th International Conference on Communication Technology, pp. 784 – 788 https://doi.org/10.1109/ICCT.2012.6511310
12. Abdulsalam Basabaa, Tarek Sheltami and Elhadi Shakshuki. (2014). "Implementation of A3ACKs Intrusion Detection System under Various Mobility Speeds", Procedia Computer Science, vol.32, pp. 571-578 https://doi.org/10.1016/j.procs.2014.05.462
13. DaehoKang, Hyung-SinKim, ChangheeJoo and SaewoongBahk. (2018). "ORGMA: Reliable opportunistic routing with gradient forwarding for MANETs", Elsevier Journals- Computer Networks, vol.131, pp. 52-64 http://dx.doi.org/10.1016/j.comnet.2017.12.001
14. ParthPatel, RajeshBansode and BhushanNemade. (2016). "Performance Evaluation of MANET Network Parameters Using AODV Protocol for HEAACK Enhancement", Elsevier Journals- Procedia Computer Science, vol.79, pp. 932-939 http://dx.doi.org/10.1016/j.procs.2016.03.118
15. S. Sarhan and S. Sarhan. (2021). ''Elephant herding optimization ad hoc on-demand multipath distance vector routing protocol for MANET,'' IEEE Access, vol. 9, pp. 39489–39499, https://doi.org/10.1109/ACCESS.2021.3065288
16. M. Sirajuddin, C. Rupa, C. Iwendi, and C. Biamba. (2021). ''TBSMR: A trust-based secure multipath routing protocol for enhancing the QoS of the mobile ad hoc network,'' Secur. Commun. Netw, pp. 1–9, https://doi.org/10.1155/2021/5521713
17. P. K. Pattnaik, B. K. Panda, and M. Sain. (2021). ''Design of novel mobility and obstacle-aware algorithm for optimal MANET routing,'' IEEE Access, vol. 9, pp. 110648–110657, https://doi.org/10.1109/ACCESS.2021.3101850
18. U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf, and B. V. Subbayamma. (2021). ''An improved hybrid secure multipath routing protocol for MANET'' IEEE Access, vol. 9, pp. 163043–163053, https://doi.org/10.1109/ACCESS.2021.3133882
19. U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi. (2022). ''A secure optimization routing algorithm for mobile ad hoc networks,'' IEEE Access, vol. 10, pp. 14260–14269 http://dx.doi.org/10.1109/ACCESS.2022.3144679
20. S. Dalal, N. Dahiya, S. Bijeta, V. Jaglan, M. Malik, S. U. Rani, D.-N. Le, and Y.-C. Hu. (2022). ''Adaptive traffic routing practice for load balance and congestion control in ad-hoc network in cloud-MANET,'' Soft Comput. Fusion Found., Methodol. Appl., vol. 26, no. 11, pp. 5377–5388, http://dx.doi.org/10.21203/rs.3.rs-723513/v1
21. Duc N. M. Hoang, Jong Myung and Sang Yoon Park.(2022). "Fault-Tolerant Ad Hoc On-Demand Routing Protocol for Mobile Ad Hoc Networks" IEEE Access Vol 10, pp. 111337 – 111350, http://dx.doi.org/10.1109/ACCESS.2022.3216066
22. Xi Chen, Gang Sun, Ling Liu , Hongfang Yu and and Mohsen Guizani. (2022). "RANCE: A Randomly Centralized and On-Demand Clustering Protocol for Mobile Ad Hoc Networks", IEEE internet of things journal, Vol. 9, No. 23,pp. 23639- 23658, http://dx.doi.org/10.1109/JIOT.2022.3188679
23. Y. Zhang, T. T. Liu, H. G. Zhang, and Y. A. Liu. (2021). "LEACH-R: LEACH relay with cache strategy for mobile robot swarms," IEEE Wireless Commun. Lett., vol. 10, no. 2, pp. 406–410, http://dx.doi.org/10.1109/LWC.2020.3033039
24. M. A. Biradarand and S. Mallapur. (2022). "Reliable MANET Routing for Multimedia Communication," 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, pp. 1-8, https://doi.org/10.1109/ACCAI53970.2022.9752573
25. N. M. Shah, H. El-Ocla and P. D. Shah, "Routing Protocol in Mobile Ad Hoc Networks based on Energy Consumption," 2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia, Spain, 2023, pp. 287-291, https://doi.org/10.1109/ICCNS58795.2023.10193472

Author

Chitra D received her BE degree in electronics and communication engineering from University of Madras, Tamil Nadu in 1996, ME degree in communication systems from Anna University, Tamil Nadu in 2008 and PhD degree in information and communication engineering from Anna University in 2018. Her areas of interest are wireless networking, antenna design, artificial intelligence, and image processing.

E-mail: chitravalli2000@gmail.com

Divya K received her BTech degree in electronics and communication engineering from Kannur University, Kerala in 2003 and ME degree in communication systems from Anna University, Tamil Nadu in 2023.Her areas of interest are networking, embedded systems design, and internet of things.

Corresponding author E-mail: divyasreedeep@gmail.com

Vijay Nath received his BSc degree in physics from DDU University Gorakhpur, India in 1998 and PG Diploma in computer networking from MMM University of Technology Gorakhpur, India in 1999 and MSc degree in electronics from DDU University Gorakhpur, India in 2001, and PhD degree in electronics from Dr. Ram Manohar Lohiya Avadh University Ayodhya (UP) and in association with CEERI Pilani (Raj), India in 2008. His areas of interest are ultra-low-power temperature sensors for missile applications, microelectronics engineering, mixed-signal design, application-specific integrated circuit design, embedded system design, cardiac pacemaker, internet of things, artificial intelligence & machine learning, and computational intelligence.

Email: vijaynath@bitmesra.ac.in