Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 1332373, 9 pages
https://doi.org/10.1155/2022/1332373

Research Article

Implementation of Hidden Node Detection Scheme for Self-Organization of Data Packet

P. Ganesh,[1] **G. B. S. R. Naidu**,[2] **Korla Swaroopa**,[3] **R. Rahul**,[4] **Ahmad Almadhor**,[5] **C. Senthilkumar**,[6] **Durgaprasad Gangodkar**,[7] **A. Rajaram**,[8] **and Alazar Yeshitla**[9]

[1]*Department of MCA, BMS Institute of Technology and Management, Bengaluru, 560064 Karnataka, India*
[2]*Department of Electronics and Communication Engineering, GMR Institute of Technology (an Autonomous Institute), Rajam, Andhra Pradesh 532127, India*
[3]*Department of Computer Science & Engineering, Aditya Engineering College (an Autonomous Institution), Surampalem, East Godavari District, Andhra Pradesh 533437, India*
[4]*Department of Mathematics, BMS College of Engineering, Bengaluru, Karnataka 560019, India*
[5]*Department of Computer Engineering and Networks, Computer and Information Sciences, Jouf University, Sakaka, Aljouf, Saudi Arabia*
[6]*.Department of Electronics & Communication Engineering, Saveetha School of Engineering, Saveetha University, Chennai, 602105 Tamilnadu, India*
[7]*Department of Electronics & Communication Engineering, Graphic Era Deemed to Be University, Society Area, Clement Town, Dehradun, Uttarakhand 248002, India*
[8]*Department of Electronics and Communication Engineering, EGS Pillay Engineering College, Nagapattinam 611002, India*
[9]*Department of Biotechnology, College of Biological and Chemical Engineering, Addis Ababa Science and Technology University, Ethiopia*

Correspondence should be addressed to A. Rajaram; drrajaram@egspec.org and Alazar Yeshitla; alazar.yeshi@aastu.edu.et

Received 31 December 2021; Accepted 11 February 2022; Published 26 March 2022

Academic Editor: Deepak Kumar Jain

The mobile nodes are infrequent movement in nature; therefore, its packet transmission is also infrequent. Packet overload occurred for routing process, and data are lossed by receiver node, since hackers hide the normal routing node. Basically, the hidden node problem is created based on the malicious nodes that are planned to hide the vital relay node in the specific routing path. The packet transmission loss occurred for routing; so, it minimizes the packet delivery ratio and network lifetime. Then, proposed enhanced self-organization of data packet (EAOD) mechanism is planned to aggregate the data packet sequencially from network structure. The hacker node present in routing path is easy to separate from network with trusty nodes. In order to secure the regular characteristics of organizer node from being confirmed as misbehaving node, the hidden node detection technique is designed for abnormal routing node identification. This algorithm checks the neighboring nodes that are hacker node, which hide the trust node in the routing path. And that trust nodes are initially found based on strength value of every node and assign path immediately. It increases network lifetime and minimizes the packet loss rate.

1. Introduction

MANET, or mobile ad hoc network, is a network of nodes and wireless devices that does not require any infrastructure. Devices including portable computers and cell phones play an important role in today's society. The nodes of a mobile ad hoc network do not contain a federal management method. This is used for its routable network resource availability, where every node operates as a gateway to broadcast the overload packet to other specified target node in the network environment [1]. The vital issue of MANET is that survival of misbehaving node due to the network structure. Protection is particularly required in force services, where it does not accept any overload analysis else packet lossing.

There arise the require for ambiguity error require to conceal the uniqueness of nodes and paths; so, facilitate no outside spectator can be familiar with the sender or accepter and therefore, the data packet is forwarding [2]. A node is required to process a packet to a specific node that is outside of its coverage limit, which is based on the gateway node for transmitting the data packets. Dissimilar wired network, mobile network faces complex problems such as the velocity of nodes which alters the network topology regularly. Protection is major anxiety in these packet transmission particularly in armed and law enforcement region. In addition to protection, the defeat uniqueness of the sender node, target node, and path selection must be concealed [3]. In MANET, a technique which offer anonymity defense to sender node, target node, and paths and also obtain the cost effectual presentation is necessary.

Unidentified position depending with efficient communication technique offers the maximum ambiguity security for sender, target, and path. ALERT actively separates a network field into sector and randomly chooses nodes in sectors as processing nodes that creates an unpredictable unidentified path. Particularly, in every communication procedure, a data transmitter else broadcaster separate the network field in instruct to divide itself and the target node into two sectors [4]. It then arbitrarily chooses a node in the former sector as the subsequent intermediate node and employs the Greedy Perimeter Stateless Routing (GPSR) scheme, which covetously propagates a data packet to the node closest to the objective node in order to forward the datagram to the intermediate node. In the last step, the data is transmitted to k-nodes in the target node sector, as long as ambiguity to the target node [5]. Additionally, awareness has approach to conceal the data invent or through an amount of initiators to support the ambiguity security of the sender node. Mobile network is susceptible to the survival of misbehaving node. Because there is ambiguity, it does not see the uniqueness of misbehaving node in aware. While aware offers full ambiguity for the network, it is susceptible for black hole intruders. So, the focal point in this process is used to offers safety so that black hole intruder does not delay the network structure [6].

A recently establish and strict protection-based intruder is called as Misleading Routing Attack that can be investigated. Misleading Routing Attack is a difference to the sinkhole intruder. In the sinkhole intruder node, overload is concerned in the direction of the misbehaving node by advertise fake paths, and the data packets are also lost otherwise its adapted by the misbehaving node [7]. In this communication process, as an option of lossing else altering data packets, which are deceptive to various paths relatively than the best path, the misbehaving node might be a focus for the traffic in the direction of itself to admission control maximum load in the network environment [8]. Overload is attracted by misbehaving node consider to speeding up intruder process. In rushing intruder, the genuine requests do not reach former as distinguished to the intruder request packet. Subsequent to attract the overload, the misbehaving node will misinform the overload to noneffective path relatively than the best one [9]. Latency will be created as the data packets are ambiguous from its best route. This proposed intruders are plan to latency the network data packets as much as potential so as to let the sender node time out earlier than it accepts the reply pack reverse from the target node as well as aim to reduce the burden of the network by improving the amount of unanticipated transmission of data packets created in the network structure [10].

Remaining subsections of the paper are planned as scheduled below. Section II includes a selection of related works. Section III proposes an enhanced self-organization of data packets (EAOD) mechanism for sequentially aggregating data packets from network structures. The algorithm for detecting hidden nodes is intended to categorize the abnormal routing node. Section IV contains a performance report that analyzes the various metrics based on the experimental results. Section V declares the conclusion of paper with a discussion of future work.

2. Related Works

Wakode [11] protecting the blackhole assault is the issued. This process is utilized to tackle malicious nodes by utilizing ad hoc request separate vector (AODV) steering by helpful snare recognition approach (CBDA) with malicious node identification calculation. The CBDA alluded receptive and proactive steering system. Vindictive node identification calculation identifies the noxious nodes in the system. It executes a switch following way to deal with accomplish the coveted objective. Reproduction results have said, AODV, presence of malevolent nodes in AODV and anchoring noxious nodes in AODV by utilizing CBDA with malicious node location calculation as far as packet conveyance proportion, end-to-end delay, standardized directing overhead, and bundle dropped proportion (taken as execution frameworks.

In Chaudhary et al. [12], because portable networks are completely devoid of any prior framework or validation point, all of the current mobile nodes that need to communicate with one another immediately form the configuration and begin the demand for information bundles to transmit and receive. From the perspective of security, correspondence between portable nodes by means of remote connections makes these systems more helpless to interior or outside attack on the grounds that anyone can join and move the system whenever. When all is said in done, packet dropping assault through the injurious node is one of the conceivable assault in the portable specially appointed system. This work stressed to build up an interruption discovery framework utilizing fluffy logic to recognize the packet dropping assault from the portable specially appointed systems and furthermore evacuate the malevolent nodes keeping in mind the end goal to spare the assets of adaptable nodes.

In the event that the nodes in MANET consists of adequate memory space for holding imitations and also some of the nodes act as the simple form and also chosen to collaborate with each other [13]. Anyway, the dynamical system topology of MANET, foundation less property, and absence of testament expert make the security problems of

MANET need to give careful consideration. The basic directing conventions in current, for example, DSR AODV, nearly consider in execution. They do not have the related instrument about location and reaction. Going for the conceivable assaults by vindictive nodes, in view of the DSR convention, this paper introduced a component to recognize pernicious nodes propelling dark/dim gap assaults and helpful dark gap assaults, known as Cooperative Bait Detection Scheme. It coordinates the assertive and responsive guard models and participates arbitrarily with a dynamical adjoining node. By incorporating the neighboring node's address as the lure goal address, it traps vindictive nodes to reply RREP and separates the pernicious nodes by the presented turn around following project, allowing them to continue their attack.

Nanaware and Babar [14] presenting mobile network is an unstable system, and the nodes are in the portable state. The node can undoubtedly enter and exit from the system. The aggressor node can without much of a stretch go into the system and influence the execution of the system. The vindictive nodes are hard to identify as any node can go into the system effectively. The location of the malevolent node is essential to anchor and enhance the execution of the system. The different parameters are considered to separate between the pernicious and authentic nodes of the system. The paper gives answer for identification of noxious nodes from the system relying upon the trust of the node. In this paper, different parameters are considered to recognize the perniciousness. The parameters incorporate the vitality of node, the portability of the nodes, and two social parameters. The recognition depends on the trust an incentive for the specific node.

In Silva et al. [15], node situating is a basic issue for differing applications in mobile networks. In any case, other than acting mischievously nodes that could cause control exhaustion, MANETs are additionally powerless to digital assaults, which can make the system temperamental as well as inaccessible. Subsequently, considering the holes previously mentioned, the objective of this paper is to propose a model for recognizing malevolent/getting into mischief nodes by the utilization of two determining strategies gray model and polynomial regression, fluctuation investigation, and reenactment of phony node positions. The acquired outcomes permit finishing up our model has high rate of exactness for identifying harmful/acting mischievously nodes.

Shirbhateet al. [16] develop a system for identifying the malignant node in a MANET. In the suggested plan, a k -implies that bunching-based inconsistency identification approach is used, and the profile is constantly refreshed. The approach is divided into three basic stages: planning, testing, and refreshing. The K-implies that bunching calculation is used in the preparation stage to build up a typical profile. Check whether the node's current movement is normal or abnormal during the testing stage. If it is normal, then refresh the standard profile generally disengage the malevolent node and disregard that node from the system. Weighted coefficients and an overlooking condition are used to periodically refresh the ordinary profile.

Muthumalathi and Raseen [17] present to limit execution degradation. In the event that the nodes in MANET consists of adequate memory space for holding imitations and also some of the nodes act as the simple form and also chosen to collaborate with each other. Narrow minded node may not share its own memory space to store reproduction for the advantages of different nodes. To build up a narrow minded node recognition calculation that considers fractional self-centeredness and novel copy portion system to legitimately adapt to egotistical imitation designation, secure hill figure calculation is to give the security in imitation information. Narrow minded imitation allotment strategies altogether decrease correspondence cost, and simulation result demonstrates completely egotistical node identification time and completely childish node erasure time.

Yoon and Ko [18] propose a strategy for condition versatile noxious node discovery in light of troupe learning. We initially get ready frail vindictive node locators prepared in assorted situations and afterward develop a solid troupe noxious node identifier, which is custom fitted to a given test condition, by combining feeble indicators whose exhibitions are assessed to be high in the test condition. We explore the execution of our technique and affirm that our strategy altogether outflanks the best in class strategies as far as identification precision and false discovery rate.

Sangeetha and Kumar [19] presenting an packet transmission characteristics of portable nodes in ad hoc organize are very confounding to comprehend attributable to the decentralized design and dynamic topology. The current framework has introduced different security arrangements to comprehend the noxious movement of the enemy. Consequently, planning a model to fortify up the interruption discovery framework in view of the questionable and capricious pernicious conduct of the foe is computationally testing issue. This paper shows a strategy called as ZIDS-Zonal-based Intrusion Detection System that utilize capability of diversion hypothesis to remove the indeterminate methodologies of the malevolent node. ZIDS offers a broad security against various and discrete aggressor. Contrasted and the ongoing investigations, ZIDS exceeds expectations best concerning exactness in location rate and handling time for guaranteeing precise identification of vindictive nodes and occasions.

Talreja and Jethani [20] present a MANET that is a remote system in which nodes can act as sender/recipients or as intermediaries such as switches. Nodes in a MANET may become overly aggressive in order to save resources. This happens as a result of constrained assets accessible for every node. This has a huge impact on the overall system execution. The proposed framework consists of a MANET divided into zones and groups, with a static agent serving as the focal node and a zonal agent for each zone. It is a departure from mobile agent-based design that is made possible by presenting zonal agents. As a result, the framework can distinguish between selfish and malicious nodes with a reduced amount of data exchange between the nodes.

3. Overview of Proposed Scheme

The movable nodes are uncommon travel in nature; consequently, that node packet broadcasting is also irregular. So,

the packet overload occurs for communication procedure, and the data packets are get dropped by accepter node, because hacker nodes are hidden from network for the usual routing node. Essentially, the unknown node that causes the issue is formed which depends on the misbehaving nodes that are designed to conceal the essential intermediate node in the communication route. The packet flow drop is occurred for communication process; so, it reduces the packet success rate, and lifespan of the network.

Then, the proposed enhanced self-organization of data packet (EAOD) mechanism is consider to collecting the data packet seriously from network environment. The hacker node is available in the routing path that is simple to divide from network with reliable nodes. While as protecting a standard behavior of data collector node from being established as a malicious node. The hidden node detection algorithm is constructed to detect the abnormal communication node. This algorithm verifies that the neighboring nodes are a hacker node and hide the reliable node in the routing path. So, toreliable nodes are originally discovered depending on strength value of every routing node and allocate the path directly. This should increase the network lifetime, and reduces the packet drop rate.

Figure 1 represents the schematic representation of enhanced self-organization of data packet (EAOD) mechanism. Monitoring the packet flow of every node, it observes the every node characteristics. Find the neighboring node in the routing path with efficient way. Enhanced self-organization of data packet mechanism is used to organize data packet sequencially. Also, it separates the reliable and hacker nodes in the routing path. Hidden node detection algorithm is used to improve network lifetime and reduce packet loss rate.

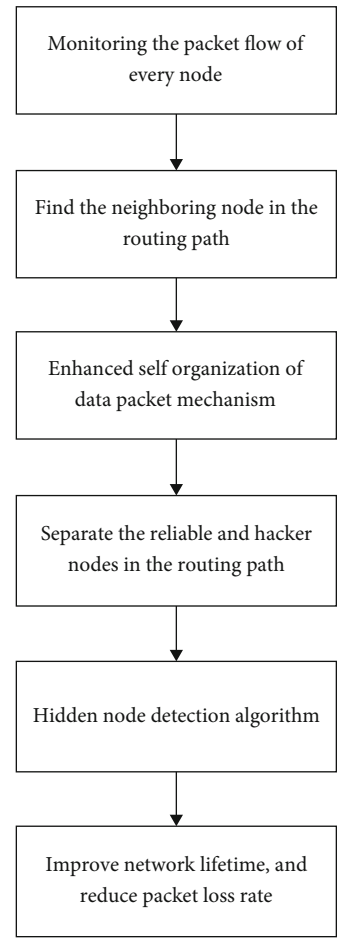

Figure 1: Block diagram of proposed enhanced self-organization of data packet (EAOD) mechanism.

3.1. Monitoring the Packet Flow of Every Node. In mobile ad hoc networks, there is no mid-point organization of the network nodes. Consequently, many misbehaving nodes can easily go into the network structure and interrupt its processing capability. On the otherwise, The ad hoc routing is a communication scheme which generate a path to the target node on demand. The sender node does not contain a straight link to the target node. The sender node launches a path request packet, which shares the data packet to its intermediate nodes. While a best route is establish, the packets are broadcasted from the sender node to target node among that route simply. As the path is created on demand, a misbehaving node can also go into the route and launches the intruders.

The packet latency for variance intruders is an attack in which the node latency for the packet before transmits it to the subsequent neighboring node. Normally, the uses such as the data transmission need a trustworthy link establishment. The transmission control scheme is used to offer this link based on the dependable link and needs a reply packet within a time instance for correct broadcasting of the data packets. This is broken by the packet latency for variance intruder node. It represents the delay of packet for before transmission. Consequently, the reply packet does not arrive at the sender node in time instance, and the source node considers that the packet has not arrived the target node, where $P(O)$ is the packet organization, $P(\text{flow})$ is the packet flow, and t is the time slot.

$$P(\text{O}) = P(\text{flow}) * t - . \tag{1}$$

As an outcome, the sender node forwards the data packet repeatedly, that can generate an overload on the network environment. This maximizes the jamming and packet latency in the network and reduces the transmission rate Also, in the condition of current packet transmissions, this reduces the latency in packet broadcasting as final results in minimum worth of data packet being forwarded and therefore minimizes the node performance. In this case, an improved on demand routing technique is proposed for calculation of packet delay and also removes the attackers in the communication path without the information. This ad hoc routing operates in the way that the every node forwards a normal broadcast data packet after assured time gap and verifies that the node through its intermediate nodes is packet latency for the packet by a time instance more than the entry rate. This threshold value is based on the network metrics such as node communication time instance and connectivity latency. Also, concern of packet latency considers to the maximum quantity of overload on the route, where

Step 1: Sender monitor the neighbor node characteritics.
Step 2: for each search the best path.
Step 3: if {node==hacker}.
Step 4: hide reliable node.
Step 5: else.
Step 6: if {node!==hacker}.
Step 7: Does not hide reliable node.
Step 8: Find next reliable routing path.
Step 9: Lesser packet loss rate.
Step 10: End if.
Step 11: end for.

Algorithm 1: Enhanced self-organization of data packet (EAOD) mechanism algorithm.

Step 1: Best path discovery in network.
Step 2: If {strengthen value ==high}.
Step 3: node is selected.
Step 4: share sequence of data packets.
Step 5: else.
Step 6: If {strengthen value ==low.
Step 7: node is rejected.
Step 8: discovery the hidden node.
Step 9: Increasing thenetwork lifetime.
Step 10: end if.

Algorithm 2: Algorithm for hidden node detection.

$S(P)$ is the size of packet, CN is the current node, ES(O) is the self-organization of packet, and $H(D)$ is the hidden node detection.

$$\begin{aligned} P(\text{flow}) &= \text{ES}(O) + H(D) - , \\ \text{ES(O)} &= S(P) * \text{CN} - , \\ \text{CN} &= \text{CN1} + \text{CN2} + .. + \text{CNn} - . \end{aligned} \tag{2}$$

In the standard conditions, while there is no hacker node available, the data packet transmission is on a route with minimum amount of nodes. Except, while a hacker node is found on the communication route, the node neighboring to the hacker node does not employ with the aim of route; moderately, it selects communication route, whether obtainable. It losses the acknowledgement packet from the hacker node, and thus the hacker node will never be in the broadcasting route. Consequently, in the mobile network, the node forces to select a longer hop count route as an alternative of selecting the routing path that is minimum distance path with hacker node. The performance indicates that the better transmission rate and the point to point packet latency minimizes as distinguished to while the route with hacker node is used. Therefore, the network presentation enhances.

3.2. Enhanced Self-Organization of Data Packet (EAOD) Mechanism. The self-organization procedure is the support of route finding process. Because an enhanced dynamic routing process is being used, sender node finds in its path which is used to share data packet towards the target node. Whether it has many path in its route reserve to arrive at the target node, the ordinary parameter which was used to choose the efficient path is amount of hop nodes. Except in this proposed scheme, the path discovery is used as the parameter to settle on the efficient path. By allowing for the steadiness of nodes connectivity, the protection of for packet flow chain is improved.

$$\begin{aligned} \text{CN} &= \sum_{i=0}^{n} \text{CN}, - \\ S(P) &= P(S) \longrightarrow P(T).- \end{aligned} \tag{3}$$

Furthermore, it minimizes the time used for packet organization without any loss, because it rejects the finding of new packet flows consider to connections termination. Whether the sender node must not contain an entry in its path can able to arrive at the target node, it initiates the path finding process. Request packet has an information and identifies the designer and destination of the route finding. This has a individual request identity, which is resolute by the expensive of the request and a verification record the identity of every relay node that is the specific reproduction of the request packet has been broadcasted. Originally, this path information is unfilled while the path finding is start. While a node accepts the request packet, whether it is the objective of the path finding, it proceeds reply packet to the path finding designer. This reply packet flows among the similar route in which it accepts the request packet.

$$\text{ES(O)} = P(S) \longrightarrow P(T) * \sum_{i=0}^{n} \text{CN}.- \tag{4}$$

During this reply packet every node that accepts, the reply packet contains the cost for the connection among itself and the node from which it accepts the path reply packet. A node should perform reevaluation of its relaying node, whether it discovers any rapid alteration of speed and way at that instant. Whether any relay node has a path to the target node in its path preservation, reply packet is started by the intermediary node and processes additionally. Consider node the sender node must not contain a path to target node in its path information. This starts the request packet and shares this packet to its nearest neighbor nodes. Target node accepts the request packet among the node intermediate nodes. Sender node chooses the path depends on the packet size, path which contains the maximum LET is resolute as the better path. Let sender node select the path; also, it is used to perform protection-based packet sharing for mutual confirmation and key sharing process.

$$\text{ES}(O) = \sum_{i=0}^{n} \text{CN} * P(S) \longrightarrow P(T) - . \tag{5}$$

Enhanced self-organization of data packet mechanism is performed as follows. In this step, hacker node forwards a reply packet, when it sends request packet to it. This aim is

Table 1: Datagram format for proposed EAOD. Packet format: packet format contains the important information of all mobile node present in the network. The details are node's location and characteristics.

Source ID	Destination ID	Monitoring the packet flow of every node	Find the neighboring node in the routing path with efficient way	Enhanced self-organization of data packet mechanism	Hidden node detection algorithm

445443.

Table 2: Simulation setup.

Node count	100
Size of the area	1170×950
Mac	802.11 g
Radio range	250 m
Duration for simulation	24 ms
Traffic source	CBR
Packet size	150 bytes
Mobility model	Random way point
Protocol	AODV

expert by making the lecture to of bait request packet, which is the lecture to the nearest node chosen arbitrarily within single sender nodes. Process is started when request packet is used for early communication process and waiting for the reply packet. After that, phase started bait analysis that is performed in condition to separate the reliable and hacker node. This hacker nodes are able to hide the routing node from network environment. Whether it must not begin blackhole intruders, then there would be remaining nodes transmit the acknowledgement packet. This shows that a misbehaving node is available in the routing acknowledgement, so that it sends to backward tracing procedure. Whether reply packet forwarded from only, that means there are no other malicious nodes happen in that network environment and send to dynamic routing. Whether it was attacker node, then remaining nodes forward an reply packet. These indicates that in path acknowledgement, there was a misbehaving node to be present.

3.3. Hidden Node Detection Algorithm. In this hidden node detection algorithm, this evaluates the every node that strengthens value for routing process. It chooses the most dependable path for routing in order to better distribute packets between the sender and receiver nodes. This is used to locate hidden reliable nodes quickly. The hidden node information are collected by neighbor node in the specific routing path. This supports to enhance the packet success rate frequently. It increases the nodes active time and minimizes the nodes packet loss because of hidden node not join for communication process.

$$P(\text{flow}) = \sum_{i=0}^{n} \text{CN} * P(S) \longrightarrow P(T) + H(D) -,$$
$$P(O) = \sum_{i=0}^{n} \text{CN} * P(S) \longrightarrow P(T) + H(D) * t - . \quad (6)$$

When an adjacent node obtains a request packet from the sender node, it searches in its routing problem by X and transmits the request packet to the next neighboring node. The similar procedure is followed awaiting the request packet closer to the target node. This sequence of reply packet follows the similar procedure in the reverse direction. The confirmation of the routing process is proceed by verifying the active time of node, and this node is called reliable node and hidden node; also, it is detected. Subsequent to checking the procedure, the sender and the target nodes are genuine with the support of the sequence of routing between nodes.

The hidden node detection algorithm is constructed to achieve unreliable path routing and detect and avoid the hacker nodes based on strengthen value. It enhances network lifetime and reduces packet loss rate.

Table 1 depicts the suggested EAOD datagram format. The sender and the receiver node ID fields each take up four bytes in this case. Path searching for robustness node, which takes five bytes, is the third. Monitoring the packet flow of every node, it observes the every node characteristics. Fourth field takes four bytes. Find the neighboring node in the routing path with efficient way. Fifth carries four bytes, and enhanced self-organization of data packet mechanism is used to organize data packet sequencially. Also, it separates the reliable and hacker nodes in the routing path to organize data packet efficiently. Final field takes three bytes, and this hidden node detection algorithm is used to improve network lifetime, and reduce packet loss rate.

4. Performance Evaluation

4.1. Simulation Model and Parameters. The suggested EAOD is tested using the Network Simulator tool (NS 2.34). In our computation, 100 node were distributed in a 1170×950 meter square region for a simulation time of 24 milliseconds. All mobile nodes were distributed at unexpected times throughout the network. The communication range of all nodes is 250 meters. constant bit rate (CBR) ensures that packets are transmitted at a constant speed in the network, thereby limiting packet traffic rate. Ad hoc on demand distance vector routing (AODV) is used to provide the best routing path that is proposed. The enhanced self-organization of data packet (EAOD) mechanism is being developed to aggregate data packets sequentially from network structure. The parameter setup for simulation is shown in Table 2.

Figure 2 shows that the proposed enhanced self-organization of data packet (EAOD) mechanism is planned to aggregate the data packet sequencially from network structure is compared with existing GAA [21] and RAT

Source ID	Destination ID	Monitoring the packet flow of every node	Find the neighboring node in the routing path with efficient way	Enhanced self organization of data packet mechanism	Hidden node detection algorithm
4	4	5	4	4	3

Figure 2: EAOD result for the proposed algorithm.

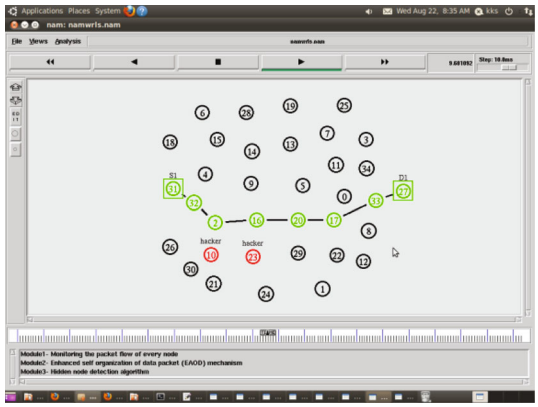

Figure 3: Graph comparing mobility and delay.

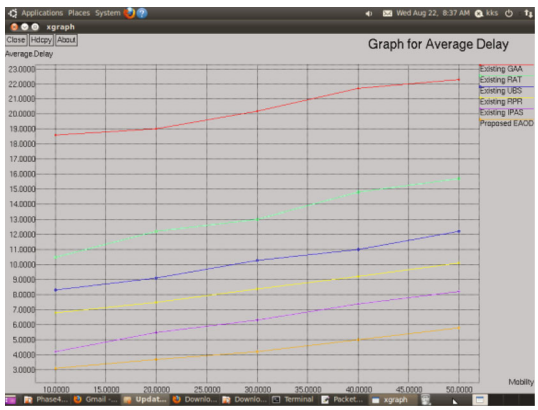

Figure 4: Graph comparing mobility and network overhead.

[22]. In this hidden node detection algorithm, this evaluates the every node strengthen value for routing process. It chooses the most efficient route for routing packets between sender and receiver node. It extends network lifetime and reduces packet loss. It increases network lifetime and reduces the packet loss rate.

4.2. Performance Analysis. The *X* graph in ns2.34 is used in simulation to evaluate the performance of a model.

4.2.1. Average Delay. Figure 3 depicts the waiting time, that is estimated by the amount of time spent communicating from the initial node to the final node; it monitors each node's characteristics by employing enhanced self-organization of data packets (EAOD). When compared to existing methods GAA, RPR, RAT, UBS, and IPAS, the proposed EAOD mechanism has the shortest delay.

$$\text{AverageDelay} = \text{EndTime} - \text{StartTime}. \tag{7}$$

4.2.2. Network Overhead. Figure 4 depicts how network load is reduced when a source node communicates datagrams to a destination point via a relay node in the routing path and how a hidden node detection algorithm evaluates each node's strength value for the routing process. It selects the reliable routing path. When compared to the current methods GAA, RPR, RAT, UBS, and IPAS, the suggested EAOD method diminishes network overhead.

$$\text{Networkoverhead} = (\text{NumberofPacketLosses/Received}) * 100. \tag{8}$$

4.2.3. Ratio of Packet Delivery. Figure 5 depicts that the packet arrival ratio is calculated by dividing the number of packets acquired by the number of packets transmitted at a given rate. In a sensor network, node speed is constant, and the modeling rate is set to 100. When compared to conventional methods GAA, RPR, RAT, UBS, and IPAS, the proposed EAOD method enhances delivery ratio.

$$\text{PacketDeliveryRatio} = \left(\frac{\text{Numberofpacketreceived}}{\text{Sent}}\right) * \text{speed}. \tag{9}$$

4.2.4. Network Lifetime. Figure 6 shows that the network's life span is predicted by the overall network process, and the amount of time the network is active to perform communication frequently. When compared to standard methods GAA, RPR, RAT, UBS, and IPAS, the stated EAOD method increases life of the network.

$$\text{NetworkLifetime} = \frac{\text{lengthofenergyusage}}{\text{overallenergy}}. \tag{10}$$

4.2.5. Energy Consumption. Figure 7 depicts an estimate of total energy consumed from the initial node to the final node. When compared with conventional methods

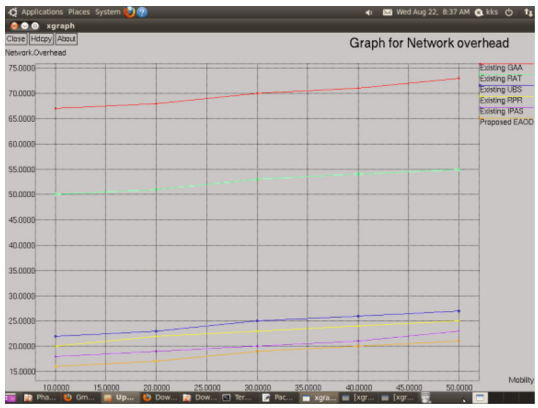

Figure 5: Analysis of node delivery rate.

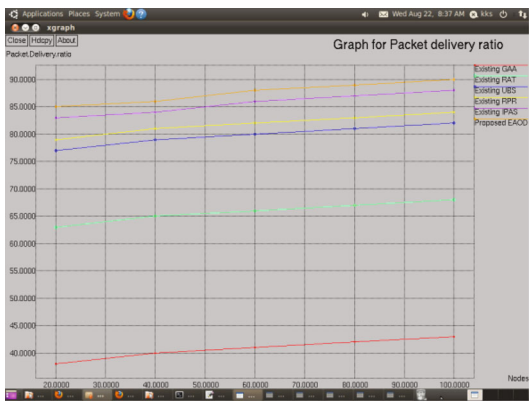

Figure 6: Graph for no. of nodes vs. network lifetime.

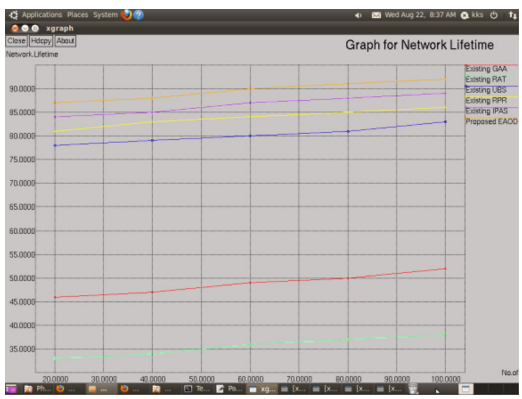

Figure 7: Analysis of a node's energy utilization.

GAA, RPR, RAT, UBS, and IPAS, the recommended EAOD method is used to obtain a reliable routing path for packet transmission; so, energy usage is diminished.

$$\text{EnergyConsumption} = \text{InitialEnergy} - \text{FinalEnergy}. \quad (11)$$

4.2.6. Packet Loss Rate. Figure 8 demonstrates that the data loss of all network transmission is scheduled the by node loss, and because of misbehaving node is detected, and avoided by using hidden node, detection

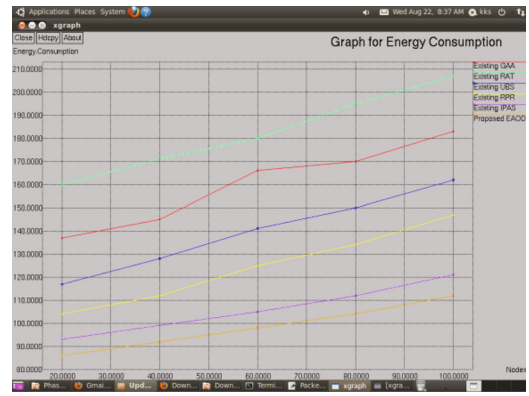

Figure 8: Analysis of the pause node's packet loss rate.

algorithm is used to select higher strengthen node for routing. When compared with previous methods GAA, RPR, RAT, UBS, and IPAS, the recommended EAOD approach minimizes packet delay.

$$\text{Packetlossrate} = \left(\text{Numberofpacket}\frac{\text{lossed}}{\text{Sent}}\right) * 100. \quad (12)$$

5. Conclusion

Nodes in a MANET are movable nodes that can be moved from one location to another. Packet jamming occurred for communication path, and packet information do not accepted by receiver node, since hackers are hidden the general relay node. Essentially, the hidden node issues are created depending on misbehaving nodes that are designed to conceal the vital communication node in the particular communication route. The packet flow loss is occurred in the route; therefore, it reduces the packet success ratio and the network lifespan. Then, presenting an enhanced self-organization of data packet (EAOD) mechanism is designed to organizing the data packet continuously from network environment. The hacker node available in the routing path is uncomplicated to split from network with reliable nodes, while as protecting a normal uniqueness of data collector node from initially established as a malicious node. The hidden node detection algorithm is constructed to detect the irregular packet transmission node. This algorithm verifies that the nearest nodes are hacker node, that hide the faith node in the communication route. Trust nodes are at first discovered based on strength value of each node and assign the route instantly. It improves the lifespan of network and reduces the packet drop rate. In future work focal point, the optimization of route with unbalanced link calculates various metrics.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest

There is no conflict of interest.

References

[1] R. R. Roy, *Handbook of Mobile Ad Hoc Networks for Mobility Models*, Springer, 2014.

[2] S. Khan and J. L. Mauri, *Security for Multihop Wireless Networks*, CRC Press, 2014.

[3] E. Fazeldehkordi, I. S. Amiri, and O. A. Akanbi, *Comparative Study of Multiple Black Hole Attacks Solution Methods in MANET Using AODV Routing Protocol*, Create Space Independent Publishing Platform, 2014.

[4] M. G. Pineda, J. Lloret, and S. Papavassiliou, *Ad-hoc Networks and Wireless*, Springer- nternational Workshops in Spain, 2014.

[5] Y. Guo, J. Ma, C. Wang, and K. Yang, *Incentive-Based Optimal Nodes Selection Mechanism for Threshold Key Management in MANETs with Selfish Nodes*, Hindawi Publishing Corporation, 2013.

[6] F. Wang, F. Wang, B. Huang, and L. T. Yang, "COSR: a reputation based secure route protocol in MANET," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, Article ID 258935, 10 pages, 2010.

[7] Z. Han and Y. L. Sun, *Distributed Cooperative Transmission with Unreliable and Untrustworthy Relay Channels*, Hindawi Publishing Corporation, 2009.

[8] Z. Li, D. Pu, W. Wang, and A. Wyglinski, "Forced collision: detecting wormhole attacks with physical layer network coding," *IEEE-Tsinghua Science And Technology*, vol. 6, no. 5, pp. 505–519, 2011.

[9] F. Maria, I. Melattia, and E. Tronci, "A multi-hop advertising discovery and delivering protocol for multi administrative domain MANET," *Mobile Information Systems*, vol. 9, 280 pages, 2013.

[10] R. Stoleru, H. Wu, and H. Chenji, "Secure neighbor discovery and wormhole localization in mobile ad hoc networks," *Ad Hoc Networks*, vol. 10, pp. 1179–1190, 2012.

[11] N. G. Wakode, "Defending blackhole attack by using acknowledge based approach in MANETs," in *2017 International Conference on IoT and Application (ICIOT)*, pp. 1–6, Nagapattinam, India, 2017.

[12] A. Chaudhary, A. Kumar, and V. N. Tiwari, "A Reliable solution against packet dropping attack due to malicious nodes using fuzzyl in MANETs," in *Optimization, Reliabilty, and Information Technology (ICROIT)*, pp. 178–181, Faridabad, India, 2014.

[13] A. C. S. Devasthali and S. Kadam, "Cooperative Bait Detection Scheme in MANETs," in *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, pp. 679–683, Chennai, India, 2017.

[14] P. M. Nanaware and S. D. Babar, "Trust system based intrusion detection in mobile ad-hoc network (MANET)," in *Next Generation Intelligent Systems (ICNGIS)*, pp. 1–4, Kottayam, India, 2016.

[15] A. A. Silva, E. Pontes, F. Zhou, and S. T. Kofuji, "Grey model and polynomial regression for identifying malicious nodes in MANETs," in *In Global Communications Conference (GLOBECOM)*, pp. 162–168, Austin, TX, USA, 2014.

[16] S. V. Shirbhate, S. S. Sherekar, and V. M. Thakare, "A novel framework of dynamic learning nased intrusion detection approach in MANET," in *Computing Communication Control and Automation (ICCUBEA)*, pp. 209–213, Pune, India, 2015.

[17] N. Muthumalathi and M. M. Raseen, "Fully selfish node detection, deletion and secure replica allocation over MANET," in *Current Trends in Engineering and Technology (ICCTET)*, pp. 413–415, Coimbatore, India, 2013.

[18] S. J. Yoon and Y. B. Ko, "JRGP: jamming resilient geocasting protocol for mobile tactical ad hoc networks," in *Information and Communication Technology Convergence (Ictc)*, pp. 437–442, Jeju, Korea (South), 2010, November.

[19] V. Sangeetha and S. S. Kumar, "ZIDS: zonal-based intrusion detection system for studying the malicious node behaviour in MANET," in *Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, pp. 276–281, Mandya, India, 2015, December.

[20] R. Talreja and V. Jethani, "A vote based system to detect misbehaving nodes in MANETs," in *Advance Computing Conference (IACC)*, pp. 391–394, Gurgaon, India, 2014.

[21] J. He and O. Yang, "Globally-aware allocation of limited bandwidth in multipath routing based on queueing performance," in *Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, San Francisco, CA, USA, 2017, March.

[22] J. Liu, Y. Xu, R. Ando, H. Takakura, and Y. Xu, "Resource allocation for throughput optimization in buffer-limited mobile ad hoc networks," in *2017 International Conference on Networking and Network Applications (NaNA)*, pp. 80–86, Kathmandu, Nepal, 2017.