International Journal of Wireless Communications and Mobile Computing
2025, Vol. 12, No. 1, pp. 23-34
https://doi.org/10.11648/j.wcmc.20251201.13

Research Article

Enhancing the Performance of AODV Routing Protocol for Selfish Node Detection in MANET

Abebaw Mebrat[1], Ermias Melku Tadesse[2, *], Tarekegn Walle Yirdaw[3], Abubuker Girma[1]

[1]Software Engineering Department, Kombolcha Institute of Technology, Wollo University, Kombolcha, Ethiopia
[2]Information Technology Department, Kombolcha Institute of Technology, Wollo University, Kombolcha, Ethiopia
[3]Department of Information System, Kombolcha Institute of Technology, Wollo University, Kombolcha, Ethiopia

Abstract

Recently, a better approach to access computing services is necessary because of the growing popularity of portable computers and consumer needs. Self-configuring wireless networks without a defined infrastructure are known as mobile ad hoc networks, or MANETs. MANETs are susceptible to a range of assaults because of their dynamic network architecture, lack of central monitoring, and inadequate security measures. Detecting a node's misbehavior in a MANET and successfully validating the selfish node using an algorithm for detecting selfish nodes are the main goals of this study. The discovery results in decreased retransmission and improved performance across all network parameters. In this study, the routing algorithm used was AODV. The suggested approach is implemented using the NS2 simulation tool. Our suggested technique enhances the packet delivery ratio, throughput, and reduces packet drop and delay—all of which are network metrics that are compared and analyzed—both with and without selfish nodes. The suggested AODV protocol improved the simulation study based on the routing performance in terms of throughput, packet lost, packet delivery ratio, and end-to-end delay. However, the simulation result analysis revealed that the end-to-end delay reduced from 1.902 to 1.08, the throughput improved from 674.52 to 724.521, the packet delivery ratio improved from 85.60 to 87.6638, and the packet lost improved from 34.40 to 32.38. We came to the conclusion that the suggested Selfish node detection algorithm showed improvement in all performance parameters examined.

Keywords

MANET, AODV, Selfish Node, Selfish Node Detection Algorithm, RREQ

1. Introduction

Mobile ad hoc networks are becoming more and more popular as a result of the rapid development of wireless technology and ubiquitous computing. Nonetheless, the MANET efficiency is significantly impacted by the behavior of the selfish node's component nodes. which must cooperate in order to guarantee the availability of the network's core operations. The performance issues with the MANET network were very challenging to resolve due to the network's complexity, which included dynamic topology changes, heterogeneous network architecture, a lack of central admin-

[*]Corresponding author: ermiasmelku3400@gmail.com (Ermias Melku Tadesse)

Received: 10 March 2025; **Accepted:** 27 March 2025; **Published:** 19 April 2025

istration, limited resources, and the network's mobility and wireless channel interference [1]. We suggested a strategy that optimizes and identifies selfish nodes that agree with the route discovery of packets from sender to recipient nodes, after which they delete the packets in order to address the selfish node issue that impacts MANET behavior. Such a self-centered node directly affects the network's trustworthy discovery in MANET [2]. Self-configuring wireless networks that operate without a fixed infrastructure are known as mobile ad hoc networks. Due to their continually shifting network topology, lack of central supervision, and inadequate security measures, MANETs are particularly vulnerable to a variety of threats. In MANETs, selfish nodes are broken nodes that drop packets that shouldn't be dropped. A preventive measure is also suggested, and a malevolent selfish node is added to the network [3]. Selfishness can be harmful within the MANET. When the neighbor's node is counted and assessed, the selfish node reacts favorably, just like any other mobile node. Since it has been given the duty of an intermediate forward, it accepts the communication but does not advance it; in order to achieve final delivery, the selfish node discards all incoming packet types. When a node is selfish, both the packet drops rate and communication delay rise [4]. Nodes that act in this manner are selfish or lack cooperation. The efficiency of MANETs is significantly impacted by non-cooperative nodes. Network splitting may result from nodes in MANETs acting in an uncooperative manner [6]. In the current research, we suggest a method for identifying a selfish node in a network architecture that is more effective. As a result, creating new routing protocols is still a difficult research topic for developers and is seen as a significant unresolved problem in MA-NET. In general, certain research (such as the watchdog approach, agent-based methods, token-based methods, and Confidant [7] employ various strategies and tactics. There is still a gap in the current routing protocol area of designing AODV routing protocol forwarding data within the node; it does not take real-time node cooperation into consideration to achieve high packet delivery ratio and low delay from one user to another in MANET. Recent studies have designed and investigated selfish node detection for data forwarding in MANET.

In order to obtain high network performance by minimising communication between selfish and non-cooperative nodes, the primary goal of this work is to develop a Selfish node detection algorithm for efficient data broadcasting over MA-NET. This enhances the AODV routing scheme, which maximises network connectivity for selfish nodes. Routing protocols increase throughput and message packet delivery ratio while reducing latency. Because of the complexity of the implementation, the main drawback of the suggested method is that it only applies to MANET. However, a number of problems, including residual energy, network lifetime, and security, are related to MANET performance. Since this thesis focusses on selfishness within the node to communicate in the network, it may not address this difficulty due to time constraints because it does not include additional threats. In order to solve the scalability and routing issues of MANET, the research aims to apply various routing concepts or approaches to determine packet delivery from source to destination inside a proposed AODV routing approach.

2. Related Work

Wireless nodes that can be continually set up without requiring an existing network and that may be used anywhere, at any time, make up a mobile ad hoc network. The networks are those. It is a self-contained system that allows mobile hosts that are wirelessly connected to roam freely and often serve as routers simultaneously. An ad hoc network's traffic kinds differ greatly from a wireless network infrastructure’s [8]. In order to identify a route with a high packet delivery ratio and guarantee that packets reach their intended destination, the MANET routing protocol is essential [5].

The on-demand routing method that makes it quite simple to alter a connection's state is the ad hoc on-demand distance vector protocol. Building a route is necessary to reduce network usage. The source node and the destination node exchange various AODV-defined message types. The three categories of responses are Route Requests (RREQs), Route Replies (RREPs), and Route Re-quest Errors (RERRs) [9]. According to the full study, AODV is generally an unsafe routing architecture that lacks any means of detecting and preventing transmission from the selfish node behavior. RREQ provides the IP address of the source node, the IP address of the destination, and the Broadcast ID. All nodes automatically create a reverse path from the source to the destination. As RREP propagates back to the source, nodes establish a forward pointer to the destination [10]. Selfish nodes only send their data packets to facilities and use the network for their own purposes; they do not assist in relaying the data packets of other nearby nodes in order to save energy. The other malicious nodes are the second category of nodes that seem to damage and alter the network infrastructure [11].

3. Research Methodology

The design research methodology was employed. The packets that need to be sent to the right place are the main subject of this study. The primary focus of the research, when seen in detail, is on the packets (RREQ and RREP) that are sent from the source to the proper destination and back to the source; in other words, minimizing the number of inaccurate RREP packets sent from the selfish node to the source node. Throughput, packet delivery ratio, and total packet loss/drop are the research's parameters. Usually, percentages and numbers are used to convey these factors. Our algorithm's primary goal is to create a method for identifying selfish nodes. We created the AODV attributes in the NS2 simulation program using the design science research methodology [12].

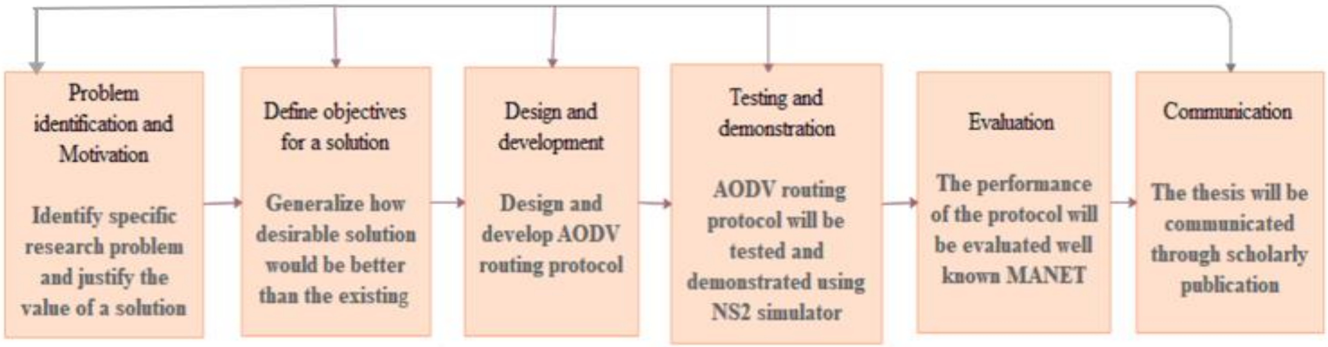
Problem identification and Motivation
Identify specific research problem and justify the value of a solution
Define objectives for a solution
Generalize how desirable solution would be better than the existing
Design and development
Design and develop AODV routing protocol
Testing and demonstration
AODV routing protocol will be tested and demonstrated using NS2 simulator
Evaluation
The performance of the protocol will be evaluated well known MANET
Communication
The thesis will be communicated through scholarly publication

Figure 1. Process Model for Design Science Research Methodology (DSRM) [12].

The suggested method implements the AODV routing protocol performance with and without selfish nodes. It is known as the "selfish node detection algorithm." The Selfish Node Detection Algorithm (SFNDA) is used to modify the AODV routing protocol in order to implement the suggested solution. The researchers concentrated on the RREP destination that transmits from any intermediate or destination node to the source node in this suggested method. Selfish nodes reduce network efficiency, and packets are discarded in transit. It is easy for a selfish node to be selfish in AODV since almost all selfish nodes desire to conserve their resources by disregarding any messages assigned to them. In order to find the path, requests are made to every neighbor during route discovery in AODV. The selfish nodes were identified in our investigation prior to performance degradation. This was accomplished when a selfish node was spotted, disrupting the entire network by losing the control message packet. The source node then chose to deliver the control message to a new node and follow a different path. Following the replay of the RREP, the target node is disabled. In this instance, the message has already been transmitted by the source node, but it has not yet reached its destination. After sending the reply, we will set up a system to allow destination nodes to get the actual message for a longer period of time.

The suggested architecture uses the AODV protocol to reduce selfish nodes in MANETs. The source node makes a route request to the destination node, which replies with a fake route if there is a selfish node in the network. The source node sends data packets to the selfish node, assuming it is the source of the RREP. When the selfish node gets a data packet from the source node, the data packet is dropped. In order to prevent becoming route members for other nodes, selfish nodes in MANET will either not forward or discard RREQ packets when they receive them. They can refrain from sending any messages to other people as a result. This behavior will necessitate the creation of the transmission path on additional nodes. When a node sends out an RREQ message, it determines if its neighbors have forwarded it or not. This node is known as the RREQ checking node. The RREQ checked node is the monitored node. After broadcasting an RREQ message, the RREQ checking node keeps track of its neighbors and logs which neighbors have rebroadcast the same message. The RREQ checking node will examine the routing table after a predetermined period of time to determine whether nodes are not sending the RREQ message. These nodes are characterized as selfish nodes since they do not forward the RREQ message. An RREQ checked node must rebroadcast the message to its neighbors, including the sender of the RREQ message, after receiving SFNDA's examination of the message. The AODV protocol is altered in order to implement this technique. To lessen selfish nodes, the researchers employed the Selfish Node Detection Algorithm approach.

The suggested architecture, which explains the Selfish Node Detection Algorithm's general architecture, is depicted in Figure 2. First, create ready node routing. Once the network's routing configuration is complete, deploy the node next to choose the source and destination addresses. Next, find the source and destination to create the route next to it. If the node is selfish, by-pass routing will occur, which will result in data transmission errors by detecting SFNDA. However, the packet will be sent to the destination node if the node is not a selfish node transmitting control message. On the basis of this, the selfish node is found by the selfish node detection algorithm. Following the detection of selfish nodes, the typical process of determining the path from the source to the destination will take place, where a route is established to ensure a successful packet transmission from the source to the destination.

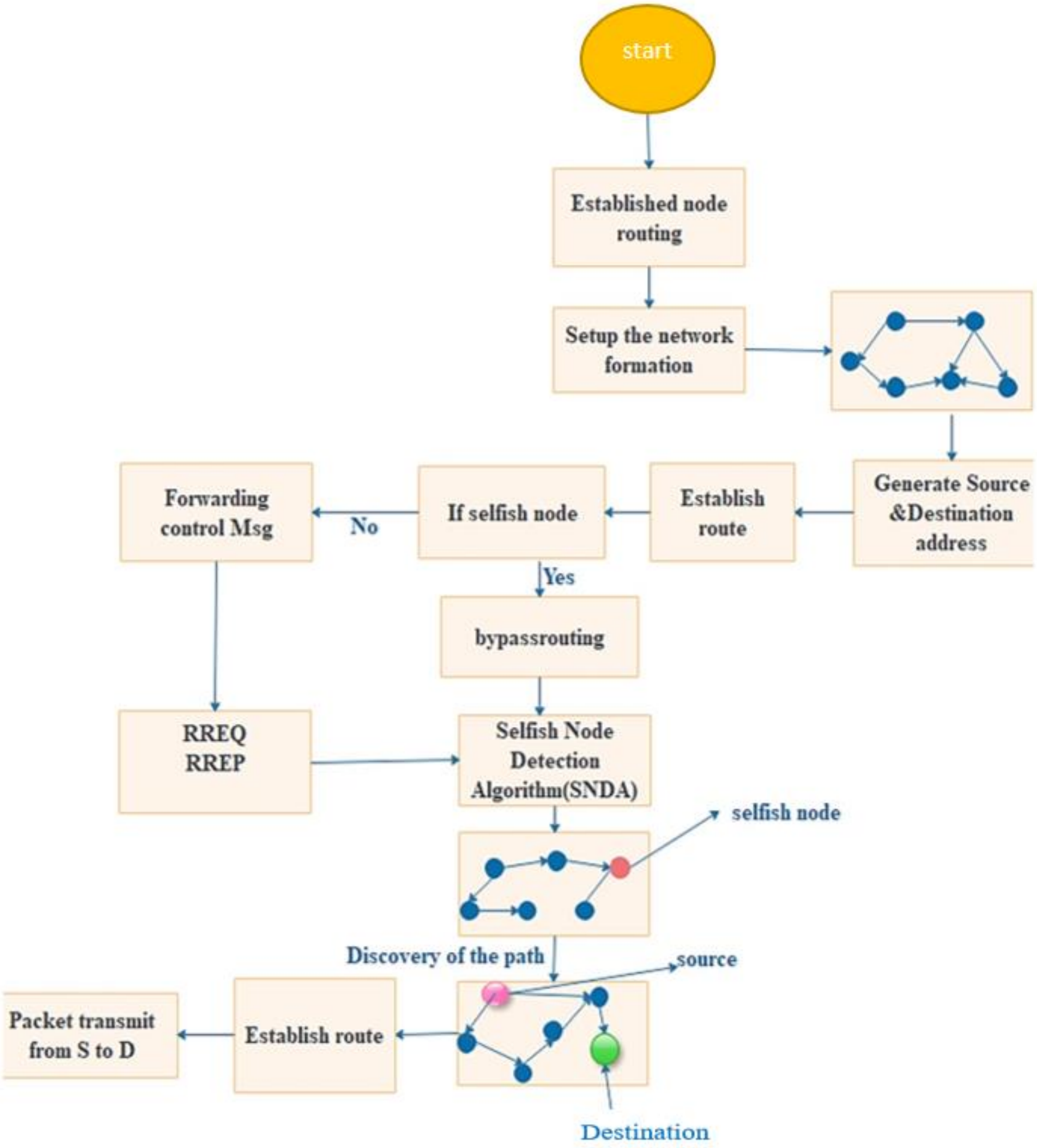

Figure 2. The Overall Proposed Architecture.

A false RREP is created and transmitted to the source node when it broadcasts RREQ to neighboring nodes, including selfish nodes. The suggested approach contrasts RREP data with current routing table data by altering the AODV protocol. Afterward, remove the selfish node's RREP from the route data and obtain a fresh route RREP from a normal node. By utilizing the Selfish Node Detection Algorithm technique in conjunction with the AODV routing protocol, the suggested solution design aims to reduce the impact of the selfish node in MANET. In particular, the Selfish Node Detection Algorithm method, which uses the suggested solution to minimize the selfish node. The Selfish Node Detection Algorithm approach is used because it can identify and counteract new and unidentified assaults. The current AODV routing protocol is modified to implement the suggested solution architecture in MANET. The suggested method identified and reduced the effects of the selfish node attacker after simulating an existent selfish node in a simulation network environment. This enhanced network performance. Figure 3 provided a detailed explanation of how to discard erroneous RREPs sent by anomalous nodes and forward data packets via a different path to the destination node.

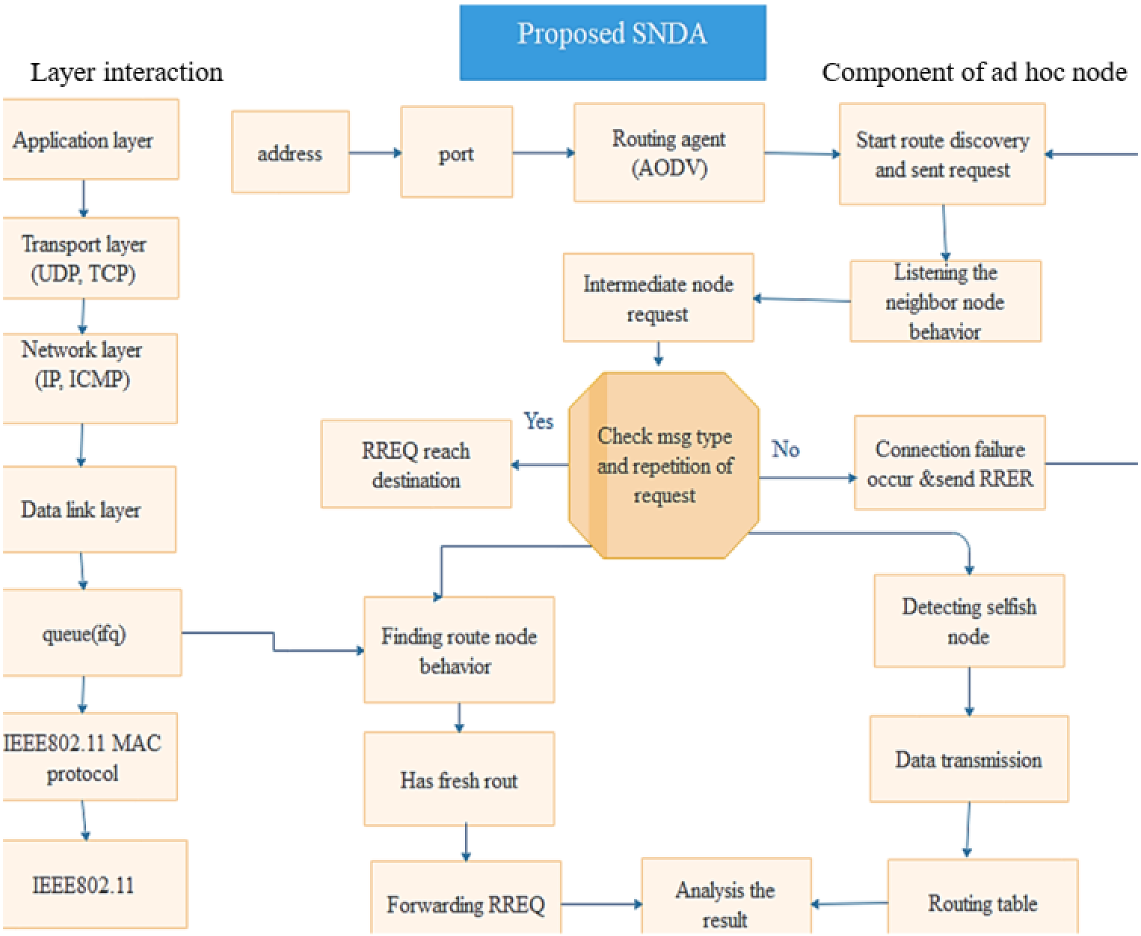

***Figure 3**. Proposed SFNDA Algorithm Flow Chart.*

Algorithm: proposed description of the SFNDA flow

Step 1: initiate the source node

Step 2: Send RREQ messages to all neighboring nodes for data packet transmission.

Step 3: start to discover a real route within the collected neighbor information and send a request

Step 4: After discovering the route that broadcast the route request in the intermediate node

Step 5: Before reaching RREQ in the destination node check the repetition of a route request, If the route request repetition has occurred it sends RRER

Step 6: after route request repetition is occurred again to start to discover the route

Step 7: If RREP is sent to the Next Node right away, re-broadcast the request to the neighbor node until it reaches the destination node. Send RREP to the source node if next node == DN; else, broadcast RREQ.

Step 8: After listening to the neighbor node behavior, it will be finding route node behavior if the route is fresh forward RREQ and Analysis the result

Step 9: if the message type and repetition of request is RRER it detects the selfish node and after detecting the selfish node the normal Data transmission will be achieved

Step 10: Choose the target node that sends the RREP to the source node, if the RREQs arrive at the destination node.

Step 11: The suggested SFNDA Approach determines whether an RREP packet originates from a normal or selfish node by comparing it with the routing table in the AODV routing protocol.

Step 12: The attacker instantly sends a false RREP to the sender node if it is present in the chosen path. On the one hand, RREP will be rejected if it fails to reach the source node, which is an anomalous node; on the other hand, RRER will be sent if the connection fails.

Step 13: Choose the shortest routing path to deliver actual data to the recipient node if the routing information matches.

Step 14: When the suggested method is used, the route table data is modified, and RREP is blocked. It then determines a new path to forward data packets and a new, fresh route for efficient communication.

Step 15: End.

4. Results and Discussion

Simulation Setup and Performance Metrics: Two different kinds of simulation scenarios are used to measure the performance metrics, including: We must employ two simulation scenarios based on the simulation environment in order to assess the suggested approach in the AODV routing protocol. In the first scenario, we compare the results of both recommended protocols with the efficacy of the currently used routing protocols, testing the effectiveness of the suggested approach with varying numbers of normal nodes and with a fixed number of normal nodes without selfish nodes [13]. We compare our results to two existing protocols: the original AODV routing protocol and the suggested selfish node discovery algorithm in the AODV routing protocol in MANET. In the second case, the security performance of the suggested architecture is assessed using a fixed number of normal nodes and a variable number of selfish nodes.

Table 1. *Simulation Parameters Set up.*

parameter	Values
Simulation tool	NS-2.35
Simulation area	1000 m * 1000 m
Routing protocol	AODV
Number of nodes	10,20
Traffic type	CBR
Packet size	1000 byte
Type of attack	Selfish node
platform	Ubuntu 16.04
Type of connection	UDP
Mobility	RWP
Simulation time	100 s

Simulation Parameter: In this simulation, a network topology dimension of 1000 m x 1000 m was used, and 20 nodes were randomly disrupted within this area. According to the random placement concept, the nodes will be moving across the network space [14]. We employed UDP connectivity in this network simulation, and tests were conducted on CBR ≤ 1000 bytes. Because the source node in a TCP connection will terminate the connection if no TCP ACK packets are received, the simulation did not employ a TCP connection. The selfish node is chosen for this simulation since it has the ability to drop a lot of data packets. We chose the place at random because we didn't take the mobility model into account. Because it can accept any trace file format without requiring any AWK file settings, the trace graph was chosen. For efficient network communication, we have set up 20 nodes and 100 ms in this network environment. This simulation uses one hundred seconds of time. Random waypoint mobility is employed as the mobility model, and there are 20 nodes participating in the tests, with the number of selfish nodes varying from 1 to 6 [14, 15]. Routing protocols such as proposed AODV, EX-AODV, and AODV under selfish node are employed. Table 1 provides a summary of the total experimental parameters. In general, we have selected the simulation configuration that was determined based on the AODV routing protocol specifications and obtained from a recent publication.

The following simulation results are simulated using the Nam window utilizing Table 2 as the simulation setup. NS-2.35 includes a new AODV agent .h and .cc file for AODV simulations. To assess the effectiveness of the routing protocols (lost packet, packet delivery ratio, end-to-end delay, and throughput), the simulation's trace file and files were parsed. The measures used to assess the routing algorithms under consideration are explained in this section. The definition of a performance statistic known as routing metrics determines routing in communication networks. Analysis and Discussion of Simulation Results: Figure 4 displays the performance of the packet delivery ratio in our simulation. shows the number of dropping packets directly increases as the number of nodes in the network increases. The reason for this is that as the number of nodes or network size increases, so do the number of route breaks. This indicates that the likelihood of a route break grows as the number of intermediary nodes between the source and destination nodes increases. The likelihood of a packet dropping in the case of our devised algorithm is lower than that of EX-AODV. The packets discarded by selfish nodes are the reason for the rise in packet dropping in AODV under selfish nodes. The algorithm's feasibility and scalability are demonstrated by the relative rise in PDR in our created proposed AODV. The PDR performance for the protocols EX-AODV (88.5%), AODV under selfish node (50%) and proposed-AODV (92.5%) on the number of nodes is observed when the network has a normal node. Due to the packets dropped by selfish nodes, the number of packets dropped in AODV under selfish nodes is rising. Nonetheless, the packet delivery ratio has been attained in proposed-AODV, which outperforms an EX-AODV routing protocol as the number of nodes grows.

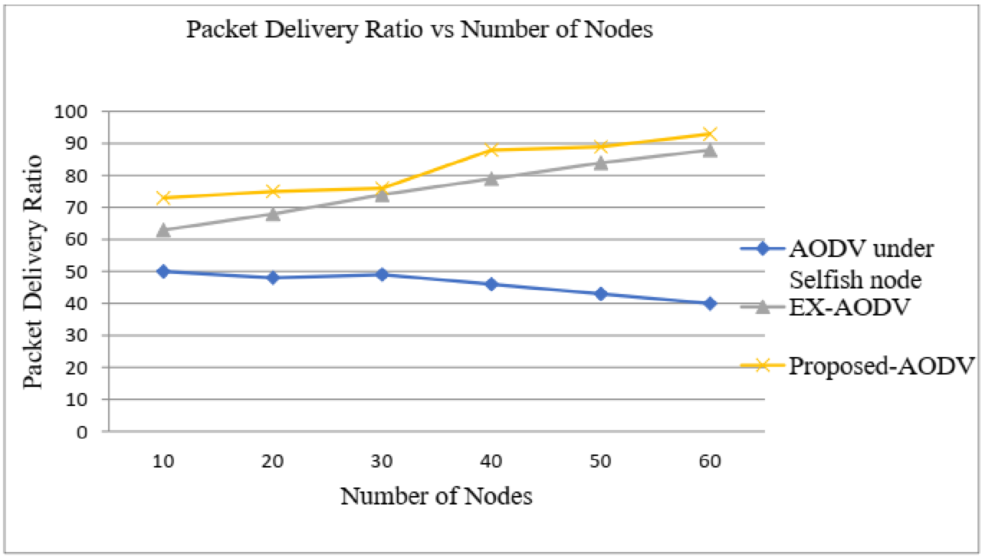

Figure 4. Packet Delivery Ratio vs Number of Nodes.

The evaluation's best performance metric is the packet delivery ratio. According to this simulation, the suggested detection approach outperforms EX-AODV and AODV under selfish node in MANET in terms of PDR. This is in contrast to the performance of the proposed AODV, EX-AODV, and AODV under selfish node. The packet delivery ratio will decrease as the number of selfish nodes rises, yet in the suggested AODV, the PDR has increased. The suggested AODV outperforms the current AODV and AODV under selfish node ratio values when compared to the existing AODV and AODV under selfish nodes. Therefore, as shown in Figure 5, the suggested AODV performs better PDR when there are a lot of selfish nodes on the network and on both protocols.

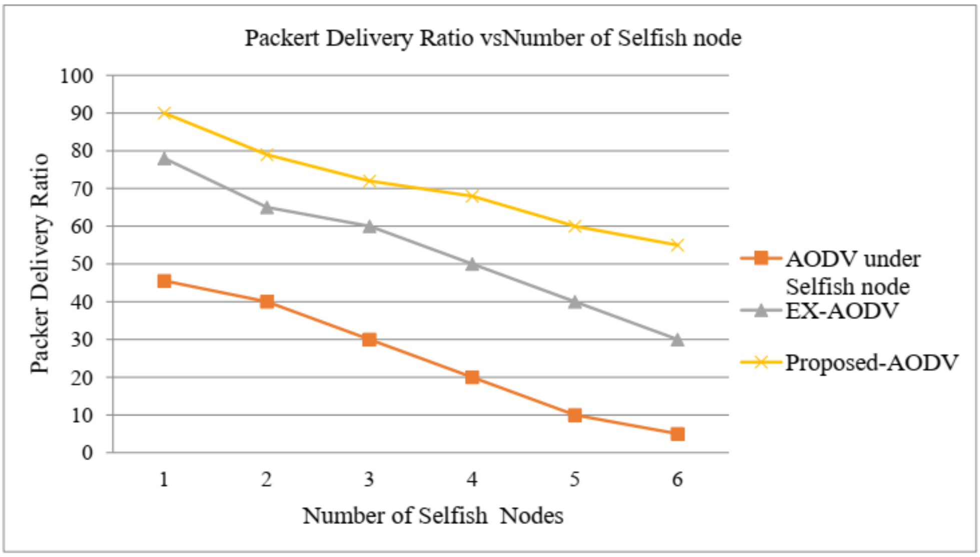

Figure 5. Packet Delivery Ratio vs Number of Selfish nodes.

The performance of EXAODV, proposed AODV, and AODV under the selfish node indicate the evaluation metrics of an end-to-end delay. Figure 6 displays the time it took for the packet to travel from its source to its destination. Selfishness and packet drops rise until the target node receives the packet since the packet sent from the source travels through the intermediate node to reach its destination. This led to an increase in the received packet's end-to-end delay. Here, the delay for a certain packet sent from a destination is specified in milliseconds. However, instead of being compared to under selfish node, the figure's end-to-end delay is in both the suggested AODV selfish node detection and EX-AODV. However, the average delay for the suggested AODV protocols is marginally the same as that of EX-AODV. Therefore, under the selfish node, the suggested AODV outperforms EX-AODV and AODV in terms of average delay. Therefore, on average end-to-end delay measurement, the suggested AODV performs better.

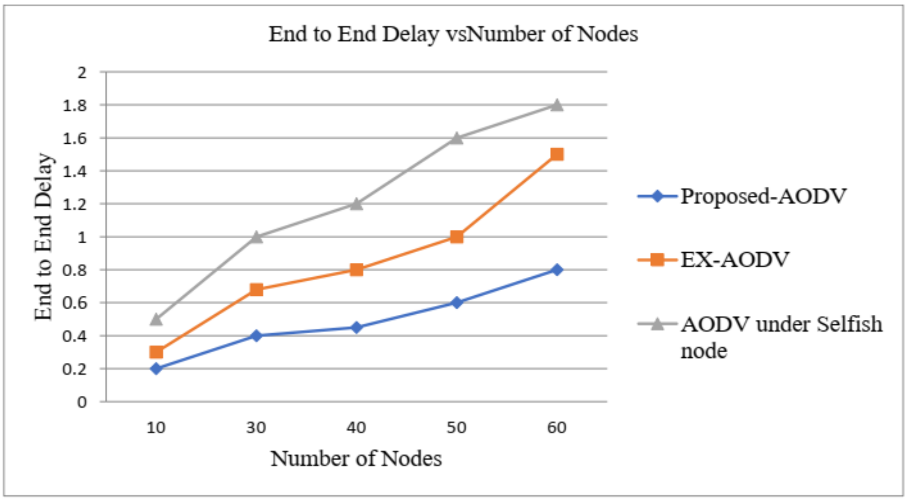

Figure 6. *End to End Delay vs Number of Nodes.*

In the current AODV, the simulation time for the sent and received events. The reason for the high received packet latency in Figure 7 is that as the number of intermediate nodes increases until the packet reaches its destination, there is a greater possibility that the intermediate node will be selfish, which leads to interference and delay at the intermediate node. In both the current AODV and the AODV under selfish node, the packet delay is greater than the packet transmission delay. It covers every potential reason for a delay, including packet drop, queuing and retransmission delays, and route finding. Figure 7's end-to-end delay performance results and average delay performance in a network with selfish nodes demonstrate that the EX-AODV protocol performs well when selfish nodes are present. Additionally, the selfish node discovery mechanism in the suggested AODV protocols results in a reduced average delay. The normal node is chosen to send packets after identifying the selfish node. The time also increases as the number of selfish nodes rises. Consequently, the suggested AODV has been enhanced to varied degrees and operates well when selfish nodes are present.

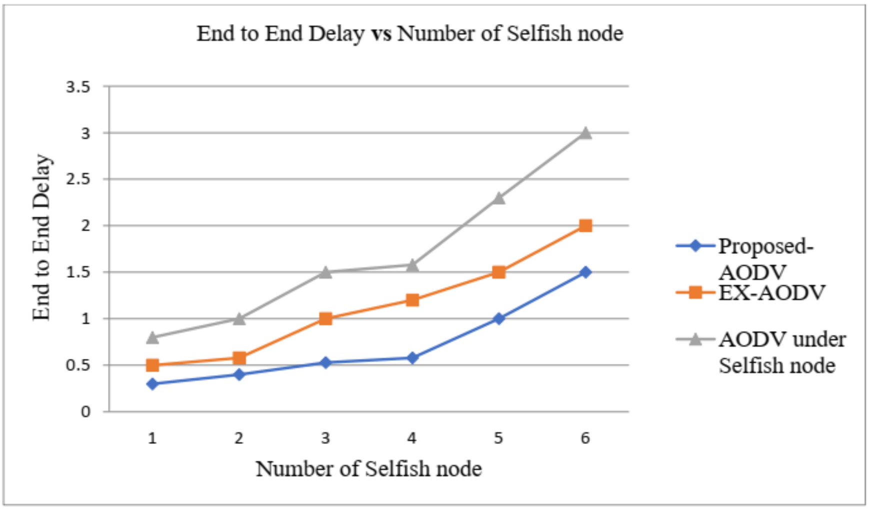

Figure 7. *End to End Delay vs Number of Selfish nodes.*

The total number of packets transmitted to a destination decreased as the simulation's average throughput time increased. Because there was no way to catch selfish nodes during route discovery, the packet dropped here for a variety of reasons. This was determined by counting how many packets were dispatched and how many reached the destination. Each source and destination node's result were extracted from the trace analyzer's network data. This outcome was obtained by incorporating the selfish node detection technique into the suggested AODV. The same number of nodes and the same parameter were used to get the same result. Under selfish node protocols, EXAODV and AODV do not significantly differ in the number of nodes in the network; nevertheless, as Figure 8 illustrates, the proposed AODV obtained differs significantly from both protocols. Nonetheless, during typical operations, the average throughput of the suggested AODV protocol outperforms both EX-AODV and AODV under selfish nodes. Good results under the selfish node are enhanced when the suggested AODV selfish node detection is evaluated. Thus, the suggested increased MANET's throughput. The findings indicate that as the number of nodes rises, so does the throughput.

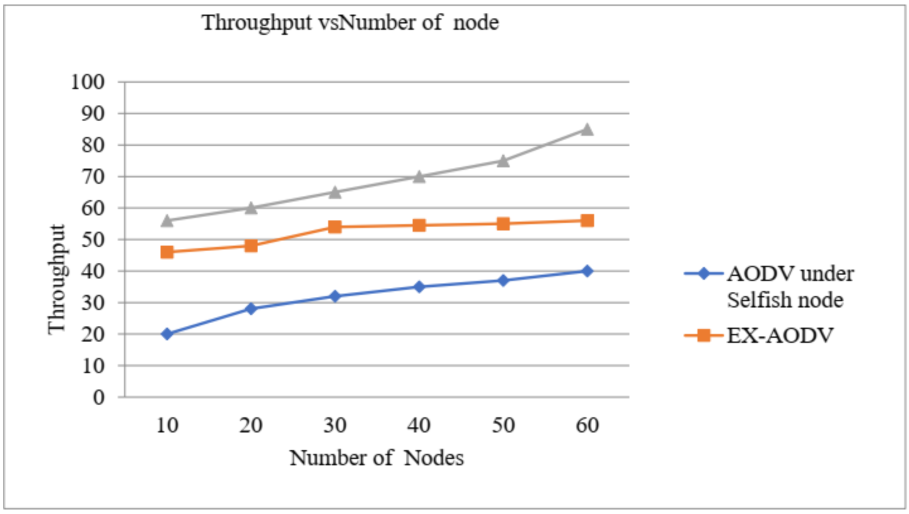

Figure 8. Throughput vs Number of nodes.

The throughput of the proposed AODV with selfish node detection algorithm, the AODV under selfish node, and the existing AODV is compared. Selfish nodes were identified by observing node behavior during route discovery, and routing was carried out using only typically behaved nodes. The number of messages delivered per second was used to analyze the data. The accompanying Figure 9 illustrates how the proposed node evaluates performance throughput on both protocols, determining the total number of received packets at the destination out of all transmitted packets. When selfish nodes are present in the network, the throughput of both EXAODV and AODV has decreased. As a result, the throughput performance of the proposed AODV protocols has improved more than that of both protocols. Thus, we deduce that the suggested approach alleviates the effect of selfish nodes more effectively than EX-AODV and AODV under selfish nodes.

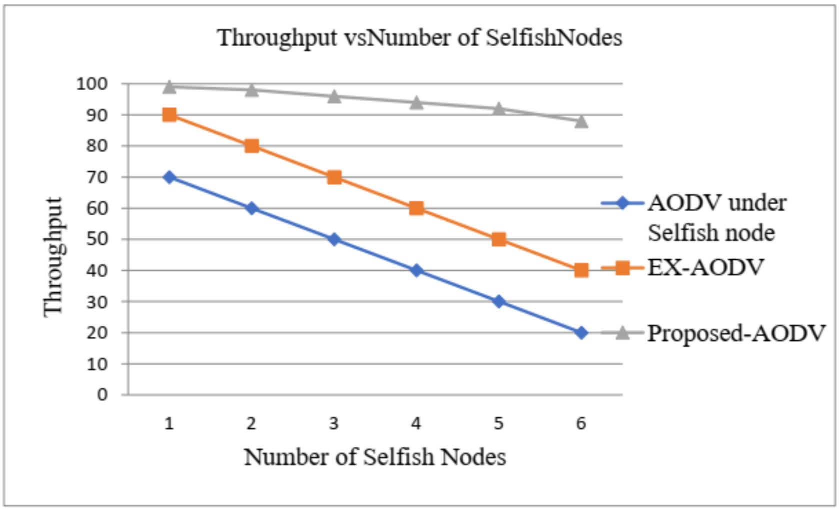

Figure 9. Throughput vs Number of Selfish Nodes.

Under the selfish node, we model the performance of AODV, suggested AODV, and EX-AODV. By choosing the normal node to transfer the data, the suggested approach enhances the performance of both the existing AODV and AODV under selfish node. The suggested selfish node discovery approach improves the performance of AODV by decreasing packet drop, increasing packet throughput, and decreasing delay because the results of all performance measures vary. The suggested AODV had the best packet delivery ratio. Thus, according to Figure 10, While AODV under selfish node has a high number of dropped packets, EX-AODV and the suggested AODV have a low number of dropped packets, which directly correlates with an increase in the number of nodes in the network. When comparing the suggested detection approach to AODV under selfish node and EX-AODV, the accompanying graph demonstrates that the packet loss is significantly identified.

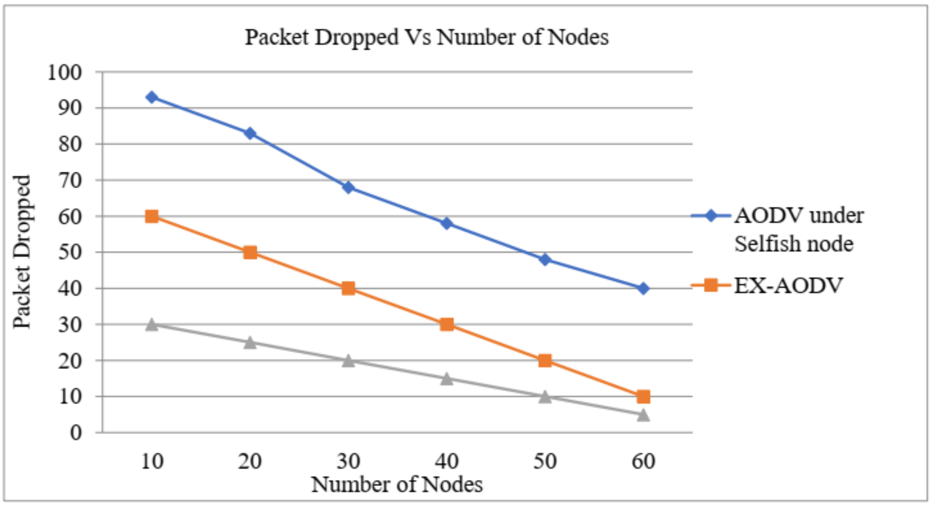

Figure 10. Packet Dropped Vs Number of Nodes.

Table 2. Summary of the comparison.

Parameters	Existing AODV	Proposed AODV	Evaluation result
Number of Nodes	10,20	10,20	The same
Number of the sent packet	4109	4109	The same
Number of a received packet	4079	4079	The same
Number of the forwarded packet	11150	11150	The same
Total dropped packet	34.40	32.38	Improved
Packet delivery ratio	85.60	87.6638	Improved
End-to-end delay	1.902	1.008	Improved
Throughput	674.52	724.521	Improved

Based on the outcome, we concluded that choosing a normal path during routing discovery required identifying the selfish node. The optimal throughput, reduced delay, and increased packet delivery (minimized packet drop) are the outcomes of this. To solve the issues brought on by retransmission, packet collisions, packet loss, and other factors that result in performance degradation, the suggested SFNDA uses the AODV protocol.

5. Conclusion and Future Work

The performance issue with the AODV routing protocol was expressed in this thesis using selfishness behavior. Through a survey of numerous literary works, the solution to the node's selfish behavior was found. The majority of MANET's suggested protocols make the assumption that all mobile users engage equally and are not self-centered. Selfish nodes want to spread the word about their successes. They may voluntarily relay messages from friends or nodes inside their communities, but not from strangers, or they may decline to relay messages from other nodes. When it comes to packet transmission, a selfish node will typically refuse to cooperate, which can seriously impair network performance. Since the purpose of this study was to determine the optimal AODV protocol through route discovery using a selfish Node Detection algorithm. Consequently, in simulation, the new AODV performs better than the existing AODV. This study employs four performance metrics—packet delivery ratio, packet drop, end-to-end delay, and throughput—to assess the proposed approach. In this study, the performance of the new AODV and the current AODV using the SFNDA routing protocol was assessed using the NS-2.35. MANET relies largely on node cooperation to perform networking operations. It is hence very susceptible to selfish nodes.

Future Work

We suggested focusing on the following areas going forward:

To test and assess our suggested approach in the AODV protocols, the suggested selfish node identification algorithm is used to the broadcast and packet dropped in the date transmission for the purpose of detecting selfish nodes in the simulation environment.

We recommended modelling and examining many performance indicators in NS2 in the future, including connection failure, queue, congestion issue, and energy use.

Future research will also include creating strategies for returning the node to the network using the NS2/NS3 environment in the event that selfish behavior returns to normal and the suggested approach is validated in a real-world setting.

Abbreviations

AODV	Ad Hoc On-Demand Distance Vector
CBR	Constant Bit Rate
DSRM	Design Science Research Methodology
MANET	Mobile ad hoc networks
NS2	Network Simulator-2
PDR	Packet Delivery Ratio
RERRs	Route Request Errors
RREPs	Route Replies
RREQs	Route Requests
SFNDA	Selfish Node Detection Algorithm
TCP ACK	TCP Acknowledgment
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Author Contributions

Abebaw Mebrat: Resources, Software, Supervision, Writing – review & editing

Ermias Melku Tadesse: Conceptualization, Investigation, Methodology, Project administration, Writing – original draft

Tarekegn Walle Yirdaw: Data curation, Funding acquisition, Visualization

Abubuker Girma: Formal Analysis, Validation

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] H. Ehsan and F. A. Khan, “Malicious AODV: Implementation and analysis of routing attacks in MANETs,” Proc. 11th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. - 11th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC-2012, pp. 1181–1187, 2012, https://doi.org/10.1109/TrustCom.2012.199

[2] A. Perti and P. Sharma, “Reliable AODV protocol for wireless ad hoc networking,” 2009 IEEE Int. Adv. Comput. Conf. IACC 2009, vol. 00, no. March, pp. 675–680, 2009, https://doi.org/10.1109/IADCC.2009.4809093

[3] M. Bharathi, R. Sairam, S. Sundar, and C. M. Vidhyapathy, “Securing AODV protocol from selfish node attack,” ARPN J. Eng. Appl. Sci., vol. 10, no. 12, pp. 5286–5290, 2015.

[4] S. Joshi, R. Arindom, T. Dikshit, B. Anish, A. G. Deep, and P. Pallav, “Conceptual paper on factors affecting the attitude of senior citizens towards purchase of smartphones,” Indian J. Sci. Technol., vol. 8, no. 12, pp. 83–89, 2015, https://doi.org/10.17485/ijst/2015/v8i

[5] P. B. H. Karthik, H. R. Nagesh, and N. N. Chiplunkar, “Mitigation and performance evaluation Mechanism for Selfish Node Attack in MANETs,” 2017 Int. Conf. Comput. Commun. Control Autom. ICCUBEA 2017, pp. 1–6, 2018, https://doi.org/10.1109/ICCUBEA.2017.8463847

[6] Z. Ullah, M. S. Khan, I. Ahmed, N. Javaid, and M. I. Khan, “Fuzzy-based trust model for detection of selfish nodes in MANETs,” Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA, vol. 2016-May, pp. 965–972, 2016, https://doi.org/10.1109/AINA.2016.142

[7] A. Patil, J. Khan, A. Khandave, A. Yadgire, and P. M. Dangore, “Selfish Nodes Detection Techniques in MANET-A,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 3, no. Xi, pp. 286–290, 2015.

[8] Agrawal, “Manet : Comparion on AODV and DSR,” no. February, pp. 77–82, 2016.

[9] K. S. Ali and U. V Kulkarni, “Comparing and analyzing reactive routing protocols (aodv, dsr and tora) in qos of manet,” Proc. - 7th IEEE Int. Adv. Comput. Conf. IACC 2017, pp. 345–348, 2017, https://doi.org/10.1109/IACC.2017.0081

[10] M. Saeed Alkatheiri, J. Liu, and A. R. Sangi, “AODV routing protocol under several routing attacks in MANETs,” Int. Conf. Commun. Technol. Proceedings, ICCT, pp. 614–618, 2011, https://doi.org/10.1109/ICCT.2011.6157949

[11] S. Nobahary, H. G. Garakani, A. Khademzadeh, and A. M. Rahmani, "Selfish node detection based on hierarchical game theory in IoT," Eurasip J. Wirel. Commun. Netw., vol. 2019, no. 1, 2019, https://doi.org/10.1186/s13638-019-1564-4

[12] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," J. Manag. Inf. Syst., vol. 24, no. 3, pp. 45–77, 2007, https://doi.org/10.2753/MIS0742-1222240302

[13] K. Agrawal, "Simulation Based Performance Comparison of Adhoc Routing Protocols Simulation Based Performance Comparison of Adhoc Routing Protocols Kushagra Agrawal *, Shaveta Jain **," no. March, 2014.

[14] A. A. Hayder Majid, "Impact of Mobility Models on Routing Protocols for Various Traffic Classes in Mobile Ad Hoc Networks," no. May, 2016.

[15] K. Gupta, H. Sadawarti, and A. K. Verma, "Performance Analysis of MANET Routing Protocols in Different Mobility Models," Int. J. Inf. Technol. Comput. Sci., vol. 5, no. 6, pp. 73–82, 2013, https://doi.org/10.5815/ijitcs.2013.06.10