Article

Not peer-reviewed version

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

Ermias Tadesse * , Abebaw Mebrate , Tarekegn Walle , Abubeker Girma

Posted Date: 12 March 2025

doi: 10.20944/preprints202503.0836.v1

Keywords: MANET; AODV; Selfish node; Selfish node detection algorithm; RREQ

Article

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

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

[1] Software engineering Department, Kombolcha Institute of Technology, Wollo University, Ethiopia.

[2] Information Technology Department, Kombolcha Institute of Technology, Wollo University, Ethiopia.

[3] Department of Information System, Kombolcha Institute of Technology, Wollo University, Ethiopia.

* Correspondence: ermiasmelku3400@gmail.com

Abstract: Nowadays, due to the popularity of portable computers and the increasing demands of users to access computing services better is required. Mobile ad hoc networks (MANET) are self-configuring wireless networks with no established infrastructure. Due to constantly changing network architecture, a lack of central monitoring, and insufficient security mechanisms, MANETs are vulnerable to a variety of attacks. The primary objectives of this study are to detect a node's misbehavior in a MANET and also effectively validate the selfish node by using an algorithm for detecting selfish nodes. Retransmission is reduced and all network metrics performance is increased resulting from the discovery. AODV was utilized as the routing algorithm in this study. The proposed algorithm is implemented using the NS2 simulation tool. In the presence of selfish nodes and without selfish nodes, our proposed algorithm improves the packet delivery ratio, and throughput, and minimizes delay and packet drop, which are all network metrics that are compared and examined. The simulation analysis evaluated based on the routing performance was enhanced in the proposed AODV protocol in terms of packet dropped, packet delivery ratio, end-to-end delay, and throughput. However, the study of the simulation result showed an improvement in packet delivery ratio from 85.60 to 87.6638, an improvement of packet dropped from 34.40 to 32.38, the throughput improved from 674.52 to 724.521 and end-to-end delay improved from 1.902 to1.08. We concluded that all performance parameters investigated by the proposed Selfish node detection algorithm demonstrate improvement.

Keywords: MANET; AODV; Selfish node; Selfish node detection algorithm; and RREQ

1. Introduction

The quick advancement of wireless technology and ubiquitous computing has generated a surge of interest in mobile ad hoc networks. However, the actions of the selfish node's constituent nodes have a major impact on the MANET efficiency. Which must work cooperatively to ensure that the network's essential functions are available. Because of the complications of the MANET design, such as dynamic topology changes, heterogeneous network architecture, less infrastructure, lack of central administration, limited resources, and the nature of mobility and wireless channel interference of the network, the MANET network's performance problems were extremely difficult to solve [1]. So that the selfish node issue affects MANET's behavior, we proposed a solution that optimizes and detects selfish nodes that agree with the route discovery of packets from sender to receiver nodes and then drop these packets. Such a selfish node has a direct impact on the reliable discovery of the network in MANET [2]. Mobile ad hoc networks are self-configuring wireless networks that function without a fixed infrastructure. MANETs are very susceptible to various threats because of their constantly changing topology of the network, absence of central monitoring and ineffective security mechanisms. Selfish nodes are malfunctioning nodes in MANETs that drop packets are not expected for them. A malicious selfish node is placed into the network, and a preventative method is also proposed [3]. Within the MANET, selfishness can be destructive. The selfish node, like any other mobile node, responds positively when the neighbor's node is enumerated and evaluated. It accepts the communication but does not forward it because it is assigned the role of an intermediate forward as a result; the selfish node discards all types of incoming packets to provide final delivery. The packet drop rate and communication delay both increase when a node is selfish [4]. Selfish or no cooperative nodes are those that behave in this way. Non-cooperative nodes have a significant impact on the efficiency of MANETs. Non-cooperative conduct of nodes in MANETs can lead to the partitioning of the network [6]. In this research, we propose a mechanism for detecting a selfish node in a more efficient network architecture. Therefore, still, the design of new routing protocols is still a challenging research area for developers and is considered a major open issue in MANET. Generally, there are some studies(token-based method, agent-based methods, and watchdog Method, Confidant [7] that use different methods and techniques Selfish node detection for data forwarding in MANET is designed and investigated in recent studies, but there is still a gap in the existing routing protocol area of designing AODV routing protocol forwarding data within the node, it does not consider real-time node cooperation to achieve high packet delivery ratio and low delay from one user to the other in MANET.

The main objective of this research is to design a Selfish node detection algorithm for effective data broadcasting over MANET to achieve high network performance by reducing communication between selfish and non-cooperative nodes. This helps to improve the AODV routing protocol that optimizes selfish nodes in network connectivity. Routing protocol minimizes delay and maximizes message packet delivery ratio and throughput. The major limitation of the proposed approach is only applicable to MANET, due to the complex nature of the implementation. On the other hand, many issues are concerned with the performance of MANET such as remaining energy, network lifetime, and security. This thesis does not incorporate other attacks so it may not address this challenge due to the time constraint but that focuses on selfishness within the node to communicate in the network. The research aims to apply different routing principles or techniques to discover packet delivery from source to destination within a proposed AODV routing approach to address the scalability and routing challenges of MANET.

2. Related Work

A mobile ad hoc network is composed of wireless nodes that may be established continuously without the need for a pre-existing network and can be utilized anywhere at any time. Those are the networks. It's a self-contained system in which wirelessly connected mobile hosts are free to move around anywhere and frequently operate as routers at the same time. The types of traffic in an ad hoc network vary significantly from that in a wireless network infrastructure[8]. The MANET routing protocol is critical for detecting a route with a high packet delivery ratio and ensuring that packets are delivered to the correct destination address [5].

The ad hoc on-demand distance vector protocol is an on-demand routing technique that makes it relatively easy to change the state of a connection. It is required to minimize network use by building a route. There are several AODV-defined message types between the source node and the destination node Route Replies (RREPs), Route Requests (RREQs), and Route Request Errors (RERRs) are the three types of responses[9]. Generally, AODV is an insecure routing system that lacks any way to identify and block transmission from the selfish node behavior, according to the entire study. The source node's IP address, the destination's IP address, and the Broadcast ID are all provided in RREQ. It establishes a reverse path from all nodes back from the source to the destination automatically. Nodes set up a forward pointer to the destination as RREP is propagated back to the source[10]. The selfish nodes use the network for their purposes and only send their data packets to facilities, but do not help to relay the data packets of the other neighboring nodes to conserve their energy resources. The other group of nodes that appear to damage and manipulate the network facilities is the other malicious nodes[11].

3. Research Methodology

We used the design research methodology. This research is focused on the packets to be transmitted to the correct destination. When we see the details of the research the main focus is on the packets (RREQ and RREP) that reach the correct destination from the source and from the correct destination to the source, in other words, to minimize the incorrect RREP packet from the selfish node to the source node. The parameters in this research are total packet lost/drop, packet delivery ratio, and throughput. These parameters are usually expressed by numbers and percentages. The main focus of our algorithm is to develop an algorithm used to detect selfish nodes. We used the design science research method to design the properties of AODV in the NS2 simulation tool[12].

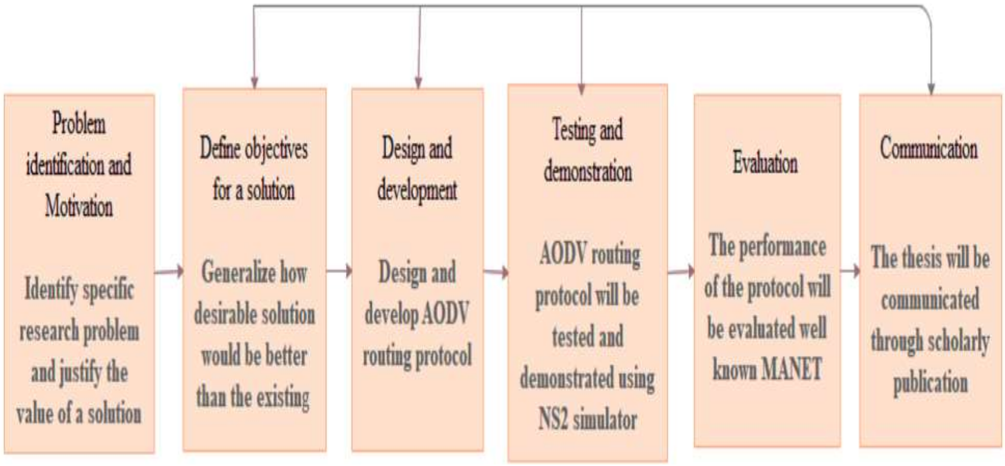
Problem identification and Motivation
Identify specific research problem and justify the value of a solution
Define objectives for a solution
Generalize how desirable solution would be better than the existing
Design and development
Design and develop AODV routing protocol
Testing and demonstration
AODV 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. Design Science Research Methodology (DSRM) Process Model[12].

Proposed Selfish Node Detection Algorithm - The proposed approach implements the AODV routing protocol performance with selfish and without selfish nodes. The proposed solution is implemented based on the modification of the AODV routing protocol using the Selfish Node Detection Algorithm (SFNDA). In this proposed approach, the researchers focused on the RREP destination that sends from any intermediate or destination node to the source node. The network efficiency is low with selfish nodes, and packets are dropped during transmission. Almost all selfish nodes want to save their resources in AODV, by ignoring all messages that are allocated to it, it is simple for the node to be selfish. For this reason, Requests are sent to all neighbors during route discovery in AODV to find the path. Before performance degradation occurred, this study detected the selfish nodes. This was achieved by a detected selfish node that disturbs the entire network, dropping the packet of the control message, and then the source node decides to send the control message to another node and takes a different path. The destination node becomes disabled after the RREP is replayed. In this case, the source node has already sent the actual message, but the destination of the message is not reached. We will establish a mechanism to extend the life of destination nodes after sending the reply to receive the actual message.

The proposed architecture is a design for reducing selfish nodes in MANETs by using the AODV protocol. If a selfish node exists in the network, the source node sends a route request to the destination node, which returns a false route reply to the source node. The source node assumes the RREP is coming from the selfish node and delivers data packets to it. When the selfish node gets a data packet from the source node, the data packet is dropped. If selfish nodes do not forward RREQ messages in MANET, they will not forward or drop these messages when they receive them to avoid becoming route members for other nodes. As a reason, they can avoid forwarding any messages to others. As a result of this behavior, the transmission path will need to be created on more nodes. If a node broadcasts an RREQ message and checks whether or not its neighbors have forwarded the message. The RREQ checking node is the name of this node. The RREQ-checked node is the monitored node. The RREQ checking node monitors its neighbors after broadcasting an RREQ message and records which neighbors have rebroadcast the same RREQ message. After a certain amount of time has passed, the RREQ checking node will analyze the routing table to see which nodes are not forwarding the RREQ message. These nodes are known as selfish nodes since they do not forward the RREQ message. After receiving SFNDA examines an RREQ message, an RREQ checked node must rebroadcast the message to its neighbors, including the RREQ message sender. This method is carried out by modifying the AODV protocol. The researchers used as Selfish Node Detection Algorithm approach to reduce selfish nodes.

Figure 7 shows the proposed architecture, which describes the overall architecture of the Selfish Node Detection Algorithm. First, to create ready node routing after creating the routing setup of the network to deploy the node next to select the source and destination address after that the discovery of the source &destination to establish the route next to if the node is selfish bypass routing that of to occur error transmission of data now by detecting SFNDA. On the other hand, if the node is not a selfish node forwarding control message it will be packet transmitted to the target node. Based on this the selfish node detection algorithm detects the selfish node. After selfish node detection, it will be the normal discovery of the path from source to the destination there establishing a route for the successful packet transmission from source to destination is done.

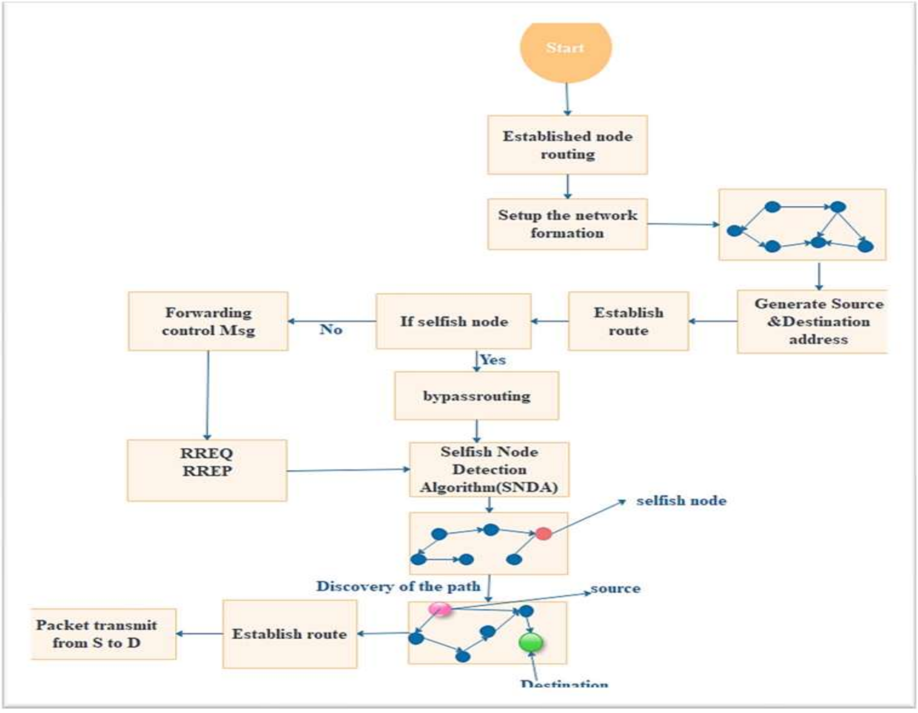

Figure 2. The Overall Proposed Architecture.

When the source node broadcasts RREQ to nearby nodes, including selfish nodes, a false RREP is generated and sent to the source node. Using the modification of the AODV protocol, the proposed algorithm compares RREP data with existing routing table data. Then, if the RREP comes from a selfish node, eliminate it from the route information and receive a new route RREP from a normal node. The proposed solution design proposes to minimize the effects of the selfish node in MANET while using the AODV routing protocol with the Selfish Node Detection Algorithm technique. Specifically, the Selfish Node Detection Algorithm approach, to minimize the selfish node by using the proposed solution. The reason for using on Selfish Node Detection Algorithm method is that it can detect and mitigate previously undiscovered and novel attacks. The proposed solution architecture in MANET is implemented by modifying the existing AODV routing protocol. The proposed solution simulated an existing selfish node on a simulation network environment, and then improved network performance by identifying and minimizing the impacts of the selfish node attacker. **Figure 8.** described in detail how to discard false RREPs delivered by abnormal nodes and send data packets to the destination node through a new route.

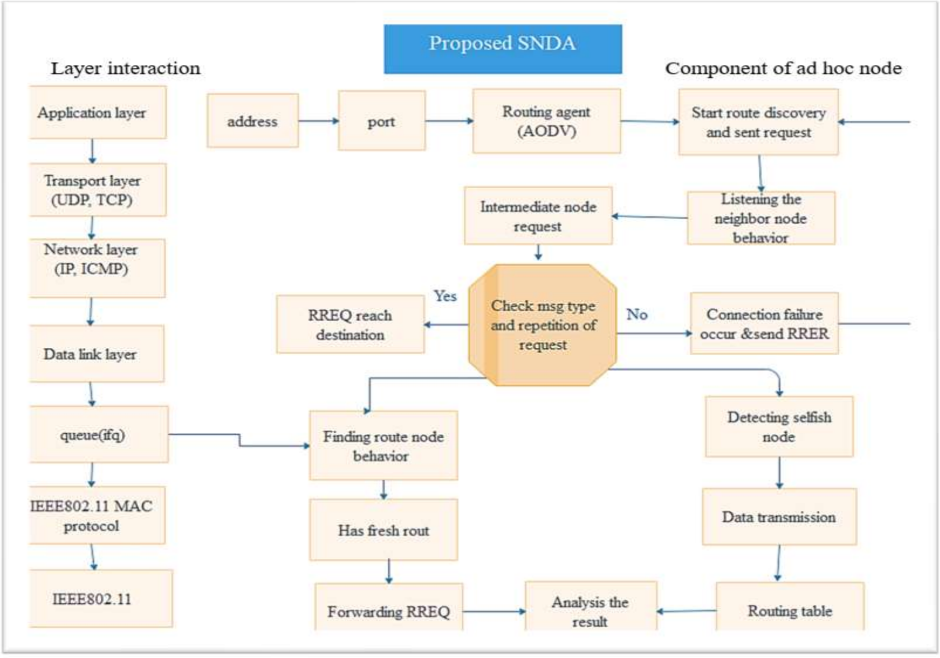

Figure 3. Flow Chart of Proposed SFNDA Algorithm.

Algorithm: The Proposed SFNDA flow description

Step 1: *initiate the source node*

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

Step3: *start* ***to*** *discover a real route within the collected neighbor information* ***and*** *send a request*

Step 4: *After discovering the route that broadcasts 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 the route request repetition occurs again* ***to*** *start* ***to*** *discover the route*

Step 7: ***If*** *the Next Node is immediately sent RREP, otherwise rebroadcast the request* ***to*** *the neighbor node until reaches* ***to*** *destination node.*

If *next node == DN {send RREP* ***to the*** *Source node*

Else IN *Rebroadcast RREQ}*

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

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

Step10: ***if*** *the RREQs reach* ***to*** *destination node then select, the target node that delivers the RREP* ***to*** *the source node.*

Step11: *The proposed SFNDA Approach compares RREP with Routing Table* ***in*** *AODV routing protocol* ***to*** *check whether the RREP packet is* ***from*** *the normal* ***or*** *selfish node.*

__Step 12__: __If__ the attacker exists __in__ the selected path, it sends immediately a false RREP __to__ the sender node. __If__ RREP does __not__ reach the source node the node is abnormal node RREP will be discarded on the other hand the connection failure occurs __and__ sent it RRER.

__Step 13__: __If__ routing information is matched then transfer real data __to__ the receiver node by selecting the shortest routing path.

__Step14__: Applied the proposed approach, change the route table information, __and__ block that RREP then finds the new path __to__ forward data packets __and__ the new fresh route __for__ effective communication.

__Step 15__: End.

4. Results and Discussion

Performance Metrics and Simulation Setup - the performance metrics are measured for two types of simulation scenarios such as: Based on the simulation environment to evaluate the proposed method in the AODV routing protocol, we have to use two simulation scenarios. In the first scenario, we test the effectiveness of the proposed approach by using variable numbers of normal nodes and a fixed number of normal nodes without selfish nodes that contrast the outcomes of both recommended protocols with the effectiveness of the routing protocols currently in use[13]. The original AODV routing protocol is the first existing protocol with which we compare our findings, and the proposed selfish node detection algorithm in the AODV routing protocol in MANET is the second. In the second scenario, a fixed number of normal nodes and a variable number of selfish nodes are used to evaluate the proposed scheme's security performance.

Simulation Parameter **-** in this simulation, a simulation is simulated on a network topology dimension of the simulation area of 1000m x 1000m and 20 nodes that are randomly disturbed in this area. The nodes will be moving within the network space according to the random placement model[14].In this network simulation, we have used a UDP connection and the tests performed on CBR under 1000 bytes. The simulation did not use a TCP connection for the simulation, because in a TCP connection the source node will stop the connection if the TCP ACK packets are not received. In this simulation, the selfish node is selected because that can be dropped a large number of data packets. Since we didn't consider the mobility model, we took the area randomly. The trace graph is selected because it can take any trace file format without any configuration AWK files. We have taken 20 nodes and 100ms in this network environment for effective network communication. The time used in this simulation is 100 seconds. The number of nodes involved in the experiments is 20, the number of selfish nodes involved in the experiments is varied from 1 to 6 and random waypoint mobility is used as the mobility model [14],[15]. Proposed AODV, EX-AODV, and AODV under selfish nodes are used as routing protocols. The overall experimental parameters are summarized in **Table 1.** Generally, we have chosen the simulation setup was settled according to which taken from recent paper depends on AODV routing protocol standards.

Table 1. Simulation Parameters Set up.

parameter	Values
Simulation tool	NS-2.35
Simulation area	1000m*1000m
Routing protocol	AODV
Number of nodes	10,20
Traffic type	CBR
Packet size	1000byte
Type of attack	Selfish node

platform	Ubuntu 16.04
Type of connection	UDP
Mobility	RWP
Simulation time	100s

By using **Table 2** the simulation set the following simulation results are simulated using the Nam window. New AODV agent .h and .cc file for AODV simulations provided with ns-2.35. The trace file generated from the simulation and files parsed to evaluate the performance of the routing protocols (dropped packet, packet delivery ratio, end-to-end delay, and throughput). This section describes the metrics adopted for evaluating the considered routing algorithms. Routing in communication networks depends on the definition of a performance indicator called routing metrics. Simulation Result Analysis and Discussion - in our simulation result, the packet delivery ratio performance the as shown **in Figure 9.**, the increase in the number of nodes in the network has a direct effect on the increase in the number of dropping packets. This is because the number of route breaks increases with the increased number of nodes or network size. This means that when the number of intermediate nodes increases between the source and the destination node then the probability of route break also increases. In the case of our developed algorithm, the probability of packet dropping is less than EX- AODV. The increase of packet dropping in AODV under selfish nodes is because of the packet dropped by the selfish nodes. The relative increase of PDR in our developed proposed AODV shows the feasibility of the algorithm along with its scalability. When there is a normal node in the network, the PDR performance for protocols namely for EX-AODV (88.5%), AODV under selfish node (50%) and proposed-AODV (92.5%) on the number of nodes. The packet dropping in AODV under selfish nodes is increasing because of the packet dropped by the selfish nodes. However, the packet delivery ratio has been achieved in proposed-AODV, as the number of node size increases proposed-AODV outsmarts an EX-AODV routing protocol.

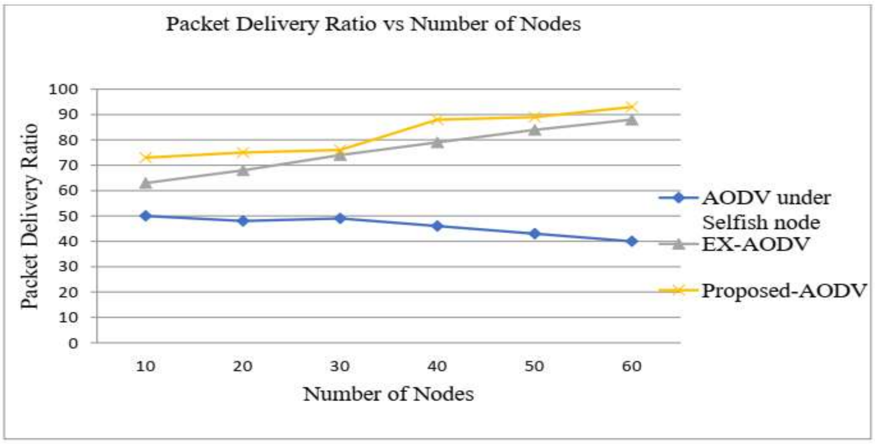

Figure 4. Packet Delivery Ratio vs Number of Nodes.

The packet delivery ratio is the best performance metric in the evaluation. However, the performance of proposed AODV, EX-AODV and AODV under selfish node in terms of PDR depends on this simulation the proposed detection method shows better PDR when compared to EX-AODV and AODV under selfish node in MANET. When the number of selfish nodes increases then the packet delivery ratio will decrease but in the proposed AODV the PDR has increased. On comparing the proposed AODV with the existing AODV and AODV under the selfish nodes, the proposed AODV provides better than existing AODV and AODV under selfish node ratio values. Therefore, proposed AODV perform better PDR under the presence of selfish nodes on both protocols is high selfish nodes on the network as illustrated in **Figure 1.5**.

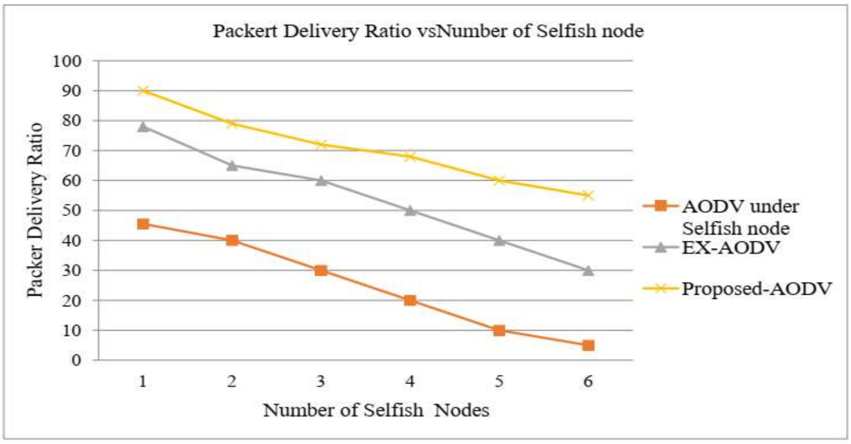

Figure 5. Packet Delivery Ratio vs Number of Selfish Nodes.

The evaluation metrics of an end-to-end delay are represented by the performance of EXAODV, proposed AODV, and AODV under the selfish node. The result shown in Figure 1.6 was the time taken to packet reach the destination from the source. Since the packet sent from the source reaches the destination through the intermediate node, selfishness and packet drop increase up to the packet received by the destination node. This was why the end-to-end delay of the received packet was increased. Here delay specifies in milliseconds for a particular packet transferred from a destination. However, to illustrate the figure end-to-end delay is in both the proposed AODV selfish node detection and EX-AODV rather than compared to under selfish node. Yet, for the proposed AODV protocols, the average delay is slightly the same as EX-AODV. Thus, the proposed AODV performs better average delay than EX-AODV and AODV under the selfish node. Thus, the proposed AODV performs better on average end-to-end delay measurement.

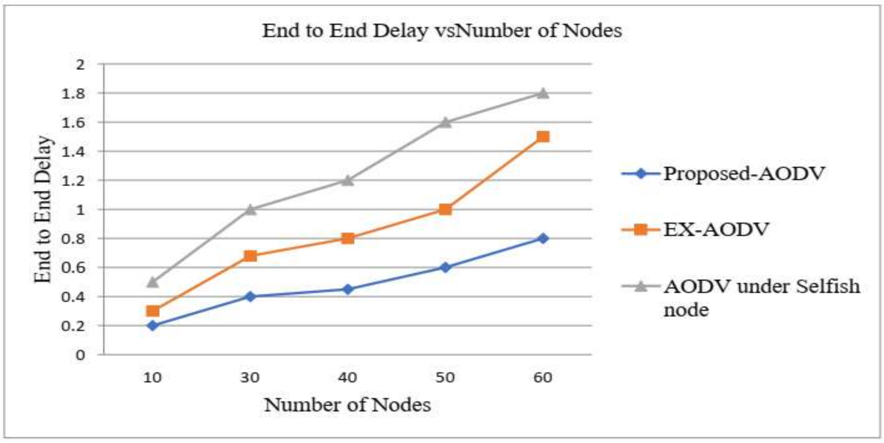

Figure 6. End-to-end Delay vs Number of Nodes.

The simulation time for the sent event and received event in existing AODV. From the **Figure 7.**, delay of the received packet was high because up to the packet reaching the destination, the number of intermediate nodes increased, thus the chance of the intermediate node being selfish was high and in this case interference and delay at the intermediate node. The delay of receiving packets higher than sending packets in existing AODV and AODV under selfish nodes. It includes all possible delay causes such as route discovery, queuing and retransmission delay, and Packet drop. The performance results in terms of end-to-end delay achieved in figure 4.8, the performance of average delay during the network under the presence of selfish nodes shows that EX-AODV protocol, AODV under the selfish node. Furthermore, the average delay improved in proposed AODV protocols provides a low delay because selfish node detection algorithm. Detect the selfish node and select the normal node to send packets. If the number of selfish nodes increases then the delay also increases. As a result, the proposed AODV performs good performance during the presence of selfish nodes and has been improved to varying degrees.

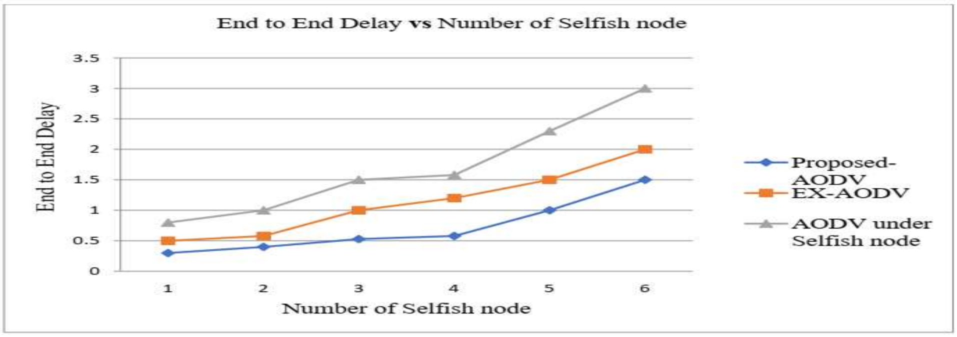

Figure 7. End-to-end Delay vs Number of Selfish nodes.

As the simulation result, the average throughput time increased the total amount of packets sent to a destination decreased. Here the packet dropped for different reasons, especially selfish nodes since there was no method to capture them during route discovery. This was calculated with the number of sent packets and the number of packets that reaches the destination. The result was taken from each source and destination node from the network information of the trace analyzer. This result was taken from the proposed AODV after adding the selfish node detection algorithm. The result was taken with the same parameter and the same number of nodes. EXAODV and AODV under selfish node protocols show no significant difference in the number of nodes in the network but, the proposed AODV achieved there is a significant difference between both protocols as depicted in **Figure 8.** However, in the proposed AODV protocol the average throughput is better than EX-AODV and AODV under selfish nodes during normal operations. When the evaluation of the proposed AODV selfish node detection enhances good results under the selfish node. So, the proposed enhanced the throughput in MANET. The results show as the number of nodes increases, as well as the throughput, also increases.

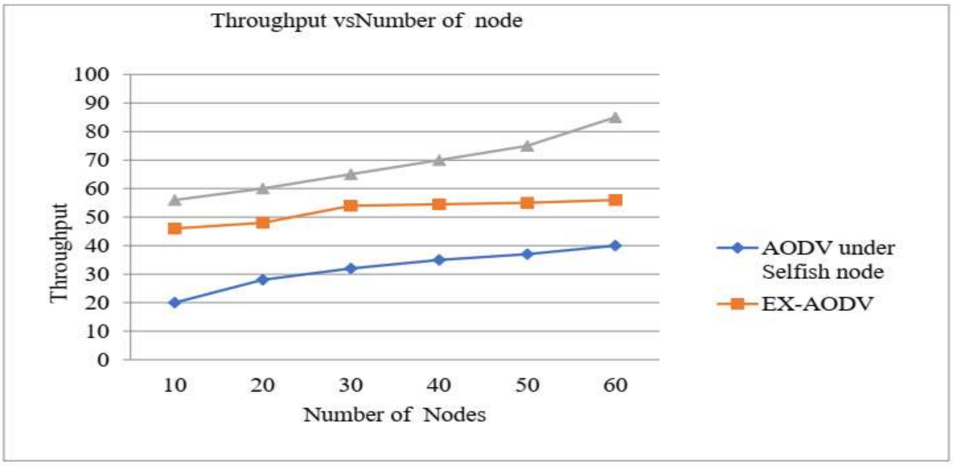

Figure 8. Throughput vs Number of nodes.

The comparison of the throughput of existing AODV, AODV under selfish node and proposed AODV with selfish node detection algorithm. After detecting the node behavior during route discovery, the selfish node is detected and the routing is done through the normally behaving node only. The metrics analyzed with the number of messages delivered per second. It is described as the total number of received packets at the destination out of the total transmitted packets depending on the proposed node evaluate performance throughput on both protocols was represented in the following **Figure9.** When the network is under the presence of selfish nodes condition, EXAODV and AODV under selfish node throughput have dropped and thus, the proposed AODV protocols throughput performance is shown better improvement than both protocols. Therefore, we conclude that the proposed algorithm is more effective than EX-AODV and AODV under selfish nodes in alleviating the effect of selfish nodes.

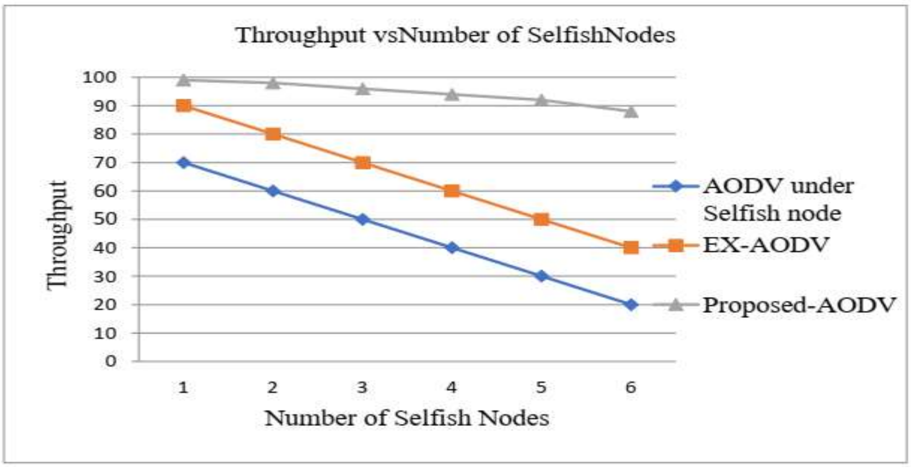

Figure 9. Throughput vs Number of Selfish Nodes.

We simulate the performance of EX-AODV, proposed AODV and AODV under the selfish node. Depending on the proposed solution improves the performance of existing AODV and AODV under selfish nodes by selecting the normal node to transfer the data. The result of all performance metrics is different thus proposed selfish node detection algorithm enhances the performance of AODV by reducing packet drop, increasing packet throughput and reducing the delay. The packet delivery ratio for the proposed AODV was best. So based on **Figure 10.** EX-AODV and proposed AODV have a low number of dropped packets that increase the number of nodes in the network has a direct effect on the increase in the number of dropping packets but AODV under selfish node has a high number of dropped packets. The following graph shows the packet dropped is very much detected in the proposed detection method when compared to AODV under selfish node and EX-AODV.

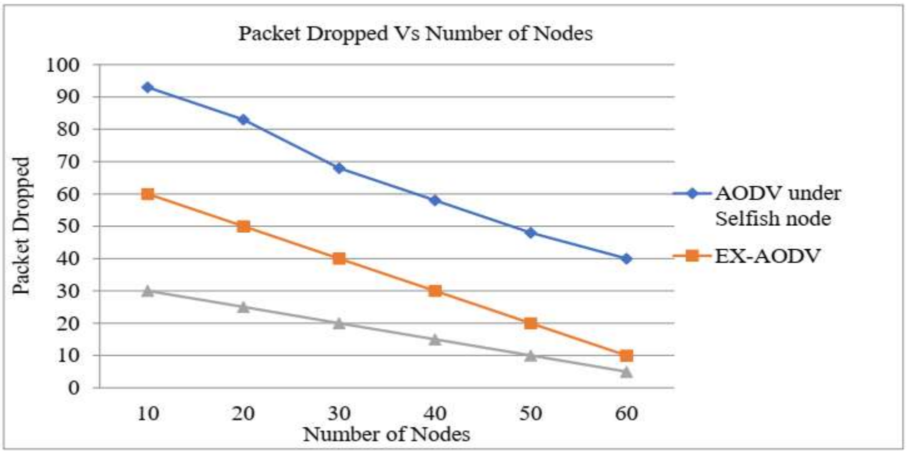

Figure 10. Packet Dropped Vs Number of Nodes.

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 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

From the result, we concluded that detecting the selfish node during routing discovery was very important to selecting a normal path. This results in the best throughput decreases delay, and increases the packet delivered (minimizes the packet drop). The proposed SFNDA used the AODV protocol to overcome the problem caused due to retransmission, packet collision, packet loss, and other factors that cause performance degradation.

5. Conclusion and Future Work

In this thesis, selfishness behavior was used to express the problem with AODV routing protocol performance. The solution to the node's selfish behavior was discovered through a review of various works of literature. Most of MANET's proposed protocols suppose that mobile users are not selfish and that they all participate to the same extent. Selfish nodes attempt to promote their gains. They may, refuse to relay messages from other nodes or may willingly relay messages from friends or nodes inside their communities but not from strangers. A selfish node will usually refuse to collaborate in packet transmission, causing major network performance issues. The goal of this research was to find the best AODV protocol by incorporating a selfish Node Detection algorithm during route discovery. As a result, the new AODV outperforms the current AODV in simulation. To evaluate the suggested method, this research focuses on four performance metrics: packet delivery ratio, packet drop, end-to-end delay, and throughput. The NS-2.35 was used to evaluate the performance of existing AODV and new AODV with SFNDA routing protocol in this research.to accomplish networking functions, MANET is heavily reliant on node cooperation. As a result, it is extremely sensitive to selfish nodes.

Future Work

In the future, we recommended to work on the following aspects:

The proposed selfish node detection algorithm is done on the broadcast and packet dropped in the date transmission for detecting selfish nodes in the simulation environment to test and evaluate our proposed method in the AODV protocols.

- In the future, we suggested simulating and analyzing different performance metrics such as
- link failure, queue, congestion problem, and energy consumption in NS2.
- Another component of future work will be to develop methods for restoring the node to the
- network utilizing the NS2/NS3 environment if the selfish behavior resumes normal and
- a real-world scenario is used to validate the proposed method.

Reference

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, doi: 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, doi: 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, doi: 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, doi: 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, doi: 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. A. Agrawal, "Manet : Comparion on AODV and DSR," no. February, pp. 77–82, 2016.
9. A. 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, doi: 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, doi: 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, doi: 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, doi: 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. A. 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, doi: 10.5815/ijitcs.2013.06.10.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.