

A cluster-based Bayesian approach to reliable route discovery in large-scale mobile ad hoc networks

A Troskie

 **orcid.org/0000-0003-4970-2006**

Dissertation accepted in fulfilment for the requirements for the degree *Master of Engineering* in Computer and Electronic Engineering at the North-West University

Supervisor: Prof ASJ Helberg

Graduation: June, 2021

Student number: 25001698

Abstract

The application of MANETs have become a central point of focus in the development of wireless networks. However, MANETs still face the challenge of reliable route discovery in large-scale networks under adverse node failure conditions. To address this issue, a novel adaptation of the AODV protocol called the Naïve Bayes Classifier Routing (NBCR) protocol is presented. Furthermore, an extension of this protocol via a clustering overlay is also presented, and respectively called the Cluster-based Naïve Bayes Classifier Routing (CB-NBCR) protocol. Using Bayes' theorem and a classifier probability framework, posterior route trust probabilities are calculated from prior evidence. These probabilities are used to select routes that would improve network performance on large-scale networks in the presence of dysfunctional/selfish nodes. The clustering overlay additionally attempts to improve network performance by reducing large ad hoc networks to more manageable topologies.

Keywords: Ad Hoc Network; Routing Protocol; Bayesian Classifier; Clustering

Contents

1	Introduction	1
1.1	Mobile Ad Hoc Networks and Routing Protocols	1
1.2	Simulation Software	3
1.3	Propagation and Mobility Models	4
1.4	Clustering Techniques	5
1.5	Machine Learning and Bayes' Theorem	6
1.6	Summary	6
2	Research Problem, Objectives and Methods	7
2.1	Literature Review and Research Problem	7
2.2	Research Aim and Objectives	10
2.3	Research Tools and Methods	10
2.3.1	Simulation Software	10
2.3.2	Propagation and Mobility Models	11
2.3.3	Evaluation Metrics	11
2.4	Notation and Assumptions	12
2.5	Research Procedure	13
2.6	Summary	15
3	Ad Hoc On-Demand Distance Vector Routing	16
3.1	Operation	16

3.2	Performance Evaluation	17
3.3	Summary	21
3.3.1	Performance Analysis	21
3.3.2	Final Remarks	22
4	Naïve Bayes Classifier Routing	23
4.1	Protocol Design	23
4.1.1	Implementation	23
4.1.2	Protocol Operation	28
4.2	Operational Evaluation	32
4.2.1	Classifier Sensitivity	32
4.2.2	Routing	33
4.3	Performance Evaluation	40
4.4	Summary	44
4.4.1	Protocol Operation	44
4.4.2	Operational Analysis	44
4.4.3	Performance Analysis	45
4.4.4	Final Remarks	46
5	Clustering Overlay	47
5.1	Protocol Design	47
5.1.1	Node Designation	47
5.1.2	Clustering Framework	47
5.1.3	Protocol Operation	50
5.2	Operational Evaluation	52
5.2.1	Multiplier Values	52
5.2.2	Neighbour Count Threshold	54

5.2.3	Clustering	56
5.3	Performance Evaluation	63
5.4	Summary	66
5.4.1	Protocol Operation	66
5.4.2	Operational Analysis	67
5.4.3	Performance Analysis	67
5.4.4	Final Remarks	68
6	Conclusion and Future Work	69
6.1	Analysis	69
6.1.1	Overview of Results	69
6.2	Final Remarks	77
A	Ad Hoc On-Demand Distance Vector Routing	82
A.1	Performance Evaluation	82
B	Naïve Bayes Classifier Routing	84
B.1	Performance Evaluation	84
C	Clustering Overlay	86
C.1	Cluster Creation Test	86
C.2	Performance Evaluation	89
D	Conclusion and Future Work	90
D.1	Analysis of Results	90

List of Figures

2.1	Node notation color scheme.	13
2.2	Stationary scenario.	13
2.3	Mobile scenario.	13
2.4	Variable transmission range; increased hop count.	14
2.5	Fixed transmission range; increased node density.	14
3.1	AODV RREQ packet propagation (a) and RREP packet propagation (b). .	17
3.2	AODV simulation results; variable transmission range; static.	19
3.3	AODV simulation results; variable transmission range; mobile.	19
3.4	AODV simulation results; fixed transmission range; static.	20
3.5	AODV simulation results; fixed transmission range; mobile.	20
4.1	NBCR RREQ packet handling flowchart.	28
4.2	Illustration of NBCR RREQ packet propagation.	29
4.3	Illustration of NBCR RREP packet propagation.	30
4.4	NBCR RREP packet handling flowchart.	31
4.5	NBCR classifier sensitivity test between feature vector variables.	32
4.6	Graphical representation; Test 1.	34
4.7	Graphical representation; Test 2.	36
4.8	Graphical representation; Test 3.	38
4.9	NBCR simulation results; variable transmission range; static.	42

4.10	NBCR simulation results; variable transmission range; mobile.	42
4.11	NBCR simulation results; fixed transmission range; static.	43
4.12	NBCR simulation results; fixed transmission range; mobile.	43
5.1	An example of inter-cluster communication.	48
5.2	CB-NBCR clustering procedure overview.	50
5.3	CB-NBCR Multiplier Values Test; Graphical representation.	53
5.4	CB-NBCR Multiplier Values Test; Simulation results.	53
5.5	CB-NBCR Multiplier Values Test; Graphical representation.	55
5.6	CB-NBCR Multiplier Values Test; Simulation results.	55
5.7	Graphical representation; Cluster Creation Test.	57
5.8	<i>First Auxiliary Timer</i> expires; Cluster Creation Test.	58
5.9	<i>Second Auxiliary Timer</i> expires; Cluster Creation Test.	58
5.10	Graphical representation; Cluster Maintenance Test 1.	60
5.11	Clusters have been formed; 0 - 50s; Cluster Maintenance Test 1.	60
5.12	Clustering is abandoned; 50s - 100s; Cluster Maintenance Test 1.	60
5.13	Graphical representation; Cluster Maintenance Test 2.	62
5.14	Clusters have been formed; 0 - 50s; Cluster Maintenance Test 2.	62
5.15	Control has been relinquished to a new cluster head; 50s - 100s; Cluster Maintenance Test 2.	62
5.16	CB-NBCR simulation results; variable transmission range; static.	64
5.17	CB-NBCR simulation results; variable transmission range; mobile.	65
5.18	CB-NBCR simulation results; fixed transmission range; static.	65
5.19	CB-NBCR simulation results; fixed transmission range; mobile.	66
6.1	Packet delivery ratio simulation results; variable transmission range; static.	70
6.2	Packet delivery ratio simulation results; variable transmission range; mobile.	70
6.3	Packet delivery ratio simulation results; fixed transmission range; static.	71

6.4	Packet delivery ratio simulation results; fixed transmission range; mobile. . .	71
6.5	Average end-to-end delay simulation results	72
6.6	Successful connections simulation results; variable transmission range; static.	73
6.7	Successful connections simulation results; variable transmission range; mobile.	73
6.8	Successful connections simulation results; fixed transmission range; static. .	74
6.9	Successful connections simulation results; fixed transmission range; mobile.	74
6.10	Throughput simulation results; variable transmission range; static.	75
6.11	Throughput simulation results; variable transmission range; mobile.	75
6.12	Throughput simulation results; fixed transmission range; static.	76
6.13	Throughput simulation results; fixed transmission range; mobile.	76

List of Tables

1.1	Recent advancements in AODV extensions.	2
1.2	Overview of common network simulation packages.	3
1.3	Examples of MANET clustering schemes.	5
3.1	AODV simulation parameters; constant	18
3.2	AODV simulation parameters; variable	18
4.1	NBCR training data.	25
4.2	NBCR training data; categorised.	26
4.3	NBCR RREP packet format.	30
4.4	NBCR <i>Trust Table</i> format.	30
4.5	NBCR classifier sensitivity test results.	33
4.6	NBCR simulation parameters; Test 1	33
4.7	Routing Table; Test 1	34
4.8	<i>Trust Table</i> for 10.0.0.10; Test 1	34
4.9	NBCR simulation parameters; Test 2	36
4.10	Node drop probability; Routing Test 2	37
4.11	<i>Trust Table</i> for node 10.0.0.8; Routing Test 2	37
4.12	Routing table; Routing Test 2	37
4.13	Simulation parameters; Test 3	39
4.14	Routing Table; Routing Test 2	39

4.15	<i>Trust Table</i> for 10.0.0.8; Routing Test 3	40
4.16	NBCR simulation parameters; constant	41
4.17	NBCR simulation parameters; variable	41
5.1	CB-NBCR <i>Hello</i> message format.	49
5.2	CB-NBCR <i>Neighbour Table</i> format.	49
5.3	CB-NBCR <i>Node Designation</i> message format.	49
5.4	CB-NBCR <i>Cluster Control</i> message format.	49
5.5	CB-NBCR Multiplier Values Test; Simulation parameters.	52
5.6	CB-NBCR Multiplier Values Test; Simulation results.	52
5.7	CB-NBCR Node Density Test; Simulation parameters.	54
5.8	CB-NBCR Node Density Test; Simulation results.	54
5.9	Simulation parameters; Clustering Creation Test	56
5.10	Node drop probability; Cluster Creation Test	57
5.11	Simulation parameters; Cluster Maintenance Test 1	59
5.12	Nodes selected for network removal; Cluster Maintenance Test 1	59
5.13	Simulation parameters; Cluster Maintenance Test 2	61
5.14	CB-NBCR simulation parameters; variable	63
5.15	CB-NBCR simulation parameters; constant	64
6.1	Observations made with regards to the simulation results.	77
6.2	Overview of suitable applications for each protocol.	78
A.1	AODV simulation results; variable transmission range.	82
A.2	AODV simulation results; fixed transmission range.	83
B.1	NBCR simulation results; variable transmission range.	84
B.2	NBCR simulation results; fixed transmission range.	85

C.1	<i>Neighbour Table</i> for cluster heads; Cluster Creation Test.	86
C.2	Trust Table for 10.0.0.1; Cluster Creation Test	87
C.3	Routing Table 1; Cluster Creation Test	87
C.4	Routing Table 2; Cluster Creation Test	88
C.5	CB-NBCR simulation results; variable transmission range.	89
C.6	CB-NBCR simulation results; fixed transmission range.	89
D.1	Tabular simulation comparison; variable transmission range; static	90
D.2	Tabular simulation comparison; variable transmission range; mobile	91
D.3	Tabular simulation comparison; fixed transmission range; static	91
D.4	Tabular simulation comparison; fixed transmission range; mobile	92

Table of abbreviations

MANET	Mobile Ad Hoc Network
AODV	Ad hoc On-Demand Distance Vector Routing
NBCR	Naive Bayes Classifier Routing
CB-NBCR	Cluster-based Naive Bayes Classifier Routing
RREQ	Route Request
RREP	Route Reply
RERR	Route Error
P2P	Peer-to-Peer

Chapter 1

Introduction

This chapter contains an overview of topics related to the main theme of the report, and provides a concrete foundation to contextually understand the content of the proceeding chapters.

1.1 Mobile Ad Hoc Networks and Routing Protocols

A mobile ad hoc network (MANET) [1] is a collection of mobile nodes that have the ability to arbitrarily and temporarily self-organise into dynamic topologies allowing the interconnection of wireless devices over geographical areas with no prior network infrastructure. However, some of the open issues to be addressed include security, routing and the scalability to large networks [2].

A key requirement for the development of MANET technology is appropriate routing protocols that provide efficient and uninterrupted transmission of data over a span of mobile nodes. To address the challenge of routing, different routing protocols have been explored and/or are still under development.

Routing protocols are generally divided into two broadly defined classes- *reactive* and *proactive* [1]. Reactive (on-demand) protocols only create routes when the need arises, and proactive (table-driven) protocols create and store routing information on an interval basis which ensures that the route from the source to the destination is immediately available at all times. Some routing protocols take advantage of both the table-driven and reactive approaches to create *hybrid* protocols for various unique applications.

Some examples of recent developments include:

Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N): [3] This protocol pro-actively maintains information about the existence of nodes in a mesh that are accessible via single-hop and multi-hop communications. The strategy of this protocol is to determine for each destination in the mesh one single-hop neighbour which can be utilised as the best gateway to communicate with a destination node. B.A.T.M.A.N also utilises very small control packets, which additionally improves network performance.

Babel Routing Protocol: [4] This protocol is based on the distance-vector algorithm augmented with mechanisms for loop avoidance as well as starvation avoidance. Babel's route loop-avoidance mechanism relies on making a route unreachable after a retraction until all neighbouring nodes have been guaranteed to have acted upon the retraction. Successful deployments of this protocol include hybrid networks, large scale overlay networks, pure mesh networks, as well as small unmanaged networks.

The most popular reactive and proactive routing protocols, however, are the Ad Hoc on Demand Distance Vector (AODV) and Destination-Sequenced Distance-Vector (DSDV) routing protocols, respectively, this is due to their flexibility/extendibility to achieve specific desired functionalities [5, 6]. For reactive routing, many adaptations of AODV have been explored to achieve desired outcomes with regards to quality of service, energy optimisation, security, and multipath routing. This proves the flexibility of AODV to accommodate a change in its functionality and has therefore been chosen as the basis for the protocols presented in this dissertation. Examples of recent AODV extensions and their conceptual designs are depicted in Table 1.1 [7].

Table 1.1: Recent advancements in AODV extensions.

Abbreviation	Descriptive Name	Conceptual Design and Objective
AOMDV	Ad Hoc On-Demand Multipath Distance Vector	Use multiple loop-free and link disjoint paths to improve end-to-end delay.
RAODV	Resilient On-Demand Distance Vector	Reduce packet loss by falling back on multiple alternatively discovered routes on link-break.
FE-AODV	Fuzzy Energy-based Ad Hoc On-Demand Distance Vector	Use fuzzy logic to consider power consumption based on bandwidth, hop count and lifetime.
ES-AODV	Energy-saving Ad Hoc On-Demand Distance Vector	Reduce energy consumption through the monitoring of various energy-draining metrics.
BP-AODV	Black-hole Protected Ad Hoc On-Demand Distance Vector	Protect against black-hole attacks through challenge-response-confirm algorithms.
Trust AODV	Trust-based Ad Hoc On-Demand Distance Vector	Secure routing between nodes through the exclusion of malicious nodes with the use of a trust model.

1.2 Simulation Software

In the evaluation of MANETs, researchers usually resort to testing through the use of experimental networks (testbeds) or simulation packages. The latter is more appealing since it only requires computational power to deliver results and is not comprised of actual physical components or measurements. Many studies have been done on the accuracy of network simulators [8, 9, 10, 11, 12] with varying results. At best, it can be said that no network simulator is accurate- instead, a good network simulator should be dependable and realistic given the scenario. Table 1.2 provides an overview of well known simulation packages and their characteristics [13, 14, 15].

Table 1.2: Overview of common network simulation packages.

Simulation Package	License	Advantages	Disadvantages
Ns-2	Open Source	1. Extensions provide realistic simulations 2. Supports the simulation of TCP 3. Provides simulation over 5 layers of the OSI model	1. Out of date documentation 2. Multi-threaded simulations are not supported 3. Does not perform well when simulating large networks
Ns-3	Open Source	1. Good documentation 2. Performs better than Ns-2	1. Not backwards compatible with Ns-2 2. Limited support in terms of visualisation
OMNET++	Open Source	1. Supports large scale network simulations well 2. Supports parallel simulations 3. Provides a graphical tool for performance analysis	1. Poor documentation 2. Does not provide a wide array of supported protocols
OPNET	Commercial	1. Provides a good protocol design environment 2. Excellent documentation 3. Supports large scale network simulations well	1. No energy model support 2. Provides limited support to wireless protocols
Glomosim	Free	1. Versatile in scalability of networks 2. Supports wireless network protocols 3. Supports parallel simulations	1. Struggles to compete with other packages and modern simulation techniques 2. Poor documentation
QUALNET	Commercial	1. Provides graphical overview of various performance metrics 2. Provides adequate animation tools 3. Provides graphical interface for performance evaluations	1. Very expensive

1.3 Propagation and Mobility Models

Radio propagation models are used to determine the path loss along a link, and are chosen based on the simulation scenario, terrain, buildings or other terrestrial obstructions. Examples of radio propagation models which are commonly readily included in many simulation packages include [16]:

1. The Free Space Propagation Model, which assumes a direct line of sight between the transmitter and receiver with no reflections or multipath variables.
2. The Two-Ray Ground Propagation Model, which assumes two paths between the transmitter and receiver; one a direct line of sight path, and the other a reflected path.
3. The Shadowing Propagation Model, which assumes that the power received is not only a function of distance from the transmitter, but also a function of fading effects.

Propagation models that more closely represent realistic scenarios, but require manual implementation, include [17]:

1. A combination of the Free Space and Two-Ray Ground propagation models.
2. The Intelligent Ray Tracing Model, which models the use of ray tracing to determine all possible signal paths between the transmitter and receiver over a geographical area.

Mobility models are categorised as homogeneous or heterogeneous, with homogeneous models exhibiting cooperation of nodes between neighbours, and heterogeneous models exhibiting singular movement patterns unique to each node. An example of a homogeneous mobility model which is included in most simulation packages is the Pursue Mobility Model, in which nodes move towards a single target with a uniform speed [18].

Heterogeneous models are more common, and include [18]:

1. The Random Waypoint Mobility Model, in which mobile nodes are randomly deployed, and arbitrarily select unique destinations.
2. The Manhattan Mobility Model, in which nodes move either vertically or horizontally in a grid topology.

Mobility models that more closely exhibit reality, require manual implementation include [19]:

1. The Smooth Random Mobility Model, where temporal dependency of velocity varies over time.
2. The Pathway Mobility Model, which implements paths and obstacles as a function of geographic restriction.

1.4 Clustering Techniques

Clustering in MANETs is a technique that groups nodes together that exhibit similar characteristics. This technique helps to maintain aggregation and network topology in large scale networks, as well as conserving communication bandwidth and reducing overall transmission overhead in some instances. [20].

Clusters are formed based on a specific combination of different metrics, such as the identity, degree, mobility, transmission range, or battery power of the nodes. A cluster typically consists of a cluster head, member nodes and gateway nodes, where the coordination within the substructure is governed by the cluster head and the communication between clusters is done through the gateway nodes. Some examples of clustering schemes are showed in Table 1.3 below [21, 22]. Since the Flexible Weight-based Clustering Algorithm (FWCA) is focussed on forming clusters based on a combination of different/mutable metrics, it provides a good basis for future adaptations by providing the means to address different scenarios through changing these variables and their weights as needed. For this reason, the FWCA forms a central part of this dissertation.

Table 1.3: Examples of MANET clustering schemes.

Abbreviation	Descriptive Name	Concept/Characteristics
DMAC	Distributed Mobility-Adaptive Clustering	Weight-based clustering algorithm based on mobility-related metrics.
FWCA	Flexible Weight-based Clustering Algorithm	Weight-based clustering algorithm based on a combination of different metrics.
k-CONID	k-hop Connectivity ID Clustering	Clustering algorithm based on a combination of two existing algorithms: 1. Lowest-ID clustering. 2. Highest-degree Clustering.
CEC	Cluster based Energy Conservation algorithm	Energy-based clustering algorithm that removes redundant nodes from the network.
CMDSR	Cluster-Based Multipath Dynamic Source Routing	Node-degree based clustering algorithm which is focussed on creating hierarchies that reduce network traffic.
ACA	Adaptive Clustering Algorithm	Clustering algorithm that allows nodes to assume new roles after clusters have already been formed through various metrics.

1.5 Machine Learning and Bayes' Theorem

Bayes' theorem is a statistical method to compute the conditional probability of an observed outcome based on prior knowledge of conditions related to the event, and has applications in fields stretching from artificial intelligence and computer systems to decision analysis [23].

Some examples of the application of Bayes' theorem in the field of MANETs include the detection of misbehaving nodes through the evaluation of posterior probability [24] and disconnection management in peer-to-peer (P2P) networks through the use of a Bayesian filter [25]. However, in the context of this dissertation the focus of application is shifted to the field of reliable routing in large scale MANETs exhibiting node failures, as discussed in the proceeding chapter.

Machine learning is the process of extracting information from considerably large data sets for the purpose of self-learning. This data is then analysed and applied through various statistical methods[26].

Machine learning primarily implements two different learning styles:

1. Supervised learning, where input/training data has a pre-determined label and a function or classifier is built and trained to predict the label of test data.
2. Unsupervised learning, where input/training data is not labelled. A classifier is then designed to deduce existing patterns or clusters in training datasets.

Implementations of supervised learning include the Naïve Bayes Classifier, Support Vector Machine and Decision Tree algorithms [26]. Naïve Bayes classifiers are simple probabilistic classifiers that are based on applying Bayes' theorem with the assumption of independence between classifier variables [27]. These classifiers are easily implemented and predominantly used to calculate probabilities based on posterior events and data. For this reason, the Naïve Bayes Classifier will form a central part in the proceeding chapters.

1.6 Summary

From the preceding sections we see that the core functionality of a MANET is directly reliant upon appropriate routing protocols for communication between nodes. We also see that many routing protocols have been developed to target certain issues with regards to MANETs. In Chapter 2 some of the issues that remain unaddressed are examined, along with their supporting literature. Later sections of Chapter 2 provide a clear overview for the research problem of this dissertation along with the tools, methods and approaches that will be taken.

Chapter 2

Research Problem, Objectives and Methods

This chapter provides an overview of the research problem as well as the literature related to it. Additionally, the objectives, methods and tools that will be used to achieve specific desired outcomes are also covered.

2.1 Literature Review and Research Problem

Efficient On-Demand Routing Protocol (EORP): For reliable route discovery in MANETs, the Efficient On-Demand Routing Protocol (EORP) [28] using a Bayesian approach is a novel way of finding the best route between two nodes by the summation of the probability or affinity of the intermediate nodes towards a particular destination. This protocol is based on AODV, with the key differences being the handling of RREQ packets as well as route selection. Each node in EORP has a history table of the node's individual id, the attributes used to calculate affinity as well as the status of every route reply (RREP) received and (RREQ) sent- this data is used to calculate each node's affinity. An affinity index (AI) is the probability that a node will forward a packet to the desired destination based on historical evidence and is calculated using Bayes' theorem. During the propagation of RREQ packets, nodes will disregard packets if an affinity index already exists within their history table which has a more appealing value to a particular destination. Upon route failure, intermediate nodes try to repair the route locally. If this fails, a route error (RERR) message is generated forwarded back to the source node.

From [28], the affinity index (AI) of a node is formulated by

$$P(C_i|X) = \frac{P(X|C_i)P(C_i)}{P(X)} \quad (2.1)$$

$$AI = P(C_{yes}) \prod P(attribute_i|C_{yes}) \quad (2.2)$$

where C_i is the response class which shows whether a reply was received for a RREQ that was sent, and $X = (X_1, \dots, X_N)$ the feature vector consisting of multiple attributes.

Thus, assuming every attribute is mutually independent[28]:

$$P(X|C_i) = \prod_{k=1}^n P(x_k|C_i) \quad (2.3)$$

$$AI = P(C_i) \prod_{k=1}^n P(x_k|C_i) \quad (2.4)$$

The EORP protocol yields better control overhead than traditional AODV once history is loaded into the primary memory of all the nodes. However, simulations of large scale MANETs exhibiting acute node failures have not been done [28]. Also, the protocol's performance is largely reliant on individual nodes and their behaviour, and not of routes in their entirety.

A Trust-based Scheme Against Packet Dropping Attacks in MANETs: In [29], a trust-based secure routing model is suggested in which the AODV protocol is adapted to carry out four mechanisms for effective routing, which include *Hello* control packet exchange, promiscuous node monitoring, a trust exchange mechanism, and the isolation of misbehaving nodes. This routing protocol isolates misbehaving nodes based on a trust threshold, and blacklists them from the rest of the network- allowing more reliable connections between source-destination pairs.

The trust-based routing protocol suggested in [29] yields better network performance than traditional AODV in terms of end-to-end delay, packet delivery and routing overhead. However, this protocol uses a weight-based trust system that provides a mechanism for node isolation which is aimed directly towards nodes that are malicious in their design, and not towards nodes that exhibit typical network failure characteristics. Future work for this protocol may include adding social trust parameters.

Flexible Weight Based Clustering Algorithm (FWCA): To manage the scalability of large scale MANETs, the Flexible Weight Based Clustering Algorithm (FWCA) [30] proposes the use of many different metrics to build clusters. These metrics include node degree, remaining battery life and node mobility. The goals are to yield a low number of overall clusters, to maintain cluster stability and to maximize the lifetime of the mobile nodes in the system by reducing large topologies to a more manageable equivalence.

Each node calculates its weight based on its degree, transmission power, battery life, and average speed. From [30], the weight of a node is calculated using the following steps:

1. Find the degree d_i of the node i by counting its neighbours.
2. Compute the degree difference $\delta_i = |d_i - N|$ for the node i , where N is a threshold for the cluster's size in terms of number of nodes.
3. Compute the remaining battery power E_i for the node i .
4. Compute the actual transmission power P_i for the node i .
5. Compute the average speed S_i for the node i until the current time T :

$$S_i = \frac{1}{T} \sum_{t=1}^T \sqrt{(X_t - X_{t-1})^2 + (Y_t - Y_{t-1})^2}$$

where (X_t, Y_t) are the coordinates of the node i at time t .

6. Calculate the weight W_i of node i :

$$W_i = a * \delta_i + b * E_i + c * P_i + d * S_i$$

where a , b , c , and d are weighted factors.

Further recommendations for the algorithm may include creating a threshold for the number of nodes that may form part of a cluster, re-election of cluster heads to better utilize the overall battery drainage and to successfully implement inter-cluster communication.

Research Problem: It is realistic to assume that in a practical scenario not all nodes would function as expected, and that the presence of selfish and/or dysfunctional nodes would be inevitable. Furthermore, since it is assumed that some MANETs engage hundreds to thousands of nodes over a large geographical span [31], it creates the research opportunity to explore the development/extension of the AODV routing protocol by virtue of the principles used in the EORP protocol [28], the FWCA algorithm [30], as well as the trust-based routing protocol suggested in [29], and to see how well these principles apply to large scale networks.

2.2 Research Aim and Objectives

Aim: The aim of the proposed research is to create a reliable route discovery protocol for large scale MANETs in the presence of selfish/dysfunctional nodes.

First Objective: The first research objective is to find a way to create a new protocol that uses AODV as a basis, and includes the following key functionalities:

1. The application of the Bayesian principles used by the EORP protocol with respect to routes.
2. The use of a trust-based framework similar to the protocol suggested [29], along with a sensible threshold mechanism for the isolation of nodes that appear to be too dysfunctional for the network.
3. The use of a clustering algorithm similar to that of [30] which serves as an extension to reduce large and complex topologies to more manageable ones.

Second Objective: The second research objective is to determine how well the new protocol functions in terms of desired functionality and design, which includes:

1. Determining how sensitive the new protocol is to a change in metric of network variables- such as node mobility, number of selfish nodes, and network scale.
2. Determining how well the concepts of Bayesian probability, trust-based isolation and clustering translates to large-scale networks under unique constraints.
3. Retrieving analytical data to compare to traditional routing algorithms which will help create sensible conclusions.

2.3 Research Tools and Methods

2.3.1 Simulation Software

Network Simulator 3 (NS3) is a discrete-event network simulator supporting C++ and Python as programming languages. Due to the software being well documented, open-source and capable of simulating the needed scenarios, it will be used to conduct the needed experiments within the scope of this dissertation.

2.3.2 Propagation and Mobility Models

Propagation Delay Model: The Constant Speed (CS) propagation delay model calculates the delay between a specified source and destination through the assumption of a constant propagation speed throughout the transmission medium.

Propagation Loss Model: The Range Propagation (RP) loss model determines path loss by a single attribute: range. Receivers within the specified range will receive transmission at the transmit power level, and receivers outside of the range will receive at a power level of -1000 dBm, which is effectively zero. The RP loss model provides a clean way of controlling the reach of each node in a geographical area without taking into account the effects of terrestrial objects, and is therefore perfect for simulating highly controlled scenarios.

Mobility Model: The Random Waypoint mobility model randomly selects a waypoint for each node along with a random speed within the bounds of specified parameters. After the node has reached its destination, it will pause for a specified amount of time after which the procedure will repeat itself. This mobility model is a novel way of simulating randomness within mobile ad hoc networks and to study the effects of mobility on routing protocols.

All three models discussed within this section will be used for the MANET simulations.

2.3.3 Evaluation Metrics

Packet Delivery Ratio: The ratio between number of packages originated by the application layer source and the number of packets received by the destination. The packet delivery ratio is denoted by PDR as follows:

$$PDR = \frac{\sum Total\ Packets\ Received}{\sum Total\ Packets\ Sent} * 100 \quad (2.5)$$

Average End-to-End Delay: The delay in packet delivery between the source and the destination. This delay includes buffer queues, transmission time, and delays caused through routing activities. The average delay between a source/destination pair is denoted by D as follows:

$$D = \frac{\sum Total\ Delay\ of\ Packets}{\sum Total\ Number\ of\ Packets} \quad (2.6)$$

Throughput: The average measure of bits per second between a source and a destination. The throughput is expressed as a percentage and denoted by P as follows:

$$P = \frac{\sum Total\ Bits\ Received}{\sum Total\ Transmission\ Time} \quad (2.7)$$

Successful Connections: The ratio of successfully created connections in relation to the desired number of connections, expressed as a percentage and denoted by C as follows:

$$C = \frac{\sum Successful\ Connections}{\sum Desired\ Connections} \quad (2.8)$$

2.4 Notation and Assumptions

Normal nodes model perfectly working nodes without any type of malicious or dysfunctional behaviour to the network. Sink, source and intermediate nodes fall under the category of normal nodes within the context of this text and are depicted as red, green and blue respectively. This is graphically depicted by Figure 2.1.

Selfish nodes are nodes that attempt to disrupt network activity by randomly dropping packets during communication. The types of packets that are dropped include both control packets and data packets. To implement this behaviour, a *drop probability* value is chosen as a percentage and assigned to an individual node. This value serves as an indication of the probability that the node will drop a data or control packet upon receiving it. A random value between 0 and 100 is generated during runtime and if the generated value is less than the *drop probability*, the received packet will be dropped.

The following *assumptions* remain constant for the remainder of the paper:

1. From [32], a “dense network” is defined as a network that consists of 50 nodes over an area of 1000m by 1000m. Similarly, [33] defines a “large scale” network as a network consisting of 60 nodes over an area of 1500m by 1500m. This proves that the term “large scale network” is arbitrary, and not well established. However, for the purpose of this dissertation a large scale network is defined as a network consisting of at least 250 nodes over an area of 1000m by 1000m.
2. An “ad hoc network” is defined as a network of nodes that are arbitrarily placed and exhibit mobility (0m/s to 25m/s) in certain scenarios. These nodes model perfectly working nodes (source, sink and intermediate nodes) as well as selfish nodes. Effects such as battery life, specific network topologies, and attempting to model vehicular or other movement patterns are not considered.

3. Each node can explicitly recognize when it has received, as well as dropped a packet.
4. There are no deteriorating effects in terms of propagation through different mediums and/or terrestrial objects.
5. In the comparison of two or more protocols, all simulations are run parallel with respect to each other. This means that for each iteration of a protocol simulation, the exact same scenario will be simulated using the same seed as the opposing simulation. Multiple iterations will be run for each simulation to achieve convergence.

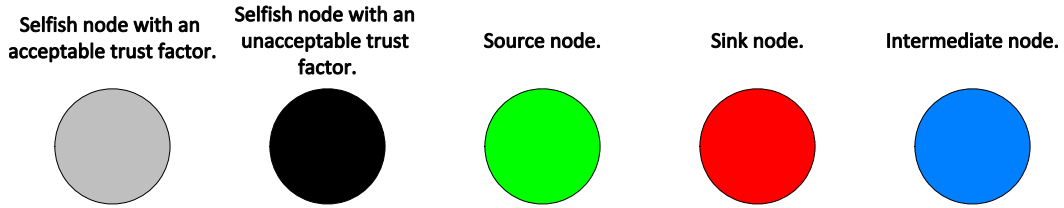


Figure 2.1: Node notation color scheme.

2.5 Research Procedure

A simulation-based study will be conducted using the NS3 simulation software. The proposed protocol will be subjected to two different types of simulations, of which both types have *static* and *mobile* node scenarios.

Mobile and Static Scenarios: Figure 2.2 and 2.3 provide a graphical overview (obtained from NS3) of stationary and mobile scenarios, respectively.

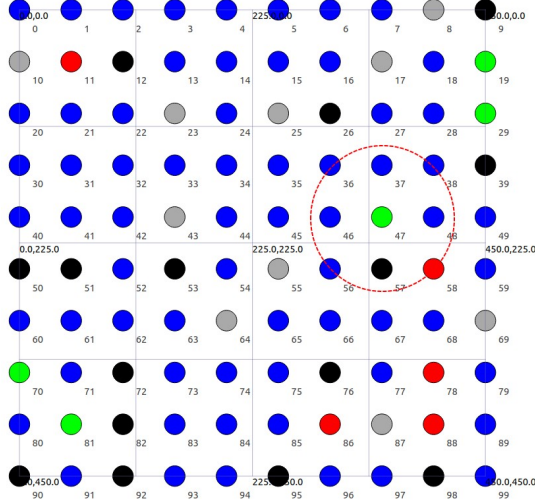


Figure 2.2: Stationary scenario.

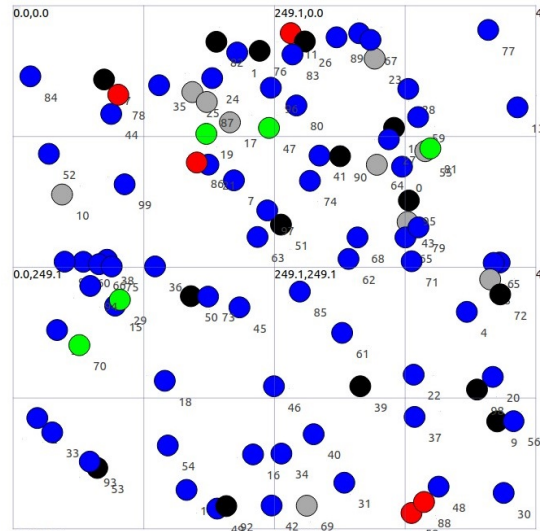


Figure 2.3: Mobile scenario.

Variable Transmission Range Configuration: To study the effect of increased hop count between source/sink node pairs, the chosen transmission range is explicitly selected such that each node will have the ability to reach a neighbouring node diagonally across from it if all nodes were equally spaced within the geographical area of simulation—regardless of network size. This is depicted in Figure 2.4 by the dashed red circle.

Fixed Transmission Range Configuration: In these types of simulations the transmission range remains fixed regardless of network size, and is depicted in Figure 2.5 by the dashed red circle. The goal of these simulations are to study the effects of increased node density.

Analytical data in terms of end-to-end delay, throughput, successful connections and packet delivery ratio will be retrieved and logged from each simulation. This data will be compared to traditional and/or opposing routing protocols under the same constraints and logical conclusions will be made.

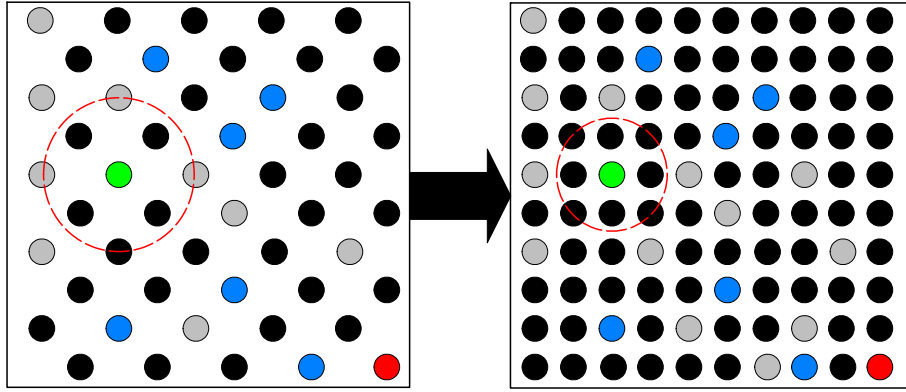


Figure 2.4: Variable transmission range; increased hop count.

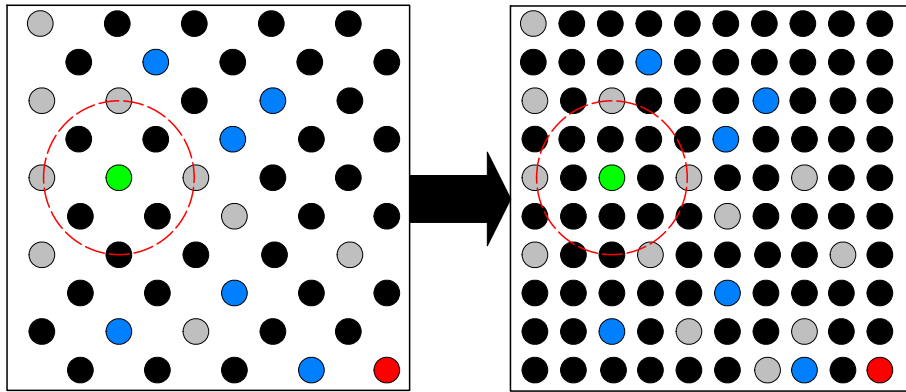


Figure 2.5: Fixed transmission range; increased node density.

2.6 Summary

From the content of this chapter, it is clear that the research objectives are aimed at combining the Bayesian principles of the EORP protocol [42], the node-isolation techniques of the trust-based AODV algorithm as described in [52], and the algorithmic clustering approach of [43] in an attempt to create a Bayesian-based reliable route discovery protocol with a clustering overlay for large scale MANETs exhibiting node failures.

A simulation-based study will be conducted using simulation software capable of handling large scale MANETs and will be used to determine the performance metrics of the proposed protocol(s) with respect to existing protocols, such as AODV.

Chapter 3

Ad Hoc On-Demand Distance Vector Routing

This chapter explores a brief “under the hood” look at the Ad hoc On-Demand Distance Vector (AODV) routing protocol and also covers a section where the AODV protocol is subjected to performance evaluation with different scenarios and specific constraints.

3.1 Operation

AODV [5] adopts conventional routing tables to store routing information between the source and destination nodes. During the route discovery process Route Request (RREQ) packets are sent symmetrically throughout the network until a destination is reached. Each RREQ control packet exhibits a unique identification code, which nodes use to determine if the packet needs to be discarded for loop avoidance or in case of a duplicate.

Route Reply (RREP) packets are sent back along the reversed path from the destination to the source, after which the most optimal route is selected based on hop count. A route timer is associated with each entry, which allows the AODV protocol to remove unused routes after a chosen amount of time. Once a link-breakage between the source-sink pair has occurred, a Route Error (RERR) packet will propagate to the source and reinitiate the route discovery process. The general process of RREQ and RREP packet propagation in AODV is depicted in Figure 3.1.

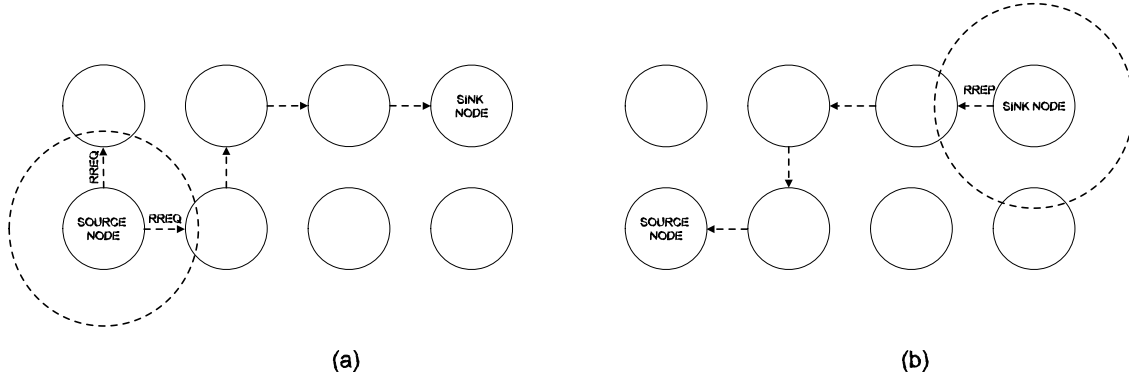


Figure 3.1: AODV RREQ packet propagation (a) and RREP packet propagation (b).

3.2 Performance Evaluation

To study the effects of *increased hop count* between source/sink node pairs, the AODV protocol is simulated under both **static** and **mobile** scenarios with the transmission range of each node chosen explicitly such that it would theoretically reach a neighbouring node placed diagonally from it on a fixed grid distribution. This ensures that an increase in network size would result in an increase in number of hops between source/sink node pairs¹.

To study the effects of *increased node density*, the AODV protocol is once again simulated under both **static** and **mobile** scenarios with the transmission range of each node fixed at 250m regardless of the network size. This ensures an increase in node density between source/sink node pairs as the network size increases².

Scenario 1; Static: In the first simulation scenario, the AODV protocol is exposed to a change in network size along with an increase in the number of selfish nodes, as shown by the simulation parameters in Table 3.1 and Table 3.2. A fixed grid distribution of 100 nodes up to 400 nodes over an area of 1000m by 1000m is simulated along with an increase in the number of selfish nodes. This increase in selfish nodes is from 0% to 70% of the total amount of nodes in the network in intervals of 10%. The data drop probability of each individual node is randomly selected between 0% and 100%.

Scenario 2; Mobile: In the second simulation scenario, the AODV protocol is exposed to the exact same simulation parameters as **Scenario 1**, with the exception of assigning a random node velocity between 0 m/s – 25 m/s to each individual node and randomly distributing the nodes within the simulation area.

The results of these simulations are depicted in tabular format by Table A.1 and Table A.2, and graphically by Figure 3.2 to Figure 3.5.

¹Chapter 2; Figure 2.4

²Chapter 2; Figure 2.5

Table 3.1: AODV simulation parameters; constant

Parameter	Value
Simulation Area	1000m by 1000m
Simulation Time	Start: 0s; End: 100s
No. of Nodes	100; 200; 300; 400
No. of Sink/Source Node Pairs	10; 20; 30; 40
No. of Selfish Nodes	0% to 70% of total nodes in intervals of 10%
Selfish Node Drop Probability	0 to 100 %
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Routing Protocol	Ad hoc On-Demand Distance Vector (AODV)
Traffic Type	Constant Bitrate (CBR)
Transport Protocol	User Datagram Protocol (UDP)
Application Throughput	2048 bp/s
Bandwidth	2 Mbp/s
Packet Size	128 bytes
Hello Enabled; Hello Interval;	No; 0 s

Table 3.2: AODV simulation parameters; variable

Parameter	Value	
Node Distribution Node Speed Mobility Model Transmission Range	Variable Transmission Range	
	Scenario 1: Fixed Grid	Scenario 2: Mobile
	Fixed Grid	Random
	0 m/s	0 m/s to 25 m/s
	None	Random Waypoint Mobility Model
Node Distribution Node Speed Mobility Model Transmission Range	Fixed Transmission Range	
	Scenario 1: Fixed Grid	Scenario 2: Mobile
	Fixed Grid	Random
	0 m/s	0 m/s to 25 m/s
	None	Random Waypoint Mobility Model
Transmission Range	145m; 100m; 85m; 75m	145m; 100m; 85m; 75m
	250m	250m

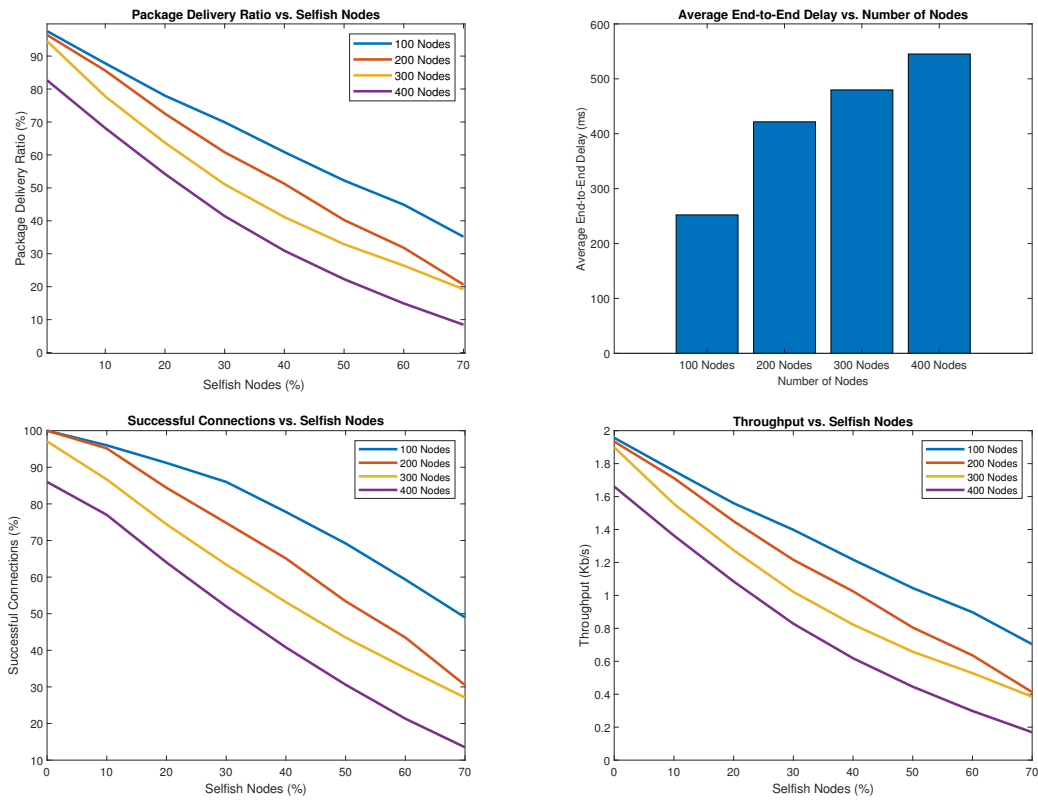


Figure 3.2: AODV simulation results; variable transmission range; static.

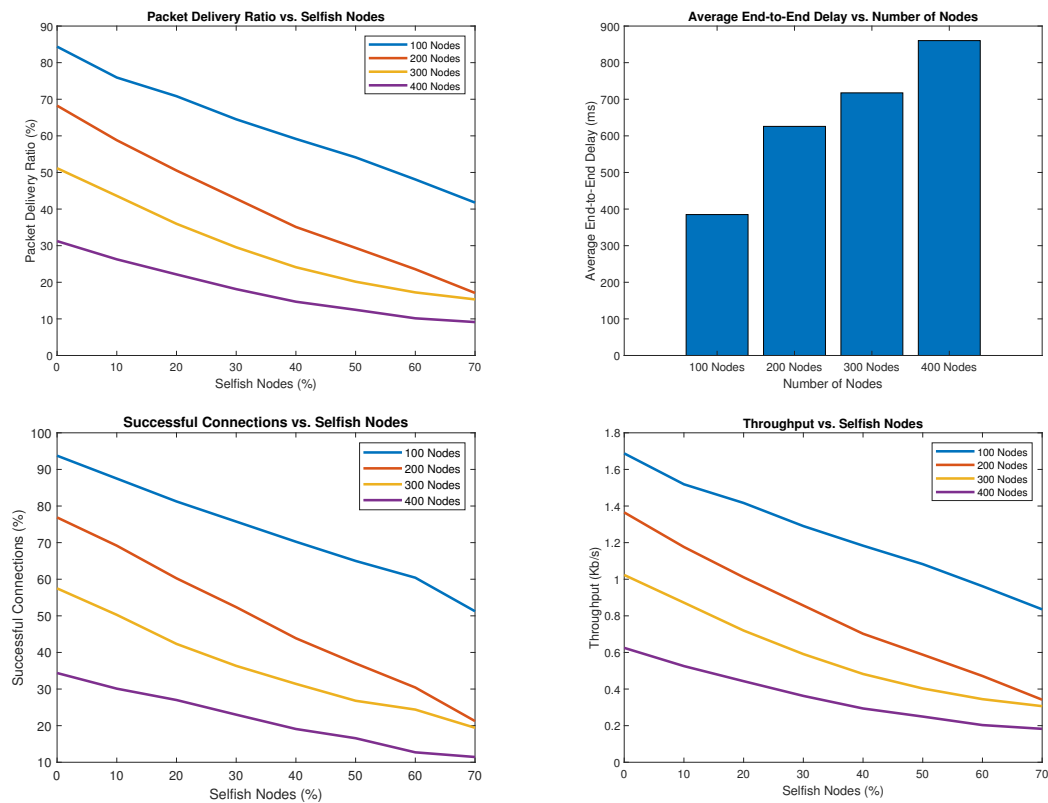


Figure 3.3: AODV simulation results; variable transmission range; mobile.

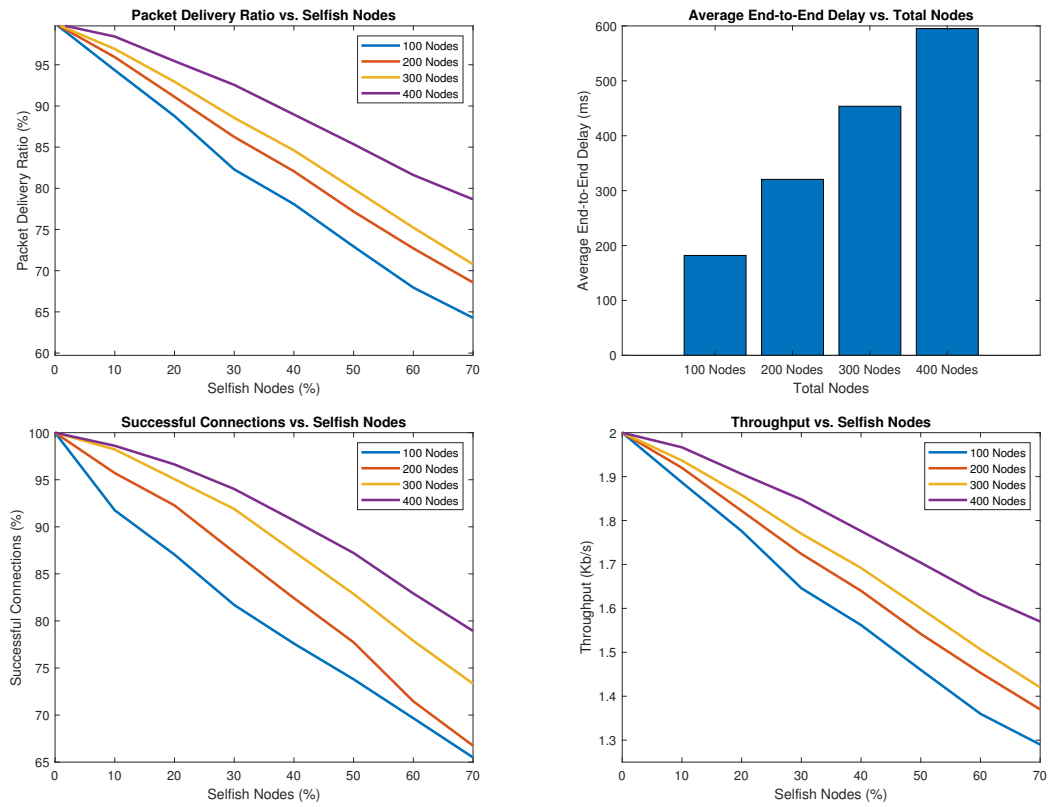


Figure 3.4: AODV simulation results; fixed transmission range; static.

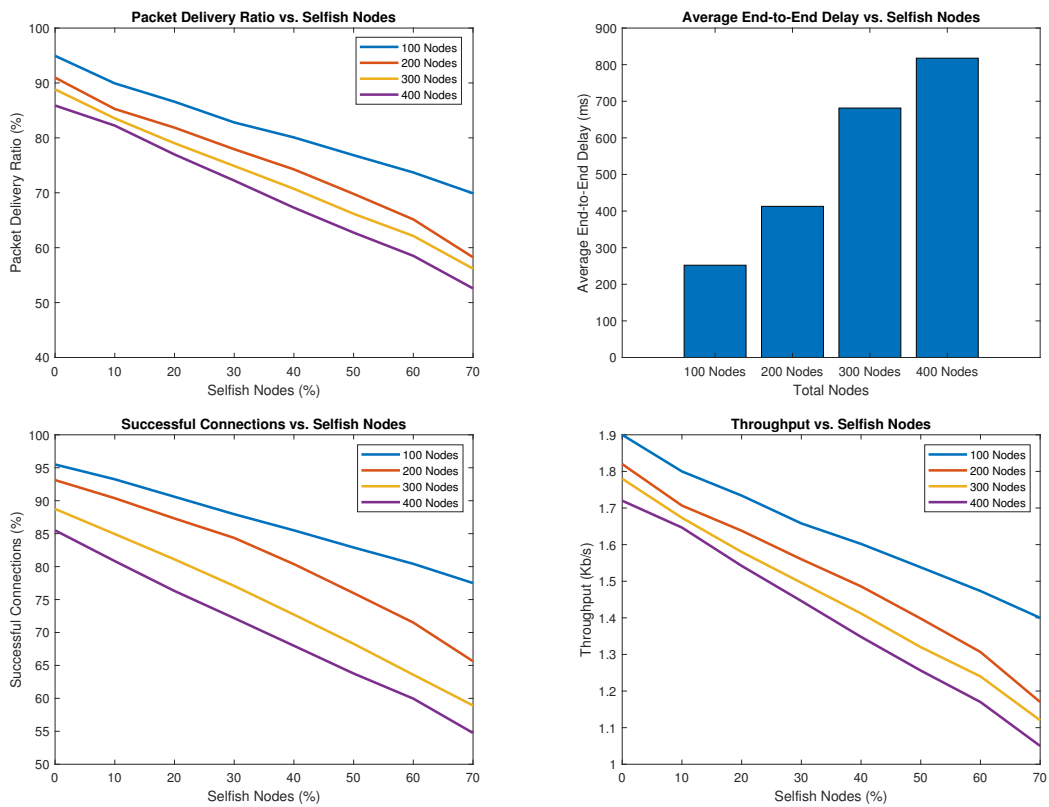


Figure 3.5: AODV simulation results; fixed transmission range; mobile.

3.3 Summary

3.3.1 Performance Analysis

We highlight the following insights with regards to the simulation results obtained for the AODV protocol and the respective evaluation metrics:

Packet Delivery Ratio: The packet delivery ratio sees an increase in deterioration as the number of selfish nodes increase for both fixed transmission range and variable transmission range configurations. However, it is evident that an increase in hop count, selfish nodes, and node mobility have the greatest effect on packet delivery within all scenarios. Under a fixed transmission range configuration with a static grid topology, larger network sizes prevail over smaller network sizes. This is due to the fact that a greater number of alternative routes exist once selfish nodes are introduced, and once the connections between source/sink node pairs have been formed, they remain throughout the remainder of the simulation.

Average End-to-End Delay: The average end-to-end increases in all simulation configurations as the network size increases. The largest overall average end-to-end delay is found in a large network with a random distribution of mobile nodes at a high node density. The lowest overall average end-to-end delay is seen in a small network, with a low node density and a static grid topology. This concludes that the most prominent variables that affect average end-to-end delay are node density due to the aggressive RREQ flooding technique used by AODV, and node mobility which leads to constant link breakages.

Successful Connections: With a fixed grid distribution of nodes and a fixed transmission range, larger network sizes with higher node densities seem to maintain a higher number of successful connections. This is in correlation with the analysis of packet delivery ratio under the same circumstances. The variables responsible for the most deterioration are notably an increase in selfish nodes, an increase in hop count, and node mobility.

Throughput: Since the application throughput is merely $2Kbps$ and the bandwidth is $2Mbps$, congestion is highly unlikely within the network. This leads to the throughput being in direct correlation with the packet delivery ratio and respectively sees the most deterioration under an increase in selfish nodes, higher hop count, and node mobility¹.

¹A larger packet size would inadvertently affect packet delivery ratio, average end-to-end delay and throughput negatively on larger networks.

3.3.2 Final Remarks

When no selfish nodes are present, the greatest impact on overall network performance is network size and node mobility. An increase in network size yields an increase in network performance for static grid topologies with the absence of selfish nodes. However, once mobility is introduced, an increase in network size has a deteriorating effect on network performance due to constant link breakages. These conclusions are similar to other studies [34, 35] who have also evaluated the performance of the AODV protocol with the absence of selfish nodes. The foremost difference between these studies and this dissertation is the focus point of evaluation, which is the effect of selfish nodes on network performance in large scale networks. The propagation model, area of simulation, and total number of nodes have been tailored specifically to accommodate this focus point. Even though the results obtained from this chapter are not directly benchmarked to those obtained in [34, 35], the correlation and similar network performance with regards to a change in metric yields similar conclusions, furthermore proving that the simulation configurations are dependable and function as expected.

Once selfish nodes are introduced network performance declines accordingly, and once the number of selfish nodes are increased we see that there is an even greater decline in network performance which is directly related to this increase. It is clear that the AODV protocol, conclusively- does not function well in the presence of selfish/dysfunctional nodes. When taking into account the effects of mobility, increased hop count, and increased node density, we get a clear picture of many areas of the protocol that need improvement. A practical ad hoc network could have of a large network scale, with a randomly distributed network structure and a number of degrading effects. Thus, the need for a more robust protocol tailored specifically for these conditions is evident.

Chapter 4

Naïve Bayes Classifier Routing

This section presents an experimental adaptation of the AODV protocol, called Naïve Bayes Classifier Routing (NBCR). A probability framework based on Bayes' Theorem [27] is used to determine the most reliable path in a network exhibiting many different features and constraints.

4.1 Protocol Design

4.1.1 Implementation

Step 1; Classifier Definition: Bayes' Theorem finds the probability of an event given the posterior probability of another event that has already occurred [27], and is mathematically represented as

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \quad (4.1)$$

1. A and B are separate events.
2. $P(A)$ is the prior probability of event A.
3. $P(B)$ is the prior probability of event B.
4. $P(A|B)$ is the probability of event A given that event B is true.
5. $P(B|A)$ is the probability of event B given that event A is true.

Naïve Bayes classifiers are simple probabilistic classifiers that are based on applying Bayes' theorem with the assumption of independence between classifier variables [27]. In the scope of this dissertation, the application of a classifier will be used to determine the probability of achieving a desired packet delivery ratio given posterior evidence based on independent variables and outcomes from training data.

The general goal of a Naïve Bayes Classifier is to calculate the conditional probability $P(y = C_k | x_1, x_2, \dots, x_n)$ for each K possible outcomes of the response vector with the classes C_k and data vector $X = x_1, x_2, \dots, x_n$ with n features. In accordance to Bayes' Theorem, equation (4.1) is then rewritten as

$$P(Y|X) = \frac{P(X|Y)P(Y)}{P(X)} \quad (4.2)$$

And therefore, substitution of equation (4.6) and (4.7) into equation (4.2) yields

$$P(y|x_1, \dots, x_n) = \frac{P(x_1|y)P(x_2|y) \dots P(x_n|y)P(y)}{P(x_1)P(x_2) \dots P(x_n)} \quad (4.3)$$

where

$$P(x_n|y) = \prod_{i=1}^n P(x_i|y) \quad (4.4)$$

Since the denominator stays consistent for each data entry, it can be removed and a proportionality is introduced:

$$P(y|x_1, x_2, \dots, x_n) \propto P(y) \prod_{i=1}^n P(x_i|y) \quad (4.5)$$

Step 2; Obtaining Training Data: To obtain the training data needed to implement a Naïve Bayes classifier, we first need to define our *feature vector* and *response vector*. The feature vector X consists of the features represented in the dataset which are assumed to have the largest influence on network performance, namely “Hop Count” and “Route Trust”¹. The response vector Y consists of the class variable “Packet Delivery Ratio”, which is a good indication of overall network performance.

$$X = (\text{Hop Count}, \text{Route Trust}) = (x_1, x_2) \quad (4.6)$$

$$Y = (\text{Packet Delivery Ratio}) = y \quad (4.7)$$

¹The concepts of *node trust* and *route trust* are discussed in Subsection 4.1.2

We conduct simulations for AODV with a configuration similar to that of Table 3.1 and 3.2, with the exception of only simulating a network with a size of 400 nodes and a variable transmission range configuration with added node mobility. This ensures that some connections have a large hop count between source/sink node pairs. The number of selfish nodes account for 50% of all nodes and have a drop probability between 0 to 100% which is randomly assigned. From each source/sink connection the amount of hops, route trust, and packet delivery ratio is monitored. The resulting data set obtained is depicted in Table 4.1.

Table 4.1: NBCR training data.

Data Entry (i)	Hop Count (x_1)	Route Trust (x_2)	Packet Delivery Ratio (y)
1	5	0.2242	0.2860
2	11	0.1245	0.1250
3	2	1.0000	1.0000
4	3	1.0000	1.0000
5	13	0.3296	0.3330
6	2	0.5700	0.5000
7	4	0.9600	0.5000
...	...	...	...
4864			

Step 3; Classifier Implementation: To reduce the amount of data needed for accurate predictions, each feature in both feature and response vectors are divided into 10 distinct categories denoted by k using equations (4.8) - (4.10). This results in a categorised data set as depicted by Table 4.2.

$$x_1 = \begin{cases} k = x_1, & x_1 < 10 \\ k = 10, & x_1 \geq 10 \end{cases} \quad (4.8)$$

$$x_2 = \left\{ k, \frac{k}{10} - 0.1 < x_2 \leq \frac{k}{10} \right\} \quad ; \quad k = 1, 2, 3 \dots 10 \quad (4.9)$$

$$y = \begin{cases} C_k = 0, & y < \text{Desired}_{PDR} \\ C_k = 1, & y \geq \text{Desired}_{PDR} \end{cases} \quad (4.10)$$

To further account for the problem of zero probability which occurs when a categorical variable is not observed in the dataset, Laplace Smoothing [27] is used. The elements of

equation (4.4) and (4.5) then reduce to their respective estimates:

$$P(x_n = k|y = C_k) = \frac{x_{ntotal} + \alpha}{N + \alpha A} \quad (4.11)$$

$$P(y = C_k) = \frac{y_{total} + \alpha}{N + \alpha B} \quad (4.12)$$

where B denotes the number of different categories in y , A the number of different categories in x_n , N the total number of data entries, and we choose our smoothing parameter α as 1. The value x_{ntotal} represents the total number of cases where $x_n = k$ for $y = C_k$, and the value of y_{total} represents the total number of cases where $y = C_k$.

Since we have 10 categories for our feature vector elements x_1 and x_2 , two possible categorical outcomes for our response vector element y , and a total number of 4864 data entries- the values of A , B and N are respectively 10, 2, and 4864. Therefore, substitution of (4.11) and (4.12) into (4.4) and (4.5) yields:

$$P(x_n = k|y = C_k) = \frac{x_{total} + 1}{4864 + 10} \quad (4.13)$$

$$P(y = C_k) = \frac{y_{total} + 1}{4864 + 2} \quad (4.14)$$

$$P(y = C_k|x_1 = k_1, x_2 = k_2) = \left(\frac{x_{1total} + 1}{4864 + 10} \right) \left(\frac{x_{2total} + 1}{4864 + 10} \right) \left(\frac{y_{total} + 1}{4864 + 2} \right) \quad (4.15)$$

where x_{1total} and x_{2total} respectively represent the total number of cases where $x_1 = k_1$ and $x_2 = k_2$ for $y = C_k$.

Table 4.2: NBCR training data; categorised.

Data Entry (i)	Hop Count (x_1)	Route Trust (x_2)	Packet Delivery Ratio (y)
1	5	3	0
2	10	2	0
3	2	10	1
4	3	10	1
5	10	4	0
6	2	6	1
7	4	10	1
...	...	...	...
4864			

Example: The probability of having more than 50% packet delivery ratio with a route trust factor of 0.7814 and a hop count of 3 would be calculated using the following steps:

1. Convert the input data vector from $(x_1 = 3, x_2 = 0.7814)$ to $(x_1 = 3, x_2 = 8)$ using equations (4.8) to (4.10).
2. Convert the training data to correspond with all 10 distinct categories using equations (4.8) to (4.10) by virtue of a desired packet delivery ratio of 50%, as depicted by Table 4.2:
3. Determine $P(x_1 = 3 \mid y = 1)$, $P(x_1 = 3 \mid y = 0)$, $P(x_2 = 8 \mid y = 1)$, and $P(x_2 = 8 \mid y = 0)$ using equations (4.13) and (4.14):

$$P(x_1 = 3 \mid y = 1) = \left(\frac{483 + 1}{4864 + 10} \right); P(x_2 = 8 \mid y = 1) = \left(\frac{192 + 1}{4864 + 10} \right)$$

$$P(x_1 = 3 \mid y = 0) = \left(\frac{308 + 1}{4864 + 10} \right); P(x_2 = 8 \mid y = 0) = \left(\frac{21 + 1}{4864 + 10} \right)$$

4. Compute $P(y = 1 \mid x_1 = 3, x_2 = 8)$ and $P(y = 0 \mid x_1 = 3, x_2 = 8)$ using equation (4.15).

$$P(y = 1 \mid x_1 = 3, x_2 = 8) = \left(\frac{2226 + 1}{4864 + 2} \right) \left(\frac{483 + 1}{4864 + 10} \right) \left(\frac{192 + 1}{4864 + 10} \right) \approx 0.0018$$

$$P(y = 0 \mid x_1 = 3, x_2 = 8) = \left(\frac{2638 + 1}{4864 + 2} \right) \left(\frac{308 + 1}{4864 + 10} \right) \left(\frac{21 + 1}{4864 + 10} \right) \approx 0.00015$$

5. To acquire the probability expressed as a percentage, the relationship between $P(y = 1 \mid x_1, \dots, x_n)$ and $P(y = 0 \mid x_1, \dots, x_n)$, and the fact that there are only two possible categorical outcomes for the response vector, is exploited:

$$P(y = 1 \mid x_1, x_2) = \frac{P(y = 1 \mid x_1, x_2)}{P(y = 1 \mid x_1, x_2) + P(y = 0 \mid x_1, x_2)} * 100\% \quad (4.16)$$

$$P(y = 1 \mid x_1 = 3, x_2 = 8) \approx 0.0018 * 100 * \left(\frac{1}{0.0018 + 0.00015} \right) \approx 92.31\%$$

Therefore, the expected posterior probability of obtaining more than 50% packet delivery ratio with a hop count of 3 hops and a route trust factor of 0.7814 is roughly 92.31%.

4.1.2 Protocol Operation

Step 1; Route Discovery and Node Isolation: One of the pillars of the correct operation of the NBCR protocol is the classification and calculation of trust factors. The NBCR protocol categorises trust factors into two different categories: *node trust factors* and *route trust factors*. The trust factor of a node $Trust_{node}$ is simply a ratio of the number of dropped packets to the total number of observed packets at the node. This means that each node in the network has a trust value with respect to its own performance that is calculated using equation (4.17) each time a new packet is received. This calculation is done throughout the entire duration of the simulation and will become more similar to the defined drop probability of the node as more data samples are presented.

$$Trust_{node} = \frac{\sum Dropped\ Packets}{\sum Total\ Packets} \quad (4.17)$$

It is assumed that initially every node is fully trusted, thus having a trust value of 1. It is also assumed that each node has the ability to recognize when it has received and/or dropped a data or control packet.

When a source node (green) attempts to create a connection with a sink node (red), it will broadcast a RREQ control packet to neighbouring nodes within range. This packet would then traditionally flood through the network, passing the packet from neighbour to neighbour until the destination is reached. This process is similar to that of normal AODV, with one exception- each node will have the ability to decide whether to forward the RREQ packet based on its own observed trust value. If the the node has a trust value below a preselected *trust threshold*, it will not forward the RREQ packet, thus eliminating itself as a possible candidate for a working route to the destination.

Assuming that all the black selfish nodes depicted in Figure 4.2 have a node trust value below the allowed trust threshold of 0.5, the RREQ packet would only be allowed to propagate through intermediate and selfish nodes (grey) with an acceptable trust factor, as depicted. This reduces the scope of control packet propagation through the network and eliminates extremely dysfunctional nodes. The procedure of RREQ forwarding is also graphically shown in flow-chart format in Figure 4.1.

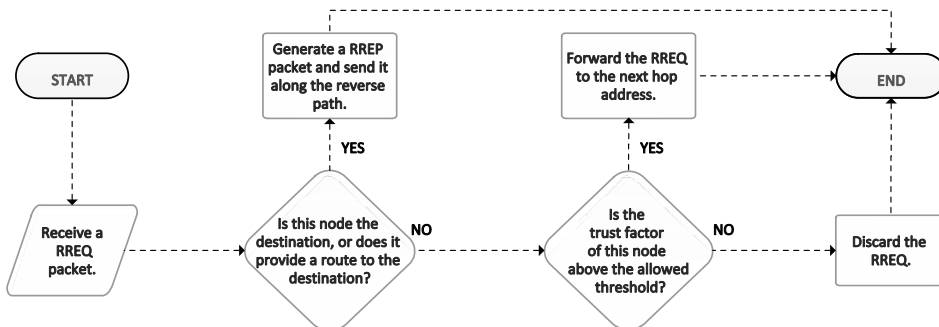


Figure 4.1: NBCR RREQ packet handling flowchart.

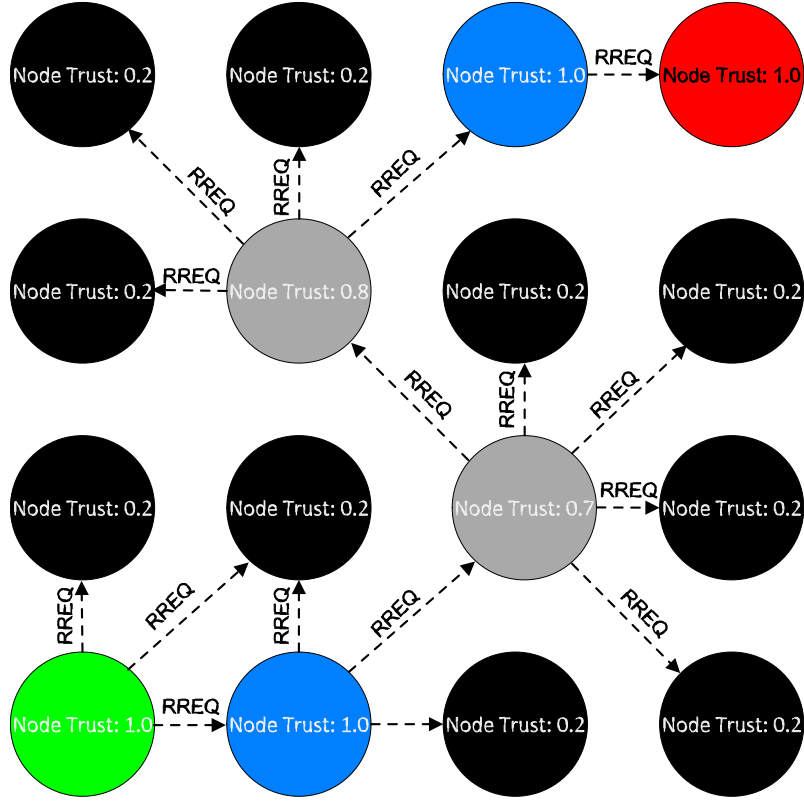


Figure 4.2: Illustration of NBCR RREQ packet propagation.

Step 2; Route Selection: Once the RREQ packet reaches its destination, a reverse path is created and a modified RREP packet is sent along the reverse path, as depicted in Figure 4.3. This RREP is similar in nature to that of an AODV RREP, with the exception of having an additional field for the accumulated trust value of the discovered route, as shown in Table 4.3.

Each node along the reverse path receives the modified RREP, reads the *Route Trust* field from the header of the packet, and modifies the value $Trust_{route}$ according to the node's own trust value $Trust_{node}$. This information is stored in each node's *Trust Table*, as shown in Table 4.4. The new accumulated trust $Trust_{route}$ is simply the product of multiplication between the old accumulated trust $Trust_{old}$ as read directly from the packet header and the receiving node's trust value $Trust_{node}$:

$$Trust_{route} = Trust_{old} * Trust_{node} \quad (4.18)$$

Just like traditional AODV makes use of routing tables to determine the best route for data propagation, NBCR makes use of an additional *Trust Table* which stores information about previous routes, as previously depicted. Routes are then selected based on a posterior probability of delivering the desired packet delivery ratio, as depicted in flowchart format in Figure 4.4.

Table 4.3: NBCR RREP packet format.

Field	Description
R	Repair flag; used for multicast.
A	Acknowledgment required.
Reserved	Sent as 0.
Prefix Size	Specifies that the indicated next hop may be used for any nodes with same routing prefix.
Hop Count	The number of hops from the Originator IP Address to the Destination IP Address.
Destination IP Address	The IP address of the destination for which a route is supplied.
Destination Sequence Number	The destination sequence number associated to the route.
Originator IP Address	The IP address of the node which originated the RREQ for which the route is supplied.
Lifetime	The time in milliseconds for which nodes receiving the RREP consider the route to be valid.
Route Trust ($Trust_{route}$)	Accumulated trust factor of the route through multiplication.

Table 4.4: NBCR *Trust Table* format.

Destination	Gateway	Interface	Route Trust	Hop Count	Probability	Timestamp
Destination address.	Gateway address.	Interface address.	Route trust factor.	Route hop count.	Route probability.	Timestamp of route.
...	...	...	...	...	...	...

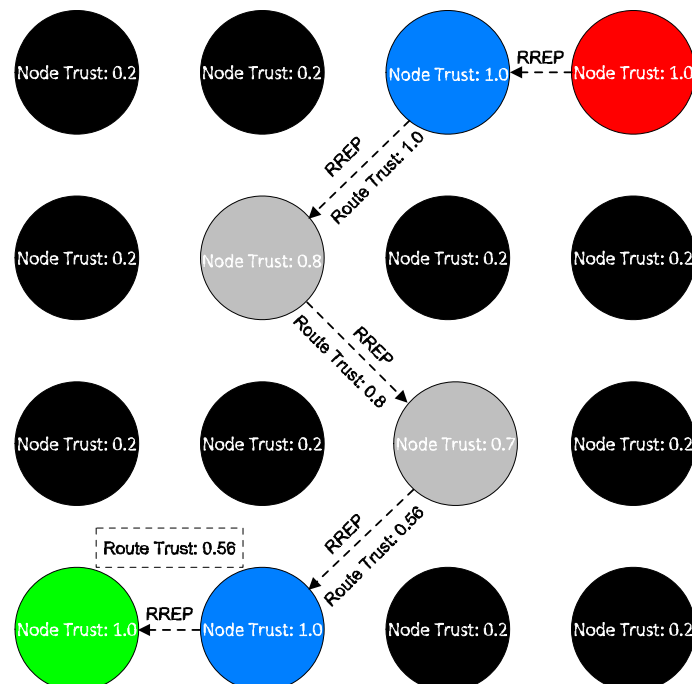


Figure 4.3: Illustration of NBCR RREP packet propagation.

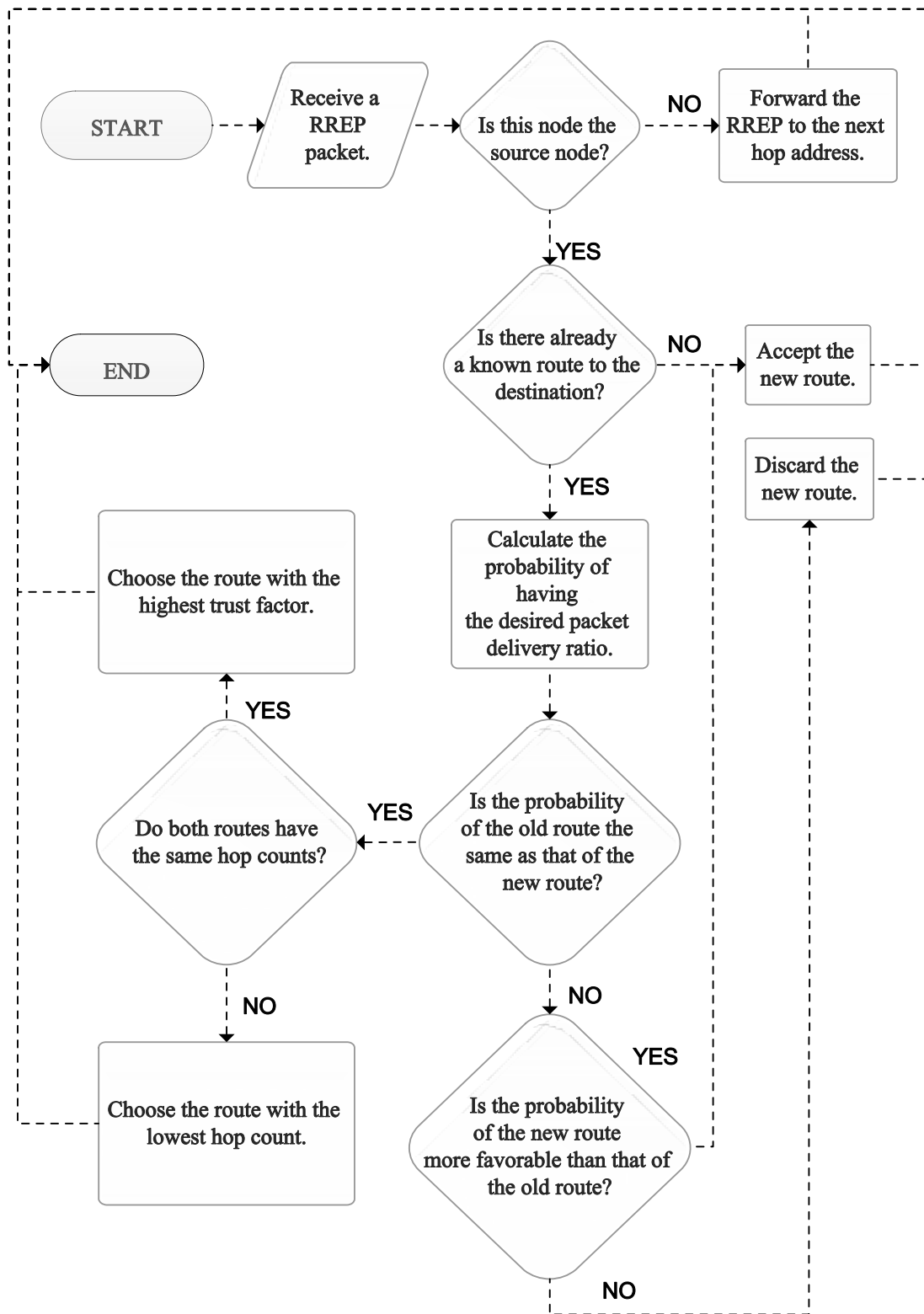


Figure 4.4: NBCR RREP packet handling flowchart.

4.2 Operational Evaluation

4.2.1 Classifier Sensitivity

To find the relationship between feature vector variables, and to determine if they are indeed independent from each other, a sweep across all 10 categories of each pair of variables in the feature vector is done with respect to each other- with the assumption that the desired packet delivery ratio is above 50 %. From the data depicted in Table 4.4, it is evident that each column contains a categorical value for the feature vector variable “Hop Count” and each row contains a categorical value for the feature vector variable “Route Trust”. Where these rows and columns intersect they represent the probability of obtaining more than 50% packet delivery ratio, expressed as a percentage.

Since it is assumed that all sink and source nodes model perfectly functional nodes, and that a single hop between these nodes would mean that there is zero possibility for any dysfunctional/selfish nodes along the route of the connection- this entry is not of interest and therefore not subjected to scrutiny. The distinction between classifier variables is depicted in Figure 4.5 and shows that an increase in the hop count category results in an overall reduction in the probability value of achieving the desired packet delivery ratio, which makes logically sense since an increase in hop count results in more variation between the random number of packets that will be dropped by selfish nodes.

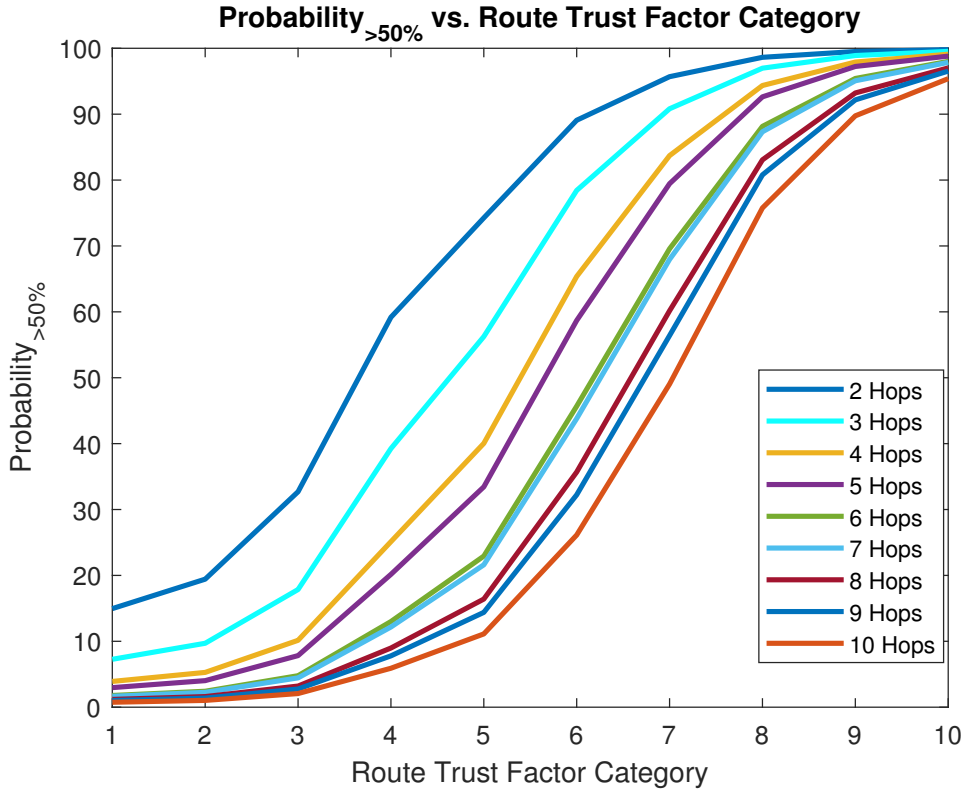


Figure 4.5: NBCR classifier sensitivity test between feature vector variables.

Table 4.5: NBCR classifier sensitivity test results.

x_1	x_2									
	1	2	3	4	5	6	7	8	9	10
1	94.68	96.06	98.01	99.32	99.66	99.88	99.96	99.99	99.99	99.99
2	14.96	19.43	32.70	59.18	74.26	89.08	95.69	98.63	99.51	99.79
3	7.27	9.70	17.86	39.25	56.25	78.43	90.82	96.98	98.90	99.53
4	3.91	5.28	10.15	25.12	40.04	65.37	83.71	94.35	97.91	99.10
5	2.97	4.03	7.83	20.16	33.44	58.69	79.45	92.63	97.24	98.81
6	1.78	2.42	4.78	13.00	22.93	45.68	69.57	88.15	95.42	98.01
7	1.65	2.25	4.45	12.17	21.61	43.80	67.96	87.33	95.07	97.86
8	1.18	1.61	3.21	8.98	16.41	35.69	60.16	83.07	93.22	97.02
9	1.01	1.38	2.76	7.79	14.39	32.23	56.40	80.79	92.17	96.54
10	0.75	1.03	2.07	5.91	11.12	26.13	49.04	75.77	89.75	95.39

4.2.2 Routing

Routing Test 1; Dropping RREQ Packets: For the correct operation of the NBCR protocol, it is imperative that selfish nodes that have a trust factor below the allowed trust threshold drop all RREQ control packets in order to eliminate themselves from the active network. To see if the NBCR protocol does indeed demonstrate this behaviour, a simulation with the parameters as displayed in Table 4.5 is done. All selfish nodes have a fixed drop probability of 80%, and therefore only one possible route exists, as depicted by Figure 4.6. The routing tables of interest are shown in Table 4.7, with the respective *Trust Table* shown in Table 4.8.

Table 4.6: NBCR simulation parameters; Test 1

Parameter	Value
Simulation Area	100m by 100m
Simulation Time	Start: 0s; End: 100s
No. of Nodes	16
No. of Sink/Source Node Pairs	1
No. of Selfish Nodes	10
Selfish Node Drop Probability	80%
Node Distribution	Fixed Grid; 25m Spacing
Mobility Model; Node Speed	None; 0 m/s
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Transmission Range	30m
Routing Protocol	Naïve Bayes Classifier Routing (NBCR)
Traffic Type	Constant Bitrate (CBR)
Transport Protocol	User Datagram Protocol (UDP)
Application Throughput	2048 bp/s
Bandwidth	2 Mbp/s
Packet Size	128 bytes
Hello Enabled; Hello Interval	No; 0 s

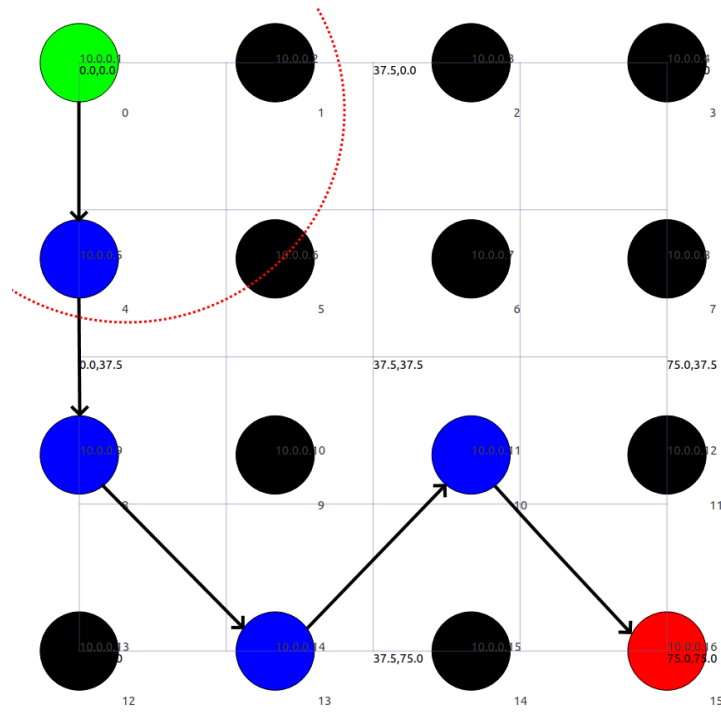


Figure 4.6: Graphical representation; Test 1.

Table 4.7: Routing Table; Test 1

Node IP	Destination	Gateway	Interface	Flag	Expire	Hops
10.0.0.1	10.0.0.5	10.0.0.5	10.0.0.1	UP	2.74	1
	10.0.0.16	10.0.0.5	10.0.0.1	UP	2.74	5
10.0.0.5	10.0.0.1	10.0.0.1	10.0.0.5	UP	2.74	1
	10.0.0.10	10.0.0.10	10.0.0.5	UP	2.74	1
	10.0.0.16	10.0.0.10	10.0.0.5	UP	2.74	4
10.0.0.10	10.0.0.1	10.0.0.5	10.0.0.10	UP	2.74	2
	10.0.0.5	10.0.0.5	10.0.0.10	UP	2.74	1
	10.0.0.7	10.0.0.7	10.0.0.10	UP	2.74	1
	10.0.0.16	10.0.0.7	10.0.0.10	UP	2.74	3
10.0.0.7	10.0.0.1	10.0.0.10	10.0.0.7	UP	2.74	3
	10.0.0.10	10.0.0.10	10.0.0.7	UP	2.74	1
	10.0.0.12	10.0.0.12	10.0.0.7	UP	2.74	1
	10.0.0.16	10.0.0.12	10.0.0.7	UP	2.74	2

Table 4.8: Trust Table for 10.0.0.10; Test 1

Destination	Gateway	Interface	Route Trust	Hop Count	Route Probability	Timestamp (s)
10.0.0.16	10.0.0.5	10.0.0.1	1	5	98.81	5.916
...	...	...	...	...	...	...

Routing Test 2; Highest Probability Route Selection: When multiple routes towards a particular destination exists with respect to a source node, the source node will accept the route with the highest probability of yielding the desired packet delivery ratio. In this case, a simulation with the scenario graphically depicted in Figure 4.7 and the parameters as displayed in Table 4.9 is done.

Assume that the first possible route P_{route1} is denoted by the *dashed lines* in Figure 4.7, the route trust is then calculated from the trust factors of the nodes along the route as:

$$x_2 = 0.8 * 0.9 * 0.7 = 0.504$$

The input vector ($x_1 = 4$, $x_2 = 0.504$) is then converted to its categorical format through the use of equations (4.8) – (4.10) as:

$$(x_1 = 4, x_2 = 0.504) \rightarrow (x_1 = 4, x_2 = 6)$$

Thus, the probability of having a packet delivery ratio of more than 50% from the first route is then calculated from equations (4.5) – (4.16) as:

$$P_{route1}(y = 1 \mid x_1 = 4, x_2 = 6) = \left(\frac{2424 + 1}{4864 + 2} \right) \left(\frac{191 + 1}{4864 + 10} \right) \left(\frac{308 + 1}{4864 + 10} \right) \approx 0.0012$$

$$P_{route1}(y = 0 \mid x_1 = 4, x_2 = 6) = \left(\frac{2440 + 1}{4864 + 2} \right) \left(\frac{104 + 1}{4864 + 10} \right) \left(\frac{325 + 1}{4864 + 10} \right) \approx 7.2282 * 10^{-4}$$

$$\therefore P_{route1}(y = 1 \mid x_1 = 4, x_2 = 6) \approx 63.26\%$$

Using the same approach, we are then able to calculate the probability for the second possible route P_{route2} , as depicted in Figure 4.7 by the *solid lines* as:

$$P_{route2}(y = 1 \mid x_1 = 6, x_2 = 7) \approx 69.59\%$$

By inspecting the *Trust Table* as depicted in Table 4.11, we are able to see that the manual calculations are in agreement with the probability calculated by the NBCR protocol for this specific route. The routing tables as depicted by Table 4.12 show that the route with the highest probability is indeed selected.

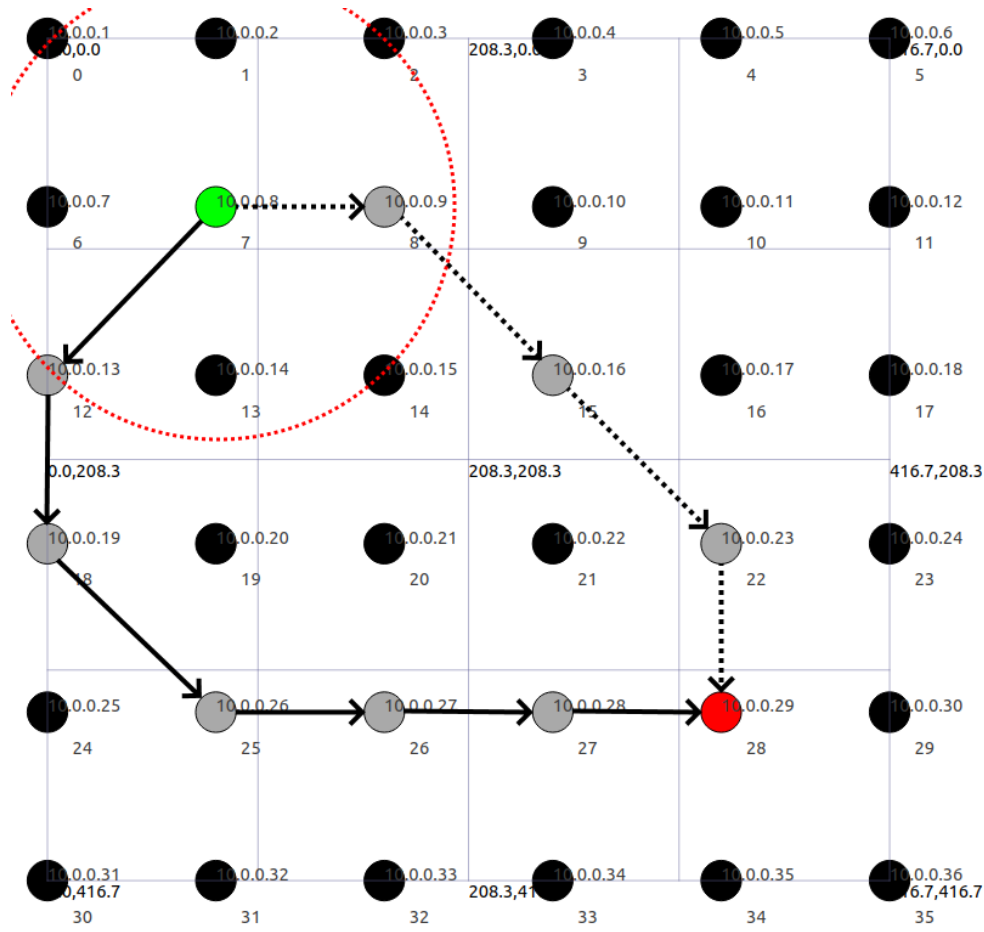


Figure 4.7: Graphical representation; Test 2.

Table 4.9: NBCR simulation parameters; Test 2

Parameter	Value
Simulation Area	500m by 500m
Simulation Time	Start: 0s; End: 100s
No. of Nodes	36
No. of Sink/Source Node Pairs	1
No. of Selfish Nodes	34
Selfish Node Drop Probability	See Table 4.10
Node Distribution	Fixed Grid; 85m Spacing
Mobility Model; Node Speed	None; 0 m/s
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Transmission Range	120m
Routing Protocol	Naïve Bayes Classifier Routing (NBCR)
Traffic Type	Constant Bitrate (CBR)
Transport Protocol	User Datagram Protocol (UDP)
Application Throughput	2048 bp/s
Bandwidth	2 Mbps
Packet Size	128 bytes
Hello Enabled; Hello Interval	No; 0 s

Table 4.10: Node drop probability; Routing Test 2

Node IP	Drop Probability (%)
10.0.0.9	20.00
10.0.0.16	10.00
10.0.0.23	30.00
10.0.0.13	10.00
10.0.0.19	5.00
10.0.0.26	5.00
10.0.0.27	10.00
10.0.0.28	5.00

Table 4.11: *Trust Table* for node 10.0.0.8; Routing Test 2

Destination	Gateway	Interface	Route Trust	Hop Count	Route Probability	Timestamp (s)
10.0.0.29	10.0.0.9	10.0.0.8	0.504	4	63.26	65.37
10.0.0.29	10.0.0.13	10.0.0.8	0.6945	6	69.59	69.59
...	...	...	...	...	...	...

Table 4.12: Routing table; Routing Test 2

Node IP	Destination	Gateway	Interface	Flag	Expire	Hops
10.0.0.8	10.0.0.9	10.0.0.9	10.0.0.8	UP	13.89	1
	10.0.0.13	10.0.0.13	10.0.0.8	UP	3	1
	10.0.0.26	10.0.0.13	10.0.0.8	UP	4.25	3
	10.0.0.29	10.0.0.13	10.0.0.8	UP	10.08	6
10.0.0.13	10.0.0.8	10.0.0.8	10.0.0.13	UP	2.49	1
	10.0.0.19	10.0.0.19	10.0.0.13	UP	2.49	1
	10.0.0.26	10.0.0.19	10.0.0.13	UP	4.33	2
	10.0.0.29	10.0.0.19	10.0.0.13	UP	10.08	5
10.0.0.19	10.0.0.8	10.0.0.13	10.0.0.19	UP	13.88	2
	10.0.0.13	10.0.0.13	10.0.0.19	UP	2.49	1
	10.0.0.26	10.0.0.26	10.0.0.19	UP	2.49	1
	10.0.0.29	10.0.0.26	10.0.0.19	UP	10.08	4
10.0.0.26	10.0.0.8	10.0.0.19	10.0.0.26	UP	13.88	3
	10.0.0.19	10.0.0.19	10.0.0.26	UP	2.49	1
	10.0.0.27	10.0.0.27	10.0.0.26	UP	10.08	1
	10.0.0.29	10.0.0.27	10.0.0.26	UP	10.08	3
10.0.0.27	10.0.0.8	10.0.0.26	10.0.0.27	UP	13.87	4
	10.0.0.26	10.0.0.26	10.0.0.27	UP	2.49	1
	10.0.0.28	10.0.0.28	10.0.0.27	UP	2.49	1
	10.0.0.29	10.0.0.28	10.0.0.27	UP	10.08	2
10.0.0.28	10.0.0.8	10.0.0.27	10.0.0.28	UP	13.87	5
	10.0.0.23	10.0.0.23	10.0.0.28	UP	12.87	1
	10.0.0.27	10.0.0.27	10.0.0.28	UP	2.49	1
	10.0.0.29	10.0.0.29	10.0.0.28	UP	10.07	1

Routing Test 3; Highest Trust Route Selection: When two possible routes towards a destination have hop counts and trust factors that fall within the same category, it will result in the same probability value for both routes. Thus, it is important for the routing protocol to choose the route with the highest trust factor, as depicted by the flowchart in Figure 4.4. To determine if the routing protocol functions as designed, a specific scenario is created as shown by the simulation parameters by Table 4.13 and the graphical representation in Figure 4.8. We assume that P_{route1} is depicted by the *dotted lines* and P_{route2} is depicted by the *solid lines*.

Following the same procedure as before, the probability of each route is calculated as:

$$P_{route1}(y = 1 \mid x_1 = 4, x_2 = 9) \approx 97.91\%$$

$$P_{route2}(y = 1 \mid x_1 = 4, x_2 = 9) \approx 97.91\%$$

The routing tables of interest are depicted in Table 4.14 with the respective *Trust Table* depicted in Table 4.15. It is clear that the selected route exhibits the highest trust factor, despite the hop counts and trust factors falling in the same category.

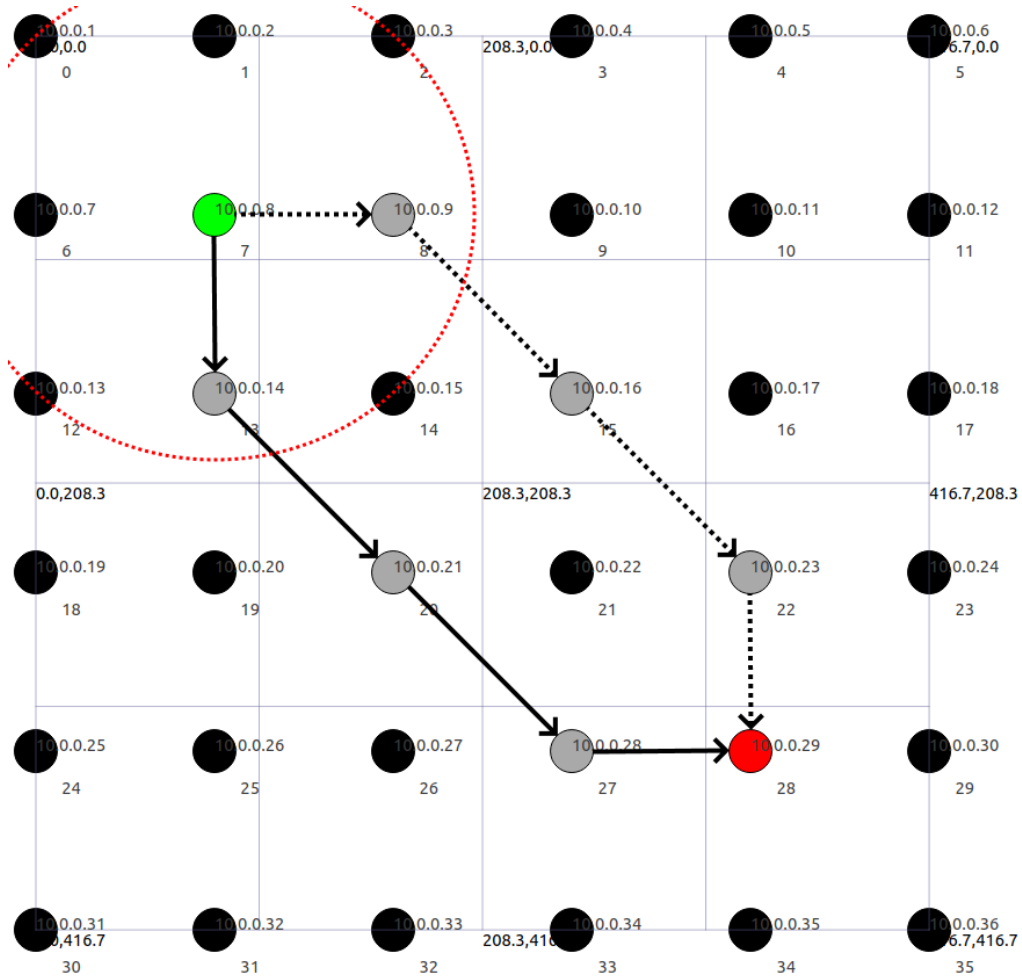


Figure 4.8: Graphical representation; Test 3.

Table 4.13: Simulation parameters; Test 3

Parameter	Value
Simulation Area	500m by 500m
Simulation Time	Start: 0s; End: 100s
No. of Nodes	36
No. of Sink/Source Node Pairs	1
No. of Selfish Nodes	34
Selfish Node Drop Probability	See Table 4.10
Node Distribution	Fixed Grid; 85m Spacing
Mobility Model; Node Speed	None; 0 m/s
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Transmission Range	120m
Routing Protocol	Naïve Bayes Classifier Routing (NBCR)
Traffic Type	Constant Bitrate (CBR)
Transport Protocol	User Datagram Protocol (UDP)
Application Throughput	2048 bp/s
Bandwidth	2 Mbps
Packet Size	128 bytes
Hello Enabled; Hello Interval	No; 0 s

Table 4.14: Routing Table; Routing Test 2

Node IP	Destination	Gateway	Interface	Flag	Expire	Hops
Node 7	10.0.0.9	10.0.0.9	10.0.0.8	UP	5.49	1
	10.0.0.14	10.0.0.14	10.0.0.8	UP	9.94	1
	10.0.0.29	10.0.0.9	10.0.0.8	UP	2.63	4
Node 8	10.0.0.8	10.0.0.8	10.0.0.9	UP	2.63	1
	10.0.0.14	10.0.0.14	10.0.0.9	UP	4.9	1
	10.0.0.16	10.0.0.16	10.0.0.9	UP	2.63	1
	10.0.0.29	10.0.0.16	10.0.0.9	UP	2.63	3
Node 15	10.0.0.8	10.0.0.21	10.0.0.16	UP	7.95	3
	10.0.0.9	10.0.0.9	10.0.0.16	UP	8.92	1
	10.0.0.21	10.0.0.21	10.0.0.16	UP	2.63	1
	10.0.0.23	10.0.0.23	10.0.0.16	UP	2.63	1
	10.0.0.29	10.0.0.23	10.0.0.16	UP	2.63	2
Node 22	10.0.0.8	10.0.0.16	10.0.0.23	UP	7.96	3
	10.0.0.16	10.0.0.16	10.0.0.23	UP	2.63	1
	10.0.0.28	10.0.0.28	10.0.0.23	UP	4.9	1
	10.0.0.29	10.0.0.29	10.0.0.23	UP	2.63	1

Table 4.15: *Trust Table* for 10.0.0.8; Routing Test 3

Destination	Gateway	Interface	Route Trust	Hop Count	Route Probability	Timestamp (s)
10.0.0.29	10.0.0.9	10.0.0.8	0.8574	4	97.91	40.9
10.0.0.29	10.0.0.14	10.0.0.8	0.8122	4	97.91	40.94
...	...	...	...	...	...	...

4.3 Performance Evaluation

¹ To study the effects of *increased hop count* between source/sink node pairs, the NBCR protocol is simulated under both **static** and **mobile** scenarios with the transmission range of each node chosen explicitly such that it would theoretically reach a neighbouring node placed diagonally from it on a fixed grid distribution. This ensures that an increase in network size would result in an increase in hops between source/sink node pairs².

To study the effects of *increased node density*, the NBCR protocol is once again simulated under both **static** and **mobile** scenarios with the transmission range of each node fixed at 250m regardless of the network size. This ensures an increase in node density between source/sink node pairs as the network size increases³.

Scenario 1; Static: In the first simulation scenario, the NBCR protocol is exposed to a change in network size along with an increase in the number of selfish nodes, as shown by the simulation parameters in Table 4.16 and Table 4.17. A fixed grid distribution of 100 nodes up to 400 nodes over an area of 1000m by 1000m is simulated along with an increase in the number of selfish nodes. This increase in selfish nodes is from 0% to 70% of the total amount of nodes in the network in intervals of 10%. The data drop probability of each individual node is randomly selected between 0% and 100%.

Scenario 2; Mobile: In the second simulation scenario, the NBCR protocol is exposed to the exact same simulation parameters as **Scenario 1**, with the exception of assigning a random node velocity of 0 m/s – 25 m/s to each individual node and randomly distributing the nodes within the simulation area.

The results of these simulations are depicted in tabular format by Table B.1 and Table B.2, and graphically by Figure 4.9 to Figure 4.12.

¹The evaluation procedure of the NBCR protocol's performance is identical to that of the AODV protocol.

²Chapter 2; Figure 2.4

³Chapter 2; Figure 2.5

Table 4.16: NBCR simulation parameters; constant

Parameter	Value
Simulation Area	1000m by 1000m
Simulation Time	Start: 0s; End: 100s
No. of Nodes	100; 200; 300; 400
No. of Sink/Source Node Pairs	10; 20; 30; 40
No. of Selfish Nodes	0% to 70% of total nodes in intervals of 10%
Selfish Node Drop Probability	0 to 100 %
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Routing Protocol	Naïve Bayes Classifier Routing (NBCR)
Traffic Type	Constant Bitrate (CBR)
Transport Protocol	User Datagram Protocol (UDP)
Application Throughput	2048 bp/s
Bandwidth	2 Mbp/s
Packet Size	128 bytes
Hello Enabled; Hello Interval;	No; 0 s
Trust Threshold	0.5

Table 4.17: NBCR simulation parameters; variable

Parameter	Value	
	Variable Transmission Range	
	Scenario 1: Fixed Grid	Scenario 2: Mobile
	Fixed Grid	Random
	0 m/s	0 m/s to 25 m/s
	None	Random Waypoint Mobility Model
Transmission Range	145m; 100m; 85m; 75m	145m; 100m; 85m; 75m
	Fixed Transmission Range	
	Scenario 1: Fixed Grid	Scenario 2: Mobile
	Fixed Grid	Random
	0 m/s	0 m/s to 25 m/s
	None	Random Waypoint Mobility Model
Transmission Range	250m	250m

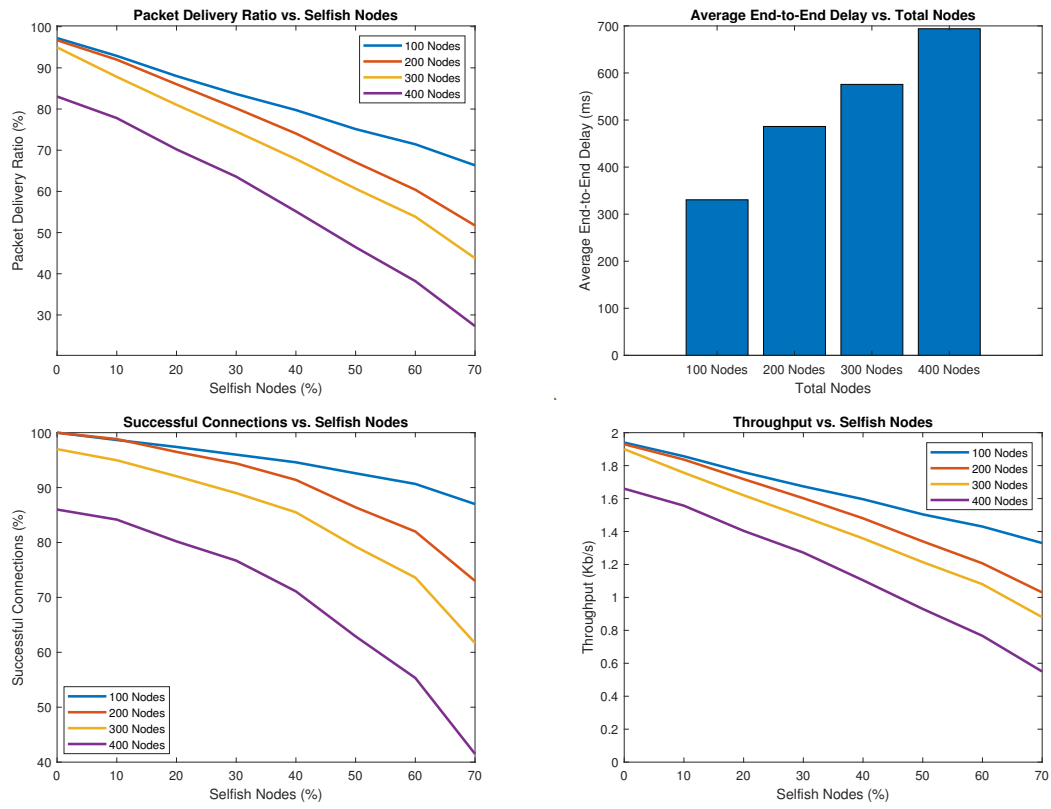


Figure 4.9: NBCR simulation results; variable transmission range; static.

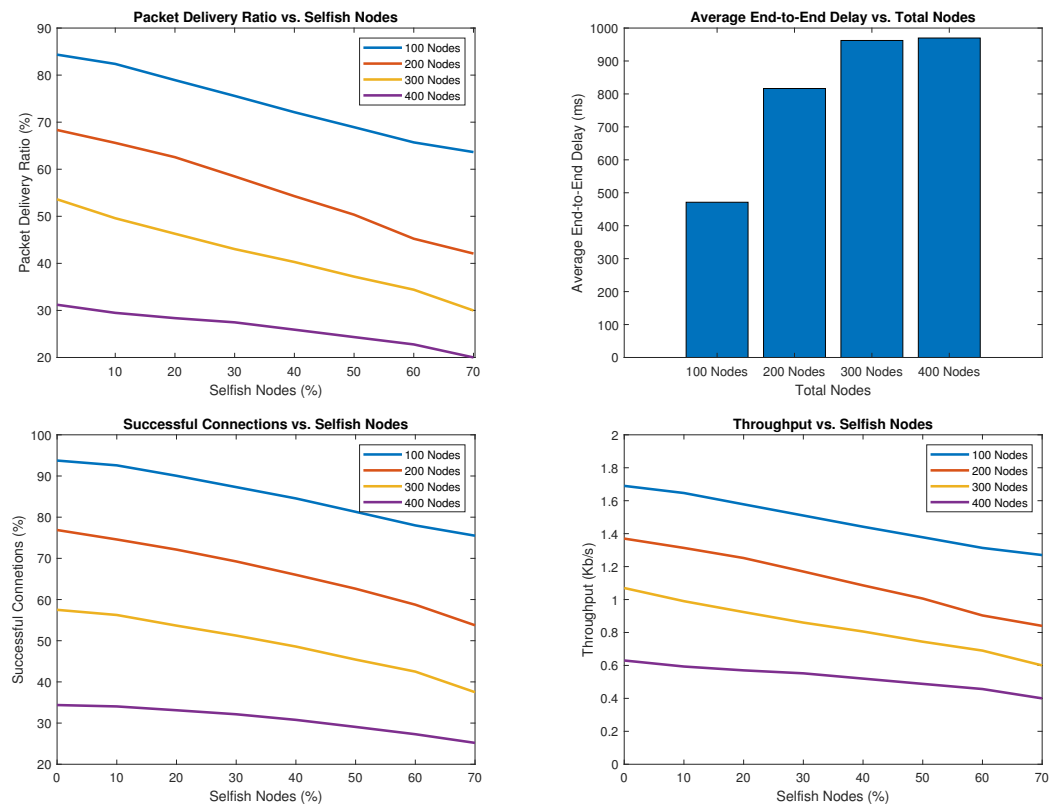


Figure 4.10: NBCR simulation results; variable transmission range; mobile.

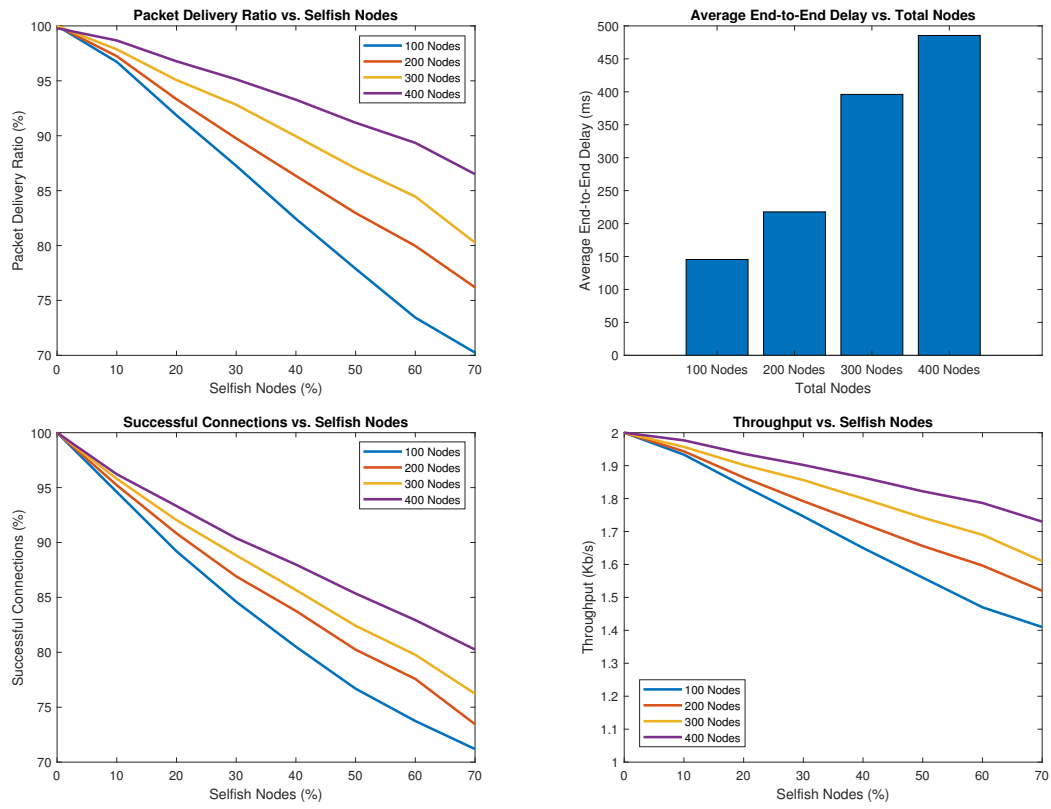


Figure 4.11: NBCR simulation results; fixed transmission range; static.

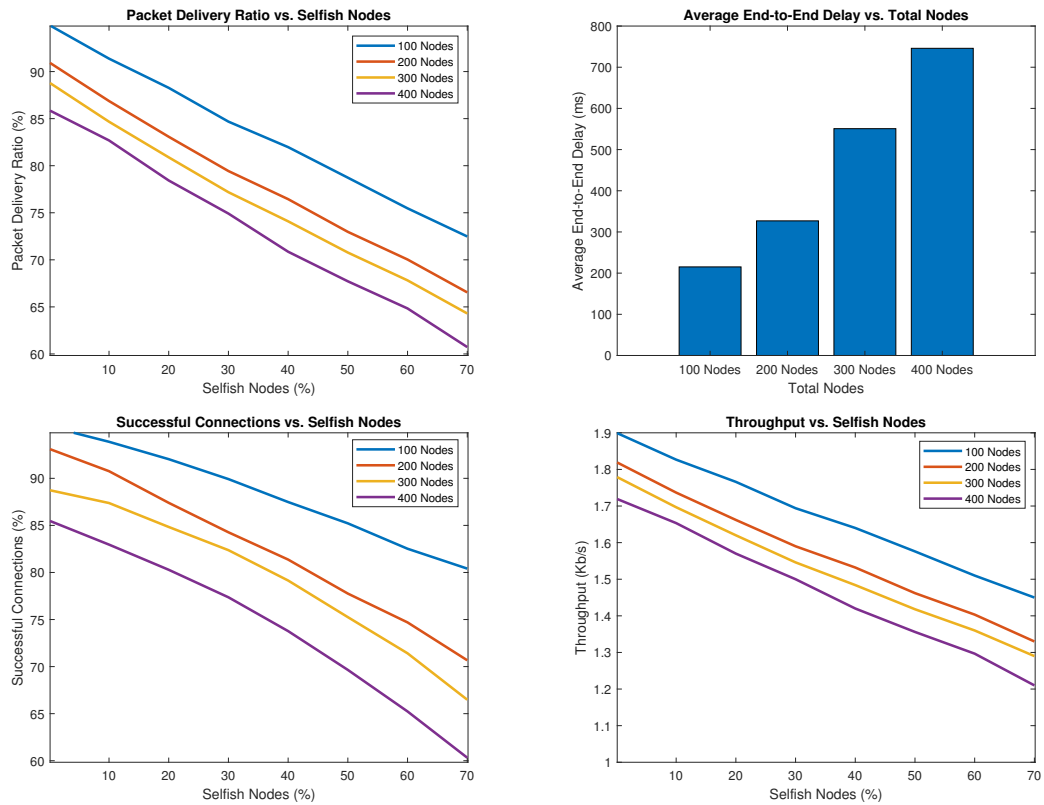


Figure 4.12: NBCR simulation results; fixed transmission range; mobile.

4.4 Summary

4.4.1 Protocol Operation

From the preceding sections, a summarized version of how the NBCR protocol operates to form a connection between source/sink nodes is given by the following steps:

1. Source node emits a RREQ control packet to all neighbouring nodes.
2. A neighbouring node will decide to forward or discard this RREQ packet based on its own observed trust factor, which is calculated by (4.17):

$$Trust_{node} = \frac{\sum DroppedPackets}{\sum TotalPackets}$$

If the neighbouring node exhibits a trust factor below the desired threshold, the packet will be discarded. This procedure is explained in Figure 4.1.

3. Once the RREQ packet has reached the destination/sink node, a reverse path is created and a RREP packet is sent along this reverse path. During this procedure, each node contributes in determining the trust value of the route using equation (4.18):

$$Trust_{route} = Trust_{old} * Trust_{node}$$

4. A route will be accepted/discarded based on the probability that the route will result in an acceptable packet delivery ratio between the source and sink node. This procedure is explained in Figure 4.4.

4.4.2 Operational Analysis

We highlight the following insights found through the evaluation of the NBCR protocol:

Classifier Sensitivity: The classifier sensitivity test has proven that there is indeed independence between classifier variables. Evidently, hop count affects the trust factor of a route, leading to inconsequential dependence. However, the independence between these classifier variables provide a distinction which is inviolable enough to make accurate predictions.

Routing Validation: *From the first routing test*, it is clear that selfish nodes exhibiting a trust factor lower than the allowed threshold will drop all RREQ packets, removing themselves as possible candidates to form a possible route to the destination. This also helps with aggregation to reduce the area of RREQ flooding and reduces control overhead.

From the second routing test, the NBCR protocol has proven itself to operate differently than traditional AODV by selecting the route with the highest probability, and not the

route with the lowest hop count- resulting in better network performance in the presence of selfish nodes.

From the third routing test, the NBCR protocol has shown that even in situations where the categorical values of the route trust and hop count are the same for two different routes (resulting in the same probability), the raw trust factor of the route will then be used to determine the best path to route data.

4.4.3 Performance Analysis

Packet Delivery Ratio: The protocol sees a decline in packet delivery ratio when an increase in number of selfish nodes are presented. The same is true for an increase in network size under both static and mobile scenarios using a variable transmission range (increased hop count) configuration. However, larger networks have a better packet delivery ratio than smaller networks when a static scenario is presented with a fixed transmission range (increased node density) configuration. This is due to static topologies providing congruous connections once RREQ packets are dropped by selfish nodes and reinitiating the route discovery process, with larger networks providing more alternative routes due to a high node density. Once mobility is introduced, the packet delivery ratio declines in all instances. The variables that seem to affect packet delivery the most are mobility, selfish nodes and node density.

Average End-to-End Delay: The average end-to-end delay increases as the network size is increased for all scenarios and configurations. The highest overall average end-to-end delay is seen in a large network with a variable transmission range (increased hop count) configuration consisting of mobile nodes due to multi-hop connections and constant link breakage. The lowest overall average end-to-end delay is seen in a small network with a fixed transmission range (increased node density) configuration and a static grid topology.

Successful Connections: The number of successful connections are in strong correlation with packet delivery ratio, and also see a decline once selfish nodes are presented/increased. As with packet delivery ratio, larger networks with a static grid topology and a fixed transmission range configuration have better packet delivery than smaller networks. However, more dense networks see a decrease in successful connections once node mobility is introduced due to constant link breakages, aggressive RREQ flooding, and node isolation.

Throughput: Since the application throughput is $2Kbps$ with a bandwidth of $2Mbps$, congestion is highly unlikely within the network. This leads to the throughput being in direct correlation with the packet delivery ratio and respectively sees the most deterioration

under an increase in selfish nodes, higher node densities, and node mobility¹.

4.4.4 Final Remarks

The goal of the NBCR protocol is to use posterior probabilities calculated from previously obtained data to select routes that would provide an improvement in network performance. From the previous subsections, we see that the protocol performs as expected. A comparative analysis with AODV is done in Chapter 6.

¹A larger packet size would inadvertently affect packet delivery ratio, average end-to-end delay and throughput negatively on larger networks.

Chapter 5

Clustering Overlay

This chapter presents the creation of an experimental clustering overlay based on the principles of [30]. This clustering overlay serves as an extension of the NBCR protocol to help maintain sensible topologies in large scale mobile ad hoc networks, and therefore called the Cluster-Based Naïve Bayes Classifier Routing (CB-NBCR) protocol.

5.1 Protocol Design

5.1.1 Node Designation

Nomenclature generally suggests that a cluster consists of three types of cluster members—the cluster head, the member nodes, and the gateway nodes. Cluster heads are chosen based on a pre-defined metric of evaluation and tend to control communication and the assignment of roles within the cluster. Gateway nodes serve as a conduit between two or more clusters by being within communication range of cluster heads outside of its designated cluster. Member nodes are considered auxiliary, and do not participate within the active network. An example of inter-cluster communication with the described cluster members is shown in Figure 5.1, with cluster heads denoted by the letter “C”, gateway nodes denoted by the letter “G” and member nodes denoted by the letter “M”.

5.1.2 Clustering Framework

Using the same approach as described in [30], we assume that each individual node has a unique variable $Weight_{node}$ assigned to it based on a combination of different metrics, and that each metric has a pre-determined multiplier associated with it. These multipliers, along with their respective metrics determine the value of $Weight_{node}$ and serve as an

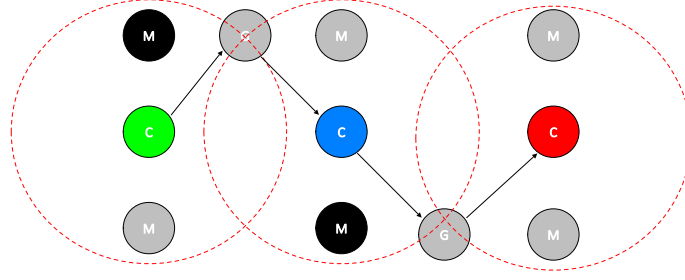


Figure 5.1: An example of inter-cluster communication.

indication for how strongly each metric affects the candidacy of a node for cluster head selection. Since the goal of this clustering overlay is to purely address aggregation of large networks in the presence of selfish nodes and mobility, $Weight_{node}$ is defined as:

$$Weight_{node} = \alpha_1 * \left(\frac{25 - Velocity_{node}}{25} \right) + \alpha_2 * Trust_{node} \quad (5.1)$$

where $Velocity_{node}$ denotes the velocity metric of the node in m/s and ranges between 0 m/s and 25 m/s. $Trust_{node}$ denotes the trust metric of the node as explained in the preceding chapter and ranges between 0 and 1. The multipliers of the two metrics are respectively denoted by α_1 and α_2 , where

$$\alpha_1 + \alpha_2 = 1 \quad (5.2)$$

In traditional AODV, nodes may offer connectivity information by broadcasting *Hello* messages in discrete time intervals to neighbouring nodes. CB-NBCR Takes advantage of this characteristic by creating new clusters in concurrence with the expiration of the *Hello Timer* associated with *Hello* messages. CB-NBCR additionally extends the amount of information shared amongst neighbouring nodes by adding another two field to the header of traditional *Hello* messages. These fields contains information regarding the $Weight_{node}$ value of the node, as well as the $Role_{node}$ of the node. The format of a CB-NBCR *Hello* message is depicted in Table 5.1.

In addition to the *Hello Timer*, CB-NBCR makes use of two additional timers for topology management. These timers and the steps associated with them are shown in Figure 5.2. Once the *Hello Timer* expires the clustering procedure is initiated, afterwards every expiration of the *Hello Timer* will initiate cluster maintenance.

When a node has been assigned to a new role, it will broadcast a *Node Designation* message with the format depicted in Table 5.2 to all relevant neighbouring nodes. Individual nodes keep track of information regarding their neighbours by making use of a *Neighbour Table*-populating it with entries relevant to the information received from *Node Designation* and *Hello* messages. The format of this table is shown in Table 5.3. *Cluster Control* messages are used to either relinquish control from one cluster head to another, or to completely abandon clustering once the conditions are not deemed favourable.

Table 5.1: CB-NBCR *Hello* message format.

Field	Description
Destination IP Address	The node's IP address.
Destination Sequence Number	The node's latest sequence number.
Hop Count	0
Lifetime	ALLOWED_HELLO_LOSS * HELLO_INTERVAL
Node Weight	The node's calculated $Weight_{node}$ value.
Node Role	The nodes's designated $Role_{node}$ tag.

Table 5.2: CB-NBCR *Neighbour Table* format.

Node IP	Node Weight	Node Tag	Cluster Head IPs
Neighbouring node IP address.	Neighbouring node $Weight_{node}$ value.	Neighbouring node role tag: 0 - Cluster head. 1 - Gateway node. 2 - Member node. 3 - Non-cluster node.	IP addresses of all cluster heads in proximity to the neighbouring node. Cluster Head IP #1 Cluster Head IP #2 Cluster Head IP #3 ...
...	...	...	...

Table 5.3: CB-NBCR *Node Designation* message format.

Field	Description
Node IP	The node's IP address
Node Tag	The node's role tag
Node Weight ($Weight_{node}$)	The node's calculated $Weight_{node}$ value.
Cluster Head IP	The most recent cluster head IP to which the node is connected to.

Table 5.4: CB-NBCR *Cluster Control* message format.

Field	Description
Control Message	Cluster control message tag: 0 - Relinquish control to a new cluster head. 1 - Abandon clustering.

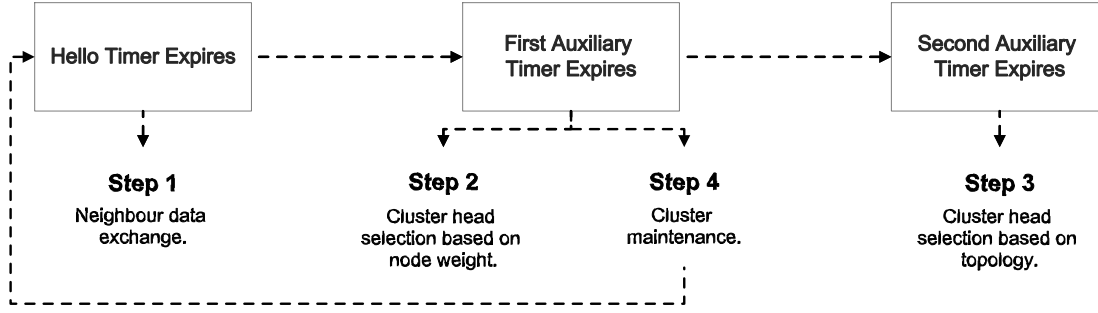


Figure 5.2: CB-NBCR clustering procedure overview.

5.1.3 Protocol Operation

Opportunistic Clustering: The simulation results from Chapter 3 show that the RREQ flooding technique used by AODV can be detrimental to network performance when a high node density is present. The creation of clusters to reduce the network to a more manageable topology will solve this issue. However, clustering where low node densities are present would have the opposite effect, resulting in the exclusion of nodes needed for successful route creation, especially in networks where mobility is present.

To address this issue, clusters are only formed in dense areas of a network by virtue of the amount of neighbours $Neighbours_{node}$ a node has. If a node should be selected as a cluster head, but does not conform to

$$Neighbours_{node} > Neighbours_{threshold} \quad (5.3)$$

where $Neighbours_{threshold}$ is the minimum number of neighbours needed for clustering, the process will abandon.

Step 1; Neighbour Data Exchange: The process of creating clusters is interval-based, and concurrently takes place along with the initial exchange of *Hello* messages. Once the *Hello Timer* has expired and a new *Hello* message broadcast is initiated, each node will clear their *Neighbour Table* and calculate their own $Weight_{node}$ value through the use of equation (5.1).

All nodes are initially considered non-cluster nodes, and will populate the needed fields of the CB-NBCR *Hello* messages with their individual $Weight_{node}$ values accordingly. These messages are then sent to all neighbouring nodes in the same fashion as traditional AODV. Upon receiving a CB-NBCR *Hello* message a node will create the respective entries in its *Neighbour Table*.

Step 2 & 3; Cluster Head Selection: Cluster head selection is a timed event which takes place after a designated period of time which would ensure that all relevant data has

been exchanged beforehand by the propagation of CB-NBCR *Hello* messages. Nodes may *only* be appointed as cluster heads if they fulfil the requirement of (5.3). Once the *First Auxiliary Timer* expires, a node will be selected as a cluster head and propagate a *Node Designation* message to all neighbouring nodes accordingly if it is a sink/source node, or if it has the best $Weight_{node}$ value amongst all its neighbours.

Once the *Second Auxiliary Timer* expires, a node will be selected as a cluster head and propagate a *Node Designation* message to all neighbouring nodes accordingly if it has no neighbouring nodes who are cluster heads, and if it has at least two neighbouring nodes who are connected to unique cluster heads.

At any point in time, if a node should receive a *Node Designation* message from a cluster head, it would respond by propagating a *Node Designation* message with the appropriate fields populated to all neighbouring nodes. The purpose of this is to notify all neighbouring nodes of the node's new connection to a cluster head, and of its new role as a member node. If more than one *Node Designation* messages are received from cluster heads, the node is assigned the role of gateway node, and will notify all neighbouring nodes by sending a *Node Designation* message with the appropriate entries.

Step 4; Cluster Maintenance: To maintain sensible topologies in a constantly changing network, every expiration of the the *Hello Timer* onwards from the initial expiration repeats **Step 1** of the clustering process- exchanging data between neighbours. Once this exchange has happened the *First Auxiliary Timer* acts as a cluster maintenance method, determining when control needs to be relinquished to another cluster head, if clustering should be abandoned, or if new clusters should be formed.

Control will be relinquished to another cluster head if a new node has entered within the range of the current cluster head and exhibits a better $Weight_{node}$ value. When this happens a *Cluster Control* message will be sent to all neighbouring nodes with the *Control Message* tag set to 1, notifying them that the cluster no longer exists and re-establishing their roles as non-cluster nodes. A *Cluster Control* message will sequentially be sent to the newly appointed cluster head with the *Control Message* tag set to 0, notifying the node of its newly appointed role. The selected node will establish itself as the new cluster head by sending a *Node Designation* message to all neighbouring nodes with the appropriate tags set, forming a new cluster.

Once a cluster head no longer meets the requirements of (5.3) or has no more gateway nodes to other cluster heads, a *Cluster Control* message will be sent to all neighbouring nodes with the *Control Message* tag set to 1. This will notify all cluster members that clustering has been abandoned, and will result in all neighbouring nodes reassigning themselves to the role of non-cluster nodes. Nodes that have been assigned the role of non-cluster nodes will form part of future clusters if the required conditions are met.

5.2 Operational Evaluation

5.2.1 Multiplier Values

To determine which values of α_1 and α_2 in (5.1) to use, consider a random distribution of 250 nodes each with a random velocity of 0 m/s - 25 m/s in a geographical area of 500m by 500m, as shown in Figure 5.3. Selfish nodes are chosen as 40% of the total nodes and the neighbour count threshold value $Neighbours_{threshold}$ is chosen as 0, such that clustering would take place regardless of node density. We choose packet delivery ratio as the observed variable to study the effects of α_1 and α_2 . These simulation parameters are shown in Table 5.5 and are chosen such that there would be enough variation in node trust values, mobility and node densities. The results of the simulation are graphically depicted by Figure 5.4 and also shown in Tabular format by Table 5.6. From these results we conclude that the most favourable conditions are found when $\alpha_1 = 0.7$ and $\alpha_2 = 0.3$ for this particular scenario.

Table 5.5: CB-NBCR Multiplier Values Test; Simulation parameters.

Parameter	Value
Simulation Area	500m by 500m
Simulation Time	Start: 0s; End: 200s
No. of Nodes	250
No. of Sink/Source Node Pairs	25
No. of Selfish Nodes	40% of total nodes
Selfish Node Drop Probability	0 to 100 %
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Routing Protocol	Cluster-based Naïve Bayes Classifier Routing (CB-NBCR)
Traffic Type	Constant Bitrate (CBR)
Transport Protocol	User Datagram Protocol (UDP)
Application Throughput	2048 bp/s
Bandwidth	2 Mbps
Packet Size	128 bytes
Hello Enabled; Hello Interval;	Yes; 5 s
Trust Threshold	0.5
Neighbour Count Threshold	0
Transmission Range	100m
$\alpha_1; \alpha_2$	Variable

Table 5.6: CB-NBCR Multiplier Values Test; Simulation results.

(α_1, α_2)	Packet Delivery Ratio
(0.0, 1.0) (0.1, 0.9) (0.2, 0.8)	58.93 59.25 61.33
(0.3, 0.7) (0.4, 0.6) (0.5, 0.5)	64.25 65.93 68.55
(0.6, 0.4) (0.7, 0.3) (0.8, 0.2)	70.48 74.14 70.17
(0.9, 0.1) (1.0, 0.0)	67.45 66.31

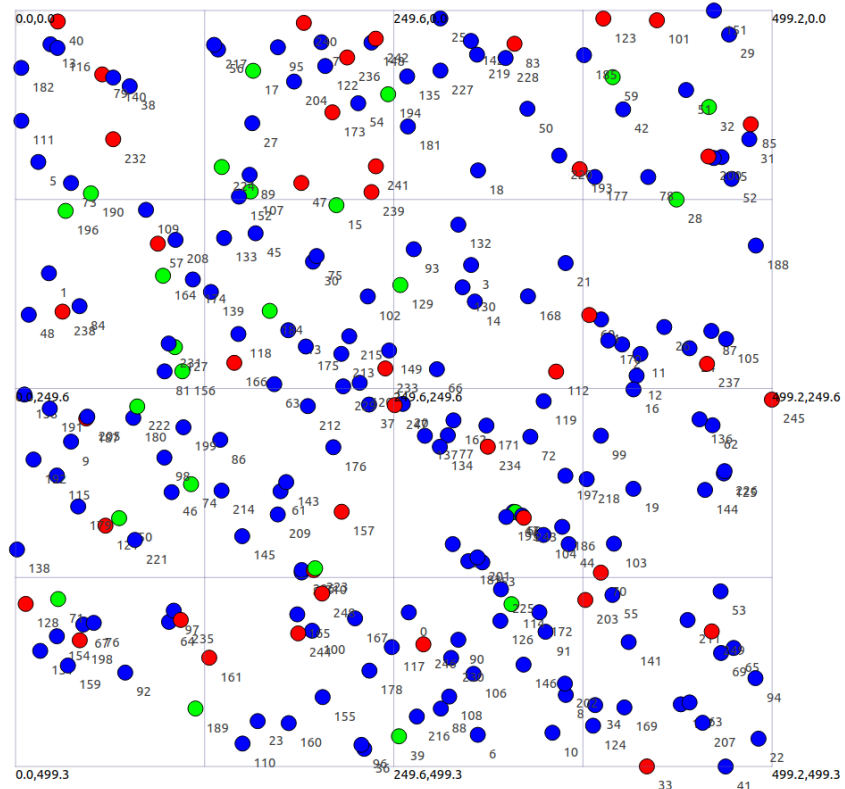


Figure 5.3: CB-NBCR Multiplier Values Test; Graphical representation.

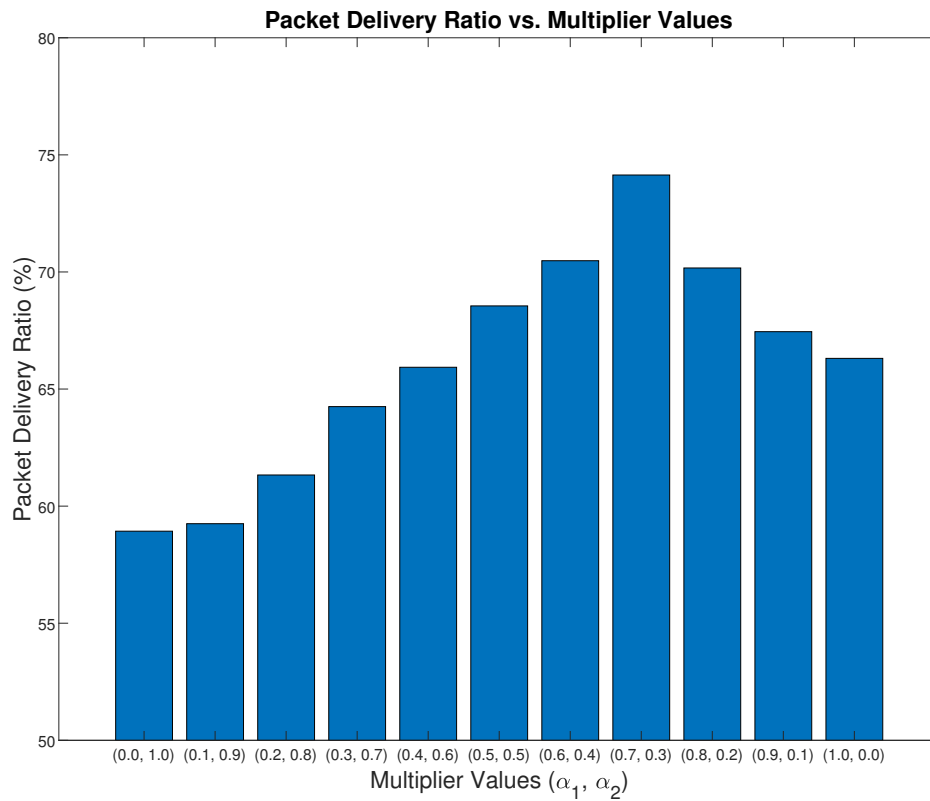


Figure 5.4: CB-NBCR Multiplier Values Test; Simulation results.

5.2.2 Neighbour Count Threshold

Since the CB-NBCR protocol is designed to only form clusters at certain node densities by virtue of the neighbour count threshold $Neighbours_{node}^1$, a simulation study is done to determine which node densities are more favourable for clustering.

Consider a random distribution of 250 nodes in an area of 500m by 500m as depicted by Figure 5.5. Each node has a random velocity between 0 m/s and 25 m/s assigned to it, and the number of selfish nodes are chosen as 40% of the total nodes. Once again the packet delivery ratio metric is used to determine the effects of a variable neighbour count threshold. From the previous test, we assign $\alpha_1 = 0.7$ and $\alpha_2 = 0.3$.

From the analysis, a threshold value of at least 15 neighbouring nodes is determined as the most suitable value under the observed conditions.

Table 5.7: CB-NBCR Node Density Test; Simulation parameters.

Parameter	Value
Simulation Area	500m by 500m
Simulation Time	Start: 0s; End: 200s
No. of Nodes	250
No. of Sink/Source Node Pairs	25
No. of Selfish Nodes	40% of total nodes
Selfish Node Drop Probability	0 to 100 %
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Routing Protocol	Cluster-based Naïve Bayes Classifier Routing (CB-NBCR)
Traffic Type	Constant Bitrate (CBR)
Transport Protocol	User Datagram Protocol (UDP)
Application Throughput	2048 bp/s
Bandwidth	2 Mbp/s
Packet Size	128 bytes
Hello Enabled; Hello Interval;	Yes; 5 s
Trust Threshold	0.5
Neighbour Count Threshold	Variable
Transmission Range	100m
$\alpha_1; \alpha_2$	0.7; 0.3

Table 5.8: CB-NBCR Node Density Test; Simulation results.

$Neighbours_{threshold}$	Packet Delivery Ratio
0 5 10	73.63 74.89 77.42
15 20 25	80.75 76.94 72.33
30	70.29

¹Equation (5.3)

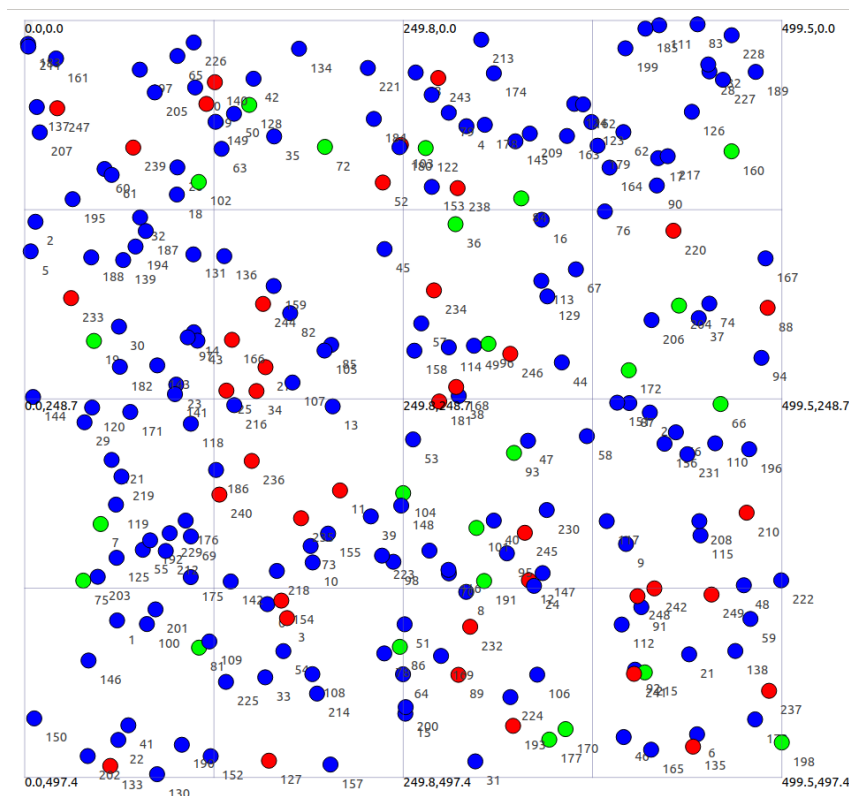


Figure 5.5: CB-NBCR Multiplier Values Test; Graphical representation.

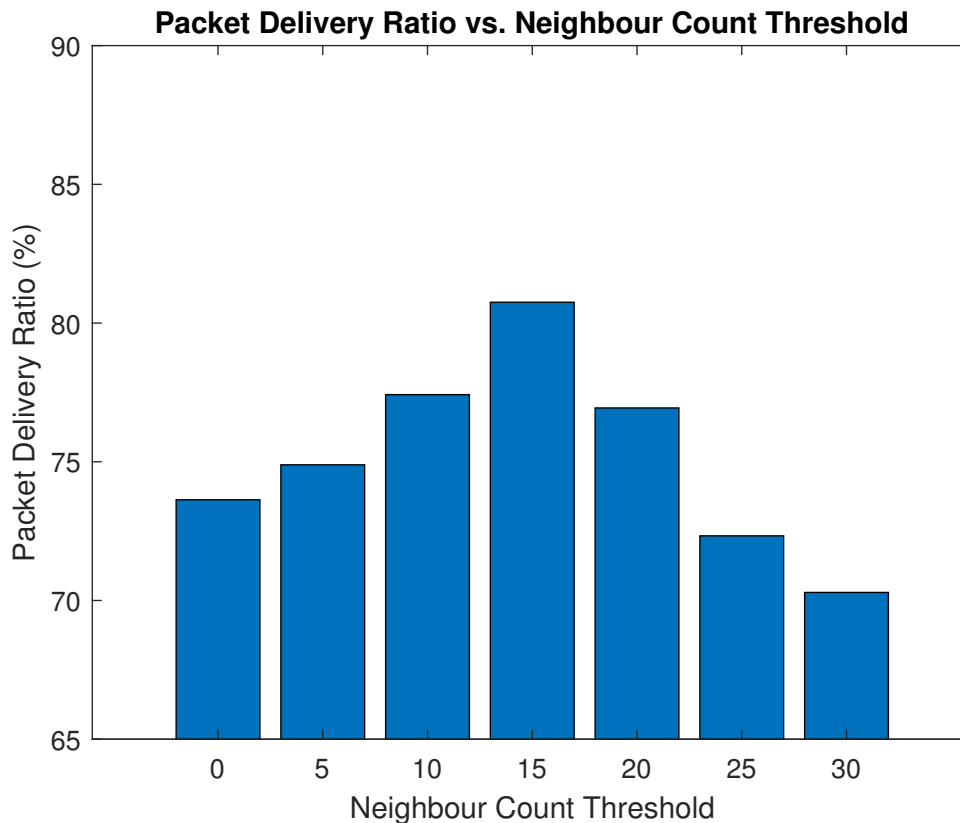


Figure 5.6: CB-NBCR Multiplier Values Test; Simulation results.

5.2.3 Clustering

Cluster Creation Test: Assume that we have a static grid topology as shown in Figure 5.7 with the simulation parameters shown in Table 5.9. All the selfish nodes have a drop probability of 80%, with the exception of some nodes which have defined drop probabilities as depicted by Table 5.10. The goal is for the grid formation to be reduced to a more manageable topology through the clustering process.

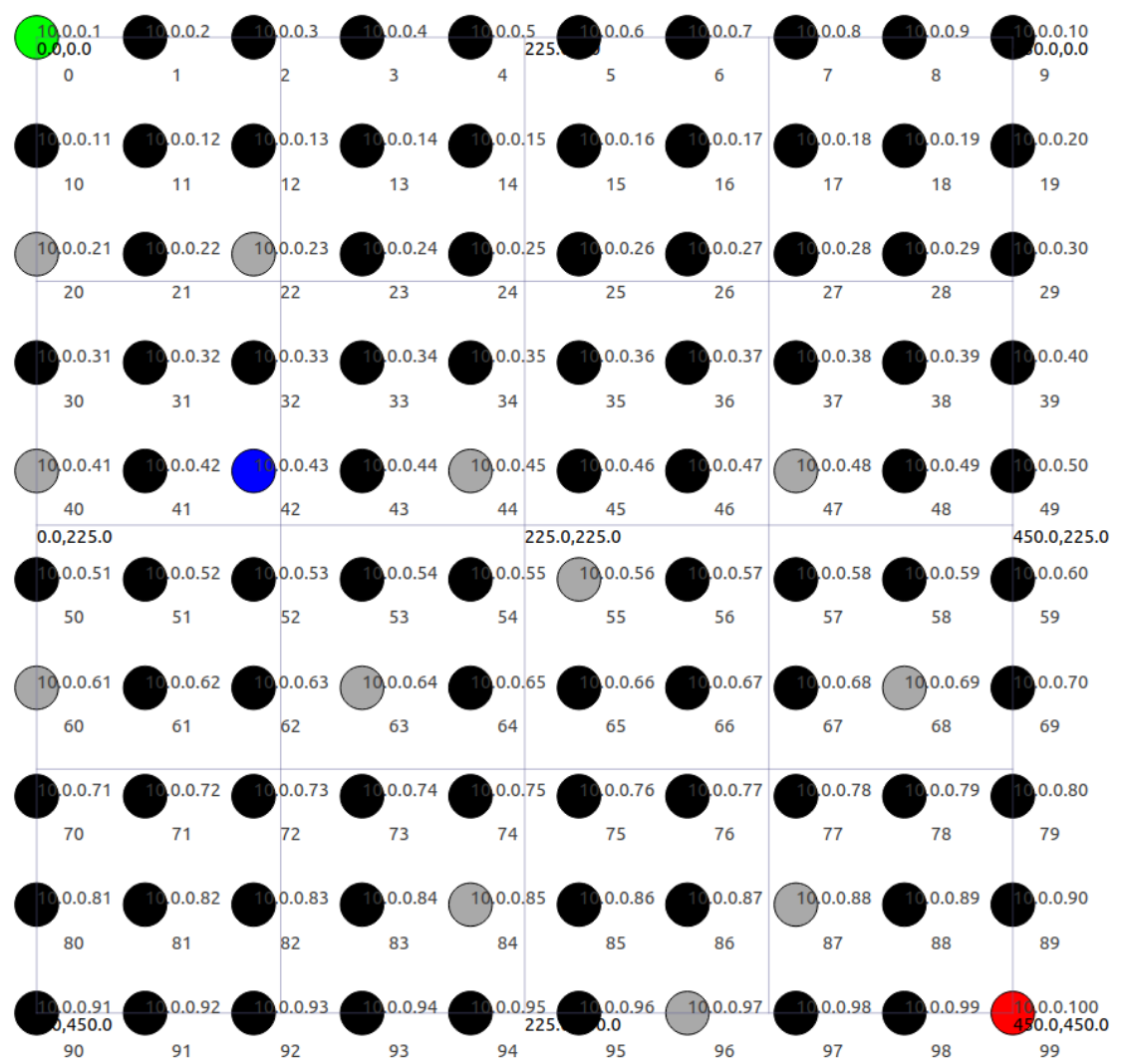
Figure 5.7 shows the network topology once the *Hello Timer* has expired and neighbours have exchanged data regarding their $Weight_{node}$ values. It is clear from this figure that none of the nodes have yet been assigned to roles and that the topology remains unchanged. Once the *First Auxiliary Timer* has expired, as depicted in Figure 5.8, the network drastically reduces to a more simple topology- nodes with the most desirable $Weight_{node}$ value amongst all their neighbours, and sink/source nodes have been assigned as cluster heads. Figure 5.9 shows the network topology once the *Secondary Auxiliary Timer* has expired. It is clear from this figure that the remaining cluster heads are selected in such a way that a route between the source and sink nodes can be formed. The final route between the source and sink nodes depicted by the *solid lines* in Figure 5.9. These graphical representations exclude member nodes for a more concise overview. From Appendix A, Table C.3 and Table C.4 show the route taken for communication between the source and sink nodes, whereas Table C.2 and Table C.1 show the *Trust Table* for the source node and *Neighbour Table* for the cluster head nodes, respectively.

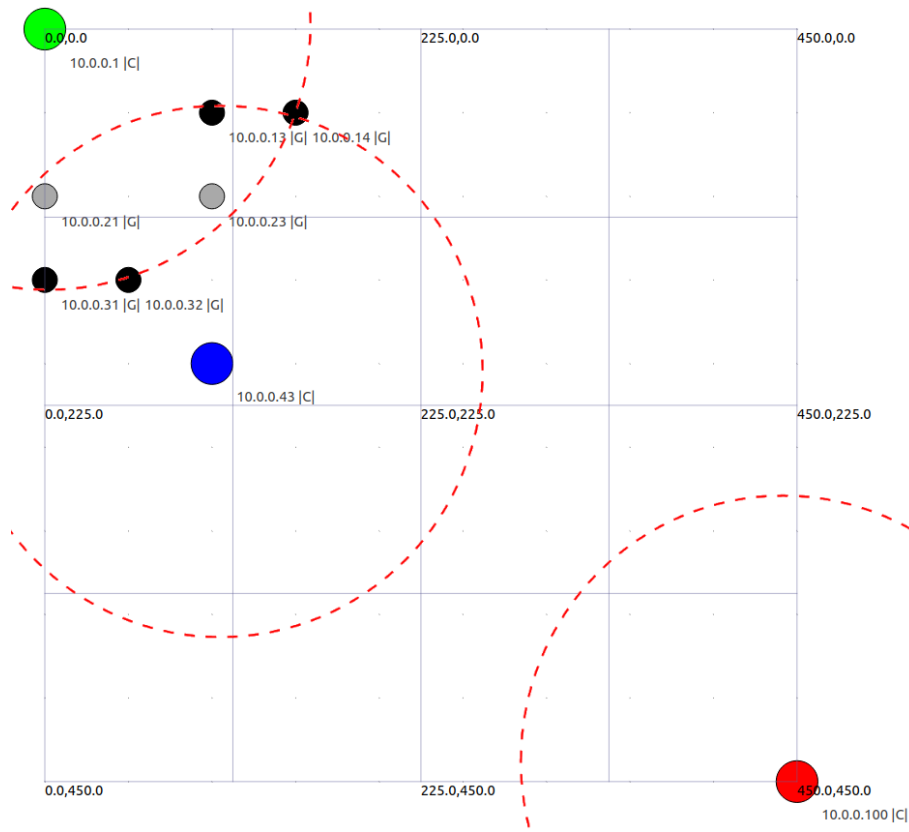
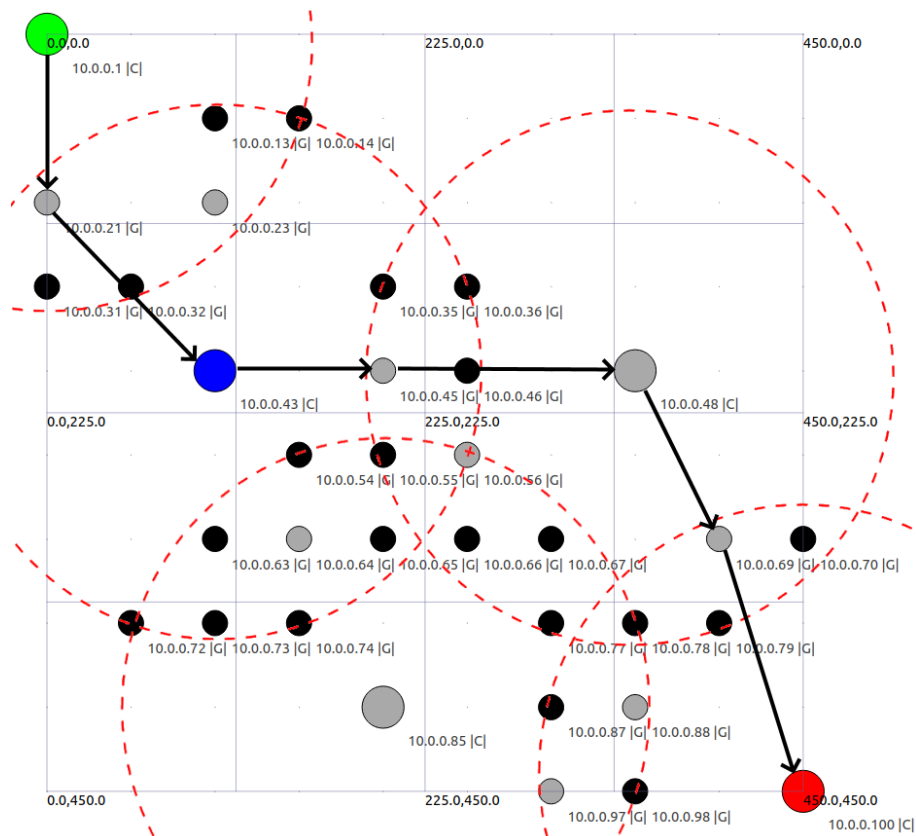
Table 5.9: Simulation parameters; Clustering Creation Test

Parameter	Value
Simulation Area; Simulation Time	500m by 500m; Start: 0s & End: 100s
No. of Nodes	100
No. of Sink/Source Node Pairs	1
No. of Selfish Nodes	97
Selfish Node Drop Probability	80% (See Table 5.10)
Node Distribution	Fixed Grid; 50m Spacing
Mobility Model; Node Speed	None; 0 m/s
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Transmission Range	175m
Routing Protocol	Cluster-Based Naïve Bayes Classifier Routing (CB-NBCR)
Transport Protocol; Traffic Type	User Datagram Protocol (UDP); Constant Bitrate (CBR)
Application Throughput	2048 bp/s
Bandwidth; Packet Size	2 Mbp/s; 128 bytes
Hello Enabled; Hello Interval	Yes; 5 s
Trust Threshold	0.5
Neighbour Count Threshold	15
$\alpha_1; \alpha_2$	0.7; 0.3

Table 5.10: Node drop probability; Cluster Creation Test

Node IP	Drop Probability (%)
10.0.0.21	15
10.0.0.23	25
10.0.0.41	25
10.0.0.45	25
10.0.0.48	35
10.0.0.56	25
10.0.0.61	15
10.0.0.64	20
10.0.0.69	10
10.0.0.85	30
10.0.0.88	10
10.0.0.97	40



Figure 5.8: *First Auxiliary Timer* expires; Cluster Creation Test.Figure 5.9: *Second Auxiliary Timer* expires; Cluster Creation Test.

Cluster Maintenance Test 1; Cluster Abandonment: Assume that we have an initial static grid topology as shown in Figure 5.10 with the simulation parameters shown in Table 5.11. All the nodes have a drop probability of 35% with the exception of nodes 10.0.0.23 and 10.0.0.28, which are chosen as intermediate nodes. After initial clustering has taken place, the network topology is reduced to that of Figure 5.11. The goal of this simulation is to determine if the protocol will abandon clustering if the conditions are not deemed favourable by virtue of equation (5.3).

During the first half of the simulation the topology remains constant, but at the start of the second half of the simulation the nodes depicted by Table 5.12 are removed from the network, and forces the clustering procedure to abandon due to the cluster heads not having enough neighbouring nodes. The network topology is changed to that depicted in Figure 5.12, and shows that clustering has been abandoned.

Table 5.11: Simulation parameters; Cluster Maintenance Test 1

Parameter	Value
Simulation Area; Simulation Time	500m by 250m; Start: 0s & End: 100s
No. of Nodes	50
No. of Sink/Source Node Pairs	0
No. of Selfish Nodes	48
Selfish Node Drop Probability	35%
Node Distribution	Fixed Grid; 50m Spacing
Mobility Model; Node Speed	None; 0 m/s
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Transmission Range	175m
Routing Protocol	Cluster-Based Naïve Bayes Classifier Routing (CB-NBCR)
Transport Protocol; Traffic Type	User Datagram Protocol (UDP); Constant Bitrate (CBR)
Application Throughput	2048 bp/s
Bandwidth; Packet Size	2 Mbp/s; 128 bytes
Hello Enabled; Hello Interval	Yes; 5 s
Trust Threshold	0.5
Neighbour Count Threshold	15
$\alpha_1; \alpha_2$	0.7; 0.3

Table 5.12: Nodes selected for network removal; Cluster Maintenance Test 1

Node IP
10.0.0.1 10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5 10.0.0.6 10.0.0.7
10.0.0.8 10.0.0.9 10.0.0.10 10.0.0.11 10.0.0.20 10.0.0.21 10.0.0.30
10.0.0.31 10.0.0.40 10.0.0.41 10.0.0.42 10.0.0.43 10.0.0.44 10.0.0.45
10.0.0.46 10.0.0.47 10.0.0.48 10.0.0.49 10.0.0.50

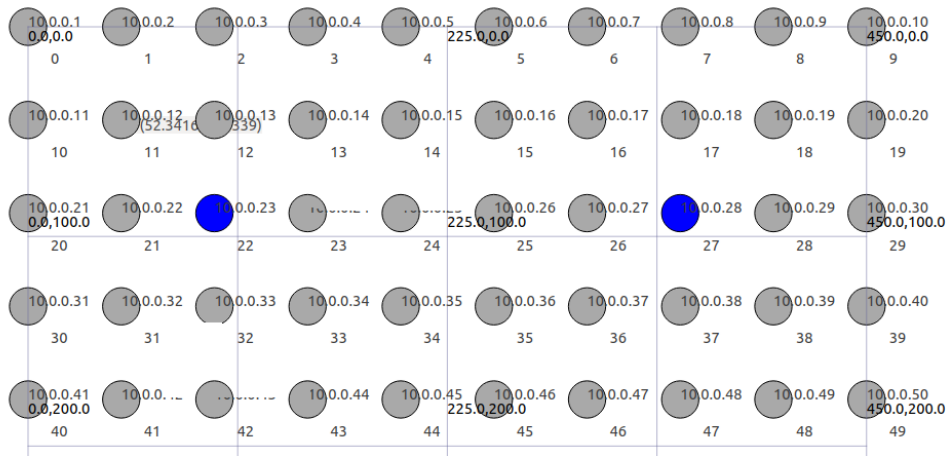


Figure 5.10: Graphical representation; Cluster Maintenance Test 1.

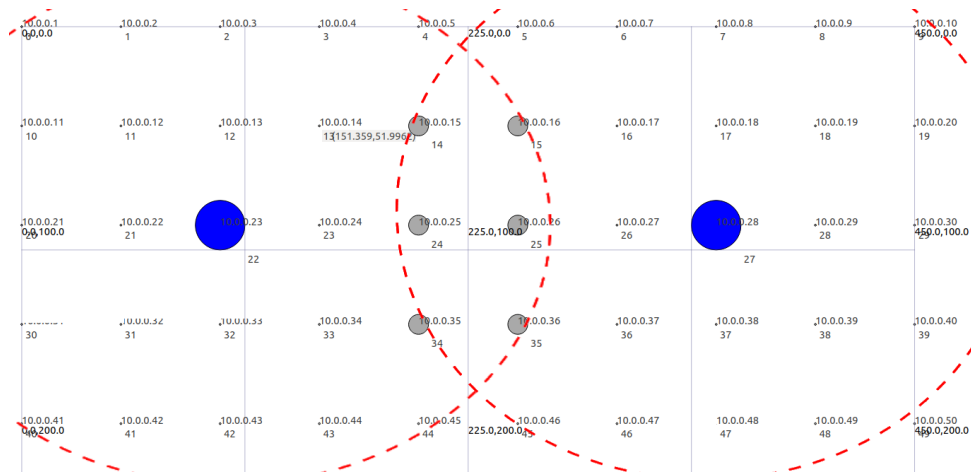


Figure 5.11: Clusters have been formed; 0 - 50s; Cluster Maintenance Test 1.

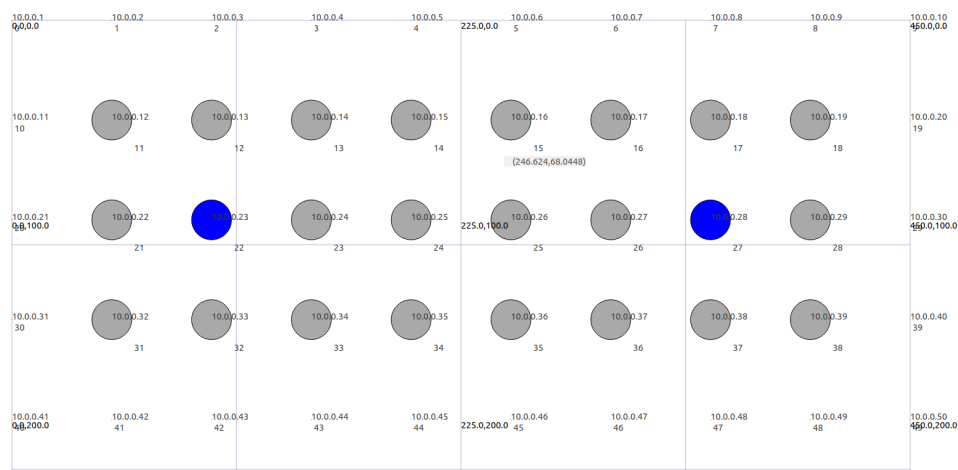


Figure 5.12: Clustering is abandoned; 50s - 100s; Cluster Maintenance Test 1.

Cluster Maintenance Test 2; Control Relinquishment: Assume that we have an initial static grid topology as shown in Figure 5.13 with the simulation parameters shown in Table 5.13. All the nodes have a drop probability of 35% except for nodes 10.0.0.23 and 10.0.0.24 who have 25% and 15% drop rates respectively, and node 10.0.0.28 which has been selected as an intermediate node. The simulation parameters are shown in Table 5.13. The goal of this simulation is to see if the cluster maintenance process will re-establish control to another prospective cluster head if it meets the requirements of equation (5.3), and provides a more appealing $Weight_{node}$ value.

During the first half of the simulation node 10.0.0.24 is excluded from the network as depicted in Figure 5.13, resulting in a reduced network topology as shown in Figure 5.14 during the initial clustering process. During the second half of the simulation node 10.0.0.24 is added back to the network, resulting in control relinquishment to node 10.0.0.24 as the new cluster head due to it exhibiting a better $Weight_{node}$ value. This forces the disbandment of the old cluster and the formation of a new one, resulting in the network structure shown in Figure 5.15. With this new structure, there are three additional gateway nodes.

Table 5.13: Simulation parameters; Cluster Maintenance Test 2

Parameter	Value
Simulation Area; Simulation Time	500m by 250m; Start: 0s & End: 100s
No. of Nodes	50
No. of Sink/Source Node Pairs	0
No. of Selfish Nodes	49
Selfish Node Drop Probability	35%
Node Distribution	Fixed Grid; 50m Spacing
Mobility Model; Node Speed	None; 0 m/s
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Transmission Range	175m
Routing Protocol	Cluster-Based Naïve Bayes Classifier Routing (CB-NBCR)
Transport Protocol; Traffic Type	User Datagram Protocol (UDP); Constant Bitrate (CBR)
Application Throughput	2048 bp/s
Bandwidth; Packet Size	2 Mbp/s; 128 bytes
Hello Enabled; Hello Interval	Yes; 5 s
Trust Threshold	0.5
Neighbour Count Threshold	15
$\alpha_1; \alpha_2$	0.7; 0.3

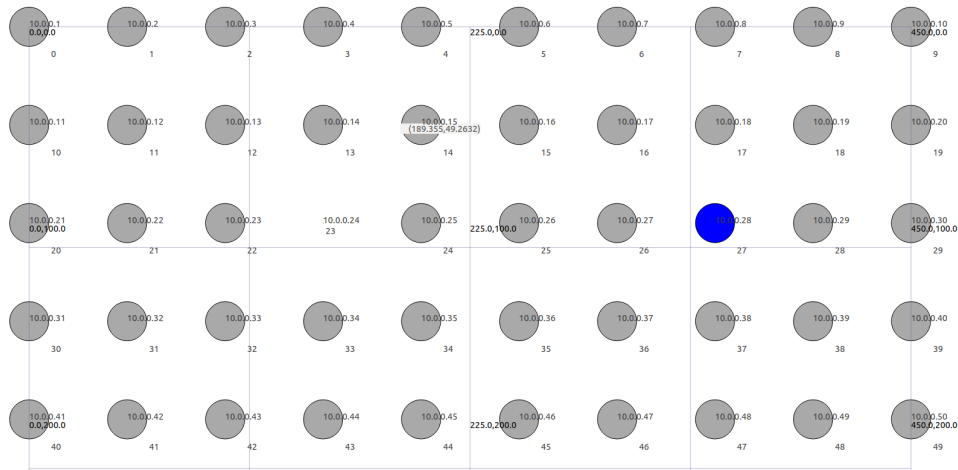


Figure 5.13: Graphical representation; Cluster Maintenance Test 2.

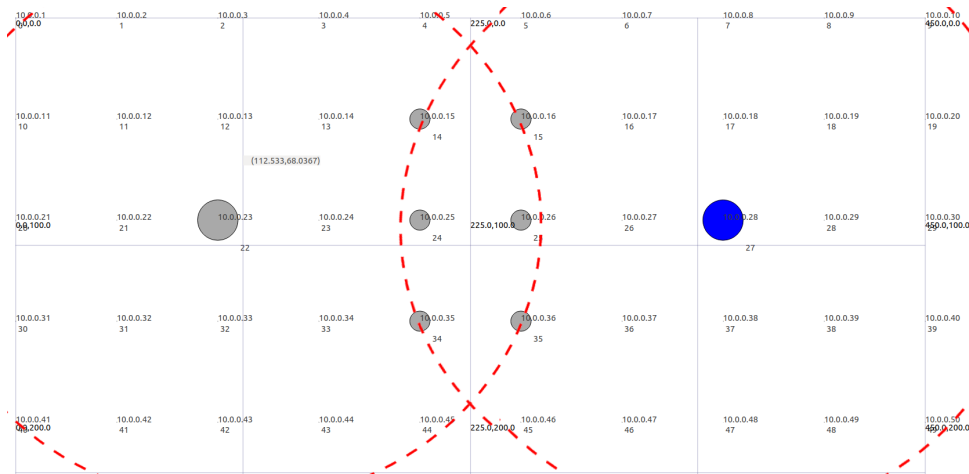


Figure 5.14: Clusters have been formed; 0 - 50s; Cluster Maintenance Test 2.

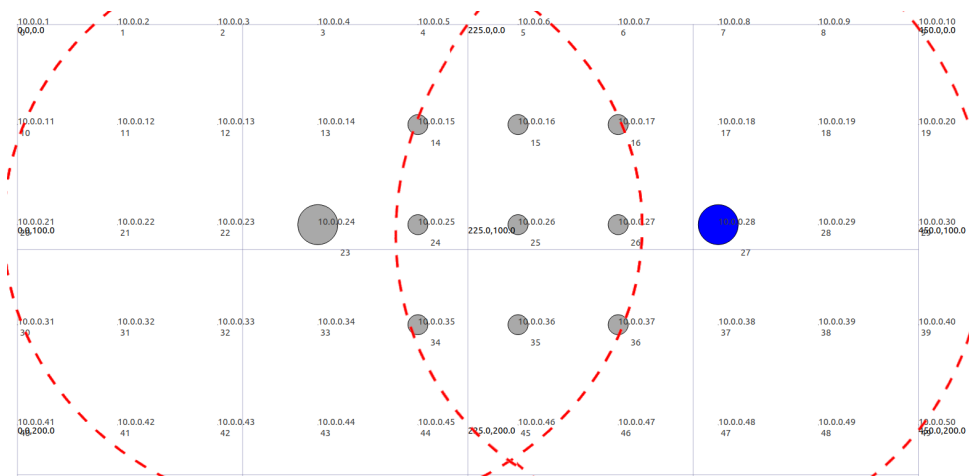


Figure 5.15: Control has been relinquished to a new cluster head; 50s - 100s; Cluster Maintenance Test 2.

5.3 Performance Evaluation

¹ To study the effects of *increased hop count* between source/sink node pairs, the CB-NBCR protocol is simulated under both **static** and **mobile** scenarios with the transmission range of each node chosen explicitly such that it would reach a neighbouring node placed diagonally from it on a fixed grid distribution. This ensures that an increase in network size would result in an increase in hops between source/sink node pairs.²

To study the effects of *increased node density*, the CB-NBCR protocol is once again simulated under both **static** and **mobile** scenarios with the transmission range of each node fixed at 250m regardless of the network size. This ensures an increase in node density between source/sink node pairs as the network size increases.³

Scenario 1; Static: In the first simulation scenario, the CB-NBCR protocol is exposed to a change in network size along with an increase in the number of selfish nodes, as shown by the simulation parameters in Table 5.14 and Table C.5. A fixed grid distribution of 100 nodes up to 400 nodes over an area of 1000m by 1000m is simulated along with an increase in the number of selfish nodes. This increase in selfish nodes is from 0% to 70% of the total amount of nodes in the network in intervals of 10%. The data drop probability of each individual node is randomly selected between 0% and 100%.

Scenario 2; Mobile: In the second simulation scenario, the CB-NBCR protocol is exposed to the exact same simulation parameters as **Scenario 1**, with the exception of assigning a random node velocity of 0 m/s – 25 m/s to each individual node and randomly distributing the nodes within the simulation area.

The results of these simulations are depicted in tabular format by Table C.5 and Table C.6, and graphically by Figure 5.16 to Figure 5.19.

Table 5.14: CB-NBCR simulation parameters; variable

Parameter	Value	
Node Distribution Node Speed Mobility Model Transmission Range	Variable Transmission Range	
	Scenario 1: Fixed Grid	Scenario 2: Mobile
	Fixed Grid	Random
	0 m/s	0 m/s to 25 m/s
	None	Random Waypoint Mobility Model
Node Distribution Node Speed Mobility Model Transmission Range	145m; 100m; 85m; 75m	145m; 100m; 85m; 75m
	Fixed Transmission Range	
	Scenario 1: Fixed Grid	Scenario 2: Mobile
	Fixed Grid	Random
	0 m/s	0 m/s to 25 m/s
Mobility Model Transmission Range	None	Random Waypoint Mobility Model
	250m	250m

¹The evaluation procedure of the CB-NBCR protocol's performance is identical to that of the AODV protocol as well as the NBCR protocol.

²Chapter 2; Figure 2.4

³Chapter 2; Figure 2.5

Table 5.15: CB-NBCR simulation parameters; constant

Parameter	Value
Simulation Area	1000m by 1000m
Simulation Time	Start: 0s; End: 100s
No. of Nodes	100; 200; 300; 400
No. of Sink/Source Node Pairs	10; 20; 30; 40
No. of Selfish Nodes	0% to 70% of total nodes in intervals of 10%
Selfish Node Drop Probability	0 to 100 %
MAC Protocol; WiFi Channel	802.11b WiFi Standard; Yans WiFi
Propagation Loss Model	Range Propagation Loss Model
Propagation Delay Mode	Constant Speed Propagation Delay Model
Routing Protocol	Cluster-based Naïve Bayes Classifier Routing (CB-NBCR)
Traffic Type	Constant Bitrate (CBR)
Transport Protocol	User Datagram Protocol (UDP)
Application Throughput	2048 bp/s
Bandwidth	2 Mbps
Packet Size	128 bytes
Hello Enabled; Hello Interval;	No; 0 s
Trust Threshold	0.5
Neighbour Count Threshold	15
$\alpha_1; \alpha_2$	0.7; 0.3

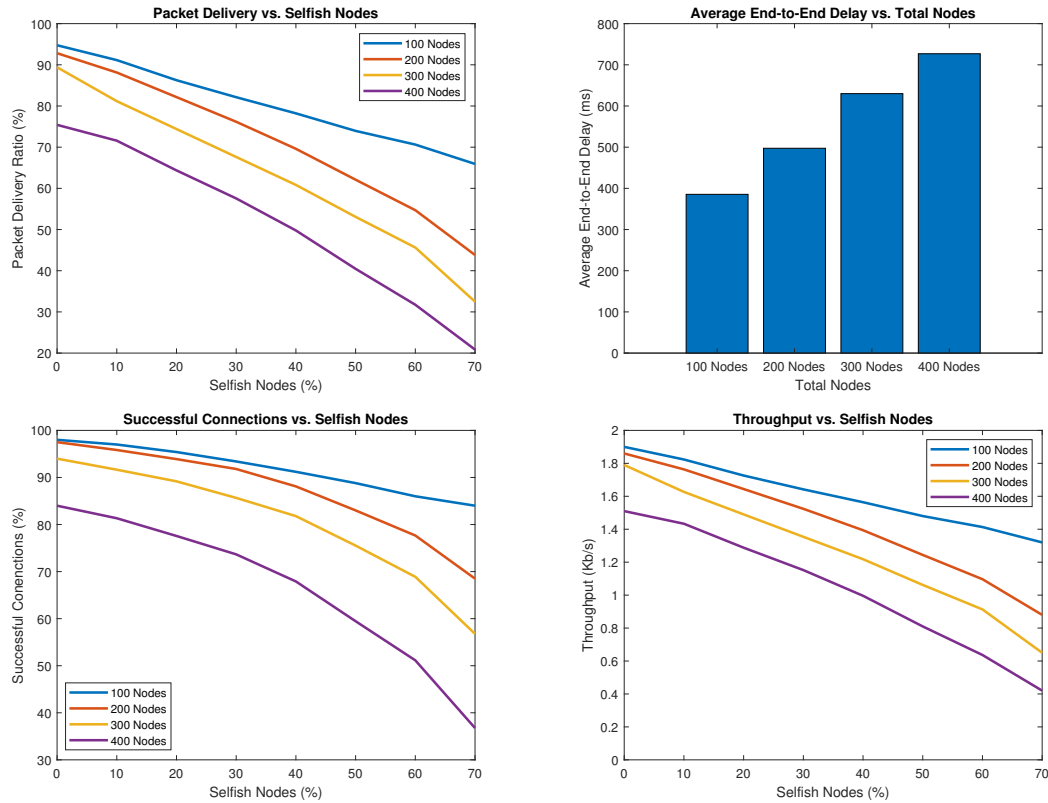


Figure 5.16: CB-NBCR simulation results; variable transmission range; static.

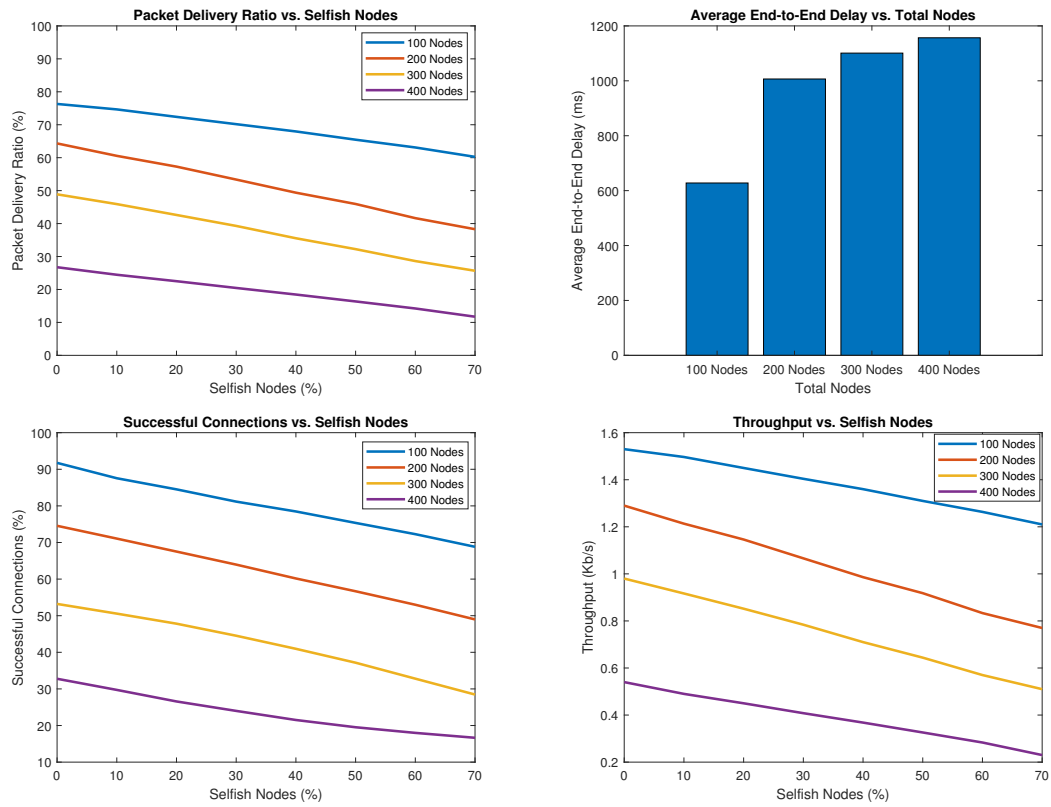


Figure 5.17: CB-NBCR simulation results; variable transmission range; mobile.

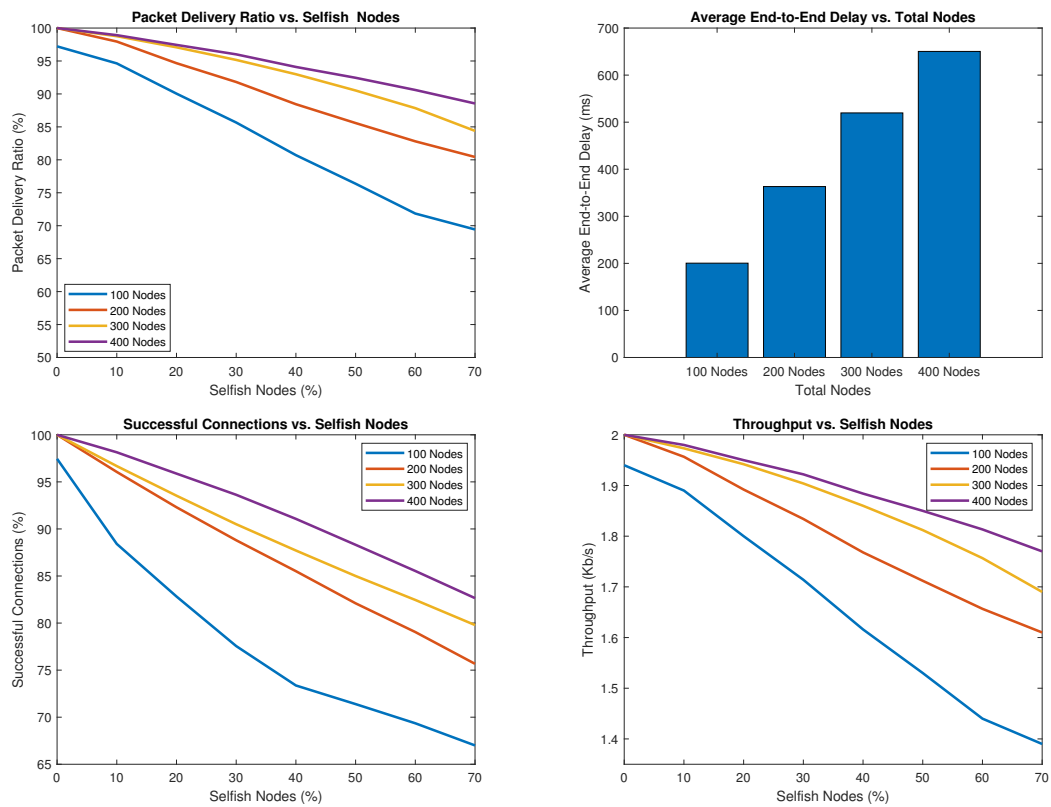


Figure 5.18: CB-NBCR simulation results; fixed transmission range; static.

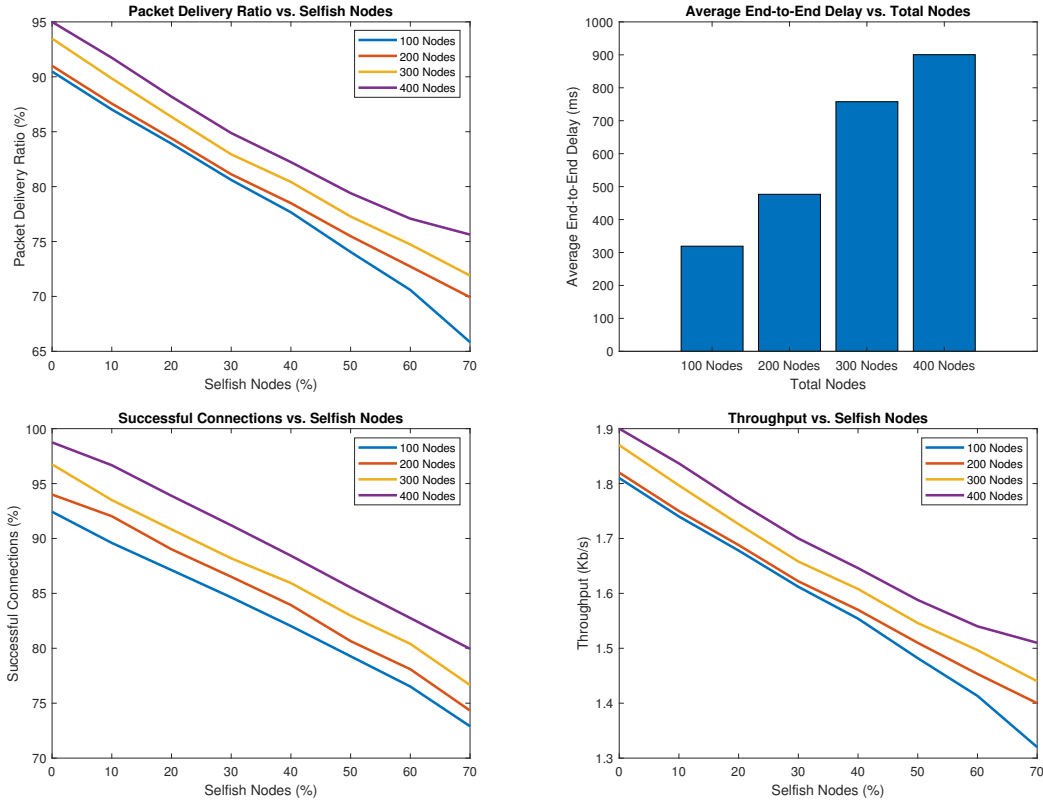


Figure 5.19: CB-NBCR simulation results; fixed transmission range; mobile.

5.4 Summary

5.4.1 Protocol Operation

From the preceding sections, a summarized version of how the CB-NBCR protocol forms clusters is given by the following steps:

1. During the exchange of *Hello* packets between nodes, additional information with regards to the weight $Weight_{node}$ of each node is added to the header of these packets. This weight is given by equation (5.1) as

$$Weight_{node} = \alpha_1 * \left(\frac{25 - Velocity_{node}}{25} \right) + \alpha_2 * Trust_{node}$$

This information is documented in each node's *Neighbour Table*.

2. Once the *First Auxiliary Timer* expires, cluster head selection takes place if a node has the minimum required number of neighbours, as given by equation (5.3)

$$Neighbours_{node} > Neighbours_{threshold}$$

, and exhibits a suitable $Weight_{node}$ value with respect to its neighbours.

3. Once the *Secondary Auxiliary Timer* expires, cluster head selection takes place based on the topology of the network.
4. Every expiration of the *Hello Timer* onwards from initial cluster creation repeats the first step- exchanging data between neighbours. Once this exchange has happened, the *First Auxiliary Timer* initiates cluster maintenance.

5.4.2 Operational Analysis

Multiplier Values: The multiplier values test showed that node mobility has a greater impact than node trust factor when forming dependable topologies through clustering. In the scenario used to conduct this test, the most suitable values for α_1 and α_2 are 0.7 and 0.3, respectively.

Neighbour Count Threshold : The neighbour count threshold test was conducted to determine at which node densities clustering would be beneficial. The results of the simulation show that having a small neighbour count threshold¹ will result in clusters appearing at low node densities where dependable topologies cannot be formed. This results in a decrease in network performance.

When the neighbour count threshold is too large clusters will form very infrequently, or not at all. This will result in the CB-NBCR protocol performing in the same manner as the NBCR protocol, with the exception of having the added deteriorating effects of redundant control packet transmissions within discrete intervals.

However, an improvement in network performance has been found at node densities where nodes have at least 15 neighbours for this particular scenario.

Clustering Validation: From the cluster creation test we see that the protocol reduces a complex topology to a more manageable equivalent through the use of opportunistic clustering. Once clusters have formed, but no longer meet the requirements of (5.3), they will disband as shown by the first cluster maintenance test. The second cluster maintenance test shows that when a new node has entered the region of an existing cluster and has a more appealing $Weight_{node}$ value, the existing cluster will disband and a new cluster will be formed with the new node selected as its cluster head.

5.4.3 Performance Analysis

We highlight the following insights with regards to the performance metrics of the CB-NBCR protocol:

¹The minimum number of neighbouring nodes required for clustering to take place. See equation (5.3).

Packet Delivery Ratio: The packet delivery ratio sees a decrease in network performance in the presence of selfish nodes for both fixed and variable transmission range configurations. The results show that an increase in hop count for both static and mobile scenarios leads to a deterioration in packet delivery ratio, leading to a decrease in performance as network size increases. However, we see that an increase in node density under the same scenarios lead to an increase in network performance due to selective clustering. The consequence thereof is that larger networks (higher node density) perform noticeably better than smaller networks (lower node density).

Average End-to-End Delay: Average end-to-end delay increases with an increase in hop count (variable transmission range) and node density (fixed transmission range). This is due to the fact that larger networks bring about more RREQ flooding during the route discovery process. However, we see the largest overall average end-to-end delay in a mobile scenario with networks exhibiting greater hop counts between source/sink node pairs.

Successful Connections: The amount of successful connections are similar to the packet delivery ratio, and also see a decrease when the amount of selfish nodes are increased for both fixed transmission range and variable transmission range configurations. On larger networks with a fixed transmission range configuration and a static grid topology, the amount of successful connections are more than for smaller networks due to an increase in alternative routes that become available. However, smaller networks benefit more when a variable transmission range configuration is used due to a lower hop count. Generally, more dense networks provide better clustering opportunities and therefore see more successful connections formed.

Throughput: Since the application throughput is merely 2Kbps and the bandwidth is 2Mbps for each node, congestion is highly unlikely- leaving the throughput in direct correlation with the packet delivery ratio. The throughput decreases as the number of selfish nodes increase for both fixed and variable transmission range configurations. However, an increase in node density leads to an increase in throughput due to selective clustering, as expected¹.

5.4.4 Final Remarks

The CB-NBCR protocol has aimed to tackle high-density networks and to reduce complex network structures to their more dependable and manageable equivalence. The results discussed in the preceding subsections show that the protocol performs as expected. A comparative analysis between the performance of AODV, NBCR and CB-NBCR is presented in Chapter 6.

¹A larger packet size would inadvertently affect packet delivery ratio, average end-to-end delay and throughput negatively on larger networks.

Chapter 6

Conclusion and Future Work

This chapter provides a comparative analysis between the AODV protocol, the NBCR protocol, and the CB-NBCR protocol- highlighting the key differences in performance results of all three.

6.1 Analysis

6.1.1 Overview of Results

To compare the AODV, NBCR, and CB-NBCR protocols, results obtained for each evaluation metric under the specified simulation constraints are presented graphically from Figure 6.1 to Figure 6.13, with their tabular equivalence shown from Table D.1 to Table D.4.

Packet Delivery Ratio: All three protocols exhibit deterioration in terms of packet delivery ratio under the constraints of increased number of selfish nodes. With a variable transmission range configuration (increased hop count) the NBCR and CB-NBCR protocols both outperform AODV under mobile and static scenarios, with the CB-NBCR showing a slightly worse performance than the NBCR protocol due to the added effects of redundant control packets. When a fixed transmission range configuration is used (increased node density) along with a static grid topology, the NBCR protocol performs equally as well as the CB-NBCR protocol with marginal difference. However, once mobility is introduced the CB-NBCR protocol has an improved performance over AODV and NBCR in a highly dense network where the opportunities for clustering are present.

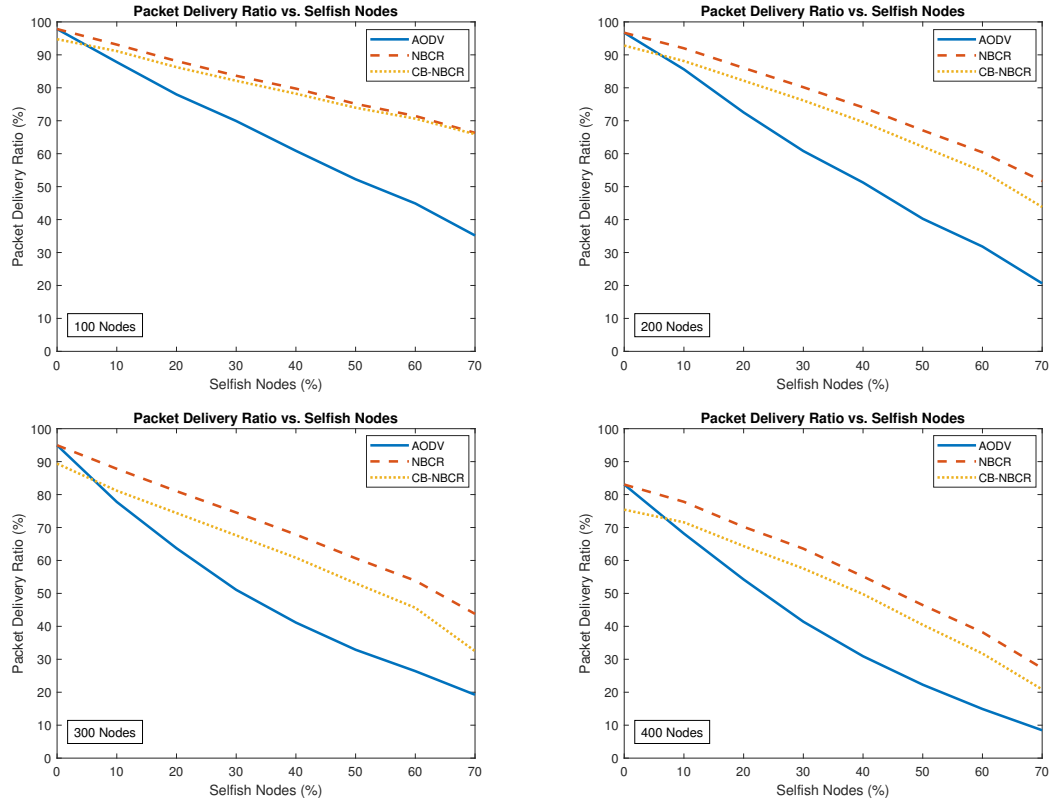


Figure 6.1: Packet delivery ratio simulation results; variable transmission range; static.

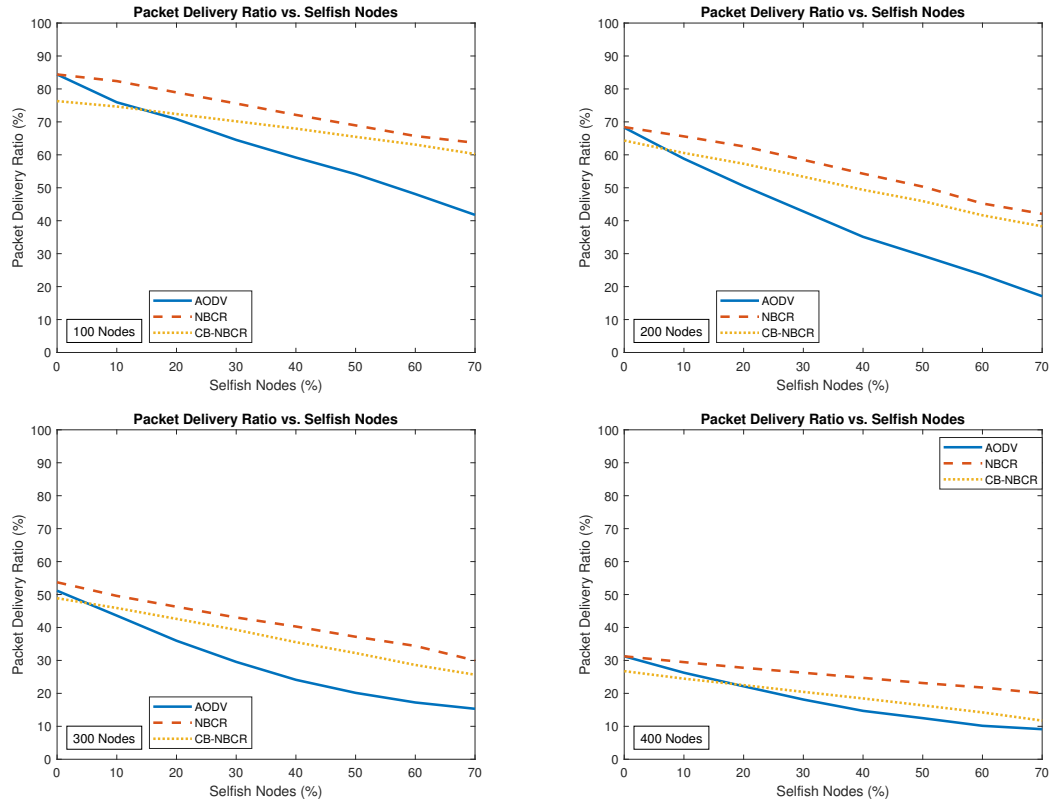


Figure 6.2: Packet delivery ratio simulation results; variable transmission range; mobile.

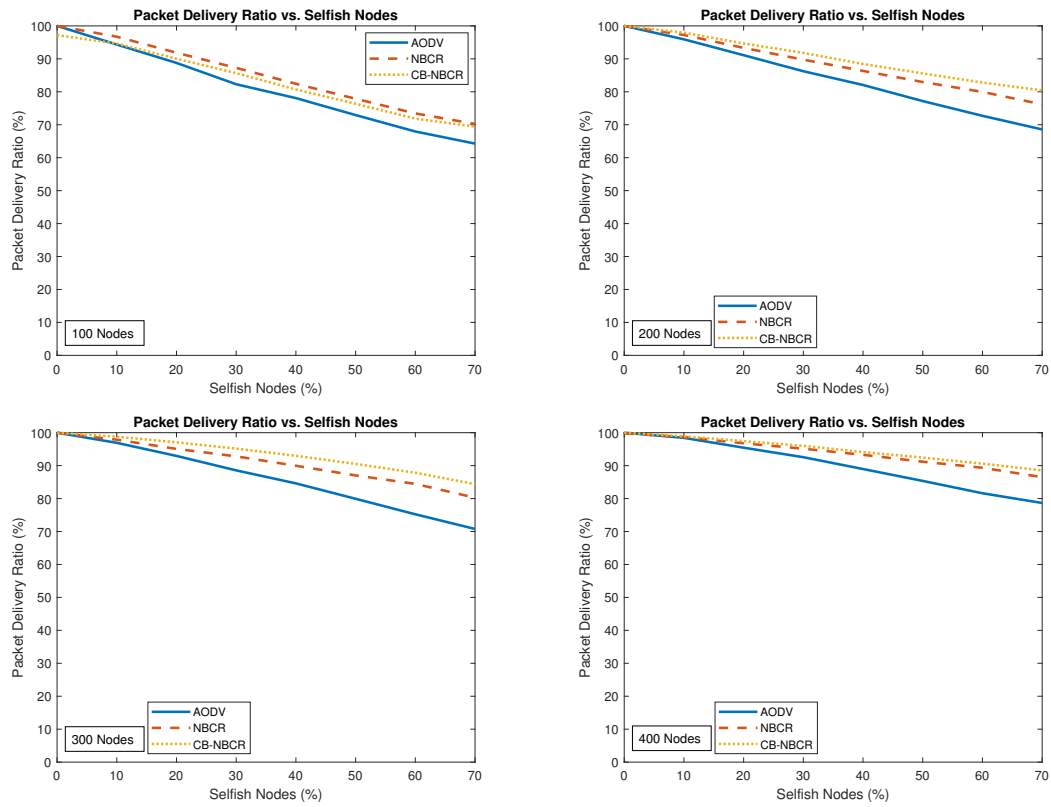


Figure 6.3: Packet delivery ratio simulation results; fixed transmission range; static.

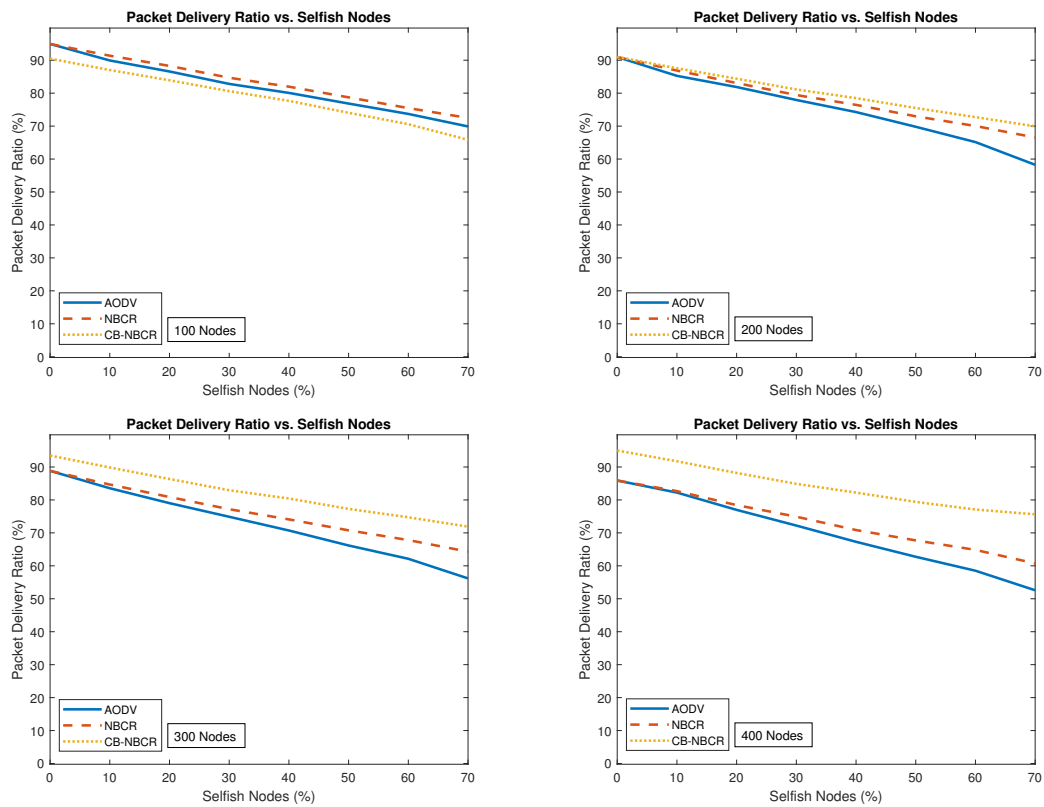


Figure 6.4: Packet delivery ratio simulation results; fixed transmission range; mobile.

Average End-to-End Delay: As the network size is increased for a variable transmission range configuration more hops are introduced between source and sink node pairs, leading to an increase in average end-to-end delay for all three protocols. Since the NBCR protocol prioritizes routes with better delivery probabilities instead of lowest hop count, it shows a larger increase in average end-to-end delay on both static and mobile scenarios in comparison to AODV when the number of nodes are increased. However, this average end-to-end delay is better than AODV when a fixed transmission range configuration is used for both mobile and static scenarios. This is because the NBCR protocol isolates multiple selfish nodes from the network within a single RREQ transmission when high node densities are present. Since the CB-NBCR protocol additionally makes use of *Hello* packet propagation and a number of additional control packets, it has the highest end-to-end delay in all scenarios.

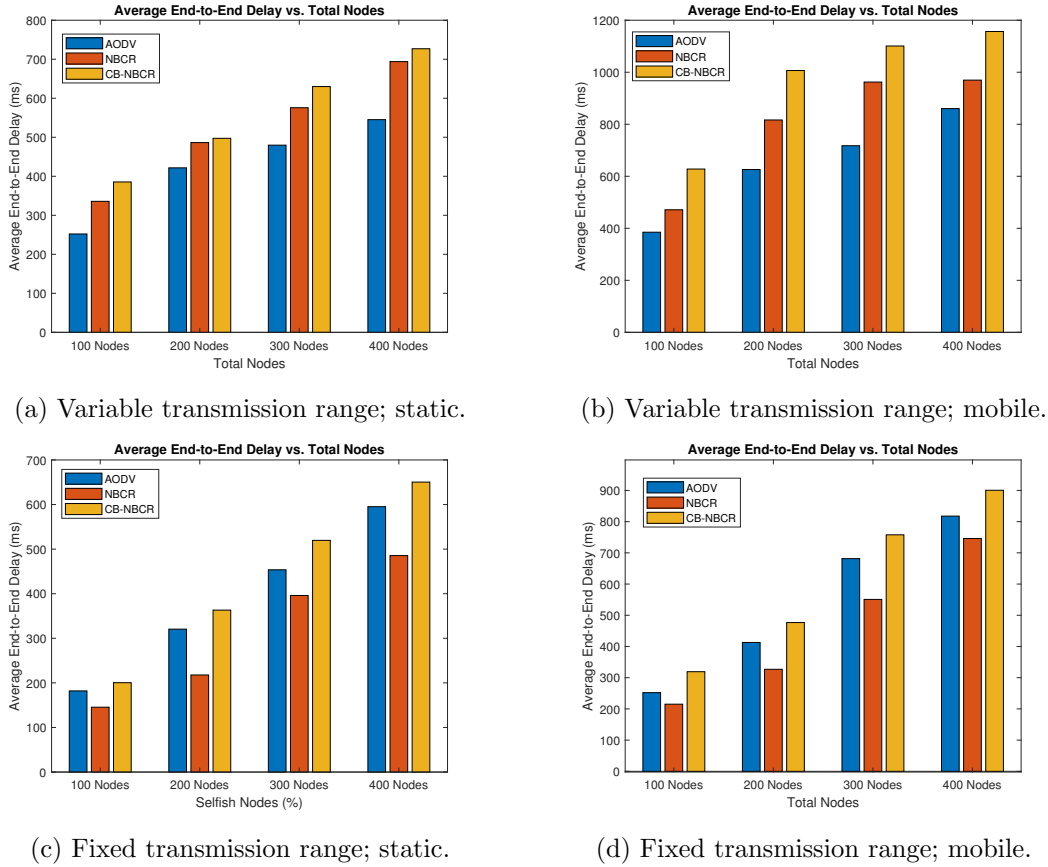


Figure 6.5: Average end-to-end delay simulation results

Successful Connections: With an increase in network size and number of selfish nodes, all three protocols experience a decrease in the number of successful connections for a fixed transmission range configuration. The NBCR protocol performs similar to that of the CB-NBCR protocol under static conditions, but once mobility is introduced the NBCR protocol once again performs worse than CB-NBCR. When a variable transmission range configuration is used the NBCR protocol performs similar to the CB-NBCR protocol, performing better than AODV in both static and mobile scenarios.

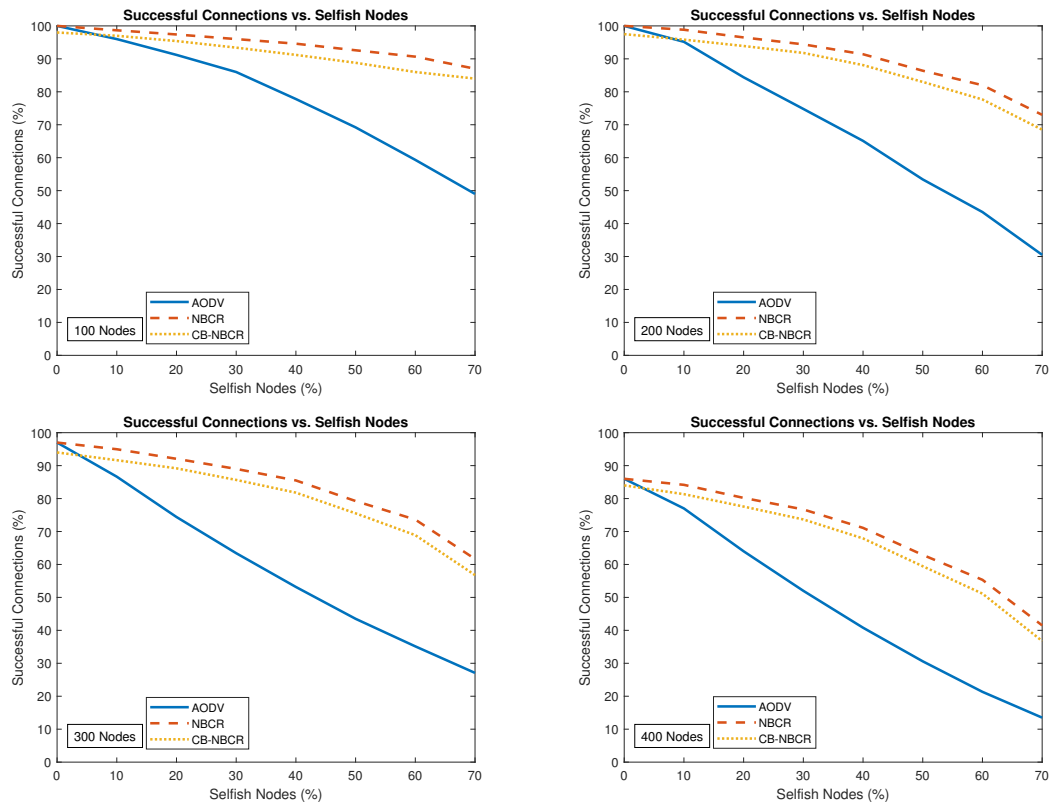


Figure 6.6: Successful connections simulation results; variable transmission range; static.

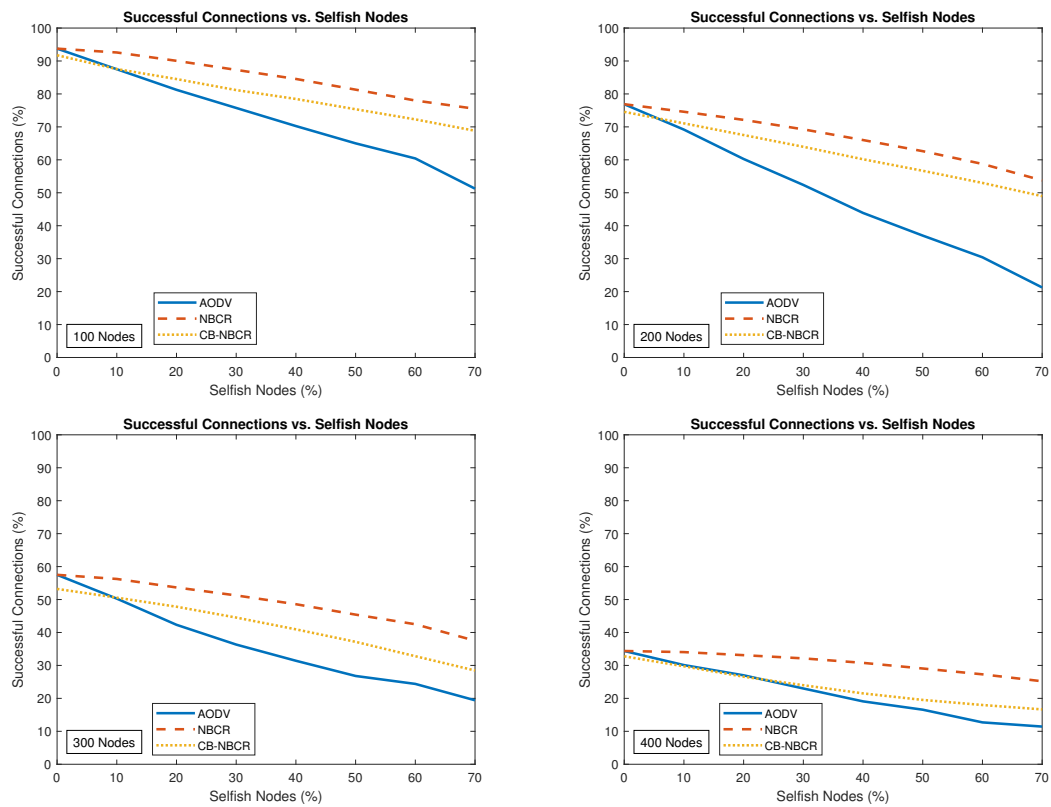


Figure 6.7: Successful connections simulation results; variable transmission range; mobile.

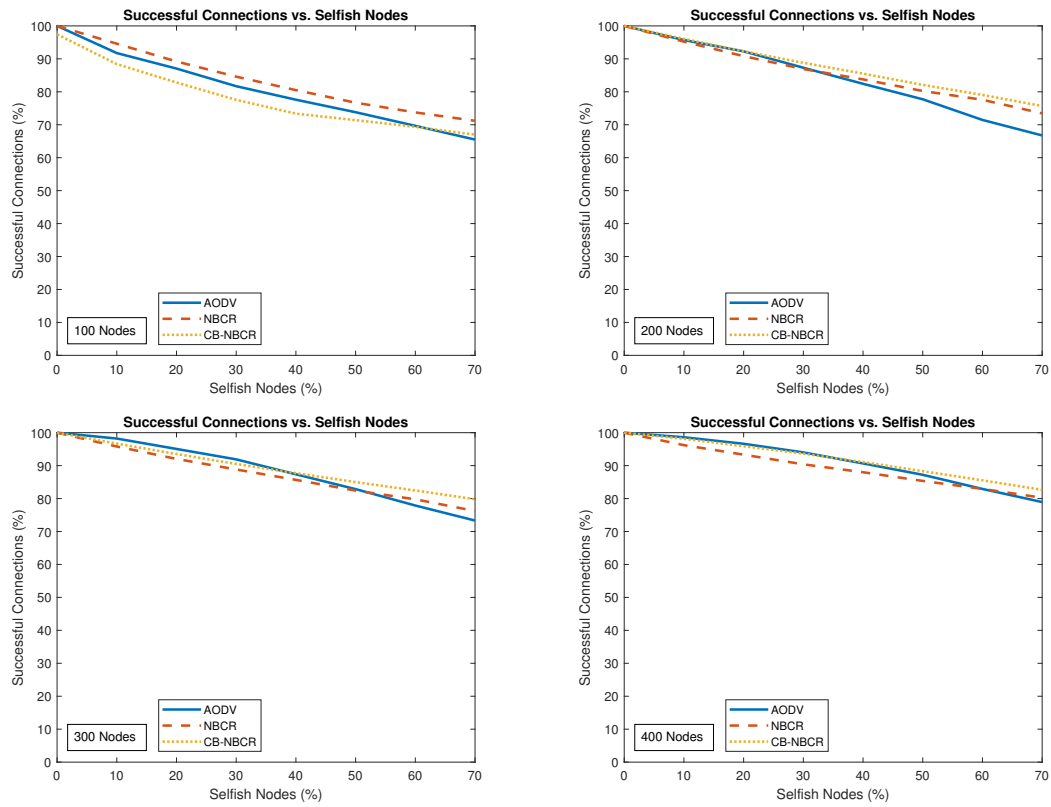


Figure 6.8: Successful connections simulation results; fixed transmission range; static.

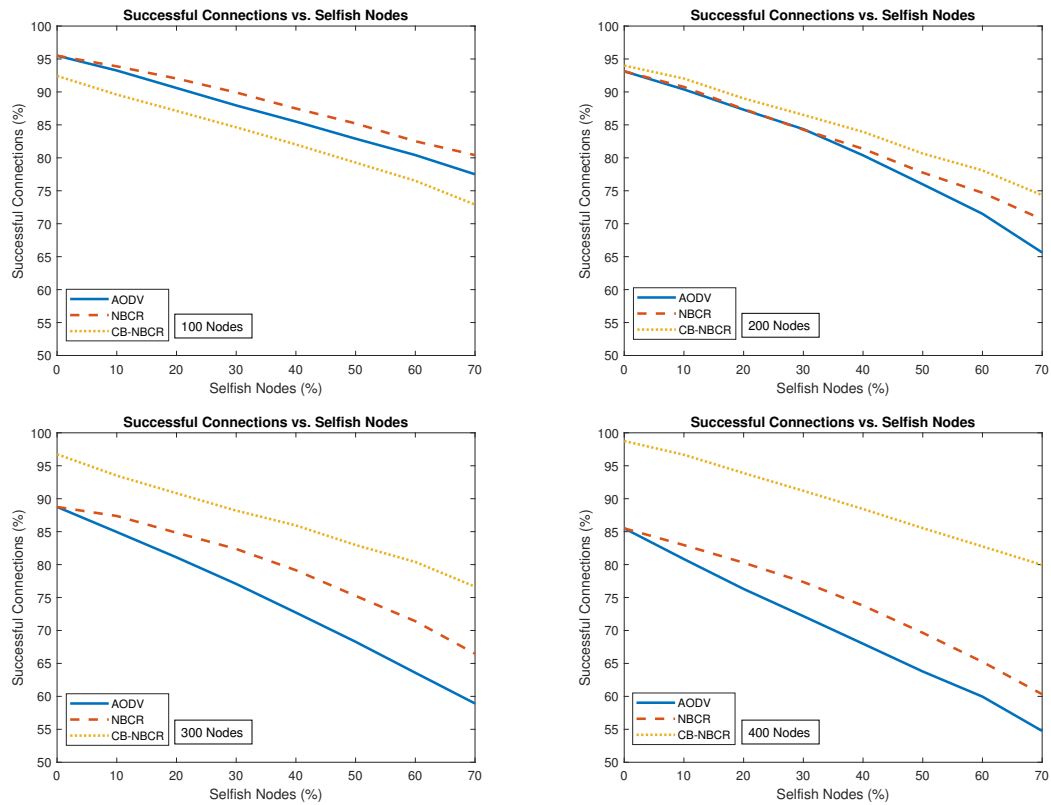


Figure 6.9: Successful connections simulation results; fixed transmission range; mobile.

Throughput : Since the application throughput is merely 2 Kb/s with a bandwidth of 2 MB/s for each node, congestion is highly unlikely. This means that the throughput is in direct correlation with the packet delivery ratio. An increase in network size and selfish nodes yield a decrease in throughput for all three protocols under static grid and mobility scenarios using a variable transmission range configuration. Using a fixed transmission range configuration the NBCR protocol performs equally as well as the CB-NBCR protocol with marginal difference with a static grid topology, but performs more poorly once mobility is introduced. As with packet delivery ratio, the CB-NBCR protocol outperforms both AODV and NBCR when mobility is present in highly dense network configurations.

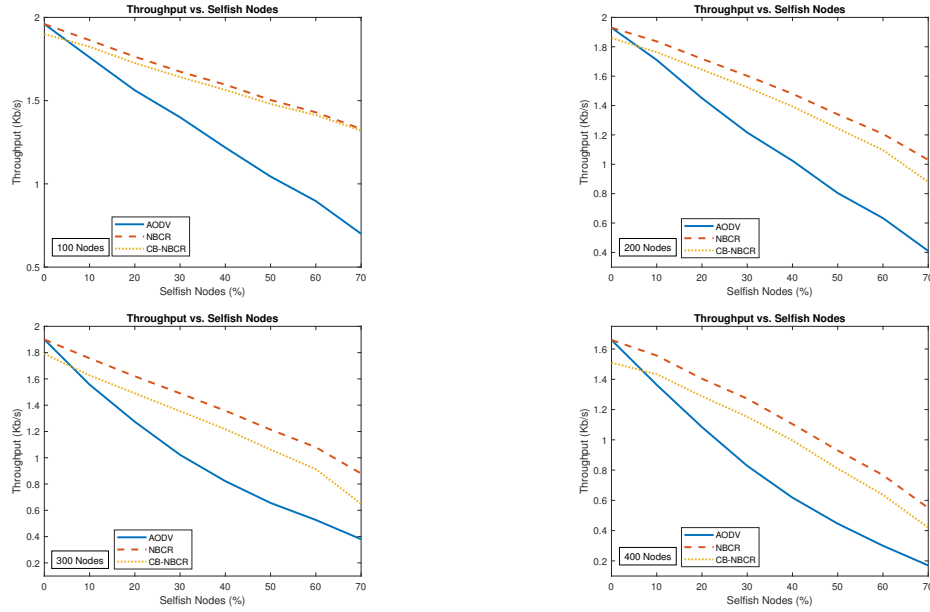


Figure 6.10: Throughput simulation results; variable transmission range; static.

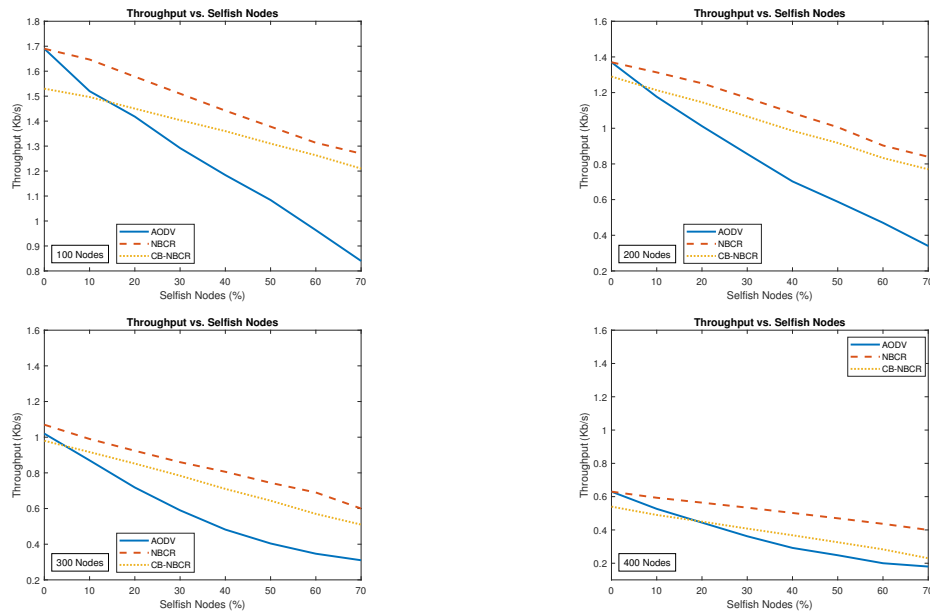


Figure 6.11: Throughput simulation results; variable transmission range; mobile.

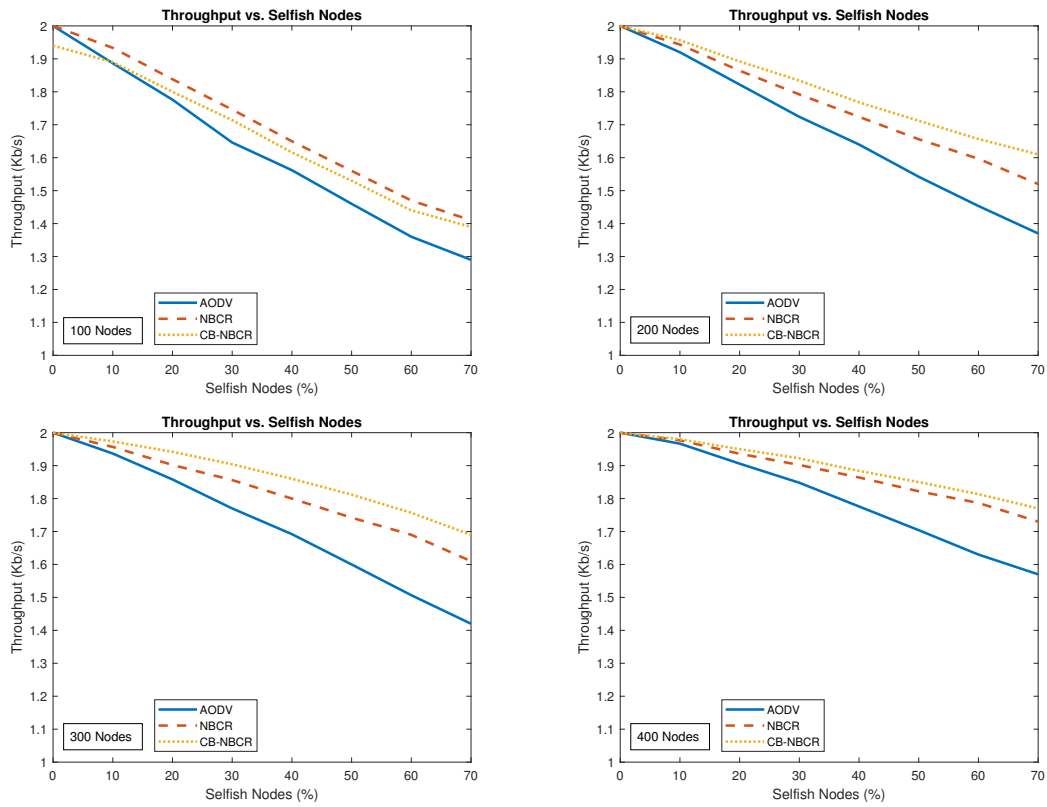


Figure 6.12: Throughput simulation results; fixed transmission range; static.

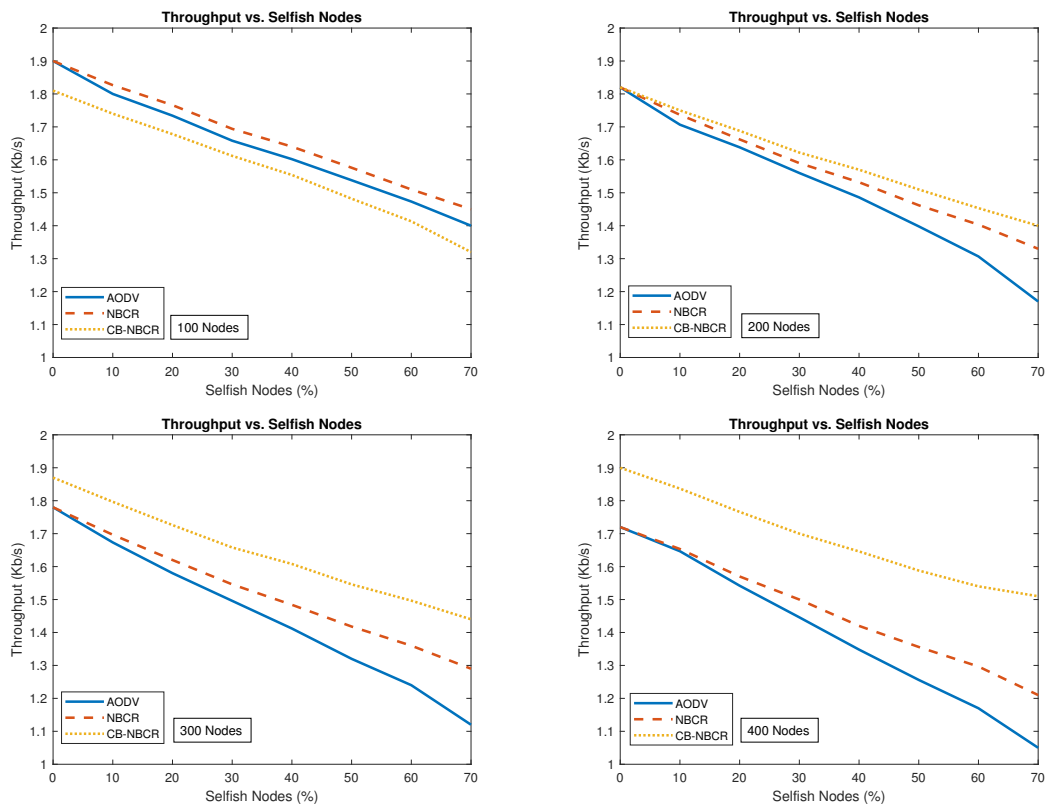


Figure 6.13: Throughput simulation results; fixed transmission range; mobile.

6.2 Final Remarks

The CB-NBCR and NBCR protocols have both outperformed traditional AODV in most aspects, with the exception of the CB-NBCR protocol displaying a significant increase in overall average end-to-end delay over both AODV and NBCR. Observations made with the regards to the simulation results obtained are shown in Table 6.1, along with the most suitable network configurations for each protocol in Table 6.2.

Table 6.1: Observations made with regards to the simulation results.

#	Observation	Explanation
1	CB-NBCR is marginally outperformed by NBCR when using a variable transmission range configuration, as well as by AODV when no selfish nodes are present.	Low node densities and the absence of selfish nodes prohibits clusters to be formed, forcing the CB-NBCR protocol to perform in the same fashion as NBCR with the addition of redundant control packages.
2	All three protocols see a decrease in network performance with regards to all metrics once mobility is introduced.	Mobility causes frequent link breakages in established connections due to a constantly changing topology.
3	The network performance increases for all three protocols as the network size is increased for a fixed transmission range configuration using a static topology.	An increase in network size for this specific case creates an increase in alternative routes that remain constant due to the static nature of the nodes.
4	NBCR has a higher overall average end-to-end delay than AODV when a variable transmission range configuration is used, but exhibits a lower overall average end-to-end delay when a fixed transmission range configuration is used.	When a variable transmission range configuration is used, an increase in network size leads to an increase in hop count between source/sink node pairs. NBCR prioritizes routes with better probabilities instead of hop count, leading to an increase in end-to-end delay. However, when a fixed transmission range configuration is used an increase in network size leads to higher node densities, increasing the amount of selfish nodes that are isolated by a single instance of RREQ propagation.
5	CB-NBCR initially performs marginally worse than NBCR when a fixed transmission range configuration is used, but outperforms NBCR on larger networks for a static grid topology.	Smaller networks do not provide node densities suitable for clustering, causing a slight performance deterioration due to the redundant transmission of control packets within discrete intervals.
6	CB-NBCR performs better on larger networks when a fixed transmission range configuration is used.	When a fixed transmission range configuration is used, an increase in network size leads to higher node densities. This is beneficial to the opportunistic clustering design of the CB-NBCR protocol, and respectively creates an increase of opportunities for sensible clusters to be formed.

Table 6.2: Overview of suitable applications for each protocol.

Protocol	Suitable Application
AODV	High density network with a static grid topology and no selfish/dysfunctional nodes.
NBCR	Low density network with multiple hops between source/sink pairs featuring selfish/dysfunctional nodes and node mobility.
CB-NBCR	High density network featuring mobile nodes as well as selfish/dysfunctional nodes.

Further Recommendations for NBCR: The NBCR protocol serves as a robust solution for the reliable discovery of routes in large-scale multi-hop networks exhibiting low node densities, outperforming traditional AODV in every aspect except average end-to-end delay. Further recommendations may include:

1. Consider using a moving window of recent values instead of a fixed set of data for the classifier to ensure more accurate predictions.
2. Consider using different variables for the feature vector and/or response vector to cater for more specific scenarios and functionality.
3. Consider adjusting the *Selfish Node Threshold* value to be better suited for different network configurations, preventing the isolation of selfish nodes needed to form connections.

Further Recommendations for CB-NBCR: The CB-NBCR protocol serves as an extension of the NBCR protocol by providing a clustering overlay to reduce dense networks to more manageable topologies- especially when mobility is present. Further recommendations may include:

1. Consider using the route discovery process as a trigger for cluster creation and/or maintenance instead of the expiration of the *Hello Timer*, creating more recent cluster topologies in a network with mobile nodes.
2. Consider experimenting with various *Hello Intervals* to determine the best results for different network sizes and configurations.
3. Consider controlling the maximum amount of nodes that may form part of a cluster.

The CB-NBCR protocol has proven itself a suitable solution for achieving the goals set in Chapter 2. The simulation results have shown that the CB-NBCR protocol is well suited for large scale networks exhibiting a high node density, as well as the added effects of mobility and adverse node failures. However, the CB-NBCR protocol operates at the expense of a significant increase in average end-to-end delay.

Bibliography

- [1] M. Ilyas, *The Handbook of Ad Hoc Wireless Networks*, 1st ed. CRC Press, 2003.
- [2] M. Conti and S. Giordano, “Mobile ad hoc networking: Milestones, challenges, and new research directions,” *IEEE Communications Magazine*, vol. 52, no. 1, 2014.
- [3] A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, “Better approach to mobile ad-hoc networking (B.A.T.M.A.N.),” Internet Engineering Task Force / Internet Engineering Task Force, Internet-Draft draft-wunderlich-openmesh-manet-routing-00, Apr. 2008.
- [4] J. Chroboczek, “Applicability of the Babel routing protocol,” Internet Engineering Task Force / Internet Engineering Task Force, Internet-Draft draft-ietf-babel-applicability-06.
- [5] S. R. Das, C. E. Perkins, and E. M. Belding-Royer, “Ad hoc on-demand distance vector (AODV) routing,” no. 3561, Jul. 2003.
- [6] C. E. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers,” in *Proceedings of the Conference on Communications Architectures, Protocols and Applications*, ser. SIGCOMM ’94. New York, NY, USA: Association for Computing Machinery, 1994.
- [7] T. K. Saini and S. C. Sharma, “Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept,” *Ad Hoc Networks*, vol. 103, 2020.
- [8] George F. Riley, “Simulation of Large Scale Networks II: Large-Scale Network Simulations with GTNetS,” in *Proceedings of the 35th Conference on Winter Simulation: Driving Innovation*, ser. WSC ’03. Winter Simulation Conference, 2003.
- [9] J. Heidemann, N. Bulusu, J. Elson, C. Intanagonwiwat, K.-c. Lan, Y. Xu, W. Ye, D. Estrin, and R. Govindan, “Effects of detail in wireless network simulation,” in *Proceedings of the SCS Multiconference on Distributed Simulation*. Phoenix, Arizona, USA: Society for Computer Simulation, 2001.
- [10] D. Cavin, Y. Sasson, and A. Schiper, “On the accuracy of MANET simulators,” in *Proceedings of the Second ACM International Workshop on Principles of Mobile Computing*, ser. POMC ’02. New York, NY, USA: Association for Computing Machinery, 2002.

- [11] S. Khan, B. Aziz, S. Najeeb, A. Ahmed, M. Usman, and S. Ullah, "Reliability of network simulators and simulation based research," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2013.
- [12] G. Borboruah and G. Nandi, "A study on large scale network simulators," *International Journal of Computer Science and Information Technologies*, vol. 5, 2014.
- [13] L. Hogie, P. Bouvry, and F. Guinand, "An overview of MANETs simulation," *Electronic Notes in Theoretical Computer Science*, vol. 150, no. 1, 2006.
- [14] R. Patel, "Survey on network simulators," *International Journal of Computer Applications*, vol. 182, 2018.
- [15] I. Minakov, R. Passerone, A. Rizzardi, and S. Sicari, "A comparative study of recent wireless sensor network simulators," *ACM Transactions on Sensor Networks*, vol. 12, no. 3, 2016.
- [16] T. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Palma, "A survey of various propagation models for mobile communication," *Antennas and Propagation Magazine, IEEE*, vol. 45, 2003.
- [17] I. Stepanov, D. Herrscher, and K. Rothermel, "On the impact of radio propagation models on MANET simulation results," In: *Proceedings of the 7th IFIP International Conference on Mobile and Wireless Communication Networks (MWCN 2005), Marrakech, Morocco, September 2005*, Sep. 2005.
- [18] M. Nisar, A. Mehmood, and A. Nadeem, "A review and performance analysis of mobility models for MANETs: A case study," in *Research Journal of Recent Sciences*, vol. 3, Sep. 2013.
- [19] Jing Tian, J. Hahner, C. Becker, I. Stepanov, and K. Rothermel, "Graph-based mobility model for mobile ad hoc network simulation," in *Proceedings 35th Annual Simulation Symposium. SS 2002*, 2002.
- [20] G. Naah and E. Boadu, "Clustering effects on wireless mobile ad-hoc networks performances," *International Journal of Computer Science and Information Technology*, vol. 6, 2014.
- [21] B. A. Correa, L. Ospina, and R. C. Hincapi  , "Survey of clustering techniques for mobile ad hoc networks," *Revista Facultad de Ingenier  a Universidad de Antioquia*, 2007.
- [22] S. Dhamodharavadhani, "A survey on clustering based routing protocols in Mobile ad hoc networks," in *2015 International Conference on Soft-Computing and Networks Security (ICSNS)*, 2015.
- [23] E. Eells, "Review: Bayes's theorem," *Oxford Mind*, vol. 113, no. 451, Jul. 2004.

- [24] J. Kundu, K. Majumder, and D. De, "Design and analysis of an efficient trust management scheme for clustered based MANET using Bayesian method," *2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, 2015.
- [25] M. de Leoni, M. Mecella, and R. Russo, "A Bayesian Approach for Disconnection Management in Mobile Ad Hoc Networks," *16th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2007)*, 2007.
- [26] R. Behera and K. Das, "A Survey on Machine Learning: Concept, Algorithms and Applications," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, Feb. 2017.
- [27] D. Barber, *Bayesian Reasoning and Machine Learning*. Cambridge: Cambridge University Press, 2012.
- [28] R. Jain, M. Parameswaran, and C. Hota, "An efficient on-demand routing protocol for MANETs using Bayesian approach," *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, 2011.
- [29] S. N. Shah and R. H. Jhaveri, "A trust-based scheme against Packet dropping attacks in MANETs," *2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, 2016.
- [30] Z. El-Bazzal, M. Kadoch, B. L. Agba, F. Gagnon, and M. Bennani, "A flexible weight based clustering algorithm in mobile ad hoc networks," in *2006 International Conference on Systems and Networks Communications (ICSNC'06)*, 2006.
- [31] J. Hsu, S. Bhatia, K. Tang, R. Bagrodia, and M. Acriche, "Performance of mobile ad hoc networking routing protocols in large scale scenarios," *IEEE MILCOM 2004. Military Communications Conference.*, 2004.
- [32] H. K. Ong, H. L. Ong, E. R. Tee, and R. Sureswaran, "Scalability study of ad-hoc wireless mobile network routing protocol in sparse and dense networks," in *The 2nd International Conference on Distributed Frameworks for Multimedia Applications*, 2006.
- [33] P. Goyal, "Simulation study of comparative performance of AODV, OLSR, FSR LAR, routing protocols in MANET in large scale scenarios," in *2012 World Congress on Information and Communication Technologies*, 2012.
- [34] M. Ikeda, M. Hiyama, E. Kulla, and L. Barolli, "Mobile ad-hoc network routing protocols performance evaluation using NS-3 simulator," in *2011 Third International Conference on Intelligent Networking and Collaborative Systems*, 2011.
- [35] A. Zakrzewska, L. Koszalka, and I. Pozniak-Koszalka, "Performance study of routing protocols for wireless mesh networks," in *2008 19th International Conference on Systems Engineering*, 2008.

Appendix A

Ad Hoc On-Demand Distance Vector Routing

A.1 Performance Evaluation

Table A.1: AODV simulation results; variable transmission range.

Selfish Nodes (%)	Scenario 1: Static				Scenario 2: Mobile			
	100 Nodes	200 Nodes	300 Nodes	400 Nodes	100 Nodes	200 Nodes	300 Nodes	400 Nodes
	Packet Delivery Ratio (%)							
0	97.83	96.71	94.97	83.04	84.40	68.26	51.16	31.25
10	87.25	84.46	77.81	69.75	76.46	62.50	44.53	27.38
20	78.33	75.63	60.52	51.67	66.98	45.68	35.12	20.18
30	62.08	60.92	49.17	37.46	65.94	42.89	26.22	16.10
40	64.42	44.88	36.08	29.21	60.42	33.36	22.86	15.83
50	57.50	38.13	31.84	19.00	52.81	29.69	19.05	11.15
60	42.00	36.67	28.13	17.29	49.69	23.92	17.33	10.19
70	35.17	20.63	19.24	8.46	41.77	17.08	15.32	9.13
	Successful Connections (%)							
0	100.00	100.00	97.00	86.00	93.75	76.88	57.50	34.38
10	96.00	96.50	87.50	80.50	91.25	75.00	50.83	31.88
20	92.00	89.00	75.42	64.50	77.50	55.63	42.50	24.06
30	85.00	75.50	62.92	49.50	72.50	53.75	32.08	23.44
40	83.00	61.00	49.17	39.50	71.25	40.00	28.75	21.25
50	74.00	52.00	42.08	26.00	66.25	37.50	27.50	14.38
60	55.00	48.00	36.25	24.50	63.75	32.50	26.25	12.31
70	49.00	30.50	27.08	13.50	51.25	21.25	19.42	11.44
	Throughput (Kb/s)							
0	1.96	1.93	1.90	1.66	1.69	1.37	1.02	0.63
10	1.75	1.69	1.56	1.40	1.53	1.25	0.89	0.55
20	1.57	1.51	1.21	1.03	1.34	0.91	0.70	0.40
30	1.24	1.22	0.98	0.75	1.32	0.86	0.52	0.32
40	1.29	0.90	0.72	0.58	1.21	0.67	0.46	0.32
50	1.15	0.76	0.64	0.38	1.06	0.59	0.38	0.22
60	0.84	0.73	0.56	0.35	0.99	0.48	0.35	0.20
70	0.70	0.41	0.38	0.17	0.84	0.34	0.31	0.18
	Average End-to-End Delay (ms)							
Average	252.12	421.62	479.77	545.15	384.98	625.87	717.45	860.22

Table A.2: AODV simulation results; fixed transmission range.

Selfish Nodes (%)	Scenario 1: Static				Scenario 2: Mobile			
	100 Nodes	200 Nodes	300 Nodes	400 Nodes	100 Nodes	200 Nodes	300 Nodes	400 Nodes
	Packet Delivery Ratio (%)							
0	100.00	100.00	100.00	100.00	94.94	90.97	88.83	85.89
10	93.02	94.77	96.59	98.58	88.75	84.26	82.90	85.52
20	90.00	93.01	94.16	96.70	86.09	80.55	78.92	75.29
30	76.98	85.10	88.51	93.70	82.29	77.69	74.24	71.39
40	83.85	82.67	85.47	88.24	80.83	75.85	70.22	66.80
50	67.60	75.66	78.06	85.58	76.09	71.32	68.16	62.11
60	71.98	73.90	76.85	80.60	75.10	65.88	62.07	60.85
70	64.27	68.57	70.78	78.66	69.90	58.25	56.18	52.58
	Successful Connections (%)							
0	100.00	100.00	100.00	100.00	95.50	93.13	88.75	85.50
10	90.75	96.88	98.83	99.63	93.75	90.38	85.00	81.19
20	84.50	90.25	95.83	96.19	90.50	87.63	81.08	75.81
30	81.50	89.50	93.58	94.63	88.50	84.38	77.25	71.69
40	78.50	84.75	87.08	92.69	84.75	81.00	73.42	67.31
50	73.25	75.13	84.17	86.94	82.25	78.38	68.58	64.88
60	70.25	72.50	76.17	82.88	81.50	70.50	63.25	60.25
70	65.50	66.75	73.33	78.94	77.50	65.63	58.92	54.75
	Throughput (Kb/s)							
0	2.00	2.00	2.00	2.00	1.90	1.82	1.78	1.72
10	1.86	1.90	1.93	1.97	1.78	1.69	1.66	1.71
20	1.80	1.86	1.88	1.93	1.72	1.61	1.58	1.51
30	1.54	1.70	1.77	1.87	1.65	1.55	1.48	1.43
40	1.68	1.65	1.71	1.76	1.62	1.52	1.40	1.34
50	1.35	1.51	1.56	1.71	1.52	1.43	1.36	1.24
60	1.44	1.48	1.54	1.61	1.50	1.32	1.24	1.22
70	1.29	1.37	1.42	1.57	1.40	1.17	1.12	1.05
	Average End-to-End Delay (ms)							
Average	181.98	320.53	453.61	595.18	252.08	412.89	681.45	817.70

Appendix B

Naïve Bayes Classifier Routing

B.1 Performance Evaluation

Table B.1: NBCR simulation results; variable transmission range.

Scenario 1: Static					Scenario 2: Mobile			
Selfish Nodes (%)	100 Nodes	200 Nodes	300 Nodes	400 Nodes	100 Nodes	200 Nodes	300 Nodes	400 Nodes
Packet Delivery Ratio (%)								
0	97.83	96.71	94.97	83.04	84.40	68.41	53.72	31.25
10	92.08	92.63	88.72	79.58	83.15	66.61	49.51	29.32
20	89.42	86.63	79.76	70.79	79.58	61.77	45.54	27.88
30	85.92	80.54	74.62	61.67	76.41	60.70	42.15	26.10
40	78.42	73.63	67.12	55.96	71.15	55.31	40.56	24.26
50	74.36	67.46	62.53	49.88	67.60	47.99	37.41	23.78
60	72.58	62.04	55.28	37.46	65.86	45.63	35.82	21.54
70	66.33	51.71	43.78	27.29	63.65	42.08	29.98	20.01
Successful Connections (%)								
0	100.00	100.00	97.00	86.00	93.75	76.88	57.50	34.38
10	99.00	98.50	95.00	84.00	92.25	76.25	57.92	34.00
20	97.00	98.00	92.92	82.50	91.75	70.63	53.33	33.75
30	98.00	95.00	90.83	76.00	91.25	70.00	50.00	33.44
40	93.00	91.00	84.58	72.50	81.25	66.88	49.58	30.00
50	93.00	89.50	81.67	68.50	80.00	62.50	45.42	29.51
60	92.00	83.50	77.50	56.00	78.50	60.00	44.58	27.19
70	87.00	73.00	61.67	41.50	75.50	53.75	37.50	25.19
Throughput (Kb/s)								
0	1.96	1.93	1.90	1.66	1.69	1.37	1.07	0.63
10	1.84	1.85	1.77	1.59	1.66	1.33	0.99	0.59
20	1.79	1.73	1.60	1.42	1.59	1.24	0.91	0.56
30	1.72	1.61	1.49	1.23	1.53	1.21	0.84	0.53
40	1.51	1.47	1.34	1.12	1.42	1.11	0.81	0.51
50	1.51	1.35	1.25	1.00	1.35	0.96	0.75	0.48
60	1.45	1.24	1.11	0.75	1.32	0.91	0.72	0.43
70	1.33	1.03	0.88	0.55	1.27	0.84	0.60	0.40
Average End-to-End Delay (ms)								
Average	335.80	486.34	575.73	693.96	471.22	816.49	962.27	969.74

Table B.2: NBCR simulation results; fixed transmission range.

Selfish Nodes (%)	Scenario 1: Static				Scenario 2: Mobile			
	100 Nodes	200 Nodes	300 Nodes	400 Nodes	100 Nodes	200 Nodes	300 Nodes	400 Nodes
	Packet Delivery Ratio (%)							
0	100.00	100.00	100.00	99.79	94.94	90.97	88.83	85.89
10	97.19	98.63	98.71	99.26	90.48	85.73	84.31	85.72
20	92.98	93.09	94.88	96.97	88.70	83.91	80.88	76.44
30	86.38	89.18	91.40	94.64	84.32	80.44	76.44	73.25
40	82.75	85.73	90.36	93.23	82.91	74.32	73.98	70.84
50	77.00	82.17	88.74	91.57	77.00	72.76	70.31	68.32
60	73.06	81.54	84.38	89.98	76.93	70.80	68.84	65.45
70	70.25	76.19	80.26	86.50	72.48	66.54	64.30	60.73
	Successful Connections (%)							
0	100.00	100.00	100.00	100.00	95.50	93.13	88.75	85.50
10	93.50	94.57	94.90	95.21	94.42	90.42	87.45	82.45
20	90.30	91.08	92.51	93.44	91.73	88.73	85.93	80.93
30	82.80	85.96	87.11	90.34	90.88	83.94	82.72	77.32
40	79.40	82.54	85.66	87.63	87.65	80.77	79.32	75.22
50	77.01	80.42	83.97	85.35	84.92	77.48	76.43	70.89
60	73.03	78.85	79.12	83.20	82.23	75.93	71.32	64.49
70	71.19	73.45	76.23	80.25	80.41	70.67	66.48	60.32
	Throughput (Kb/s)							
0	2.00	2.00	2.00	2.00	1.90	1.82	1.78	1.72
10	1.94	1.97	1.97	1.99	1.81	1.71	1.69	1.71
20	1.86	1.86	1.90	1.94	1.77	1.68	1.62	1.53
30	1.73	1.78	1.83	1.89	1.69	1.61	1.53	1.47
40	1.66	1.71	1.81	1.86	1.66	1.49	1.48	1.42
50	1.54	1.64	1.77	1.83	1.54	1.46	1.41	1.37
60	1.46	1.63	1.69	1.80	1.54	1.42	1.38	1.31
70	1.41	1.52	1.61	1.73	1.45	1.33	1.29	1.21
	Average End-to-End Delay (ms)							
Average	145.47	217.71	396.02	485.48	215.13	326.90	550.80	745.93

Appendix C

Clustering Overlay

C.1 Cluster Creation Test

Table C.1: *Neighbour Table* for cluster heads; Cluster Creation Test.

Cluster Head IP	Neighbour IP	Neighbour Weight	Neighbour Tag	Neighbour Head IPs	Cluster
10.0.0.1	10.0.0.21	0.895	1	10.0.0.1 10.0.0.43	
10.0.0.43	10.0.0.56	0.825	1	10.0.0.48 10.0.0.43 10.0.0.85	
	10.0.0.45	0.895	1	10.0.0.48 10.0.0.43	
	10.0.0.64	0.860	1	10.0.0.85 10.0.0.43	
10.0.0.85	10.0.0.64	0.860	1	10.0.0.85 10.0.0.43	
	10.0.0.56	0.825	1	10.0.0.48 10.0.0.43 10.0.0.85	
	10.0.0.88	0.930	1	10.0.0.85 10.0.0.100	
10.0.0.48	10.0.0.45	0.895	1	10.0.0.48 10.0.0.43	
	10.0.0.56	0.825	1	10.0.0.48 10.0.0.43 10.0.0.85	
	10.0.0.69	0.930	1	10.0.0.48 10.0.0.100	
10.0.0.100	10.0.0.88	0.930	1	10.0.0.85 10.0.0.100	
	10.0.0.69	0.930	1	10.0.0.48 10.0.0.100	

Table C.2: Trust Table for 10.0.0.1; Cluster Creation Test

Destination	Gateway	Interface	Route Trust	Hop Count	Route bility	Proba- bility	Timestamp (s)
10.0.0.2	10.0.0.2	10.0.0.1	0.2	1	96.06		0.043
10.0.0.3	10.0.0.3	10.0.0.1	0.2	1	96.06		0.038
10.0.0.4	10.0.0.4	10.0.0.1	0.2	1	96.06		0.098
10.0.0.11	10.0.0.11	10.0.0.1	0.2	1	96.06		0.087
10.0.0.12	10.0.0.12	10.0.0.1	0.2	1	96.06		0.08817
10.0.0.13	10.0.0.13	10.0.0.1	0.2	1	96.06		0.03939
10.0.0.14	10.0.0.14	10.0.0.1	0.2	1	96.06		0.014
10.0.0.21	10.0.0.21	10.0.0.1	0.85	1	100		0.011
10.0.0.100	10.0.0.21	10.0.0.1	0.4016	6	22.92		41.14
10.0.0.22	10.0.0.22	10.0.0.1	0.2	1	96.06		0.09325
10.0.0.23	10.0.0.23	10.0.0.1	0.75	1	99.99		0.096
10.0.0.31	10.0.0.31	10.0.0.1	0.2	1	96.06		0.02839
10.0.0.32	10.0.0.32	10.0.0.1	0.2	1	96.06		0.004001
...	...	...	...	...	...		...

Table C.3: Routing Table 1; Cluster Creation Test

Node ID	Destination	Gateway	Interface	Flag	Expire	Hops
10.0.0.1	10.0.0.2	10.0.0.2	10.0.0.1	UP	150.04	1
	10.0.0.3	10.0.0.3	10.0.0.1	UP	150.04	1
	10.0.0.4	10.0.0.4	10.0.0.1	UP	150.1	1
	10.0.0.11	10.0.0.11	10.0.0.1	UP	150.09	1
	10.0.0.12	10.0.0.12	10.0.0.1	UP	150.09	1
	10.0.0.13	10.0.0.13	10.0.0.1	UP	150.04	1
	10.0.0.14	10.0.0.14	10.0.0.1	UP	150.01	1
	10.0.0.21	10.0.0.21	10.0.0.1	UP	150.01	1
	10.0.0.22	10.0.0.22	10.0.0.1	UP	150.09	1
	10.0.0.23	10.0.0.23	10.0.0.1	UP	150.1	1
	10.0.0.31	10.0.0.31	10.0.0.1	UP	150.03	1
	10.0.0.32	10.0.0.32	10.0.0.1	UP	150	1
	10.0.0.100	10.0.0.21	10.0.0.1	UP	13.39	6
10.0.0.21	10.0.0.1	10.0.0.1	10.0.0.21	UP	1.38	1
	10.0.0.2	10.0.0.2	10.0.0.21	UP	150.04	1
	10.0.0.3	10.0.0.3	10.0.0.21	UP	150.04	1
	10.0.0.11	10.0.0.11	10.0.0.21	UP	150.09	1
	10.0.0.12	10.0.0.12	10.0.0.21	UP	150.09	1
	10.0.0.13	10.0.0.13	10.0.0.21	UP	150.04	1
	10.0.0.14	10.0.0.14	10.0.0.21	UP	150.01	1
	10.0.0.22	10.0.0.22	10.0.0.21	UP	150.09	1
	10.0.0.23	10.0.0.23	10.0.0.21	UP	150.1	1
	10.0.0.24	10.0.0.24	10.0.0.21	UP	150.1	1
	10.0.0.31	10.0.0.31	10.0.0.21	UP	150.03	1
	10.0.0.32	10.0.0.32	10.0.0.21	UP	150	1
	10.0.0.33	10.0.0.33	10.0.0.21	UP	150.03	1
	10.0.0.34	10.0.0.34	10.0.0.21	UP	150.07	1
	10.0.0.41	10.0.0.41	10.0.0.21	UP	150.09	1
	10.0.0.42	10.0.0.42	10.0.0.21	UP	150.05	1
	10.0.0.43	10.0.0.43	10.0.0.21	UP	1.38	1
	10.0.0.51	10.0.0.51	10.0.0.21	UP	150.05	1
	10.0.0.52	10.0.0.52	10.0.0.21	UP	150.03	1
	10.0.0.100	10.0.0.43	10.0.0.21	UP	13.38	5
10.0.0.43	10.0.0.1	10.0.0.21	10.0.0.43	UP	3.03	2
	10.0.0.12	10.0.0.12	10.0.0.43	UP	150.09	1
	10.0.0.13	10.0.0.13	10.0.0.43	UP	150.04	1
	10.0.0.14	10.0.0.14	10.0.0.43	UP	150.01	1
	10.0.0.21	10.0.0.21	10.0.0.43	UP	1.38	1
	10.0.0.22	10.0.0.22	10.0.0.43	UP	150.09	1
	10.0.0.23	10.0.0.23	10.0.0.43	UP	150.1	1
	10.0.0.24	10.0.0.24	10.0.0.43	UP	150.1	1
	10.0.0.25	10.0.0.25	10.0.0.43	UP	150.04	1
	10.0.0.34	10.0.0.34	10.0.0.43	UP	150.07	1
	10.0.0.35	10.0.0.35	10.0.0.43	UP	150.02	1
	10.0.0.41	10.0.0.41	10.0.0.43	UP	150.09	1
	10.0.0.42	10.0.0.42	10.0.0.43	UP	150.05	1
	10.0.0.45	10.0.0.45	10.0.0.43	UP	1.37	1
	10.0.0.46	10.0.0.46	10.0.0.43	UP	150.08	1
	10.0.0.51	10.0.0.51	10.0.0.43	UP	150.05	1
	10.0.0.52	10.0.0.52	10.0.0.43	UP	150.03	1
	10.0.0.56	10.0.0.56	10.0.0.43	UP	150.11	1
	10.0.0.61	10.0.0.61	10.0.0.43	UP	150.01	1
	10.0.0.64	10.0.0.64	10.0.0.43	UP	150.1	1
	10.0.0.65	10.0.0.65	10.0.0.43	UP	150.08	1
	10.0.0.72	10.0.0.72	10.0.0.43	UP	150.01	1
	10.0.0.73	10.0.0.73	10.0.0.43	UP	150.09	1
	10.0.0.74	10.0.0.74	10.0.0.43	UP	150.08	1
	10.0.0.100	10.0.0.45	10.0.0.43	UP	13.37	4

Table C.4: Routing Table 2; Cluster Creation Test

Node ID	Destination	Gateway	Interface	Flag	Expire	Hops
10.0.0.45	10.0.0.1	10.0.0.43	10.0.0.45	UP	5.11	3
	10.0.0.14	10.0.0.14	10.0.0.45	UP	150.01	1
	10.0.0.23	10.0.0.23	10.0.0.45	UP	150.1	1
	10.0.0.24	10.0.0.24	10.0.0.45	UP	150.1	1
	10.0.0.25	10.0.0.25	10.0.0.45	UP	150.04	1
	10.0.0.26	10.0.0.26	10.0.0.45	UP	150.1	1
	10.0.0.27	10.0.0.27	10.0.0.45	UP	150.11	1
	10.0.0.34	10.0.0.34	10.0.0.45	UP	150.07	1
	10.0.0.35	10.0.0.35	10.0.0.45	UP	150.02	1
	10.0.0.36	10.0.0.36	10.0.0.45	UP	150.07	1
	10.0.0.38	10.0.0.38	10.0.0.45	UP	150.01	1
	10.0.0.42	10.0.0.42	10.0.0.45	UP	150.05	1
	10.0.0.43	10.0.0.43	10.0.0.45	UP	12.93	1
	10.0.0.44	10.0.0.44	10.0.0.45	UP	150.02	1
	10.0.0.46	10.0.0.46	10.0.0.45	UP	150.08	1
	10.0.0.48	10.0.0.48	10.0.0.45	UP	12.93	1
	10.0.0.52	10.0.0.52	10.0.0.45	UP	150.03	1
	10.0.0.53	10.0.0.53	10.0.0.45	UP	150.09	1
	10.0.0.54	10.0.0.54	10.0.0.45	UP	150.08	1
	10.0.0.55	10.0.0.55	10.0.0.45	UP	150.05	1
	10.0.0.56	10.0.0.56	10.0.0.45	UP	150.11	1
	10.0.0.58	10.0.0.58	10.0.0.45	UP	150.06	1
	10.0.0.63	10.0.0.63	10.0.0.45	UP	150.04	1
	10.0.0.64	10.0.0.64	10.0.0.45	UP	150.1	1
	0.0.0.65	10.0.0.65	10.0.0.45	UP	150.08	1
	0.0.0.66	10.0.0.66	10.0.0.45	UP	150.06	1
	10.0.0.67	10.0.0.67	10.0.0.45	UP	150.08	1
	10.0.0.74	10.0.0.74	10.0.0.45	UP	150.08	1
	10.0.0.76	10.0.0.76	10.0.0.45	UP	150.01	1
	10.0.0.100	10.0.0.48	10.0.0.45	UP	12.93	3
10.0.0.48	10.0.0.1	10.0.0.45	10.0.0.48	UP	5.12	4
	10.0.0.17	10.0.0.17	10.0.0.48	UP	150.06	1
	10.0.0.18	10.0.0.18	10.0.0.48	UP	150.06	1
	10.0.0.19	10.0.0.19	10.0.0.48	UP	150.1	1
	10.0.0.26	10.0.0.26	10.0.0.48	UP	150.1	1
	10.0.0.28	10.0.0.28	10.0.0.48	UP	150.03	1
	10.0.0.29	10.0.0.29	10.0.0.48	UP	150.01	1
	10.0.0.30	10.0.0.30	10.0.0.48	UP	150.06	1
	10.0.0.35	10.0.0.35	10.0.0.48	UP	150.02	1
	10.0.0.36	10.0.0.36	10.0.0.48	UP	150.07	1
	10.0.0.40	10.0.0.40	10.0.0.48	UP	150.06	1
	10.0.0.46	10.0.0.46	10.0.0.48	UP	150.08	1
	10.0.0.47	10.0.0.47	10.0.0.48	UP	150.02	1
	10.0.0.49	10.0.0.49	10.0.0.48	UP	150.02	1
	10.0.0.55	10.0.0.55	10.0.0.48	UP	150.05	1
	10.0.0.56	10.0.0.56	10.0.0.48	UP	9.23	1
	10.0.0.57	10.0.0.57	10.0.0.48	UP	150.08	1
	10.0.0.58	10.0.0.58	10.0.0.48	UP	150.06	1
	10.0.0.59	10.0.0.59	10.0.0.48	UP	150.01	1
	10.0.0.67	10.0.0.67	10.0.0.48	UP	150.08	1
	10.0.0.68	10.0.0.68	10.0.0.48	UP	150.06	1
	10.0.0.69	10.0.0.69	10.0.0.48	UP	150.1	1
	10.0.0.70	10.0.0.70	10.0.0.48	UP	150.01	1
	10.0.0.78	10.0.0.78	10.0.0.48	UP	150.04	1
	10.0.0.79	10.0.0.79	10.0.0.48	UP	150.01	1
	10.0.0.100	10.0.0.69	10.0.0.48	UP	2.13	2
10.0.0.69	10.0.0.1	10.0.0.48	10.0.0.69	UP	5.12	5
	10.0.0.38	10.0.0.38	10.0.0.69	UP	150.01	1
	10.0.0.39	10.0.0.39	10.0.0.69	UP	150.02	1
	10.0.0.40	10.0.0.40	10.0.0.69	UP	150.06	1
	10.0.0.47	10.0.0.47	10.0.0.69	UP	150.02	1
	10.0.0.48	10.0.0.48	10.0.0.69	UP	9.23	1
	10.0.0.49	10.0.0.49	10.0.0.69	UP	150.02	1
	10.0.0.50	10.0.0.50	10.0.0.69	UP	150.09	1
	10.0.0.56	10.0.0.56	10.0.0.69	UP	150.11	1
	10.0.0.57	10.0.0.57	10.0.0.69	UP	150.08	1
	10.0.0.59	10.0.0.59	10.0.0.69	UP	150.01	1
	10.0.0.66	10.0.0.66	10.0.0.69	UP	150.06	1
	10.0.0.67	10.0.0.67	10.0.0.69	UP	150.08	1
	10.0.0.68	10.0.0.68	10.0.0.69	UP	150.06	1
	10.0.0.70	10.0.0.70	10.0.0.69	UP	150.01	1
	10.0.0.76	10.0.0.76	10.0.0.69	UP	150.01	1
	10.0.0.78	10.0.0.78	10.0.0.69	UP	150.04	1
	10.0.0.87	10.0.0.87	10.0.0.69	UP	150.1	1
	10.0.0.88	10.0.0.88	10.0.0.69	UP	150.04	1
	10.0.0.89	10.0.0.89	10.0.0.69	UP	150.03	1
	10.0.0.90	10.0.0.90	10.0.0.69	UP	150.1	1
	10.0.0.99	10.0.0.99	10.0.0.69	UP	150.04	1
	10.0.0.100	10.0.0.100	10.0.0.69	UP	12.96	1

C.2 Performance Evaluation

Table C.5: CB-NBCR simulation results; variable transmission range.

Selfish Nodes (%)	Scenario 1: Static				Scenario 2: Mobile			
	100 Nodes	200 Nodes	300 Nodes	400 Nodes	100 Nodes	200 Nodes	300 Nodes	400 Nodes
	Packet Delivery Ratio (%)							
0	94.75	92.82	89.40	75.42	76.31	64.33	48.88	26.75
10	91.45	90.21	82.86	71.89	74.89	61.89	46.67	24.45
20	87.23	81.35	71.26	67.43	72.77	55.45	42.19	22.19
30	81.12	76.67	67.47	56.44	70.83	53.67	39.78	20.42
40	76.75	69.75	61.02	50.63	67.15	51.11	35.55	18.73
50	74.12	62.85	55.48	41.37	65.23	44.67	32.24	16.49
60	71.84	57.41	48.93	32.99	63.83	41.98	27.95	14.46
70	65.93	43.82	32.48	20.85	60.25	38.29	25.67	11.73
	Successful Connections (%)							
0	98.00	97.50	94.00	84.00	91.75	74.56	53.22	32.77
10	97.00	96.00	92.82	81.00	86.45	72.19	51.06	29.86
20	96.00	94.00	88.12	79.00	84.46	66.45	47.43	26.56
30	95.00	92.50	86.49	74.52	82.19	63.29	44.43	23.68
40	91.00	89.50	84.44	69.33	77.73	61.11	42.97	20.00
50	88.00	87.00	76.42	64.45	75.00	56.75	36.75	19.86
60	86.00	77.50	73.48	52.22	73.00	53.25	33.19	17.45
70	84.00	68.50	56.77	36.76	68.82	48.98	28.46	16.65
	Throughput (Kb/s)							
0	1.90	1.86	1.79	1.51	1.53	1.29	0.98	0.54
10	1.83	1.80	1.66	1.44	1.50	1.24	0.93	0.49
20	1.74	1.63	1.43	1.35	1.46	1.11	0.84	0.44
30	1.62	1.53	1.35	1.13	1.42	1.07	0.80	0.41
40	1.54	1.40	1.22	1.01	1.34	1.02	0.71	0.37
50	1.48	1.26	1.11	0.83	1.30	0.89	0.64	0.33
60	1.44	1.15	0.98	0.66	1.28	0.84	0.56	0.29
70	1.32	0.88	0.65	0.42	1.21	0.77	0.51	0.23
	Average End-to-End Delay (ms)							
Average	385.47	497.33	629.99	726.90	627.83	1006.64	1100.93	1156.72

Table C.6: CB-NBCR simulation results; fixed transmission range.

Selfish Nodes (%)	Scenario 1: Static				Scenario 2 : Mobile			
	100 Nodes	200 Nodes	300 Nodes	400 Nodes	100 Nodes	200 Nodes	300 Nodes	400 Nodes
	Packet Delivery Ratio (%)							
0	97.22	100.00	100.00	100.00	90.48	91.00	93.48	95.00
10	95.56	99.12	99.56	99.98	86.67	86.73	88.43	90.43
20	91.12	94.73	96.73	96.78	83.91	84.95	87.64	89.77
30	85.53	90.57	95.32	95.68	80.79	81.34	82.20	84.39
40	80.79	88.91	93.76	94.77	77.68	77.93	80.00	81.37
50	75.31	85.73	90.44	92.83	74.00	74.67	76.43	78.43
60	70.80	82.26	88.70	90.42	71.93	73.57	75.87	77.19
70	69.43	80.43	84.39	88.55	65.84	69.93	71.90	75.63
	Successful Connections (%)							
0	97.45	100.00	100.00	100.00	92.43	94.00	96.75	98.75
10	90.88	95.42	96.70	98.00	89.70	91.32	92.25	96.83
20	76.89	92.75	93.33	96.43	86.65	90.76	91.50	94.43
30	75.61	88.42	90.18	93.78	84.33	85.76	88.75	91.77
40	73.29	84.93	87.45	91.19	82.50	83.23	84.90	87.65
50	71.11	82.47	84.85	88.74	80.00	81.50	83.56	85.31
60	69.95	79.00	82.73	85.21	76.65	78.45	81.00	83.00
70	67.00	75.67	79.79	82.65	72.90	74.33	76.65	79.95
	Throughput (Kb/s)							
0	1.94	2.00	2.00	2.00	1.81	1.82	1.87	1.90
10	1.91	1.98	1.99	2.00	1.73	1.73	1.77	1.81
20	1.82	1.89	1.93	1.94	1.68	1.70	1.75	1.80
30	1.71	1.81	1.91	1.91	1.62	1.63	1.64	1.69
40	1.62	1.78	1.88	1.90	1.55	1.56	1.60	1.63
50	1.51	1.71	1.81	1.86	1.48	1.49	1.53	1.57
60	1.42	1.65	1.77	1.81	1.44	1.47	1.52	1.54
70	1.39	1.61	1.69	1.77	1.32	1.40	1.44	1.51
	Average End-to-End Delay (ms)							
Average	200.43	363.19	519.66	650.32	319.19	476.67	757.77	900.48

Appendix D

Conclusion and Future Work

D.1 Analysis of Results

Table D.1: Tabular simulation comparison; variable transmission range; static

Simulation Results: Variable Transmission Range; Static												
Selfish Nodes (%)	100 Nodes			200 Nodes			300 Nodes			400 Nodes		
	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR
Packet Delivery Ratio (%)												
0	97.83	97.83	94.75	96.71	96.71	92.82	94.97	94.97	89.40	83.04	83.04	75.42
10	87.25	92.08	91.45	84.46	92.63	90.21	77.81	88.72	82.86	69.75	79.58	71.89
20	78.33	89.42	87.23	75.63	86.63	81.35	60.52	79.76	71.26	51.67	70.79	67.43
30	62.08	85.92	81.12	60.92	80.54	76.67	49.17	74.62	67.47	37.46	61.67	56.44
40	64.42	78.42	76.75	44.88	73.63	69.75	36.08	67.12	61.02	29.21	55.96	50.63
50	57.50	74.36	74.12	38.13	67.46	62.85	31.84	62.53	55.48	19.00	49.88	41.37
60	42.00	72.58	71.84	36.67	62.04	57.41	28.13	55.28	48.93	17.29	37.46	32.99
70	35.17	66.33	65.93	20.63	51.71	43.82	19.24	43.78	32.48	8.46	27.29	20.85
Successful Connections (%)												
0	100.00	100.00	98.00	100.00	100.00	97.50	97.00	97.00	94.00	86.00	86.00	84.00
10	96.00	99.00	97.00	96.50	98.50	96.00	87.50	95.00	92.82	80.50	84.00	81.00
20	92.00	97.00	96.00	89.00	98.00	94.00	75.42	92.92	88.12	64.50	82.50	79.00
30	85.00	98.00	95.00	75.50	95.00	92.50	62.92	90.83	86.49	49.50	76.00	74.52
40	83.00	93.00	91.00	61.00	91.00	89.50	49.17	84.58	84.44	39.50	72.50	69.33
50	74.00	93.00	88.00	52.00	89.50	87.00	42.08	81.67	76.42	26.00	68.50	64.45
60	55.00	92.00	86.00	48.00	83.50	77.50	36.25	77.50	73.48	24.50	56.00	52.22
70	49.00	87.00	84.00	30.50	73.00	68.50	27.08	61.67	56.77	13.50	41.50	36.76
Throughput (Kb/s)												
0	1.96	1.96	1.90	1.93	1.93	1.86	1.90	1.90	1.79	1.66	1.66	1.51
10	1.75	1.84	1.83	1.69	1.85	1.80	1.56	1.77	1.66	1.40	1.59	1.44
20	1.57	1.79	1.74	1.51	1.73	1.63	1.21	1.60	1.43	1.03	1.42	1.35
30	1.24	1.72	1.62	1.22	1.61	1.53	0.98	1.49	1.35	0.75	1.23	1.13
40	1.29	1.51	1.54	0.90	1.47	1.40	0.72	1.34	1.22	0.58	1.12	1.01
50	1.15	1.51	1.48	0.76	1.35	1.26	0.64	1.25	1.11	0.38	1.00	0.83
60	0.84	1.45	1.44	0.73	1.24	1.15	0.56	1.11	0.98	0.35	0.75	0.66
70	0.70	1.33	1.32	0.41	1.03	0.88	0.38	0.88	0.65	0.17	0.55	0.42
Average End-to-End Delay (ms)												
Average	252.12	335.80	385.47	421.62	486.34	497.33	479.77	575.73	629.99	545.15	693.96	726.90

Table D.2: Tabular simulation comparison; variable transmission range; mobile

Simulation Results: Variable Transmission Range; Mobile												
Selfish Nodes (%)	100 Nodes			200 Nodes			300 Nodes			400 Nodes		
	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR
Packet Delivery Ratio (%)												
0	84.40	84.40	76.31	68.26	68.41	64.33	51.16	53.72	48.88	31.25	31.25	26.75
10	76.46	83.15	74.89	62.50	66.61	61.89	44.53	49.51	46.67	27.38	29.32	24.45
20	66.98	79.58	72.77	45.68	61.77	55.45	35.12	45.54	42.19	20.18	27.88	22.19
30	65.94	76.41	70.83	42.89	60.70	53.67	26.22	42.15	39.78	16.10	26.10	20.42
40	60.42	71.15	67.15	33.36	55.31	51.11	22.86	40.56	35.55	15.83	24.26	18.73
50	52.81	67.60	65.23	29.69	47.99	44.67	19.05	37.41	32.24	11.15	23.78	16.49
60	49.69	65.86	63.83	23.92	45.63	41.98	17.33	35.82	27.95	10.19	21.54	14.46
70	41.77	63.65	60.25	17.08	42.08	38.29	15.32	29.98	25.67	9.13	20.01	11.73
Successful Connections (%)												
0	93.75	93.75	91.75	76.88	76.88	74.56	57.50	57.50	53.22	34.38	34.38	32.77
10	91.25	92.25	86.45	75.00	76.25	72.19	50.83	57.92	51.06	31.88	34.00	29.86
20	77.50	91.75	84.46	55.63	70.63	66.45	42.50	53.33	47.43	24.06	33.75	26.56
30	72.50	91.25	82.19	53.75	70.00	63.29	32.08	50.00	44.43	23.44	33.44	23.68
40	71.25	81.25	77.73	40.00	66.88	61.11	28.75	49.58	42.97	21.25	30.00	20.00
50	66.25	80.00	75.00	37.50	62.50	56.75	27.50	45.42	36.75	14.38	29.51	19.86
60	63.75	78.50	73.00	32.50	60.00	53.25	26.25	44.58	33.19	12.31	27.19	17.45
70	51.25	75.50	68.82	21.25	53.75	48.98	19.42	37.50	28.46	11.44	25.19	16.65
Throughput (Kb/s)												
0	1.69	1.69	1.53	1.37	1.37	1.29	1.02	1.07	0.98	0.63	0.63	0.54
10	1.53	1.66	1.50	1.25	1.33	1.24	0.89	0.99	0.93	0.55	0.59	0.49
20	1.34	1.59	1.46	0.91	1.24	1.11	0.70	0.91	0.84	0.40	0.56	0.44
30	1.32	1.53	1.42	0.86	1.21	1.07	0.52	0.84	0.80	0.32	0.53	0.41
40	1.21	1.42	1.34	0.67	1.11	1.02	0.46	0.81	0.71	0.32	0.51	0.37
50	1.06	1.35	1.30	0.59	0.96	0.89	0.38	0.75	0.64	0.22	0.48	0.33
60	0.99	1.32	1.28	0.48	0.91	0.84	0.35	0.72	0.56	0.20	0.43	0.29
70	0.84	1.27	1.21	0.34	0.84	0.77	0.31	0.60	0.51	0.18	0.40	0.23
Average End-to-End Delay (ms)												
Average	384.98	471.22	627.83	625.87	816.49	1006.64	717.45	962.27	1100.93	860.22	969.74	1156.72

Table D.3: Tabular simulation comparison; fixed transmission range; static

Simulation Results: Fixed Transmission Range; Static												
Selfish Nodes (%)	100 Nodes			200 Nodes			300 Nodes			400 Nodes		
	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR
Packet Delivery Ratio (%)												
0	100.00	100.00	97.22	100.00	100.00	100.00	100.00	100.00	100.00	100.00	99.79	100.00
10	93.02	97.19	95.56	94.77	98.63	99.12	96.59	98.71	99.56	98.58	99.26	99.98
20	90.00	92.98	91.12	93.01	93.09	94.73	94.16	94.88	96.73	96.70	96.97	96.78
30	76.98	86.38	85.53	85.10	89.18	90.57	88.51	91.40	95.32	93.70	94.64	95.68
40	83.85	82.75	80.79	82.67	85.73	88.91	85.47	90.36	93.76	88.24	93.23	94.77
50	67.60	77.00	75.31	75.66	82.17	85.73	78.06	88.74	90.44	85.58	91.57	92.83
60	71.98	73.06	70.80	73.90	81.54	82.26	76.85	84.38	88.70	80.60	89.98	90.42
70	64.27	70.25	69.43	68.57	76.19	80.43	70.78	80.26	84.39	78.66	86.50	88.55
Successful Connections (%)												
0	100.00	100.00	97.45	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
10	90.75	93.50	90.88	96.88	94.57	95.42	98.83	94.90	96.70	99.63	95.21	98.00
20	84.50	90.30	76.89	90.25	91.08	92.75	95.83	92.51	93.33	96.19	93.44	96.43
30	81.50	82.80	75.61	89.50	85.96	88.42	93.58	87.11	90.18	94.63	90.34	93.78
40	78.50	79.40	73.29	84.75	82.54	84.93	87.08	85.66	87.45	92.69	87.63	91.19
50	73.25	77.01	71.11	75.13	80.42	82.47	84.17	83.97	84.85	86.94	85.35	88.74
60	70.25	73.03	69.95	72.50	78.85	79.00	76.17	79.12	82.73	82.88	83.20	85.21
70	65.50	71.19	67.00	66.75	73.45	75.67	73.33	76.23	79.79	78.94	80.25	82.65
Throughput (Kb/s)												
0	2.00	2.00	1.94	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00
10	1.86	1.94	1.91	1.90	1.97	1.98	1.93	1.97	1.99	1.97	1.99	2.00
20	1.80	1.86	1.82	1.86	1.86	1.89	1.88	1.90	1.93	1.93	1.94	1.94
30	1.54	1.73	1.71	1.70	1.78	1.81	1.77	1.83	1.91	1.87	1.89	1.91
40	1.68	1.66	1.62	1.65	1.71	1.78	1.71	1.81	1.88	1.76	1.86	1.90
50	1.35	1.54	1.51	1.51	1.64	1.71	1.56	1.77	1.81	1.71	1.83	1.86
60	1.44	1.46	1.42	1.48	1.63	1.65	1.54	1.69	1.77	1.61	1.80	1.81
70	1.29	1.41	1.39	1.37	1.52	1.61	1.42	1.61	1.69	1.57	1.73	1.77
Average End-to-End Delay (ms)												
Average	181.98	145.47	200.43	320.53	217.71	363.19	453.61	396.02	519.66	595.18	485.48	650.32

Table D.4: Tabular simulation comparison; fixed transmission range; mobile

Simulation Results: Variable Transmission Range; Mobile												
Selfish Nodes (%)	100 Nodes			200 Nodes			300 Nodes			400 Nodes		
	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR	AODV	NBCR	CB-NBCR
	Packet Delivery Ratio (%)											
0	94.94	94.94	90.48	90.97	90.97	91.00	88.83	88.83	93.48	85.89	85.89	95.00
10	88.75	90.48	86.67	84.26	85.73	86.73	82.90	84.31	88.43	85.52	85.72	90.43
20	86.09	88.70	83.91	80.55	83.91	84.95	78.92	80.88	87.64	75.29	76.44	89.77
30	82.29	84.32	80.79	77.69	80.44	81.34	74.24	76.44	82.20	71.39	73.25	84.39
40	80.83	82.91	77.68	75.85	74.32	77.93	70.22	73.98	80.00	66.80	70.84	81.37
50	76.09	77.00	74.00	71.32	72.76	74.67	68.16	70.31	76.43	62.11	68.32	78.43
60	75.10	76.93	71.93	65.88	70.80	73.57	62.07	68.84	75.87	60.85	65.45	77.19
70	69.90	72.48	65.84	58.25	66.54	69.93	56.18	64.30	71.90	52.58	60.73	75.63
	Successful Connections (%)											
0	95.50	95.50	92.43	93.13	93.13	94.00	88.75	88.75	96.75	85.50	85.50	98.75
10	93.75	94.42	89.70	90.38	90.42	91.32	85.00	87.45	92.25	81.19	82.45	96.83
20	90.50	91.73	86.65	87.63	88.73	90.76	81.08	85.93	91.50	75.81	80.93	94.43
30	88.50	90.88	84.33	84.38	83.94	85.76	77.25	82.72	88.75	71.69	77.32	91.77
40	84.75	87.65	82.50	81.00	80.77	83.23	73.42	79.32	84.90	67.31	75.22	87.65
50	82.25	84.92	80.00	78.38	77.48	81.50	68.58	76.43	83.56	64.88	70.89	85.31
60	81.50	82.23	76.65	70.50	75.93	78.45	63.25	71.32	81.00	60.25	64.49	83.00
70	77.50	80.41	72.90	65.63	70.67	74.33	58.92	66.48	76.65	54.75	60.32	79.95
	Throughput (Kb/s)											
0	1.90	1.90	1.81	1.82	1.82	1.82	1.78	1.78	1.87	1.72	1.72	1.90
10	1.78	1.81	1.73	1.69	1.71	1.73	1.66	1.69	1.77	1.71	1.71	1.81
20	1.72	1.77	1.68	1.61	1.68	1.70	1.58	1.62	1.75	1.51	1.53	1.80
30	1.65	1.69	1.62	1.55	1.61	1.63	1.48	1.53	1.64	1.43	1.47	1.69
40	1.62	1.66	1.55	1.52	1.49	1.56	1.40	1.48	1.60	1.34	1.42	1.63
50	1.52	1.54	1.48	1.43	1.46	1.49	1.36	1.41	1.53	1.24	1.37	1.57
60	1.50	1.54	1.44	1.32	1.42	1.47	1.24	1.38	1.52	1.22	1.31	1.54
70	1.40	1.45	1.32	1.17	1.33	1.40	1.12	1.29	1.44	1.05	1.21	1.51
	Average End-to-End Delay (ms)											
Average	252.08	215.13	319.19	412.89	326.90	476.67	681.45	550.80	757.77	817.70	745.93	900.48