The Design of a Defence Mechanism to Mitigate the Spectrum Sensing Data Falsification Attack in Cognitive Radio Ad Hoc Networks

By

ISSAH NGOMANE

Research Dissertation

Submitted in fulfilment of the requirements for the degree of

MASTER OF COMPUTER SCIENCE

In the

Faculty of Science and Agriculture

(School of Mathematical and Computer Sciences)

At the

University of Limpopo

SUPERVISOR: Prof M Velempini

2018

DECLARATION

I, Issah Ngomane, hereby declare that ***The Design of a Defence Mechanism to Mitigate the Spectrum Sensing Data Falsification Attack in Cognitive Radio Ad Hoc Networks*** is my original work and that all sources that have been used are fully acknowledged and correctly referenced. I further declare that this work has not previously been submitted to any other university for a qualification.

Signature: ______________________________

Date: __________________________________

ACKNOWLEDGMENTS

First, I would like to thank God for giving me the strength I needed to complete my dissertation. I am more than grateful to my supervisor Prof. M Velempini for the support, guidance and encouragement he gave to me over the years of my master's degree. His constructive feedback and comments have helped me in completing my dissertation, without his honest mentoring, I would have never been able to complete my studies.

I would like to express my sincere appreciation to all my co-workers at maths building for their encouragement and support. I would like to acknowledge the role of my parents and family in motivating and supporting my desire of pursuing my studies.

I would like to thank my masters' colleagues for their support and encouragement. I would like to express my gratitude to the CSIR, NRF and University of Limpopo research office for providing me with the support and funding I needed to complete my studies and publish conference and journal papers.

ABSTRACT

Dynamic spectrum access enabled by cognitive radio networks is envisioned to address the problems of the ever-increasing wireless technology. This innovative technology increases spectrum utility by allowing unlicensed devices to utilise the unused spectrum band of licenced devices opportunistically. The unlicensed devices referred to as secondary users (SUs) constantly sense the spectrum band to avoid interfering with the transmission of the licenced devices known as primary users (PUs). Due to some environmental challenges that can interfere with effective spectrum sensing, the SUs have to cooperate in sensing the spectrum band. However, cooperative spectrum sensing is susceptible to the spectrum sensing data falsification (SSDF) attack where selfish radios falsify the spectrum reports. Hence, there is a need to design a defence scheme that will defend the SSDF attack and guaranty correct final transmission decision.

In this study, we proposed the integration of the reputation based system and the q-out-of-m rule scheme to defend against the SSDF attack. The reputation-based system was used to determine the trustworthiness of the SUs. The q-out-of-m rule scheme where m sensing reports were selected from the ones with good reputation and q was the final decision, which was used to isolate the entire malicious nodes and make the correct final transmission decision. The proposed scheme was implemented in a Cognitive Radio Ad Hoc Network (CRAHN) where the services of a data fusion centre (FC) were not required. The SUs conducted their own data fusion and made their own final transmission decision based on their sensing reports and the sensing reports of their neighbouring nodes. Matlab was used to implement and simulate the proposed scheme. We compared our proposed scheme with the multi-fusion based distributed spectrum sensing and density based system schemes. Metrics used were the success probability, missed detection probability and false alarm probability. The proposed scheme performed better compared to the other schemes in all the metrics.

Table of Contents

List of tables

List of figures

CHAPTER 1: INTRODUCTION

1.1 Introduction

Cognitive radio networks (CRN) address the problems of spectrum scarcity by allowing unlicensed users known as secondary users (SUs) to utilize the vacant spectrum band of licensed users known as primary users (PUs) without causing interference to the PUs [1] [2] [3] [4] [5] [6]. However, this imposes some unique security challenges due to malicious users (MUs) who report incorrect spectrum observations to the SUs [7].

Security issues in CRN have become a major concern; we have attackers who take advantage of CRN by reporting incorrect spectrum observation to the SUs in an attempt to cause interference to PUs or denial of service to SUs. Reddy in [8] mentions some attacks launched against SUs also referred to as cognitive radios (CRs). This attacks which include jamming, jellyfish, and interference by malicious nodes, overlapping secondary users, primary user emulation attack and spectrum sensing data falsification attack.

This study investigates the spectrum sensing data falsification (SSDF) attack [9]. We propose the integration of the reputation and q-out-of-m rule schemes to mitigate the effects of the SSDF attack. The integrated scheme filters incorrect reports, identifies outliers, which are malicious SUs who do not belong in the network [10], and makes the correct transmission decision. The reputation-based system was used to determine the trustworthiness of the SUs based on their past reports [11]. The q-out-of-m rule, in which the final decision is made based on q sensing reports out of m polled reports [12] was used to suppress the SSDF attack. This scheme was deployed on an ad hoc network and does not require the presence of a common receiver or fusion centre (FC) to perform the data fusion.

1.1.1 Background of the problem

In 1985, the Federal Communications Commission (FCC) issued a mandate defining several portions of the spectrum as licenced-exempt [13] [14] [15]. This authorized unlicensed device to make use of the unutilized spectrum band, which presented attackers with an opportunity to launch attacks against both the PUs and the SUs.

SUs determine the presence of PUs by incorporating spectrum sensing. Spectrum sensing can be conducted in one of two ways, either cooperatively or non-cooperatively [16] [17] [18]. Non-cooperatively, whereby the SUs conduct PUs detection and make the final decision by themselves regarding the status of the spectrum band [19]. Cooperatively in which all the SUs in the network conduct PUs detection and share the information with each other [20]. Authors in [21], [22] have discovered that cooperative spectrum sensing (CSS) is superior to non-cooperative spectrum sensing due to Byzantine failures in the network which lead to primary user signal fading, hidden terminal problem and shadowing. In order to improve the performance of spectrum sensing, authors have proposed cooperation among the SUs in conducting spectrum sensing, [23] [24]. However, CSS is susceptible to the SSDF attack [25].

1.1.2 The research problem

There is still a need to fill the gap in addressing the SSDF attack in Cognitive Radio Ad Hoc Networks (CRAHN). The SSDF attack disturbs CRN by reporting incorrect spectrum observations to the neighbouring nodes in an attempt to enforce an incorrect transmission decision making. This may lead to PUs interference or SUs denial of service. This research will attempt to mitigate the SSDF attack in CRAHN by implementing the reputation-based system and the q-out-of-m-rule scheme.

1.1.3 Aim of the study

The aim of the study is to contribute to the existing body of knowledge in infrastructure-less CRN security. We aim at using the reputation and q-out-of-m-rule to mitigate the SSDF attack in CRAHN where the services of a FC are not required. We aim at using the proposed scheme to distinguish between honest users, malicious users and unintentionally misbehaving SUs, which are SUs that temporarily report incorrect observations because of the Byzantine failures in the network [26].

1.1.4 Research objectives

The objectives of the research are:

1. To deploy the reputation and q-out-of-m rule scheme in CRAHN and assess its effectiveness in defending against the SSDF attack.
2. To examine the ability of the reputation based system in removing attackers in CRAHN.
3. Investigate the hit and run attack, always yes attack, always no attack and assess their impact on the network.
4. Investigate unintentionally misbehaving nodes and distinguish them from outliers.

1.1.5 Hypothesis

If the reputation and q-out-of-m rule scheme can be deployed in CRAHN, the SSDF attack will be mitigated.

The reputation-based system can be deployed in CRAHN and nodes with bad reputations will be excluded from the network.

Reputation restoration can be implemented to accommodate unintentionally misbehaving SUs

The q-out-of-m rule can be able to prevent malicious nodes from performing the hit and run attack to escape a bad reputation.

1.1.6 The research questions

This research seeks to mitigate the SSDF attack in CRAHN by implementing an effective mechanism known as reputation and q-out-of-m rule scheme. This research aims to answer the following research questions.

1. Can the reputation and q-out-of-m rule scheme be deployed in CRAHN to mitigate the SSDF attack?

1. Can the reputation-based system be used to remove outliers in CRAHN?
2. Can the q-out-of-m rule scheme be used to discourage the hit and run attack?
3. Can temporary misbehaving nodes be distinguished from outliers?

1.2 Brief Literature review

Due to the ever-changing topology of CRAHN and the openness of wireless channels, the SUs are prone to various security challenges that attempt to cause denial of service or interference to PUs [27] . The SSDF attack is one of the attacks launched by attackers with the aim of enforcing an incorrect transmission decision [28]. Researchers have proposed different schemes to counter the SSDF attack in CRAHN. Seif in [29] proposed a censoring based hard decision distributed detection framework for infrastructure-less CRN. Their proposed scheme does not require the services of a FC for decision-making, rather they used a binary consensus algorithm that allowed SUs to exchange binary information and make the final decision based on the observations and decisions of their direct neighbours. Our research does not require the presence of a FC to perform the data fusion; the SUs conduct cooperative spectrum sensing (CSS) and perform their own data fusion.

Yu *et al.* in [30] presented a consensus-based CSS scheme to counter SSDF attacks in CRN. Their scheme was based on recent advances in bio-inspired consensus algorithms. Each user in the proposed scheme used a selected criterion to exclude a suspicious neighbour and then compared the average results with a pre-defined threshold to make the final decision. The shortcoming of the scheme was that it filtered out honest SUs if they behaved suspiciously. We addressed this shortcoming by deploying a reputation-based system that restores the reputation of nodes that temporarily misbehave so that they are not filtered out as outliers.

Wang *et al.* in [31] proposed a system that calculates the untrustworthiness or the suspicious level of SUs using a reputation based system that removes the suspicious SUs before the final transmission decision could be made [31]. Their system required the presence of a FC to make the data fusion which was a shortcoming in our research. We addressed this shortcoming by deploying the reputation-based system in a distributed environment where the services of a FC were not required.

The study in [32], proposed a consensus-based cooperative spectrum-sensing scheme that is based on advances in consensus algorithms looking at the character and self-organising behaviour of animal groups such as fish, ants, honeybees and birds. Their proposed scheme did not require a FC to do the data fusion, the SUs had the ability to maintain themselves. To improve the security level of their proposed scheme, the researchers proposed an authentication scheme using identity-based cryptography that shared a threshold value secretly. One drawback of their proposed system was delay. The time the nodes take to encrypt and decrypt the information was long; the spectrum band might not remain unutilized for a long time. We proposed a reputation-based scheme that did not require the presence of a common controller but is more effective in countering against the SSDF attack; it is easy to implement and fast to make the final transmission decision.

Pongaliur *et al* [33] presented a defence mechanism for infrastructure-less cognitive networks using a lightweight- fusion based spectrum sensing scheme which can sense data fusion, propagate the reputation of SUs and make the final transmission decision [33]. The scheme was able to detect outliers and remove them before making the final transmission decision. This scheme did not propose a mechanism that deals with nodes that can change their reports estimating their reputation probability. One way to counter this shortcoming was to use a mechanism that will be able to identify such malicious nodes and eliminate them from the final decision-making.

1.3 Proposed methodology

This research aims to mitigate the SSDF attack in CRAHN by using the reputation and q-out-of-m rule scheme whereby:

A SU attains the spectrum observations of its direct neighbours and then assesses their reputation to select the neighbours with a good or almost good reputation to be considered in the final decision-making. Due to some MUs which are able to change their reports to prevent having a bad reputation and be classified as outliers, we used the q-out-of-m rule, in which the final decision is made based on q sensing reports out of m polled nodes from the ones with good reputation, to guard against the hit and run attack [34].

Since we were dealing with a mobile topology, reputation propagation was used to propagate the reputation of the SUs to all the secondary networks. If the reputation of a node reaches a predefined threshold value (TV), then that node was considered as an outlier. Legitimate SUs that temporarily misbehave or report incorrect observations reputations were restored if the SUs stopped reporting incorrect observations. The proposed scheme was compared with the multi fusion-based distributed spectrum sensing scheme and density based system scheme in [33], [52]. Matlab was used to implement and simulate the proposed scheme. We tested the proposed scheme considering the number of nodes, the number of malicious nodes in the network and attack strategy deployed by the SSDF attack.

1.4 Research motivations

This research project was motivated by the fact that not a lot of contributions have been given to infrastructure-less cognitive networks thus this research adds to the knowledge of SSDF attack security in infrastructure-less cognitive networks. Learning that infrastructure-less cognitive networks are important in military battlefields, emergencies, and disaster relief motivated us to partake research in this field.

1.4.1 Contributions of the research

1. Ngomane, I, Velempini, M & Dlamini, S.V, 2016. *The design of a defence mechanism to mitigate the spectrum sensing data falsification attack in cognitive radio ad hoc networks*. Durban, ICACCE 2016 IEEE Xplore Digital Library.

This paper showed the theoretical analysis of the proposed scheme in CRAHN. It showed how the scheme can minimize the effects of the SSDF attack. The reputation-based system isolated the extreme outliers and the q-out-of-m rule scheme isolated the remaining outliers that have passed the first fusion step.

2. Ngomane, I, Velempini, M & Dlamini, S.V. *Detection and mitigation of the spectrum sensing data falsification attack in cognitive radio ad hoc networks*. Spain, SATNAC 2017.

This paper investigated the integration of the reputation based system and majority rule on CRAHN to detect and isolate the SSDF attack. The paper contributed to the detection of the SSDF attack. It showed how the integration of the two schemes minimized the effects of the SSDF attack.

3. Ngomane, I, Velempini, M & Dlamini, S.V. *The Detection of the Spectrum Sensing Data Falsification Attack in Cognitive Radio Ad Hoc Networks.* Durban, South Africa 2018.

This paper investigated the SSDF attack in CRAHN using an integrated scheme known as the modified Z-test and q-out-of-m rule scheme. The modified Z-test was used to isolate extreme outliers in the network. The q-out-of-m rule scheme was implemented to mitigate the SSDF attack, where a random number m is selected from the sensing results and q is the final decision from m. The scheme did not require the services of a fusion centre for decision making. We contributed to the detection and isolation of the SSDF attack in CRAHN.

4. Ngomane, I, Velempini, M & Dlamini, S.V. *Statistical-based versus Trust-based approach in defending against the spectrum sensing data falsification attack in Cognitive Radio Ad Hoc Networks*. Cape Town, SATNAC 2018.

This paper investigated statistical approaches versus trust-based approaches in CRAHN. It investigated which approach best mitigates the SSDF attack. The paper contributed to the discovering improved methods of defending against the SSDF attack.

5. Ngomane, I, Velempini, M & Dlamini, S.V. *Trust-based system to defend against the Spectrum Sensing Data Falsification Attack in Cognitive Radio Ad Hoc Networks*. Durban, icABCD 2018.

This paper investigated the reputation based system in CRAHN. We presented motivation of why the reputation-based system was integrated with the q-out-of-m rule scheme. The paper contributed to the detection of the SSDF attack. It showed how the reputation-based system effectively mitigates the SSDF attack but requires improvement.

1.5 Scope and delimitations

The proposed scheme was tested on a network size of 10, 50,100,150 and 250. It is required that the network size be increased to determine the behaviour of the proposed scheme. There is also a need to increase the attack sizes to determine the effects of the SSDF attack when the attack exceeds the legitimate SUs. The reputation based system is integrated with the q-out-of-m rule scheme, we needed to test the effectiveness of the scheme when integrated with other well performing schemes thus the conference papers address this delimitation.

1.6 Overview

Chapter two reviews the related work conducted in SSDF attack both in CRN and CRAHN. We investigated the challenges and limitations the authors encountered in conduction their study in SSDF. We focused on ways we can address the challenges mostly in CRAHN. Chapter three overviews the design implications followed in designing and implementing the proposed scheme. We looked at the methodology followed and the parameters implemented in designing the proposed scheme. Chapter four discusses the network configurations

Chapter five discusses the simulation results. We compared the results of the proposed schemes to the density based distributed spectrum sensing and the multi-fusion based distributed spectrum sensing schemes. We showed how the proposed scheme performs better in detecting and isolating the SSDF attack looking at success probability, missed detection probability and false alarm probability.

In chapter six we concluded the study by summarising the work done. We discussed the challenges encountered and the limitations of the study. Future work and recommendations that need to be conducted to improve the performance of the proposed scheme are highlighted.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Wireless sensor networks have received significant attention from the research community due to their impact on both military and civilian applications [35] [36], However, wireless networks are characterized by a static spectrum assignment policy. Due to this policy, a large portion of the spectrum remains unutilised while there is a need for the utilisation of the unused spectrum [37]. Cognitive radio technology was proposed to address these spectrum inefficiency problems [38] [39]. Cognitive radio allows SUs to utilise the available spectrum band of PUs [40]. The SUs are equipped with cognitive capabilities to opportunistically utilise the spectrum band without causing interference to the licenced devices, which exposes nodes to SSDF attack. This chapter reviews related work done by researchers in attempting to mitigate the effects of the SSDF attack. Analysis of their proposed schemes is done to determine their drawbacks and caps that need to be filled.

2.2 Wireless networks

Since the early 1970`s, wireless networks have become increasingly popular due to their provision of information regardless of the user`s geographic location [41]. Wireless networks can be classified into two types, infrastructure-less and infrastructure-based [42], [43], [44]. Infrastructure-based wireless networks are governed by base stations or centralised controllers, which communicate with each other through links. Nodes are linked to the base stations, which act as their guide for communication with other nodes. Infrastructure-less wireless networks, commonly referred to as ad-hoc wireless networks are network topologies that are not guided by base stations. Nodes form a temporary network for communication then terminate their connection when transmissions are completed.

2.3.1 Multi-fusion based distributed spectrum sensing [33].

SSDF is an attack whereby a malicious SU reports incorrect local sensing reports to other SUs. This attack misleads the SUs, to cause interference to PUs or because of selfish intentions of utilising the band. Pongaluir *et al* in [33] conducted a study in infrastructure-less SSDF attack where the presence of an FC was not required. Their research work suppresses the effects of the SSDF attack by using a mechanism known as multi-fusion based distributed spectrum sensing (MFDSS). The MFDSS includes three steps, sensing data, reputation propagation, fusion, and decision fusion.

The researchers first isolate extreme outliers by using sample kurtosis and significance table or z-test, which removes extreme outliers caused by byzantine failures. They used a reputation value to remove the extreme outliers. The fusion node decides whether the sensing inputs of the neighbouring nodes should be included in outlier detection using their reputation values. If the reputation value of a node is not present, the node is put in an incubation period chosen randomly by that particular fusion node.

MFDSS was tested in different network sizes from 50,100,150 to 200 with different malicious users (MUs) sizes from 10% to 40%. This scheme performs well with a number of malicious devices close up to 50% and degrades gracefully beyond that, which can be a drawback. In some network environment, the number of MUs can be above 50%. Our research considered MUs above 50%.

2.3.2 The weight sequential probability ratio test (WSPRT) [45], [46].

The work in [45], [46] addressed the SSDF attack by assigning each SU a weight value. It assessed the output of each user to determine how close it is to the output produced by the FC. If the binary output of a node was the same as that produced by the FC the reputation metric of the node was incremented by one, otherwise it was decremented. Each SU decided between two hypotheses when sensing the spectrum band, PUs being absent or present. The authors studied two types of attacks in this work, always reporting true attackers, that reports that the band is idle and the always-reporting false attackers that report the opposite of what they have sensed.

The advantage of this work was that it restored the reputation of nodes that temporarily misbehave. Results show that the drawback of this work was when the number of attackers was greater than the number of SUs because of the majority rule used. As the probabilities of the two hypotheses were fixed, the weight sequential probability ratio test (WSPRT) may not perform properly in a highly dynamic environment. Another drawback of this work was that it required a FC to make the final decision. In a distributed environment, a FC may not be favourable. Our research did not require the services of the FC for decision-making. Each SU performed its own fusion using its own observations and the observations of its neighbouring nodes. The sample sizes selected by the researchers were insufficient. Large sample sizes are required in order to achieve comparative results.

2.3.3 The hit and run attack [47].

The authors in [47] studied a different kind of attack known as the hit and run attack. This attack can change its reports by estimating its suspicious level. As long as the suspicious level of the attacker is below a predefined threshold value it will report incorrect observations. If it determines that its suspicious level is above the threshold value it will start reporting correct spectrum observations until its reputation is restored.

The authors defended against such an attack by determining the suspicious level of the nodes. If the suspicious level of the node becomes larger than the predefined value, a point value was assigned to the node. When it exceeds the predefined value its decisions were ignored permanently which was the drawback of this work. Unintentionally misbehaving nodes were permanently removed from final decision-making. This drawback was addressed by restoring the reputation of nodes that unintentionally misbehaved. Another drawback was that this attack type was investigated in CRN. Our research investigated this attack type in CRAHN and used the q-out-if-m rule scheme to defend against the attack.

2.3.4 Trust-based detection scheme [48].

Yu *et al.* in [48] proposed a scheme to mitigate the effects of the SSDF attack in CRAHN. In this proposed scheme, SUs perform spectrum sensing and exchanged their observations amongst each other. The SUs then computed the maximum deviation of the received information from the mean value. Users with the maximum deviation were assumed attackers and their inputs were ignored in the final decision-making. Each user decided that the band under test is occupied if the consensus was greater than a pre-defined threshold.

The final decision made by each SU depended on its own observation and the observations of its neighbouring nodes. The simulation results showed that the scheme performed well only with one attacker, which was a drawback of this work. In the simulation results, when the number of attackers were more than one the performance of the scheme seemed to degrade. In a network, the number of attackers may be more than one. Our research considered an environment with more than one attacker and three different types of attacks.

2.3.5 Double-Sided Neighbor Distance (DSND) algorithm [49].

Authors proposed in [49] the Double-Sided Neighbour Distance (DSND) algorithm to detect outliers. In this scheme, the SU was characterised as an outlier if its reports to the FC was too far or too close to the reports reported by other neighbouring nodes. There were two attack types that were studied, the independent attack where an attacker is unaware of the SUs reports and the dependent attack where the attacker knows the reports of the SUs. It was possible to detect the attacker in the independent attack but in the dependent attack, the attacker could not be detected. The drawbacks of this study were that the authors did not specify why the reports of secondary users that was too close or too far from the reports of others were regarded as malicious reports. The scheme filtered out legitimate SUs. Another drawback of this work was the presence of a FC, which was a disadvantage in a distributed environment. Our research uses a reputation-based approach to detect and discriminate outliers from SUs.

2.3.6 Adaptive reputation based clustering algorithm [50].

Chowdhury *et al.* in [50] proposed an adaptive reputation based clustering algorithm to defend against independent and collaborative SSDF attacks in CRN. The algorithm first clustered the nodes based on their sensing history and initial reputation. Each cluster took its decision about the channel availability by considering the relative closeness of the nodes from the median of that cluster. The spectrum band status was then decided on the majority of clusters decision. The final decision was then propagated back to the clusters and then to the individual nodes. Each node was assigned a share of the final decision and the reputation of each node was adjusted based on its participation in the decision-making process.

The work considered various numbers of attackers. Simulation results showed that the proposed scheme did not perform better in detecting attackers because of its majority rule. If in a cluster more than one SU is malicious, this can affect the final decision negatively. The drawback of the work was when there were many clusters containing malicious nodes that report incorrect spectrum observations, and then the final transmission decision would be incorrect.

Another drawback of the proposed scheme was that it depended on the majority rule for which majority can be incorrect. With a large number of attackers in a network, the error rate of this proposed scheme would be very high. We addressed this drawback by using the reputation-based system that considered the reputation of nodes. The reputation system filtered out outliers based on their reputation from several reports; it does not rely on majority rule.

2.3.7 Insistent SSDF (iSSDF) attack [51].

The work in [51] proposed a trust management scheme to mitigate the SSDF attack in CRAHN. The authors studied the SSDF attack and the insistent SSDF (iSSDF) attack. The iSSDF attack does not only report incorrect spectrum observations but it also broadcasts the falsified value in every iteration of the consensus and refrains from performing updates according to the protocol.

A trust management scheme was proposed to evaluate the performance through extensive Monte Carlo simulations. The author's implemented trust scores as weights for the average consensus update rule to mitigate the iSSDF attacks. Our research also suppresses the effects of the iSSDF by isolating the malicious nodes or outliers before the final decision is made using the reputation based system.

2.3.8 Density-based SSDF detection (DBSD) [52].

Chen *et al.* in [52] proposed a distributed scheme to mitigate the SSDF attack in cooperative spectrum sensing known as density based SSDF detection (DBSD). The scheme excluded abnormal sensing reports rather than detecting malicious users. They estimated the probability density of the random variable using the kernel-density estimator technique. Each sensing report was tested for abnormality. If a report is deemed as abnormal, the report would be excluded from decision making. The DBSD excludes all abnormal reports even reports from unintentionally misbehaving nodes. The scheme then calculated the average value based on the remaining sensing reports and compared the value to a PU detection threshold.

The drawback of this work was the assumption of a secure end-to-end connection between SUs. The work assumes that the communication is error-free and would not be tempered by attackers while attackers can tamper with the communication. An attacker can be part of the communication between the SUs and send incorrect data. Our research filtered all incorrect reports by using the q-out-of-m rule. Another drawback of this work was the assumption of malicious nodes being relatively small compared with the number of nodes in the network. The number of MUs in a network can vary; in our research, we tested our proposed scheme with varying number of MUs.

2.3.9 Joint Spectrum Sensing and data transmission (JSSDT) [53].

Wei *et al.* in [53] proposed a trust-based framework to protect both distributed cooperative spectrum sensing and data transmission from joint dynamic spectrum sensing and data transmission attack. The proposed scheme used a weight average consensus algorithm with trust values. The authors studied a new attack known as joint spectrum sensing and data transmission (JSSDT) attack. In this attack, MUs report falsified data in spectrum sensing and drop packets in the data transmission process. Nodes, which are found to have low trust values, are regarded as outliers and they are eliminated from decision-making.

The drawback of this work was that it can isolate nodes that are temporarily misbehaving as they have low trust values. One way of addressing this drawback was to eliminate nodes with low trust values from decision making but not permanently. The nodes with low trust value should be eliminated permanently once their threshold value reaches a predefined threshold. If the nodes start behaving non-maliciously again, their trust values could be restored. Our research accommodates unintentionally misbehaving nodes by restoring their reputation.

2.4 Conclusion

Different researchers have proposed different schemes in attempting to mitigate the effects of the SSDF attack. This chapter focused on evaluating the proposed schemes to identify caps that need to be filled. We compared our proposed scheme with the existing schemes to evaluate its scientific contribution and its efficiency in filing up the caps that need to be filled in other researcher’s work.

CHAPTER THREE: METHODOLOGY

3.1 Introduction

This chapter presents the methodology used to implement the proposed scheme. We discuss the simulation tools that were used and the simulation parameters. Selection of the number of nodes used to simulate the scheme and the analysis of the chosen tools are discussed.

3.2 Methodology

This research proposed the integration of two infrastructure-based schemes in an infrastructure-less topology. The reputation and the q-out-of-m rule schemes were used to mitigate the effects of the SSDF attack.

In the proposed scheme, the SUs attained the spectrum observations of their direct neighbours. They assessed their reputation and selected the reports of the neighbours with good reputation for further evaluation in the q-out-of-m rule.

The q-out-of-m rule was used to defend against MUs that were able to alter their reports to not be considered as outliers. The q-out-of-m scheme selected 60% of m out of n reports, n which was the SUs with good reputation and m which was the random selection. Q, which is the final transmission decision, was selected from m. The final transmission decision was based on q which was the majority number of nodes. If q nodes reported that the spectrum band was not utilised, the final decision was that the spectrum band was idle. If q number of nodes reported that the spectrum band was utilised, the final decision was that the spectrum band was utilised by PUs.

We used reputation propagation to propagate the reputation of the nodes to other SUs. In the reputation-based system, If the reputation of a node reached a predefined threshold value of 0.6, that node was considered as an outlier and isolated from the network. Non-malicious users that unintentionally report incorrect observation`s reputation were restored if the SUs discontinued reporting incorrect observations.

Matlab was used to implement and simulate the proposed scheme in Windows 10 operating system because it was compatible with Matlab tools. The results of the proposed scheme were compared with the Multi-fusion-based distributed spectrum-sensing scheme (MFDSS) [33] and Density-based Distributed Scheme (DBSD) [52]. The MFDSS scheme was implemented by pongaliur [33] in a distributed environment. The scheme also used the reputation-based system to filter out outliers from the final decision-making. The authors also considered different network sizes. The DBSD scheme used a statistical approach to detect and isolating the SSDF attack, which was desirable in our study to compare the two different approaches.

3.3 Evaluation plan

The simulation tool that was used was Matlab simulation tool in Windows 10 operating system. The scheme was tested considering the network sizes and the number of malicious nodes in the network. The evaluation was done using different network sizes from a small sized network to a large-sized network choosing the malicious nodes from 10%, 20%, 40%, and 50% to 60%. The simulation parameters are shown in table 1.

Table 1: List of simulation parameters

Parameter	Setting
Antenna type	OmniAntenna
MAC protocol	IEEE 802.11 with extension to support CR networks
Data channel	8
Common control channel	1
Channel data rate	11 M bits/s
Number of SUs	10, 20, 50,100,250
Number of selfish SU	10%,20%,40%,50%,60%
Propagation model	TwoRayGround
Grid size	1000m * 1000m
Fusion Time	0.5s
Primary user detection type	Energy detection
Mobility type	Random waypoint model

Sensing type	Cooperative spectrum sensing
Figures	E-Draw was used to design and draw figures

Matlab simulation tool was considered in this research because different researchers in their work have used it. It had the necessary tools needed to effectively simulate the proposed scheme. Matlab works best in windows operating system thus it was installed in windows 10 operating system.

There are several methods used to detect PU signals, which include energy detection, cyclostationary, based sensing, radio identification and matched filtering [54], [55], [56]. The SUs in this research sensed the spectrum band using energy detection because it was simple to implement and it did not require prior knowledge of the SUs [57], [58].

Spectrum sensing can be conducted in one of two ways. Cooperatively or non-cooperatively. Cooperatively, whereby the SUs sense the spectrum band and share the information with each other before making the final transmission decision. Non-cooperatively, where a SU senses the spectrum band and makes the decision. In this research, we considered cooperative spectrum sensing because it was more effective and more recommended than non-cooperative spectrum sensing.

3.4 Conclusion

This chapter has discussed the simulation tools that were used and the simulation parameters. Discussion of the reputation and q-out-of-m rule scheme has been discussed along with the performance metrics that were used in simulating the scheme. The numbers of nodes chosen for simulation were 10, 20, 50,100 and 250. This varying number has been chosen to evaluate the performance of the proposed scheme in a small-sized network, a medium-sized network and a large-sized network. The simulation tool that was chosen to simulate the scheme is Matlab simulation tool.

CHAPTER FOUR: DESIGN AND IMPLEMENTATION

This chapter presents the design and implementation of the reputation and q-out-of-m (R-and-q-out-of-m) rule scheme. The overview of the network model is presented and we model the CRAHN environment implemented in the study. We used the detection theory to model sensing technique used. The results of the scheme are presented using binomial distributions and theoretical results are presented.

4.1 Network model

The network environment consists of two types of users, The PUs that are licenced to utilise the spectrum band at any time and the SUs that utilise the band opportunistically when the PUs are inactive. The SUs have cognitive capabilities that enable them to utilise the band without causing interference to the PUs transmission. We use the detection theory to model the relationship between The SUs and the PUs. The SUs perform spectrum sensing using energy detection to determine the vacant channels as depicted in figure 1.

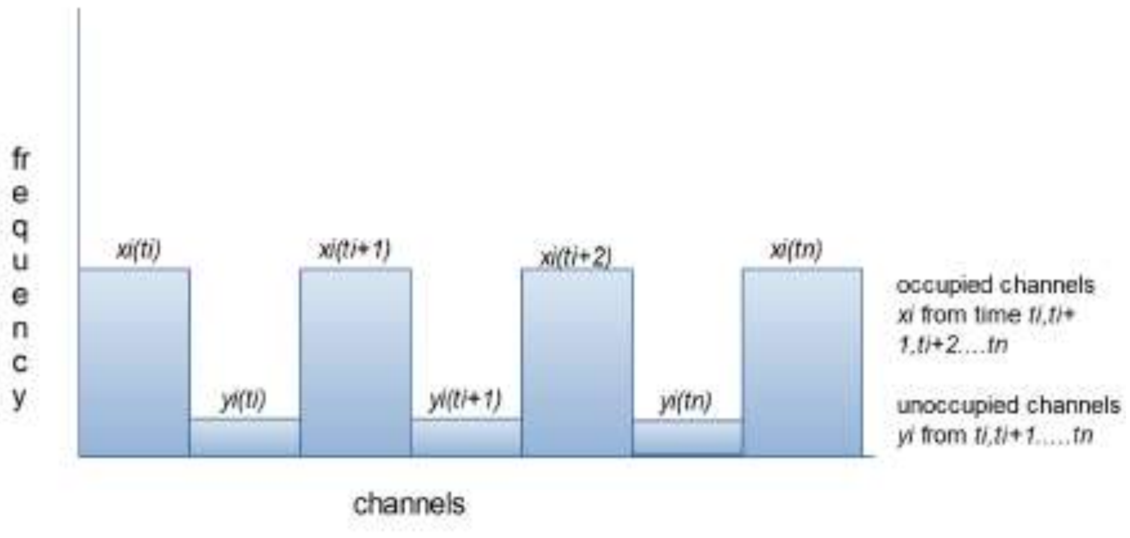

frequency
xi(ti)
xi(ti+1)
xi(ti+2)
xi(tn)
yi(ti)
yi(ti+1)
yi(tn)
occupied channels xi from time ti,ti+1,ti+2....tn
unoccupied channels yi from ti,ti+1.....tn
channels

Figure 1: channel selection model

Figure 1 depicts spectrum sensing in Reputation and q-out-of-m rule scheme (R-and-q-out-of-m). Given L number of channels, the SUs sensed the channels cooperatively at different time intervals from $t0 \dots \dots tn$ to detect the white spaces or the off periods in the band of PUs modelled as $y_i, y > 0$ and $i = 1, 2., , 3 \dots \dots n$ at different time intervals, $ti, ti + 1, ti + 2 \dots \dots tn.$ The vacant channels y_i are the channels that the SUs used for transmission. We model the channels states using probability density function (PDF). The function $F_pon(i)(x), x > 0$ denotes the probability density function of the ON periods of PU transmission at a particular channel i. The function $F_poff(i)(y), y > 0$ denotes the probability density function of the OFF states of PU transmission at channel i, from $i1, i2 \dots . in - 1.$ This can be modelled as a semi Markov state diagram as shown in figure 2.

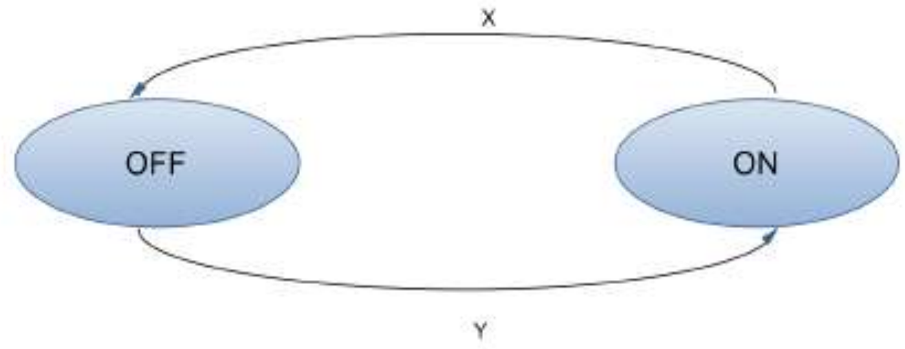


Figure 2: Semi-Markov state diagram

Figure 2 shows a semi Markov state diagram of the channel periods. We assume that the ON and OFF periods are independent of each other. The channels periodically transit between states $(ON|OFF)$ at different time intervals $i1, i2 \dots . in\ 1$. The PDF is given by:

$$P.D.F\ Fp_{ON}(i)(x)|Fp_{OFF}(i)(y) \qquad (1)$$

The SUs determine the off periods by detecting the signal strength of the PUs in the channels using energy detection. For a given frequency band, spectrum sensing was formulated as a binary hypothesis as follows:

$$H_0: x_i(t) = n_i(t), i = 1,2 \dots . \qquad (2)$$

$$H_1: x_i(t) = c_i(t)s_i(t) + a_i(t), i = 1,2 \dots , N, \qquad (3)$$

Where H_0 denotes that the PU signal is absent and H_1 denotes that the PU is present. N being the number of SUs $x_i(t)$ is the i^{th} sample of the received signal,

$s_i(t)$ is the PU transmission signal and $c_i(t)$ is the channel gain, while $a_i(t)$ denotes the additive white Gaussian noise (AWGN). The energy E of a given signal $x_i(t)$ is:

$$E = \int_{-\infty}^{\infty} |x_i(t)\,|\text{^}2\; dt \qquad (4)$$

This can be modelled using Perceval's theorem as:

$$\int_{-\infty}^{\infty} |x_i(t)\,|\text{^}2\; dt = \int_{-\infty}^{\infty} |x_i^{\pi}(f)\,|\text{^}2\; dt \qquad (5)$$

Where $x_i^{\pi} = \int_{-\infty}^{\infty} e^{-2\pi i}\, dt$ (6)

The received energy observation E_o can be modelled as a Normal random variable with mean u and variance σ^2 following the hypotheses H_0 and H_1

$$\begin{cases} H_0: E_o \sim N(u_i, \sigma_i^2) \\ H_1: E_o \sim N(u_{i_1}, \sigma_{i_1}^2) \end{cases} \qquad (7)$$

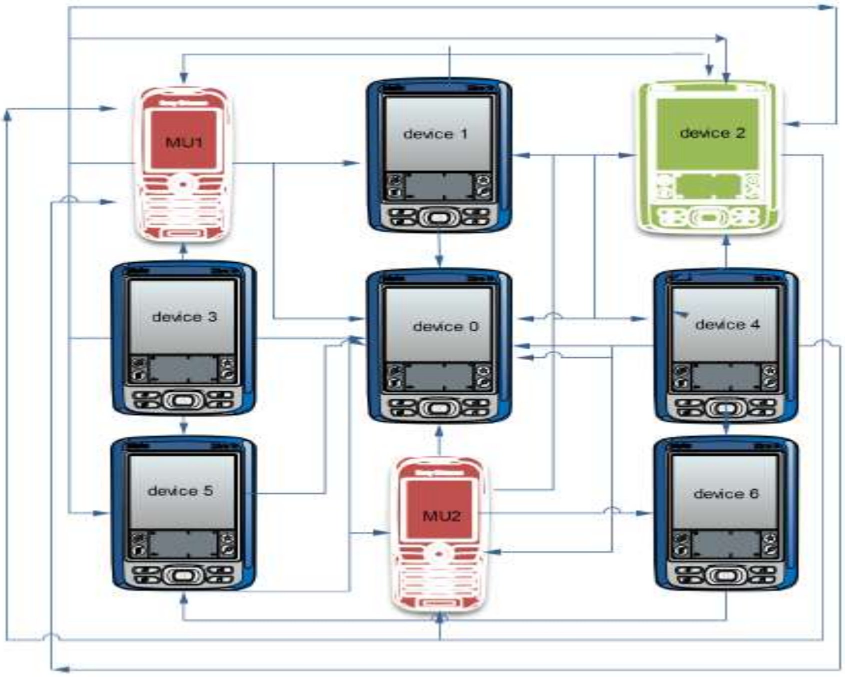
Comparing $E_o$with a given threshold value γ_1, the local binary decision φ was obtained as:

$$\begin{cases} H_0: E_o < \gamma_1 \quad where \quad E_o \sim N(u_i, \sigma_i^2) \\ H_1: E_o > \gamma_1 \quad where \quad E_o \sim N(u_{i_1}, \sigma_{i_1}^2) \end{cases} \qquad (8)$$

The local binary decision φ was based on the following criteria

$$\begin{cases} \varphi > E_o \; accept \; H_1 \,, conclude \; that \; PU \; is \; present \\ \varphi < E_o \; accept \; H_0, conclude \; that \; PU \; is \; absent \\ E_o < \varphi < E_o \; accept \; H_1 \,, make \; another \; observation \end{cases} \qquad (9)$$

After the SUs in R-and-q-out-of-m rule scheme cooperatively sense the spectrum band, they establish a link for data exchange to share their observations with each other as illustrated in figure 3.



🟩 Unintentionally misbehaving secondary users

🟦 Honest secondary users

🟥 Malicious secondary users

Figure 3: cooperative spectrum sensing

Figure 3 illustrates cooperative spectrum sensing, where each SU or node collects the sensing data from its neighbouring nodes $Nni\ , i = \ 0,1,2 \ldots \ldots n$ at different time intervals $t0, t1 \ldots tn$ .The fusion node, Node$i$ (ni) receives the sensing results from its neighbouring nodes. The sensing results (sr) of Nni at ni are given as follows:

$Sr(ni)\ = \{Nn1, Nn2, Nn3, Nn4, Nn5 \ldots \ldots \ldots \ldots .Nnn\}\ OR$

$$Sr(ni) = \sum_{i=1}^{n} Nni \qquad (10)$$

$Where\ Sr\ = \ \{0\ if\ PUs\ is\ absent, 1\ if\ PUs\ is\ present.$

$H0: PUs\ present$

$H1: PUs\ absent$

The neighbouring nodes compute the binary report using (1) and report the binary decision 0 or 1 to the fusion node as given in (2). The variable ni accesses the reputation of the nodes to determine their trustworthiness, isolates the nodes with bad reputation and implements the q-out-of-m rule scheme to make the final transmission decision.

4.2 Malicious nodes

We assume the presence of one or more MUs that either cooperate or do not cooperate in performing the SSDF attack. Cooperative attack occurs when the MUs launch the SSDF attack by collaborating in the channels they want to falsify. Non-cooperative SSDF attacks do not collaborate in conducting the SSDF attack. Figure 4 illustrates the reputation and q-out-of-m network architecture the study has implemented.

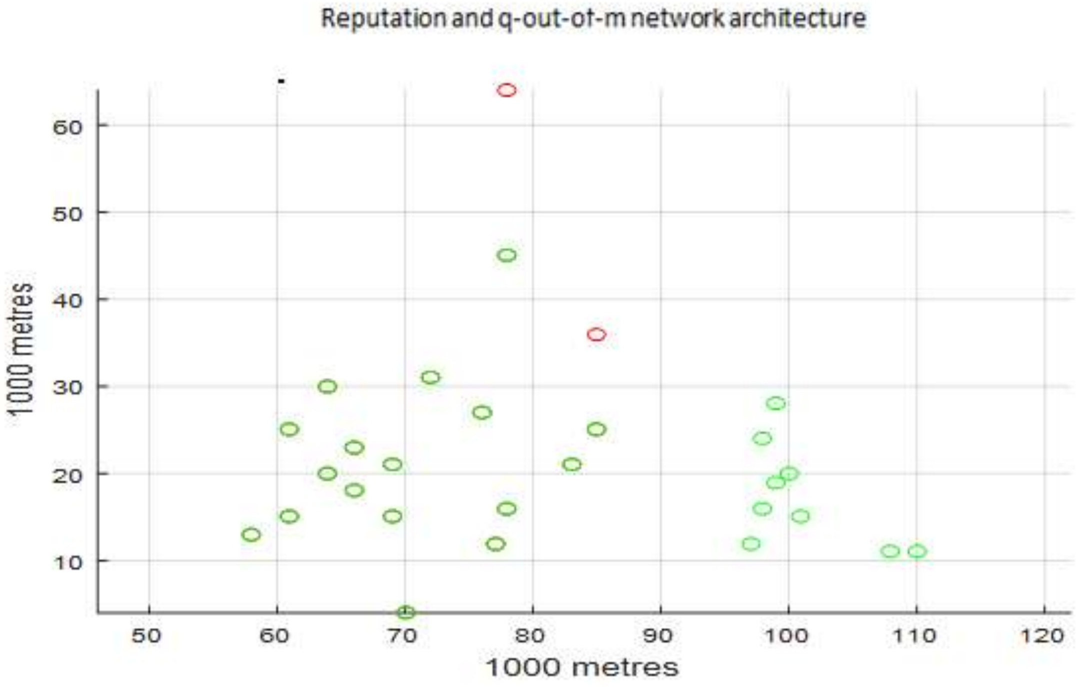


Figure 4: network model

Malicious Users ○ Honest Users● Misbehaving Users ○

Figure 4 illustrates the R-and-q-out-of-m network architecture, where we have honest Users, misbehaving users, and malicious users (MUs). MUs are classified into two types, the always true and always false attacks. The always true report that spectrum band which is idle is occupied. The always-false attacks report that the band is idle while it is occupied by PUs. Let $g_m(t)$ be the final decision at ni at any given time t from $t0\ to\ tn - 1$, and then the always-true MUs are defined as:

$\forall i\ where\ i\ \in \{Nni\}, gm(t) = 1\ when\ PU = 0$

$\exists i \; where \; i \in \{Nni\}, gm(t) = 1 \; when \; PU = 1$ (11)

The always false attacks:

$\forall i \; where \; i \in \{Nni\}, gm(t) = 0 \; when \; PU = 0$

$\exists i \; where \; i \in \{Nni\}, gm(t) = 0 \; when \; PU = 1$ (12)

The always true and always false attacks are easy to detect and can be filtered out of the network by implementing any fusion scheme. We studied a new attack known as the hit and run attack. The hit and run attack can alter its observations so that it cannot be detected as an outlier. This type of attack is difficult to detect in an ever-changing mobile topology such as CRAHN. We also studied Byzantine failures in the network which are caused by malfunctioning sensing terminals which cause the unintentionally misbehaving nodes. These nodes report incorrect sensing observations to their neighbouring nodes because of the Byzantine failures; caused by multipath fading, signal fading and hidden terminal problem. To correctly detect the PUs transmission; we can use the following binomial distribution:

Let s measure successful PU detection with Φ number of successes and f measure the success probability with $\delta = 1 - \Phi$ failure rate, with N SUs given by $\sum_{i=1}^{N} s_i$. Given Φ and δ, the probability of correctly detecting PUs transmission can be measured by a binomial probability distribution as follows:

$$\binom{n}{\Phi} = \frac{n!}{\Phi!(n-\Phi)!} = P(\Phi) = \binom{n}{\Phi} s^{\Phi} f^{n-\Phi}, \Phi = 0,1 \ldots \ldots, n \; and \; 0 \leq p \leq 1. \tag{13}$$

With mean

$$E(\Phi) = \sum_{\Phi=1}^{n} \Phi \frac{n!}{(n-\Phi)!\Phi!} s^{\Phi} f^{n-\Phi} = \sum_{\Phi=1}^{n} \Phi \binom{n}{\Phi} s^{\Phi} f^{n-\Phi} = ns. \tag{14}$$

And variance

$$\sigma^2 = ns[(n-1)s + 1 - ns] = ns(1-s) = nsf. \tag{15}$$

4.3 Probability of false alarm, detection and missed detection

We used the detection theory using binomial distributions to analyse the proposed scheme results with the MFDSS and DBSD results in figure 5 to 7. We evaluated the proposed scheme effectiveness in reducing the probability of both the positive and negative false alarm. Positive false alarm is the detection of legitimate SUs as MUs. Negative false alarm is the detection of MUs as legitimate SUs. We obtained the results of figure 5-7 using Matlab and we used chart-blocks plot to plot the graphs. The results from figure 5-7 show that the proposed scheme managed to reduce the false alarm probabilities effectively.

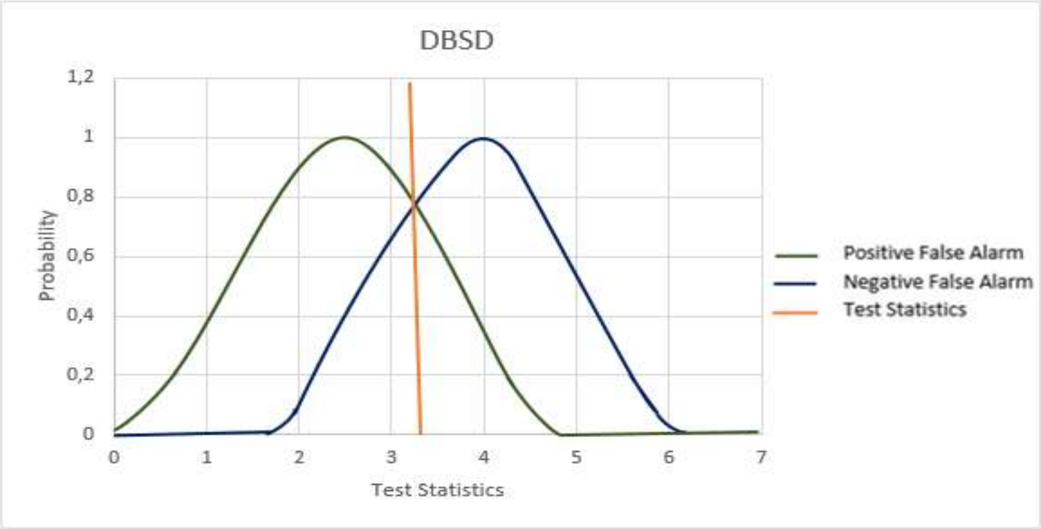


Figure 5: Binomial distribution for Density Based System

Figure 5 shows the binomial distribution for the DBSD scheme. The negative false alarm for the DBSD was reduced by 55% while the positive false alarm was reduced by 45%. The binomial distribution for MFDSS scheme using detection theory is shown in figure 6.

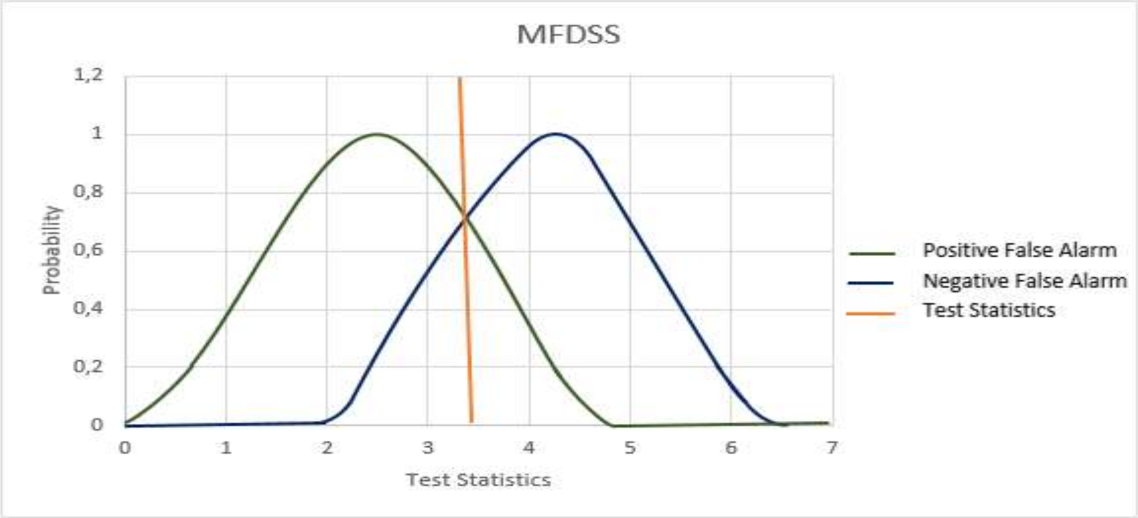


Figure 6: Binomial distribution for Multi-Fusion Based System

Figure 6 shows the binomial distribution for the MFDSS scheme. The negative false alarm was reduced by 62% while the positive false alarm was reduced by 70%. The binomial distribution for the proposed scheme using detection theory is shown in figure 7.

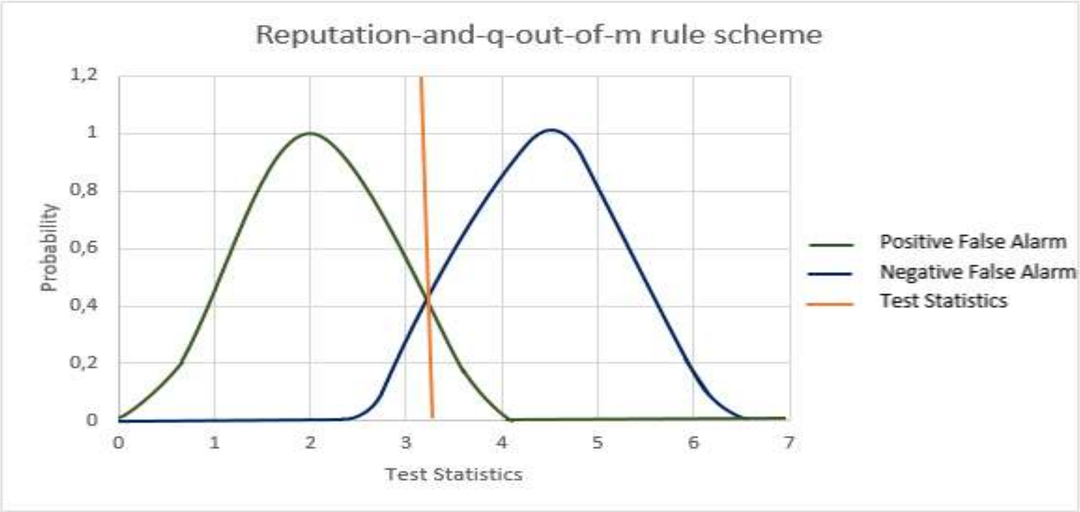


Figure 7: Binomial Distribution for r-and-q-out-of-m rule scheme

Figure 7 shows the binomial distribution for the proposed scheme. The negative false alarm for the scheme was reduced by 82% while the positive false alarm was reduced by 88%. The figures 5-7 show that the proposed scheme in figure 7 has the lowest margin of the test statistics. This means that the positive and negative false alarms in the proposed scheme are significantly reduced compared to the other schemes. The proposed scheme performed better in reducing the positive and negative false alarms. Chapter five gives more results of the proposed scheme.

4.4 Mobility

We used the random waypoint model to model the movement pattern of the nodes given a mobile network. We implement the random waypoint to discourage malicious devices conducting the hit and run attack. The random waypoint model is illustrated in figure 8.

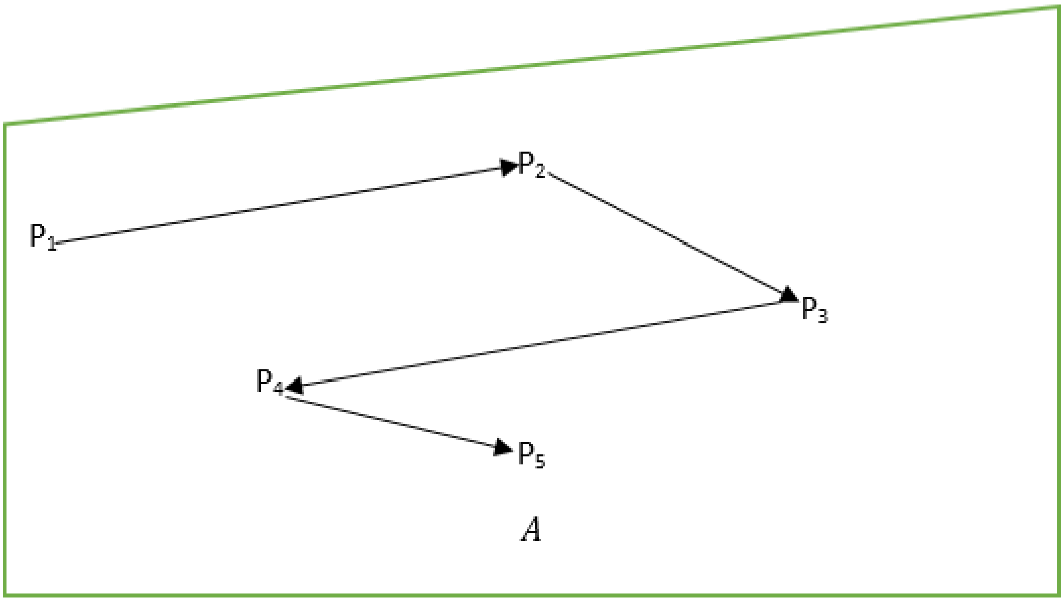


Figure 8: Random waypoint model [59]

The points in figure 8 are uniformly distributed and are independently and identically distributed (iid) with mean 0 and variance 0.They move at a random distance d given by:

$$d = \sqrt{(\Delta x)^2 + (\Delta y)^2} = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \qquad (16)$$

Where $(x_1, y_1), (x_2, y_2)$ are the coordinates in the network model. [59]

4.5 Reputation-Based System

After sensing the spectrum band, the SUs exchanged their local binary measurements of the status of the PUs with their neighbours. The comprehensive reputation of node *i* on node *j* at time *n* is denoted as Tnj which is computed as a combination of the current trust and the historical trust at time $tn - 1$. The value update scheme based on reputation can be described as

$$Xi(n + 1) = Xi(n) + y \qquad (17)$$

In the reputation-based system, the SUs assessed the reputation of the neighbouring nodes to determine their trustworthiness based on the threshold value $\gamma = 0.6$. Nodes with reputation values above 0.6 were isolated from the network because we classify them as MUs. Each node was assigned a reputation value. The reputation threshold γ is chosen to be 0.6 because we were accommodating unintentionally misbehaving nodes. All the values that are below the threshold γ were selected for the q-out-of-m rule fusion. The main objective was to not cause interference to CRAHN thus we integrated the reputation-based system with q-out-of-m rule scheme to isolate all the remaining outliers that were missed by the first fusion step. In algorithm 1, the SUs binary reports are either selected or not selected. If the sensed data of the SUs does not contain malicious observations, then the algorithm states that the final decision made by the particular SU at a particular time should be the same as the report of the SUs. If the report is not the same, we increment the reputation value of the SUs by 0.1 otherwise we decrement by 0.1. The following algorithm 1 gives the reputation-based system:

Algorithm 1

```
$if\ s_i(t) < \gamma\ then$
        $s_i(t) = 1$
  $else$
        $s_i(t) = 0$
  $if\ s_i(t) \not\subset outlier\ then$
        $if\ d_i(t) == g_m(t)\ then$
$r_{m_i} = r_{mi}$
              $else$
$if\ d_i(t) \neq g_m(t)\ then$
$r_{mi} = r_{mi} + 0.1$
$else$
$r_{mi} = r_{mi} - 0.1$
```

Where m is the node-id of the assessor node at that particular time. The assessor node is the node that is conducting the fusion at a given time to isolate outliers. All the SUs in our network are assessor nodes. i is the node-id of the neighbouring node, $d_i(t)$ is the status of the PU. $S_i(t)$ is the value of the report from the neighbouring node i with 1 denoting selected and 0 denoting not-selected. The $g_m(t)$ is the final decision at node m. The $r_m i$ is the current reputation of node i at device m. The γ_2 is the threshold value. This algorithm shows that the decision submitted to the assessor node is either selected 1 or not selected 0 depending on its reputation metric. If the node is not an outlier, the node is not panelised. A node that is an outlier and reports incorrect spectrum occupancy is penalised by increasing its reputation value by 0.1. A node which misbehaves for a while but is not a malicious node, its reputation value is decreased by 0.1.

4.6 Reputation Management

To manage the reputation of the nodes in the mobile topology, reputation propagation was implemented to propagate the reputation of the nodes to all the secondary networks. The reputation is updated periodically to maintain the freshness of the reputation information.

4.7 Q-out-of-m rule scheme

The q-out-of-m rule scheme polls 60% of the nodes from the nodes with good reputation and decides that the PU is present if q or more sensing reports report 1 as follows:

Algorithm 2

```
Step 1: Poll a random number m from reports with good reputation $Nri\ at\ t0, t1 \dots\dots tn - 1$.
Step 2: check majority report ($m_r$) from the randomly polled m.
$If$
$m_r > m$
$then$
$m_r = q$
Step 3: Make the final transmission decision ($g_m(t)$) at $t0 \dots\dots tn\ g_m(t)\varepsilon[0,1]$.
$if$
$q = 1$
$then$
$g_m(t) = 1$
$else$
$g_m(t) = 0$
```

In algorithm 2, a random number of reports *m* from the ones with good reputation were selected. The majority of reports were assessed to determine q, q=mode value. If the majority of nodes report that, the spectrum band is occupied by PUs then $q = 1$ and the final transmission decision $gm(t)$ is one. In figure 9 we show the flow diagram of the reputation-and-q-out-of-m rule scheme.

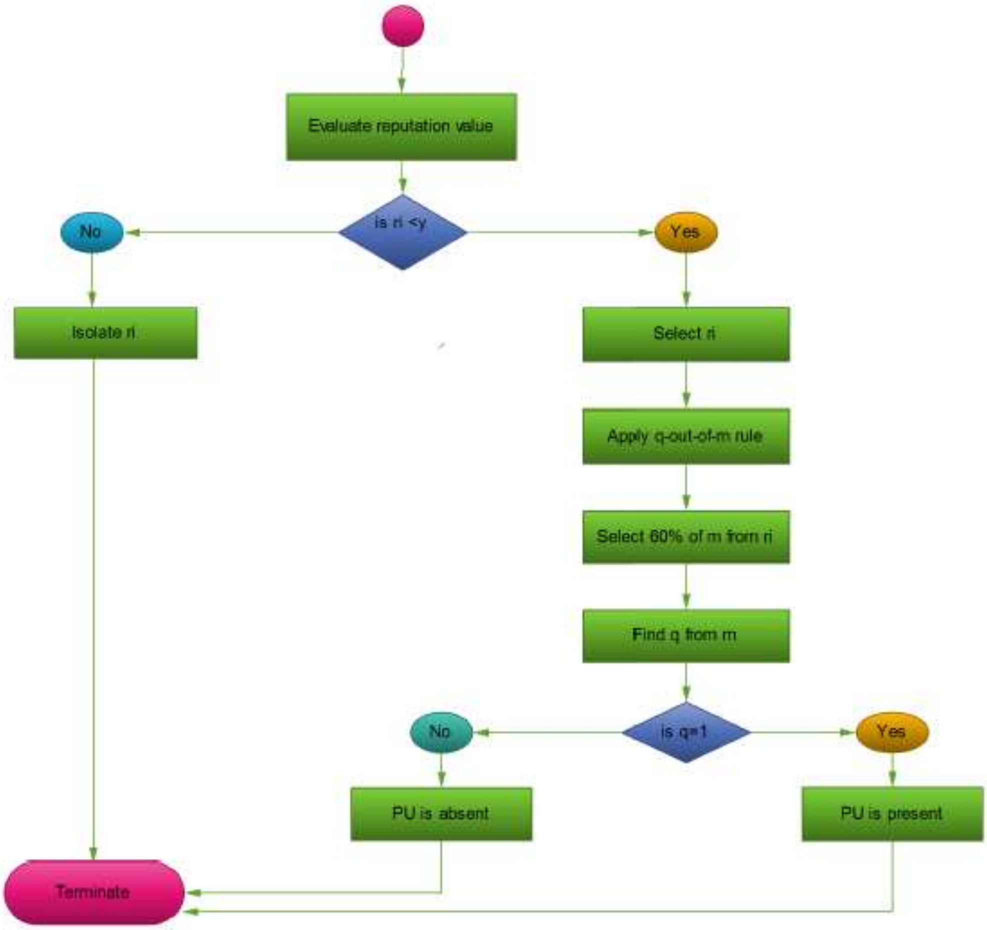


Figure 9: flow diagram of the reputation and q-out-of-m rule scheme.

Figure 9 shows a flow diagram of the proposed scheme. The SUs share their sensing reports with each other. Each SU evaluates its neighbour's reputation to determine their trustworthiness. All the nodes with reputation values that are above 0.6 are isolated. The nodes with reputation values below 0.6 are selected for the next fusion phase. In q-out-of-m rule scheme, 60% of the nodes are selected from the nodes with a good reputation and the final transmissions decision is based on q. if q is 1, the final decision is that the spectrum band is utilised by PUs. If q is 0, the final decision is that the spectrum band is not utilised by PUs.

4.8 Metrics

The metrics used to evaluate the proposed scheme were the success probability, missed detection probability and false alarm probability which are given by the following equations:

Let $DSUs$ be the detected SUs and $TSUs$ be the total number of SUs. The false alarm probability is given by:

$$\boldsymbol{FAp} = \frac{\boldsymbol{DSUs}}{\boldsymbol{TSUs}} \tag{18}$$

Let TA be Total attack and AD be attacks detected. The missed detection probability is given by:

$$MDp = \frac{TA - AD}{TA} \tag{19}$$

Let AD be the attacks detected .The success probability is given by:

$$Sp = \frac{AD}{TA} \tag{20}$$

The probability of false alarm is the probability that a channel is occupied by PUs $(H0)$ while it is not. This is denoted by:

Pf or $P(H1|H0)$ (21)

The probability of missed detection is the probability that a channel which is occupied by PUs is detected to be idle $(H1)$. This is denoted by the following:

Pd or $P(H0|H1)$. (22)

4.8 Theoretical results of the proposed scheme

In this section, we present the theoretical analysis of the proposed scheme. We Studied and analysed the behaviour of MUs comparing it to the behaviour of honest users. We used Matlab to implement the proposed scheme. We selected some results we obtained from Matlab to draw the graphs using excel because we wanted to distinguish the behaviour of outliers compared to SUs, misbehaving SUs and the hit and run attack. Figure 10 shows the behaviour of the each studied SU in this research work. We show the Normal SUs, the unintentionally misbehaving SUs, the hit and run attack and the always yes and always no attack.

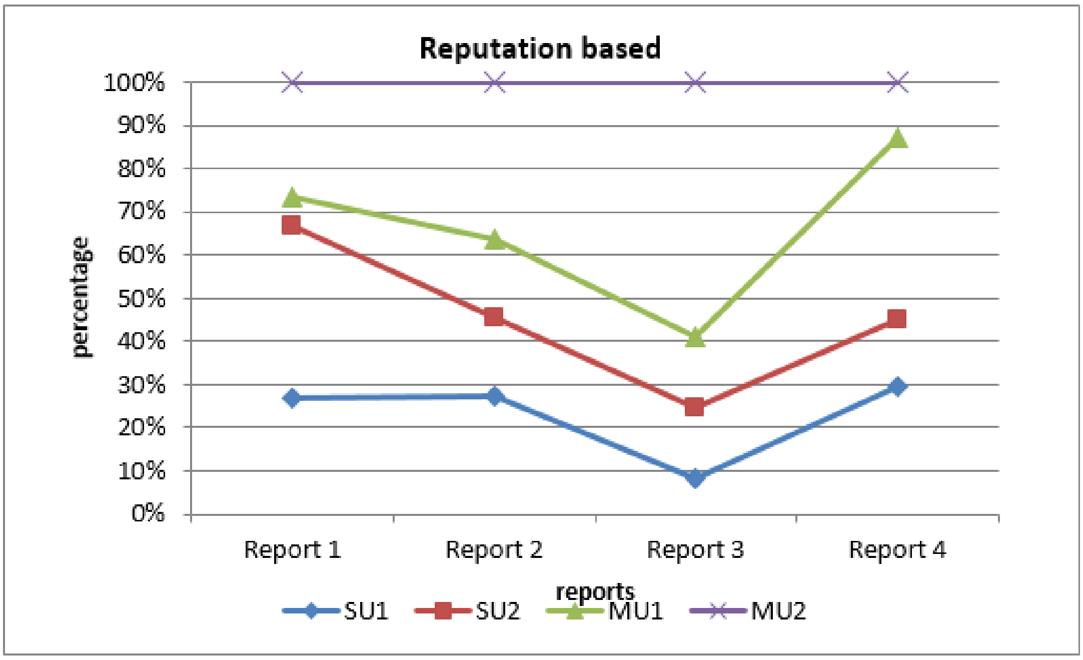


Figure 10: Studied SUs in the network

In figure 10, we plot the results of the different kinds of SSDF attacks strategies studied in this work. We studied the honest SUs referred to as SU1 and denoted by the blue star line that has reputation values below the threshold value of 60%. These SUs do not exhibit MUs properties in their reports hence their reputation values are always below 60%. We also studied the unintentionally misbehaving SUs that report the opposite of what they sensed due to Byzantine failures in the network. The second type of SU, the SU2 denoted by the red line in figure 10 known as the unintentionally misbehaving SUs, which exhibits some malicious behaviour that makes its reputation metric percentage to rise above 60%. MU1 in figure 10 can alter its reports to avoid being classified as an outlier; as a result, its reputation index will fluctuate below and above the threshold. MU2 always report incorrect observations. We studied two types of MU2, the always yes which always reports that the spectrum band is occupied while it is not. The always no, which reports the unoccupied spectrum band is occupied. These MUs are regarded as outliers and their observations are excluded from the decision making phase.

The q-out-of-m rule scheme, which is the second fusion phase of the proposed scheme, is implemented after the reputation based system. After evaluating the reputation of the nodes using the reputation-based system, nodes with a good reputation are selected for the q-out-of-m rule scheme. The q-out-of-m rule is implemented again to address the hit and run attack. We discuss the q-out-of-m rule in detail in the sequel:

Suppose we have a network model with 21 SUs from node 0 to 21. Nodes 1 to 21 report their sensed data to node 0 at different time intervals $t1 - tn$. Let Nr be the SUs with good reputations. Let 1 denote the presence of a PU and zero denote the absence of PUs in the spectrum band. Then 60% of m which is the average number of nodes with good reputation is polled from m. Then q which is the majority of reports from m , is used to make the final transmission decision. If the majority of nodes from m report 1, the SUs can conclude that there is an on-going PU transmission. If the majority report 0, the SUs can conclude that the spectrum band is idle as depicted in figure 11.

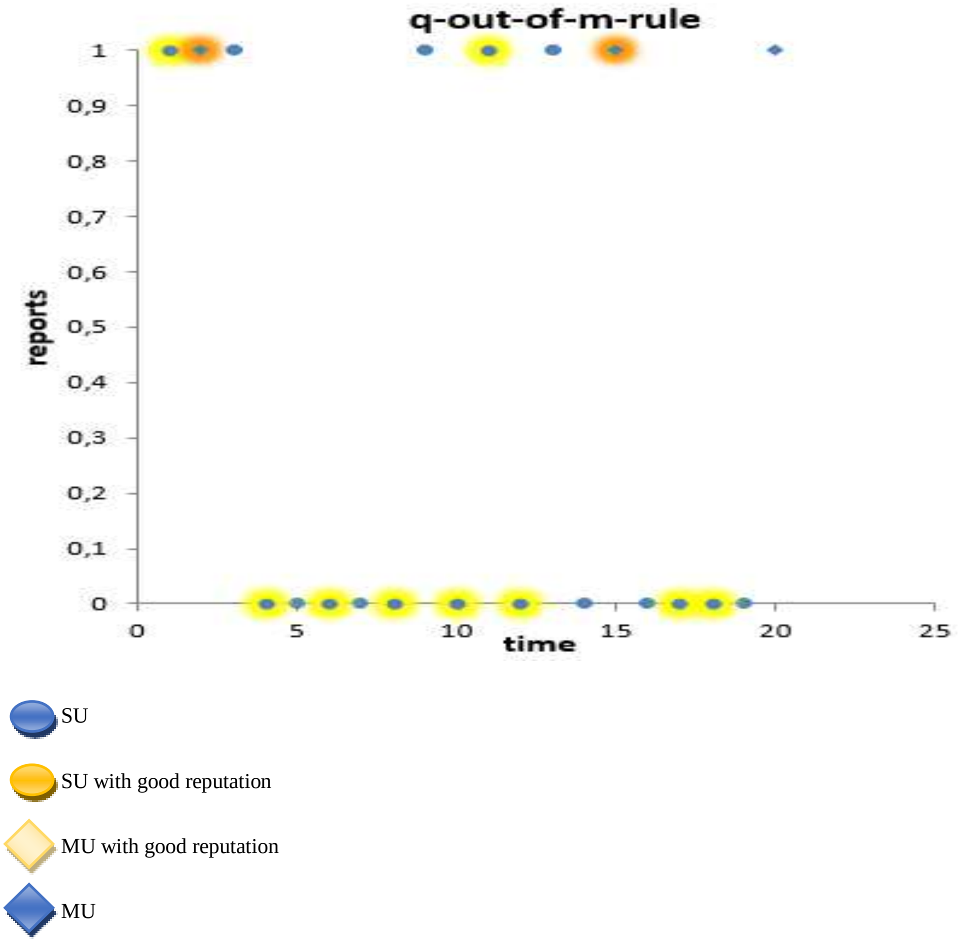


Figure 11: Q-out-of-m rule scheme

Figure 11 shows the q-out-of-m rule scheme performed by node 0. In this case, all the 20 nodes reported their observations to node 0. The reported reports can be 0 or 1. Node 0 then selects the nodes with good reputations at random time intervals from $t0 - t25$ mini-seconds as highlighted in figure 11. The nodes which are not highlighted are the ones with bad reputation, thus they are excluded in the decision making process. Nodes highlighted in yellow denote non-malicious SUs with good reputation. Nodes highlighted in orange denote the hit and run attack. After Nr has been selected, 60% of m nodes are randomly polled from Nr depicted in figure 12 with a green highlight. In figure 12 have only one node reporting 1, that the spectrum band is occupied and 7 nodes reporting 0, that the spectrum band is idle. The final decision is informed by $(q = 7)$. The final decision made by node 0 will be that the spectrum band is idle.

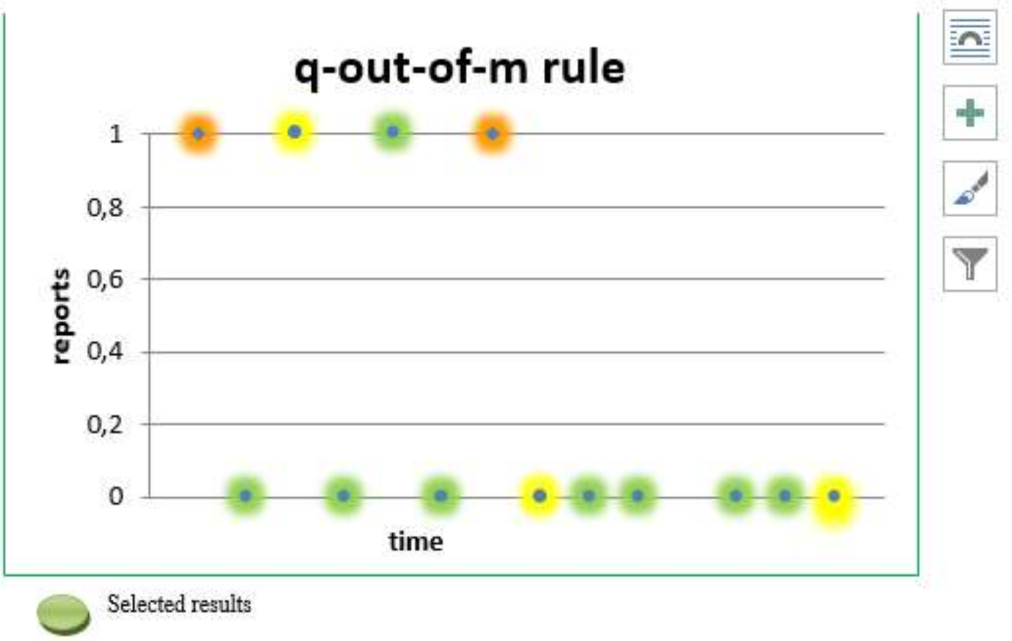


Figure 12: Final decision-making

When transmissions were completed, the SU updates its reputation table by decrementing the reputation of the nodes that reported correct observations and incrementing the reputations of those which reported incorrect observations. The reputation information and the time stamp of the last update of the reputation were propagated.

4.7 Conclusion

Chapter four, the proposed scheme was modelled using detection theory, semi Markov diagram, binomial distribution, algorithms and a flow diagram. The network architecture was designed and the proposed scheme was evaluated using theoretical results. The mobility of the study was presented and the evaluation methods are given with formulas. MUs were explained and the types of MUs we studied were given with their behaviour. We managed to categorise MUs according to their behaviours and we managed to distinguish between the unintentionally misbehaving SUs and MUs.

CHAPTER FIVE: RESULTS AND DISCUSSIONS

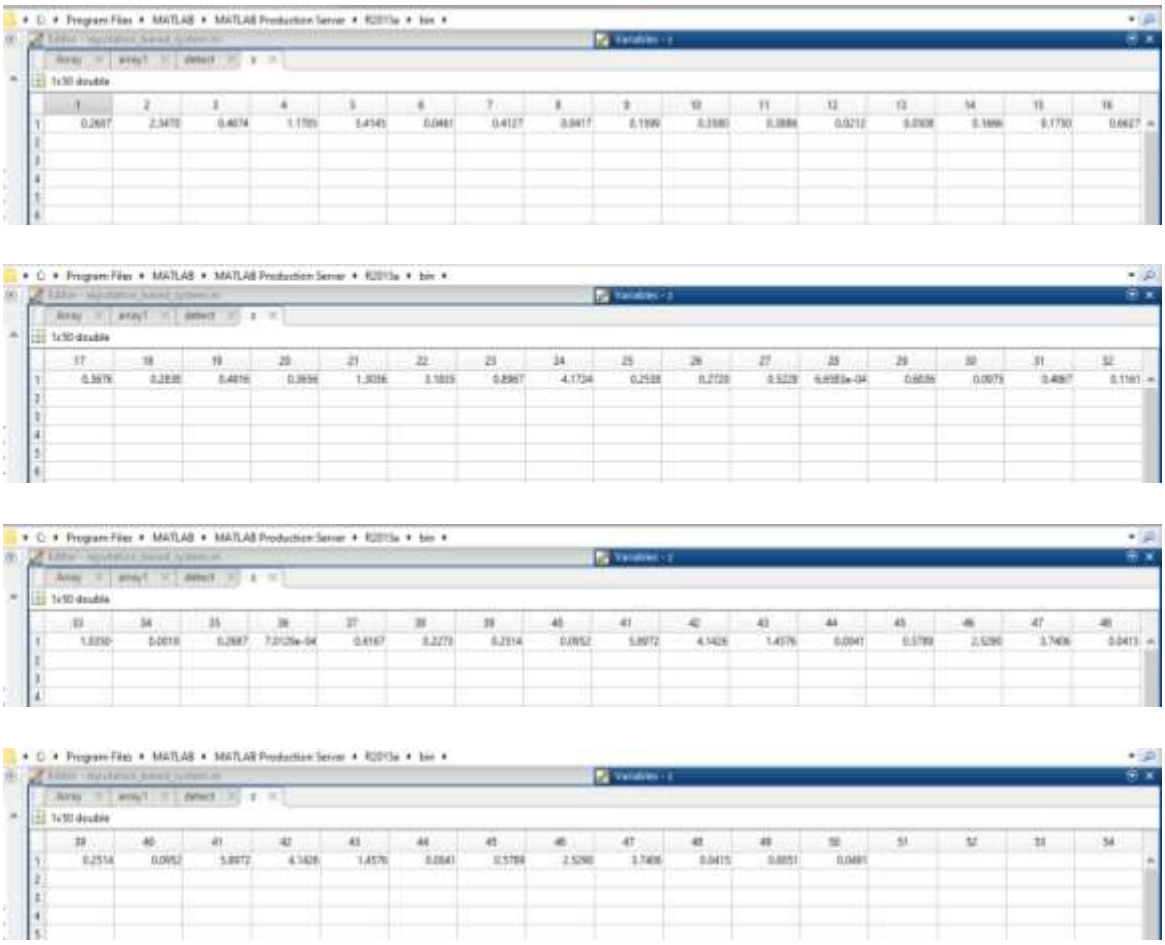
In this chapter, we present the simulation results of the performance analysis of the reputation and q-out-of-m rule scheme. We compare the proposed scheme to the Density Based Distributed System (DBSD) scheme [52] and the Multi-Fusion Based Distributed Spectrum Sensing (MFDSS) scheme [33], in terms of their effectiveness in detecting malicious nodes, the accuracy of cooperative sensing under attack, and making the correct final decision.

The following metrics were used to evaluate the scheme: success probability, missed detection probability, and false alarm probability. The scheme was compared with two existing schemes that combat the SSDF attack, the MFDSS and DBSD schemes. The schemes were implemented in CRAHN. The MFDSS was implemented using the reputation-based system to combat the SSDF attack. The DBSD scheme was implemented using the kernel-based system to combat the SSDF attack. To evaluate the effectiveness of the proposed scheme, a number of different network sizes were considered. The network sizes ranged from the smallest network with 10 nodes to 250 nodes. In each network size, we selected a percentage of malicious nodes ranging from the smallest percentage to the highest percentage, 10% to 60%.

We evaluated the different attack methods of the SSDF in each network size. The following SSDF attack strategies were considered: the hit and run, the always yes, and the always no. We evaluated the unintentionally misbehaving SUs to determine their effect on the performance of the network and the performance of the proposed scheme.

5.1 Simulation 1: The SSDF Attack

Figures 13 to 22 shows the implementation of the R-and-q-out-of-m rule scheme in CRAHN network with 50 nodes where 20% of the nodes were malicious. Initially, cooperative spectrum sensing was conducted to determine the state of the spectrum band. Energy levels of the PUs were returned as illustrated in figure 13.



C: ▸ Program Files ▸ MATLAB ▸ MATLAB Production Server ▸ R2013a ▸ bin ▸

1x30 double

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0.2687	2.3470	0.4674	1.1705	5.4145	0.0461	0.4127	0.0417	0.1599	0.2580	0.3886	0.0212	0.0308	0.1666	0.1730	0.6627

C: ▸ Program Files ▸ MATLAB ▸ MATLAB Production Server ▸ R2013a ▸ bin ▸

1x50 double

	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	0.3676	0.2838	0.4816	0.3656	1.3036	3.1015	0.8967	4.1734	0.2508	0.2720	0.5228	6.6583e-04	0.6036	0.0675	0.4867	0.1161

C: ▸ Program Files ▸ MATLAB ▸ MATLAB Production Server ▸ R2013a ▸ bin ▸

1x50 double

	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
1	1.0350	0.0018	0.2687	7.0126e-04	0.6167	0.2273	0.2514	0.0952	5.8972	4.1426	1.4576	0.0041	0.5789	2.5290	3.7406	0.0415

C: ▸ Program Files ▸ MATLAB ▸ MATLAB Production Server ▸ R2013a ▸ bin ▸

1x50 double

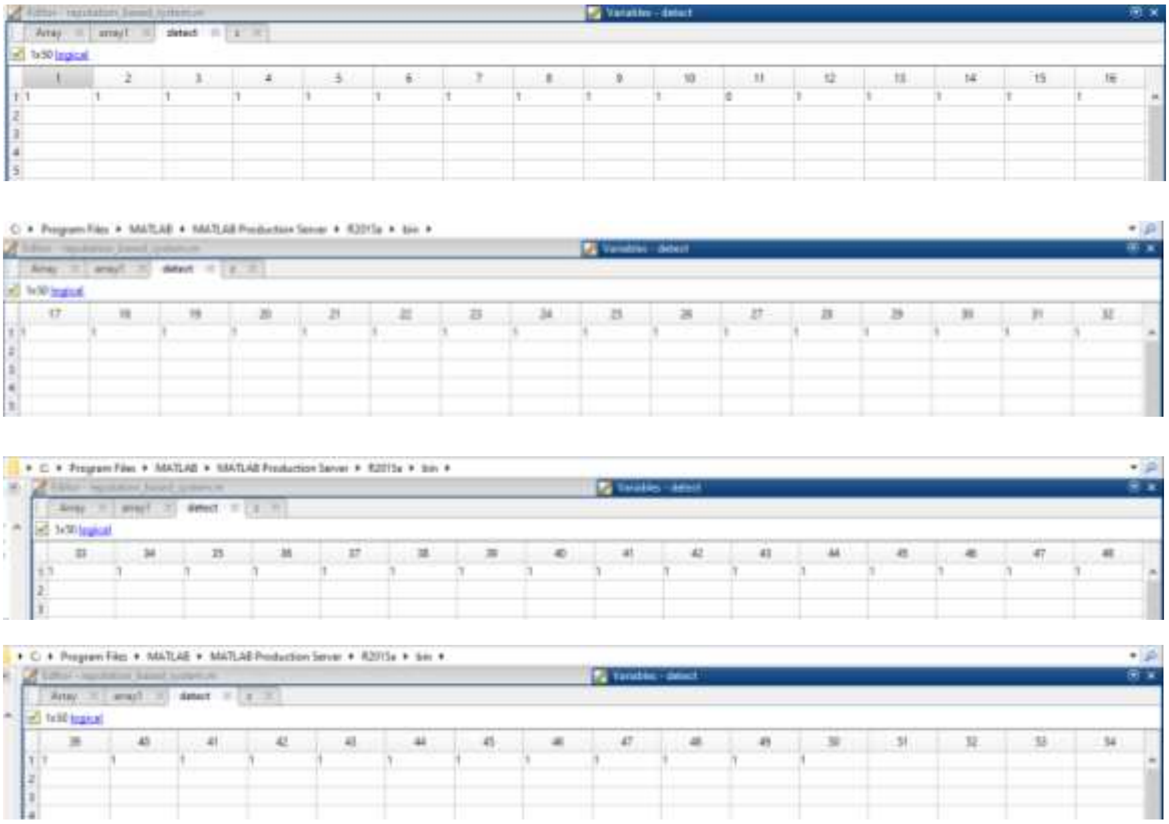
	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
1	0.2514	0.0952	5.8972	4.1426	1.4576	0.0841	0.5789	2.5290	3.7406	0.0415	0.0051	0.0481				

Figure 13: Retuned sensed energy observations

Figure 13 shows the PUs energy levels. The Energy detection technique was used to determine the energy strength of the PUs transmission. The sensing nodes had to compute the binary values based on their observations of the PUs energy level. In this study, we set the PU energy threshold value to zero. If the returned PU energy is below zero, the SUs computed their binary decision to 0. The value of 0 denotes that the spectrum band is idle and 1 denotes that the spectrum band is occupied. For the received energies greater than 0, the SUs compute their binary decision to 1 as illustrated in figure 14.

5.2 Returned energy

The returned energy levels of the nodes are shown in figure 14 before the SSDF attack is introduced in the network.


C: ▸ Program Files ▸ MATLAB ▸ MATLAB Production Server ▸ R2015a ▸ bin ▸
Editor - reputation_based_system.m
Variables - detect
Array
array1
detect
z
1x50 logical

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
2																
3																
4																
5																

	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2																
3																
4																
5																

	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2																
3																

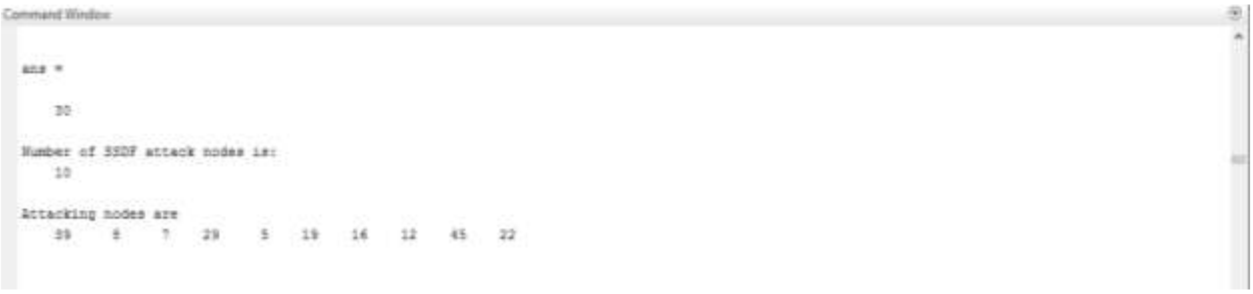
	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
1	1	1	1	1	1	1	1	1	1	1	1	1				
2																
3																
4																

Figure 14: Binary values of the sensed energy

Figure 14 shows the binary decisions computed by the SUs before the SSDF attack is introduced in the network. Based on the observed energy strength of the PUs, the SUs computed the final binary decision to share with their neighbouring nodes. As shown in figure 14, node 11's binary decision differs from the decision of other nodes because the node has been compromised by Byzantine failures and is classified as an unintentionally misbehaving node.

5.3 SSDF attack in CRAHN

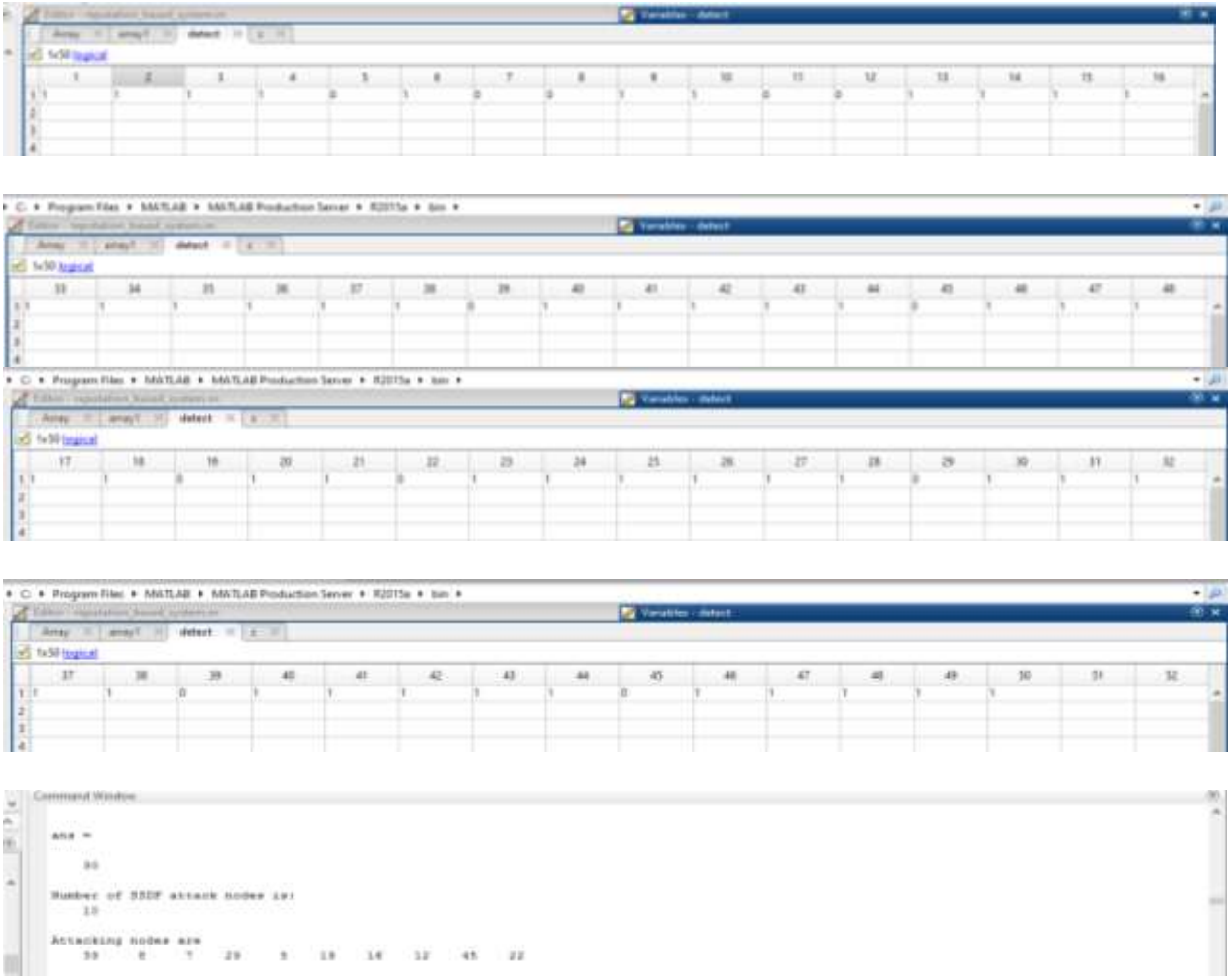
We configured the network to identify the malicious nodes as shown in figure 15.



```
ans =

    50

Number of SSDF attack nodes is:
    10

Attacking nodes are
    39     8     7    29     5    19    16    12    45    22
```

Figure 15: Attacking nodes in the network

The SSDF attack was introduced in the network as illustrated in figure 15 in which a network with 50 nodes of which 10 of them are malicious was considered. The MUs alter the binary decision as depicted in figure 16.


Variables - detect
Array
array1
detect
C: ▸ Program Files ▸ MATLAB ▸ MATLAB Production Server ▸ R2015a ▸ bin ▸
Command Window

1x50 logical

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	1	1	0	1	0	0	1	1	0	0	1	1	1	1
2																
3																
4																

1x50 logical

	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
1	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1
2																
3																
4																

1x50 logical

	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	1	1	0	1	1	0	1	1	1	1	1	1	0	1	1	1
2																
3																
4																

1x50 logical

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
1	1	1	0	1	1	1	1	1	0	1	1	1	1	1		
2																
3																
4																

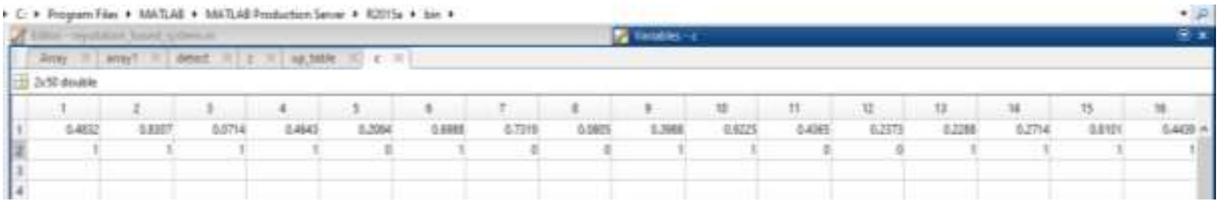
```
ans =

    50

Number of SSDF attack nodes is:
    10

Attacking nodes are
    39     8     7    29     5    19    16    12    45    22
```

Figure 16: The SSDF attack

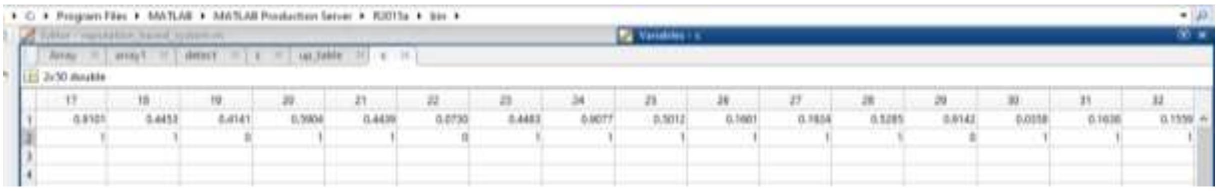
Figure 16 shows how the attacking nodes alter their actual observations and report false results. Nodes 5,7,8,12,16,19,22,29,39 and 45 altered their results from 1 to 0 compared to figure 15. Node 11 was set to be an unintentionally misbehaving node thus it reported an incorrect value of 0. We present results of the always yes (Ay) attacks, which are SSDF attacks that always report that the spectrum band is occupied while it is not. Always no (Ay) attacks, which report that spectrum band that is idle is not.

5.4 sensing reports and reputation of the nodes

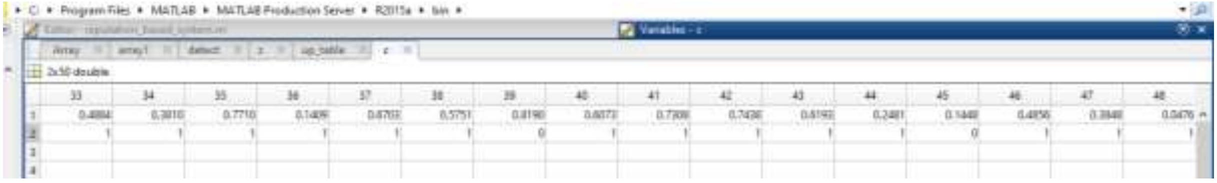
Figure 17 depicts reputation values of the nodes and sensing reports.


C: ▸ Program Files ▸ MATLAB ▸ MATLAB Production Server ▸ R2015a ▸ bin ▸
Editor - reputation_based_system.m
Variables - c
Array
array1
detect
z
up_table
c
2x50 double

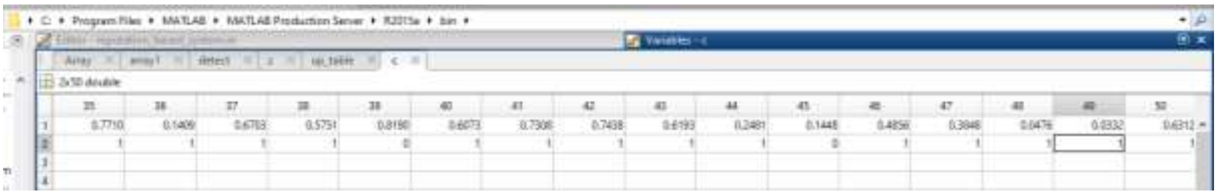
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0.4832	0.8307	0.0714	0.4643	0.2084	0.6888	0.7319	0.0805	0.3988	0.9225	0.4365	0.2373	0.2288	0.2714	0.8101	0.4409
2	1	1	1	1	0	1	0	0	1	1	0	0	1	1	1	1
3																
4																


C: ▸ Program Files ▸ MATLAB ▸ MATLAB Production Server ▸ R2015a ▸ bin ▸
Editor - reputation_based_system.m
Variables - c
Array
array1
detect
z
up_table
c
2x50 double

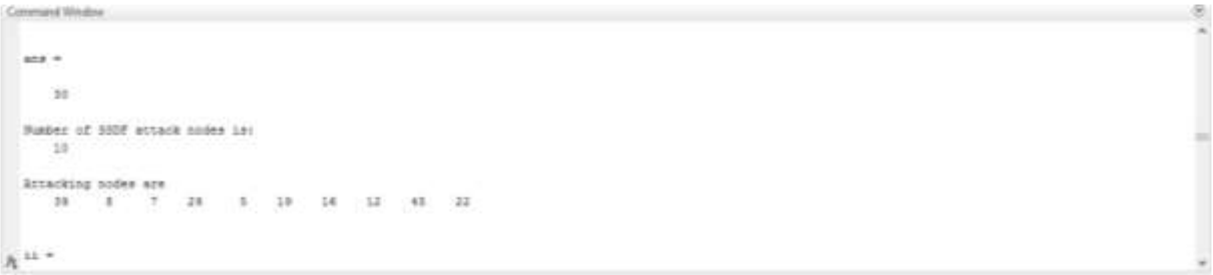
	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	0.8101	0.4453	0.4141	0.3904	0.4439	0.0730	0.4483	0.9077	0.5012	0.1661	0.1834	0.5285	0.8142	0.0358	0.1636	0.1559
2	1	1	0	1	1	0	1	1	1	1	1	1	0	1	1	1
3																
4																


C: ▸ Program Files ▸ MATLAB ▸ MATLAB Production Server ▸ R2015a ▸ bin ▸
Editor - reputation_based_system.m
Variables - c
Array
array1
detect
z
up_table
c
2x50 double

	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
1	0.4884	0.3810	0.7710	0.1409	0.6703	0.5751	0.8190	0.6073	0.7308	0.7438	0.6193	0.2481	0.1448	0.4856	0.3848	0.0476
2	1	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1
3																
4																


C: ▸ Program Files ▸ MATLAB ▸ MATLAB Production Server ▸ R2015a ▸ bin ▸
Editor - reputation_based_system.m
Variables - c
Array
array1
detect
z
up_table
c
2x50 double

	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
1	0.7710	0.1409	0.6703	0.5751	0.8190	0.6073	0.7308	0.7438	0.6193	0.2481	0.1448	0.4856	0.3848	0.0476	0.0332	0.6312
2	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1
3																
4																



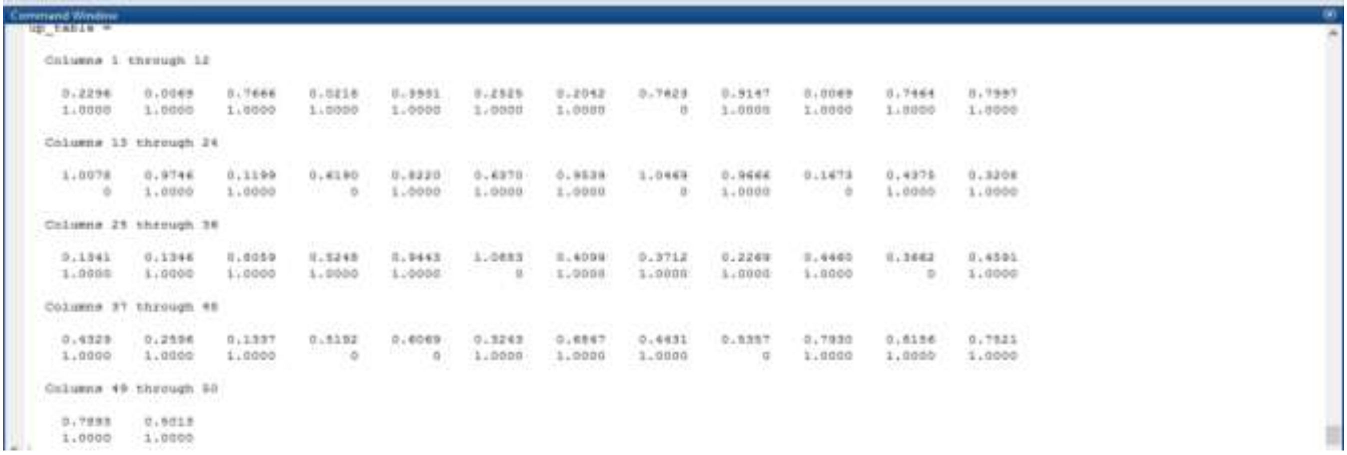
```
ans =

    10

Number of SSDF attack nodes is:
    10

Attacking nodes are
    39     8     7    29     5    19    11    12    45    22


ii =
```

Figure 17: Sensed data and reputation values of all the nodes

Figure 17 shows the reputation values and SUs sensing reports before they are updated by the proposed scheme. Each node had a reputation value associated with the sensing report. The nodes with incorrect sensing reports reputation values are updated by 0.1 as shown in figure 18 and all the nodes with unaltered sensing reports reputation values are decremented by 0.1.

5.5 Updating the reputation values

We update the reputation values to prevent MUs from changing their identities. Figure 18, shows the reputation values are updated in reputation and q out of m rule scheme.



```
up_table =

  Columns 1 through 12

    0.2296    0.0069    0.7666    0.0218    0.3991    0.2525    0.2042    0.7623    0.9147    0.0069    0.7464    0.7997
    1.0000    1.0000    1.0000    1.0000    1.0000    1.0000    1.0000         0    1.0000    1.0000    1.0000    1.0000

  Columns 13 through 24

    1.0078    0.9746    0.1199    0.4190    0.8220    0.6370    0.9538    1.0469    0.9666    0.1473    0.4375    0.3208
         0    1.0000    1.0000         0    1.0000    1.0000    1.0000         0    1.0000         0    1.0000    1.0000

  Columns 25 through 36

    0.1341    0.1346    0.6059    0.5248    0.9443    1.0883    0.4098    0.3712    0.2269    0.4460    0.3662    0.4591
    1.0000    1.0000    1.0000    1.0000    1.0000         0    1.0000    1.0000    1.0000    1.0000         0    1.0000

  Columns 37 through 48

    0.4329    0.2596    0.1337    0.5192    0.6069    0.3243    0.6867    0.4431    0.5357    0.7930    0.6156    0.7521
    1.0000    1.0000    1.0000         0         0    1.0000    1.0000    1.0000         0    1.0000    1.0000    1.0000

  Columns 49 through 50

    0.7893    0.9012
    1.0000    1.0000
```

Figure 18: Updated table of the reputation values

In figure 18, all the SUs whose reports were not equal to the final decision reputation values were incremented by 0.1. The SUs whose reports were equal to the final decision reputation values were decremented by 0.1 except for the MUs, which are indicated in figures 16 and 17.

5.6 Reputation-based system: Nodes IDs and the node's reputation

We depict the reputation based system node IDs and their reputation values in figure 19.

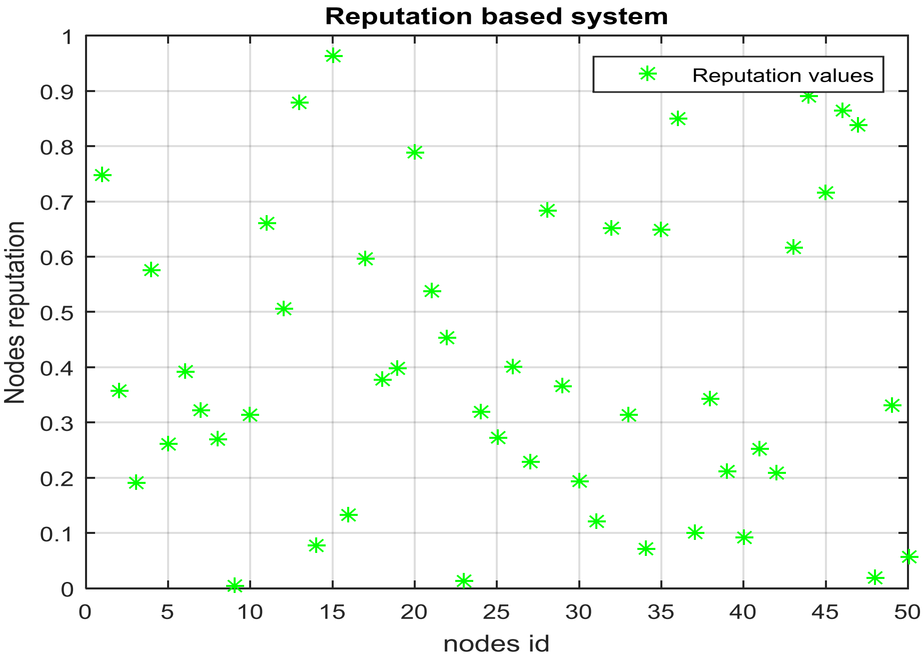


Figure 19: Reputation-based system

In figure 19, we present the reputation values of nodes ranging from 0 to 1 against the node IDs. The reputation-based system was implemented to determine the trustworthiness of the nodes. We have set our threshold value (TV) to 0.6 in order to accommodate Um SUs. The threshold value is used to determine which nodes will be selected for final decision-making. Our reputation values range from 0 to 1. We have set our nodes to 50 in figure 19 where 20% of the total nodes are malicious nodes

5.7 Isolated nodes with reputation above the threshold value of 0.6

In figure 20, we present the results of all the nodes from figure 19 that have been isolated in the network because of their reputation values which are above TV.

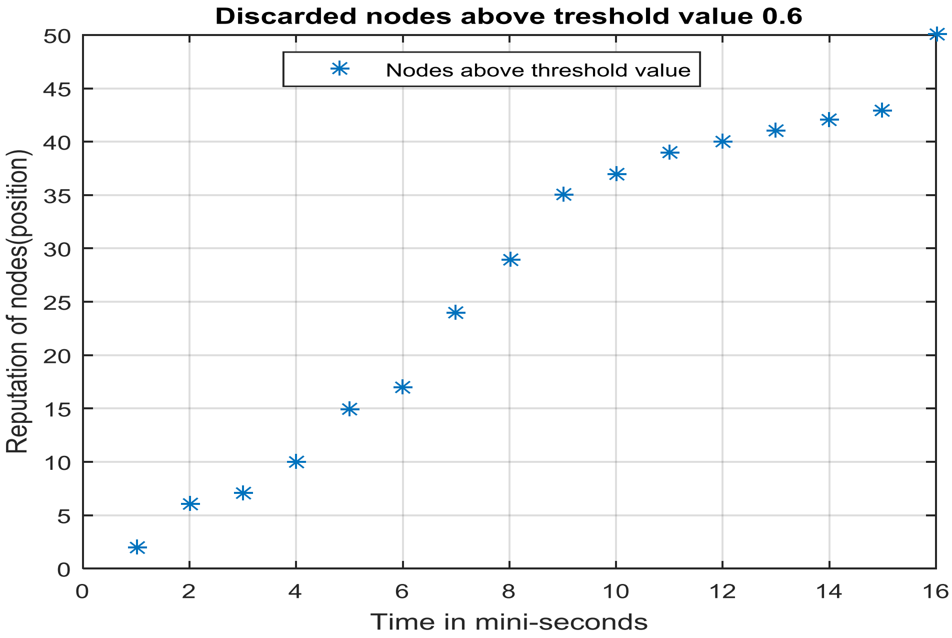


Figure 20: Nodes above threshold value

Figure 20 depicts the isolated nodes whose reputation values are above the TV. The simulation time is plotted against the position of the nodes in the network. The following nodes: 3,6,7,10,15,18,24,28,35,37,38,40,41,43,43 and 50 were isolated since their reputation values were above the selected TV. The inputs of these nodes were not considered in the final decision-making.

5.8 Selected nodes below TV 0.6

We present the results of all the nodes whose reputation values are below the TV in figure 21.

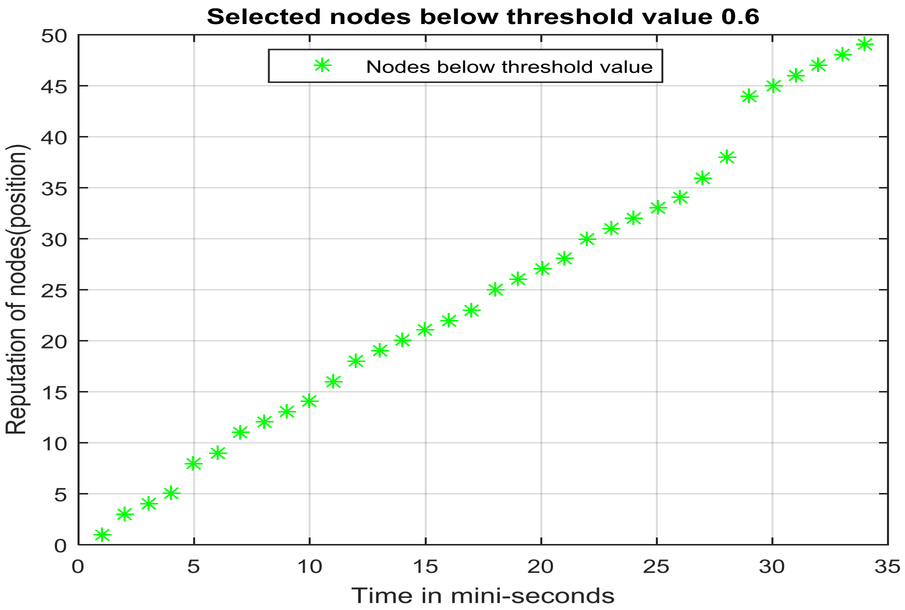


Figure 21: Nodes below threshold value

Figure 21 shows the results of the nodes that have reputation values that are below the TV. The reputation values of these nodes are included in the final decision-making.

5.9 Simulation of sensing reports that are not equal to the final decision

Figure 22 depicts the results of all the nodes whose reputation values are incremented by 0.1

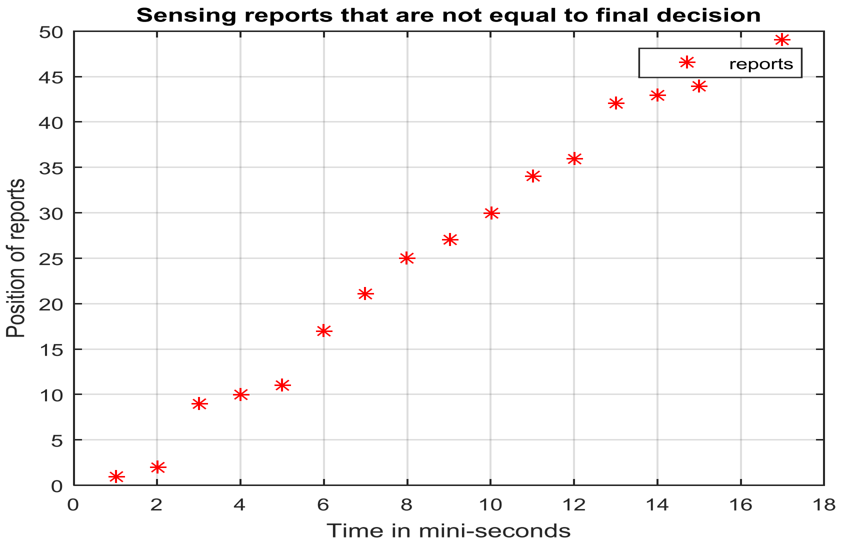


Figure 22: Updated sensing reports

Figure 22 present the reputation values of nodes whose values were incremented by 0.1. The sensing reports of these nodes are not equal to the final decision hence their reputation values were incremented by 0.1.

5.10 Success Probability with 10% malicious users

We evaluated the success probability with 10% malicious users in the network of 10, 50,100.150, and 250 in figure 23.

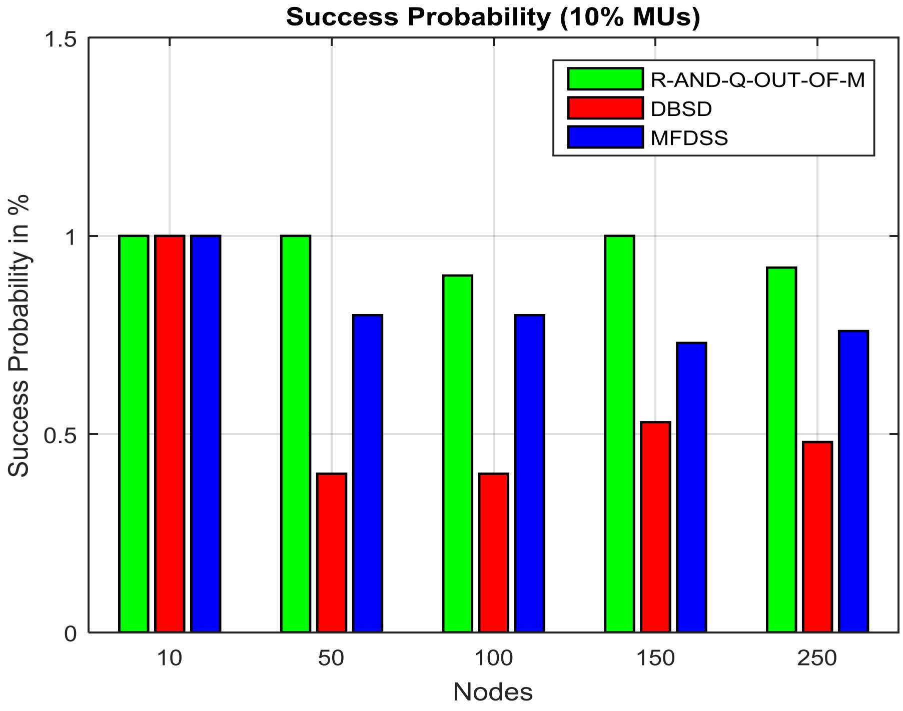


Figure 23: Success Probability with 10% malicious users

In figure.23, the schemes success probability in detecting and isolating the SSDF attack was evaluated. We varied the number of nodes from $(N = 10\, to\, N = 250)$ with a fixed percentage of MUs $(MUs = 10\%)$. The emphasis was to investigate the hit and run attack strategy (HnR), the always yes (Ay) attack strategy and the always no attack strategy (An). We also evaluated the impact of the unintentionally misbehaving nodes (Um) in the success probability and missed detection probability on the schemes. In $N = 10$, we did set 1 node to be the Ay SSDF attack. We observed that the proposed scheme, the DBSD scheme and the MFDSS scheme were able to detect the malicious node. The schemes showed to have better performance in detecting the Ay SSDF attack when the network size was 10 because there was a single attack.

We then increased the number of nodes to 50 while evaluating 10% MUs. To effectively evaluate the performance of the schemes in different attack strategies of the SSDF attack, we set 1 Ay, 1 always no attack(An), 2 misbehaving SUs (Um), and 1 hit and run attack (HnR). The proposed scheme showed to perform better in detecting and isolating the attacks. The MFDSS scheme's limitation was in detecting the HnR attack. The DBSD scheme only detected the Ay and An and was able to remove the extreme outliers. The DBSD was not designed to distinguish between misbehaving nodes and malicious nodes in the network.

In $N = 100$ we set 10% of the nodes to be malicious with 4 Um. We set 2 Ay attacks, 2 An attacks, and 2 HnR attacks, to examine the schemes' effectiveness in distinguishing between the SSDF attack and byzantine failures. The Um nodes where not detected in the first fusion phase which led to a slight decrease in the success probability of the proposed scheme in detecting the attack. Analysing the results of the DBSD scheme, we observed that it managed to detect the Ay and An attacks. The MFDSS scheme performed better in detecting all the attack strategies of the SSDF attack except the HnR attack.

When we increase the number of nodes to $N = 150$ with a fixed percentage of malicious nodes we observed that the performance of the schemes is affected. We randomly varied the attack strategies in $N = 150$ by setting Ay attack to 4. The An attack was set to 4, the HnR attack to 4, and Um to be 3. The proposed scheme showed to have the highest success probability in detecting and isolating the SSDF attack. The DBSD scheme is prone to byzantine failures and cannot distinguish unintentionally misbehaving nodes and malicious nodes [52].

In $N = 250$, we evaluated the proposed scheme's performance when the number of MUs were 25 in the network with 6 Ay attacks, 6 An attacks, 6 HnR attacks, and 7 Um allocated randomly. From the results, the performance of the schemes shows to have degraded as we increased the number of nodes and the number of malicious nodes. The increase in the number of nodes had a negative impact in the success probability of the schemes. The proposed scheme performed better in the success probability of detecting MUs compared to the other schemes. We can conclude that the DBSD scheme does not perform well in a large network with higher number of

MUs. This is because the DBSD detected the Ay and An attack strategies of the SSDF attack.

5.11 Success Probability with 20% malicious users

The results of success probability with 20% malicious users are plotted in figure 24.

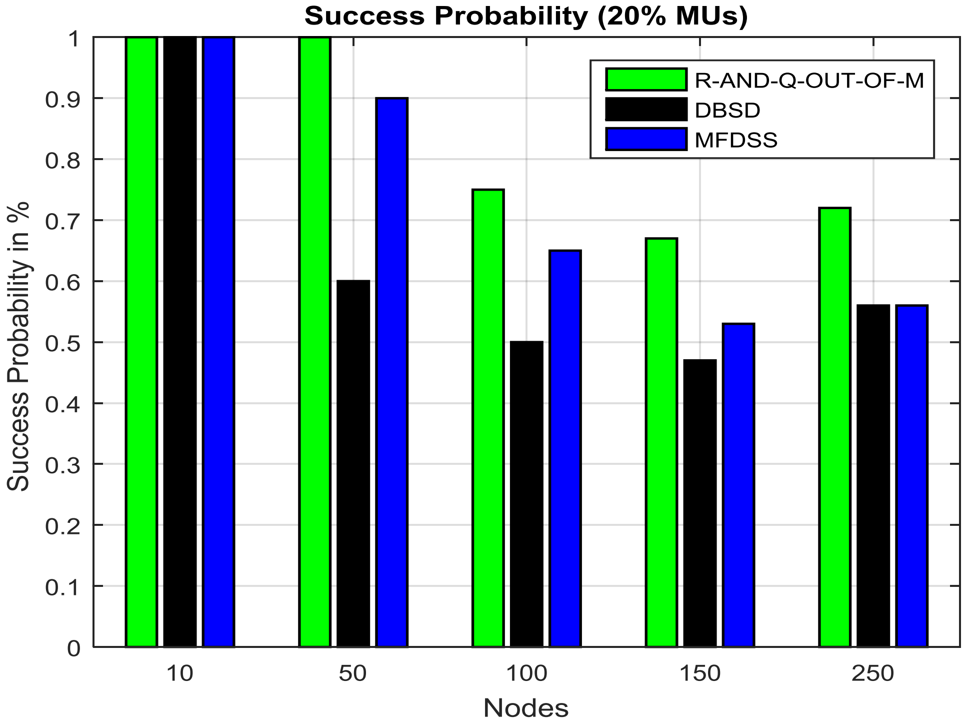


Figure 24: Success Probability where 20% of the SUs are malicious

In figure 24, we evaluated the success probability of the schemes in $N = 10, 50{,}100{,}150\ to\ 250$ with different SSDF attack strategies. We evaluated the performance of the network with $Ay = 1$ and $An = 1$ SSDF attack for $N = 10$,. We observed that there was no effect in the success probability of the schemes because the HnR attack and MUs where not considered. In $N = 50$ we set 10 nodes to be malicious where 3 nodes where the Um nodes. We set 3 Ay and 3 An, and 1 HnR attack. We observed that the DBSD had the highest decrement of success probability because the HnR attack and Um nodes were considered. However, when the Um nodes and HnR attack were not present in the network, the performance of the DBSD scheme improves gradually. The proposed scheme performed better because of the q-out-of-m rule scheme implemented which isolated the Um nodes and HnR attack before the final decisions were made. The MFDSS scheme degraded because the implemented reputation-based scheme could not isolate the HnR attack before the final decisions were made.

In $N = 100$ we evaluated the performance of the schemes with $MUs = 20$. We set $Ay = 5$,$An = 5$, $Mn = 5$ where 2 had bad reputation and $HnR = 5$. We analysed the performance of the proposed scheme and noticed that 30% of the MUs were not detected. This is because the Um nodes without bad reputation were not isolated from the network before the final transmission decision was made. The HnR attack were not detected by the reputation-based system. The DBSD scheme performs better in a case where only the Ay and An attacks were considered but when the other attack strategies were incorporated the performance of the scheme degraded. We implemented the MFDSS scheme using the modified z-test strategy. The scheme performs better in detecting the Ay, An, and Um attacks but cannot detect the HnR attack.

In $N = 150$, we test the ability of the schemes to detect byzantine failures. We considered 30 nodes to be malicious with 10 nodes experiencing byzantine failures. We set 8 Ay, 8 An, and 4 HnR attack. The results show that the success probability of the schemes to detect MUs decreases when the network size increases and the percentage of the byzantine failures increases.

In $N = 250$ and $MUs = 50$, we randomly set 8 nodes to experience byzantine failures with 18 Ay, 18 An, and 4 HnR attacks. When we have a large number of Ay and An attacks in the network, the performance of the schemes improved. The results showed that the Ay and An attack strategies of the SSDF attack are easily detected by the schemes. The proposed scheme outperformed the other schemes and it managed to detect 80% of the Um nodes, 33% of the An nodes and 50% of the HnR nodes because the increase in the number of malicious users from 10% to 20% did not have a negative impact on the performance of the proposed scheme. However, The DBSD scheme is not robust enough to handle different SSDF attack densities and was worst affected. The MFDSS scheme was impacted by the variation in the HnR attack and Um nodes because they were not detected by the first fusion stage.

5.12 Success Probability with 40% malicious users in the network

Figure 25 shows the results of success probability with $MUs = 40\%$ in the network of 10, 50,100.150, and 250.

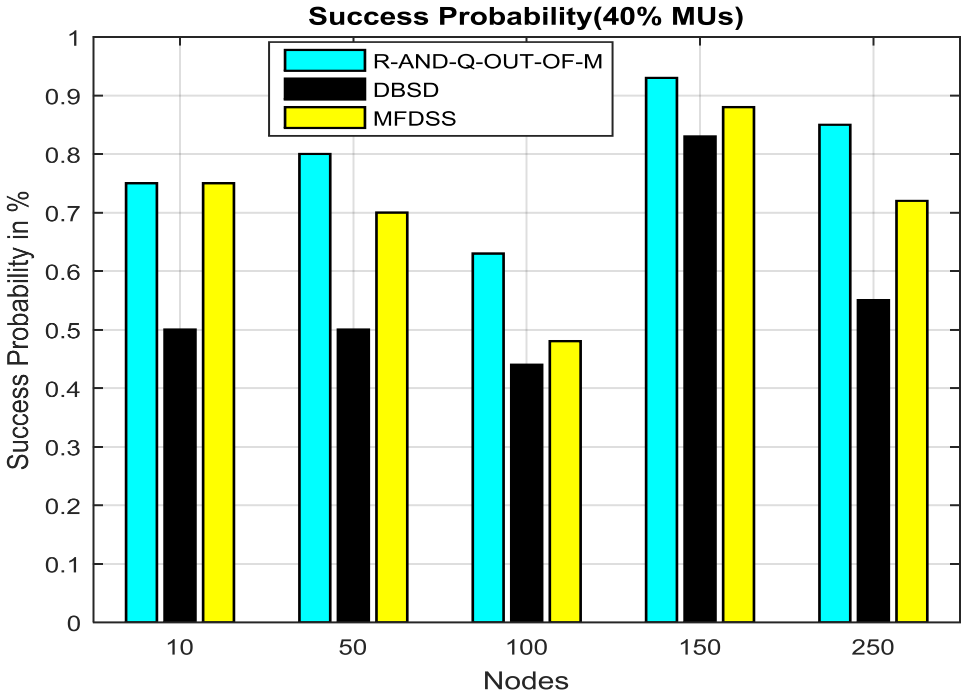


Figure 25: Success Probability with 40% malicious users

In figure 25 we present the success probability of the R-AND-Q-OUT-OF-M rule scheme, the DBSD scheme, and the MFDSS scheme in detecting the presence of malicious nodes in a network with 10, 50, 100, 150, and 250 nodes given a fixed percentage of MUs $(40\ \%)$. We varied the attack methods of the SSDF attack to evaluate the attack strategy of the SSDF with the highest impact on the network. In $N = 10$, we had $MUs = 4$. We set 1 UM, 1 Ay, 1 An, and 1 HnR attack. The performance of the proposed scheme and MFDSS scheme were slightly affected because both schemes managed to detect 75% of the MUs. Their performance was affected by the HnR attack, which was not detected. The performance of the DBSD scheme achieved a detection accuracy of 50% because the HnR attack and the Um node were not detected by the scheme. Figure 25 exhibited different trends compared to figure 24 because of the increase in the number of MUs in figure 25.

In $N = 50$, we present the results of $MUs =\ 20$ where we had $Ay =\ 5, An = 5, HnR = 5,$ and $Um =\ 5.$ The results show that the proposed scheme outperformed the MFDSS and DBSD schemes. The performance of the proposed scheme increased by 5% in $N = 50$ compared to when the network had 10 nodes. The performance of the MFDSS scheme reduced due to the unintentionally misbehaving nodes which were not detected by the scheme. The DBSD scheme achieved constant detection accuracy when the network size and the number of MUs was increased.

In $N = 100$, we had $MUs = 40$. To test the effect of the hit and run attack on the network, we set $HnR = 18$ while $Ay = 8, An = 8,$ and $Um = 6$. We observed a huge drop in the performance of the schemes but the proposed scheme achieved the highest detection accuracy which is more than 60% compared to the MFDSS and DBSD schemes. When the number of hit and run attacks increases the DBSD scheme, detection accuracy reduces drastically. This is because in its current form, the DBSD scheme is not designed to combat the hit and run attack and unintentionally misbehaving SUs. The MFDSS scheme is designed to combat the hit and run attack but is not optimized to combat a large number of hit and run attack. MFDSS scheme was implemented using modified Z-test, which performs better when the byzantine failure rate cannot be estimated. The results show that the Um nodes have an effect on the performance of the MFDSS scheme.

In $N = 150$, we test the impact of the Ay and An SSDF attack strategies on the success probability of the schemes. We set a fixed number of Mus (40%) while we increased the attack probability of the $Ay = 25$ and $An = 25$. We set the $Um = 6$ and $HnR = 4$. We observed an increase in the schemes' performance in detecting the MUs.

In $N = 250$ and $MUs = 100$, we evenly distributed the SSDF attack strategies. We set the Ay attack to 25, An attack to 25, the HnR attack to 25, and the Um to 25. The detection accuracy of the schemes dropped compared to $N = 150$. With an equal number of attack strategies and an increase in the network size, the performance of the schemes was degraded.

5.13 Success Probability with 50% malicious users

We present the results of success probability with 50% malicious users in the network in figure 26.

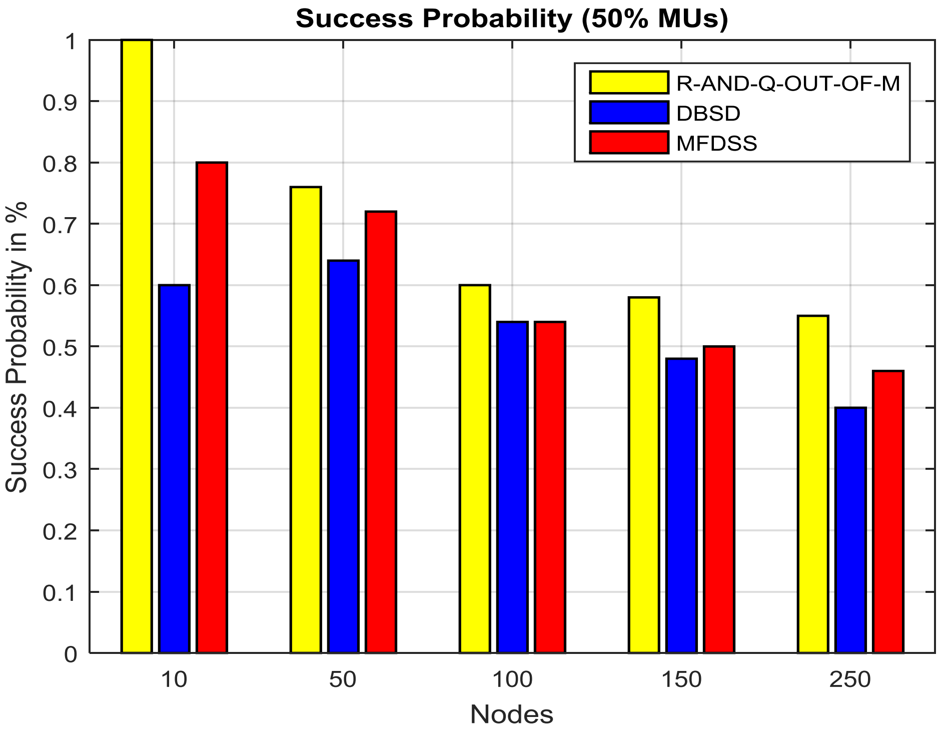


Figure 26: Success Probability: 50% malicious users

We present the success probability of the schemes in detecting the SSDF with $MUs = 50\%$ in figure 26. In $N = 10$, $MUs = 5$, we evaluated the performance of the network under 1 Um, 1 Ay, 1 An, and 2 HnR attack. From the given results, the proposed scheme managed to detect all the attacks in the network because it is optimized to detect all the attack strategies of the SSDF attack. The DBSD scheme managed to detect 60% of the MUs in the network while the MFDSS scheme managed to detect only 80% of the MUs in the network.

For $N = 50$, we increased the number of MUs to 25 while randomly distributed the SSDF attack strategies in the network. We had the $Um = 5, Ay = 6, An = 8,$ and $HnR = 6$. We evaluated the performance of the schemes in detecting and isolating the SSDF attack before the final transmission decision was made. The results show that the Um nodes have a negative impact on the detection accuracy of the proposed scheme because 60% of the attack could not be detected by the proposed scheme. The performance of the DBDS scheme improved compared to $N = 10$ but it is still under performing in detecting the MUs. The performance of the MFDSS scheme decreased by 8% compared to when $N = 10$ due to the Um nodes and HnR attack.

The detection probability in $N = 100$ when MUs were 50% of the total nodes decreased gradually. We set $Um = 12, Ay = 15, An = 15$, and $HnR = 8$ because the Ay and An attacks are the most common SSDF attack strategies. In $N = 150$ with $MUs = 75$, we randomly set $Um = 18, Ay = 25, An = 15$, and $HnR = 17$. The results show that with an increase in the number of SUs and MUs where many Um and HnR attacks were considered, the schemes success probability reduced.

5.14 Success Probability with 60% malicious users

The results of success probability with 60% malicious users in 10, 50,100.150, and 250 nodes are shown in figure 27.

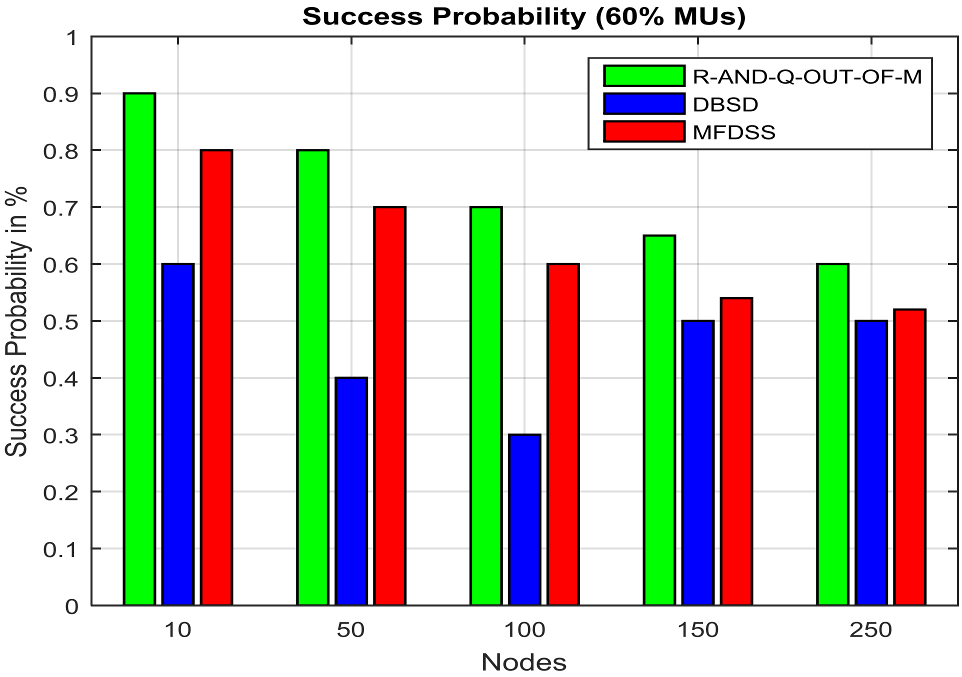


Figure 27: Success Probability: 60% malicious users

We purposely assigned 40 MUs in the network to show that a mitigation scheme against the SSDF attack to assess the effectiveness of the schemes in networks with high number of SSDF attacks in figure 27. We present the results of $MUs = 60\%$ in which varied types of attack methods were considered. In $N = 10$, we have $6\ MUs$ where 3 were the Ay and 3 were the An SSDF attack. We tested the performance of the schemes with only the always yes and always no attacks. In $N = 50$, we tested the performance of the schemes with $10\ Ay, 10\ An$, and $10\ Um$. In $N = 100$ to test the resiliency of the Ay, An, and HnR attacks, we set $Ay = 20\ An = 20$, and $HnR = 20$. In $N = 150$ we had $HnR = 45$ and $Um = 45$ while in $N = 250$ we set $Ay = 45\ An =$

45 $HnR = 30$, and $Um = 30$. With a large number of SSDF attacks in the network, regardless of the attack strategies implemented by the SSDF attack, the schemes performance reduces. We noted that the HnR attack and Um nodes were the attacks with the highest negative impact on the network. The HnR attack can contain characteristics of legitimate SUs which reduces the detection probability of the schemes. The Um nodes with incorrect spectrum observation values can have a negative impact on the final transmission decision and because they are classified as SUs, they are not easily detected.

5.15 Missed Detection Probability with 10% MUs

Figure 28 shows the results of Missed Detection probability with 10% malicious users in a network with 10, 50,100.150, and 250 nodes.

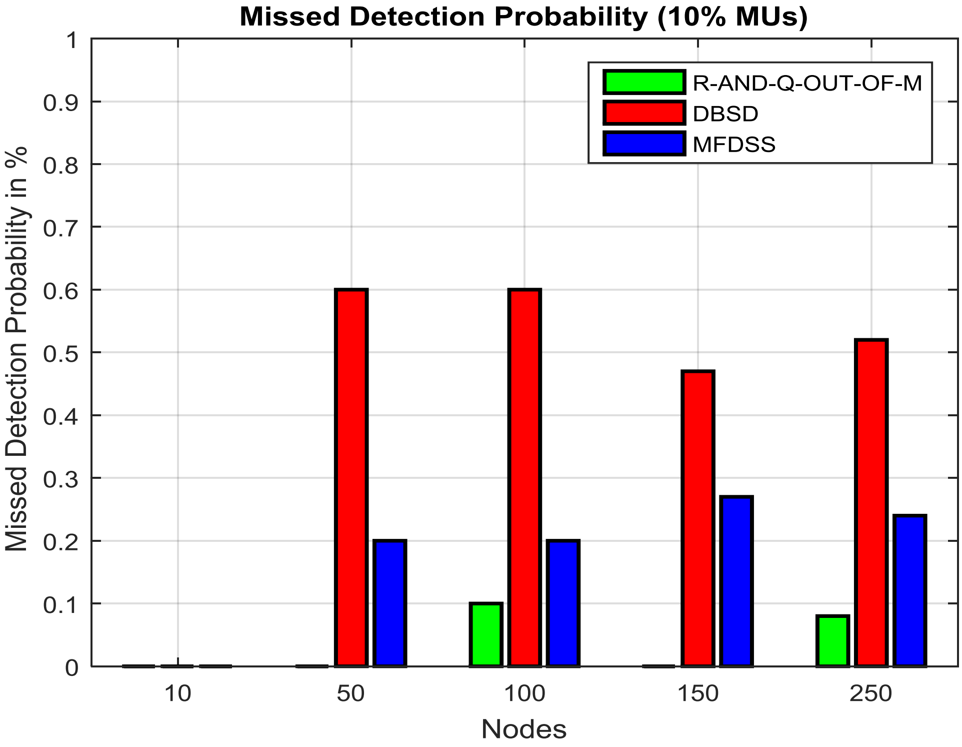


Figure 28: Missed detection Probability: 10% MUs

In figure 28, we examined the schemes' missed detection probabilities in detecting the SSDF attack in the network under different scenarios in each network size. In $N = 10$, we had only one attack method implemented, the Ay attack method. We observed that the proposed scheme, the DBSD scheme, and the MFDSS scheme were able to detect the Ay attack because the attack probability of the Ay exhibits the attributes of an outlier which can be easily detected by any fusion scheme. All the schemes had low miss detection probabilities in detecting the Ay SSDF attack.

Increasing the nodes to 50 with $10\%\,MUs$ and using the same parameters as in success probability; We set 1 Ay attack, 1 An attack, 2 misbehaving SUs, and 1 HnR attack. The proposed scheme had the lowest missed detection probability. In $N = 100$ with 10% of the nodes being malicious where 4 were Um nodes, 2 were the Ay attack, 2 An attack, and $2\,HnR$ attack. We observed an increase in the missed detection probability of the proposed scheme.

We increased the number of nodes to $N = 150$, with a random variation of the attack strategies. The Ay attack was set to 4, the An attack to 4, the HnR attack to 4, and Um nodes to 3. The proposed scheme had positive missed detection probability results. The proposed scheme detected and isolated all the malicious nodes because of the q-out-of-m rule scheme implemented that detects all the MUs and Um nodes in the first fusion phase. The DBSD scheme is prone to byzantine failures and Um nodes.

In $N = 250$ we evaluated the proposed scheme's performance when the number of MUs were 25 in the network with 6 Ay attacks, 6 An attacks, 6 $HnR,$ and Um allocated randomly. The results showed an increase in the percentage of missed detection probabilities of all the schemes. We conclude that the HnR attack and the Um nodes have a negative impact on the performance of the schemes.

5.16 Missed Detection Probability with 10% malicious users

The Missed Detection probability with 20% malicious user's results are presented in figure 29.

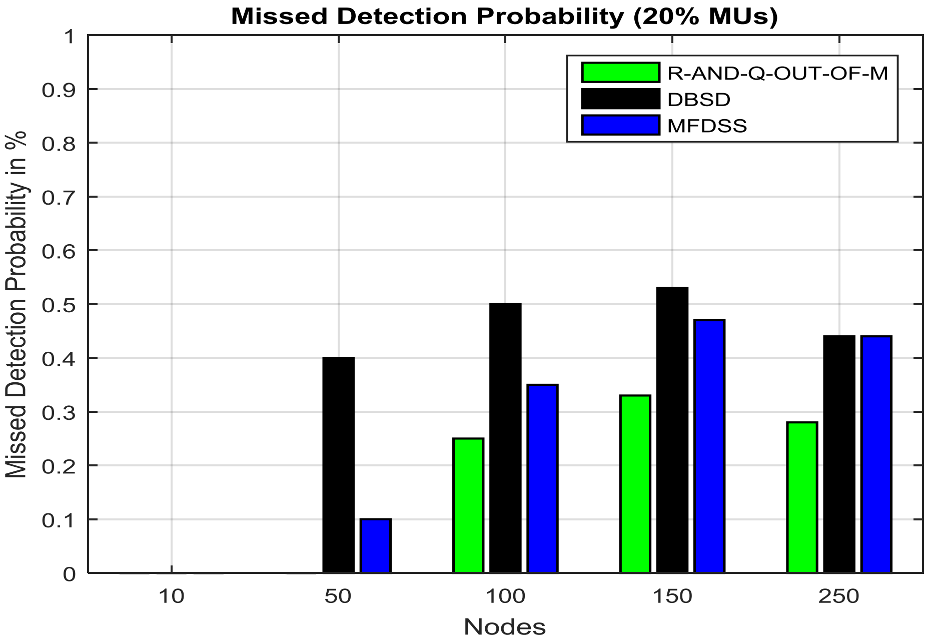


Figure 29: Missed detection Probability: 20% malicious users

In figure 29, we discuss the missed detection probability results obtained through Matlab simulation tool. The performance of the schemes was investigated under different SSDF attack scenarios in figure 29. For $N = 10$, we set two different scenarios, we set 1 Ay attack and 1 An attack. We observed that with the Ay and An attacks, the schemes can detect and isolate them given their estimated attack probabilities. In $N = 50$ we had 10 malicious nodes with 3 nodes experiencing byzantine failures. We set 3 Ay and 3 An to examine their effect and 1 HnR attack. We observed that the DBSD had the highest missed detection probability due to the byzantine failures and HnR attack which were not easy to detect.

For $N = 100$ we evaluated the performance of the schemes with $MUs = 20$. We set the $Ay = 5, An = 5, Um = 5$ where 2 had bad reputation and $HnR = 5$. The proposed scheme had increased missed detection probability of 30% due to the byzantine failures. The HnR attack also had an impact on the missed detection probability of the schemes and caused it to increase.

In $N = 150$, we examined the ability of the schemes to detect byzantine failures in scenario with 30 nodes being malicious with 10 nodes experiencing byzantine failures. We set $8\, Ay, 8\, An,$ and $4\, HnR$ attack. The missed detection probability of the schemes increased when the network size increased and the percentage of the byzantine failures also increased. This increase was caused by the implementation of the HnR attack and the Um nodes. These nodes have a negative impact on the network when not detected.

In $N = 250$ and $MUs = 50$, we randomly set 8 nodes to be the Um nodes with 18 Ay attacks, 18 An attacks, and 4 HnR attacks. The results showed that with a high number of Ay and An attacks in the network, the missed detection probability reduced significantly compared to $N = 150$. The Ay and An attack strategies of the SSDF attack had the lowest effect in the performance of the schemes. This means that the Ay and An attacks can be detected even by the soft fusion rules but the Um nodes and HnR attack had the highest number of attack probabilities, which cannot be easily detected.

5.17 Missed Detection Probability with 40% malicious users

The results of missed detection probability where 40% of the nodes in the network are malicious are presented in figure 30.

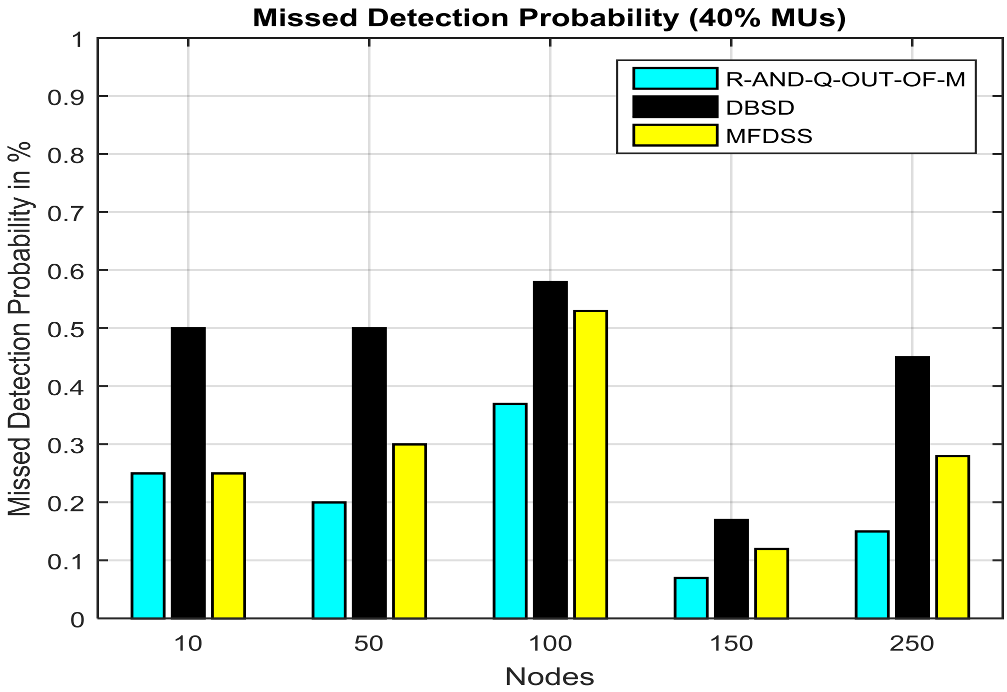


Figure 30: Missed detection Probability: 40% malicious users

Figure 30 show the missed detection probability of the R-AND-Q-OUT-OF-M rule, DBSD scheme, and MFDSS schemes in $N = 10, 50, 100, 150\ to\ 250$, with $MUs = 40$. In $N = 10$, we had $MUs = 4$. We set 1 Um, 1 Ay, 1 An, and 1 HnR attack. In $N = 50$, we set $MUs = 20$ where $Ay = 5$, $An = 5, HnR = 5, and\ Um = 5$. The results show that the proposed scheme outperformed the MFDSS and DBSD schemes in missed detection probability

In $N = 100$, we have $MUs = 40$. To investigate the effect of the hit and run attack in missed detection probability, we set $HnR = 18$ while $Ay = 8, An = 8,$ and $Um = 6$. We observed an increase in the missed detection percentage of the schemes. The HnR attack had a negative impact on the network.

In $N = 150$, we examine the impact of the Ay and An SSDF attack strategies on the performance of the schemes. We set a fixed 40% MUs while we increased the attack probability of the $Ay = 25$ and $An = 25$. We set the $Um = 6$ and $HnR = 4$. We observed n decrease in the missed detection rate of the schemes. The decrease was caused by the Ay and An attacks which were easily detected by the schemes due to their simple attack probabilities.

In $N = 250$ and $MUs = 100$, we evenly distributed the SSDF attack strategies. We set the Ay attack to 25, An attack to 25, the HnR attack to 25, and the Um to 25. The missed detection rate of the schemes increased compared to $N = 150$.

5.18 Missed Detection Probability where 50% of the nodes are malicious

When the number of malicious nodes is increased to 50%, the behaviour of the missed detection probability is plotted in figure 31.

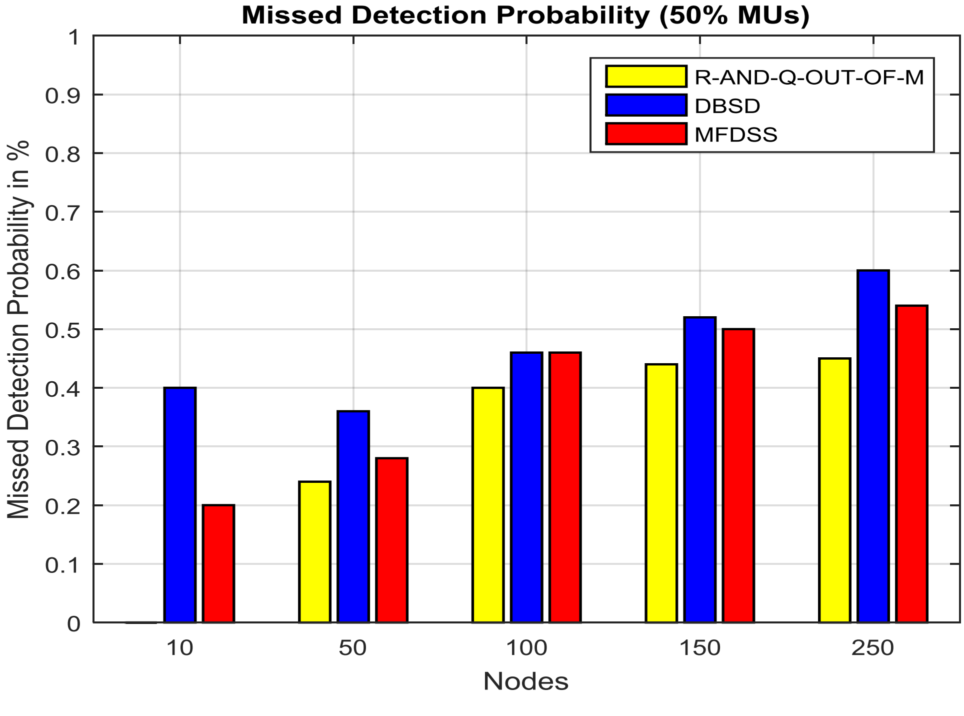


Figure 31: Missed detection Probability: 50% malicious users

In figure 31, the number of MUs was the same as the number of SUs, this caused the results to exhibit a different pattern from figure 31. The attack strategy implemented by the SSDF attack also caused a different behaviour in the results. In $N = 10$, $MUs = 5$, we had $1\ Um, 1\ Ay, 1\ An,$ and $2\ HnR$ attack. The results show that the proposed scheme performed better than the other schemes and had the lowest missed detection percentage. The DBSD scheme had a missed detection percentage of 40% and the MFDSS had a missed detection percentage of 20%. This was caused by the HnR attack and Um nodes. The MFDSS scheme and DBSD scheme had limitations in detecting the HnR attack and Um nodes due to their design properties discussed in chapter 2.

For $N = 50$, we had 25 MUs with randomly distributed SSDF attack strategies in the network. We set $Um = 5, Ay = 6, An = 8,$ and $HnR = 6$. The missed detection probability in $N = 100$ when MUs were 50% showed to increase. We set $Um = 12, Ay = 15, An = 15,$ and $HnR = 8$. In $N = 150$ we set $MUs = 75,$ we randomly set $Um = 18, Ay = 25, An = 15,$ and $HnR = 17$. With an increase in the number of SUs and MUs where we had a high number of Um and HnR attacks, the schemes' missed detection probability increased.

5.19 Missed Detection Probability with 60% malicious users

The number of malicious nodes is further increased to 60% in figure 32 and the missed detection probability results are plotted in form of bar graphs for the proposed scheme, the DBSD scheme and the MFDSS scheme.

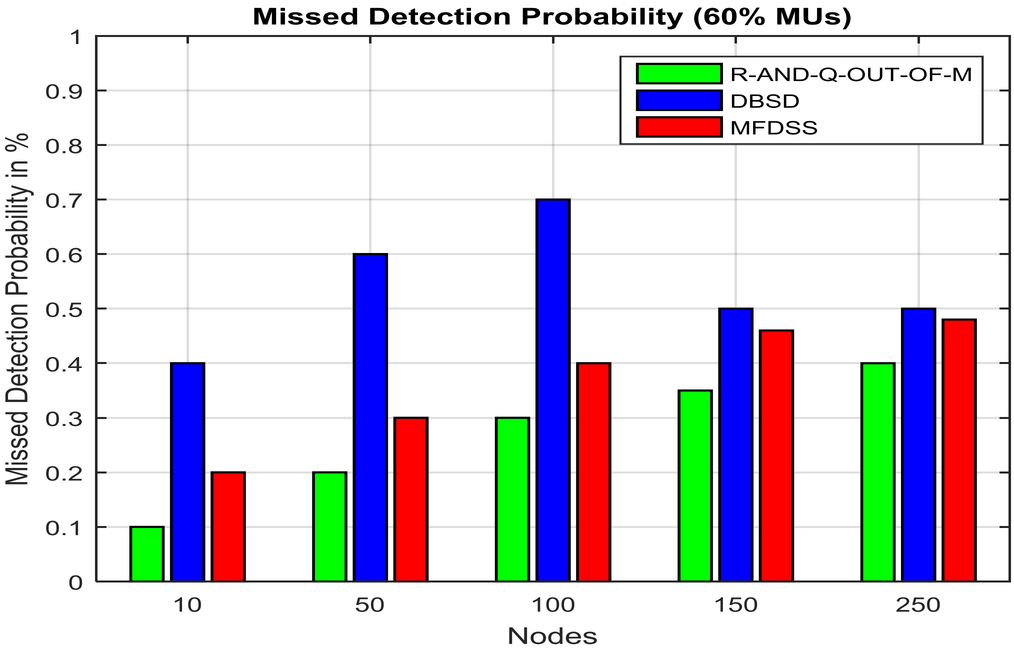


Figure 32: Probability of missed detection: 60%MUs

In figure 32, the number of MUs was more than the number of SUs, which caused the missed detection probability to increase gradually. In $N = 10$, we had $6\,MUs$ where we had $3\ Ay$ and $3\ An$ SSDF attack strategies. In $N = 50$ we had $10\ Ay, 10\ An$ and $10\ Um$. In $N = 100$ we set $Ay = 20, An = 20$, and $HnR = 20$. In $N = 150$ we had $HnR = 45$ and $Um = 45$ while in $N = 250$ we set $Ay = 45\ An = 45\ HnR = 30$, and $Um = 30$. With a large number of SSDF attacks in the network, the missed detection probability increased especially when we increased the HnR attack and the Um nodes. This was as a result of the HnR attack can alter its results to avoid being detected as a MU. This makes it difficult to estimate the attack probability of the HnR attack. The Um nodes can contain malicious results while they have good reputations, making it difficult for them to be detected.

5.20 False Alarm Probability with 10% malicious users

The results of False Alarm Probability with 10% malicious users in a network of 10, 50,100.150, and 250 are presented in figure 33.

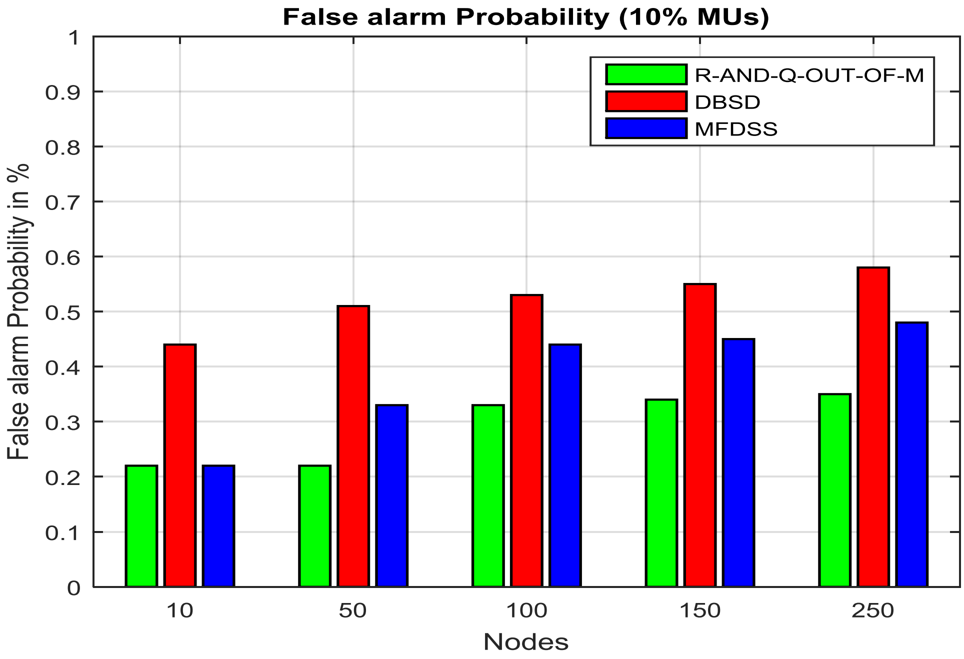


Figure 33: False Alarm Probability with 10% malicious users

Figure 33 shows the ineffectiveness of the schemes which results in isolating legitimate SUs in the network classifying them as malicious nodes. In $N = 10$, we had 9 SUs and 1 MU. $In\ N = 50$, we set 5 MUs and 45 SUs, in $N = \ 100$, we set 10 MUs and 90 SUs, in $N = 150$ we set 15 MUs and 135 SUs and in $N = 250$ we set 15 MUs and 225 SUs. As the number of SUs increased in the network the false alarm probability increased as well. The false alarm rate increased as the number of SUs increase. The false alarm rate continued to increase as we increased the number of MUs.

5.21 False Alarm Probability with 20% malicious users

Figure 34 shows the results of False Alarm Probability with 20% increased number of malicious users.

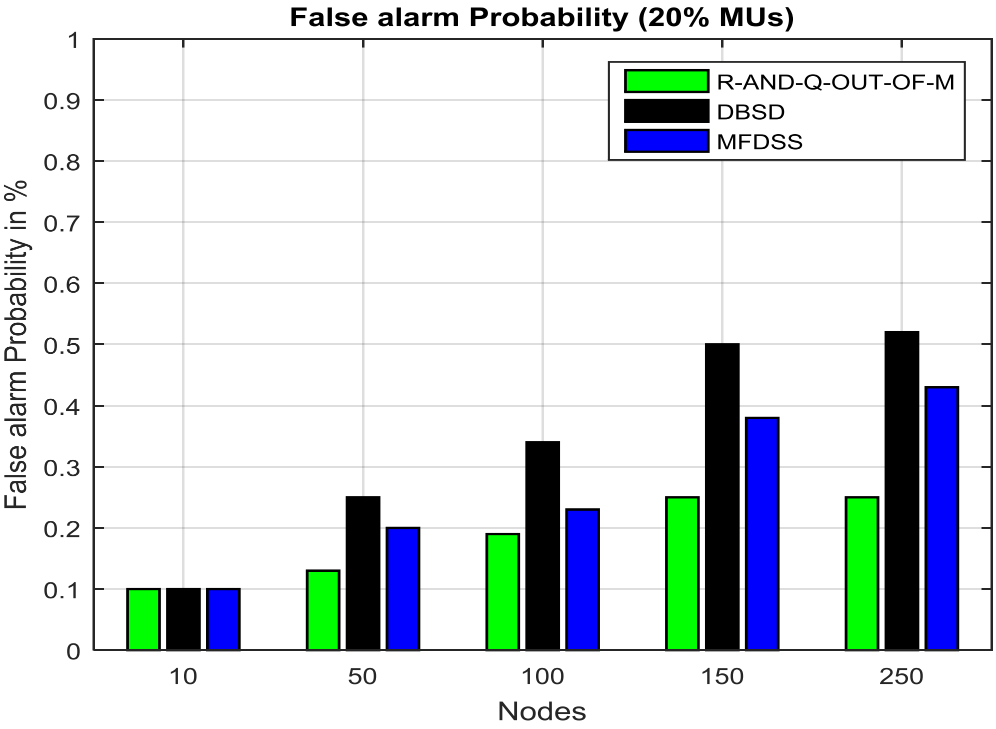


Figure 34: False Alarm Probability: 20% malicious users

In figure 34, we present the results of false alarm probability with 20% MUs in the network. In $N = 10$, we set 8 SUs and 2 MU. In $N = 50$ we set 10 MUs and 40 SUs, in $N = 100$, we set 20 MUs and 80 SUs, in $N = 150$ we set 30 MUs and 120 SUs and in $N = 250$ we set 50 MUs and 200 SUs. All the schemes recorded false alarm probability that is less than 60%. The behaviour of the results was caused by the attack strategy implemented by the SSDF attack. Unintentionally misbehaving SUs were discarded from the network due to their reports, which increased the false alarm probability of the proposed scheme.

5.22 False Alarm Probability with 40% malicious users

We present the results of False Alarm Probability with 40% malicious users in figure 35.

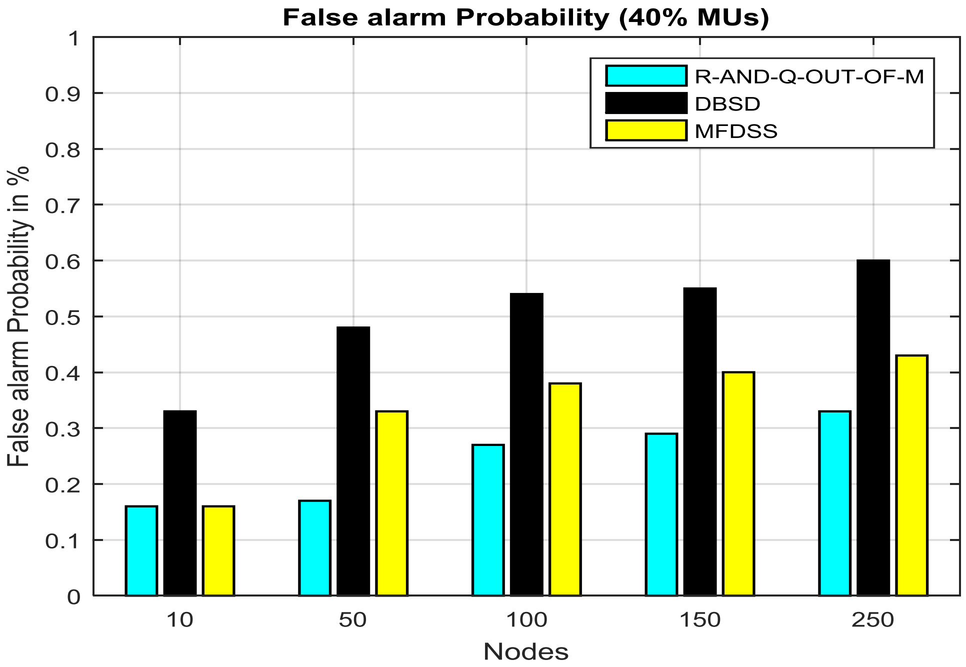


Figure 35: False Alarm Probability: 40% malicious users

In figure 35 we simulate the results of false alarm probability with 40% MUs in the network. In $N = 10$, we had 6 SUs and 4 MU. The results show that in the proposed and MFDSS schemes 1 SU was isolated in the network before the final transmission was made and 2 SUs were classified as MUs. In $N = 50$ we set 20 MUs and 30 SUs, in $N = \ 100$, we set 40 MUs and 60 SUs, in $N = 150$ we set 60 MUs and 90 SUs and in $N = 250$ we set 100 MUs and 150 SUs. The results show that as the number of SUs increased the number of MUs increased.

5.23 False Alarm Probability with 50% malicious users

Figure 36 presents the results of False Alarm Probability with 50% malicious users in a network of 10, 50,100.150, and 250 nodes.

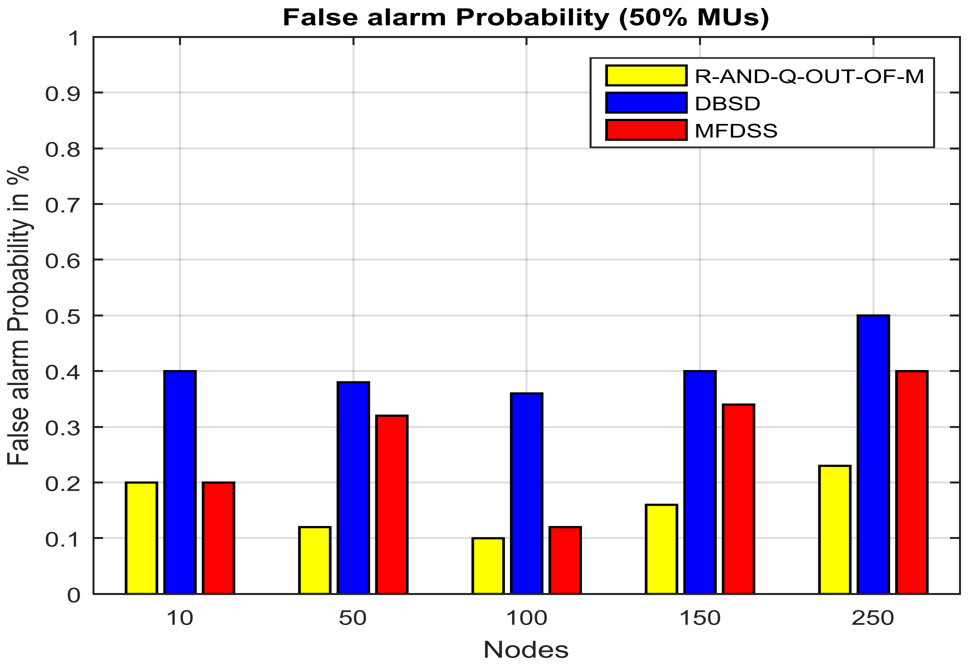


Figure 36: False Alarm Probability: 50% malicious users

In figure 36 we presented the results of false alarm probability with 50% MUs in the network. In $N = 10$, we set 5 SUs and 5 MU. In $N = 50$ we set 25 MUs and 25 SUs, in $N = 100$, we set 50 MUs and 50 SUs, in $N = 150$ we set 75 MUs and 75 SUs and in $N = 250$ we set125 MUs and 125 SUs. The results show that when we had 50% SUs in the network, the false alarm probability of the schemes reduced compared to when the MUs were 40%.

5.24 False Alarm Probability with 60% MUs

In figure 37, we present the results of False Alarm Probability with 60% malicious users in a network of 10, 50,100.150, and 250 nodes.

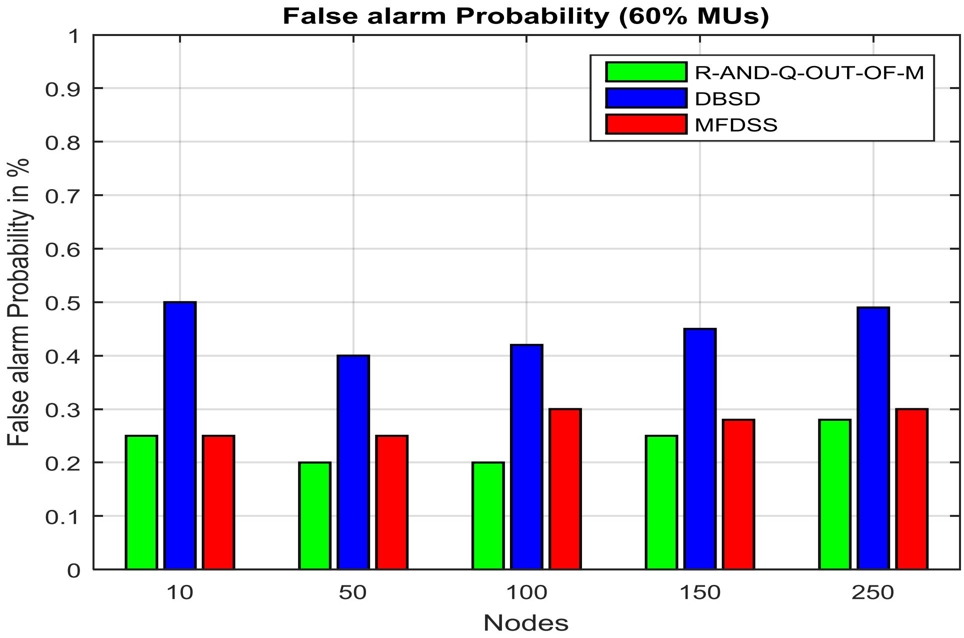


Figure 37: False Alarm Probability: 60% malicious users

In figure 37 we present the false alarm probability with 60% MUs in the network. In $N = 10$, we set 4 SUs and 6 MU. In $N = 50$ we set 30 MUs and 20 SUs, in $N = 100$, we set 60 MUs and 40 SUs, in $N = 150$ we set 90 MUs and 60 SUs and in $N = 250$ we set 150 MUs and 100 SUs. With less SUs in the network, the false alarm probability is less than 50%. The increase in the false alarm probability was caused by the increase in the percentage of MUs in the network from 50% to 60%. Even though the proposed scheme had the lowest false alarm probability and the DBSD scheme had the highest false alarm probability, the false alarm probability is still high compared to figure 36. This means that the high percentage of MUs in the network compared to SUs has a negative impact on the performance of the network.

5.3 Discussion of Findings

The proposed scheme showed to perform better compared to the DBSD scheme [52] and the MFDSS scheme [33]. The success probability of the proposed scheme outperformed the success probability of the DBSD scheme and the MFDSS scheme. The study proved that the integrated reputation and q-out-of-m rule scheme can be deployed in a CRAHN network to mitigate the SSDF attack. The simulations proved that the reputation based system can be deployed to isolate the SSDF attack. We implemented the q-out-of-m rule scheme to discourage the hit and run attack and from the results, this was proven to be effective as it increased the success probability while it minimized the missed detection probability. The implemented reputation based system managed to distinguish between the misbehaving SUs and outliers because the proposed scheme had the lowest false alarm probability compared to the DBSD scheme and the MFDSS scheme.

Conclusion

Chapter 5 compares the performance results of the proposed scheme with the MFDSS and the DBSD schemes. We focussed on the success probability of the schemes in detecting MUs, missed detection probability, and false alarm probability in classifying legitimate SUs to be MUs. The results show that the proposed scheme was superior in all the evaluation metrics. We evaluated the schemes by increasing the MUs attack percentages and by varying the attack strategies and increasing the network sizes. We evaluated the schemes and attack strategies of the SSDF attack with different percentages. We can, therefore, conclude that the most effective attack strategies of the SSDF attack are the HnR attack and the Um nodes because they can bypass the defence schemes. The always yes and always no attacks were easily detected because their values were distinct in comparison to the normal SUs values.

CHAPTER 6: CONCLUSION

6.1 Introduction

CRN technology promises to address the limitations of the spectrum shortage by allowing SUs to transmit in the white space of the PUs licenced band. However, security attacks such as the SSDF leads to new challenges in CRN. The potential of CRN has attracted a significant number of researchers, however, the security aspect of CRN especially CRAHN still requires further research. In this study, we investigated the SSDF attack in CRAHN and implemented a defence mechanism known as the R-AND-Q-OUT-OF-M rule scheme. We compared the scheme against the MFDSS and DBSD to evaluate its effectiveness in detecting the SSDF attack and isolating MUs or compromised nodes. In this chapter, we discuss the summary of the findings from the investigations and make recommendations and outline possible future research direction.

6.2 Research Summary

This study investigated the three types of SSDF attacks. The always yes, always no, and hit and run attack focusing on the MAC layer of CRN. The always yes, consistently reports that idle spectrum band is occupied. The always no reports that occupied spectrum band is idle. The hit and run attack can modify its report to avoid being detected. We have established that the aim of these attacks is to cause denial of service either to the SUs or interference to the PUs. We have also discussed unintentionally misbehaving SUs that report incorrect observations due to challenges in the network environment.

In an attempt to address the security challenges, we implemented the reputation and the q-out-of-m rule scheme in CRAHN. The reputation-based system evaluates the past reports of the SUs to determine their level of trustworthiness. The q-out-of-m rule scheme selects 60% from the reports with a good reputation. The final transmission decision is based on the majority of reports q. reputation updating was implemented to update the reputation of malicious nodes. We set our TV in the reputation-based system to 60% to accommodate the unintentionally misbehaving SUs. We implemented energy detection as the sensing technique as it is widely used by other researchers.

The simulation results show that the Reputation-and-q-out-of-m rule scheme is the best performing algorithm for detecting and isolating MUs. We analysed the DBSD, MFDSS, and the R-AND-Q-OUT-OF-M rule schemes. The results show that the hit and run attack and the unintentionally misbehaving SUs could negatively affect the performance of the scheme if not detected and isolated.

6.3 Recommendations

There is a need to conduct more extensive research in CRAHN security in large networks to evaluate the performance of the proposed scheme in detecting the SSDF attack. The attack strategies of the hit-and-run attack still require further investigation. The non-collaborative SSDF attack with different attack probabilities needs to be further investigated. There is need to investigate the unintentionally misbehaving nodes and implement a scheme that will accommodate them without causing interference to PUs transmission.

6.4 Conclusion

The study investigated the spectrum sensing data falsification attack in cognitive radio ad hoc networks. We implemented the reputation-based system and q-out-of-m rule scheme to mitigate the effects of the attack. We studied the always yes attack, always no attack and hit and run attack. We also studied unintentionally misbehaving SUs and used the reputation-based system to accommodate them. We compared our proposed scheme with the multifusion-based distributed spectrum sensing scheme and the density based scheme. Our metrics were the success probability, missed detection probability and false alarm probability. Our proposed scheme performed better in detecting malicious users and isolating them from the network before the final transmission decision was made.

References

[1] R. Kishore, C. . K. Ramesha and S. Tanuja , “uperior Selective Reporting mechanism for cooperative spectrum sensing in cognitive radio networks,” in *Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on wireless communications*, Chennai, India, 2016.

[2] A. Chakraborty , . J. S. Banerjee and A. Chattopadhyay, “Non-Uniform Quantized Data Fusion Rule Alleviating Control Channel Overhead for Cooperative Spectrum Sensing in Cognitive Radio Networks,” in *IEEE 7th International Advance Computing Conference (IACC)*, Hyderabad, India, 2017.

[3] H.K. Boddapati, M. . R. Bhatnagar and S. Prakriya, “Performance of Incremental Relaying Protocols for Cooperative Multi-Hop CRNs,” *IEEE Transactions on Vehicular Technology,* vol. PP, no. 99, pp. 1-1, 2018.

[4] Z.H. Wei and B.-j. Hu, “A Fair Multi-channel Assignment Algorithm with Practical Implementation in Distributed Cognitive Radio Networks,” *IEEE Access,* vol. PP, no. 99, pp. 1-1, 2018.

[5] B. Chen, Z. Gao, M. Yang, Q. Ning, C. Yu, W. Pan, M. Nian and D. Xie, “Packet. Multicast. in Cognitive. Radio. Ad. Hoc. Networks: A Method. Based. on Random. Network. Coding,” *IEEE ACCESS,* vol. 14, no. 9, pp. 1-13, 2017.

[6] O. Elnahas, M. Elsabrouty, O. Muta and H. Furukawa, “Game Theoretic Approaches for Cooperative Spectrum Sensing in Energy-Harvesting Cognitive Radio Networks,” *IEEE Access ,* vol. PP, no. 99, pp. 1-1, 2018.

[7] Y. Gan, C. Jiang, N. C. Beaulieu, J. Wang and Y. Ren, “Secure Collaborative Spectrum Sensing: A Peer-Prediction Method,” in *IEEE Transactions and Communications*, 2016.

[8] Y. B. Reddy, “Security Issues and Threats in Cognitive Radio Networks,” in *The Ninth Advanced International Conference on Telecommunications*, Louisiana, USA, 2013.

[9] H. Wang, Y.-D. Yao and S. Peng, "Prioritized Secondary User Access Control in Cognitive Radio Networks," *IEEE Transactions on Vehicular Technology,* vol. PP, no. 99, pp. 1-1, 2018.

[10] J. HAN, M. KAMBER and J. PEI, "Outlier Detection," in *Chapter 12 of Data Mining: Concepts and Techniques*, 2017, pp. 1-25.

[11] P. Bai, X. Zhang and F. Ye, "Reputation-based Beta reputation system against SSDF attack in cognitive radio networks," in *2017 Progress in Electromagnetics Research Symposium* , PIERS, 2017.

[12] M. Abdelhakim, L. Zhang, J. Ren and T. Li, "COOPERATIVE SENSING IN COGNITIVE NETWORKS UNDER MALICIOUS ATTACK," in *ICASSP*, IEEE, 2011.

[13] H. su and X. Zhang, "Cognitive Radio Based Multi-Channel MAC Protocols for Wireless Ad Hoc Networks," in *global communications conference* , 2007.

[14] P. S. Yawada, A. J. Wei and M. M. Kiki, "Performance evaluation of energy detection based on non-cooperative spectrum sensing in cognitive radio network," in *Computer Science and Network Technology (ICCSNT), 2015 4th International Conference on Computer Science and Network Technology(ICCSNT)*, Harbin, China, 2015.

[15] X. Dong, Y. Gong, J. Ma and Y. Guo, "Protecting Operation-Time Privacy of Primary Users in Downlink Cognitive Two-Tier Networks," *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY,* vol. PP, no. 99, pp. 1-1, 2018.

[16] A. N. Jadhav and S. C. Shinde, "centralized cooperative and non cooperative spectrum sensing using energy detectionin cognitive radio," *International Journal of Recent Scientific Research,* vol. 6, no. 8, pp. 5764-5767, 2015.

[17] I. F. Akyildiz, B. F. Lo and R. Balakrishnan, "Coperative spectrum sensing in cognitive radio networks," *A survey,"phy.commun",* vol. 4, no. 1, pp. 40-62, 2011.

[18] C. Wong, W. C. Molani, W. Molani and A. Nallanathan, “Cooperative spectrum sensing strategies for cognitive radio mesh networks,” *IEEE J.sel. Topics Signal Process,* vol. 5, no. 1, pp. 56-67, 2011.

[19] K. Kumar and V. Sindhu, “Comparison of Non-Cooperative Spectrum Sensing Techniques in Cognitive Radio,” *International Journal of Wired and Wireless Communications,* vol. 4, no. 1, pp. 16-18, 2015.

[20] J. Tong, M. Jin, Q. Guo and Y. Li, “Cooperative Spectrum Sensing: A Blind and Soft Fusion Detector,” *IEEE Transactions on Wireless Communications,* vol. PP, no. 99, pp. 1-1, 2018.

[21] H. Chen, M. Zhou, L. Xie and J. Li, “Cooperative Spectrum Sensing With M-Ary Quantized Data in Cognitive Radio Networks Under SSDF Attacks,” *IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS,* vol. 16, no. 8, pp. 5244-5257, 2017.

[22] M. Sun, M. Jin , . Q. Guo and . Y. Li, “Cooperative Spectrum Sensing Under Ambient Malicious Interferences,” *IEEE Communications Letters,* vol. 22, no. 2, pp. 432-435, 2018.

[23] D. Wang and A. H. Tewfik, “Efficient Cooperative Spectrum Sensing in Cognitive Radio,” in *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, Honolulu, HI, USA, 2009.

[24] I. Ngomane, M. Velempini and S. V. Dlamini, “The design of a defence mechanism to mitigate the spectrum sensing data falsification attack in cognitive radio ad hoc networks,” in *International Conference on Advances in Computing and Communication Engineering (ICACCE)*, Durban, South Africa, 2016.

[25] A. Vosoughi, . J. R. Cavallaro and . A. Marshall, “A cooperative spectrum sensing scheme for cognitive radio ad hoc networks based on gossip and trust,” in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Atlanta, GA, USA, 2015.

[26] E. Soltanmohammadi and M. Naraghi-Pour, “Fast Detection of Malicious Behavior in Cooperative Spectrum Sensing,” *IEEE Journal on Selected Areas in*

Communications, vol. 32, no. 3, pp. 377-386, 2013.

[27] H. S. Magdalene and . L. Thulasimani, “Analysis of Spectrum Sensing Data Falsification (SSDF) Attack in Cognitive Radio Networks: A Survey,” *Journal of Science & Engineering Education,* vol. 2, pp. 98-100, 2017.

[28] G. Nie , G. Ding, L. Zhang and Q. Wu, “Byzantine Defense in Collaborative Spectrum Sensing via Bayesian Learning,” *IEEE Access,* vol. 5, pp. 20089-20098, 2017.

[29] S. M. Karmoose and M. Youssef, “Censoring for improved sensing mperformance in infrastructure-less cognitive radio networks,” in *Wireless intelligent network center(WINC)*, Egypt, 2015.

[30] F. R. Yu, M. Huang and H. Tang, “Biologically Inspired Consensus-Based Spectrum Sensing in Mobile Ad Hoc Networks with Cognitive Radios,” *IEEE Networks,* vol. 24, no. 3, pp. 26-30, 2010.

[31] W. Wang , H. Li , Y. Sun and Z. Han, “Attack-proof collaborative spectrum sensing in cognitive radio networks,” in *43rd Annual Conference on Information Sciences and Systems*, Baltimore, MD, USA, 2009.

[32] Z. Li, F. R. Yu and M. Huang, “A Distributed Consensus-Based Cooperative Spectrum-Sensing Scheme in Cognitive Radios,” *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY,* vol. 59, no. 1, pp. 383-393, 2010.

[33] K. Pongaliur and . L. Xiao, “Multi-fusion Based Distributed Spectrum Sensing against Data Falsification Attacks and Byzantine Failures in CR-MANET,” in *2014 IEEE 22nd International Symposium on Modelling, Analysis & Simulation of Computer and Telecommunication Systems*, Paris, France, 2014.

[34] K. Sindhuja, A. NasrinBanu and K. Elavarasi, “Survey on Malicious Node Detection and Reliable Data Fusion in MANET,” *International Journal of Scientific Research Engineering & Technology (IJSRET),* vol. 4, no. 3, pp. 2278-0882, 2015.

[35] S. Couturier, . J. Krygier , . O. . I. Bentstuen and . V. . L. Nir, “Challenges for

network aspects of Cognitive Radio," in *2015 International Conference on Military Communications and Information Systems (ICMCIS)*, Cracow, Poland, 2015.

[36] K. K. Patel, . A. Durvesh and D. F. Matibe, "Multi-selfish attacks and detection in cognitive radio network using CRV," in *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, India, 2017.

[37] X. ZHANG, X. ZHANG, L. HAN and R. XING, "Utilization-Oriented Spectrum Allocation in an Underlay Cognitive Radio Network," *IEEE Access,* vol. PP, no. 99, pp. 1-1, 2018.

[38] D. Pang, . Z. Deng, G. Hu, Y. Chen and M. Xu, "Cost Sharing Based Truthful Spectrum Auction with Collusion-Proof," *China Communications,* vol. 2, no. 15, pp. 74-87, 2018.

[39] Z. Li, F. Xiao, S. Wang, T. Pei and J. Li, "Achievable Rate Maximization for Cognitive Hybrid Satellite-Terrestrial Networks with AF-Relays," *IEEE Journal on Selected Areas in Communications,* vol. PP, no. 99, pp. 1-1, 2018.

[40] T. Xiong, Y.-D. Yao, Y. Ren and . Z. Li, "Multiband Spectrum Sensing in Cognitive Radio Networks with Secondary User Hardware Limitation: Random and Adaptive Spectrum Sensing Strategies," *IEEE Transactions on Wireless Communications,* vol. PP, no. 99, pp. 1-1, 2018.

[41] N. Mansoor, A. M. Islam, M. Zareei and C. Vargas-Rosales, "RARE: A Spectrum Aware Cross-Layer MAC Protocol for Cognitive Radio Ad-Hoc Networks," *JOURNAL OF IEEE ACCESS,* vol. PP, no. 99, pp. 1-1, 2018.

[42] M. Seif, M. Karmoose and M. Youssef, "Censoring for Improved Sensing Performance in Infrastructure-Less Cognitive Radio Networks," in *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)*, Glasgow, UK, 2015.

[43] T. S. Syed and G. . A. Safdar , "History-Assisted Energy-Efficient Spectrum Sensing for Infrastructure-Based Cognitive Radio Networks," *IEEE Transactions*

on Vehicular Technology , vol. 66, no. 3, pp. 2462 - 2473, 2016.

[44] J. Kumar and M. K. Panda, “Ad hoc network routing protocols on random waypoint model,” in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, India, 2016.

[45] R. Chen and K. Brian, “Robust distributed spectrum sensing in cognitive radio networks,” in *In 27th Conference on Computer Communication,INFOCOM*, Phoenix,USA, 2008.

[46] R. Chen, J. Park and K. Brian , “Robustness against byzantine failures in Distributed spectrum sensing,” *Elsevier Computer Communications,* pp. 2115-2124, 2012.

[47] E. Noon and H. Li, “Defending against hit-and-run attackers in collaborative spectrum sensing of cognitive radio networks,” in *In Proceedings of the 71st IEEE Vehicular Technology conference*, VTC Spring, 2010.

[48] F. Yu, M. Huang, Z. Li and P. Mason, “Defence against specrtum sensing data falsification attacks in mobile ad hoc networks with cognitive radios,” in *In proc* , milcom, 2009.

[49] H. Li and Z. Han, “Catching Attacker(s) for Collaborative Spectrum Sensing in Cognitive Radio Systems: An Abnormality Detection Approach,” in *2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN)*, Singapore, 2010.

[50] C. S. Hyder, . B. Grebur, . L. Xiao and . M. Ellison, “ARC: Adaptive Reputation based Clustering Against Spectrum Sensing Data Falsification Attacks,” *IEEE Transactions on Mobile Computing,* vol. 13, no. 8, pp. 1707 - 1719, 2014.

[51] A. Vosoughi , . J. R. Cavallaro and A. Marshall, “Robust Consensus-Based Cooperative Spectrum Sensing under Insistent Spectrum Sensing Data Falsification Attacks,” in *2015 IEEE Global Communications Conference (GLOBECOM)*, San Diego, CA, USA, 2015.

[52] C. Chen, . M. Song and C. Xin, “density based scheme to countermeasure

spectrum sensing data falsification attacks in cognitive radio networks," in *2013 IEEE Global Communications Conference (GLOBECOM)*, Atlanta, GA, USA, 2014.

[53] Z. Wei, "Trust Management for Security Enhancements in Ad hoc Networking Paradigms with Uncertain Reasoning," Ottawa-Carleton Institute for Electrical and Computer Engineering (OCIECE), Ottawa, Ontario, Canada, 2016.

[54] A. Bagwari and G. . S. Tomar, "Multiple Energy Detection vs Cyclostationary Feature Detection Spectrum Sensing Technique," in *2014 Fourth International Conference on Communication Systems and Network Technologies*, Bhopal, India, 2014.

[55] S. Helif, R. Abdulla and S. Kumar, "A review of energy detection and cyclostationary sensing techniques of cognitive radio spectrum," in *2015 IEEE Student Conference on Research and Development (SCOReD)*, Kuala Lumpur, Malaysia, 2015.

[56] R. T. Khan, M. I. Islam , S. Zaman and M. R. Amin, "Comparison of cyclostationary and energy detection in cognitive radio network," in *2016 International Workshop on Computational Intelligence (IWCI)*, Dhaka, Bangladesh, 2016.

[57] X. Liu, Y. Wang, Y. Chen, . J. Xia, X. Zhang, W. Lu and F. Li , "A Multichannel Cognitive Radio System Design and Its Performance Optimization," *IEEE Access,* vol. PP, no. 99, pp. 1-1, 2018.

[58] Y. Arjoune, Z. El Mrabet, H. El Ghazi and A. Tamtaoui, "Spectrum sensing: Enhanced energy detection technique based on noise measurement," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2018.

[59] P. Santi , The Random Waypoint Model, Wiley Telecom, 2012.

[60] w. m. Scheaffer, Mathematical statistics with applications 7th edition, Duxbury Pr; 7th ed.edition, 2007.

[61] D. B. Johanson and D. A. Maltz, “Dynamic source routing in ad hoc wireless networks,” in *Mobile computing Volume 353*, kluwer Academic publishers, 1996, pp. 153-181.