AIRO JOURNALS

Free / Unpaid
Peer Reviewed
Multidisciplinary
International

ISSN:2320-3714
Volume:3 Issue:3
September 2022
Impact Factor:5.7
Subject:Engineering

SYBIL AVOIDANCE USING HYBRID MULTIHOP AND SUPERNODE ROUTING

Vineeta Babu
Research Scholar
University of Technology, Jaipur
Dr. Pramod Sharma
Professor
University of Technology, Jaipur

DECLARATION: I AS AN AUTHOR OF THIS PAPER / ARTICLE, HEREBY DECLARE THAT THE PAPER SUBMITTED BY ME FORPUBLICATION IN THE JOURNAL IS COMPLETELY MY OWN GENUINE PAPER. IF ANY ISSUE REGARDING COPYRIGHT/PATENT/ OTHER REAL AUTHOR ARISES,THE PUBLISHER WILL NOT BE LEGALLY RESPONSIBLE. IF ANY OF SUCH MATTERS OCCUR PUBLISHER MAY REMOVE MY CONTENT FROM THE JOURNAL WEBSITE. FOR THE REASON OF CONTENT AMENDMENT/OR ANY TECHNICAL ISSUE WITHNO VISIBILITY ON WEBSITE/UPDATES, I HAVE RESUBMITTED THIS PAPER FOR THE PUBLICATION. FOR ANY PUBLICATION MATTERS OR ANY INFORMATION INTENTIONALLY HIDDEN BY ME OR OTHERWISE, I SHALL BE LEGALLY RESPONSIBLE. (COMPLETE DECLARATION OF THE AUTHOR AT THE LAST PAGE OF THIS PAPER/ARTICLE

Abstract:

This paper defines the physical reputation-based routing (PRBR) protocol and presents the integration of physical-layer information to facilitate reputation routing in the presence of supernodes. It is possible that nodes will not always be able to reach a supernode coordinator due to the fluctuations in deployment density that occur in stochastic topologies. Additionally, it is possible that supernode data delivery will not always be successful, necessitating retransmissions, which will lead to capacity reductions. As a result, one of the requirements for resilience is that several data relaying mechanisms should be made available, and if at all possible, the selection process amongst them should be dynamic. Simulation results in a malicious topology that is vulnerable to attack from malicious Sybil nodes have been presented. It has been proved that the scheme can bypass the supernodes that are vulnerable to a Sybil attack by routing the majority of its traffic through supernodes that are not vulnerable to Sybil attacks.

Keywords: Supernode, Physical, Reputation, Routing, Sybil.

I. INTRODUCTION

A variety of problems, such as temporary obstructions of nodes because of shadowing from mobile obstructions, time-dependent changes such as slow fading, and malicious jamming attacks from external devices, can change network conditions and therefore make it more difficult for supernode data to be delivered.

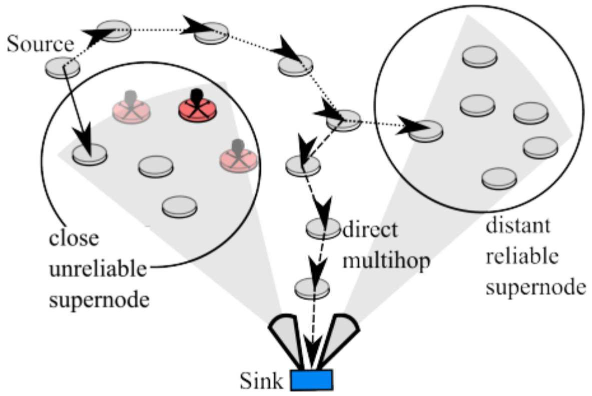

Figure 1: Methods for routing in the context of supernodes that are only intermittently trustworthy

Therefore, even if a node is located in close proximity to a specific supernode, it is still feasible that other mechanisms may give superior performance when it comes to the delivery of data. Figure 1 is an illustration of the data relaying options available. It shows a node adjacent to an unreliable supernode (as a result of a malicious attack), but it also shows the possibility of relaying data via a more reliable supernode located further away (highlighted by a dotted line), or using a pure multihop route to get to the sink (dashed line). In physical-reputation-based routing, the reputation-based routing protocol is altered so that it uses cross-layer information obtained from the physical layer (PRBR). This protocol takes into consideration information from the physical layer by utilising the signal-to-interference-and-noise ratio (SINR) of any supernodes that make up the last connection in the route. Because the supernode is the last limiting factor in delivery success, this is an important metric to consider when evaluating the likelihood of successful data delivery in the future. By evaluating these physical-layer metrics, the PRBR protocol is able to gradually learn the performance characteristics of these supernodes during the operation of the network and distribute this knowledge throughout the network as part of the route construction process. If a supernode is able to give consistently good performance at the physical layer, then it will be reinforced, and it will have a greater chance of being included in multihop routing from other sources.

Increased robustness is one of the benefits that come with using this strategy. In the event that a supernode is unable to deliver the idealised physical layer gain due to issues with the physical layer, such as channel changes (caused by obstruction), or local oscillator instability, this will be reflected in a poorer performance as determined by the sink upon reception of the signal. Those supernodes that are experiencing performance issues should be able to relay a smaller volume of traffic if alternative supernodes are allowed to take over. This is likely to occur in this scenario.

II. LITERATURE REVIEW

Dr. E.N. Ganesh (2022) - "Wireless sensor networks" have been a topic of active attention as a result of recent developments in low-cost and low-power wireless communication as well as advancements in ad-hoc networking routing and protocols. Sensor circuits, analog-to-digital converters, microprocessors, and wireless communications transceivers are examples of the types of hardware components that are often included in a wireless sensor network. In order for these pieces of hardware to collaborate toward the completion of a user-defined job, they need to be programmed to do so with the help of various software tools. The collecting of data and the transmission of RF signals are going to be the primary focuses of this kind of network. In this work, we will discuss basic notions in this developing multidisciplinary study field, and we will support those concepts with references to commercial products that are now accessible. Two distinct categories of applications for wireless sensor networks in the real world have been discovered. As part of the continuous work that we have been doing, we have developed a thorough design framework for an intelligent wireless patient monitoring system. It is anticipated that the subsequent research initiatives and strategic partnerships in the microelectronics and wireless sectors in Canada will be initiated as a result of this introductory presentation.

Huda M. Abdulwahid and Alok Mishra (2022) - In recent years, numerous types of monitoring systems have been built for a variety of purposes in order to change urban settings into smart cities. The goal of this transformation is to make cities more intelligent. The vast majority of these systems are wireless sensor networks (WSNs), and the process of creating these systems has been plagued by a number of challenges. The installation of sensor nodes is the primary and most significant challenge. The primary purpose of wireless sensor networks (WSNs) is to collect the necessary data, process that data, and then transmit it to far-flung locations. Since a large number of sensor nodes were placed in the monitored region, the primary objective of the research is to identify the optimal deployment strategy that provides optimum coverage and connectivity with the fewest possible sensor nodes. This work presents a systematic mapping analysis that encompasses the most current studies that have focused on solving the deployment problem by utilizing optimization algorithms, particularly heuristic and meta-heuristic algorithms throughout the period of time (2015–2022). It was discovered that thirty-five percent of these research improved their swarm optimization methods in order to address the deployment issue. The academics and practitioners who read this paper will find it useful for figuring out new algorithms and seeking objectives for sensor deployment. Along with a comparison chart, this section explains the fundamental ideas behind smart cities and wireless sensor networks (WSNs). In conclusion, an outline of the difficulties and unresolved problems is presented.

S. Sharma and Vijay Chahar (2022) -Typical realistic challenges have a number of goals that are in direct opposition to one another. As a result, approaching the engineering challenges as multi-objective optimization problems comes naturally. In this study, the multi-objective optimization methods and their variations are discussed, along with the benefits and drawbacks of each. There is an in-depth discussion of representative algorithms from each of the categories. The discussion is on the applications of a variety of multi-objective algorithms in a variety of engineering subfields. The authors identify both open difficulties and potential future avenues for multi-objective algorithms. This paper includes pertinent features of multi-objective algorithms, which will assist new researchers in applying these algorithms in their respective research fields.

Dipayan Guha, et al (2022) - A careful selection and fine-tuning of the controller's parameters is very necessary in order to get the most possible performance out of the frequency controllers that are being used in the system. This chapter presents a variety of population-based meta-heuristic techniques that have recently been presented for the purpose of examining near-optimum settings of the applied/designed frequency controllers. In depth discussion has been had on the idea for the applied algorithms, which were based on their mathematical model. Comparative research has demonstrated that the meta-heuristic strategies that are utilized in controller parameter tuning have the computational capabilities to achieve the desired results. In addition, the necessity for hybridised algorithms that combine computational and mathematical models has been laid forth in this chapter as a means of enhancing the overall performance of optimization methods. Approaches based on chaotic mapping and quasi-oppositional learning are discussed in this article in order to investigate the performance of hybridised algorithms.

Pallavi Joshi, et al (2022) - Energy dissipation is the primary problem when it comes to ensuring effective data transmission in a wireless network. Because of the increased size of the network, there is a greater need to aggregate the information, which results in the nodes running out of energy. In order to address problems of this nature, it is necessary to devise a data transmission paradigm that is both effective and efficient. In this research, the notion of modified LEACH, also known as MOD-LEACH, is implemented for clustering nodes. The suggested model is supported by an optimized strategy known as cuttlefish optimization (CO), which makes use of two objective functions in order to optimize the parameters of the network. In addition to the efficient cluster head selection, the model also includes this strategy. Comparisons are made between the novel work that has been proposed and two methods that are already in use. Both experimental and theoretical findings indicate that the proposed model is superior to the two similar pre-existing methods in terms of the average amount of energy consumed, the number of nodes that are still alive, and the total number of packets that are delivered to the base station. The solution that has been presented results in a decrease of around 75% in the amount of energy that the network consumes.

III. SIMULATION METHODOLOGY AND VALIDATION

Simulation Methodology

MATLAB is used to create the simulation's environment. The process begins with the generation of a topology realisation and the establishment of supernode clique memberships. Randomness is incorporated into the source activation model, and three sources are turned on for each routing period. The reputation level values for the network graph are used to compute routes to all potential supernode coordinators. These values are then used to calculate RMi; j for all links, and the route that has the lowest aggregate reputation metric is selected and given an increment to make it more reliable. The increment in reputation that is acquired for these routes is determined by the suitable sink SINR for the simulated supernode transmission. This simulation takes into consideration the fact that the aggregate transmission includes supernode transmission at a certain level. According to Equation 5.3, a decay factor of exponential proportion is provided to each of the route level values.

Simulation Validation

In this section, we will discuss the validation of the simulations for reputation-based routing over physical networks (PRBR). MATLAB was utilised in the development of the simulation software used in this chapter. The prototype for disturbance-based and reputation-based routing was constructed, and it was successfully validated against an independent version written in OCaml. This prototype served as the basis for the routing engine.

Fixed-Supernode Topology for Simulation Validation

A simplified topology known as the fixed-supernode topology was utilised in order to validate the simulations. In this topology, supernodes are viewed as abstract entities whose performance is hard-coded into the simulation topology. This aids in verifying the simulations by making the anticipated behaviour analytically tractable, in addition to simplifying the simulation by removing the complications of supernode member recruitment and the fluctuations in performance that emerge from those complications. An example topology is presented in Figure 5.3. This topology consists of a single source and three candidate supernodes, each of which has a sink SINR performance of either 0 dB, 12 dB, or 4 dB. Through a member node that is located on their boundary, any of the three supernode coordinators can be contacted from the source node S.

Validating Choosing of Best Candidate Supernodes

The values of the reputation metric are taken into consideration when PRBR routing chooses which supernodes to use. When starting out the simulation, if no reputation is applied, all connection metrics will be equal to the reputation null constant (RNK). In this scenario, PRBR-RREQ packets will be flooded through the several possible supernodes and will arrive at the sink with the same reputation metric; nevertheless, a choice will be made between them based on their physical signal-to-noise ratio. The path that has the greatest SINR will have reinforcements added to it. From that point forward, any time S makes a routing request in the future, its continued reinforcement will lead it to be selected as the best option. For example, the supernode depicted in Figure 5.3 that has a SINR that is equal to or greater than 12 dB will be chosen for all subsequent requests.

This is seen in Figure 2, which depicts the SINR for all of the routing requests that were processed by 100 trials of supernodes with fixed performance. There were a total of 20 successive routing requests made from the source, and each subsequent routing request was issued after the preceding one had expired. The signal-to-noise ratio (SINR) performance of the supernodes was evenly distributed between 0 and 12 dB, but there was guaranteed to be at least one supernode with a performance of more than 4 dB. (Which according to the protocol logic is the minimal threshold SIRthresh to receive a reputation increment). The results are displayed with their SINRs arranged according to the best performing supernode that was accessible during that experiment. It has been demonstrated that the modal SINR for all routing requests is exactly equal to the maximum SINR that is accessible in the topology. This demonstrates that the initial route request was responsible for selecting the supernodes with the highest level of performance. This demonstrates the right behaviour of the reputation routing increment and the simulator's sensitivity to the SINR characteristics of the supernode, both of which are necessary for validating the simulator.

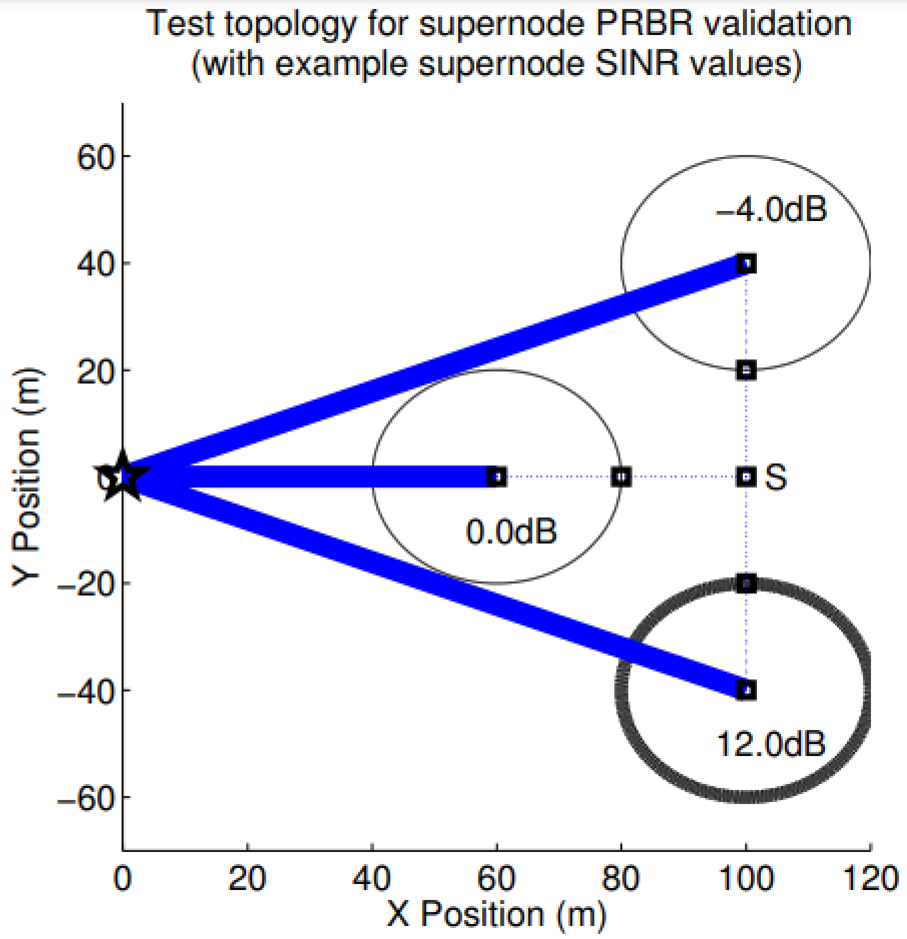

Figure 2: The fixed-supernode topology with a single source

IV. TOPOLOGY STRUCTURE

The topology is a uniform random topology, and it is square in shape with a side length of 1000 metres. It consists of three supernodes in addition to the multihop relaying nodes. The deployment density of nodes is adjusted so that the expected number of relaying nodes within a supernode is equivalent to the smallest possible clique size, K. The sink is strategically placed in the middle of the network, and it sends its data out of the network via an external out-of-band channel or a wired link so that it can be processed or analysed elsewhere. The polar coordinates for the location of the supernodes are (400m; =2), (400m; =3), and (400m; 2 =3) respectively. Figure 3 depicts one realisation of this topology that can be implemented.

It is presumed that a predetermined percentage of the participating nodes are Sybil nodes, and that the number of Sybils is distributed in an even manner across the topology. This corresponds to a scenario in which there is an adversary with sufficient resources who is capable of either manually inserting malicious nodes throughout the network or having the ability to remotely reprogram a significant proportion of network nodes. During the process of neighbour discovery, Sybils will answer several times with additional falsified identities; yet, they will not be able to make the anticipated contribution to the beam forming broadcast. Due to the inability of these nodes to live up to their responsibilities and make a contribution to the transmission to the sink, the performance of the supernodes that are centred upon Sybils will be far worse than what was originally envisaged.

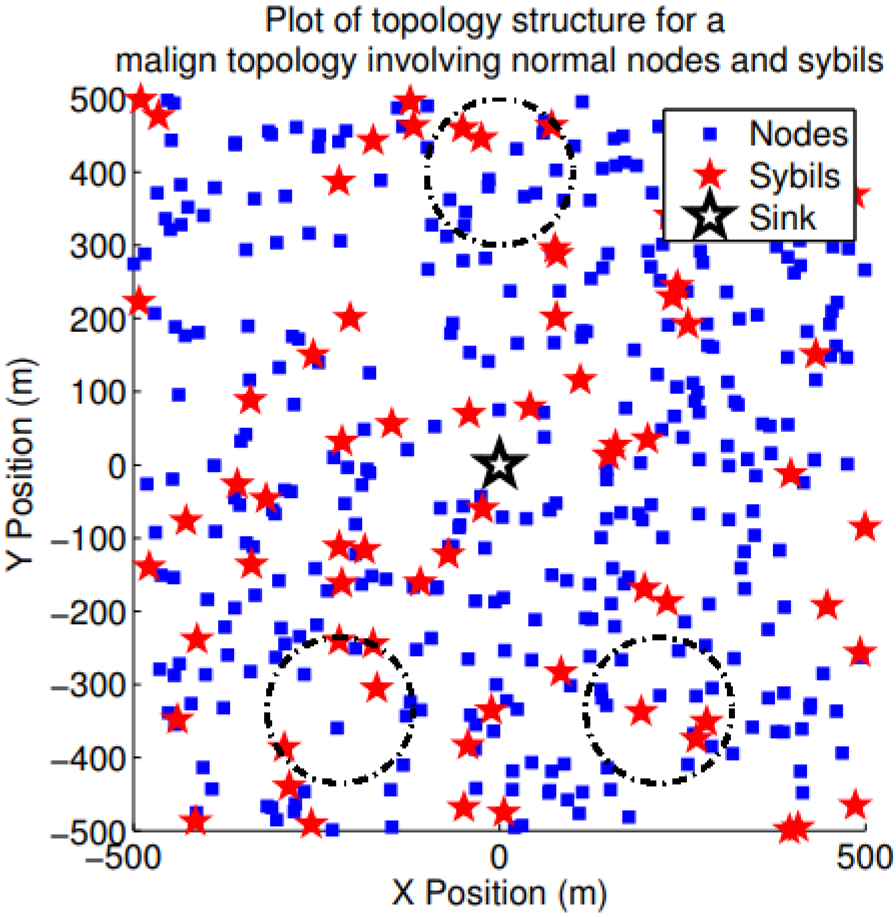

Figure 3: The structure of a standard topology that is infected with Sybils that are malevolent.

V. RESULTS

In the following subsection, the findings of an investigation into the functionality of PRBR routing while Sybil nodes are present will be described. The values for the parameters that were used in the simulations can be found in Table 1. It is possible to think of the level of instantaneous change in supernode performance as an approximation of a log-normal variable with a standard deviation of 0:6dB. This amount is equivalent to a figure that results from an oscillator drift of less than 0.5 radians, which, in 95% of cases, results in a loss of the beam forming gain of less than 3 dB.

Table 1: Simulation parameters for topology and routing protocol

Symbol	Parameter	Value
T	Topology ensemble size	20
DP	Supernode communication radius	100m
AG	Sink Antenna gain	40 (dB)
kdB	One-metre loss constant	35 (dB)
	Log-distance rolloff exponent	4
K	Supernode membership including coordinator	13
p	Sybil proportion	2/12
SI	Sybil total identities	3
PTX	Max transmission power	0 (dBW)
ItotdBW	Interference/noise floor	-100 (dBW)
SINRthresh	Minimal threshold SINR for reception	4 (dB)
RNK	Reputation null constant	100
Df	Reputation decay factor	0.99
PBEST	Best supernode reputation reward proportion	0.3

The signal-to-interference-and-noise ratio (SINR) of the supernode is plotted over time in Figure 4. This graph was produced by recording the SINR for each route request sent across an ensemble of uniform random topologies. The findings are provided to the reader in the form of cumulative distribution functions. The nominal SINR that is applied to the packets that are delivered by traditional multihop routing is represented as SINRcutoff = 4dB. The series for route requests 1-10 is meant to depict the initialization state of PRBR as well as the early route discovery that it performed. At this juncture, the median SINR is only marginally higher than the minimal routing, and around thirty percent of the traffic that is delivered by supernodes has a SINR that is lower than four decibels. The steep surge in rapid jump displayed at 4dB in the series for route requests 1-10 reveals that approximately 15% of traffic is supplied by multihop routing. This can be seen by examining the data for route requests 1-10.

The subsequent CDF series reveals that between route requests 90 and 100, nearly 70 percent of the total requests are being fulfilled by the high performance supernodes (achieving SINR of 8dB or above). There are fewer than 25 percent of routes that use the supernodes that have a SINR that is lower than the SINRcutoff. Because there is no sign of a vertical spike at 4 dB, this shows that supernode delivery has completely taken the position of multihop routing. This demonstrates how quickly the algorithm converges towards higher performance supernodes once the initial one hundred route requests have been processed.

The simulation was run for a longer period of time in order to explore the long-term behaviour, specifically to determine whether or not additional performance gains take place over time. The closer together the CDF series get, the more it suggests that as the system converges towards higher performance, subsequent increases are gained more slowly. There is a slight vertical step at 4 dB that occurs between route request numbers 290 and 300, which is an intriguing part of the data. This suggests that the algorithm's investigation has switched to employing multihop routing rather than one of the supernodes with lesser performance. However, given that the vertical step will be eliminated in the subsequent CDF series, this decision about the routing is only a temporary one.

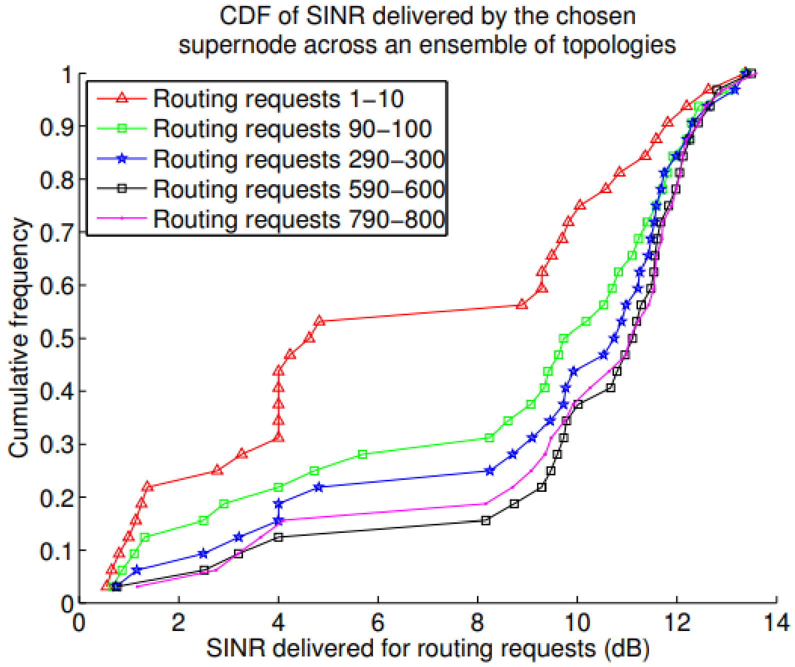

Figure 4: SINR that was simulated for a group of topologies while Sybil nodes were present in the network

Only about 10 percent of transmissions are still being made by low-performing supernodes between route requests 590 and 600. This can be understood, in part, by examining the exploratory nature of the algorithm itself, which is exemplified by the decay that is applied to the reputation levels. The expiration of a reputation generates the pressure to retest supernodes in order to determine whether or not there has been an increase in performance. This constant expiration can, in some circumstances, result in momentary, slight declines in performance. The

CDF series for route 790-800 provides an illustration of this point. In spite of the fact that the distribution has remained the same from the series for 590-600 points higher than the median, the lower quartile has shown a slight decline in performance as a result of these exploratory decisions.

The scatter figure indicates that when there are four Sybils grouped together in one area, the eventual proportion of traffic using each of them is less than thirty percent. This often includes the nodes that are geographically close to that specific supernode, as well as other nodes that are experimentally testing it to determine whether or not there has been a change in its level of performance. According to these findings, PRBR provides a powerful incentive for avoiding Sybils in scenarios in which several Sybils are grouped together to a sufficient degree that they reduce the SINR produced by supernodes.

VI. CONCLUSION

It has been established that the reputation routing approach possesses the power to adapt to certain topologies and the SINR features of such topologies. This enables the strategy to discover with a high probability the locations of the best performing supernodes for relaying. It has been demonstrated that the reputation routing protocol is responsive to the empirical SINR qualities that a given supernode can supply, and that it penalises supernodes that do a bad job of performing. Additionally, it has been demonstrated that the system is resistant to the existence of Sybil nodes, which is demonstrated implicitly by the impact of these nodes on the supernode relaying. This is provided as part of the beam forming, eliminating the need for separate Sybil detection techniques that would otherwise be required.

REFERENCES

1. Dr. E.N. Ganesh. (2022). Study of Self Organizing Wireless Sensor Networks. Journal of Information Technology. 11. 12-17. 10.6084/m9.figshare.20418132.

2. Abdulwahid HM, Mishra A. Deployment Optimization Algorithms in Wireless Sensor Networks for Smart Cities: A Systematic Mapping Study. Sensors (Basel). 2022 Jul 7; 22(14):5094. Doi: 10.3390/s22145094. PMID: 35890774; PMCID: PMC9317050.

3. Sharma, s & Chahar, Vijay. (2022). a Comprehensive Review on Multi-objective Optimization Techniques: Past, Present and Future. Archives of Computational Methods in Engineering. 3. 10.1007/s11831-022-09778-9.

4. Guha, Dipayan & Roy, Provas & Banerjee, Subrata & Purwar, S. (2022). Optimization Techniques. 10.1007/978-981-19-0444-8_3.

5. Joshi, Pallavi & Gavel, Shashank & Raghuvanshi, Ajay. (2022). Developed Optimized Routing Based on Modified LEACH and Cuttlefish Optimization Approach for Energy-Efficient Wireless Sensor Networks. 10.1007/978-981-19-1906-0_3.

6. Cao, Bin & Zhao, Jianwei & GU, Yu & Fan, Shanshan & Yang, Peng. (2019). Security-Aware Industrial Wireless Sensor Network Deployment Optimization. IEEE Transactions on Industrial Informatics. PP. 1-1. 10.1109/TII.2019.2961340.

7. Wang, Shanshan & Chen, Yun. (2021). Optimization of Wireless Sensor Network Architecture with Security System. Journal of Sensors. 2021. 1-11. 10.1155/2021/7886639.

8. Palopoli, Luigi & Passerone, Roberto & Rizano, Tizar. (2011). Scalable Offline Optimization of Industrial Wireless Sensor Networks. Industrial Informatics, IEEE Transactions on. 7. 328 - 339. 10.1109/TII.2011.2123904.

9. Palopoli, Luigi & Passerone, Roberto & Rizano, Tizar. (2011). Scalable Offline Optimization of Industrial Wireless Sensor Networks. Industrial Informatics, IEEE Transactions on. 7. 328 - 339. 10.1109/TII.2011.2123904.

10. Bin Cao, Jianwei Zhao, Zhihan Lv, Xin Liu, Xinyuan Kang and Shan Yang, Deployment Optimization for 3D Industrial Wireless Sensor Networks Based on Particle Swarm Optimizers with Distributed Parallelism, Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2017.08.009

Author’s Declaration

I as an author of the above research paper/article, hereby, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website/amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by meis not correct I shall always be legally responsible. With my whole responsibility legally and formally I have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and the entire content is genuinely mine. If any issue arise related to Plagiarism / Guide Name / Educational Qualification/ Designation/Address of my university/college/institution/ Structure or Formatting/ Resubmission / Submission /Copyright / Patent/ Submission for any higher degree or Job/ Primary Data/Secondary Data Issues, I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the data base due to some technical fault or hacking and thereforethe process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Aadhar/Driving License/Any Identity Proof and Address Proof and Photo) in spite of demand from the publisher then my paper may be rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds any complication or error or anything hidden or implemented otherwise, my paper may be removed from the website or the watermark of remark/actuality may be mentioned on my paper. Even if anything isfound illegal publisher may also take legal action against me.

Vineeta Babu
Dr. Pramod Sharma