electronics

MDPI

Article

Maintaining Effective Node Chain Connectivity in the Network with Transmission Power of Self-Arranged AdHoc Routing in Cluster Scenario

Kiruthiga Devi Murugavel [1,*], Parthasarathy Ramadass [2], Rakesh Kumar Mahendran [3], Arfat Ahmad Khan [4,*], Mohd Anul Haq [5,*], Sultan Alharby [5] and Ahmed Alhussen [6]

[1] Department of Information Technology, Dr. M.G.R. Educational and Research Institute, Chennai 600095, India
[2] Department of Computer Science and Engineering, Vel Tech Rangarjan Dr. Sagunthala R&D Institute of Science and Technology, Chennai 600062, India
[3] Department of Computational Intelligence, School of Computing, SRM Institute of Science and Technology, Chennai 603203, India
[4] College of Computing, Khon Kaen University, Khon Kaen 40000, Thailand
[5] Department of Computer Science, College of Computer and Information Sciences, Majmaah University, Al-Majmaah 11952, Saudi Arabia
[6] Department of Computer Engineering, College of Computer and Information Sciences, Majmaah University, Al-Majmaah 11952, Saudi Arabia
* Correspondence: kiruthiga.it@drmgrdu.ac.in (K.D.M.); arfatkhan@kku.ac.th (A.A.K.); m.anul@mu.edu.sa (M.A.H.)

check for updates

Citation: Devi Murugavel, K.; Ramadass, P.; Mahendran, R.K.; Khan, A.A.; Haq, M.A.; Alharby, S.; Alhussen, A. Maintaining Effective Node Chain Connectivity in the Network with Transmission Power of Self-Arranged AdHoc Routing in Cluster Scenario. *Electronics* **2022**, *11*, 2455. https://doi.org/10.3390/electronics11152455

Academic Editor: Cheng-Chi Lee

Received: 19 June 2022
Accepted: 18 July 2022
Published: 6 August 2022

Abstract: Mobile Ad hoc Networks (MANETs) are intended to work without a fixed framework and provide dependable interchanges to ground vehicles, boats, airplanes, or people and structure a self-mending process that will empower persistent correspondences in any event, when at least one of its nodes are debilitated or briefly expelled from the system. Notwithstanding, MANETs demonstrate themselves to be progressively harder to create for enormous systems with hundreds or thousands more nodes than initially envisioned. In our proposed technique, the node switches its communication mode depending on the connectivity of the adjacent nodes. The transmission power of each node will be calculated with the help of two major scenarios i.e., tree scenario and zone scenario. The autonomous clustering of the nodes among the tree and the zone scenario will be channelized by a comparison of the transmission power (residual energy) among the nodes. The inter and the intra communication of the node is also discussed in the paper. The result will be carried out by the simulation work in various perspectives, such as checking the percentage level of malicious nodes, traffic density, transmission power, and the longevity of nodes.

Keywords: ad hoc networks; cluster; self-mending; traffic density; transmission power

1. Introduction

MANET is a powerful self-composed mobile network with the absence of foundation and focal help. A mobile ad hoc network allows nodes to speak directly with one another, while nodes not in direct correspondence extend and utilize halfway nodes as switches to communicate. Nodes rely on different nodes to send data because of dynamic topologies, open systems, and energy constraints that make the MANET vulnerable to many attacks. Many secure routing protocols have been planned so far, such as SAODV, SEAD, ARIAN, and so forth, which practice numerous verification plots, including hash-chains and computerized mark.

This safe routing protocol manages assaults made by malicious nodes yet does not manage the proximity of these pernicious nodes. To keep up the security and honesty of information while sending messages, we need to start to finish reliable correspondence. Due to the open medium and characteristic trust between nodes, it is exceptionally difficult to differentiate between ordinary and malicious nodes. As of late, many trust-based arrangements have been recommended that dodge the noxious nodes from correspondence by allotting some measurement to the node that chooses the trust level of those specific nodes. These protocols, nevertheless, face issues, such as face ID, distorted trust, and age-old distrust esteems. Likewise, either the source or goal node profoundly takes part in verifying trust levels of middle-of-the-road nodes in a similarly [1–4].

It is an assortment of autonomous nodes associated with methods for short-run remote connections, shaping a dynamic multi-jump arrangement in a decentralized manner [5]. With the system topology evolving progressively and the absence of a pre-built foundation, such systems require appropriate self-sorting of calculations to oversee themselves successfully. Task-based self-organizing critical significance right now depends on which few nodes are consecutively chosen as pioneers, relying upon their presentation-related qualities [6]. Such pioneer-based calculations have a wide assortment of utilizations, among which are routing coordination [7] and suitable interruption location [8]. For instance, on account of helpful interruption recognition, one node is chosen as a pioneer so as to fill in as the interruption location framework (IDS) for all system individuals, rather than every node running its own IDS. In addition to the benefits of pioneer-based self-sorting calculations, such calculations ought to consider the nearness of getting out-of-hand nodes in the system. Further, such systems can be powerless because of the nonappearance of an accreditation authority and a unified administration unit [9–11].

2. Literature Survey

R. Akbani et al. [12] proposed security issues and discussed a convincing solution. In Mobile Ad hoc Networks, the nodes cannot be connected between two points because they are powerless. Y. Hu et al. [13] depicted the assortment of nodes in the remote systems.

D. Johnson et al. [14] proposed the maximum number of nodes in the network. Basically, all the nodes will communicate and connect each other one to one in a heterogeneous environment. Each node will manage itself by preventing malicious nodes and performing the recovery process of the network in a successful manner. This paper focuses on a novel approach for the detection method by preventing and detecting the system in a secure way.

D. Maltz et al. [15] deals with the centralization and decentralization of the nodes and the networks. It deals with the routing protocol of MANET, which has the ability to connect with nodes. The protocol in the network has the ability to adapt to environmental conditions.

N. Kang et al. [16] proposed a sequential probability of nodes that helps to identify the malicious nodes among the network. Howard [17] approached the greedy methodology to approach the nodes and deployed the mobile sensor network. The deployment methodology was discussed in detail. A node can optimize the optimal location by using data with a history of nodes.

Sunil Kumar [18] observed that when a network link fails, the shortest path estimating routing scheme creates extra energy and delay for data transfer. This research presented an efficient innovative hello-based path recovery (HBPR) routing protocol for the shortest path calculation to address this difficulty. If a link fails in the network layer during transmission, the HBPR system creates an alternate path, reducing delay time and energy usage. The unique simplified honey pot optimization (SHPO) is then developed to predict the network's hazardous nodes.

Zhijie Han, Weiqiang Xue, Xiaoyu Du [19] found that to avoid the local optimal solution, the elbow approach is merged with the silhouette coefficient before clustering, and similarity inside the cluster and dissimilarity across clusters are incorporated. Finally, the nodes are clustered using the clustering algorithm. The ring model is used to optimize the cluster head selection process by taking into account the residual energy of nodes as well as the distance between nodes and the cluster center. It effectively extends the lifetime of mobile ad hoc networks, increases network performance, and lowers packet loss rates.

Parthasarathy Ramadass et al. [20] showed the different routing protocols and MANET security issues. It also discusses the OSI model and the link between security systems, the expanded and precise approach to the various protocol's aids in the development of a progressive MANET security concept. Various challenges and solutions aid in the discovery of threats' flaws and it clearly describes the MANET efficiency study. The simulation analysis aids in the understanding of protocol comparisons.

3. Proposed Technique

The proposed SAARICS method enlightens the self-arranged ad hoc routing in cluster scenarios. The self-organized autonomous clustering helps to organize the nodes themselves with the transmission power, i.e., energy. The residual energy of each node helps to connect with the neighbouring node to form a cluster-based scenario to broadcast the information from the initial point to the destination point. Figure 1 represents the flowchart of the self-organizing chain.

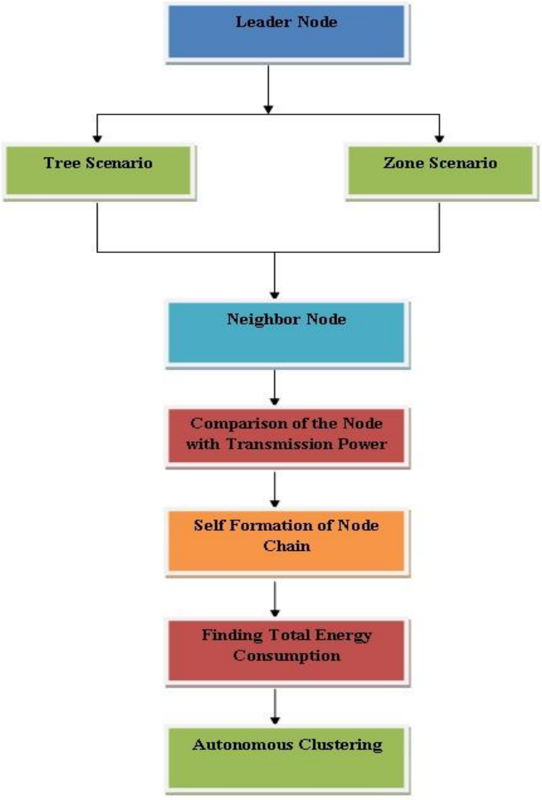
Leader Node
Tree Scenario
Zone Scenario
Neighbor Node
Comparison of the Node with Transmission Power
Self Formation of Node Chain
Finding Total Energy Consumption
Autonomous Clustering

Figure 1. Flowchart of the Self-Organizing Chain.

3.1. Autonomous Clustering

Hierarchical clustering will lead to autonomous clustering. Autonomous clustering will be conducted in two possible ways, internal clustering (Intra Cluster) and external clustering (Inter Cluster). The intra-cluster scenario will work with the tree mode of transaction. It uses tree scenarios along with CH activity. The inter cluster works among the different cloud leads to route searching and route holding. It uses standard AODV protocol to broadcast the information from source to destination.

Without the support of the CH, the node in both scenarios will not operate. The CH node kicks the next neighbor node to connect with the communication flow. The residual energy of each node plays a vital role to connect with the next node in the scenario.

In the proposed technique, the self-organizing of nodes in the cluster was deeply discussed. Self-organizing among the nodes of the independent cluster forms a temporary backbone node and an energy consumption process with the help of the Initialize node, named the kick node or leader node. The kick node is the first and the starting node in the cluster. While at the formation of the cluster, the first node will be the leader node and search for the other nearest node to connect to. Self-organizing will happen in two major ways: (1) tree-based scenario and (2) zone-based scenario. The tree-based scenario helps to connect the individual node to form a chain. The information from the source to the destination will be channelized through the tree-based structure. It mainly helps to form the initial work of the self-organizing scenario. However, in the zone-based scenario, the interconnected nodes will be formed in a bunch, which helps to segment similar energy nodes among the clusters.

In SAARICS, controlling of the node density plays a major role to avoid unnecessary issues in the cluster scenario. The node will be controlled in the MANET with the help of transmission power. SAARICS predominantly works as a high-assurance network. Moreover, the proposed SAARICS avoids packet loss and energy consumption by controlling and reducing the density of nodes because each node in the cluster avails the transmission power to transmit the data from place to place. Even though the possibility of the nodes will be in two scenarios, the intra-cluster scenario plays a vital role. By merging, splitting, and holding the nodes, the transmission power of the nodes will be managed and controlled.

The self-clustering technique, or the algorithm, is a distributed algorithm that executes each node and the cluster node relationship autonomously. The failure of the individual node never affects the other node in the network. As it is a self-organized cluster of nodes, automatically, the failure node will be diminished or dropped down by the leader of the cluster CH [20]. That helps to continue the network communication without any disturbances. The pairing of the basic two nodes is shown clearly in Figure 2.

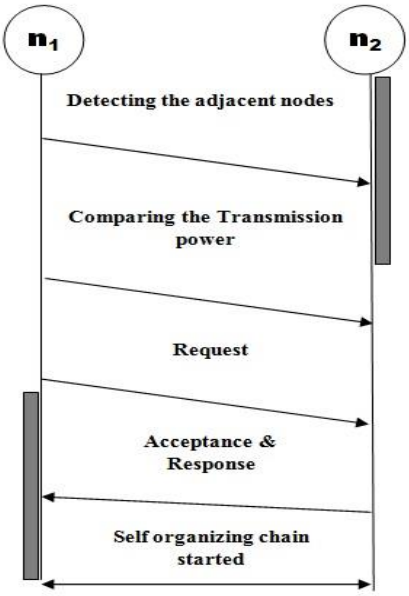
n₁
n₂
Detecting the adjacent nodes
Comparing the Transmission power
Request
Acceptance & Response
Self organizing chain started

Figure 2. Pairing of Two Nodes.

Initially, node n_1 starts to identify the adjacent node, considering the adjacent node as n. After identifying the adjacent node, node n_1 will compare the transmission power of the adjacent node. Upon comparing the transmission power, node n_1 forwards the node chain request to node n_2 and receives a response from node n_2 to form a self-organizing node chain connection.

Since the cluster leader or head is the dominant power producer in the cluster group, the complete transmission energy of the cluster makes a beeline to be limited to diminish the impedance created by the groups. The total energy consumption of each node will be calculated to obtain the overall frequency range of the cluster formation. The individual *i*th node transmission power is more important than the summation of all nodes in the cluster:

$$\sum_{i=1}^{H} Po_{ik} \tag{1}$$

where Po_{ik} is the transmission power needed for the *i*th cluster head to reach the next *k*th node. *K* is the number of nodes controlled by *i*th cluster head:

$$\sum_{S=1}^{K_i} D_{ik}^{n} F \tag{2}$$

D_{ik} is the distance between the *i*th cluster head and the *k*th node in the cluster. *F* is the constant that is related to the signal frequency. *n* is the transmission propagation path loss factor. The interference factor of a cluster to be the product of a cluster selection head's interference factors, L_i and K_i, is the maximum number of nodes in the cluster technique to minimize the summation of total transmission power factor of all clusters subject to the following constraints.

$$min \sum_{i=1}^{j} K_i L_i = min \sum_{i=1}^{j} \sum_{S=1}^{K_i} D_{ik}^{n} \tag{3}$$

All nodes within the cluster range or adjacent to CH are considered as potential nodes in the cluster. $n_i \leq n_v$ for i = 1 ... H, where H is the total number of nodes in the cluster in the network. The first constraints ensure that the first node n_i never cancels the chain of process when the value of n_i is less than n_v. Even though the n_v is greater than the first node n_i, the node chain will not be terminated. However, as per our proposed concern, the leader node position will be changed. The maximum transmission power node will act as a CH in the flow of the node chain.

3.2. Finding Positions of the Nodes

In our proposed technique, the node switches its communication method depending upon the connectivity of the adjacent node. An autonomous self-positioning technique using SAARICS to aid nodes in improved locations was used. Each node runs independently with the help of a local sensing area to make a decision on where to move. For node n_i, the positions that are closer to it than to any of its neighbors belong to the SAARICS node S_i of n_i. We formally defined the node n_i as

$$S_i \ = \{\omega \, \epsilon \, \beta \ : di(n_i, \ \omega \ ) < di(n_j, \ \omega \ ) \ , \ \forall \ n_j \in I\{n \ _i \ \} \tag{4}$$

where β represents the set of all positions in *Ls*, *i*, *I* is a set of all nodes and $di(n_i)$, and ω stands for Euclidean distance between nodes n_i where x_i, y_i and locations x_w, $y_w \in \beta$.

The interval between the node to node is defined as time *j* and time *k*. At that time, the cluster will never divide or merge during the process. *Dis*(*h*) is defined as the range of *h* nodes among the inter cluster and the intra cluster. *Disintra*(*h*) is the distance between the nodes in the intra cluster and the $Dis_{inter}(h)$ is classified into the node distance in the inter cluster between the *K* and G.

$$Dis(h) = \alpha 1 \times Dis_{intra(h)} + \ \alpha 2 \ \times Dis_{inter(h)} \tag{5}$$

where $\alpha 1$ and $\alpha 2$ are the weights of the $Dis_{intra}(h)$ and $Dis_{inter}(h)$, respectively. The ry node (the intermediate node present in every cluster) can calculate the distance *Dis*(*h*) and delivers the node information through the spanning tree. Then, the cluster head calculates *Dis*(*h*) divided by the transmission power (K-G) for all nodes in the cluster. The estimated cluster mobility range will be mentioned as Dis_{maxs}.

In Figure 3, the nodes are moved inside the cluster to connect with the flow of nodes from source to destination. The inter-cluster connection among the nodes is shown with 10 nodes, which are represented with three clusters, namely C1, C2, and C3. C1 consists of nodes 1, 2, 3, and 4. Node 5, 6, and 7 in C2 and cluster C3 contain nodes 8, 9, and 10, respectively. In Figure 4, the border node or the neighbour nodes to the other cluster nodes were moved to the adjacent cluster. Nodes 5, 3, 7, and 9 were moved from one cluster to another cluster, as shown in Figure 4. Node 3 switches its position from C1 to C2 without connections. It moves independently like node 6 and 7. Instead, node 5 moves to the first cluster and links with the node chain of 1, 2, and 4. In the same way, the nodes 6, 7, and 9 move inside the cluster. Figure 4 show the inter-cluster connection among the clusters. The maximum number of nodes crosses cluster to cluster and connects with the node chain in the individual cluster.

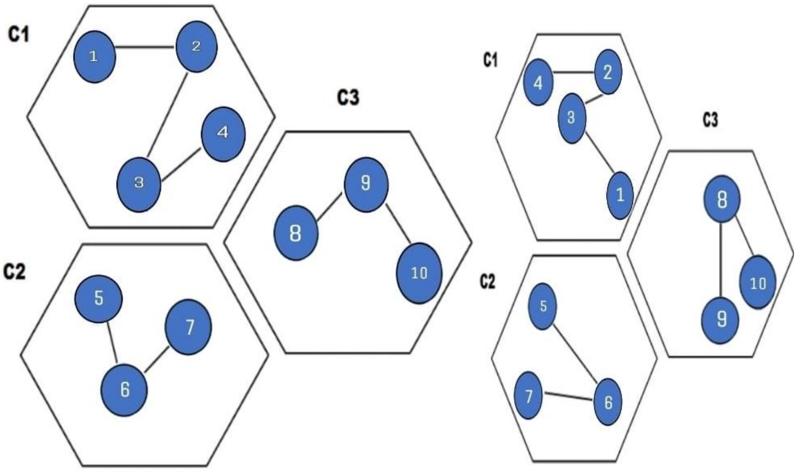

Figure 3. Intra-Cluster Connection Among Nodes.

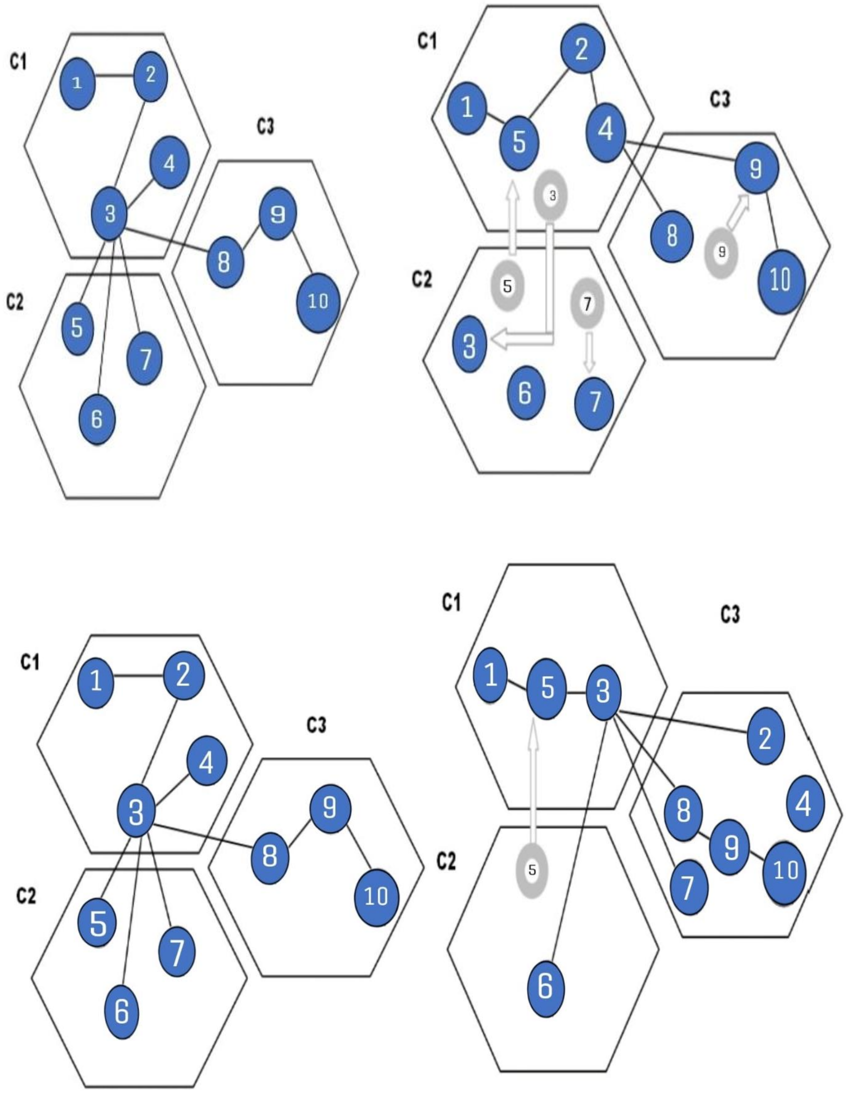

Figure 4. Inter-Cluster Model with Movement of Nodes.

In Figure 5, the single and multiple cluster scenarios are explained clearly. In the single cluster scenario, the nodes can be connected within a range and be automatically managed by themselves. In some cases, the nodes can be moved to the nearby clusters to connect the chain of the high-residual-energy nodes. Therefore, it has to transmit the information from one cluster to another cluster. Various possibilities for the node movement in the cluster scenario are also revealed. The nodes from the different cluster regions were connected with various aspects to transmit the information from one point to another. Sometimes, the source will be in one cluster and destination will be in another cluster region.

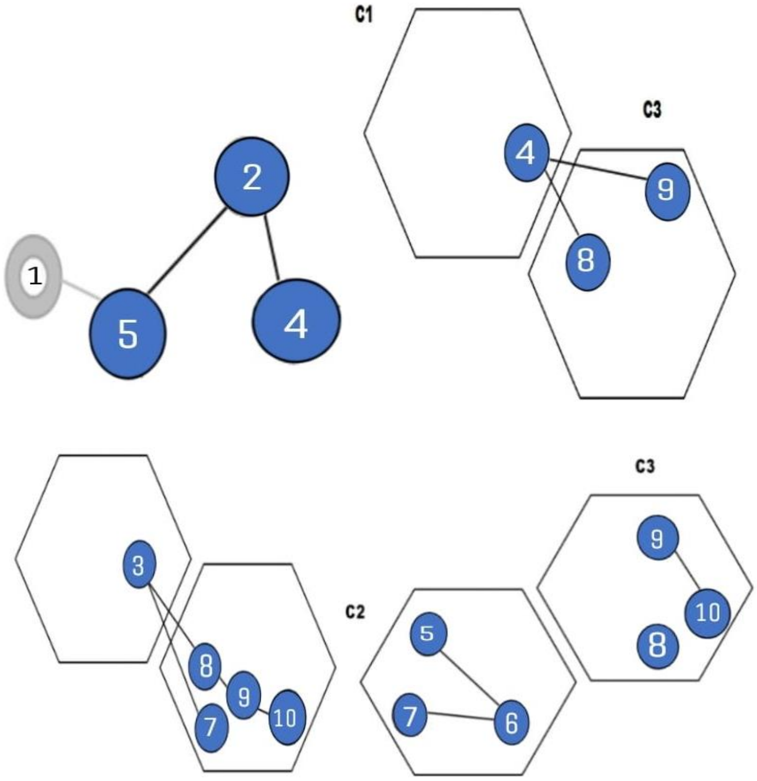

Figure 5. Tree Scenario Cluster—Single and Multiple Clusters. Inter- and Intra-Cluster Tree Scenario.

4. Simulation Analysis

The simulation analysis was analyzed in a network simulator 3 (NS3) simulator tool for finding the below parameter of the MANET nodes has shown in Table 1. The proposed SAARICS was compared with DMR, SAODV, and SRP. The parameters, such as transmission power range, longevity of node, malicious node, and traffic density of the nodes, were analyzed to strengthen the proposed methodology. As such, 100 to 500 nodes were deployed in the MANET area to find the parameter values in a proper manner.

Table 1. SAARICS Simulation—Parameter Table.

Simulator	NS3 Simulator
Area	1000 × 1000 m
Network Size	100 to 500 nodes
Mobility Model	Random Way Point
Traffic Type	FTP
Simulation Time	600 s
Standard	IEEE 802.11 G
Routing protocol	SAODV, SZRP, DMR

4.1. Transmission Power Range

In Figure 6, the transmission power of each node will be analyzed with the other successive techniques. When compared with the other techniques, the SAARICS performs better than other methodologies. The SAARICS level stands high, so the transmission energy among the nodes will be adequate enough to broadcast the information from source to destination.

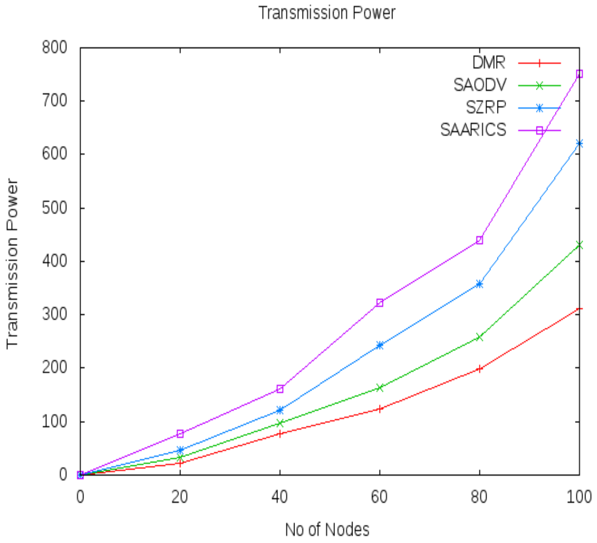

Figure 6. Transmission Power Range vs. Number of Nodes.

4.2. Longevity of Nodes

Longevity of Node analysis clearly describes the longevity of each node in the proposed technique. Sometimes, the node will diminish in the chain of processes for various reasons. Poor communication among nodes leads to improper connectivity. Figure 7 will be compared with a few other techniques to reveal the betterment of the SAARICS.

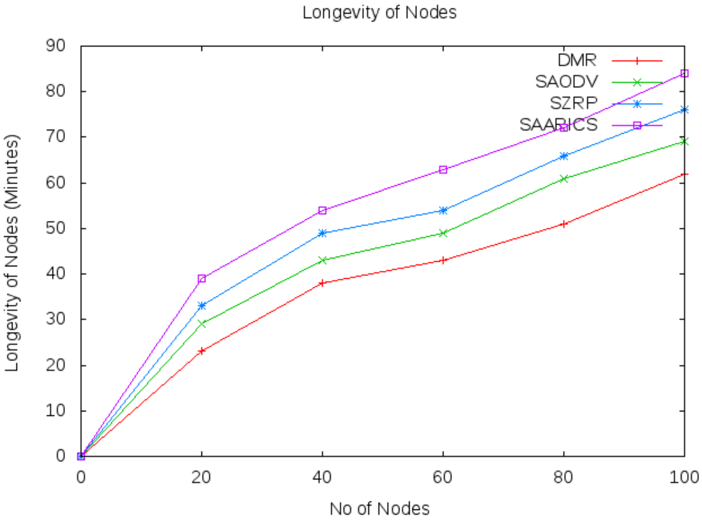

Figure 7. Longevity of Nodes.

4.3. Ratio of Malicious Nodes

The rate of malicious nodes is analyzed to avoid poor communication. The malicious nodes disturb the network flow in various ways. That completely collapsed the cluster chain and presented a poor result. While finding the malicious nodes, the CH and the TH try to repair the node or it denies the malicious node connection, to get a better formation of the network chain. In Figure 8, SAARICS techniques have a minimum number of malicious nodes when compared with all other existing routing protocols. Therefore, the cluster chain will be smart enough to transmit the information from the source to the end point.

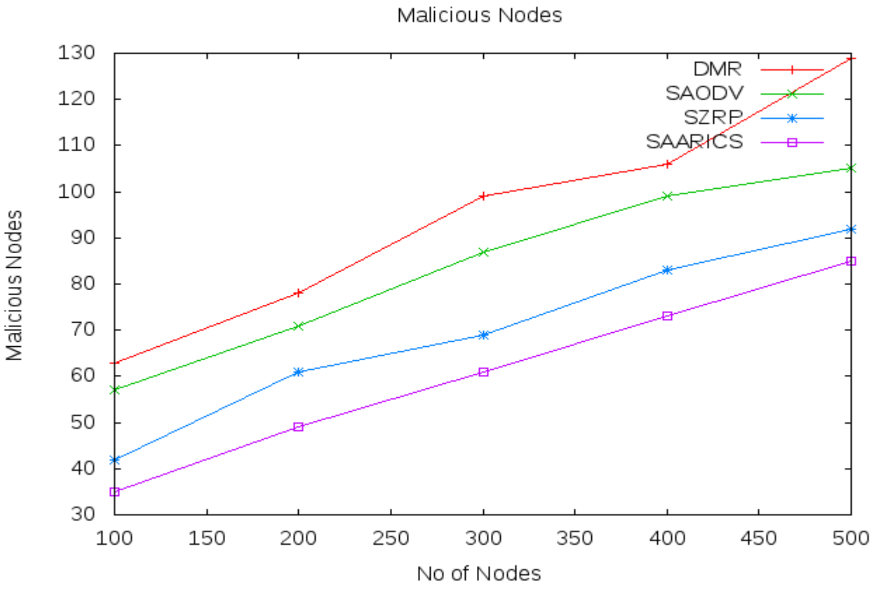

Figure 8. Ratio of Malicious Nodes.

4.4. Traffic Density Analysis

The high traffic density collapses the communication flow. Moreover, the maximum number of nodes in a single or multiple clusters leads to a lot of issues among the node chain. In Figure 9, the traffic density is analyzed. The comparison table helps to observe the exact values of the node's density.

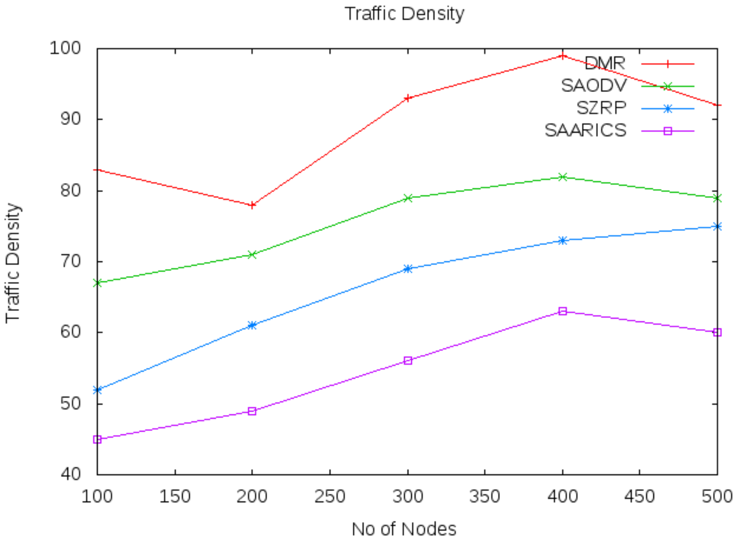

Figure 9. Traffic Density of Nodes.

5. Conclusions

The proposed technique, SAARICS, is evaluated and the performance is calculated in terms of parameters, such as transmission power range, longevity of nodes, ratio of malicious nodes, and traffic density. The transmission power of each node will be highlighted to strengthen the node chain. The transmission energy helps to connect the node chain and communicates the information from source to destination. The tree and the zone scenario clusters help to connect the inter and the intra nodes in a proper logic. The simulation results clearly show the transmission power range, longevity of each node, traffic density, and the malicious node level with a clear definition. The inter and the intra connections among the cluster region face various challenges with the nodes. The node's longevity helps to sustain the node chain for a long time and to communicate with the alternate node without any disturbances, while for disturbances or breaks of the node chain, the energy level of each node helps to connect with the neighbouring node rapidly. Thus, the SAARICS proposed a new methodology to flow the node chain in a successive manner.

Author Contributions: Conceptualization, K.D.M., P.R., R.K.M. and A.A.K.; methodology, R.K.M., A.A.K., M.A.H. and S.A.; software, K.D.M., P.R., A.A.K. and M.A.H.; validation, P.R., S.A. and A.A.; formal analysis, K.D.M., P.R. and A.A.K.; investigation, R.K.M., S.A. and A.A.; resources, A.A.K. and M.A.H.; data curation, P.R., R.K.M., A.A.K. and M.A.H.; writing—original draft preparation, K.D.M., P.R., A.A.K. and M.A.H.; writing—review and editing, R.K.M., S.A. and A.A.; visualization, A.A.K. and M.A.H.; supervision, R.K.M., S.A. and A.A.; project administration, R.K.M. and A.A.K.; funding acquisition, M.A.H., S.A. and A.A. All authors have read and agreed to the published version of the manuscript.

Funding: Sultan Alharby would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project No. R-2022-233. Moreover, this research was supported by College of Computing, Khon Kaen University, Thailand.

Acknowledgments: Sultan Alharby would like to thank Deanship of Scientific Research at Majmaah University for supporting this work under Project No. R-2022-233. Also, we would like to thank College of Computing, Khon Kaen University, Thailand.

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the publication of this paper.

References

1. Gupta, P.; Kumar, P.R. The capacity of wireless networks. *IEEE Trans. Inf. Theory* **2000**, *46*, 388–404. [CrossRef]
2. U.S. Department of Defense, Office of Operational Test and Evaluation (DOT&E). *Joint Tactical Radio System (JTRS) Ground Mobile Radio (GMR)*. 2010. Available online: https://www.dote.osd.mil/ (accessed on 18 June 2022).
3. Gilmore, J.M. Operational Test and Evaluation Office of the Secretary of Defense. In *Testimony before House Armed Services Subcommittee On Air And Land Forces*. 2010. Available online: https://www.acq.osd.mil/fo/docs/HASC (accessed on 24 May 2019).
4. Wolfgang, K.; Mauve, M. A survey on real-world implementations of mobile ad-hoc networks. *Ad. Hoc. Netw.* **2007**, *5*, 324–339.
5. Wei, Q.; Bai, K.; Zhou, L.; Hu, Z.; Jin, Y.; Li, J. A Cluster-Based Energy Optimization Algorithm in Wireless Sensor Networks with Mobile Sink. *Sensors* **2021**, *21*, 2523. [CrossRef] [PubMed]
6. Hubaux, J.P.; Gross, T.; le Boudec, J.Y.; Vetterli, M. Toward self-organized mobile ad hoc networks: The Terminodes Project. *IEEE Commun. Mag.* **2001**, *39*, 118–124. [CrossRef]
7. Razzaque, M.A.; Dobson, S.; Nixon, P. Enhancement of Self- organization in Wireless Networking through a Cross-layer Approach. In *International Conference on Ad Hoc Networks*; Springer: Berlin/Heidelberg, Germany, 2009.
8. Basagni, S. Distributed clustering for ad hoc networks. In Proceedings of the Fourth International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN'99), Perth/Fremantle, WA, Australia, 23–25 June 1999.
9. Mohammed, N.; Otrok, H.; Wang, L.; Debbabi, M.; Bhattachary, P. Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET. *IEEE Trans. Dependable Secur. Comput.* **2011**, *8*, 89–103. [CrossRef]
10. Mishra, A.; Nadkarni, K.; Patcha, A. Intrusion detection in wireless ad hoc networks. *IEEE Wirel. Commun.* **2004**, *11*, 48–60. [CrossRef]
11. Otrok, H.; Mohammed, N.; Wang, L.; Debbabi, M.; Bhattacharya, P. An Efficient and Truthful Leader IDS Election Mechanism for MANET. In Proceedings of the Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), White Plains, NY, USA, 8–10 October 2007.
12. Akbani, R.; Korkmaz, T.; Raju, G.V.S. Mobile Ad hoc Network Security. In *Lecture Notes in Electrical Engineering*; Springer: New York, NY, USA, 2012; Volume 127, pp. 659–666.
13. Hu, Y.; Perrig, A.; Johnson, D. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wirel. Netw.* **2002**, *11*, 21–38. [CrossRef]
14. Hu, Y.; Johnson, D.; Perrig, A. SEAD: Secure efficient distance vector routing for mobile wireless. *Ad. Hoc. Netw.* **2003**, *1*, 175–192. [CrossRef]
15. Johnson, D.; Maltz, D. Dynamic Source Routing in ad hoc wireless Networks. In *Mobile Computing*; Springer: Boston, MA, USA, 1996; Chapter 5; pp. 153–181.

16. Kang, N.; Shakshuki, E.; Sheltami, T. Detecting misbehaving nodes in MANETs. In Proceedings of the 12th International Conference on Information Integration and Web-Based Applications & Services, Bangkok, Thailand, 8 November 2010; pp. 216–222.
17. Howard, A.; Mataric, J.; Sukhatme, G. Mobile sensor network deployment using potential fields: A distributed, scalable solution to the area coverage problem. In *Distributed Autonomous Robotic Systems 5*; Springer: Tokyo, Japan, 2002; pp. 299–308.
18. Kumar, S. Prediction of Node and Link Failures in Mobile Ad Hoc Network Using Hello Based Path Recovery Routing Protocol. *Wirel. Pers. Commun.* **2020**, *115*, 725–744. [CrossRef]
19. Han, Z.; Xue, W.; Du, X. Research on Clustering Protocol in Mobile Ad Hoc Networks. In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, Melbourne, Australia, 14–17 December 2021; pp. 471–475.
20. Parthasarathy, R. A Collective and Comparative Study of Various Routing Protocols and the Threats in MANET. *Int. J. Knowl. Syst. Sci. (IJKSS)* **2021**, *12*, 11.