International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 18, Issue 2 (Mar.-Apr. 2022), PP. 07-13

An Efficient Neighbor Discovery Scheme for Mobile using Wireless Sensor Networks

Dr.Vijay B T [1],Prashanth T N [2]
[1]*Department of Electronics and communication Engineering, asst Professor*
[2]*Department of Electronics and Communication Engineering(M.Tech student)*
The National Institute of Engineering, Mysore, Karnataka, INDIA
Corresponding Author: vijaybt@*nie.ac.in*

ABSTRACT
Wireless Sensor network is used nowadays almost everywhere. A sensor node, in a sensor network that is capable of performing some processing, gathering sensory information and communicating with other connected nodes in the network. A Sensor is a device that responds and detects some type of input from both the physical or environmental conditions, such as pressure, heat, light, etc. The output of the sensor is generally an electrical signal that is transmitted to a controller for further processing. Wireless Sensor Network (WSN) is a self-organizing network which formed with huge sensors which are located in an application specific environment to monitor the physical pheromone like temperature, fire, and pressure. Mostly sensors are equipped with battery power through which they can perform sufficient operations and communication among neighboring nodes. Wireless Sensor Networks suffers from energy exhaustion problem. A large share of energy in wireless sensor network is consumed in routing the data and control packets as compare to other operations like sensing and sleep state. There are various protocols that use optimal path for data routing to conserve energy. An optimal path for routing can be obtained by using Swarm intelligence (SI) techniques. Consequently, in the last period, various routing protocols for sensor networks have been established bestowing to the ideologies of swarm intelligence. Swarm intelligence is the cooperative behavior of distributed, self-established systems, simulated or natural.

KEYWORDS: *Sensor node, Wireless Sensor Network, Controller, Particle Swarm Optimization, clustering, power consumption.*

Date of Submission: 11-04-2022 Date of Acceptance: 27-04-2022

I. INTRODUCTION

A wireless sensor network (WSN) is composed of a collection of sensor hubs that work together to accomplish a task (for example, environmental factors management, target follow-up, and so on), and then transmit the gathered data to a base station or sink hub through a remote communication. WSN may be viewed as a group of cooperating hubs with detecting, reasoning, and distant correspondence capabilities. The sensor hubs collect as well as transfer data to a remote base station, from which the end-client may obtain the necessary information. The sensed data is also collected and aggregated within in the organization at sink hubs, which may be sensors or other hubs lucky enough to be in potential just as assets. The data is eventually delivered to the end-clients via sinks or a higher-request hub, the base station, on a particular circumstance basis. Wireless sensor networks are used in a wide range of applications, including common, medical, and environmental care, as well as the military. Target follow-up in combat, territorial control, common work management, environmental aspects management, and infrastructure maintenance are only few of the applications. As a result of a large number of sample hubs working under difficult circumstances, certain malicious hubs may infiltrate the organization.

In the sensor networks different sensors convey their data towards a global observing data collecting node usually known as a sink that accomplishes complete data aggregation and analysis. Nodes can also transmit data to the intermediate relay nodes that can independently or jointly manage the data before transmitting it to the global sink or towards a global sink, and perform incomplete data aggregation on the route. This is known as in-network data aggregation that is used for energy optimization WSN security has become a serious problem that has drawn the attention of various studies. Denial of service (DoS) attacks, Sybil attacks, Black hole attacks, wormhole attacks, selective forwarding attacks, and sinkhole attacks are some of the attacks that exploit WSN vulnerabilities. Because of the limited resources on the sensor nodes, most routing protocols in WSNs are not built with security in mind. As a result, they may be exposed to a variety of assaults. Sinkhole attacks against WSNs have the potential to degrade the network's efficacy by luring neighbouring nodes with

misleading information and allowing them to launch more assaults. Sensors have short communication span and these form an infrastructure less network across a common wireless channel. Both data and control packets are directed through single hop or through multi-hop. Sensors communicate with each other in the network so as to complete distinctive activities. During communication and other activities, sensors consume a lot of energy.

Motivation

Clustering is one of the most essential jobs in a wireless sensor network (WSN), in which any one of the nodes from a group of nodes is chosen to be a cluster head, and the cluster head is responsible for the cluster's overall operation as well as interfacing with the other nodes in the cluster. Malicious node identification is also critical in wireless sensor networks (WSNs), since it ensures that a malicious node never becomes the cluster head. Furthermore, as the number of malicious nodes grows, so does the chance of becoming a malicious node as cluster head. A Particle swarm optimization harmful node detection system was used to detect malicious nodes as well as to choose a high-potential node for cluster head.

II. RELATED WORK

By using the Swarm Intelligence (SI) optimization method, this paper proposes and implements a detection strategy for sinkhole attacks. In order to improve the detection accuracy of sinkhole attacks, the suggested method combines a weight estimation technique with an Ant Colony (AC) optimization algorithm. The suggested work [1] was written in MATLAB, and comprehensive simulations were run to assess its performance in terms of accuracy rate, detection time, convergence speed, packet overhead, and energy usage. The findings demonstrate that our suggested technique is effective and reliable at detecting sinkhole attacks, with a high rate of accuracy rate.To identify and eliminate malicious nodes, a cluster-based malicious node detection approach is suggested in this paper. The cluster key is given to each node in the cluster by the cluster head, and this key is used for transaction data between the cluster head and the node. For every data transaction from a node, the cluster head verifies this key and compares it to their cluster table. If the match is valid, it will identify that this node is a member of this cluster; otherwise, it will be classified as a malicious node. This [2] study also addresses measuring the gain of each link in the network to identify link failure owing to the existence of a malicious node.

This [3]study significantly presents a malicious node detection model based on a hybrid clustering network for WSNs (ESMCH) that is built on a trusted mobile node that is both efficient and safe. WSNs are still vulnerable to assaults such as the Man-in-the-Middle Attack and the Black Hole Attack, but we may mitigate these risks by employing the ESMCH model. Finally, simulation results show that the proposed model may extend the lifetime of a network and create an efficient and safe clustering network.

In [11] authors used average residual battery level of the entire network and it was calculated by adding two fields to the RREQ packet header of a on-demand routing algorithm i) average residual battery energy of the nodes on the path ii) number of hops that the RREQ packet has passed through.According to their equation re-transmission time is proportional to residual battery energy. Those nodes having more battery energy than the average energy will be selected because its re-transmission time will be less. Small hop count is selected at the stage when most of the nodes have same re-transmission time.

Individual battery power of a node is considered as a metric to prolong the network lifetime in[12]. Authors used an optimization function which considers nature of the packet, size of the packet and distance between the nodes, number of hops and transmission time are also considered for optimization.

In [13] initial population for Genetic Algorithm has been computed from the multicast group which has a set of paths from source to destination and the calculated lifetime of each path. Lifetime of the path is used as a fitness function. Fitness function will select the highest chromosomes which is having highest lifetime. Cross over and mutation operators are used to enhance the selection.

In [14] authors improved AODV protocol by implementing a balanced energy consumption idea into route discovery process. RREQ message will be forwarded when the nodes have sufficient amount of energy to transmit the message otherwise message will be dropped. This condition will be checked with threshold value which is dynamically changing. It allows a node with over used battery to refuse to route the traffic in order to prolong the network life.

In [15] Authors had modified the route table of AODV adding power factor field. Only active nodes can take part in rout selection and remaining nodes can be idle. The lifetime of a node is calculated and transmitted along with Hello packets.

In [16] authors considered the individual battery power of the node and number of hops, as the large number of hops will help in reducing the range of the transmission power. Route discovery has been done in the same way as being done in on-demand routing algorithms. After packet has been reached to the destination, destination will wait for time δt and collects all the packets. After time δt it calls the optimization function to

select the path and send RREP. Optimization function uses the individual node's battery energy; if node is having low energy level then optimization function will not use that node.

Maximum of the SI inspired routing protocols that are developed for sensor networks are inspired by activities perceived in ant and, bee colonies. Additionally, the searching patterns of the insect colonies have assisted a chief source of motivation to design a variety of new routing techniques. Hence, the cooperative searching progression contains dispersing exploration, detection, establishing, and practice of optimized routing paths in lively atmospheres. This procedure is much similar to the route establishing process by sensor nodes in the sensor networks. Here, sensor nodes collectively establish multi-hop routes towards the sink node. The sensors exchange the control packets, establish routes and then select an optimal path towards the sink for data transmission.

WSN is used in many applications. In these applications, nodes may be of heterogeneous or homogeneous or it may be mobile nodes, number of nodes deployed may be varied etc. In order to meet these criteria, the following important design issues of the sensor network have to be considered.

Node deployment: Node placement in WSNs is application-dependent and can be whichever manual or randomized. In manual placement, the sensors are manually allocated and data is routed across predetermined paths.

Fault tolerance: Some sensor nodes could block due to lack of domination, physical damage, or environmental interference. Individual nodes are liable to unexpected failure with a much higher probability when compared with other type of network.

Scalability: Sensor network is made up hundreds or thousands of nodes. The designed Protocol should be able to work to such high degree of nodes and take advantage of such high density of networks. So the routing protocol should not limit with the fixed nodes.

Coverage: In WSNs, every single sensor node obtains a precise think of the environment. A given sensors think of the nature is manipulated in both scope and accuracy; it can only cover a manipulated physical distance of the environment.

III. PROPOSED SYSTEM ARCHITECTURE AND WORKING

In the proposed framework reliant upon trust feature malignant centre point finding computation is used. The estimation for trust-based harmful centre acknowledgment is shown. All perceived threatening centre points are then cleared out for instance while picking the pack head they will be not picked. Then, at that point discover the possibilities of every hub In this stage the ability of each centre in the association is found using PSO. The ability of each centre point in the association is found using PSO with cushy reasoning by using three information limits, for instance remaining energy of a centre, upheld consideration, and association quality.

The PSO algorithm is an evolutionary computing technique, modeled after the social behavior of a flock of birds. In the context of PSO, a swarm refers to a number of potential solutions to the optimization problem, where each potential solution is referred to as a particle. The aim of the Particle Swarm Optimization is to find the particle position that results in the best evaluation of a given fitness function. In the initialization process of Particle Swarm Optimization, each particle is given initial parameters randomly and is „flown" through the multi-dimensional search space. The during each generation, each particle uses the information about its previous best individual position and global best position to maximize the probability of moving towards a better solution space that will result in a better fitness.

IV. RESULTS

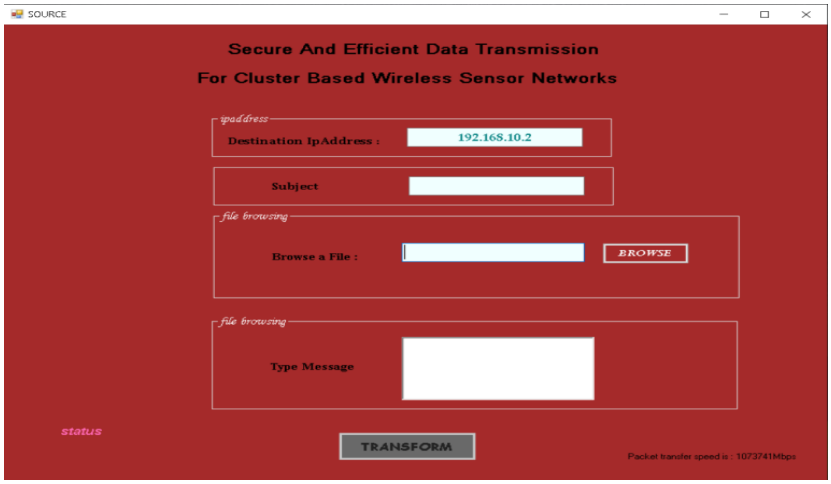

Figure 1: Source

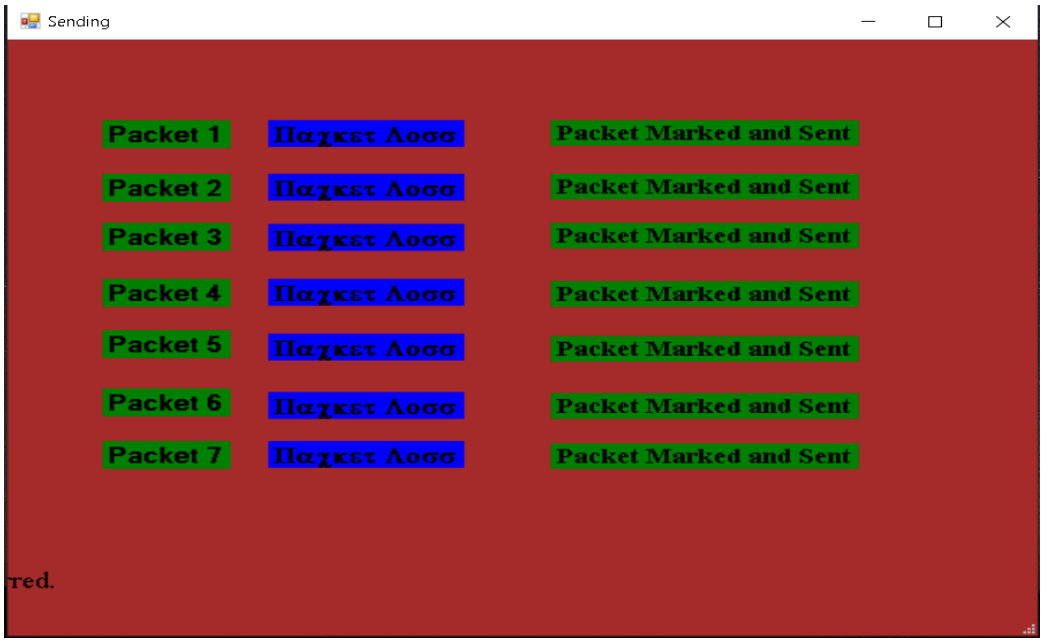

Figure 2: Data converted into packets and sent

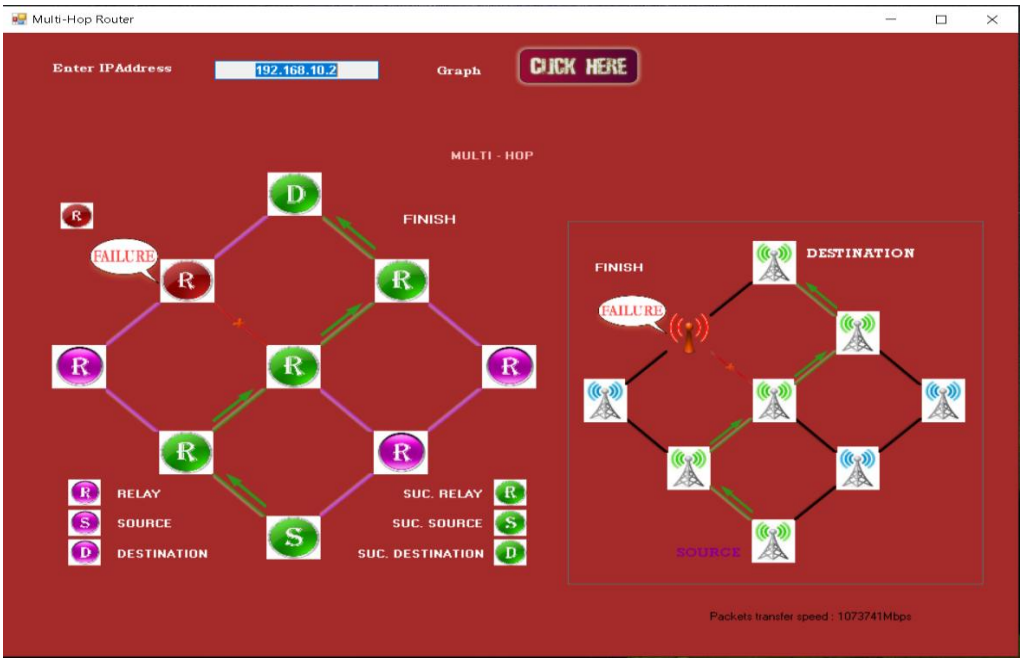

Figure 3: Router finding shortest path for data transmission

Figure 4:Path of the data sent from source to destination

Figure 5:Destination End

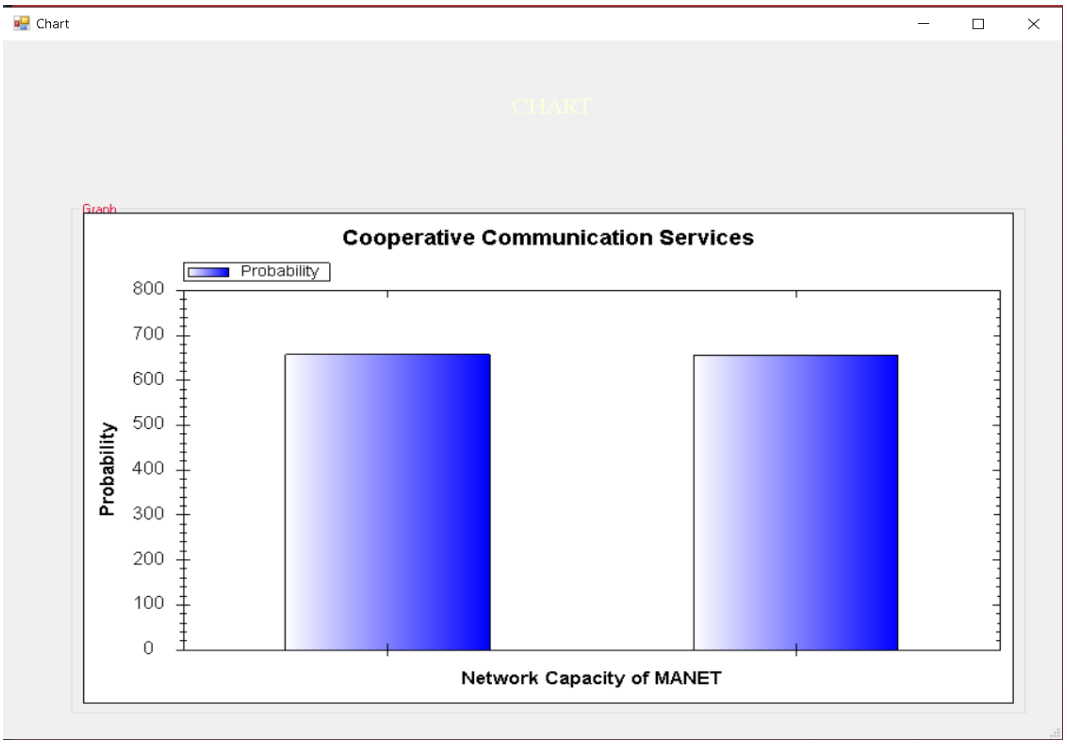

Figure 6:Cooperative Communication Services

V. CONCLUSION

The show utilized should be energy consumption, which can be further enhanced by utilizing a nice quality grouping method, in order to boost the association lifespan similarly to strong and viable connection in remote sensor networks. A PSO-based approach for noxious centre identification and selecting a bundle head in a remote sensor network is proposed in this study. The suggested algorithm is based on three data constraints: the centre point's remaining energy, upheld consideration, and the association quality, which determines the capacity of each and every centre point in the WSN. These three data restrictions are enlisted utilizing PSO to determine the ability of each centre point. As a consequence, PSO-NMDC redirects CHFL's present insufficiency, such as bunch coverage and overhead. As a result of these characteristics, the suggested computation PSO-NMDC attests to be the preferred option when less energy is required while improving the association lifespan.

In the future, Multiple attacker nodes can be added to the suggested detection method to improve it even further. The suggested method may also be used to identify other attacks in WSNs, such as the Sybil attack and the wormhole assault. To minimize computing cost and enhance battery life on individual nodes, a hybrid model that incorporates the features of both centralized and distributed models might be used.

REFERENCES

[1]. J. R. Vacca, Computer and information security handbook. Newnes. 2012.
[2]. C. Karlof and D. Wagner, " Secure routing in wireless sensor networks: Attacks and countermeasures,". Ad hoc networks, 1(2-3), pp. 293-315, 2003
[3]. D. Martins and H. Guyennet, "Wireless sensor network attacks and security mechanisms: A short survey". in Network-Based Information Systems (NBiS), 2010 13th International Conference, IEEE, 2010. pp. 313-320.
[4]. E. C. H. Ngai, J. Liu and M. R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," 2006 IEEE International Conference on Communications, Istanbul, pp. 3383- 3389. 2006.
[5]. L. J. Villalba, A. L. Orozco, A. T. Cabrera, and C. J. Abbas, "Routing protocols in wireless sensor networks," Sensors (Basel), vol. 9, no. 11, pp. 8399–8421, 2009 .
[6]. A. A. Pirzada, and C. McDonald, Circumventing sinkholes and wormholes in wireless sensor networks. In IWWAN'05: Proceedings of International Workshop on Wireless Ad-hoc Networks , 2005. pp. 132-150.
[7]. S. D. Roy, S. A. Singh, S. Choudhury and N. C. Debnath, "Countering sinkhole and black hole attacks on sensor networks using Dynamic Trust Management," 2008 IEEE Symposium on Computers and Communications, Marrakech, 2008, pp. 537-542.
[8]. Changlong Chen, M. Song and G. Hsieh, "Intrusion detection of sinkhole attacks in large-scale wireless sensor networks," 2010 IEEE International Conference on Wireless Communications, Networking and Information Security, Beijing, 2010, pp. 711-716.
[9]. H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," Journal of Computer and System Sciences, vol. 80, no. 3, pp. 644-653. 2014
[10]. C. Blum, and X. Li, "Swarm intelligence in optimization," Swarm Intelligence . Springer, Berlin, Heidelberg. pp. 43-85, 2008.
[11]. C. Raghavendra, K. Krishna, T. Znati (Eds.), Wireless Sensor Networks, Springer-Verlag, 2004.
[12]. K. Sohraby, D. Minoli, T. Znati, Wireless Sensor Networks: Technology, Protocols, and Applications, Wiley, 2007.
[13]. J. Kephart, D. Chess, The vision of autonomic computing, IEEE Computer Magazine Vol. 36, Issue 1, pp. 41–50, 2003.

[14]. R.Sharma, D.K. Lobiyal, Proficiency Analysis of AODV, DSR and TORA Ad-hoc Routing Protocols for Energy Holes Problem in Wireless Sensor Networks, Procedia Computer Science, Elsevier, Vol. 57, pp.1057-1066, 2015.
[15]. R. Sharma, D.K. Lobiyal, Energy Based Proficiency Analysis of Ad-hoc Routing Protocols in Wireless Sensor Networks, in IEEE Conference Proceedings (ICACEA), pp. 882-886, March 2015.
[16]. K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Ad Hoc Networks Vol. 3, Issue 3, pp. 325–349, 2005.