Particle Swarm Optimization Based QoS Aware Routing for Wireless Sensor Networks

K.kavitha[1] Dr. M.Mohamed Surputheen[2]
[1]Student [2]Associate Professor
[1,2]Department of computer Science
[2]Jamal Mohamed College, Tiruchirappalli

Abstract— Efficiency in a Wireless Sensor Network can only be obtained with effective routing mechanisms. This paper uses Particle Swarm Optimization (PSO), a metaheuristic algorithm to perform the process of routing. Since PSO does not have a defined fitness function, it is flexible to incorporate user defined QoS parameters to define the fitness function.

Key words: PSO, Routing, Wireless Sensor Networks

I. INTRODUCTION

A Wireless Sensor Network is a distributed structure containing sensors operating wirelessly over a network. A WSN can be divided intodata acquisition network and data dissemination network. The data acquisition network contains the sensor network. A collection of sensor nodes measure the physical data of its surroundings and forwards this information to the base. The data dissemination network provides an interface of the data acquisition network for ease of use.

Energy is the rarest resource of WSN nodes, and the lifetime of a WSNs is largely dependent on it. Tree-structured routing is one of the mostly used structures in a WSN, with the base station at the root. While recent work has begun to consider DAG structured networks with redundant transmission of values, such approaches are limited in the functions they can compute.

Particle Swarm Optimization (PSO) [4] is a metaheuristic optimization technique that can be used in the process of optimization. This technique considers particles as the optimization agents. These agents are distributed in the swarm and movement of these particles in the swarm determines the efficiency of the optimization process.

II. RELATED WORKS

Motivated by [6], Lee and Cho [7] propose an enhanced interleaved authentication scheme called the key inheritance-based filtering was proposes. This method prevents forwarding of false reports. The keys of each node used in the message authentication consist of the node's own key and the keys inherited from its upstream nodes. Other than these works, [1, 5, 10] focus only on energy efficiency in wireless sensor network, and the works like [8, 2, 3] deal with the security measures for routing in WSN.

A protocol, which creates a tree structure in the network based on the energy levels and distances (from the base station) of the sensor nodes has been proposed. Along with the energy-efficient structuring of the network, it initializes an efficient security scheme down the paths of the tree to ensure secure data transmission in the network. This scheme addresses secure data transmission from the source sensors to the base station along with energy-efficient structuring and operation of the network. Deception through false injection of data is prevented. The forwarding nodes can detect the irregularities with a minimum effort and thus drop unnecessary or flawed packets. By stopping the false packets to travel a long distance along the created paths in the network, it helps for greater energy efficiency, as the intermediate nodes are thus saved from extra transmissions. Periodic restructuring of the network is proposed to keep a balance among the nodes to dissipate energies in nearly equal proportion.

III. SYSTEM ARCHITECTURE

The current method uses Particle Swarm Optimization (PSO) as the base algorithm for generating routes. Figure 1 shows the overall system architecture of PSO based routing.

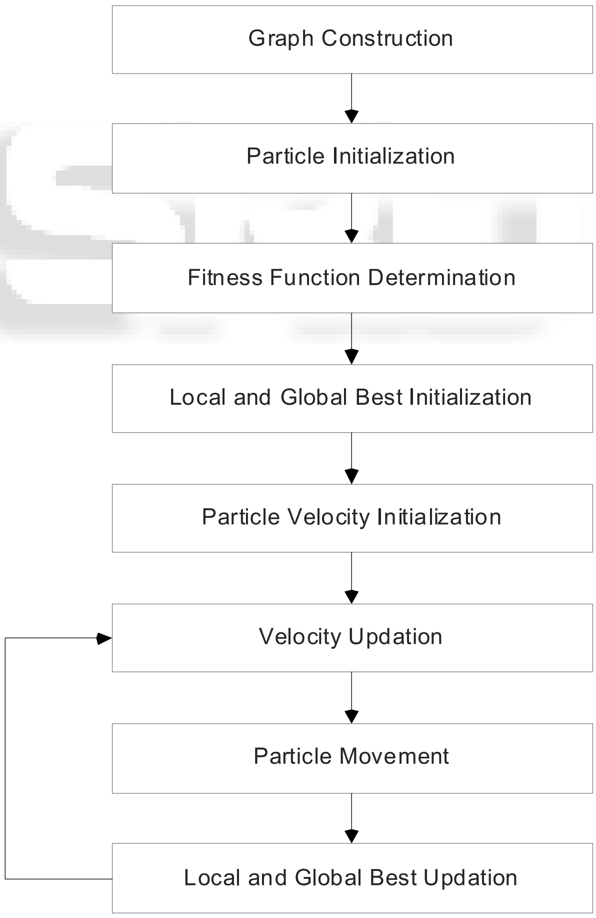

Fig. 1: System Architecture

The base topology is determined and a directed graph is constructed. Particle initialization is performed on the graph and the fitness function is determined. Initial velocity of the particles are determined, and the global best result is determined by iteratively modifying the velocity values with respect to the local and global best results.

IV. PARTICLE SWARM OPTIMIZATION BASED QOS AWARE ROUTING FOR WIRELESS SENSOR NETWORKS

A. Graph Construction

The initial phase deals with detecting the topology of the WSN. This can be performed by transmitting *hello* packets in the network, or by external tools of the user's convenience. Topology is detected and a graph is constructed with vertices and edges depending on the connections existing in the network.

B. Initialization and Fitness Function Determination

The number of particles to be placed in the swarm is initially determined. There is no standard method for determining the number of particles to be placed on a graph. It is obtained using the trial and error method and is mostly dependent on the size of the problem being analyzed.

Fitness function in PSO [9] is not defined, hence the user can define their own fitness functions to suit the needs of the problem in hand.

C. Particle Movement and Velocity Determination

The particles are placed in the swarm and the local best (*pbest*$_i$) is calculated for each particle. All the *pbest* values are analyzed and the global best for the swarm (*gbest*) is determined. Initial velocity for the particles is determined by generating a random velocity value.

$$V_i \sim U\left(-|b_{up} - b_{lo}|, |b_{up} - b_{lo}|\right) \quad (1)$$

Where b_{up} and b_{lo} are the upper and lower boundaries of the search space being used and v_i is the velocity of the ith particle. The random velocity is generated in accordance with equation 1.

A termination condition is defined according to the user's requirement. This can correspond to maximum number of iterations allowed or a maximum time limit for obtaining the result. Movement is defined for every particle based on the particle's *pbest*and the global *gbest.*

$$V_{i,d} \leftarrow \omega V_{i,d} + \varphi_p \gamma_p (p_{i,d} - x_{i,d}) + \varphi_g \gamma_g (g_d - x_{i,d}) \quad (2)$$

Where v_{id} is the velocity of the ith particle's dth dimension, ω, φ_p and φ_g are defined by the user. The efficiency of the algorithm is determined by these parameters, $x_{i,d}$ represents the position of the ith particle, $p_{i,d}$ represents the particle best and g_d refers to the global best of the swarm. Velocity of a particle is determined using equation 2 and the particle is moved according to the resultant velocity. After every movement, the particle best and the global best are checked, and if the current *pbest*value of a particle is better than the *gbest*, then the *gbest*value is replaced with the current particle's *pbest.*

V. RESULTS AND DISCUSSION

A. Simulation setup

All the experimental simulations were performed on a desktop, with the following configuration: Intel® Core™ i3-4130 Processor (3.40GHz), 4GB DDR3 SDRAM 20 MB Cache, 32 GB ECC RAM in a Windows 7 - 64 bit environment. Implementation was done in C# language using the Visual Studio 2012 development environment.

A network topology consisting of 35 nodes is considered for the process.

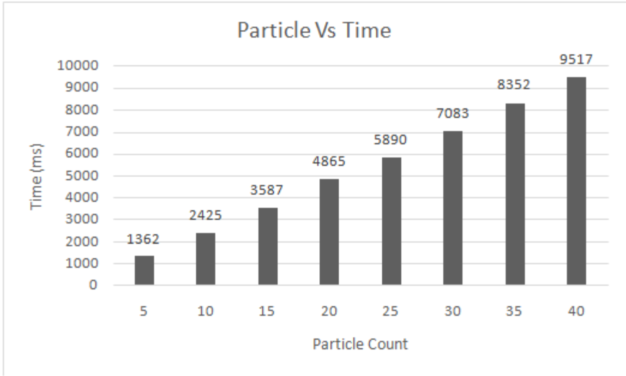

Fig. 2: Time Analysis

From the graph, it is clearly seen that as the number of particles increase, the time taken for processing increases.

VI. CONCLUSION

Fitness function is PSO is user defined. Hence the user can include the necessary constraints required for the problem into the fitness function, while most of the other metaheuristic methods such as Ant Colony Optimization, Bee Colony Optimization, Firefly Algorithm etc. define their fitness functions according to the distance or other factors. This makes PSO one of the best candidate for solving optimization problems dealing with quality constraints.

REFERENCES

[1] Boukerche, A, El-Khatib, K, Xu, L &Korba, L 2004, 'A novel solution for achieving anonymity in wireless ad hoc networks', In: Proceedings of the 1st Association for Computing Machinery international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks,Coimbra, Portugal, pp. 30–38.

[2] De, S, Qiao, C & Wu, H 2003, 'Meshed multipath routing with selective forwarding: An efficient strategy in sensor networks' Computer Networks, vol. 43, pp. 481–497.

[3] Greenwald, MB &Khanna, S 2004, 'Power-conservative computation of order-statistics over sensor networks', Proceedings 23th SIGMOD Principles of Database Systems, Paris, France.

[4] Kennedy, J.; Eberhart, R. (1995). "Particle Swarm Optimization". Proceedings of IEEE International Conference on Neural Networks IV. pp. 1942–1948. doi:10.1109/ICNN.1995.488968.

[5] Khushvinder Gill &Shuang-Hua Yang 2009, 'A scheme for preventing denial of service attack on wireless sensor networks' Proceedings of annual conference of the IEEE industrial electronics society, Porto, Portugal, pp.2603- 2009.

[6] Lee SJ &Gerla, M 2001, 'Split Multipath Routing with Maximally Disjoint Paths in Ad Hoc Networks', Proceedings. IEEE International Conference Communications, vol. 10, pp. 3201-3205.

[7] Lee, SB& Choi, YH 2006, 'A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks', In: Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks, New York, USA, pp. 59–70.
[8] Ray CC Cheng, Nicolas Jean-baptiste, Wayne Luk&Peter YK Cheung 2005, 'Customizable Elliptic Curve Cryptosystems', IEEE Transactions on VLSI Systems, vol. 13, no. 9, pp. 1048-1059.
[9] Shi, Y.; Eberhart, R.C. (1998). "A modified particle swarm optimizer". Proceedings of IEEE International Conference on Evolutionary Computation. pp. 69–73.
[10] Zhan, G, Shi, W & Deng, J 2009, 'Poster abstract: 'Sensortrust - a resilient trust model for WSNs', Proceedings of the 7th International Conference on Embedded Networked Sensor Systems, Berkeley, California.