International Journal of Computer Science and Management Studies Vol. 13, Issue 02, March 2013
ISSN: 2231-5268
www.ijcsms.com

Malicious Node Detection and Path Optimization: A Review

Bhawna Bansal[1], Deepak Goyal[2]

[1] M.Tech Student, Vaish College of Engineering, MDU, Rohtak, Haryana (India)
bbansal9@gmail.com

[2]Associate Prof., Vaish College of Engineering, MDU, Rohtak, Haryana (India)
deepakgoyal.vce@gmail.com

Abstract
Detection of a malicious node in neighbourhood is a requirement because otherwise that node may cause incorrect decisions or energy depletion. The methods to detect malicious node include the role-based trust approach, event-based trust approach, collaborative trust approach, and agent-based trust approach, neural-based approach. After malicious node detection we need to either correct it or choose another path. For choosing path we need to select optimized path from alternatives available. An optimization method that requires moderate memory and computational resources and produces good results is desirable. Swarm Intelligence is subfield of provides solution for complex optimization problems which are not easily tackled by other approaches. SI mainly consists on Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO) and Honeybees paradigms.
Keywords: *Swarm intelligence, Trust-based approach, Wireless sensor networks.*

1. Introduction

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network to a main location.
The main characteristics of a WSN include:

- Power consumption constrains for nodes using batteries or energy harvesting.
- Ability to cope with node failures.
- Mobility of nodes.
- Dynamic network topology.
- Communication failures.
- Heterogeneity of nodes.
- Scalability to large scale of deployment.
- Ability to withstand harsh environmental conditions.
- Ease of use.
- Unattended operation.
- Power consumption. [1]

Wireless sensor networks (WSNs) in recent years, have shown an unprecedented ability to observe and manipulate the physical world, however, as with almost every technology, the benefits of WSNs are accompanied by a significant risk factors and potential for abuse. So, someone might ask, how can a user trust the information provided by the sensor network?
Sensor nodes are small in size and able to sense events, process data, and communicate with each other to transfer information to the interested users [2]. With the advent of real-world applications in the area of Wireless Sensor Networks (WSNs), the need for applicable secure communications increasingly moves into the attention of research.
There are certain security requirements needed by the state of the art that a security system needs to cover in order to be able to call it secure and these are Congeniality, Integrity, Authenticity, Freshness, Semantic Security, Availability, Access Control [3].

2. Survey Report

Two issues in WSN: There are basically two issues in WSN that need to be studied:
Malicious node detection and path optimization, Path optimization is studied according to swarm intelligence and other protocols.

2.1 Malicious Node Detection

In a wireless sensor network, operating in a harsh and unattended environment, sensor nodes may generate in-correct sensor readings and wrong reports to their neighbours, causing incorrect decisions or energy depletion. The potential sources of incorrect readings and re-ports include noise, faults, and malicious nodes in the network. Unlike noise and faults, malicious nodes can arbitrarily modify the sensed data and intentionally generate wrong reports. To ensure reliable event detection in the presence of such wrong data and reports, it is necessary to detect and isolate malicious nodes, greatly reducing their impact on decision-making. [4]

There are varieties of methods to calculate the trust of a successive node. The methods include the role-based trust management, event-based trust management, collaborative trust management, and agent-based trust management, neural-based approach.

2.1.1 Role-based Trust Management

In [5] author uses Role-based approach and used RT for representing security policies and credentials in decentralized, distributed access control systems. A credential provides information about the privileges of users and the security policies issued by one or more trusted authorities.

2.1.2 Event-based Trust Management System

The trust is calculated at particular time events or periodically. In [6] author used ETSN protocol and says that the sensor node has different trust rating for different event. Watchdog model scheme to observe the behaviour in different events of these nodes and broadcast their trust ratings.

2.1.3 Collaborative Trust Management System

The business models are used to calculate the trust similar to product trust management. In [7] author used the cooperative and collaborative approach which helps to eliminate the suspicious node from the communication path.

2.1.4 Agent-based Trust Management System

Agent-based trust management systems, an agent node is introduced to store the packet transfer information from a cluster of nodes within communication distance. In [8] author used two approaches as: Trust of each node in the cluster transmitting the packets through same node and must be within communicating distance, Trust of a node (constant and less than 1) to its neighboring node(s).

2.2 Path Optimization

WSN have many issues related to the Path optimization. There are many protocols to solve it which we will discuss below.

2.2.1 Survey of Swarm Intelligence

Swarm Intelligence (SI) provides solution for the complex optimization problems which are not easily solved by other approaches. Swarm Intelligence mainly consists of Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO) and Honeybees paradigms. Swarm Intelligence approaches are nature and bio inspired.

Particle Swarm Optimization : Bio-inspired optimization methods are computationally efficient alternatives to analytical methods. Particle swarm optimization (PSO) is a popular multidimensional optimization technique. PSO models social behaviour of a flock of birds. It consists of a swarm of s candidate solutions called particles, which explore an n-dimensional hyperspace in search of the global solution (n represents the number of optimal parameters to be determined). A particle i occupies position Xid and velocity Vid in the dth dimension of the hyperspace, $1 \cdot i \cdot s$ and $1 \cdot d \cdot n$. Each particle is evaluated through an objective function. The cost (fitness) of a particle close to the global solution is lower (higher) than that of a particle that is farther. PSO thrives to minimize (maximize) the cost (fitness) function. In the global-best version of PSO, the position where the particle i has its lowest cost is stored as (pbestid). Besides, gbestd, the position of the best particle. In each iteration k, velocity V and position X are updated using (1) and (2). The update process is iteratively repeated until either an acceptable gbest is achieved or a fixed number of iterations kmax is reached.

$$Vid(k + 1) = w \cdot Vid(k) + c_1 r_1(k) \cdot (pbestid - Xid) + c_2 \cdot r_2(k) \cdot (gbestd - Xid) \quad (1)$$

$$Xid(k + 1) = Xid(k) + Vid(k + 1) \quad (2)$$

Here, c_1 and c_2 are constants, and $r_1(k)$ and $r_2(k)$ are random numbers uniformly distributed in [0,1] [9].

In [10] author considers Sensor Deployement Problem using Particle Swarm Optimization(PSO).

In[11] author considers sensors that move according to the well-known Particle Swarm Optimization (PSO) scheme in order to improve network coverage. Here unlike the original PSO, particle speed is updated by considering a consensus algorithm based on local optimum position.

In[12] author proposed a virtual force co evolutionary PSO for dynamic deployment of Nodes.

In [13] author used multi-base for optimal positioning of base station according to minimum distance.

Ant Colony Optimization: Ant Colony Optimization (ACO) is a flavour of Swarm Intelligence based approaches applied for optimization problems. ACO meta-heuristic approach models the real ants. In ACO, a number of artificial ants uild solutions to an optimization problem. In ACO, the exchange of information is done by pheromone value like real ants. The path optimization between nest and food is achieved by ant colonies by exploiting the pheromone quantity dropped by the ants [14].

Research shows that ants have the ability to select the shortest path among few possible paths connecting their nest to a food site. The pheromone, a volatile chemical substance laid on the ground by the ants while walking and

affecting in turn their moving decisions according to its local intensity, is the mediator of this behaviour.

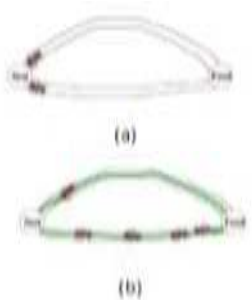

Fig. 1 Principle of Ant Colony Optimization

As shown in Fig. 1, at the beginning, no pheromone is laid on the branches and the ants do not have any bit of information about the branches length. However, since one branch is shorter than the other, the shorter branch receives pheromone at a higher rate than the longer one. As ants can smell pheromone, and their probabilistic decisions are based in favor of paths marked with higher amount of pheromone. Eventually, the shorter path will be selected by almost all ants of the colony (as shown in Fig. 2(b)).Ant colony optimization metaheuristic, a novel population-based approach was recently proposed in 1992 by Marco Dorigo et al. to solve several discrete optimization problems. The ACO mimics the way real ants find the shortest route between a food source and their nest. The ants communicate with one another by means of pheromone trails and exchange information about which path should be followed. The more the number of ants traces a given path, the more attractive this path (trail) becomes and is followed by other ants by depositing their own pheromone.

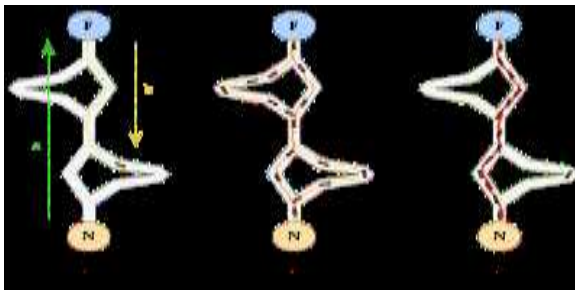

Fig. 2 Ant Colony system

This auto catalytic and collective behaviour results in the establishment of the shortest route as shown in Fig. 2.
In[15] author combined Path Selection Routing along with the concept of Ant Optimization.
Honeybees : The bees algorithm is population based, bio inspired approach for optimization problems that mimics the food foraging behaviour of swarms of honey bees. The bee's algorithmic approaches exploit the concept of honey bees for food searching, defence and locatable behaviour of real honey bees. The artificial bees mostly are divided into three groups namely as employed bees, onlooker bees and scout bees performing their corresponding duties. The literature survey shows that the Honey Bee Algorithm (HBA) was proposed by Craig A Tovey in 2004, Vertia Bee Algorithm (VBA) formulated by Xing-She Yang in 2005 and same time Artificial Bee Colony (ABC) by D Karabogo for numerical function optimization. The working of the bee's algorithm starts with the placement of scout bees in the search space and fitness of the scout bees is evaluated. The bees having higher fitness then a threshold is chosen as selected bees and corresponding visited sites by then are selected for neighbourhood search. As SI based approaches are iterative and termination criteria are proposed for the termination of the algorithm. Like other SI approaches, Honeybee algorithms have vase domain of application, training neural networks, scheduling jobs, data clustering, tuning a fuzzy logic controller, computer vision and multi-objective optimization. The prominent application of Honeybees based algorithms are in the field of ad hoc and wireless sensor networks [16].
In [17] author applied ABC algorithm to the dynamic deployment problem in WSNs with mobile sensors. In the network's scenario, author assumed that: The detection radii of the sensors are all the same (r). All of the sensors have the ability to communicate with the other sensors. All sensors are mobile.

2.2.2 Survey of Routing Protocols not based on Swarm Intelligence

In [18] LEACH (Heinzelman et al., 2000, 2002) became the most popular and the first energy-efficient hierarchical algorithm proposed for power consumption reduction in sensor networks. LEACH rotates the clustering task among the participating nodes based on duration. Each cluster head communicates directly to the sink.
In [19] author surveyed some routing protocols not based on SI principles. These are :
Lindsey and Raghavendra have proposed Power-Efficient Gathering in Sensor Information Systems (PEGASIS), which avoids the assumption of direct communication and reduces the relatively large overhead of the LEACH protocol.
Directed diffusion, proposed by Intanagonwiwat et al., is a popular data-centric routing protocol for WSNs. The sink node floods queries (termed "interests") containing the attributes of the required data towards a target region. When an interest is received by a node in the specified region, it tasks its sensors to start collecting data at the prescribed rate. Sensed data is then routed back to the sink along the reverse links. Directed diffusion makes use of a complex algorithm

for interest/data matching that puts a relatively large computational overhead on resource-constrained sensor nodes.

Haas and Small have proposed Shared Wireless Info-station Model (SWIM), which targets the delivery of the sensed events to a base station as early as possible. For this purpose, after sensing an event, a node transmits the event information to its neighbors. In this way, the information about the event is rapidly spread throughout the network. As soon as one of the nodes in the vicinity of a mobile sink becomes aware of the event, it promptly delivers the related information to the sink.

3. Conclusion

Wireless Sensor Network is emerging as a hot topic today. There are various issues in this networking .This paper studied the various techniques for Malicious Node Detection and Path Optimization. In future we would try to minimize the issues effectively.

References

[1] Mohammad Momani and Subhash Challa, "Survey of Trust Models in Different Network Domains".

[2] Jochen Schiller, Mesut Gunes, Nicolai Schmittberger and Norman Dziengel, "Secure Communications for Event-Driven Wireless Sensor Networks".

[3] Sung-Jib Yim and Yoon-Hwa Choi, "Neighbor-Based Malicious Node Detection in Wireless Sensor Networks", www.SciRP.org/journal/wsn, sept. 2012.

[4] Anna Felkner, "How the Role-Based Trust Management Can Be Applied to Wireless Sensor Networks", Journal of Telecommunications and Information Technology, April 2012.

[5] Chuanshan Gao, Jinchu Hu, Haiguang Chen and Huafeng Wu, , "Event-based Trust Framework Model in Wireless Sensor Networks", International Conference on Networking, Architecture, and Storage,IEEE Computer Society, 2008.

[6] "Secure Packet Transfer in Wireless Sensor Networks[Sensors & Transducers(Canada)]", IFCA, April 2012.

[7] Yenumula B. Reddy, "Trust-Based Approach in Wireless Sensor Networks Using An Agent to Each Cluster", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.1, No.1, February 2012.

[8] Ganesh Kumar Venayagamoorthy and Raghavendra V. Kulkarni, "Particle Swarm Optimization in Wireless Sensor Networks:A Brief Survey", IEEE Transactionson Systems, MAN, and CYBERNETICS, March 2010.

[9] Babu Rao Thella, Nikitha Kukunuru and Rajya Lakshmi Davuluri, "Sensor Deployment Using Particle Swarm Optimization", Nikitha et. al. / International Journal of Engineering Science and Technology, vol. 2(10), 2010.

[10] Enrico Natalizio, Francesca Guerriero and Valeria Loscrí, "Particle Swarm Optimization Schemes Based on Consensus for Wireless Sensor Networks", MSWiM, 2012.

[11] J. J. Ma, S. Wang and X. Wang, "An improved co-evolutionary particle swarm optimization for wireless sensor networks with dynamic deployment," Sensors, vol. 7, 2007, pp. 354–370.

[12] G. N. Shiu and T. P. Hong, "Allocating multiple base stations under general power consumption by the particle swarm optimization," in Proceedings of the IEEE Swarm Intelligence Symposium (SIS), 2007, pp.23–28.

[13] A.A. Boudhir1, M. Ben Ahmed1 and M. Bouhormal, "New Routing Algorithm Based on ACO Approach for Lifetime Optimization in Wireless Sensor Networks", International Journal of Networks and Systems, Vol. 1, No. 2, Oct. - Nov. 2012.

[14] Anamika, Neeru Singla and Neha Sharma, "A Dynamic Network Reconstruction Approach using ACO", IOSR Journal of Electronics and Communication Engineering (IOSRJECE), Sep. – oct. 2012, pp. 27-35.

[15] Waseem Shahzad and Zulfiqar Ali, "Analysis of Routing Protocols in AD HOC and Sensor Wireless Networks Based on Swarm Intelligence", International Journal of Networks and Communications, 2013.

[16] Celal Ozturk, Beyza Gorkemli and Dervis Karaboga, "Artificial Bee Colony Algorithm for Dynamic Deployment of Wireless Sensor Networks", Turk J Elec Eng & Comp Sci, Vol.20, No.2, 2012.

[17] Adamu Murtala Zungeru, Li-Minn Ang and Kah Phooi Seng, "Classical and swarm intelligence based routing protocols for wireless sensor networks: A survey and comparison", Journal of Network and Computer Applications 35 1508–1536, Elsevier, 2012.

[18] Muhammad Saleem, Gianni A. Di Caro and Muddassar Farooq, "Swarm Intelligence Based Routing protocol for Wireless Sensor Networks : Survey and Future Directions", Elsevier, Volume 181, Issue 20, 15 October 2011, pp. 4597–4624.