ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(7), DOI: 10.17485/ijst/2016/v9i7/87790, February 2016* ISSN (Online) : 0974-5645

Designing an Algorithm to Improve the Trust and Reputation of the Gaussian in Wireless Sensor Networks

Leila Khalili[1*], Ali Ghaffarinejad[2] and Mansour Esmaeilpour[1]

[1]Computer Engineering Department, Faculty of Engineering, Islamic Azad University, Hamedan Branch, Hamedan, Iran; Leilakhalili.en@gmail.com, esmaeilpour@iauh.ac.ir
[2]Hamedan University of Technology, Hamedan, Iran; alighf@gmail.com
p.a.irfankhan@gmail.com, ravi.19053@lpu co.in

Abstract

Background/Objectives: A wireless sensor network, from the large number of nodes (which may reach to thousands of nodes) has been formed. These nodes, each are called a sensor that can sense a special feature of the environment (temperature, humidity, pressure, etc.) and to send to its neighbours.Trust level algorithms are often based on conditions and criteria of current environment in a particular application of wireless sensor networks are defined. The ultimate goal of these algorithms is reach to a network, respondingtofunctional and economic needs of operating environments in wireless sensor networks. **Methodology:** Each node from two sources is used to obtain trust values of its neighbouring nodes.At firstobtained the known value of direct trust of intended node;next,of indirect trust that by the rest of the common node in the radio range of the two nodes is obtained.Then by combination of direct and indirect trust, a total trust value for each node is calculated. **Findings:** For simulation, the MATLAB software is used; the number of 30 nodes are at interval of 500*500 meters randomly. A subnet of 5 nodes with node numbers of 10, 12, 15, 16 and 19 are examined to broadcast reports in specified time intervals.Neighbouring nodes view these reports and perform calculations and simulation continues for100 seconds. This simulation both for different scenarios such as: the presence of 5% misbehaving node in the neighbourhood, 10% misbehaving node in the neighbourhood, 20% of misbehaving node in the neighbourhood, being carried out. **Applications/Improvements:** Since the energy consumption is still low and scalability is also intermediate, according to this proposed method,it did not make changes in other parameters and by keeping them fixed increased the reliability. It is clear that the proposed method is more successful than other methods.

Keywords: Gaussian, Trust and Reputation, Wireless Sensor Networks

1. Introduction

Wireless sensor network, from the large number of nodes (which may reach to thousands of nodes) has been formed. These nodes, each other called a sensor and can sense a special feature of the environment (temperature, humidity, pressure, etc.) and communicate to the neighbours. In other words, two main features of these sensors are: ableto sense certain parameter from the environment and the ability to communicate. Although it is possible in some applications, these nodes are connected by cables, but in most cases a sensor network, completely wireless. Nodes in these networks are generally fixed or moving very limitedly. There is generally a central node called as sink to which all nodes can communicate directly. But in most cases such situation does not exist. For this reason, all the nodes need to knowthe path to the central node. The issue is that we need to design a system using Gaussian probability by that nodes in a wireless sensor network can be trustful to each other and prevent the entry of malicious nodes to the system.As well we exclude the network of presence of nodes that do not have enough trust. It is a potential model and uses Bayesian rules but the problem is a reputation assessment based on the observation data that some of trust models of these observations have used[1,2].

* *Author for correspondence*

2. Importance of Issue

By increasing computing capabilities and wireless communications of sensor networks more crucial role lie in most applications. This issue means to be very important of the role of the sensors causes that sensors give us information that they have high degree of importance. This helps to ensure the correct functioning of these systems, a series of issues, including classification of sensors, calculation of reliability, fault tolerance, combination of sensors is investigated[3].

2.1 Objectives of Trust and Reputation

Trust level algorithms are often based on conditions and criteria of current environment in a particular application of wireless sensor networks are defined. These definitions clearly, of general purposes of the trust level policies[4]. About the problem trust level of many algorithms has been presented. The ultimate goal of these algorithms is to achieve the network accountableto the economic and functional needs of operational environments in wireless sensor networks.

2.2 Fault Tolerance

In many applications, wireless sensor networks used in environments which usually nodes are under threat of destruction and physical events. Tolerance of cluster heads against the risks, often considered and has a special importance; because the cluster heads failure can cause the loss of the sensor data. The proposed solution to deal with the failure of cluster heads is the re-clustering of the network. Re-clustering of network in nodes demands extra load power, it also prevents the running operations of implementation[5].

3. Previous Works

Trust and reputation are important in many fields including social, economic and computer science. Trust systems are useful method to identify threats, deception or members of endangered of a network. These systems identify malicious nodes and remove them from the network[6].

3.1 RFSN Method

It is first trust model that is designed exclusively for wireless sensor networks while the other method-watchdog 2 is also find use. But watchdog because of its defects cannot record all behaviours and therefore there is some uncertainty value in the system[7].

3.2 ASTM Method

A trust management scheme for wireless sensor networks is based on agent that trust management, locally and with the little overhead in term of message and delay is executed. But one of the disadvantages of this model is that a trusted entity is responsible for establishing and maintaining agents.Agents against unauthorized analysis and correction of computational logic are vulnerable[8].

3.3 ATSN Method

It is a model that keeps sensor nodes of the other nodes trust of network. A node has the responsibility of monitoring the other nodes and acquires their reputation and of this reputation for reliability assessment and the prediction of future behaviour is used. At the time of the transaction, each node works only with the nodes that trust them[9].

4. Methodology

The majority of methods attempts to increase the efficiency and lifetime of sensor networks have built on the basis of having a reliable environment. Trust models, help to network nodes, for more effective to detect the malicious nodes from the normal node. Since the sensor networks have usually a large number of nodes, scalability in model of trust is very important. In this paper, a distributed trust model and scalability for sensor networks has been proposed. In the proposed method to calculate the trust of each node, the combination of direct and indirect trust a limited number of neighbouring nodes of given node is used.

4.1 System Reputation and Trust based on Gaussian Function

We assume that the sensor network of N nodes (n1, n2, n3... nN) has been formed and its adjacency matrix is the form of a symmetric matrix that when element of ij, is equal to 1 that node j, with the node i, be associated. Otherwise, the value of element will be zero. That is visible in Figure 1[10–12].

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Figure 1. The adjacency matrix of nodes.

4.2 Calculation of the Reputation of Node

Each node of the two sources is used to obtain trust values of its neighbouring nodes; firstly the value of direct trust of desired node is knownand secondly the indirect trust of desired node.It is obtained by other common nodes at the range of the radio, is used and then with the combination of direct and indirect trust an overall trust value for each node is calculated.

$$R_{i,j}(n) = \frac{1}{N}\sum T_{i,k} * T_{k,j} \qquad \text{Formula (1)}$$

In above relation the number of common nodes between i and j, with N has been shown and k is the number of node. According to the explanations above the value of total trust for node of i to node of j from Equation (2)is calculated.

$$T_{i,j}(n) = w_1 T_{i,j}(n) - w_2 R_{i,j}(n) \qquad \text{Formula (2)}$$

W1 and w2 are the weight of direct and indirect of trust and relation of w1 + w2 = 1 is established these two values according to ambient conditions are changed. Increase or decrease in trust of a node that receiving a service from it has taken, with the Relation of (3) is done.

$$T_{i,j}(n+1) = \begin{cases} (1+\beta) * T_{i,j}(n) S_i(n+1) = 1 \\ (1+p\beta) * T_{i,j}(n) S_i(n+1) = 0 \end{cases} \qquad \text{Formula (3)}$$

In this regard, β is a number in the interval of [0, 1] and p is a coefficient for controlling the rate of decline in trust. Si (n + 1) is the consent of the node of i, from the received service i is applicant node of service and j is the node that receiving service has taken through it.

4.3 Difference Report between Two Nodes

To calculate the difference report submitted by node of I and received by the node of J at time of t the Formula of (4) is used. Where in RR is reliability of routing and RMLD reliability of missing messages.

$$Ei, j\ (t) = 1-\{(1-RR)*(1-(RR*RMLD))\} \qquad \text{Formula (4)}$$

Through the Formula of (5), value of variance and mean of difference reports two nodes is obtained.

$$\sigma_{ij} = \frac{\sum_{i=1}^{n} x_i^2}{n} - \frac{\left(\sum_{j=1}^{n} x_j\right)^2}{n} \qquad \text{Formula (5)}$$

μ*i*, *j* average error is calculated of the Formula (6). It (difference) indicates value of error reported, σ*i*, *j* 2 variance of μ*i*, *j* will be average error.

$$\mu_{ij} = \frac{\sum_{i=1}^{n} x_i^2}{n-1} - \frac{\left(\sum_{j=1}^{n} x_j\right)^2}{n-1} \qquad \text{Formula (6)}$$

5. Results of the Simulation

MATLAB software is used for simulation using total of 30 nodes in the range of 500*500 meters randomly. A subnet of 5 nodes with node numbers of 10, 12, 15, 16 and 19 are examined to broadcast reports in specific time intervals. Neighbouring nodes view and perform calculations that simulation continues for 100 seconds. The simulation topology has been shown in Figure 2.

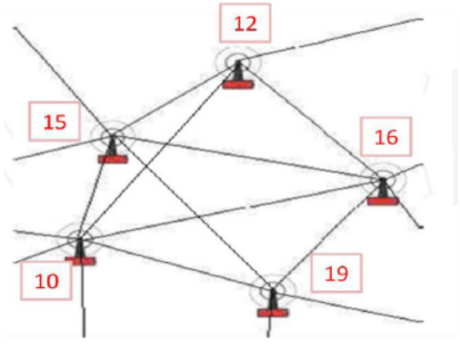

Figure 2. Topology of simulation.

Subnet used in the simulation node of 10, as the basis node for judgment is considered, that assesses the performance of other nodes. This simulation for different scenarios including: With the presence of 5% misbehaving

node in the neighbourhood, 10% misbehaving node in the neighbourhood, 20% misbehaving node in the neighbourhood, being carried out. Initially 15 node as the misbehaving node will start sending false reports and nodes of 12, 16 and 19 as the common nodes correct reports are sent. Node of 10 monitors the performance of all sender nodes of reports, and assigns trust values to them. In the scenario of simulation, node of 10 as the node monitoring, and node of 15 as the misbehaving node and node of 12, 16 and 19 behave as the normal nodes. In this case, node of 10 trust value to the rest of nodes measured and is shown in the chart.

Figure 3 Shows that the proposed method exhibits reduced misbehaving. In fact, this method identifies better the misbehaving node.

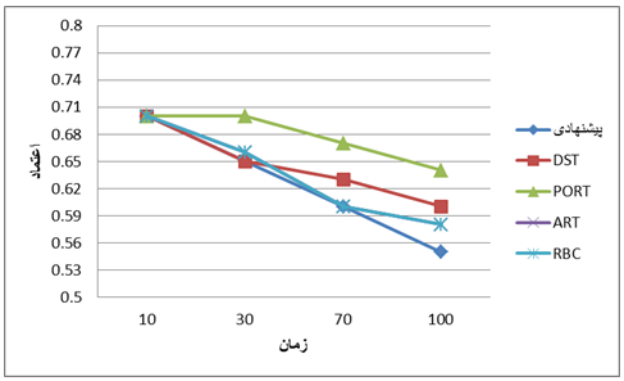

Figure 3. Comparison of trust in misbehaving node of 15.

Figure 4 and Figure 5 indicate that the proposed approach to standard nodes are not misbehaving has high trust.

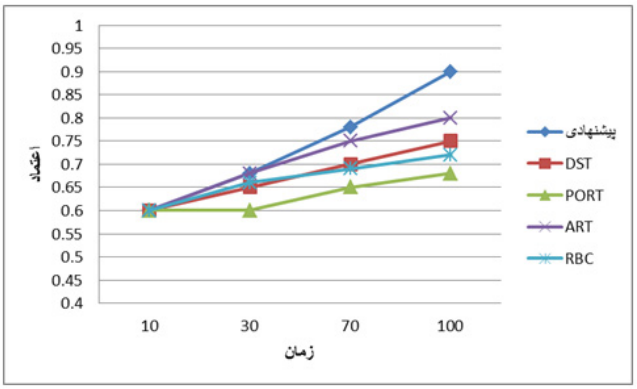

Figure 4. Comparison of trust in the nodes of 12, 16, and 19.

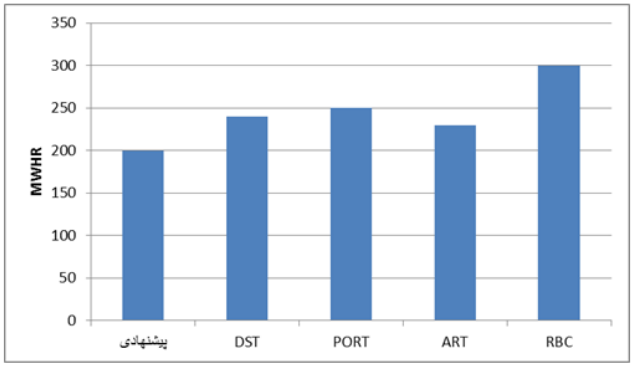

Figure 5. Average energy consumption.

The proposed method, due to low computational overhead, consumes less energy than other methods.

Result of performing comparisons of previous methods and the proposed method has been shown in Table 1.

Table 1. Comparison of methods

Methods	Reliability	energy consumption	Complexity	Scalability
DST	High	Low	High	Average
PORT	High	Low	High	Average
ART	High	Low	High	Average
RBC	High	High	High	Low
Proposed method	Very high	Low	High	Average

6. Conclusion

Using Gaussian method increases reliability. Since the energy consumption is still low and scalability is also intermediate, according to this proposed method did not make changes in other parameters and by keeping them fixed it able to increase reliability. It is clear that the proposed method is more successful than the other methods.

7. References

1. Stankovic J, Ramamrithm K, Spuri M, Buttazzo G.Deadline scheduling for real-time systems: EDF and related algorithms. USA:Springer Publishing Company;2012.
2. Deng Z, Liu L.Scheduling real-time applications in an open environment.In: Proceedings of the 18th IEEE Real-Time Systems Symposium. San Francisco, CA, USA:IEEE Computer Society; 1997. p. 308–19.

3. Stankovic J,Rammaritham K. Tutorial: Hand real-time. Los Alamitos:IEEE Computer Society Press; 2013.
4. Jeffay K, Stanat DF, Martel CU. On non-preemptive scheduling of periodic and sporadic tasks. Proceedings 12th IEEE Real-time Systems Symposium;San Antonio, TX. 1991. p. 129–39.
5. Cho M. Efficientand Secure Network Servicesin Wireless Sensor Networks. US: University of Michigan; 2009.
6. Sasirekha S, Swamynathan S. A comparative study and analysis of data aggregation techniques in WSN. Indian Journal of Science and Technology. 2015 Oct; 8(26):234–44.
7. Annadurai A, Ravichandran A. flexural behavior of hybrid fiber reinforced high strength concrete. Indian Journal of Science and Technology. 2016 Jan; 9 (1):455–66.
8. Ramya R, Saravanakumar G, Ravi S. MAC protocols for wireless sensor networks.Indian Journal of Science and Technology. 2015 Dec; 8(34):126–37.
9. Douceur J.Complex queries in DHT-based peer-to-peer networks.Proceeding IPTPS '01 Revised Papers from the1stInternational Workshop on Peer-to-Peer Systems; London: Springer-Verlag; 2012. p. 251–60.
10. Mashadi B, Mahmoodi-K M, Kakaee AH, Hosseini R. Vehicle path following control in the presence of driver inputs.Proceedings of the Institution of Mechanical Engineers Part K Journal of Multi-Body Dynamics. 2013 Jun; 227(2):115–32.
11. Park T. Lisp: Lightweight Security Protocols for Wireless Sensor Networks. US: University of Michigan; 2007.
12. Balasubramaniam T, Thirugnanam GS.an experimental investigation on the mechanical properties of bottom ash concrete.Indian Journal of Science and Technology. 2015 May; 8(10):345–54.