Calculating Trust and Aggregation of a node using Poisson Distribution in WSN

Arnab Ghosh
School of Education Technology,
Jadavpur University,
Kolkata

Sovan Bhattacharya
School of Education Technology,
Jadavpur University,
Kolkata

ABSTRACT

Designing an accurate and efficient trust model in WSN is nowadays aresearch challenge**.**Trust in wirelesssensor networks is an important issue and it solves theproblem of access control, privacy, secure routing scheme and reliable communication.The notion of trust can bedefined as an aggregation of consensus given a set of past interactions. Aggregating data is a way of compressing the transmitted packet, in a sense that the packet is comprised of only necessary information. This paper present, total Trust calculation in WSN nodes. We calculate the total trust by direct trust using probabilistic approach and indirect trust using Dempstar-Shafer theory (combination of evidence).Here we also find out aggregation value of a node using Poisson distribution and alsocompare between PDR value and average cumulative Poisson distribution.Results of various simulation experiments show that theproposed system can be highly effective for aggregation value of a node than to aggregate of node using coding by ordering technique.

KEYWORDS

Trust, Aggregation, Packet Delivery Ratio, Poisson distribution.

1. INTRODUCTION

Wireless sensor networks (WSNs) have wideapplications due to these sensor nodes ease ofdeployment, such as environment monitoring, rescuemissions, and smart houses. A lot of interest and effortare being focused on this new network topic.But Wireless Sensor networks (WSNs) are also highly vulnerable to attacks due to the nature of the wireless media and restricted resource. Recently, a new kind of mechanism for security in WSNs [4,5,6] has been presented, which is trust system. The definition of trust by [7] is:

Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before he can monitor such action (or independently of his capacity ever to be able to monitor it) and in a context in which it affects his own action.In WSN,a node can have two type of trust-

1) Direct Trust

2) Indirect Trust

Efficient power management is vital for increasingthe life of wireless sensor networks (WSN). The main reason is that the radio transmission consumes energy approximately three times comparing to other operations. Thus, techniques such as data aggregation have been widely used in WSN to preserve energy. A sensor node senses the environment and passes the reading to its local aggregator. An aggregator aggregates the data and pass it to another aggregator or forwarder. Aforwarder simply forwards the data to another aggregator or forwarder closer to the base station. To save energy, sensed data may be merged at one of many *aggregators*. The data aggregation process must be entrusted to protect aggregated data as well as reducing the wireless communication expenses.The goals of this paper are-

- To build a trust modelwithout a central trust authority, and it combines boththe direct trust value of the target node and the indirect trust value of the third-party nodes together and provides a reliable approach to establish trust for WSNs.
- Compare the packet delivery ratio and average cumulative Poisson distribution of aggregate node.
- Efficient approach than coding by ordering technique and determine, in spite of presence malicious nodes, the aggregator node aggregated correctly.

Approach of this paper fulfils the above-mentioned requirements. Contribution of this paper is threefold: 1) presenting a trust model that calculated total trust (direct trust +indirect trust) 2) calculated packet delivery ratio and aggregated value of any node in WSN using Poisson distribution.

The remainder of this paper is structured as follows. The related work is discussed in section 2. Proposed approach is presented in section 3. Simulation results are presented in section 4. In Section 5, conclusions and future work are describes.

2.RELATED WORK

Many activities in the human society are based ontrust mechanism. Trust in the human society hasbecome the basis of human beings' communications,work and lives.Trust can be regarded as acriterion for making a judgment under complex socialconditions and can be used to guide further actions.The trust mechanism in the human society was firstintroduced to security field in computer science. Trustand security are closely interdependent that cannot beseparated from each other. Nowadays, establishingtrust for WSNs is still an open and challengingproblem.

In[1],The trust is computed depending upon some parameterswhich have a primary role in enforcing security and cooperationbetween the nodes. They also developed a clustering mechanism and security is enforced by local

monitoring system by a newkind of nodes referred as guard nodes.Trust model[8] also calculated and eliminatesthe malicious behavior ofrogue nodes with high probability. In[9], trust value of the node inthe network depend on the trust attributes, metrics and trustparameters. In[10,11],aggregate data by any node in WSN is basically used Data Funneling routing which is based upon coding by ordering data compression scheme.

3. PROPOSED WORK

Total trust calculation is more or less same as the paper[1] have done, but in paper[1] works only with PDR and compare it with traditional watchdog mechanism. If we follow the same procedure and try to calculated the aggregation value of aggregator in WSN with 20 or more neighbour nodes then result is very low and aggregator node act as a malicious as per coding and ordering technique. In this paper we improve aggregation value of the aggregator in WSN using the POISSON DISTRYBUTION,which also supported coding and ordering technique.

3.1 Trust Calculation

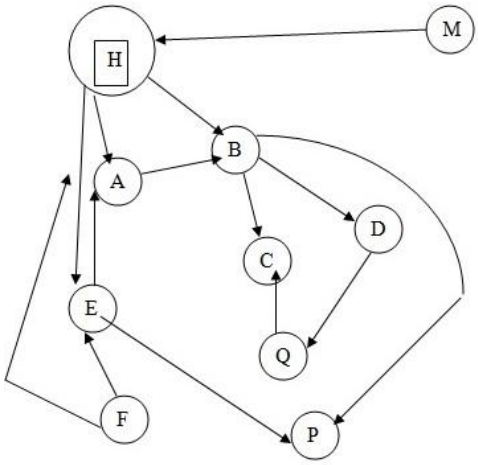

Fig1: Network Topology

Here m is the master node, which monitor all the node. H is the header node where all trust value of each node in WSN is to be calculated . A,B,C,D are common node. Now the following section is describe how trust will be calculated of a node.

3.1.1 Direct Trust Calculation

Let's to calculated direct trust of node A by the header. First header sends some number of packets to node A. After gating all the message from header A sends the acknowledgement to the header. Now will calculating direct trustusing following algorithm

Trust Parameters

f = No. of packets forwarded

d = No. of packets dropped

m = No. of packets misrouted

Step 1 : Collect data for *f, d,m, .*

Step 2 : Calculated total number of packets which will dropped and misrouted. i e(d+m)

Step 3 : Calculate total number of packet which will be successfully reach to node A. i.e { f-(d+m)}

Step 4 : Calculate the Direct Trust by using the formula

$Trust(t) = \{f-(d+m)\}/f$

3.1.2Indirect Trust Calculation

Let's to calculated trust of node C by node A .Here C is call review node and A is called query node. As there is no direct link between A and C , So A must collect trust by the neighbouring node of C i.e B and Q. Here we use *Modified Dempster Shafer Theory of combining Evidences.*Dempster-Shafer evidences theory [12], [13] is an approach forrepresent epistemic or uncertain knowledge. For instance, each node say *Ni*, will contribute its observation byassigning belief over Θ. The assignment function is known asthe Basic Probability Function(BPA) or the Mass Function $m:2^{\Theta} \rightarrow [0, 1]$ of the node *Ni*, denoted by *mi*. So according to *Ni* observation, the probability that " the node underreview is Trusted" is indicated by a "confidence interval"

[*Beliefi*(*T*), *Plausibilityi*(*T*)].The BPA which satisfies:

$\sum m(A) | A \subseteq \Theta = 1, m(\varphi) = 0$ (1)

if m(*A*)>0, *A* is the focal element.

The belief function is defined as

$$\sum_{A \subseteq T} m(A)$$

$$Plausibility_i(T) = 1 - \sum_{A \cap T = \varphi} m(A)$$

For each possible proposition (e.g., "Trusted") DS Theorygives a rule of combining node *Ni*'s observation *mi* and node*Nj* 's observation *mj* :

$$m_1 \oplus m_2(T) = \sum_{ak \cap ak1 = A} m_i(A_k) m_j(A_{k1}) / \sum_{ak \cap ak1 = \emptyset} m_i(A_k) m_j(A_{k1})$$

3.2 Packet delivery ratio

Packet delivery ratio is calculated as the totalnumber of packet received successfully at the final destinationand total number of packets sent.

Suppose that node B has 4 neighbor node n1, n2, n3, n4. Node B sends p packets to each neighbor node. But each neighbor gets r1, r2, r3, r4 packets respectively. So PDR is calculated as

PDR=(r1/n1)+(r2/n2)+(r3/n3)+(r4/n4).

This paper calculated average packet delivery ratio which is=(PDR/number of neighbor nodes)

3.3 CODING BY ORDERING

The main idea behind .Coding by Ordering is that when transmitting many unique pieces of data, and the order in which the data is sent is not important to the application then the choice of the order in which those pieces of data are sent can be used to convey additional information to the receiver.

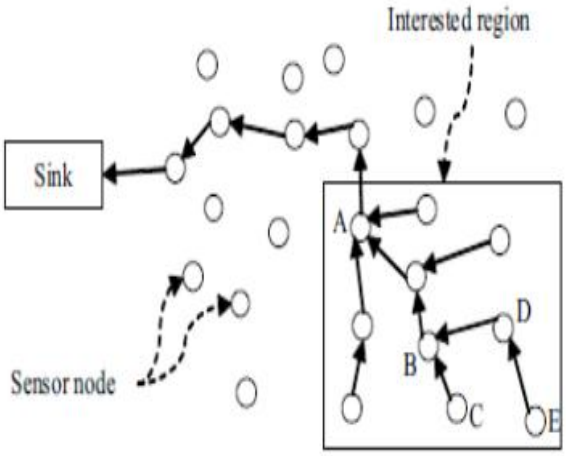

Fig2:Data Path

Here node A, B, and D are a data aggregation node. At an aggregation node, sensing data collected by other nodes is combined, and the aggregated data is sent to its parent node. At node D, data collected by node E is combined with data collected by node D itself. Then, the aggregated data is transmitted to node B.When data is combined at an aggregation node, some data is dropped. To include the information of dropped data in the aggregated data, the order of data packet is utilized. For a general case, let's assume that n is the total number of sensor nodes – each node has different a node ID, m is the number of nodes sending a packet to an aggregation node, k is the possible range of data value, and l is the number of sensor node dropped at the aggregation node.Therefore, the following inequality has to be satisfied

$(m-l) \geq (n-m+l)C$

Theoretically, when n = 2^7, k = 2^4, and m = 100,approximately 44% of packets can be dropped at theaggregation node by applying Coding by Ordering.Since this method has good compression ratio andsimple algorithm, it may be possible to use for WSNs.

4. PERFORMANCE ANALYSIS AND COMPARISON

4.1 Simulation & Networks Setup

Here proposed trust model is implemented in omnetpp-4.2.2.. The research question that we attempt to answer in this section is to what extent the proposed trust-based approach can aggregate the neighbour nodes including malicious nodes. To answer that question one must simulate network with different numbers of neighbour nodes including different numbers of malicious nodes also over time. The network set up is as follows

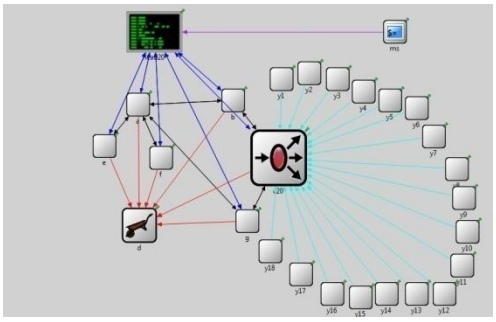

Fig 3: Typical proposed network setup model

In above model ms is the master node which monitor all node's trust values. The head node sending, receiving messages to and from the nodes and calculating all trust value, Poission value and packet delivery ratio.c20 is an aggregator which aggregate 20 neighbour nodes. Though the network is very simple and small but result to be expected same as a real network.

4.2 Experimental Results

The simulation results are presented in Figures 4-8. In this simulation where ones iterate different number of rounds and take Aggregation value, packet delivery ratio(PDR), each time of review node or aggregate node. In Figure 4-7 shows that comparison between PDR v/s POISSON DISTRIBUTION of aggregator with different neighbour nodes, while figure 8 shows maximum how many malicious nodes can take part in aggregation so that a node's aggregation does not affected. The x-axis denotes the no of rounds and the values in the y-axis are percentage of probability p .whether in figure 8 the values of x –axis denotes number of malicious nodes.

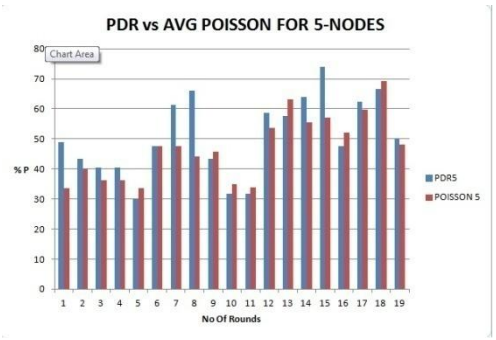

Fig4:PDR VS POISSON WITH 5 NEIGHBOUR NODES

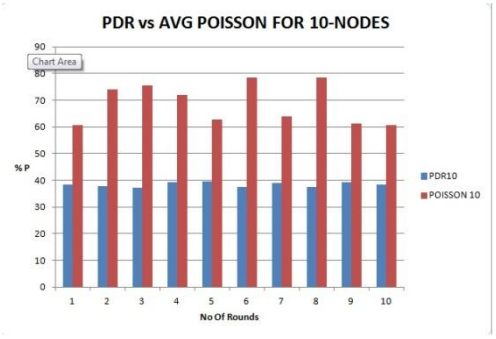

Fig5:PDR VS POISSON WITH 10 NEIGHBOUR NODES

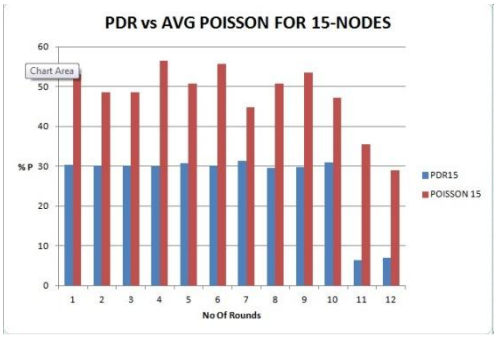

Fig6:PDR VS POISSON WITH 15 NEIGHBOUR NODES

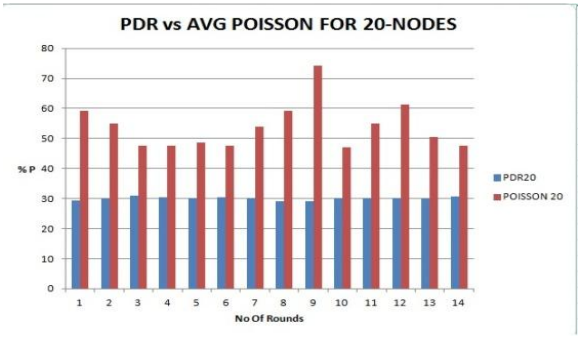

Fig7:PDR VS POISSON WITH 20 NEIGHBOUR NODES

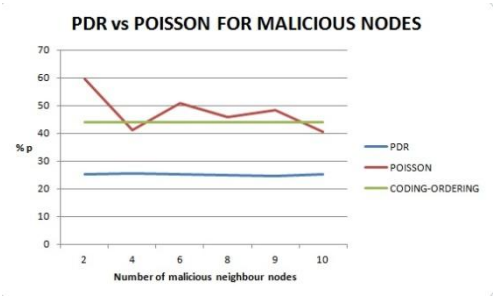

Fig8:DELIVERY RATIO VS POISSON

By observing figure 4- 7, it shows that if neighbour nodes areincreased more and more than proposal of this paper works efficiently than PDR. In figure 4, it seen that Poisson value does not work so accurately as expected, but in figure 6-7, shows the desire result. If network size and neighbour nodes of aggregator will be increased then result comes more accurately. In figure 8, there are 20 neighbour nodes of aggregator and it also seen that if almost half of neighbour nodes is to be malicious then it aggregation function works properly, but if number of malicious node is more than half of neighbour then it fails to aggregate by violating coding by ordering technique[10,11].

5.CONCLUSION AND FUTURE WORK

This paper present a trust framework model which calculated direct and indirect trust of any node in WSN based on aggregation. Here the review node or aggregated node improved the packet delivery ratio by replacing it with Poisson distribution.Dempster Shafer theory of combiningevidences always gives more accurate outputto find indirect trust. This paper also calculated the performance of aggregated node that means if though there are some malicious nodes are present, aggregated node do preformed aggregation correctly. In future, try to find out any other distribution which will be apply the above approach and it would give better result, and also try to calculate the energy savings of aggregator node.

6.ACKNOWLEDGEMENT

This paper was fully supported by school of education technology ,Jadavpur University.

7.REFERENCES

[1] Pushpita Chatterjee, Indranil Sengupta, S.K.Ghosh " A Distributed Trust Model for Securing Mobile Ad Hoc Networks"2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing,2010

[2] Dragan Petrovic, Rahul C. Shah, Kannan Ramchandran, Jan Rabaey" Data Funneling: Routing with Aggregation and Compression for Wireless Sensor Networks"

[3] Ian Ruthven Mounia Lalmas" Using Dempster-Shafer's Theory of Evidence to combine aspects of information use"

[4] Haiguang Chen, Huafeng Wu , Xi Zhou, Chuanshan Gao Agent-based Trust Model in Wireless Sensor Networks 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/DistributedComputing (SNPD2007) PP 119-124,July 30 -Aug 1, 2007 Qingdao,China

[5] S.Ganeriwal and M. Srivastava. "Reputation-based framework for high integrity sensor networks". In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), pp. 66-77, Oct 2004.

[6] Haiguang Chen, Huafeng Wu , Xi Zhou, Chuanshan Gao Agent-based Trust Model in Wireless Sensor Networks. 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/DistributedComputing (SNPD2007) PP 119-124,July 30 -Aug 1, 2007 Qingdao,China.

[7] D. Gambetta, Can we trust trust? in: D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations, 2000, pp. 213–237, Published Online, Ch. 13.

[8] Arijit UkilTrust and Reputation Based Collaborating Computing in Wireless Sensor Networks, Second International Conference on Computational Intelligence, Modelling and Simulation

[9] N.Karthik, V.R.Sarma Dhulipala TRUST CALCULATION IN WIRELESS SENSOR NETWORKS, IEEE,2011

[10] Naoto Kimura and Shahram Latifi A Survey on Data Compression in Wireless Sensor Networks, 0-7695-2315-3/05, IEEE,2011

[11] D. Petrovic, R. C. Shah, K. Ramchandran, and J.Rabaey, "Data Funneling: Routing withAggregation and Compression for WirelessSensor Networks," In Proceedings of First IEEEInternational Workshop on Sensor NetworkProtocols and Applications, May 2003.

[12] A. P. Dempster, A generalization of Bayesian interface, in :*Journalof Royal Statistical Society 30, 1968, pp. 205-447* .

[13] G. Shafer, A Mathematical theory of Evidence,*Princeton UniversityPress, 1976.*