Asian Journal of Information Technology 15 (5): 951-954, 2016
ISSN: 1682-3915

Fuzzy Based Node Trust Estimation in Wireless Sensor Networks

K. Selvakumar, L. Sai Ramesh and A. Kannan
Department of Information Science and Technology,
CEG Campus, Anna University, Chennai, India

Abstract: Trust management is an important aspect to enhance pattern and increase the secured packet transmission in Wireless Sensor Networks (WSNs). The kernel of the trust management is estimation of trust. If a trust prediction model is not enough to withstand against the malicious nodes from the network it affects performance as well as energy consumption of the entire system. This research study presents a novel node trust estimation model which is very active and robust in contact with malicious nodes. Furthermore, this research combines fuzzy expert system based inference mechanism with trust to achieve the secured data transmission which optimizes the energy of the WSNs. Extensive simulations have been conducted in this research and evaluation of results proves that this model is better than the other existing trust models.

Key words: Trust model, WsNs, malicious node, fuzzy expert systems, fuzzification and fuzzy rules

INTRODUCTION

WSNs comprises of huge number of sensor nodes that are tiny and have restricted process capablenesses and energy supports is proposed by Forghani and Rahmani (2008). It performs multi role like servers, routers, etc., in general during active mode and in stand by behaviour also goes to processing mode while detecting events in encircled space. Particularly in explode cases of subtle packets generated by malicious nodes, network traffic as well energy consumption problem increases. Moreover, presence of malicious nodes with magnified tendency of malfunctioned would worsen the network performance. Designing an optimal path based routing and energy consumption system in WSNs has been proposed previously without and with fuzzy expert system.

These research works deals with the packet routing and energy saving by establishing a trust model to measure the trust value of nodes in WSNs. A fuzzy logic based research model is proposed by. Aivaloglou and Gritzalis (2010) to efficiently construct network traffic and reduces the packet transmission loss for prioritized event-driven traffic approach. Bao *et al.* (2012) proposed an energy consumption based QoS packet routing algorithm for WSNs was developed to run effectively with best-attempt traffic. However, these models are assay to cut down the packet transmission overhead based on trust value of the nodes and stable environment without considering the current trust values of the untrusted nodes which are trying to increasing the network traffic as well as energy consumption.

The main aim of the trust estimation model is to predict trust values that are used to depict the trustworthy, reliableness, or competency of each node, with the aid of some management techniques is proposed by Crosby *et al.* (2006). Hence, the estimated trust information is used to for top level layer to perform packet routing shown in work proposed by Leligou *et al.* (2012) and Deng *et al.* (2010), data accumulation shown as in Lopez *et al.* (2010) and energy optimization process discussed in the research of Akkaya and Younis (2003) and Poolsappasit and Madria (2001). This research study proposes a Fuzzy Expert System (FES) based Node trust estimation with the help of trust estimation model in order to optimize the packet transmission as well as energy consumption.

MATERIALS AND METHODS

Trust manifests the assurance on the quality service of node's succeeding activeness. It addition, it performs the reciprocal relationships wherever an afforded node acts in a trustful manner and holds authentic communications with nodes which are extremely trusted by the committed node. The proposed heuristic based trust model consists of three different types of trust

Corresponding Author: K. Selvakumar, Department of Information Science and Technology, CEG Campus, Anna University, Chennai, India

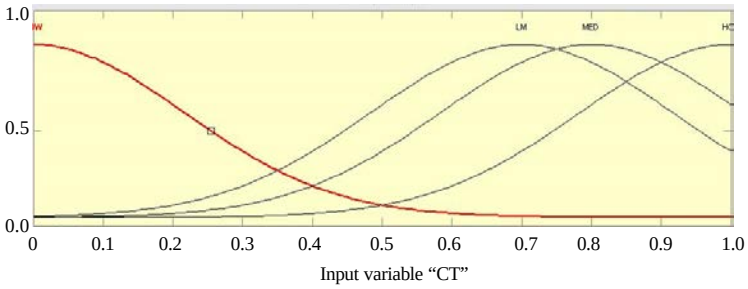

Fig. 1: Fuzzy membership function representation of node's Basic Trust (BT)

values namely basic, current and route trust values. In this new model, we first compute the basic trust using direct discussion with the neighbours. In each node, intelligent agents are deployed in order to compute the basic trust and to maintain history about the neighbours.

This basic trust is updated dynamically based on the communication using the metrics namely energy consumed, delay, number of packets dropped by the node, capacity of the node and cooperation of the node with its neighbours. The updated trust values are known as current trust. The two types of trusts namely basic and current trust are represented by BTij and current trust denoted by CTij. The node trust is computed by using basic trust and current trust and is denoted by NTVij. The basic trust value Btij denotes node vj's trust level from the evaluating node vi's point of view, which is calculated by:

$$NTV(t)_{ij} = \alpha BT(t)_{ij} + \beta CT(t)_{ij}, t_1 \le t \le t_2 \quad (1)$$

The weights α and β (α, $\beta > 0$, $\beta > \beta$ and $\alpha + \beta = 1$) are assigned to BT_{ij} and CT_{ij}. Now the basic trust is computed using the relation represented by $SE_m(i,j)$:

$$BT(t)_{ij}^{tk} = \frac{\sum_{m=1}^{Njk} SE_m(i,j)}{N_{tk}} \quad (2)$$

Current Trust (CT) value is estimated in this model is the trust value of the node in the time interval between t and t+1. This proposed trust model from this research work is compute the node's entire trust value based on the fuzzy expert system approach. If a node has trust value greater than the threshold, then its creditability is high else if it is near the threshold and goes up and down dynamically, it is called medium. Otherwise, it is called as low:

$$CT(t)_{irj} = CC(t)_{ir} \times BT(t)_{rj}, t_1 \le t \le NOW \quad (3)$$

In this research, Current Trust (CT) is computed using the following mathematical representation is:

$$CC(t)_{ir} = BT(t)_{i1} \times BT(t)_{12} \times BT(t)_{23} \times, \times BT_{(r-1)} t_1 \le t \le NOW \quad (4)$$

If n nodes are present in the communication, we have current trust values:

$$CT(t)_{rP1j}.CT(t)_{ip2j...}.CT(t)_{iP2j},...CT(t)_{ipnj} \quad (5)$$

Using these n values, CT (t) is computed using the form

$$CT(t)_{ij} = \sum_{k=1}^{n} w_{PK} \times CT(t)_{iPkj} \quad (6)$$

This model estimates the trust value of the node i on node j in time interval t+1 is represented as (T_{ij} (t+1)) is derived with the help of both basic trust of i on j at time t (BT_{ij} (t)) and current trust on j to i by few other nodes at the time of t as (CT_{ij} (t)) as shown in the equation as follows:

$$T^i(t+1) = \alpha \times BT_j^i(t) + (1-\alpha) \times CT_j^i(t), 0 \le \alpha \le 1, t_1 \le t \le NOW \quad (7)$$

Also this model incorporates Gaussian fuzzifiers for estimating membership values of the number of packets transmitted by each node using the eq. 8. Based on the knowledge of domain experts, input parameters (Low, Low-Medium, Medium and High) as well as output parameters (Low, Low-Medium, Medium and High) are selected:

$$\mu_{Trust-value}(X) = e^{\left(\frac{-(x-c)^2}{2\sigma^2}\right)} \quad (8)$$

The range of fuzzy value for each linguistic variables of trust parameters is shown in Table 1. Fuzzification process begins with the transubstantiation of the given node based trust parameters using the functions that are represented in eq. 8. Both Basic and Current trust of node's related fuzzy membership representation are shown in Fig 1 and 2, respectively.

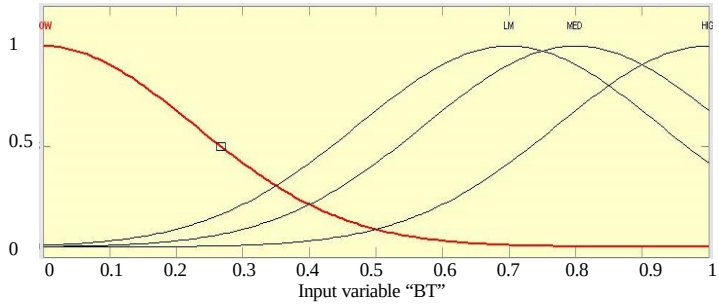

Fig. 2: Fuzzy membership function representation of node's Current Trust (CT)

Table 1: The range of fuzzy values for each input trust parameter Basic Trust (BT), Current Trust (CT) and path-trust

Linguistic variables	Fuzzy values	Symbols
Low	0.0= z = 0.4	LOW
Low-medium	0.3 = z = 0.6	LM
Medium	0.5 = z = 0.8	MED
High	0.7 = z = 1.0	HGH

Table 2: FES based trust estimation of nodes and its trust classes

NODE	BT	BT_MF	BT_LTM	CT	CT_MF	CT_LTM	TV	TV_MF	TRUST_CLS
N1	0.98	0.681849	MED	0.804	0.941919	HGH	0.892	0.819655	MED
N2	0.984	0.671108	MED	0.84	0.877001	HGH	0.912	0.76934	MED
N3	0.966	0.718986	MED	0.891	0.755925	MED	0.9285	0.725373	MED
N4	0.795	0.999009	HGH	0.907	0.713284	MED	0.851	0.908152	MED
N5	0.961	0.732033	MED	0.873	0.80169	MED	0.917	0.756218	MED
N6	0.911	0.852302	HGH	0.852	0.851118	HGH	0.8815	0.844413	HGH
N7	0.754	0.990311	HGH	0.975	0.524318	LMD	0.8645	0.881575	MED
N8	0.372	0.17909	LOW	0.433	0.391793	LMD	0.4025	0.252918	LOW
N9	0.977	0.689871	MED	0.773	0.979677	HGH	0.875	0.859074	MED
N10	0.925	0.820922	HGH	0.852	0.851118	HGH	0.8885	0.828048	HGH
N11	0.333	0.12746	LOW	0.277	0.112574	LOW	0.305	0.107043	LOW
N12	0.819	0.98847	HGH	0.73	0.999992	HGH	0.7745	0.996703	HGH
N13	0.923	0.825533	HGH	0.846	0.864295	HGH	0.8845	0.83747	HGH
N14	0.937	0.792451	MED	0.715	0.99786	HGH	0.826	0.949458	MED
N15	0.437	0.294878	LOW	0.361	0.235038	LOW	0.399	0.246115	LOW
N16	0.652	0.836519	MED	0.497	0.562255	LMD	0.5745	0.694499	LMD
N17	0.963	0.72683	MED	0.885	0.771475	MED	0.924	0.737544	MED
N18	0.652	0.836519	HGH	0.634	0.907792	HGH	0.643	0.867305	HGH
N19	0.628	0.779817	MED	0.702	0.99215	HGH	0.665	0.911407	MED
N20	0.935	0.797287	MED	0.839	0.879071	HGH	0.887	0.831603	MED
N21	0.872	0.926678	HGH	0.919	0.680443	MED	0.8955	0.81113	MED
N22	0.337	0.132171	LOW	0.244	0.080896	LOW	0.2905	0.092537	LOW
N23	0.939	0.78758	MED	0.885	0.771475	MED	0.912	0.76934	MED
N24	1	0.627781	LMD	0.967	0.546446	LMD	0.9835	0.571087	LMD
N25	0.575	0.640932	LMD	0.528	0.649018	MED	0.5515	0.629911	LMD

RESULTS AND DISCUSSION

The proposed model combines both global as well as local based trust optimization and provides acceptable and accurate prediction of malicious nodes and path recommendation. The simulation of this model has been carried out using NS-2 simulator version 2.3.5. In the simulation model, there are 25 (N_1 to N_{25}) WSN placed in a 500x500 square meter area. All nodes have equal energy of 1 Joule at the start of the simulation.

The simulation times were set to 1 h to 1 h 30 min. All the nodes are set as dynamic nodes (Base stations are stable i.e., no Mobility). In this research, 25 nodes are used for trust estimation process. The node representation starts from N_1 to N_{25}. From these nodes, Basic Trust (BT) value and Current Trust (CT) value are calculated. The Node trust (NT) values are shown in Table 2 which contains all nodes information. From these values, we determine the membership value of the same using the Gaussian fuzzy membership function. In crisp set approach, minimum threshold value is assumed as 0.4.

If the trust value is greater than threshold value, it is represented as 0 i.e., trusted node and if it is less than threshold value then it is represented as 1 i.e., untrusted node (malicious node) in crisp set Table 2. Even though the crisp set values are accurate but they don't explain

anything about the range of trust values. In order to overcome this dynamism of truth value, we form and use fuzzy rules to make low, low medium, medium and high values. Fuzzy rule values are more accurate than the crisp set value which does not provide anything about range of trust value. With help of fuzzy expert system, trusted path is established for transferring data from source to destination. Hence, fuzzy rule based trust evaluation model produces a better, accurate, reliable outcome than existing approaches.

CONCLUSION

In this research study, a completely new dimension of representation in fuzzy expert system based trust model through heuristic approach is proposed to measure the trust of nodes. This newly proposed model furnishes versatility and feasibility to select a better node altogether based on the trust constraints and energy consumption. For further work, we have a tendency to incorporate other influencing imputes to the trust model in order to enhance the accuracy of this proposed model.

ACKNOWLEDGEMENTS

One of the researchers K. Selvakumar is thankful to the UGC, New Delhi India, for funding through UGC-BSR fellowship to carry out this research work.

REFERENCES

Aivaloglou, E. and S. Gritzalis, 2010. Hybrid trust and reputation management for sensor networks. Wireless Networks, 16: 1493-1510.

Akkaya, K. and M. Younis, 2003. An energy-aware QoS routing protocol for wireless sensor networks. Proceedings of the 23rd International Conference Distributed Computer System, May 19-22, 2003, Providence, Rhode Island, pp: 710-715.

Bao, F., I.R. Chen, M.J. Chang and J.H. Cho, 2012. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE Trans. Network Service Manage., 9: 169-183.

Crosby, G.V., N. Pissinou and J. Gadze, 2006. A framework for trust-based cluster head election in wireless sensor networks. Proceedings of the 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems, April 24-28, 2006, Columbia, MD., USA., pp: 10-22.

Deng, H., Y. Yang, G. Jin, R. Xu and W. Shi, 2010. Building a trust-aware dynamic routing solution for wireless sensor networks. Proceedings of the Global Communications Conference, December 6-10, 2010, Miami, FL., USA., pp: 153-157.

Forghani, A. and A.M. Rahmani, 2008. Multi-state fault tolerant topology control algorithm for wireless sensor networks. Proceedings of the 2nd International Conference on Future Generation Communication and Networking, Volume 1, December 13-15, 2008, Hainan Island, China, pp: 433-436.

Leligou, H.C., P. Trakadas, S. Maniatis, P. Karkazis and T. Zahariadis, 2012. Combining trust with location information for routing in wireless sensor networks. Wireless Commun. Mobile Comput., 12: 1091-1103.

Lopez, J., R. Roman, I. Agudo and C. Fernandez-Gago, 2010. Trust management systems for wireless sensor networks: Best practices. Comput. Commun., 33: 1086-1093.

Poolsappasit, N. and S. Madria, 2011. A secure data aggregation based trust management approach for dealing with untrustworthy motes in sensor network. Proceedings of the International Conference on Parallel Processing, September 13-16, 2011, Taipei City, pp: 138