International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

# Trust Model for Secure Routing and Localizing Malicious Attackers in WSN

[1] Navami Patil G M [2] Dr. P I Basarkod
Department of Electronics and Communication
REVA Institute of Technology and Management, VTU, Bengaluru, India
[1]navamipatil92@gmail.com, [2]basarkod@revainstitution.org

***Abstract:*** **the principle venture resist through remote sensor systems is security. Acknowledge as valid with models had been nowadays guided as a productive security way for WSNs. In this errand, it prompt a trust model for secure directing and restricting malignant assailants in WSN. To start with, report conviction, vitality conviction and data acknowledge as valid with are mulled over at some stage in the estimation of direct consider. Moreover, if the source and destination hubs are far away, then exhortation and diagonal concur with are figured. Consider consistency and consideration are characterized to reinforce the rightness of exhortation conviction. Malignant hubs might be related to low conviction values that is distinguished in direct and proposal concur with figuring. The proposed model can think about constancy of sensor hubs more prominent effectively and maintain a strategic distance from the security breaks additional accurately**

***Keywords*— Security, Routing protocols, Belief levels**

## I. INTRODUCTION

WSN's are developing advances that have been extensively used as a part of various congruity , for instance, crisis reaction, restorative administrations checking, fight zone recognition, environment watching, action association. This expect inspected the sorts of hypothesis estimations used to deal with the strikes by checking firm activities of framework. It tells methods for building conviction model. It moreover looks at present proposition models used as a piece of different fundamental initiative method of remote sensor frameworks.

### *1.1 Conceptual Diagram*

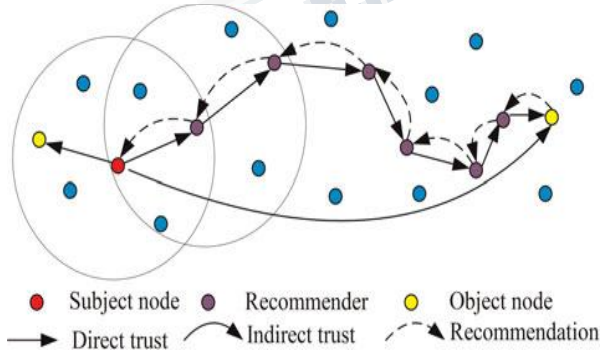


***Fig. 1. The network structure.***

## II. PAPER ORGANIZATION

This paper is organized into eight parts. Part 1gives a general idea of Trust Model. Part 2 is about literature survey. Part 4 describes the objective of the paper. Part 5 gives the scope of the work. Part 6 gives the methodology used to solve the problem. Part 7 gives derived results and followed by conclusion and future works.

## III. OBJECTIVE

To set up safe connections, we want to assure that all intertwining nodes are believed. This shows the reality that it is noteworthy to set up a belief model making a sensor node to deduce the reliability of other node.

## IV. SCOPE OF THE WORK

The conviction structure has end up wide for horrendous center points reputation in WSNs. It can control in piles of hindrances which join safe coordinating, secured substances add up to, and relied on upon key switch. Due to the remote natures of WSNs, it fancies a scattered trust adjustment with none center point, in which neighbor center points can check each other. Absolutely, a fit agree with model is fundamental to hold consider related in estimations in a shielded and persisting way.

## V. PROPOSED WORK

In this project, Firstly try to know all the trust values and by adding those trust values, finding a shortest path for transaction to take place.
The communication trust is measured by,

$$T = \{b, d, u\}$$

The verbal exchange trust Tcom is measured primarily based on a hit (s) and unsuccessful (f) verbal exchange packets:

$$T_{com} = \frac{2b + u}{2},$$

where $b = \frac{s}{s+f+1}$, $u = \frac{1}{s+f+1}$.

The energy trust is measured by:

$$T_{ene} = \begin{cases} 1 - p_{ene}, & if\ E_{res} \geq \theta, \\ 0, & else, \end{cases}.$$

The data trust is measured by,

$$T_{data} = 2\left(0.5 - \int_{\mu}^{v_d} f(x)\, dx\right) = 2\int_{v_d}^{\infty} f(x)\, dx.$$

By combining all these trust values,

$$T_{n-direct} = w_{com}T_{com} + w_{ene}T_{ene} + w_{data}T_{data},$$

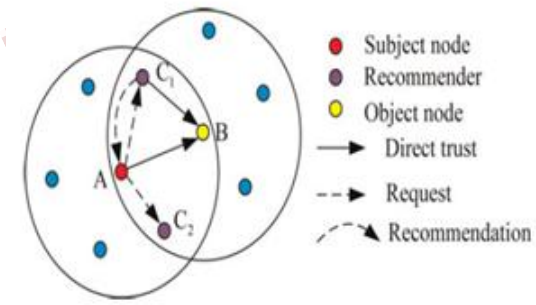


*Fig. 2. Calculation of Recommendation Trust*

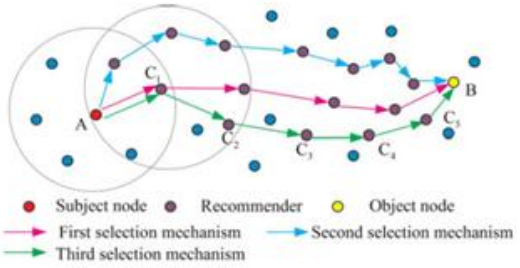


*Fig. 3. Calculation of indirect trust*

As an enhancement, while finding the route for transaction by the belief values it can also find the malicious node and can omit that. Means that node cannot removed from the network but it can localized to the other nodes as malicious and can inform not to use that node for further process.

## VI. RESULT AND ANALYSIS

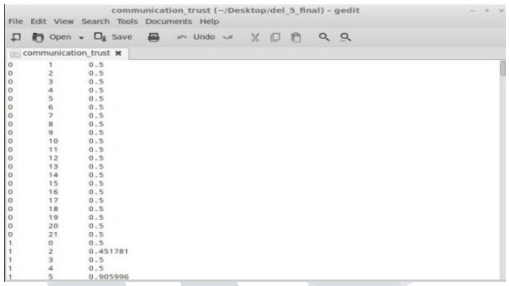

*Fig. 5: Communication trust values*

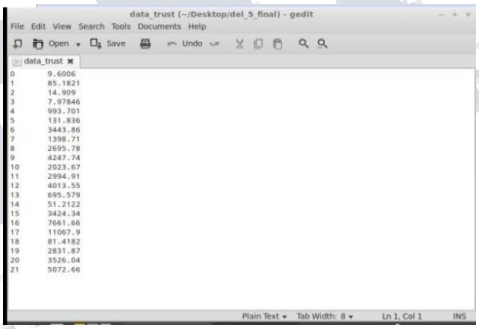

*Fig. 1: Data trust values*

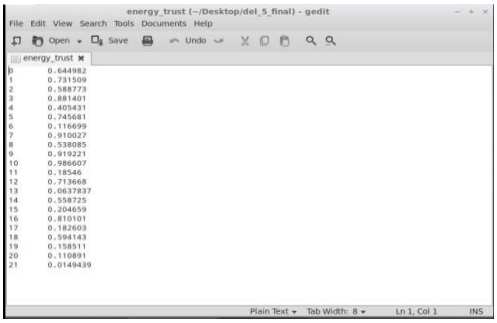

*Fig. 2: Energy trust values*

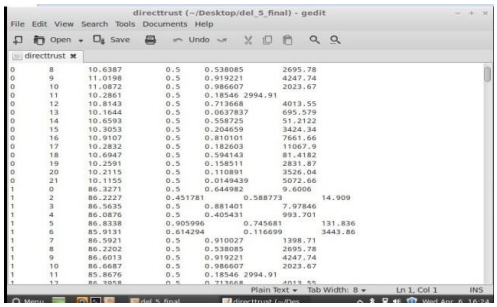


*Fig. 3: Direct trust values*

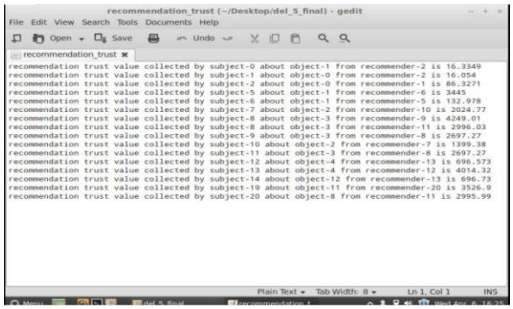


*Fig. 4: Recommendation trust values*

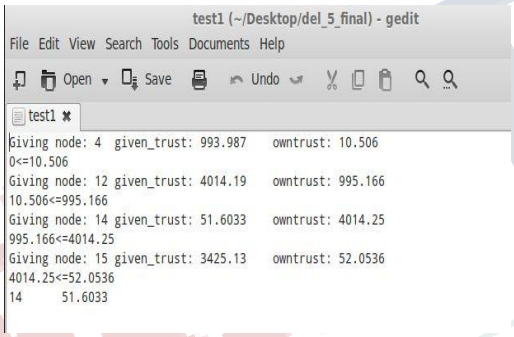


*Fig. 5: Indirect trust values*

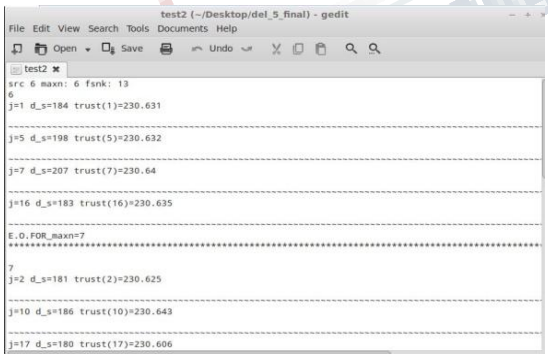


*Fig. 6:Indiect trust calculation*

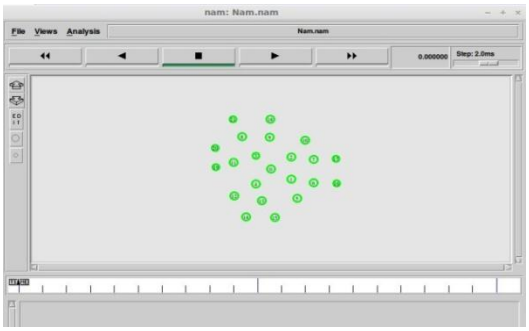


*Fig. 7:Network setup*

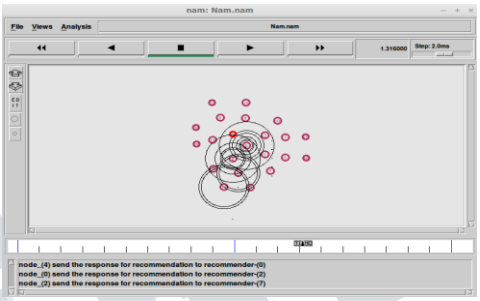


*Fig. 8: Choosing for shortest path on the basis of trust values*

Figures 5,6,7,8,9,10,11 shows the direct, recommendation and indirect trust values. Figure 12 shows the network setup and figure 13 shows the selection of route from the belief values measured.

## VII. CONCLUSION

Trust model for secure routing is built by the trust values and the path is traced. As an enhancement detecting and localizing of malicious node is also done. The node which is having the lowest belief value is considered as the malicious node. Choosing the recommenders based on their trust value so can eliminate the malicious node taken as the recommender.

## REFERENCES

[1] Jinan Jiang, Guangjie Han, Feng Wang, Lei Shu, Member, IEEE, and Mohsen Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks" Fellow, IEEE Transactions on Paralel and Distributed Systems, vol.26, no 5, may 2015.

[2] H. Chan and A Perrig, "Security and privacy in sensor networks," Comput., vol. 36, no. 10, pp. 103–105, Oct. 2003.

[3] Y. M. Huang, M. Y. Hsieh, H. C. Chao, S. H. Hung, and J. H. Park, "Pervasive, secure access to a hierarchical-

based healthcare monitoring architecture in wireless heterogeneous sensor networks," IEEE J. Sel. Areas Commun., vol. 24, no. 7, pp. 400– 411, May 2009.

[4] V. C. Gungor, L. Bin, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

[5] G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, "Managements and applications of trust in wireless sensor networks: A Survey," J. Comput. Syst. Sci., vol. 80, no. 3, pp. 602–617, 2014.

[6] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation based framework for high integrity sensor networks," in Proc. 2nd ACM Workshop Security Ad Hoc Sensor Netw., 2004, pp. 66–77

[7] Z. Yao, D. Kim, and Y. Doh, "PLUS: Parameterized and localized trust management scheme for sensor networks security," in Proc. IEEE Int. Conf. Mobile Adhoc Sensor Syst., 2008, pp. 437–446.

[8] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory," Sensors, vol. 11, pp. 1345–1360, 2011