International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

TRUST-BASED HIERARCHICAL TRUST ALGORITHM FOR WIRELESS SENSOR NETWORK

Sheera sahari,prasanna.P[1],
Maragatharajan.M[2],
[1]Post Graduate Student, [2]Assistant Professor,
Department of Information Technology,
Kalasalingam University,
Krishnankoil,Tamil Nadu, India.
sheera15041995@gmail.com ,
maragatharajanm@gmail.com

May 29, 2018

Abstract

Now a days, the Wireless Sensor Networks (WSN) usage is increased because of its broad application. Providing security is a crucial issue in wireless sensor network. Trust management provides security to sensor nodes in wireless sensor networks. This paper presents a Trust-based Hierarchical Trust Algorithm for Wireless Sensor Network (TBHTA-WSN), which is based on Interactive Trust, Honesty Trust, and Content Trust. The main objective of this paper is to reduce the chance of misleading of nodes and reduce the routing overhead using trust level. The proposed method is implemented using MATLAB and the simulation results shows that the malicious nodes are identified and avoided, by which we can enhance the security of WSN effectively.

***Key Words*:**Wireless Sensor Network, Hierarchical Trust Algorithm, security in routing, Trust model, Cluster architecture.

1 Introduction

Wireless Sensor Network (WSN) is implemented in many applications such as health care, Industries and Military applications. In WSN, Sensor nodes (SN) are deployed in larger region which collects and send information to base station through wireless medium.SN can act as both transmitter and receiver. Each SN deployed in wireless has energy, limited computing and communication power. The major challenges facing is security, since sensor nodes are deployed in open atmosphere, which results in exposing to various attacks. So it is necessary to provide security to the nodes by adapting trust mechanism, which works based on the trust value of the neighbor nodes. Trust is not stable and it varies event to event. Trust mechanism identifies the malicious nodes based on the behavior, reputation and trustworthiness of node. Trust value is calculated and behavior, reputation and trustworthiness of node is determined by comparing with threshold value. The trust model reduces the route overhead by providing secure routing in wireless sensor network and it is allows trustworthy nodes to communicate and block the access of untrustworthy nodes to the network .The purpose of trust is to set up a secure transformation on the one node to another node.

The rest of paper is structures as follows: section II gives an overview of related works. Section III explains trust mechanism of the proposed method. In section IV, result of the proposed work is analyzed. Finally, conclusion and future work presented in section V.

2 RELATED WORKS

Trust has been broadly used in wireless sensor network for accessing possibility, scalability and providing security for the nodes. For example, the check whether the node is malicious or not. Many research works has been carried out for providing security by adapting trust mechanism in WSN. Few works are discussed in this section.

Liu et al[2]proposed for trust model, which uses Active Detection routing protocol to avoid the block hole attack. Zhang et al[3] proposed Bio Inspired Trusted Routing Framework (B-ITRF) model to access the neighbor behavior in real time. B-ITRF combines Trust assessment, Ant colony Optimization, physurum Auto-

nomic optimization for evaluating the trust behavior of node. Adel et al[4] proposed a new trust model to secure routing protocol, which used a Box plot theory to detect a Denial Of Service (DOS) attack. The trust can be measured in three ways like the experience of the node and recommendation of the neighbor node then the old value of the trust. Mohamed et al [6] proposed Trust based Energy Aware Incentive Routing protocol, which encouraged the nodes cooperation and established the stable route. This protocol not only cooperate the node but also provide the high packet delay ratio.

Xia et al[7] proposed a Dynamic Trust Prediction Model, which computes trust based on historical trust, node current trust and route trust. The trust-based source routing protocol is used for providing a shortest path between the nodes and a packet delivery ratio. Y.L.Sun et al [8] proposed two models namely, Entropy based Trust model and Probability based trust model. The Entropy based Trust model calculated the trust value directly and the Probability based trust model calculated the multipath trust propagation using probability values of the trust relationship. Fenyo Bao et al[9] proposed for a hierarchical trust management protocol, which learned from past experience and adapted to changes of the environmental conditions. Thus, it increased the performance of application.

3 PROPOSED WORK

In proposed work, the cluster- based WSN is considered as multiple clusters environment. Cluster Head(CH) of each cluster have maximum energy when compared with other SN in the cluster. In this section, network assumption, cluster formation, cluster head selection. Hierarchical Trust Algorithm for trust calculation and Intrusion Detection System are described. Figure 1 shows the deployment of sensor node in TBHTA-WSN using MATLAB simulator.

A) Assumption

1. Sensor Nodes (SN) are deployed in Cluster-based WSN.

2. SNs are grouped to form a cluster which has unique SN ID and energy.

3. SN are fixed in position after deployment.

4. Network is equipped with Base Station (BS).

5. SNs are energy constraint and can broadcast information to CH. CH can broadcast the information to the Base Station (BS) directly or to another CH.

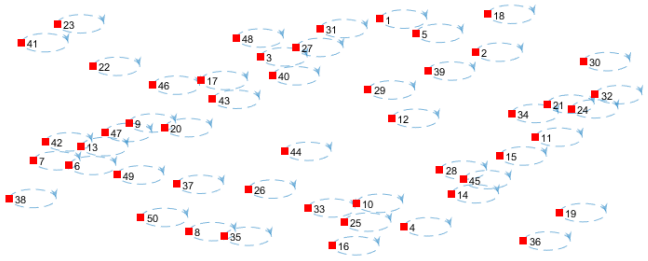

Figure 1: Deployment of sensor node in TBHTA-WSN

B) Cluster Formation

After the deployment of SN, the process is the formation of cluster, which contains the group of sensor nodes. Sensor nodes are grouped based upon the distance measurement. SNs which are nearer to each other forms a cluster.

C) Cluster Head Selection

The Cluster Member(CM) exchanges the information or message their Cluster Head (CH) and CH will send it to BS. All the sensor nodes have initial energy to transfer the information to one node to another node. CH have a significant impact on lifetime of network. In each round of communication CH needs to be selected. Wrong selection of CH reduces the energy consumption, which minimize the lifetime of network. In this paper, node with highest energy is selected as a Cluster Head (CH).

D) Hierarchical Trust Algorithm

In (TBHTA-WSN), Hierarchical Trust Algorithm is used for trust calculation based on Multidimensional trust evaluation process. The upper level trust denotes the communication between CH-CH. The lower level trust denotes the communication between CH-SN. Hierarchical Trust Algorithm is applicable for Multidimensional perceiving data and stable for Multidimensional trust in cluster-based wireless sensor networks. In the proposed work social metric trust namely honesty trust, content trust and interactive trust is used. The malicious node can be easily identified and

blocked based on the trust value. Figure 2 shows the flow chart of TBHTA-WSN.

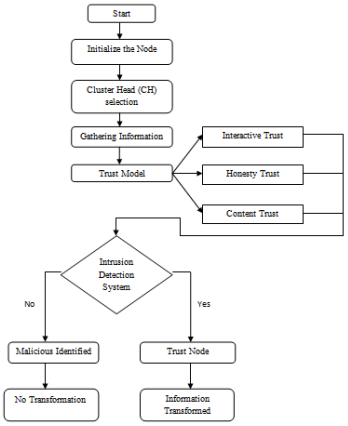

Figure 2: Flow chart of TBHTA-WSN

In upper level trust evaluation, CH evaluates the trust level of other SNs in the same cluster and other CHs of network. In lower level trust evaluation, each SN evaluates the trust level of other SNs within same cluster and send the value to CH of that cluster [5].

Algorithm for calculating trust value is given below:

```
Algorithm – Trust Value Calculation
Input : Sensor Nodes (SNode);                    Output: Trust Value of Sensor Node;
Initialize array for Trust nodes &Untrust Node as Trust=[], unTrust=[] ;
Initialize Trust Connection & Un Trust Connection as Tcn, UTcn;
Data Rate (dr) =0;
for (i=1:nc)
snode[i].honestyc<- T_i^honest;
snode[i].interactive<-T_i^interactive;
snode[i].content<- T_i^content;
        if (snode[i].honestyc>-1 &&snode[i].interactive >=1 &&snode[i].content >-1)
        Trust (1,Tcn) = i;  Tcn =Tcn +1;
        dr = dr + snode[i].datarate;
        else
unTrust(1,UTcn) = i;
UTcn =UTcn +1;
    endif;
snode[i]=snode(i,randperm(nc));
endfor;
```

Trust Model

Trust is not stable, and it varies event to event. Each Sensor nodes deployment in wireless sensor network has trust value and is evaluated using social metrics. The overall trust value of a node i to a node j denoted by Tij and calculated by combining honesty trust, content trust and interactive trust of the node. Tij is indicated as a real number and lies in the range of 0 to 1. When a new node arrives, trust value is initially evaluated. Periodically trust value of the node is computed based on the trust components at specific interval of time. The Trust node is calculated as follows:

$T_{ij} = W_1 T_{ij}^{honest} + W_2 T_{ij}^{interactive} + W_3 T_{ij}^{content}$

Where

$W_1 T_{ij}^{honest}$represents the honesty trust between nodes i and j

$W_2 T_{ij}^{interactive}$represents the interactive trust between nodes i and j

$W_3 T_{ij}^{content}$represents the content trust between nodes iand j

w1, w2, w3 are the weights associated with honesty, interactive and context trust respectively and the sum of the weights is always equal to 1 (w1+ w2+ w3 = 1).

Interactive Trust

Interactive Trust is based on the number of interactions between nodes in the network.

The interaction is defined as communication taking place when sending data from one SN to another and receiving data from that destination SN. The SN with greatest number of communications is considered as high trustworthy node. In interactive trust, the malicious node is identified based on the threshold value. The SN communication is compared with the threshold value. If it exceeds the threshold value, then SN is considered as a malicious node and SN will be blocked for further communication.

The Interactive trust is denoted by $W_2 T_{ij}^{interactive}$ is the interactive trust from node i to node j with respect to time t and level of the interaction is the total number of interaction between the nodes i and j Figure 4 shows the communication between CH and SN in a cluster and observed that SN1 is the high trustworthy node since its interaction with CH is 9. Figure4 shows the communication between CH and BS in the whole network

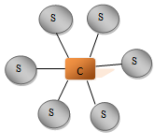

Figure 3:

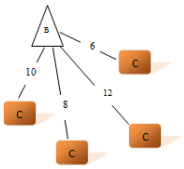

Figure 4:

Figure 3: Interactive Trust Communication between CH and SN

Figure 4: Interactive Trust Communication between CH of all clusters and Base Station (BS)

Honesty Trust The Honesty Trust is based upon the successful and unsuccessful interactions. The interaction is said to be successful when a SN or CH transmits the data successfully to another SN or CH or to BS If the SN or CH failed to transmit the data to another SN or CH or to BS, then the interaction is said to be unsuccessful. The higher ratio of honesty trust value depends upon the number of successful interaction to total number of interaction.The Interactive trust is denoted by $W_1T_{ij}^{honesty}$ Tijhonestyis the interactive trust from node i to node j with respect to time t. The value of $W_1T_{ij}^{honesty}$ is 1 if the node i successfully transmits the data to node j and 0 if unsuccessful. The maximum and minimum value of a node depends upon the successful interaction. The Algorithm for honesty trust is given below:

```
Algorithm – MIN-MAX Trust in SNode
Initialize the minimum and maximum value as maxV,minV;
for i=1 :nc
  if snode[i].successful>0
        if snode[i].trust>maxV
maxV = snodes[i].trust;
         else
minV=snodes[i].trust;
        endif;
endif;
endfor;
```

Content Trust

This Trust model is based on capacity of each node. The Content Trust is observing all the details of the node like energyand how much data is transfer for the other node. In content trust the malicious node is identified based on the capacity. When the node transmits data, it starts consuming energy. A node will become selfish to save energy which leads to reduction of malicious node. The content trust is denoted by $W_3 T_{ij}^{content}$and computed based on energy of a node with respect to time t.

E. Intrusion Detection System (IDS)

In WSN, there are high possibilities of SN prone to attack since SNs are deployed randomly in open atmosphere with minimum energy and limited computational power. So, it is very essential to detect malicious node to prevent the network from attack. If a node is detected as malicious node, then the node is dropped and no further communication from the node will takes place. For detecting malicious node, dynamic threshold value is used in proposed mechanism. The trust value for each node is calculated dynamically and compared with threshold value. When node become malicious, trust value will decrease. If trust value exceeds the threshold value, then node is detected as the malicious node.

4 Experimental Result and Analysis

Our proposed model is implemented using MATLAB and the cluster-based WSN is predefined with 100 Sensor Nodes deployed randomly in 100*100 m2 simulation area as shown in Figure 1.The parameters used to implement our model is listed in Table 1.

Parameter	Value
Simulation time	500s
Deployment Area	100 * 100 m^2
Sensor Nodes	100
Initial Energy	100J
Trust Range	[0,1]
BS Location	(75,75)
Threshold	Varying
Txp	.5
Rxp	0.8

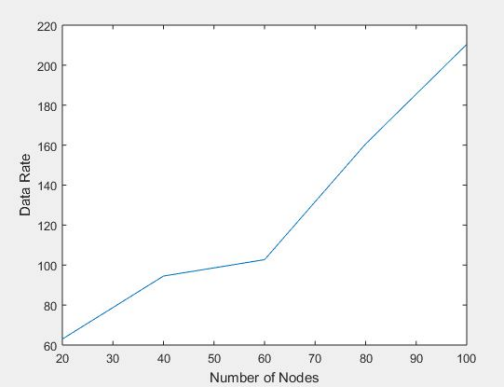

Figure 5: Trust Data Rate of the Sensor Nodes in TBHTA-WSN

Initially, data rate for each node is evaluated and trust value is calculated by using data rate value. The maximum and minimum data rate for a node is taken into consideration for trust value calculation. Figure5 shows the graphical representation of data rate for SN evaluated in the proposed mechanism. Depending on the trust value, most trustworthy devices is found based on the trust components. From the Figure 6, it is observed that most trust device is identified among 100 sensor nodes, which communicates with CH without losing the data that leads to reduction the route overhead and increase the life time of network.

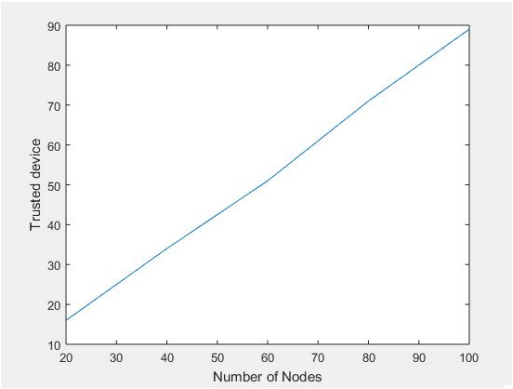

Figure 6: Trust Device in TBHTA-WSN

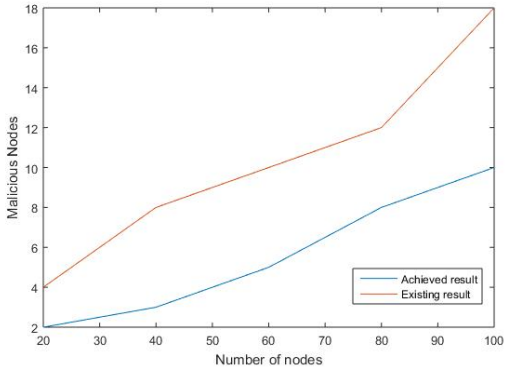

Figure 7: Comparison of Malicious Nodes Vs Number of Nodes

Figure 7 shows the comparison of reduction of malicious node with existing trust model. In proposed method, every SN have initial energy and trust value of a node is evaluated periodically in each round to detect whether the node is malicious. Since the node sends the data or message based on the trust value, node has become trustworthy node and malicious node is reduced.

5 Conclusion

Security has become the major concern in Wireless Sensor Network due to the distributed deployed nature of the network. A Trust-based Hierarchical Trust Algorithm for Wireless Sensor Network (TBHTA-WSN) is proposed to improve the security of the network by evaluated the trust of each node in the network based on honesty, content and interactive trust. Malicious node is identified based on the trust date rate and dynamic threshold value. Simulation results shows that TBHTA identifies the malicious node, most trust devices and reduce the routing overhead effectively, which significantly enhances the security of the network.

References

[1] Danyang qin, Songxiang yang, Shuang jia, Yan zhang, Jingya ma, and Qun ding, Research on Trust Sensing Based Secure

Routing Mechanism for Wireless Sensor Network, IEEE ACCESS,vol. 5, pp. 9599-9609, June.2017.

[2] Y. X. Liu, M. X. Dong, O. Kaoru, and A. F. Liu, ActiveTrust: Secure and trustable routing in wireless sensor networks, IEEE Trans. Inf. Forensics Security, vol. 11, no. 2, pp. 20132027, Sep. 2016.

[3] M.C.Zhang,C.Q.Xu,J.F.Guan,Q.T.Wu,R.J.Zheng,andH.K.Zhang, B-iTRF: A novel bio-inspired trusted routing framework for wirelesssensornetworks,inProc.IEEEWirelessCommun.Netw.Conf.(WCNC), Istanbul, Turkey, Apr. 2014, pp. 22422247.

[4] E. Adel, K. Abdellatif, and E. Mohammed, A new trust model to secure routing protocols against DoS attacks in MANETs, in Proc. 10th Int. Conf. Intell. Syst. Theories Appl. (SITA), Taipei, Taiwan, Oct. 2015, pp. 16.

[5] Reshmi.v, Sajitha.M , A survey on Trust Management in Wireless Sensor Network, International Journal of Computer Science & Engineering Technology (IJCSET) , ISSN: 2229-3345 Vol. 5 No.2 , Feb 2014.

[6] Mahmoud M.E and Shen .X ,Trust-based and energy aware incentive routing protocol for multihop wireless networks, in Proc. IEEE Int. Con Commun (ICC),Budapest,Hungary,Jun.2008.pp88-91.

[7] H. Xia, Z. Jia, X. Li, L. Ju, and E. H. M. Sha, Trust prediction and trustbased source routing in mobile ad hoc networks, Ad Hoc Network., vol. 11, no. 7, pp. 20962114, 2013.

[8] Y. L. Sun, W. Yu, and Z. Han, Information theoretic framework of trust modeling and evaluation for ad hoc networks, IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 305315, Feb. 2006.

[9] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho, Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection in IEEE Transactions on network and service management, vol. 9, no. 2, pp.169183,2012.