IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

A Leverage Based Trust Scheme for Wireless Sensor Networks

M.Ranjitha[1], R.Gopal[2]

PG Student, Department of CSE, Chettinad College of Engineering & Technology, Karur, India[1]

Assistant Professor, Department of CSE, Chettinad College of Engineering & Technology, Karur, India[2]

Abstract: Various technologies enable the development of large scale sensor networks in a variety of fields. Sensor networks are placed in lot of secured decision making areas. The data collected from it must be trustworthy. In existing system the security mechanism for wireless sensor networks is not present accurate and so we cannot achieve secured trust models. There are several trust models available, but still there are various kinds of attacks on the network. Trust is a dynamic phenomenon which changes along with time and environment conditions. However, most existing trust models do not solve the trust dynamic problem to overcome that a (Leveraging Trustworthiness Topology) LTWT has been proposed which is more trustworthy and prevent the security more effectively.

Keywords: wireless sensor networks, leveraging, trustworthiness, trust models.

I. INTRODUCTION

The technological development in various fields leads to the importance of Wireless sensor networks. It is used widely in all applications such as Healthcare, Military, Satellites and in Agriculture. Hence it allows a large ways for the trespassers to affect the network in different ways and so achieving security in WSN is one of the challenging tasks.

Several security mechanisms are used in WSN to avoid the security threats such mechanisms are cryptography, authentication, confidentiality and message integrity. However, the above approaches are not protective enough and so various attacks happen in the network. Present security mechanisms help with the external attacks, but the internal attacks affect the nodes easily. To establish a secured networks various trust models are developed in order to protect the network from attacks.

Nowadays, many researchers have developed trust models to build a secured sensor node[2]. For example [5] Dynamic source routing (DSR) technique was introduced for secure transmission which prevents the intruders from finding the secure path between the source and destination for the trust model of the network. It has various techniques to perform the operation such as Watchdog and pathrater. Node behavioral strategies Banding belief theory of the trust Evaluation algorithm (NBBTE) are proposed, [8] which integrate the approach of nodes behavioral strategies and modified evidence theory. According to the behaviors of sensor nodes, a variety of trust factors and coefficients related to the network application are established to obtain neighbor and remote trust values by leaving a weighted average of trust factors. Meanwhile, the fuzzy set method is applied to form the basic input vector of evidence. On this basis, the evident difference is calculated between the remote and neighbor trust values, which link the revised D-S evidence combination rule to finally synthesize integrated trust values of nodes. NBBTE establishes various trust models based on the communication behavior and it takes the transmission of packets.

From the above research work it is clearly known that the present technique is based on the following aspects

a) The communication point plays a main role in assessing the trust values of the sensor nodes and it also includes energy level. b) Obtaining trust assessment from the non neighbor nodes is also important it is done in proposed system based on the recommendations from other nodes. c) The trust assessment is obtained only for the neighbor nodes, but trust values for the non neighbor nodes is also important to obtain a protective network. d) In WSN the trust is a dynamic phenomenon since it changes based on the time and the environment to avoid this problem we propose the LTWT trust model.

II.OVERVIEW OF LTWT

Trust between the nodes in the wireless sensor network is a challenging field. In general trust means belief between the nodes. It is used to identify the misbehavior nodes and provide belief between the nodes. In this paper trust value changes from zero to one. One means trusting and zero means untrusted.

Neighbor trust :It defines the straight communication between the neighbor nodes .

Proposal trust : the proposal from other nodes are not safer,inorder to obtain a perfect information the proposal trust is used to calculate.

Remote trust : remote trust implies the oblique communication between the nodes.If node one wants to pass a message to node four, remote trust is used.

III.STRUCTURE OF LTWT

In this section it has two main components : one hop trust and multi hop trust.In one hop trust if a soruce node wants

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

to gain the belief of destination node , it first checks whether the destination node ID is present in the neighbor list. If it has been present then it is used or the multi hop trust is checked with the proposal gained.

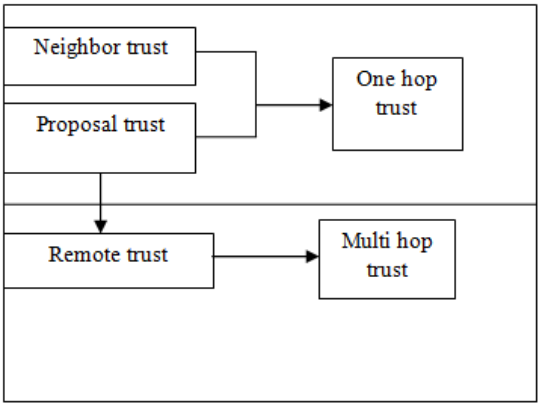

Fig 1.Structure of LTWT

IV.TRUST CALCULATION IN LTWT

Calculation of Neighbor Trust

The neighbor trust can be achieved from transmission trust, power trust and information trust. During the transmission the loss of information between the nodes is possible, so the energy level of the data is reduced it is due to malicious node, power level is used to detect the node capability.

Calculation of Transmission Trust

In this sending of packets takes place by reviewing to the already how many successes of packets has been received from that node .To clear that doubt I have used the subjective logic framework [9]. The value present in it is T ={c,m,i} here c,m and i implies to certainty,mistrust and insecurity, c,m,i ϵ [0,1]; c+m+i=1.Trust [6] calculated based on successful and unsuccessful transmission packets is given as

$$T_{trans} = \frac{2c+m}{2}; \text{ where } c = \frac{a}{a+b+1}, \; m = \frac{1}{a+b+1}$$

Calculation of power trust

Power is the main metric for the sensor nodes.If the power level decreases in a high level ,then the malicious attacks take place.here energy threshold is defined as t.Power trust is obtained based on the energy consumption rate $p_{pow}, p_{pow} \epsilon [0,1]$.power trust is calculated as $T_{pow} = 1-p_{pow}$; if $E_{res} \geq t$,where p_{pow} is determined based on the ray projection method[3].The power gained by the destination node in n previous time slot $p_{pow}=\{p_{pow}(1);p_{pow}(2);\ldots\ldots p_{pow}(n))$ and the current time slot is $p_{pow}(n+1)$,according to ray projection method. The change of power at each time slot is $s_i=p_{pow}(i)-p_{pow}(i-1)$, where i=2,3,….n.

Calculation of the information trust

In this paper data send between the nodes is received without any loss of data.the distribution of data here is considered as normal distribution[7],[4],for the set of data th pdfis $g(x)=1/s\sqrt{2q}\iiint e^{(x-m)2/2s2}$, where x is attributed ,m is mean,s is variance .The mean of the data is used to reflect value similarityof the data,mean is supposed to have highest belief value.the Trust value of data defined as $T_{info}=2_{vd}{}^{z}{}_{\infty} f(x)\, dx$.

Depend on the transmission T_{trans} ,the power T_{pow},and the information trust T_{info}, we receive the neighbor trustbetween the nodes.

$T_{u\text{-}neighbor}=W_{trans}T_{trans}+W_{pow}T_{pow}+W_{info}T_{info}$,where W is the weight values.$W_{trans} \; \epsilon[0,1], W_{pow} \epsilon[0,1], W_{info} \epsilon[0,1]$ and $W_{trans}+W_{pow}+W_{info}=1$.

Calculation of the Proposal trust

There is no direct communication between source and destination node in proposal trust.to obtain the positive proposal is a challenging task since it plays main role in calculating the trust.

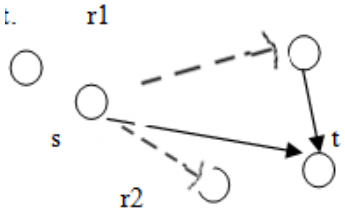

Fig 2.Calculation of proposal trust

Calculation of proposal trustworthiness

In this calculation the proposal received from the other recommender is verified whether it is correct or not ,that verification is done with several detection schemes.I consider the trustworthiness to calculate $T_{trus.}$

$$T_{trus}=1-|T^{t}_{r1}-T^{t}_{ave}|$$

Where T^{t}_{r1} is the proposal degree of destination node t given by recommender r1andT^{t}_{ave} is the regular value of all proposals.

Calculation of Proposal familiarity

The familiarity of the proposal depends on a long term of a neighbor node.The node with longer life time will have a high belief value.

$$T_{pf}= num^{t}_{r1}/num_{r1}*a^{1/numt}{}_{r1}$$

where num^{t}_{r1} is the successful transmission between proposals. The proposal trust is established as P

$$T_{u\text{-}pro}= \frac{i^{u}{}_{=1+Tr1}{}^{t}{}_{0.5}*T_{trus}*T_{pf}}{U}$$

where u is the recommender

Calculation of remote trust

When there is no direct communication between the source and the destination nodes remote trust is determined. In remote trust it has two steps in it.firstit check for the multi hop recommenders,then it findsthe trust continuity by using the recommenders. The path from the source node and destination node is achieved by the proposals it is called as Trust Line.

$T_{n\text{-}remote}(^{t}_{r1}) = (T_{r1}*T_{r1}{}^{t}$; if $T_{r1}{}^{t}<0.5$
$0.5+(T_{r1}-0.5)*T_{r1}{}^{t}$; else;
$\sum T_{r1+1} * T_{n\text{-}remote}(r1^{t})$;

$T_{n\text{-}remote}(r1^{t}) =$ if $T_{n\text{-}remote}(r1^{t}) < 0.5$
$\sum 0.5+(T_{r1+1}- 0.5)*T_{n\text{-}remote}(r1^{t})$; else

DOI 10.17148/IJARCCE.2016.53199

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

V.SIMULATION RESULT AND ANALYSIS

This experiment has been done using the matlab. Here we evaluate the performance of LTWT using different parameters .The malicious node detection is done. In this it has 100 sensor nodes has been placed in a sensing area. A different ways have been present to detect the malicious nodes.

Performance of LTWT: Selection of Threshold Th

In order to save an energy a threshold of transmission packets Th is used .It is considered as a save energy because if a source and a destination node has higher value than the Th only the neighbor trust takes place.The other power,transmission are saved. In initial malicious node are set as 10 percent.As in fig 3 & 4 we observe that the trust value of safer node is 1 and harmful node is close to 0.

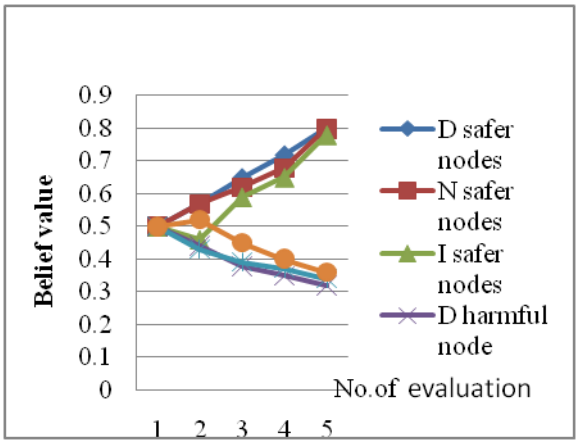

Fig 3.Transmission Packets are higher than threshold

Fig 3the result of the destination trust value (D – trust),neighbor trust value(N-trust),integrated trust value(I trust)of safer and harmful nodes have been given.and calculating neighbor trust is done efficiently.

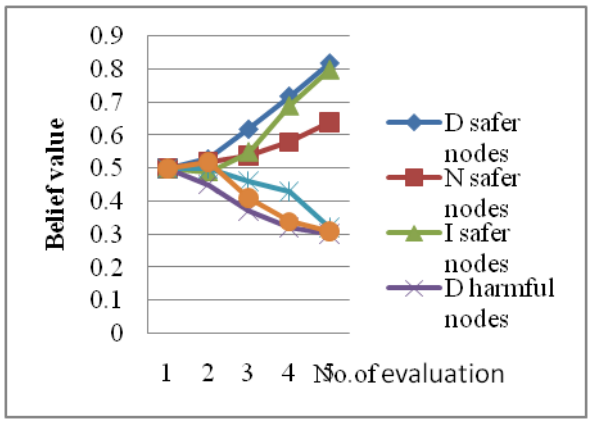

Fig 4. Transmission packets are lower than threshold

In fig 4 when the transmission packets between the neighbor and destination nodes are lesser than the Th. The integrated trust values are closer to destination trust values compared with the neighbor trust value. When the transmission time is small,it is hard to differentiate safer nodes and harmful nodes due to certain forwarding attack.

Fig 5 shows the similarity between the trust value and transmission packets threshold Th.The X axis represent the total mean of transmission packets.If a packets changes from 0 to 1000 then the trust value also changes in several ways.If a packet is below 400 then it has Th = 40%.while it exceeds 400,if choosing Th= 60%.However the selection of trust value for an destination node with transmission node is done .

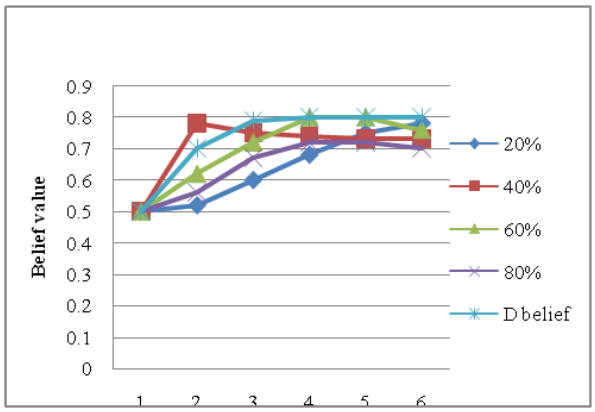

Fig 5. Similarity between belief value and transmission packets

choosing the weight value

By combining the neighbor trust and proposal trust the value is concluded.The correct weight value is collected from the nodes.the percentage of harmful node vary from 6 percent to 55 percent.If more harmful nodes have been present then the trust value will be low. In fig 6 the trust value comes low when there is increase in harmful nodes. Calculating weight value is done based on the recommendation ,trust value lowering leads to more involvement of harmful node.The correct selection of weight value in different environment need further research and I not used in this paper

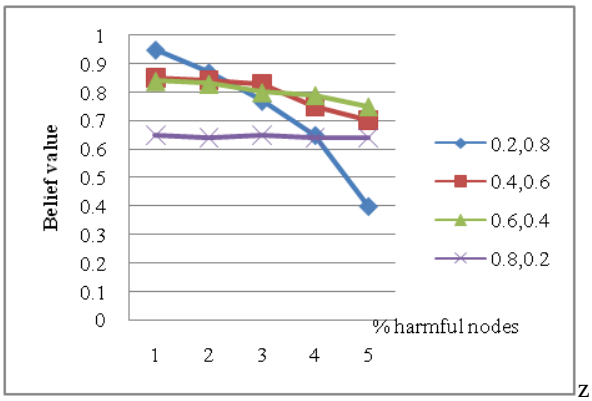

Fig 6. Effect of weight value

Selection of trust update time cycle

Dynamically the trust value needs to be updated.If it is not done a lot of energy waste will be present. Here we have compared the experiment with and without harmful nodes.For true trust values the update time should be long and for the other the time should be small.

VI.CONCLUSION

The attacks happening in the wireless sensor network are inevitable and so the trust model is most important.Sincethe wireless sensor network is a wireless

environment it should have a trust model in all nodes so that the attacks can be detected properly.In this paper, a Leveraging Trustworthiness topology was proposed.In LTWT the calculation of neighbor trust,proposal trust and remote trust are taken .Simulation result show that LTWT is very effective and attack resistant.But untill now selection of correct weight value and threshold is a challenging one which will be discussed in future research.

REFERENCES

[1] E.Elnahrawy and B.Nath,"Cleaning and querying noisy sensors,"in proc.2nd ACM Int.Conf.Wireless Sens.Netw.Appl., 2003,pp.78-87

[2] G.Han,J.Jiang,L.Shu,J.NiuandH.C.Chao,"Managements and applications of trust in wireless Sensor networks:ASurvey,"*J.Comput.Syst.Sci.*,vol.80,no.3,pp.602-617,2014.

[3] H.S.Lim,Y.S.Moon,and E.Bertino,"Provenance based trust worthiness assessment in sensor networks,"in *proc.7th Int.work-shop Data Manage.Sens.Netw.,2010,pp.2-7*.

[4] K.Shao,F.Luo,N.Mei/and Z.Liu,"Normal distribution based dynamical recommendation trust model,"J.Softw.,vol.23,no.12,pp.31 30-3148,2012

[5] Kulreja,D Sch.of inf &common.Technol.,Guru Gobind Singh Indra Prastha University (GGSIP), NewDelhi,India,Miglani.M Reddy,B.V.R.,IEEE trans 20-21 Feb 2014.

[6] M.Chen,Y.Zhou,and L,Tang, "Ray projection method and its applications based on Grey Prediction,"*Chinese J.Statist.Decision*,vol.1,p.13,2007.

[7] M.Rabbat and R.Nowak, "Distributed optimization in sensor network," *in proc.3rd Int.Symp.Inf.Process.sens.Netw.,2004,pp20-27*

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

[9] W.Gao,G.Zhang,W.Chen,and Y.Li,"A trust model based on subjective logic," in Proc.4th*Int.Conf.InternetComput.sci.Eng.*, 2009,PP.272-276.