An improved light-weight trust model in WSN

Na Wang[1, 2*], Yanxia Pang[2]

[1] *MoE Engineering Center for Software/Hardware Co-design Technology and its Application, East China Normal University, No.3663 North Zhongshan Rd, Shanghai 200062, China*

[2] *School of Computer and information, Shanghai Second Polytechnic University, No. 2360 Jinhai Rd, Shanghai 201209, China*

Received 1 March 2014, www.tsi.lv

Abstract

WSN is often deployed in unattended or even hostile environments. Therefore, providing security in WSN is a major requirement for acceptance and deployment of WSN. Furthermore, establishing trust in a clustered environment can provide numerous advantages. We proposed a light-weight trust model which considers data aggregation and communication failure due to wireless channels. It computes retransmission rate to get success, failed and uncertain value, and details the data in parameters to depend against attacks. With comparing our model with LDTS and Model using Trust Matrix, we conclude that our model has implemented a trade-off between detection rate and communication consumption.

Keywords: direct trust, light-weight, trust matrix, retransmission rate, indirect trust

1 Introduction

A large amount of applications ranging from health, home, environmental to military and defence make use of sensor nodes for collection of appropriate data. The sensor nodes comprising of data collecting, processing, and transmitting units are very small in size and can be densely deployed owing to their low cost [4]. Cluster WSN such as LEACH is broadly used. Clustering algorithms can effectively improve network scalability and throughput. Using clustering algorithms, nodes are grouped into clusters, and within each cluster, a node with strong computing power is elected as a cluster head (CH). CHs together form a higher-level backbone network. After several recursive iterations, a clustering algorithm constructs a multi-level WSN structure [5].

However, WSN is often deployed in unattended or even hostile environments. The wireless and resource-constraint nature of a sensor network makes it an ideal medium for attackers to do any kinds of vicious things. Therefore, providing security in WSN is a major requirement for acceptance and deployment of WSN [6]. Establishing trust in a clustered environment provides numerous advantages, such as enabling a CH to detect faulty or malicious nodes within a cluster. In the case of multi-hop clustering, a trust system aids in obtain correct data aggregation.

The rest of the paper is organized as follows. The models and definitions are proposed in section 3. The detailed trust model is depicted in Section 4. The comparison and evaluation of our trust model with other models are given in Sections 5. The related work and our conclusions are presented in Sections 2 and 6.

2 Related work

Research on trust management systems for WSN received considerable attention from scholars. A number of studies have proposed such systems for WSNs. However, these systems suffer from various limitations such as the incapability to meet the resource constraint requirements of the WSNs, more specifically, for the large-scale WSN. Recently, a few trust management systems have been proposed for clustered WSNs, such as GTMS [1], Model using Trust Matrix [3], a light-weighted Trust Model [16]. To our best knowledge, a universal trust system designed for clustered WSNs to achieve light-weight remains lacking.

In Group based Trust Management Scheme [1], the authors proposed a new light weight trust management scheme for WSN. It works with two different topologies: intragroup and intergroup, where distributed trust management and centralized trust management is adopted respectively. And the trust states are represented as Trusted, Untrusted and Uncertain respectively. The advantage of the scheme is that, it evaluates the trust for the group of nodes rather than a single node in the cluster. However, GTMS relies on a broadcast-based strategy to collect feedback from the CMs of a cluster, which requires a significant amount of resources and power.

In a Fault-Event Detection Model Using Trust Matrix in WSN (DMUTM) [3], the author proposed a method of fault and event detection using trust model in WSN based on similarity matrix. They used similarity matrix which is based on data aggregation distinguish groups from each other in one cluster to detect fault. The trust was calculated by cluster head either directly or indirectly. When in indirectly case, the head calculated the trust by

**Corresponding author* e-mail:wnoffice@126.com

transitivity algorithm. However, the trust transitivity required a high complexity, which leads to amount of power consumption.

In [8], Xiao proposed a trust system LDTS for WSNs, which employ clustering algorithms. First, a lightweight trust decision-making scheme is proposed based on the nodes' identities in the clustered WSNs. Then a dependability-enhanced trust evaluating approach is defined for co-operations between CHs. Moreover, a self-adaptive weighted method is defined for trust aggregation at CH level. But the method focuses on transmit process but not considers data property in the network. Therefore, it can only depend against Garnished attack and bad mouthing attack.

In [13], the author proposes a trust-based defending model against multiple attacks. Considering the characteristics of resource-constrained sensor nodes, trust values of neighbouring nodes on the routing path can be calculated through the Dirichlet distribution function, which is based on data packets' acknowledgements in a certain period instead of energy-consuming monitoring. But the data packets' acknowledgements may consume much energy.

In A light-weighted Trust Model [16], the authors proposed a trust model based on data aggregation and detailed the data in parameters to depend against attacks. But it did not consider the retransmission rate and use only data similarity to make a trust decision while omit the transmission quality.

Therefore, it is necessary to build a light-weight trust model which consider data aggregation and detailed the data in parameters to depend against more attacks. Work in this paper is an improvement of our former work [16], the contributions are:

1) Use retransmission rate to compute success value.
2) Create an improved light-weight trust model based on our former work.
3) Combine transmission and data similarity to evaluate the total trust of a node to another.
4) Compare our model with LDTS, Model using Trust Matrix and our former work.

3 Models and definitions

3.1 NETWORK MODEL

WSN in a two dimensional plane with n sensors, denoted by a set N = (n_1, n_2, ……, n_n), where n_i is the ith sensor. These sensors are placed in an area and the transmission radius is r_s. Each node maintains its ID, sensing data and location. In such a network, we use LEACH protocol to create clusters. A node in the clustered WSN model can be identified as a CH, or a CM. Members of a cluster can communicate with their CH directly. A CH can forward the aggregated data to the central BS through other CHs.

3.2 TRUST MODEL

Trust models are classified into two categories that are node trust models and data trust models [6].

A data trust model is proposed to distinguish forged data of illegal nodes from innocent data of legal nodes. Sensor nodes evaluate trustworthiness of their neighbour nodes by cross checking the neighbour nodes' redundant sensing data with their own result. The trust value is calculated through a light-weighted method, and the data considering is a structure composed of three parameters: the consistency value of sensing data, the communication ability and the remained lifetime of a node. After the trust assertion, inconsistent data from malicious or compromised nodes can be detected.

3.3 DEFINITION OF TRUST MATRIX

When consider a cluster, we get a G = (V, E, s) consists of vertexes V, edges E and similarity weight s. Each vertex is a node and each edge is the connection of two neighbours. We compute the similarity among sensor nodes as Eq. (1) where node i and node j is adjacent in location. X is the sensing data of node. If $s_{i,j}$>0.9, we set new $s_{i,j}$ as 1, otherwise as 0.

$$s_{i,j} = \left\lceil \frac{10 * X_i X_j}{X_i^2 + X_j^2 - X_i X_j} \right\rceil . \quad (1)$$

We consider a window of time Δt. Thus, as time elapses, the window deletes old experiences but adds newer experiences. The trust value between two nodes can be calculated according to (2):

$$DSTi,k(\Delta t) = \left\lceil \left(\frac{10 * s_{x,y}(\Delta t)}{s_{x,y}(\Delta t) + d_{x,y}(\Delta t)} \right) \left(\frac{1}{\sqrt{d_{x,y}(\Delta t)}} \right) \right\rceil , \quad (2)$$

where $\left\lceil \left(\frac{10 * s_{x,y}(\Delta t)}{s_{x,y}(\Delta t) + d_{x,y}(\Delta t)} \right) \left(\frac{1}{\sqrt{d_{x,y}(\Delta t)}} \right) \right\rceil$ is the nearest integer function. $s_{i,k}(\Delta t)$ is the total number of similar data comparison of node i with k in Δt time, and $d_{i,k}(\Delta t)$ is the total number of dissimilar data comparison. Specially, if $d_{i,k}(\Delta t) = 0$, we set $ST_{i,k}(\Delta t)$=10.

The cluster head will periodically broadcast the request packet within the cluster. In response, all CMs in the cluster will forward their data values to CH. Then, CH will maintain these values in a matrix as shown below where the real number is the similarity of node i for node j and 1is a default value presenting the similarity of the node for itself.

$$\begin{matrix} DST_{1,1} & \dots & DST_{1,n} \\ \vdots & \ddots & \vdots \\ DST_{n,1} & \dots & DST_{n,n} \end{matrix} . \quad (3)$$

3.4 DEFINITION OF COMMUNICATION TRUST

The trust value based on communication between two nodes can be calculated according to (4):

$$DCT_{i,k}(\Delta t)=\left\lceil\left(\frac{10*s_{i,k}(\Delta t)}{s_{i,k}(\Delta t)+f_{i,k}(\Delta t)}\right)\left(\frac{1}{\sqrt{f_{i,k}(\Delta t)}}\right)\right\rceil, \quad (4)$$

where $\left\lceil\left(\frac{10*s_{i,k}(\Delta t)}{s_{i,k}(\Delta t)+f_{i,k}(\Delta t)}\right)\left(\frac{1}{\sqrt{f_{i,k}(\Delta t)}}\right)\right\rceil$ is the nearest integer function. $s_{i,k}(\Delta t)$ is the success number of communication between node i and k in Δt time, and $f_{i,k}(\Delta t)$ is the failed number of communication. Specially, if $f(\Delta t) = 0$, we set $CT_{i,k}(\Delta t)$=10 [8].

CH will maintain a matrix as shown in Eq. (5) where the number is the direct trust of node i for node k based on communication and 1is a default value presenting the trust toward itself.

$$\begin{matrix} DCT_{1,1} & \dots & DCT_{1,n} \\ \vdots & \ddots & \vdots \\ DCT_{n,1} & \dots & DCT_{n,n} \end{matrix}. \quad (5)$$

4 A light-weighted trust model

4.1 CALCULATE DIRECT TRUST

A CM's trust value can be calculated by direct and indirect observation. Direct trust is evaluated by the number of successful and unsuccessful interactions, similar or dissimilar data comparison. In this work, interaction refers to the cooperation of two CMs and comparison refers to data aggregation. Indirect trust is evaluated by aid of similarity matrix in CH. That is, if node x wants to calculated the trust value for node y, first it checks whether it has a valid interaction with y during a specific time interval. If a past valid interaction record exists, then it compares its data value with y. Otherwise, if its remaining energy is less than ten percent, it will send a request to its CH. The model considers the consistency value of sensing data, the communication ability and the remained lifetime of a node. The process can be depicted in Figure 1.

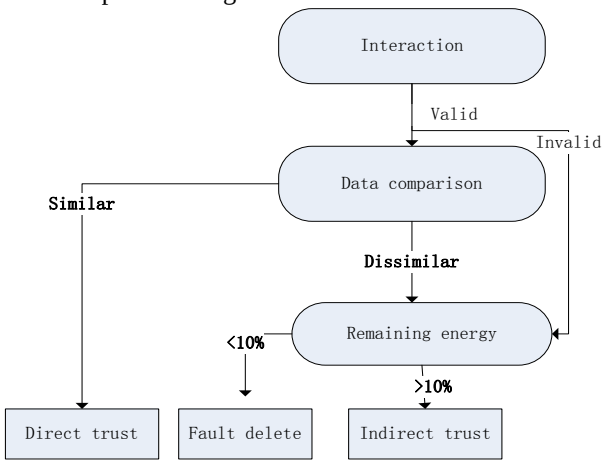

FIGURE 1 Process of the model

If the interaction $DCT_{i,k}$ is more than 5 according to Eq. (4), it is regarded as valid. Then start second stage to calculate data comparison using Eq. (1). If data similarity is more than 5, the direct similar trust is as Eq. (2). The combined trust is as Eq. (6). Otherwise, check the remaining energy to decide whether to calculated the indirect trust or assert the node is fault to delete from the network:

$$DT_{i,k}=\left\lfloor\frac{DCT_{i,k}*DST_{i,k}}{10}\right\rfloor. \quad (6)$$

If the interaction $DCT_{i,k}$ is less than 5, it is regarded as invalid. Then we check the remaining energy to do the same work as above.

4.2 COMPUTE RETRANSMISSION RATE

After node i sends a data packet to its neighbouring node j in one-hop transmission range, it should receive an acknowledgement from node j. Otherwise, node i will retransmit the data packet. Retransmission in the link layer is supposed to be caused by some non-malicious factors such as the quality of wireless channels, node malfunction, etc., and by attacks in the routing layer. For node i, the non-malicious impact factor is calculated in (7) based on the retransmission rates of all its neighbours:

$$\theta=\frac{\sum_{K=1}^{N} t_{i,k}}{N}, \quad (7)$$

where N represents the number of node i's neighbouring nodes, and for node i the retransmission rate of the neighbouring node k within a certain period is denoted as t_{ik}, which is calculated by (8):

$$t_{i,k}=\frac{l}{m}, \quad (8)$$

where l represents the number of packets retransmitted from node i to node k, and m represents the total number of packets sent by node i to node k.

During Δt, if node i receives an acknowledgement from its neighboring node k, node i considers that the data packet has been successfully forwarded to the destination node through node k, and the number of successful forwarding times for node k is added by 1. Otherwise, the number of failed forwarding attempts for node k is added by 1. But the retransmission may compensate part of failed communication, so the real failed communication should be calculated again.

Since $cs_{i,k}(\Delta t)$ is the success number of communication between node i and k in Δt time, we can detail failed communication as uncertain communication as (9) and failed communication as (10):

$$cu_{i,k}(\Delta t)= cf_{i,k}(\Delta t)\,\theta\,, \quad (9)$$

$$cf_{i,k}(\Delta t)= cf_{i,k}(\Delta t)\,(1-\theta)\,. \quad (10)$$

4.3 CALCULATE INDIRECT TRUST

When entering the stage of calculating indirect trust, node i cannot determine the trust on k, it will request to CH for a feedback that can calculate the probability expectation based on data. We use the beta probability density functions to compute the indirect trust as Eq. (11) based on Eq. (3).

$$IST_{ch,k}=\left\lfloor 10 * \frac{s_{i,k}+1}{s_{i,k}+d_{i,k}+2} \right\rfloor. \quad (11)$$

Here, $s_{i,k}$ denotes the number of similar feedback to node k except itself and $d_{i,k}$ denotes the number of dissimilar data to node k in a period Δt. For example, as shown in Figure 3, which is deduced from Figure 2 with setting the threshold as 9, we want to calculate indirect trust of node 1. The value is a real number of 6.7.

$$\begin{bmatrix} 10 & 9 & 0 & 9 & 9 \\ 9 & 10 & 1 & 0 & 9 \\ 0 & 1 & 10 & 0 & 1 \\ 9 & 0 & 0 & 10 & 9 \\ 9 & 9 & 1 & 9 & 10 \end{bmatrix}$$

FIGURE 2 Similarity matrix

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{bmatrix}$$

FIGURE 3 Trust matrix

At the same time, the feedback can also calculate the probability expectation based on communication. We use the beta probability density functions to compute the indirect trust as Eq. (12) based on matrix (5).

$$ICTch,\ k=\left\lfloor 10 * \frac{cs_{i,k}+1}{cs_{i,k}+cf_{i,k}+cu_{i,k}+3} \right\rfloor, \quad (12)$$

where, $cs_{i,k}$ denotes the number of success communication to node k except itself, $f_{i,k}$ which is calculated from Eq. (10) denotes the number of failed communication to node k and $u_{i,k}$ denotes the number of uncertain communication in a period Δt.

Then the total indirect trust can be described as (13):

$$IT_{i,k}=\left\lfloor \frac{ICT_{i,k}*IST_{i,k}}{10} \right\rfloor. \quad (13)$$

5 Evaluations

Our experiment uses *ns3* to design. Fifty sensor nodes are distributed in a space of 500×700, and the communication radius is set as 60. Each node has two to five neighbours in the experiment and the node's location is already known. The detailed value is shown in Table 1. Each node maintains a structure as shown in Table 2.

TABLE 1 Values in evaluation

Symbol	Description	Values
N	Number of nodes	50
n	Number of CMs in a cluster	6-8
m	Number of CM's neighbours	4-6

TABLE 2 Structure of nodes

Node ID	The number of interaction			The number of similar	
	$s_{x,y}$	$f_{x,y}$	$u_{x,y}$	$s_{x,y}$	$d_{x,y}$
2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes
	Direct trust			Indirect trust	
	communication	*similar*	*communication*		*similar*
	0.5 bytes	0.5 bytes	0.5 bytes		0.5 bytes

We only consider the communication overhead with ignoring calculation cost. It is also assumed that the route is reliable without considering the case of route failure. We compare the communication consumption and error detection rate for simulation to LDTS and DMUTM.

It is shown in Figure 4 that when data error rate is changed, DMUTM maintains an average of packets by 2800. But LDTS and ours algorithm gets an increased average of packets as the data error rate growing. This is due to the calculating of indirect trust, which will consume more communication. While for LDTS, it only considers interaction, so the probability of calculating indirect trust is less than ours since our method considers both the interaction and data similarity.

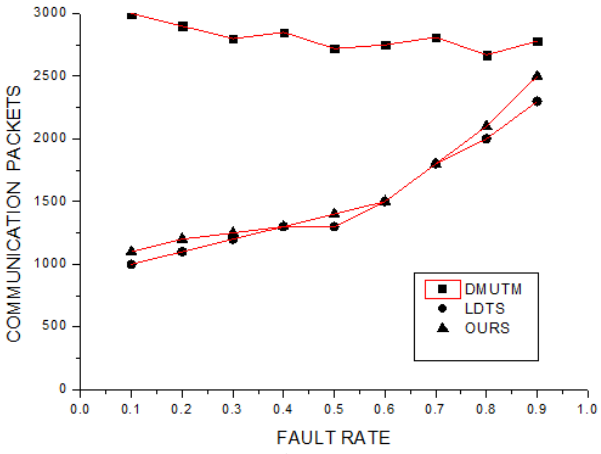

FIGURE 4 Comparison of communication consumption

Except for energy consumption, error detection rate is another important merit to measure a trust algorithm. We define error detection rate as f_s/f, where f_s is the number of fault nodes that have been detected and f is the total number of fault nodes.

Simulation result shown in Figure 5 indicates that the detection rate of DMUTM is higher than the other two methods because it handles all cases with indirect trust. And the higher detection rate is an exchange for communication consumption. LDTS has a lower detection rate than ours since it omits the data fault. And our former model has a lower detection rate than the current model since it omits the retransmission to regard fine node as error. Our model implements a balance between detection rate and communication consumption.

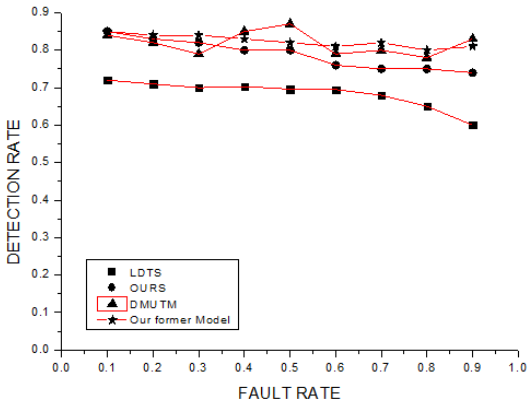

FIGURE 5 Comparison of fault detection rate

Although the advantage of our model, we can see from the structure that the memory overhead is double that of the LDTS.

6 Conclusions

In this paper, we investigate a method of light-weight trust calculating. A CM's trust value can be calculated by direct and indirect observation. Direct trust is evaluated by the number of successful and unsuccessful interactions, similar or dissimilar data comparison. Indirect trust is evaluated by aid of similarity matrix and communication matrix stored in CH. In order to distinguish uncertain from failed, we introduced a retransmission factor to make the communication result more explicit. This model can successfully detect fault nodes but consume more memory since it stored both data information and communication information. We did a series of simulations to test the performance of our proposed model. The simulation results have showed that our model has implemented a trade-off between detection rate and communication consumption.

In future, we should make full use of data information such as aggregating data at the same time when the trust is updated.

Acknowledgements

This work is supported by the National Basic Research Program of China (Grant No. 2011CB302802) and the National Natural Science Foundation of China (Grant No 61370100). Wang acknowledges the supported of the key discipline of Shanghai second polytechnic University named software engineering (No.XXKZD1301). The authors would like to thank the referees for their invaluable comments and suggestions.

References

[1] Riaz A S, Jameel H, d'Auriol B J, Sungyoung Lee H, Song Y-J *IEEE Transactions on Parallel and Distributed Systems* **20**(11) 1698-712
[2] Ganeriwal S, Srivastava M B 2004 Reputation-Based Framework for High Integrity Sensor Networks *Proceedings of ACM workshop security of ad hoc and sensor networks (SASN '04)* 66–7
[3] Wang Na, Chen YiXiang 2013 *Sensors &Transducers* **158-159**(12) 190-4
[4] Krasniewski M, Varadharajan P, Rabeler B, Bagchi Saurabh 2005 TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks *Proceedings of the International Conference on Dependable Systems and Networks* 2005 672-81
[5] Ganeriwal S, Balzano L K, Srivastava M B 2008 *ACM Trans. Sensor Networks* **4**(3) 1–37
[6] Han Guangjie, Jiang Jinfang, Shu Lei, Niu Jianwei, Chao Han-Chieh 2014 Management and applications of trust in Wireless Sensor Networks: A survey *Journal of Computer and System Sciences* **80**(3) 602–17
[7] Sarma Dhulipala V R, Karthik N, Chandrasekaran R M 2013 A Novel Heuristic Approach Based TrustWorthy Architecture for Wireless Sensor Networks *Wireless Pers Commun* **70** 189–205
[8] Li Xiaoyong, Zhou Feng, Du Junping 2013 *IEEE Transactions on Information Forensics and Security* **8**(6) 924-35
[9] Chen Yixiang, Bu TianMing, Zhang Min, Zhu 2010 Measurement of Trust Transitivity in Trustworthy Networks *Hong Journal of Emerging Technologies in Web Intelligence* **2**(4) 319-25 *(in Chinese)*
[10] Liu Chen-xu, Liu Yun, Zhang Zhen-jiang 2013 Improved Reliable Trust-Based and Energy-Efficient Data Aggregation for Wireless Sensor Networks *International Journal of Distributed Sensor Networks* **2013** Article ID 652495 11 pages
[11] Wu Chunxue, Feng Bin 2007 Based on Single-hop Flow Control Scheme for Wireless Sensor Networks *IET Conference on Wireless, Mobile and Sensor Networks 2007 December 2007*
[12] Wu Chunxue 2006 Practical models and control methods with data packets loss on NCS *The IET International Conference on Wireless Mobile and Multimedia Networks January 2006*
[13] Zhang Guanghua, Zhang Yuqing, Chen Zhenguo 2013 Using Trust to Secure Geographic and Energy Aware Routing against Multiple Attacks *PLOS ONE* **8**(10) Oct 21 2013
[14] Wang Na, Wu YuePing 2013 Data aggregation for failure tolerance in wireless sensor network *Applied Mechanics and Materials* **347-350** 965-9
[15] Wang Na, Liu Dongqian, He Kangli 2013 A formal description for protocols in WSN based on STeC language *Proceedings of the 8th International Conference on Computer Science and Education, ICCSE 2013* 921-4
[16] Wang Na, Gao Liping, Wu Chunxue 2014 A Light-Weighted Data Trust Model in WSN *International Journal of Grid and Distributed Computing* **7**(2)

Authors

Na Wang, born on June 6, 1979 He Nan

Current position, grades: PhD candidate , a lecturer of Shanghai second University
University studies: East China Normal University, Shanghai Second Polytechnic University
Scientific interest: Wireless sensor networks
Publications: 12

Yanxia Pang, born on December 23, 1980 Shan Dong

Current position, grades: PhD candidate, a lecturer of Shanghai second University
University studies: Shanghai Second Polytechnic University
Scientific interest: Data mining
Publications: 5