International Journal of Grid and Distributed Computing
Vol.7, No.2 (2014), pp.33-40
http://dx.doi.org/10.14257/ ijgdc.2014.7.2.04

A Light-Weighted Data Trust Model in WSN

Na Wang[1], Liping Gao[2*] and Chunxue Wu[2]

[1]*School of Computer and information, Shanghai Second Polytechnic University, Shanghai, 201209, China*
[2]*School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, 200093, China.*
wnoffice@126.com; lipinggao@fudan.edu.cn; tyfond@126.com

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-weighted trust model which consider data aggregation and detailed 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, similarity, trust matrix, WSN, indirect trust*

1. Introduction

Applications ranging from health, home, environmental to military and defense 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.

* Corresponding Author

ISSN: 2005-4262 IJGDC
Copyright ⓒ 2014 SERSC

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, very few trust management systems have been proposed for clustered WSNs, such as GTMS [1], RFSN [2], HATWA [7] and [3]. 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 Reputation based Framework for Sensor Networks [2], each node in the network maintains the reputation for neighboring nodes. The values of the trust are evaluated on the basis of that reputation and Bayesian formulation was used for representing the values of reputation. According to this scheme, each node in the sensor network develops a reputation for other node in the network by making direct observations. The disadvantage of this model is that, the mobility makes there is no enough interaction with the nodes and hence the reputation information will not be stabilized.

HATWA proposes a Heuristic Approach based Trust Worthy Architecture for WSN that considers the challenges of the system and focus on the collaborative mechanism for trust evaluation and maintenance. The proposed Architecture could also be capable of fulfilling critical security, reliability, mobility and performance requirements for reliable communication while being readily adaptable to different applications. But it introduced an additional network monitoring node to record and calculate the whole trust during four stages. And data aggregation is not included in the four stages. They also assume the monitor node is no fault.

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 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. So it can only depend against Garnished attack and bad mouthing attack.

So it is necessary to build a light-weighted trust model which consider data aggregation and detailed the data in parameters to depend against more attacks. The contribution of our work is:

 Copyright ⓒ 2014 SERSC

1) Create a light-weighted trust model based on our former work.

2) Parameterize the sensing data according to three factors.

3) Compare our model with LDTS and Model using Trust Matrix.

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 rs. Each node maintains its ID, sensing data and location. In such a network, we use LEACH protocol to create clusters illustrated in Figure1. A node in the clustered WSN model can be identified as a CH, or a CM (See Figure. 1). Members of a cluster can communicate with their CH directly. A CH can forward the aggregated data to the central BS through other CHs.

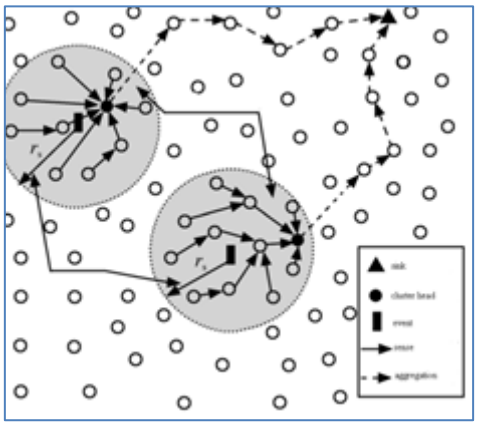

Figure 1. Model of Network

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 neighbor nodes by cross checking the neighbor 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 neighbors. We compute the similarity among sensor nodes as formula (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.

Copyright ⓒ 2014 SERSC

$$s_{i,j} = \frac{X_i X_j}{X_i^2 + X_j^2 - X_i X_j} \quad (1)$$

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 formula (2).

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

⌈ ⌉ is the nearest integer function. $s_{x,y}(\Delta t)$ is the total number of similar data comparison of node x with y in Δt time, and $d_{x,y}(\Delta t)$ is the total number of dissimilar data comparison. Specially, if $d_{x,y}(\Delta t) = 0$, we set $T_{x,y}(\Delta t)=10$.

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.

$$\begin{matrix} s_{1,1} & \cdots & s_{1,n} \\ \vdots & \ddots & \vdots \\ s_{n,1} & \cdots & s_{n,n} \end{matrix} \quad (3)$$

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 remain 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 2.

 Copyright ⓒ 2014 SERSC

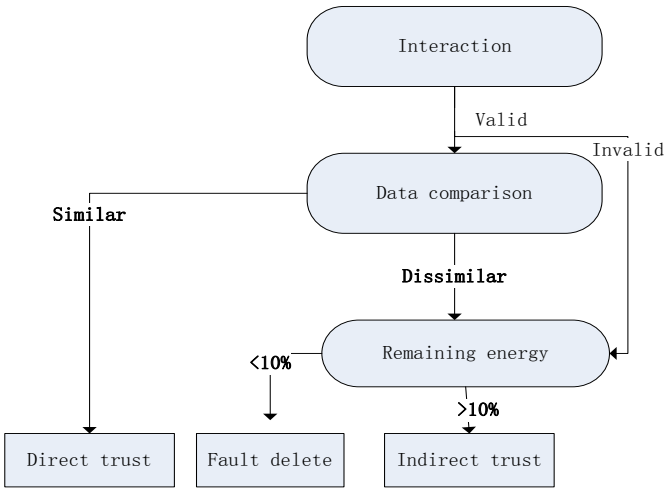

Figure 2. Process of the Model

In the first stage of interaction, we use LDTS model in [8]. If the interaction $I_{x,y}$ is more than 5, it is regarded as valid. Then start second stage to calculate data comparison using formula (2). If data similarity is more than 5, the direct trust is as formula (4). Otherwise, check the remaining energy to decide whether to calculated the indirect trust or assert the node is fault to delete from the network.

$$IT_{x,y=}\frac{I_{x,y}*S_{x,y}}{10} \quad (4)$$

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

4.2. Calculate Indirect Trust

When enter the stage of calculating indirect trust, the node request to CH for a feedback that if there are some nodes that are not its neighbors have the similar data as it sensing. We use the beta probability density functions to compute the indirect trust as formula (5) based on matrix (4).

$$DT_{ch,y}=10*\frac{s_{x,y}+1}{s_{x,y}+d_{x,y}+2} \quad (4)$$

Here, $s_{x,y}$ denotes the number of similar data to node y except itself and $d_{x,y}$ denotes the number of dissimilar data to node y at one moment. For example, as shown in Figure 4 which is deduced from Figure 3, we want to calculate indirect trust of node 1. The value is a real number of 6.7.

$$\begin{bmatrix} 1 & 0.9 & 0 & 0.95 & 0.98 \\ 0.9 & 1 & 0.1 & 0 & 0.92 \\ 0 & 0.1 & 1 & 0 & 0.1 \\ 0.95 & 0 & 0 & 1 & 0.9 \\ 0.98 & 0.92 & 0.1 & 0.9 & 1 \end{bmatrix}$$

Figure 3. Similarity Matrix

Copyright ⓒ 2014 SERSC

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

Figure 4. Trust Matrix

5. Evaluation

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 neighbors in the experiment and the node's location is already known. The detailed value is shown in Table 1.

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 neighbors	4-6

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.

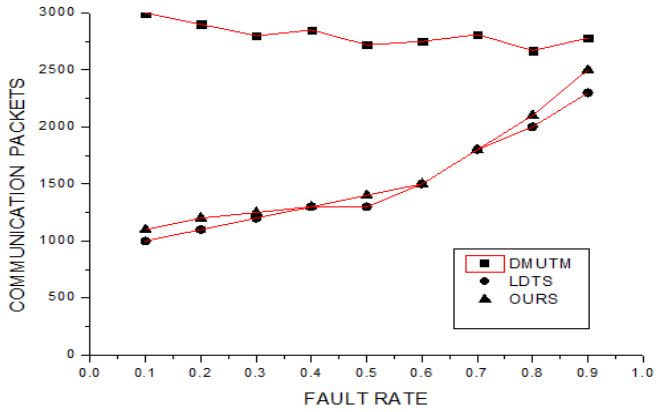

Figure 5. Comparison of Communication Consumption

It is shown in Figure 5 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 consider interaction, so the probability of calculating indirect trust is less than ours since our method considers either the interaction and data similarity.

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

Simulation result shown in Figure 6 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

 Copyright ⓒ 2014 SERSC

detection rate is an exchange for communication consumption. LDTS has a lower detection rate than ours since it omit the data fault. Our model implements a balance between detection rate and communication consumption.

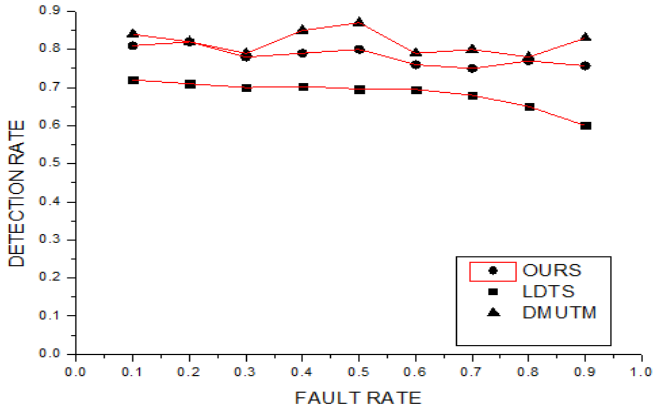

Figure 6. Comparison of Fault Detection Rate

6. Conclusions

In this paper, we investigate a method of light-weighted 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 in CH. This model can successfully detect fault nodes. 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 balance between detection rate and communication consumption.

Acknowledgements

The work is supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61202376 and No. 61003031, "Chen Guang" project sponsored by Shanghai Municipal Education Commission and Shanghai Education Development Foundation under Grant No.10CG49, Innovation Program of Shanghai Municipal Education Commission under Grant No. 13YZ075 and 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] S. Riaz Ahmed, H. Jameel, B. J. d'Auriol, H. Sungyoung Lee and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks", IEEE Transactions on Parallel and Distributed Systems, **(2011)**.

[2] S. Ganeriwal and M. B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks", Proceedings of ACM workshop security of ad hoc and sensor networks (SASN '04), **(2004)** October, pp. 66-67.

[3] N. Wang and Y. Xiang Chen, "A Fault-Event Detection Model Using Trust Matrix in WSN", Sensors &Transducers journal, vol. 159, no. 12, **(2013)** December.

[4] M. Krasniewski, P. Varadharajan, B. Rabeler and S. Bagchi, "TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks", Proceedings of the International Conference on Dependable Systems and Networks, **(2005)**, pp. 672-681.

Copyright ⓒ 2014 SERSC

[5] S. Ganeriwal, L. K. Balzano and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks", ACM Trans. Sensor Netw., vol. 4, no. 3, **(2008)** May, pp. 1-37.
[6] G. Han, J. Jiang, L. Shu, J. Niu and H.-C. Chao, "Management and applications of trust in Wireless SensorNetworks: A survey", Journal of Computer and System Sciences, **(2013)** July 4.
[7] V. R. Sarma Dhulipala, N. Karthik and R. M. Chandrasekaran, "A Novel Heuristic Approach Based TrustWorthy Architecture for Wireless Sensor Networks", Wireless Pers Commun., vol. 70, **(2013)**, pp. 189-205.
[8] X. Li, F. Zhou and J. Du, "LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, **(2013)** June.
[9] Y. Chen, T. M. Bu, M. Zhang and H. Zhu, "Measurement of Trust Transitivity in Trustworthy Networks", Journal of Emerging Technologies in Web Intelligence, vol. 2, no. 4, **(2010)**, pp. 319-325.
[10] C.-Xu Liu, Y. Liu and Z.-J. Zhang, "Improved Reliable Trust-Based and Energy-Efficient Data Aggregation for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Article ID 652495, 11 pages, **(2013)**.
[11] W. Chunxue and F. Bin, "Based on Single-hop Flow Control Scheme for Wireless Sensor Networks", IET Conference on Wireless, Mobile and Sensor Networks 2007, **(2007)** December.
[12] W. Chunxue, "Practical models and control methods with data packets loss on NCS", 2006 The IET International Conference on Wireless Mobile and Multimedia Networks, **(2006)** January.

Authors

Na Wang, (1979-) is a lecturer of Shanghai second University. At the same time, she studies in East China Normal University as a PH.D candidate. Her major interests include WSNs and theory of software formalization. She has published more than 10 journal and conference articles.

Chunxue Wu, (1964-)received the Ph.D. degree in Control Theory and Control Engineering from China University of mining and technology, Beijing, China, in 2006.He is a Professor with the Computer Science and Engineering and software engineering Division, School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, China. His research interests include, wireless sensor networks, distributed and embedded systems, wireless and mobile systems, networked control systems.

Liping Gao, (1980-) graduated from Fudan University, China with a PhD in 2009 in Computer Science. She received her BSc and master degree in Computer Science from Shandong Normal University, China in 2002 and 2005 respectively. She is doing her research work in University of Shanghai for Science and Technology as an assistant professor. Her current research interests include CSCW, heterogeneous collaboration, consistency maintenance and collaborative engineering.

 Copyright ⓒ 2014 SERSC