Power-Aware and Reliable Sensor Selection Based on Trust for Wireless Sensor Networks

Guangjie Han[1], Lei Shu[2, 3], Jianhua Ma[4], Jong Hyuk Park[5], Jianjun Ni[1]
[1]Department of Information & Communication Systems, Hohai University, Changzhou, China
hanguangjie@gmail.com, njjhhuc@gmail.com
[2]Digital Enterprise Research Institute, National University of Ireland, Galway, Ireland
[3]Department of Multimedia Engineering, Osaka University, Japan
lei.shu@ieee.org
[4]Faculty of Computer & Information Sciences, Hosei University, Japan
jianhua@hosei.ac.jp
[5]Department of Computer Science and Engineering, Seoul National University of Technology, Korea
parkjonghyuk1@hotmail.com

***Abstract*—Wireless Sensor Networks (WSNs) is temporarily formed, operated and managed by the nodes themselves. In a complex WSN, malicious nodes are well disguised, and they can attack the entire network on specific purpose by utilizing the natural cooperation of nodes. The error-prone characteristic of sensor nodes can also cause instability in WSN. Therefore, how to choose one or more suitable sensor nodes to collaborate towards a better system performance is a critical issue. In this paper, we construct a new trust model for WSNs based on the trust mechanism in human society. Based on this trust model, we propose a novel power-aware and reliable scheme for sensor selection (PRS). The remaining energy of a node can be considered as an important restrictive factor for the proposed scheme. Simulation results show that PRS scheme can improve the system stability, defend against the attacks of malicious nodes, and prolong the lifetime of WSNs, effectively.**

***Index Terms*—Wireless Sensor Networks, trust mechanism, power-aware, sensor node selection, direct trust, indirect trust**

I. INTRODUCTION

With the rapid increasing computing complexity and high demand on mobility, more and more complex tasks cannot be accomplished by a single sensor node [1], thus there must be networks of sensor nodes cooperating together [2]. The sensor nodes cooperate to perform different tasks, e.g., localization and tracking, which they work with each other based on trust is the cooperation. However, this cooperative feature among sensor nodes can be easily utilized by malicious nodes for attacking the whole network, e.g., military applications [3, 4]. Beside attacks from malicious nodes, normal sensor nodes are also vulnerable to system faults because of simple and low-cost hardware configuration, and these kinds of system faults generally cannot be handled by authentication and cryptographic mechanisms [5].

Manuscript received February 26, 2009; revised Sep 19, 2009; accepted Dec 1, 2009.
Corresponding author: Guangjie Han.

On the other hand, battery powered sensor nodes are equipped with very limited energy resource, which makes the reserving of energy in WSNs as one of the most challenging issues for design consideration, which means the selection of sensor nodes for participating any task should be conducted carefully, in order to prolong the lifetime of WSNs, and further if an inappropriate node was chosen, and it has no capability to accomplish the task or cannot complete the task with an acceptable result, the WSN might be ultimately leaded to serious system performance degradation. In addition, by selecting the appropriate sensor node during the cooperation process, the entire system stability of WSNs can be improved. Thus, how to choose one or several suitable nodes as the cooperation partners for any node is one of the most important issues in a WSN.

To the best of our knowledge, several methods have been recently proposed to enable collaborations of sensor nodes for data collection and information processing. Local greedy algorithm has been developed in [6, 7] to select the next most informative sensor node to build the optimal routing path based on information utility and entropy respectively. However, the problem of this work is that the suitable path is always chosen for transmitting data, in which the nodes will deplete energy much quickly than others, and this can greatly affect the network lifetime (*the active time until the first node dies*). Instead, Shah and Rabaey [8] proposed that sometimes sub-optimal routing paths should be chosen depending on the probabilities to prolong the whole network lifetime. In paper [9], the proposed strategy involves partitioning the networks into zones and computing the power level, which may increase the overhead and lead to the degradation of the performance. The authors in [14] proposed a tree based structure that uses a lot of sensors to collaborate the detection mechanism and to collect precise data. However, the proposed method always wastes the resources, if a target moves to certain area iteratively. In [15], the authors proposed an energy efficient selection of cooperative nodes with respect to their geographical location and the number of nodes participating in cooperative communication in WSNs.

doi:10.4304/jcm.5.1.23-30

The authors in [16] proposed probabilistic multipath routing algorithms, which generate braided multipath based only on local information. In paper [17], the author proposed a power-aware algorithm for configuring the CST and scheduling a class of communications. The algorithm requires only local information at processing elements. In short, the above-mentioned methods do not either consider the attacks of malicious nodes nor the error-prone characteristic of sensor nodes, which can highly affect the entire network performance, especially, in a hostile environment.

In this paper, we propose a novel power-aware and reliable scheme (PRS) for sensor selection, integrating the idea of trust mechanism in the human society. In PRS, the remaining energy of any node is considered as a restrictive factor for sensor selection, which enables PRS not only effectively defends against attacks from malicious nodes but also balances the load of energy consumption in WSNs.

The scientific research contributions of this paper are summarized as follows: (1) We summarize the trust relationship of the human society, transition it to WSNs, and propose a new trust model – PRS, which mode fully consider the cooperation relationship of the nodes and make up the shortcomings of the traditional model. (2) In PRS, we use the opinions of the thrid-party as the assistant decision-making, adjust the trust relationship of the nodes based on the tradtional trust model, and defend the attacks of the malicious modes. (3) Our PRS model considers the energy and the packet forwarding probability of the node as the new attribute, which can effectly improve the network perfomance of WSNs.

The remainder of this paper is organized as follows: in section II, we describe the trust transition of human society. In Section III, we present the architecture of our PRS. In Section IV, we present our node selection algorithm. The simulation results are shown in Section V. Finally, in Section VI, we summarize our results.

II. TRUST TRANSITION

Trust in human society is the basis of human beings' communications, work and daily life. We all have a sense of what it means to trust someone. Trust can be gradually obtained during the frequent interaction processes. When people gradually form the standard of mutual trust, and they always refer to the opinions of the third-party people. Trust can be regarded as a criterion for making a judgment under complex social conditions and can be used to guide further actions. A simplified trust model in the human society is shown in Figure 1.

As shown in Figure 1, when Alice needs help from other people, she sends a request to many people who can help her. Some people, who are willing to help her, will respond to the request. Then Alice selects the most suitable person (for instance, Bob) with high trust value to work together, and the cooperation process increases mutual trust value between Alice and Bob. At the same time, Bob is possibly deceptive, so Alice always needs the information provided by the third-party person (for instance, Tina) to assist her to make a better decision.

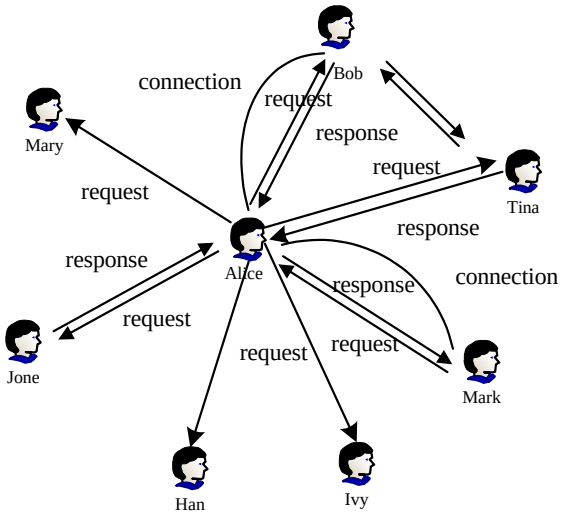

Figure 1. Simplified trust model in human society

The trust model of the traditional system is shown in Figure 2. The manager will collect the cooperation information from both parties as a system administrator. The trust value of a node can be seen by other nodes when they belong to the same domain. In this case the trust relationship of both nodes is regarded as the direct trust. When two nodes do not belong to the same domain, one node needs the manager to provide the trust value of the other node. In this case, the trust relationship between two nodes is indirect trust [10].

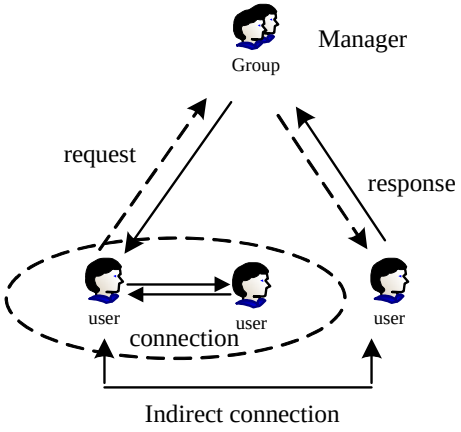

Figure 2. Trust model in traditional system

In a WSN environment, some tasks, e.g., packet transferring, localization and tracking, need several nodes to cooperate together. It is shown in [11] that rather than merely relying on the functions of sensor nodes, information exchanging among sensor nodes should also consider their trust values. Thus, a node with high trust value is the preferred cooperative target. We propose a trust model for WSN that refers to the trust mechanism in the human society.

III. ARCHITECTRUE OF PRS

A. Abstract Description of Sensor Node

In a WSN, typically one node needs the services provided by other nodes. A node can provide some services such as temperature, humidity, pressure, e.g., every service consists of several different attributes. A traditional node can be denoted by $Node < ID, A, V >$, where *ID* denotes the identity of the node, *A* denotes the attribute set of node ID and *V* denotes the value set of the attributes. The relationship between a node and its attributes is shown in Figure 3.

In PRS, we extend the definition of a node, which is now denoted by $Node < ID, A, V, T >$, where *T* denotes the trust value set of the attributes (*every attribute has its own trust value*). The extended definition includes energy, etc. In the traditional computing [12], researchers do not consider the energy of sensor nodes, which, on the contrary, is an important factor in WSNs. We consider the energy as one attribute of a sensor node in PRS, which other trust models neglect this factor.

With extended definition of a node, the quality of service can be measured by different attributes of a node. No matter which node provides better service, it will have more opportunities to increase its trust value of the cooperative node. Thus, the node with higher trust value will work more than other nodes. In order to avoid the node with higher trust value dying out early, the energy level of a node should be considered as a restrictive factor to decrease its trust value. The node with less energy decreases its opportunity of cooperation to make the network system stable.

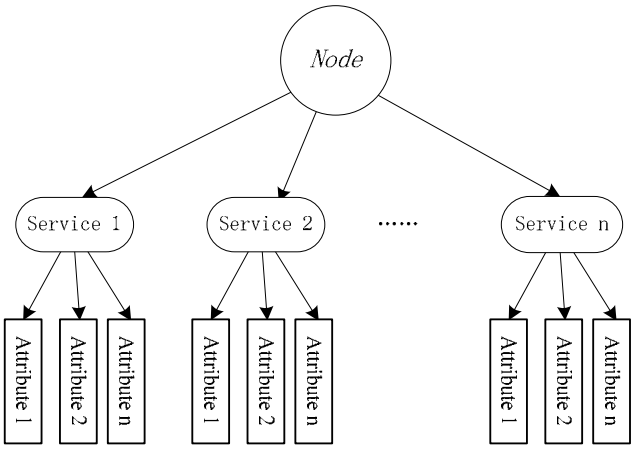

Figure 3. Relationship of a node and its attributes

In PRS, the node can be divided into three categories: (1) the sponsor node, (2) the target node and (3) the third-party node. A sponsor node is the initiator of the cooperation, denoted by N_S. It needs to select one or more nodes from the candidate nodes to cooperate together. In general, there is only one N_S during a single cooperation process. A target node is the chosen node that provides the service to the sponsor node during the cooperation process, denoted by N_T. There may be many such nodes during a single cooperation process. A third-party node is the reference node that provides its trust value of the target node to the sponsor node, denoted by N_R. There may be many such third-party nodes during a single cooperation process.

B. Abstract Description of Trust Value

In PRS, trust is represented by a real number ranging from 0 (corresponding to complete distrust) to 1 (corresponding to complete trust). The trust value among the nodes can also be divided into three categories: direct trust value, indirect trust value and integrated trust value. Direct trust value is the type of trust value can be established between N_S and N_T, denoted by $T_{directtrust}$. Indirect trust value is established when N_R provide its trust value of N_T to N_S, denoted by $T_{indirecttrsut}$. Integrated trust value can be calculated based on the direct trust value of the target node and the indirect trust value of the third-party nodes, denoted by $T_{integtrust}$.

In a complex WSN environment, the direct trust sometimes cannot provide overall evaluation of the target nodes. Due to the resource limitation of the sponsor node, a malicious node can be easily selected during the cooperation process. In order to avoid this problem, we use the indirect trust value provided by the third-party nodes, which can give an overall evaluation of the target node to the sponsor node.

C. Architecture of Trust Model

In PRS, we refer to other traditional trust models [12] and extract the influential factors to construct the new trust model. The architecture of our PRS is shown in Figure 4.

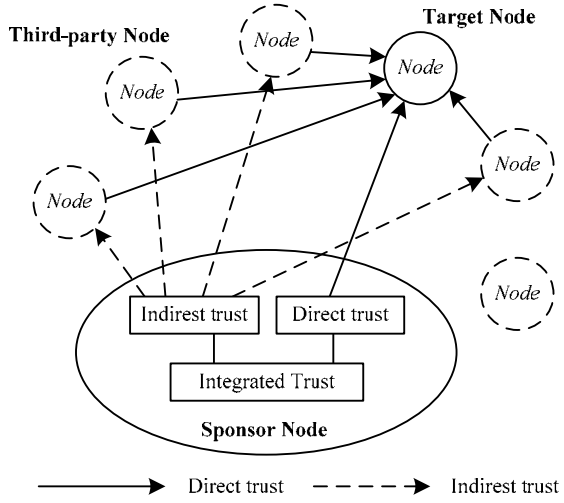

Figure 4. The architecture of PRS

As shown in Figure 4, when the sponsor node gets the direct and indirect trust value, the integrated trust module combines both the direct trust value and the indirect trust value to get the integrated trust value. Finally, the sponsor node calculates the integrated trust value of all available target nodes, then chooses one or more nodes based on the requirement of the cooperation. The process of establishing trust is iterative with gradually increased interactions, many factors such as cooperative time,

energy, etc., should be considered. Thus, the effect of time delay can be reduced to the greatest extent possible.

IV. Sensor Node Selection Algorithm

A. Calculation of Direct Trust Value

The direct trust value of a target node can be calculated by its multi-attribute trust value. The conditions of a node are always changing, thus the sponsor node needs to evaluate the direct trust value of the target node based on its multi-attribute trust value. We assume that all attributes of the node are independent in a WSN, thus the direct trust value of the target node can be calculated by the sponsor node.

During the interaction process, the sponsor node and the target node evaluate the result of the cooperation, and record it. Since every attribute of the node is independent, the sponsor node doesn't need all attributes of the node to cooperate together in a certain task. Thus, the cooperation only relates to some attributes of the node and affects the trust values of these attributes. The information about the past cooperations is listed as cooperation records, as shown in Table I. Each attribute $(A_i, i = 1,2 \ldots n)$ has two relevant values: the value of the successes $(S_i, i = 1,2 \ldots n)$, and the value of the cooperations $(C_i, i = 1,2 \ldots n)$.

TABLE I.
COOPERATION RECORD TABLE

Attribute	Success	Sum
A_1	S_1	C_1
A_2	S_2	C_2
…	…	…
A_n	S_n	C_n

The trust value for attribute A_i can be computed based on the Table 1 as follows:

$$T_{A_i} = \frac{S_i}{C_i},$$

Thus, the overall trust value for the target node with n attributes $A_i, i = 1,2 \ldots n$ (denoted by T_{node}) can be computed using T_{A_i} as follows:

$$T_{node} = \frac{\prod_{i=1}^{n} T_{A_i}}{\prod_{i=1}^{n} T_{A_i} + \prod_{i=1}^{n} (1 - T_{A_i})} \quad (1)$$

Since all T_{A_i}, $i = 1,2,...,n$ can be calculated using data in Table 1, the trust value of every available target node can be easily calculated by the sponsor node.

B. Calculation of Indirect Trust Value

When the cooperation request of the sponsor node is sent out, it can get three kinds of trust value returned by neighboring nodes (*the node is within the other node's communication range*). The trust values of the reliable and strange nodes can be kept, and the trust values of the unreliable nodes must be discarded. Therefore, these two kinds of trust values can be combined as follows:

$$T_{indirecttrust} = W_{reliable} \times T_{reliable} + W_{strange} \times T_{strange} \quad (2)$$

where $T_{reliable}$ and $T_{strange}$ denote as the trust value returned by the reliable third-party nodes and the strange third-party nodes respectively, $W_{reliable}$ and $W_{strange}$ denote as the weight of the reliable third-party nodes and the strange third-party nodes respectively, thus $W_{reliable} + W_{strange} = 1$.

The indirect trust value of the third-party nodes should be transferred to the sponsor node. The trust value of the third-party nodes has been fully considered which make the trust calculation process be more comprehensive thus it can efficiently enhance system stability.

C. Calculation of Integrated Trust Value

In the human society, people have different opinions to the same matter. In PRS, this feature is manifested and our sponsor node can choose the different weights in accordance with the cooperative requirements of the nodes. The weight of the direct trust is denoted by W_{dtrust}, with $W_{dtrust} \in [0,1]$, the weight of the indirect trust is denoted by W_{itrust}, with $W_{itrust} \in [0,1]$. The integrated trust value can be calculated as follows:

$$T_{integtrust} = W_{dtrust} \times T_{directtrust} + W_{itrust} \times T_{indirecttrust} \quad (3)$$

where $W_{dtrust} + W_{itrust} = 1$. The nodes adjust the weights of the direct trust and the indirect trust based on its own different application circumstances. For example, during the cooperation of message transferring, the sponsor node sets the value of W_{itrust} to be zero. When the integrated trust value of every available target node is calculated, the suitable target node can be chosen in the cooperation process.

The trust value of a node varies with time. In the direct trust model, once there is no further cooperation for a long time, the trust value of the cooperative node is still constant. However, the people with high trust value and more cooperations can keep a long-term trust relationship, or their trust will gradually weaken in the human society. In our PRS, we also mimic the trust mechanism in the human society: if a node cannot provide cooperation for other nodes, and the other nodes will gradually decrease its trust value.

D. Sensor Node Selection Algorithm

The procedure of sensor node selection algorithm is listed as following, as shown in Table II.

TABLE II.
SENSOR NODE SELECTION ALGORITHM

Step 1	The sponsor node broadcasts its cooperative request to neighboring nodes to accomplish one target task together and also gets the trust value of the cooperative node at the same time.
Step 2	When the sponsor node gets some responses from the target nodes, it calculates the direct trust value of every target node. In this process, a simple formula is adopted to compute the trust value of the target node based on its multi-attribute trust value.
Step 3	The sponsor node broadcasts the reference request of the available target node to its neighboring nodes and gets the indirect trust value of target node from the third-party nodes.
Step 4	The sponsor node combines every reference trust value provided the third-party nodes and uses the weight of trust value method to adjust the trust proportion based on its different standards and circumstances.
Step 5	The sponsor node combines both the direct trust value and the indirect trust values. Therefore, the sponsor node calculates the final trust value of all possible nodes in the target node set. Based on the selection rule of trust value, the sponsor node chooses one or more nodes with high trust value to cooperate together.

As analyzed in previous section, the indirect trust relationship of third-party nodes has effect on the chosen target node. In this section, we propose a sensor node selection scheme based on our PRS, which can provide compressive selection. Namely, the sponsor node receives all reference opinions of the target node and combines them together. This way, the sponsor node can comprehensively estimate the target node from different resources including itself and the reference nodes. Thus the opportunity of malicious nodes being involved in the cooperative process can be largely reduced.

V. PERFORMANCE ANALYSIS

We have implemented our PRS algorithm in the network Simulator NS2 version 2.30 [13]. In our experiments, 100 sensor nodes are randomly distributed with a uniform density in a region of 100*m*×100*m* and 3 out of 100 nodes are malicious nodes, as shown in Figure 5. A fixed base station is located at the bottom.

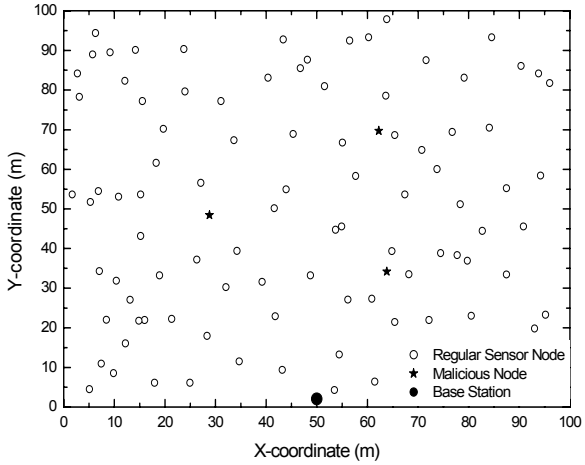

Figure 5. 100-Nodes random sensor network

In PRS, we consider the energy of a sensor node as its trust attribute and a node is dead if its energy level reaches 0. So, we assign each sensor node a different randomly generated initial energy from 0.2 to 0.6 Joules, the transmit power of a sensor node is 0.5W and the receiving power of a sensor node is 0.2W. We also assign each sensor node a generated initial trust value 0.5. The two-phase positioning algorithm is run to evaluate the performance of our PRS algorithm based on trust with sub-optimal algorithm, greedy algorithm and PADR algorithm (reference 17). Herein, we assume that the channel is collision free, and we assume a dense network, which guarantees full connectivity.

To measure the performance of our PRS algorithm, we mainly consider three metrics: (1) System stability: high system stability means that the network is not susceptible to the attacks from malicious nodes. (2) Energy consumption: we are trying to maximize minimum life span of the nodes in the network (the number of rounds which it takes for the first node to die), so that we can prolong the lifetime of sensor network. (3) Trust value evolution: we can obtain trust value evolution trend line of a normal node and a malicious node, which means we can efficiently identify a malicious node using our PRS algorithm.

A. System Stability

We run the simulation 100 times and all the analyzed data are averaged from the 100 runs. In the following, we compare the system stability for different algorithms, as shown in Figure 6, where x-axis represents time, and y-axis represents the percentage of stability.

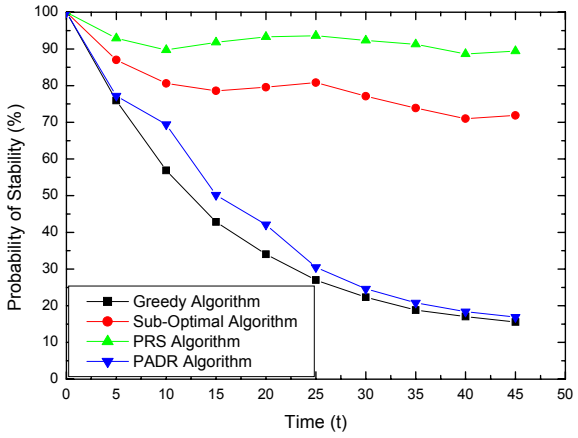

Figure 6. Comparison of system stability

As shown in Figure 6, the system performance using our PRS algorithm is much better than the sub-optimal algorithm and the percentage of stability is increased by 30-40%. The bigger the percentage is, and the more stable the system is. In the beginning, four curves are very close to each other; as the interactions among nodes increase, our PRS algorithm greatly improve the system stability and perform much better than the other three algorithms. Compared to the sub-optimal algorithm, the greedy algorithm and the PADR algorithm, the

performance of our PRS algorithm recover much faster when the attacks from malicious nodes are present, which shows our PRS algorithm can greatly improve the system stability. The experiment shows that sensor node selection based on trust are an effective way to improve system stability.

B. Energy Consumption

To further check the ability of load balancing among sensors, we investigate the situations when the sensors have unequal initial energy levels. We summarize the energy consumption conditions along the time line for different algorithms, as shown in Figure 7, where x-axis represents the number of sensor node, and y-axis represents the round when the first node dies.

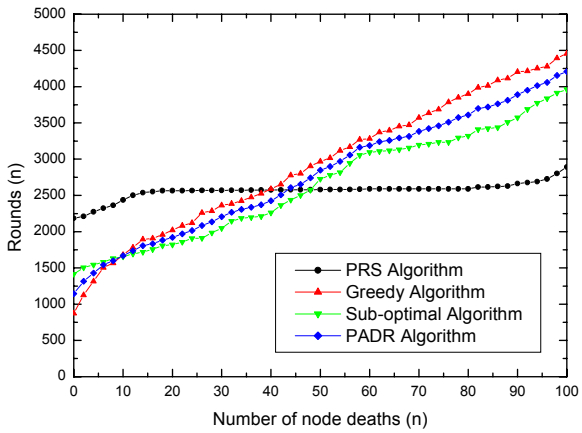

Figure 5. Comparison of energy consumption

As shown in Figure 7, the greedy algorithm always selects the next most informative sensor based on information utility and entropy, thus the sensor node will use up the energy earlier than other three algorithms. We conclude that our PRS algorithm is robust enough to balance the energy consumption among sensor nodes even if the initial energy levels of all sensor nodes are different greatly. Our PRS algorithm improves minimum life span by about 35% compared to the sub-optimal algorithm, and by about 47% compared to the PADR algorithm, and by about 60% compared to the greedy algorithm.

C. Trust Value Evolution

The trust value evolution of a normal node and a malicious node along the time line is shown in Figure 8, where x-axis represents time, and y-axis represents trust value.

As shown in Figure 8, in the beginning, the trust value of a normal node and a malicious node are both increasing gradually, however, in our PRS algorithm the false data sent by the malicious node is successfully blocked, so the trust value of the malicious node is gradually decreasing. For the normal node, as the interactions with other normal nodes increase, its trust value will increase (during the short sleeping period when the node can not participate in the interaction with other nodes, its trust value may decrease a little). In our PRS algorithm, we also consider the effect of energy. For the node with energy less than a predefined threshold, we decrease its cooperation opportunity. So the trust value of the normal node will eventually decrease.

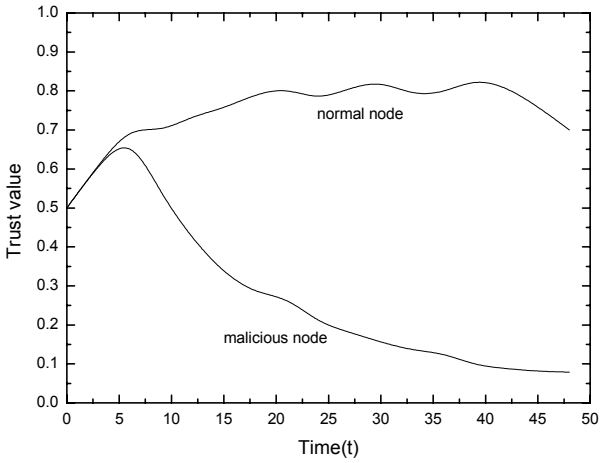

Figure 6. Comparison of trust value evolution

VI. CONCLUSIONS

In this paper, we firstly introduce the trust mechanism of the human humanity into a WSN and propose a novel power-aware and reliable scheme (PRS) for sensor selection. Based on the PRS, we propose a reliable sensor selection algorithm with power-aware for WSNs. Our algorithm not only considers the multi-attribute value of the target node based on its cooperation records among the nodes, but also uses the integrated trust value of the third-party nodes. The simulation results show that our PRS algorithm achieves a better system stability performance of sensor networks and a better lifetime performance.

ACKNOWLEDGMENTS

This work was supported by a grant from HOHAI University, China. The work of Mr. Lei Shu is supported by the Lion project supported by Science Foundation Ireland under grant no. SFI/08/CE/I1380 (Lion-2). This research was partially supported by Grant-in-Aid for Scientific Research (S)(21220002) of the Ministry of Education, Culture, Sports, Science and Technology, Japan.

REFERENCES

[1] Mohammad Ilyas and Imad Mahgoub: *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC Press, New York, Washington, D.C, 2005.

[2] Himsoon, T.; Siriwongpairat, W.P.; Zhu Han; Liu, K.J.R, Lifetime maximization by cooperative sensor and relay deployment in wireless sensor networks, *Wireless Communications and Networking Conference*, 2006. WCNC 2006. IEEE Vol.1, 3-6 April 2006, pp: 439-444

[3] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless Sensor Netowks Survey", *International Journal of Computer Networks*, 2008, Vol.52, pp: 2292–2330.
[4] A.Srinivasan, J.Wu, A survey on secure localization in wireless sensor networks, in: B. Furht (Ed.), *Wireless and Mobile Communications*, CRC Press/Taylor and Francis Group, Boca Raton/London, 2007.
[5] Haiguang Chen, Huafeng Wu, Xi Zhou, Chuanshan Gao, Reputation-based Trust in Wireless Sensor Networks, *in Proceeding of 2007 International Conference on Multimedia and Ubiquitous Engineering (MUE'07)*, 2007.
[6] M.Chu, H.Haussecker, and F.Zhao, Scalable information-driven sensor querying for ad-hoc heterogeneous sensor networks, *International Journal of Performance Computing Applications*, 2002, Vol.16, pp: 90-110.
[7] H.Wang, G. Pottie, K.Yao and D.Estrin, Entropy-based sensor selection heuristic for target localization, *Information Processing and Sensor Networks 2004*, Berkeley, California, April 2004, pp:36-45.
[8] R.C.Shan and J.M.Rabaey, Energy aware routing for low energy ad hoc sensor networks, *in proceeding of Wireless Communications and Networking Conference (WCNC)* 2002, Vol.1, pp: 350-355.
[9] Q. Li, J.Aslam and D.Rus, "Online power-aware routing in wireless sensor networks, *Proceedings of the 7th annual international conference on Mobile computing and networking*, Rome, Italy, July 2001, pp: 404-409.
[10] Tao Lin, Jiyong Wang, Guangjie Han, Jin-dong Wang, Hai Zhao, An embedded Internet cooperation network model based on trust, *Journal of China Institute of Communication*，2004, Vol.25, No.3, pp: 134-143.
[11] Blaze M, Feigenbaum J, Ioannidis J, "The role of trust management in distributed system security, Secure Internet Programming", *Issue for Mobile and Distributed Objects*, Berlin: Springer-Verlag, 1999, pp: 185-210
[12] Wang Y and Vassileva J: Bayesian network-based trust model in Peer-to-Peer Networks, *in Proceedings of Workshop on Deception, fraud and trust in agent societies at the Autonomous Agents and Multi-agent Systems (AAMAS-03)*, Australia, 2003.
[13] "The Network Simulator – NS2," http://www.isi.edu/nsnam/ns/.
[14] C.Y.Lin, W.C.Peng and Y.C.Tseng, Efficient in Network Moving Object Tracking in Wireless Sensor Networks, *IEEE Trans. On Mobile Computing*, Aug, 2006, Vol.5, No.8, pp: 1044-1056,
[15] Ahmed, I.; Mugen Peng; Wenbo Wang, Energy Efficient Cooperative Nodes Selection in Wireless Sensor Networks, *International Conference on Parallel Processing Workshops*, ICPPW 2007, 10-14 Sept. 2007, pp: 50-55.
[16] Shibo Wu, K.Selcuk Candan, Power-aware single- and multipath geographic routing in sensor networks, *Ad Hoc Networks*, 2007, No.5, pp: 974-997.
[17] Hatem M.El-Boghdadi, Power-aware routing for well-nested communications on the circuit switched tree, *Journal of Parallel and Distributed Computing*, Vol.69, 2009, pp: 135-142.

Guangjie Han is currently an Associate Professor of Department of Information & Communication Engineering at the Hohai University, China. He finished the work as a Post doctor of Department of Computer Science at the Chonnam National University, Korea, in February 2008. He received his Ph.D. degree in Department of Computer Science from Northeastern University, Shenyang, China, in 2004. He has published over 70 papers in related international conferences and journals. He has served as guest editor of International Journal of Future Generation Communication and Networking. He has served as Publicity Co-Chair of MMASN 2009，APNOMS 2008, IEIF/IEEE NPC 2007, etc. He has served as reviewer of a number of journals: (Wiley) WCMC, IJVT, JCSNC, JSS, JCCS, and ARC. His current research interests are security and trust management, localization and tracking, cooperative computing for Wireless Sensor Networks. He is a member of ACM and IEEE.

Lei SHU is a currently Specially Assigned Research Fellow in Osaka University, Japan. He received the B.Sc. degree in South Central University for Nationalities, China, 2002, and the M.Sc. degree in Kyung Hee University, Korea, 2005, and the PhD degree in NUIG, 2010. He has published over 80 papers in related conferences, journals, and books, including around 40 papers during the PhD course. He has been awarded the MASS 2009 IEEE TCs Travel Grant and the Outstanding Leadership Award of EUC 2009 as Publicity Chair. He has served as guest co-editor of International Journal of Sensor Networks, Journal of Communications; editor of 16 international journals: Information Technology Journal, Journal of Applied Sciences, etc. He has served as Program Co-Chair of PMSN 2009, Publicity Co-Chair of EUC 2009, CPSE 2009, TPC members of more than 30 conferences, including BROADNETS (08-09), ChinaCom'09, TridentCom'09, IWCMC'09, etc. He has served as reviewer of many journals, including. His research interests include wireless multimedia sensor networks, wireless sensor networks, context aware middleware, and sensor network middleware, and security. He is a member of ACM and IEEE.

Jianhua Ma is a Professor in Hosei University since 2000. Previously, he had 16 years' teaching/research experience at NUDT, Xidian University and the University of Aizu (Japan), respectively. His research 1983-2003 covered coding techniques for wireless communications, secure data/audio/ video transmissions, speech recognition and synthesis, multimedia QoS, hyper-interface, graphics ASIC, e-learning and virtual university, CSCW, multi-agents, mobile web service, P2P network, etc. Dr. Ma is the Co-EIC of the journals: Journal of Ubiquitous Computing and Intelligence, Journal of Mobile Multimedia and Journal of Autonomic and Trusted Computing, etc. He is on the editorial boards of IJCPOL, IJDET, IJWMC, IJSH, IJSIA and IJICT, and has edited over 15 journal special issues as a Guest Editor. He organized many conferences: DMS'99, CW'02, AINA'04. He is a founder of UIC and ATC, both of which started from 2005. He is the Chair of IEEE CIS Task Force on Autonomic and Trusted Computing.

Jong Hyuk Park received his Ph.D. degree in Graduate School of Information Security from Korea University, Korea. Before August, 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. He is now a professor at the Department of Computer Science and Engineering, Seoul National University of Technology, Korea. Dr. Park has published many research papers in international journals and conferences. Dr. Park has served as Chairs, program committee or organizing committee chair for many international conferences and workshops; Chair of SH, MUE, IPC, FGCN, TRUST, etc, and PC member of PerCom, ATC, EUC and so on. Dr. Park is the founder of MUE, IPC, SH. Dr. Park is the managing editor of the IJSH and SCN. Dr. Park' s research interests include Mobile robots, Digital Forensics, Security, Ubiquitous and Pervasive Computing, Context Awareness, Multimedia Service, etc. He is a member of the IEEE, KICS, KIISC, KMS, and IEICE.

Jianjun Ni is currently an Associate Professor of Department of Information & Communication Engineering at the Hohai University, China. He received his Ph.D. degree in Department of Information and Electrical Engineering from China University of Mining and Technology, China, in 2005. He has published over 20 papers in related international conferences and journals. He has served as reviewer of a number of international conferences: (ISICA 2007) The 2th International Symposium on Intelligence Computation and Applications, (CIS 2008) 2008 International Conference on Computational Intelligence and Security. His current research interests are control and decision-making, modeling and simulating of complex system, Data Fusion and Wireless Sensor Networks. He is a member of the IEEE and ACM.