A Fuzzy-based Trust Management in WSNs

Guowei Wu, Zuosong Liu, Lin Yao*, Zhenzhen Xu, and Wei Wang
Dalian University of Technology, Dalian, China
wgwdut@dlut.edu.cn, sandyliu1988@163.com, yaolin@dlut.edu.cn,
dlxzz@qq.com, oscarww@sohu.com

Abstract

Wireless sensor networks (WSNs) are composed of a large number of sensor nodes that are self-organized. The open nature of WSNs makes them easily exposed to a variety of attacks and brings many security challenges. Furthermore, because of the potentially dynamic behavior of WSNs, there is hardly any infrastructure or centralized control. To enhance the security in WSNs, it is necessary to evaluate the trustworthiness of nodes since some of them may refuse to forward packets for saving their limited resources. In this paper, we propose a fuzzy-based trust management in WSNs. All neighbors of one nodes are ranked by their trust value. Only those with higher trust values can be chosen to forward packets. Our trust model exploits multiple metrics, rather than a single metric, and converts them into a single numerical ranking. We perform an thorough evaluation of our proposed approach. The results indicate that our trust model can not only identify abnormal nodes' behaviors, but can also reduce query traffic while improving the reliability of the exchange messages.

Keywords: Wireless sensor networks, Fuzzy, Trust management

1 Introduction

Wireless sensor networks (WSNs) are composed of a large number of sensor nodes that are self-organized. These nodes are expected to carry out tasks in military and civilian applications such as battlefield surveillance, forest fire detection, patient health monitoring, and smart environment [1]. In WSNs, sensor nodes are densely deployed, and multi-hop communications are more commonly used than single-hop communications in order to conserve energy as well as to lower mutual interference. A WSN has several salient characteristics, such as dynamic topologies, bandwidth constrained, variable capacity links, energy constrained operation, limited physical security. These characteristics of WSNs make them easily exposed to a variety of attacks such as deny of service, eavesdropping, node compromising and physical disruption. So security becomes a critical issue to wireless network.

Although there are many traditional security services, such as confidentiality and authentication for WSNs[12][14]. Most of them can work well depending on the assumption that all the nodes are cooperative and willing to relay the messages. However, because wireless mobile nodes are usually constrained by limited power and computation resources, some selfish nodes may refuse to forward packets in order to conserve their limited resources. Therefore, recently it has been recognized that new security mechanisms, beyond conventional security services, must be developed in order to defend attacks that may be launched by selfish and malicious entities [4][8]. The concept of ”Trust” originally derives from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity. Trust management in WSNs is needed when participating nodes, without any previous interactions, desire to establish a network with an acceptable level of trust relationships among themselves [6].

Journal of Internet Services and Information Security (JISIS), volume: 3, number: 3/4, pp. 124-135

*Corresponding author: Dalian University of Technology, No.2 Linggong Road, Ganjingzi District, Dalian City, Liaoning Province, China, Tel: +86-41184706116

In this paper, considering the security threat from the selfish malicious nodes, we propose a fuzzy-based trust management in WSNs. Based on this trust management, every node can isolate misbehaving nodes based on the trust values. Furthermore these trust information can also be shared with its neighbors to evaluate the trust degree of a certain neighbor. Furthermore, we can effectively assess direct or indirect trust between users in this trust management scheme. We combine the probability of successful interactions, feedback of messages exchanging and the battery energy into a composite trust metric for selecting the highly trustworthy nodes for forwarding messages . Our scheme is able to maximize message delivery ratio without incurring a high delay or a high message overhead. Our technique has the following salient features:

(i) Every node has the same role and we do not need to assign any special functions to a subset of nodes.

(ii) Our trust model makes no assumptions on Pisson or Bayesian in order to compute trust. This is different to other trust models [13][19][16].

(iii) Instead of using a single trust metrics, we adopt different kinds of trust metrics and calculate them according to their different characteristics.

(iv) We use fuzzy set to value the credible of recommendation trust information and represent the belief of users' trust value instead of 1 or 0.

The remainder of this paper is organized as follows. In section 2, we introduce the foundations of trust evaluation. In section 3, we present the trust calculation based on fuzzy sets. The simulation results are given in Section 4. In Section 5, we describe the related work.

2 Trust evaluation foundations

In this section, we will introduce the trust metrics we used and the relationship of these trust metrics.

A. Trust Concepts

The concept of ”Trust” originally derives from social sciences and is defined as the degree of subjective belief about the behaviors of a certain entity. In social society, trust always refers to the trusting belief, that one believes that the other person is willing to and able to act in the other person's best interests. Although definitions and classifications of trust have been borrowed from the social science, there is no clear consensus on the definition of trust in Computer Networks. In this paper, we adopt the trust concept proposed in [4] where trust is the belief that an entity has about other nodes, from their past experience, knowledge about the entity's nature and/or recommendations from other nodes.

B. Trust Metrics

In our scheme, we adopt three trust metrics, the probability of successful interactions, feedback of messages exchanging and battery energy.

The probability of successful interactions: In many existing trust models, the probability of successful interactions is chosen as the basic trust metric [11]. In this paper, we assume that every node uses omni-directional transceivers to monitor its neighbors in the promiscuous mode. Therefore, every node can calculate the Ns_{ij} (the total number of packets sent to n_j by n_i) and Nf_{ji} (the total number of packets forwarded for n_i by n_j). According to these, we can calculate the probability of successful interactions as follows:

$$Psi_{ij} = \frac{Nf_{ji}}{Nf_{ji} + \lambda(Ns_{ij} - Nf_{ji})} \quad (1)$$

Here λ represents the *weight* of the negative behavior which can be seen as a penalty to the selfish node action. The bigger λ, *the higher* is the penalty.

Feedback of messages exchanging: We use Fme_{ij} to denote the Feedback of messages exchanging between n_i and n_j. Whenever n_i and n_j have direct interaction experiences, they can have a trust judgment about each other. Here, Fme_{ij} is used as a metric to represent the trust attitude of n_i towards n_j.

Energy : In WSNs,sensors are usually constrained by limited power and computation resources. Moreover, we need to tell whether a certain node has the ability for the services. So we choose battery energy as a metric to determine the ranking order of neighbors. In our scheme, we adopt the method proposed in [21] to detect a neighbor's energy, denoted as E_{ij}.

C. Trust Relationship

In this paper, a node evaluate the trust value of a certain node based on both direct and recommendation information. The trust relationship is shown in Figure 1. According to the figure, n_i determines the trust level of n_j based solely on n_i's direct experiences with n_j. While n_i does not have any direct experiences with n_k, then it can evaluate n_k's trust value by gathering the trust evaluation information of n_k from its neighbors or other nodes. For example, n_i has the direct interaction experiences with n_j while n_j has the direct interaction experiences with n_k. Then n_j may forward the direct trust values of n_k to n_i, so n_i can use the recommendation information to evaluate the trust level of n_k.

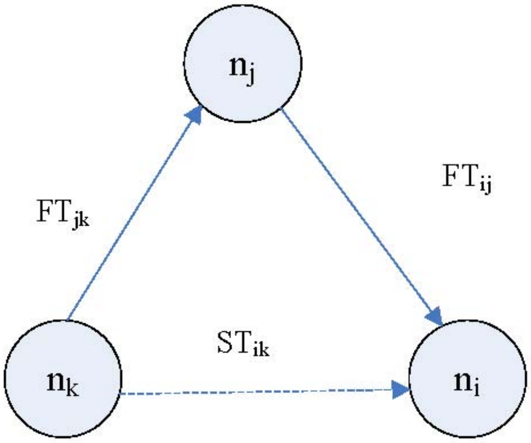


Figure 1: Trust Relationship

3 Trust calculation

Since trust always depends on the observation or recommendations, it will lead to subjectivity and uncertainty characteristics. What is more, as trust is usually used to describe a complex nodes' behaviors, it is not clear and accurate in most cases. Therefore, we cannot simply use 1 or 0 to describe trust value. In this paper, we adopt fuzzy set to solve this problem which is used to value the credible of recommendation trust information and represent the belief of users' trust value instead of 1 or 0.

Different from other trust models, we divide the trust metrics into two categories based on their characteristics. For example, we can use the Psi_{ij} (probability of successful interactions) and Fme_{ij} (feedback of messages exchanging) as the recommendation information. While the E_i can only be used when we select the next hop node. For the recommendations, we use fuzzy sets to calculate them.

Whenever n_i has a direct experience with n_j, n_i will has a trust opinion about it and store the trust information in the following vector:

$$< \text{destination}, Psi_{ij}, Fme_{ij} >$$

To evaluate these trust information, we have to calculate its trust degree by using fuzzy mathematics. In this paper, we assign four trust levels to every node, that is, $V = \{v_1, v_2, v_3, v_4\}$ which represent ”fully trust”, ”relatively trust”, ”general trust” and ”not trust” respectively. According to these four trust levels, we can use the membership function to calculate the trust degree for each metric. The membership degree function is shown in Figure 2. The x-axis represents the value of this metric and the y-axis represents the membership degree. We can see the membership degree of v_1 increases from 0 while the membership degree of v_4 decreases from 1. For level v_2 and v_3, they have the same membership function image as shown in Figure 2. The membership degree is 1 when the u_1 falls right into the middle and linear decreasing process is done from midpoint to both sides.

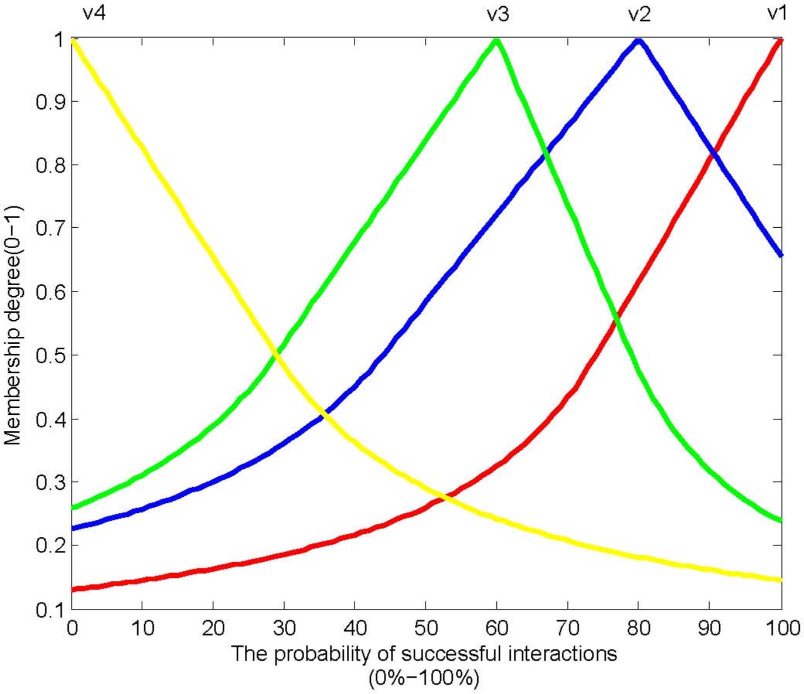


Figure 2: Membership degree function

Based on the trust degree, we can get the first hand matrix FH, where FH_{ij} represents the membership degree of metrics i to comprehensive evaluation level j.

$$FH = \begin{pmatrix} FH_{11} & FH_{12} & FH_{13} & FH_{14} \\ FH_{21} & FH_{22} & FH_{23} & FH_{24} \\ FH_{31} & FH_{32} & FH_{33} & FH_{34} \end{pmatrix} \tag{2}$$

As we know, second hand trust information is formed by exchange FH information between neighbors. Therefore, we can calculate SH (second hand information)as well. To evaluate the trust value of a certain node, we need to consider both first and second hand information. Obliviously, in most cases we consider that the first hand information is more important than second hand information. So, we introduced ω to represents the weight of the first hand information and we can adjust the proportion by changing the value of ω, $R = \omega \cdot FH + SH$.

Finally combining the E_i (battery energy) with trust information, we can rank the neighbors when we decided to forward messages as follows. Here we use w_1, w_2 to represent the weight of trust information and battery energy. According to the ranking order, the sender chooses the more trusted neighbors to forward the key request messages. The percentage of nodes may vary as the application changes.

$$Trust_value = w_1 * \frac{\sum_{i=1}^{n} u(v_i) \cdot {s_i}^k}{\sum_{i=1}^{n} {s_i}^k}, U = \{4,3,2,1\} + w_2 * E_j \tag{3}$$

4 Performance Evaluation

4.1 Simulation setup and configuration parameters

We use the ONE simulator [3] in our simulations to evaluate our Fuzzy Trust Model. In this section, we will first introduce the setup of our experiments and then investigate the scheme performance. We focus on the delivery ratio for the destination and the number of transmitted messages due to the delivery (overhead). The parameters used in the simulations are summarized in Table 1.

In our simulation, we adopt the more sophisticated version of the map-based movement model (ShortestPathMapBasedMovement) using Dijkstra's shortest path algorithm to find its way through the map area. Once a node reaches its destination, it waits for a pre-defined pause time. Then a new random map node is chosen and it moves toward the map node using the shortest path that can be taken using only valid map nodes. The map is based on Helsinki which is shown in the Figure 4 and the simulation scenario is shown in the Figure 5.

4.2 Protection against selfish nodes

In our scheme, we assume that there are some selfish nodes in the network who may refuse to forward messages for others to save its resource. One of the most important thing for trust management is to distinguish selfish nodes. Here, we present a simple 8-nodes network, among which nodes 3 and 7 are selfish. The selfish nodes try to pretend normal during early stages and begin to behave selfishly by refusing to forward messages for others. We calculate the average trust value of each node after a while. The results are shown in Figure 3. From the results, we can easily distinguish normal nodes and selfish nodes.

4.3 Protocol comparison

We conduct a comparative analysis, contrasting our trust model with T-PROPHET in [17] and non-trust based epidemic (Epidemic) [23]. In [17], T-PROPHET is proposed which used the positive feedback message as the evidence of the forwarding behavior of a node. They also consider both direct observation and indirect recommendations. For epidemic routing scheme, a message carrier forwards a message to every encountering user whenever the node has not seen the user before.

4.3.1 Comparison of delivery ratio

Figure 6 compares the message delivery ratio generated by our trust protocol against T-PROPHET [17] and epidemic routing [23]. The results shows that the epidemic routing achieves the best performance in delivery ratio. This is because it forwards messages to every encounters. Our trust-based context routing scheme has better performance than T-PROPHET, because we chose better trust metrics to make the best choice for selecting the next hop.

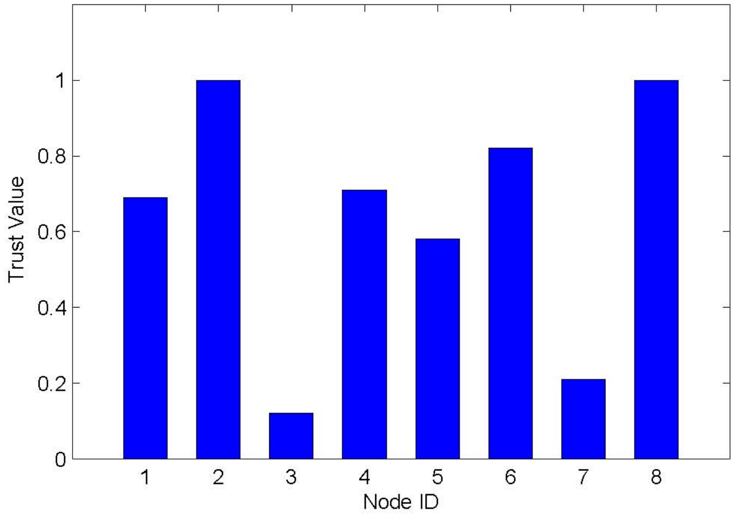


Figure 3: Trust value of 8 nodes

Table 1: Parameters used for simulation

Network area	4500×3400 m^2
Simulation time	12 hours
TTL time	5 hops
Warmup time	1000 sec
Number of total nodes	300
Ratio of selfish nodes	0-45%
Speed	1-30 m/s
Transmission rate	2 Mbps
Mobility pattern	ShortestPathMap BasedMovement

4.3.2 Comparison of overhead

Figure 7 compares the overhead of the three routing schemes. We calculate the copies propagated for per message. In the non-trust scheme, all nodes are trusted. For epidemic routing, all neighbors are utilized to forward the messages, resulting in a large overhead. However our trust model and T-PROPHET reduces the overhead significantly with the help of selecting some to the neighbors to forward messages instead all of them based on trust or context information. Our trust-based context routing scheme further reduces the overhead compared to the T-PROPHET, demonstrating the benefits of its accurate trust relationship. When there are more and more selfish nodes in the network, the overhead increases because of the negative effect caused by the selfish nodes' dropped packets. However by increasing the number of selfish nodes, our trust-based context routing scheme can still guarantee a better performance in delivery ratio while controlling the overhead.

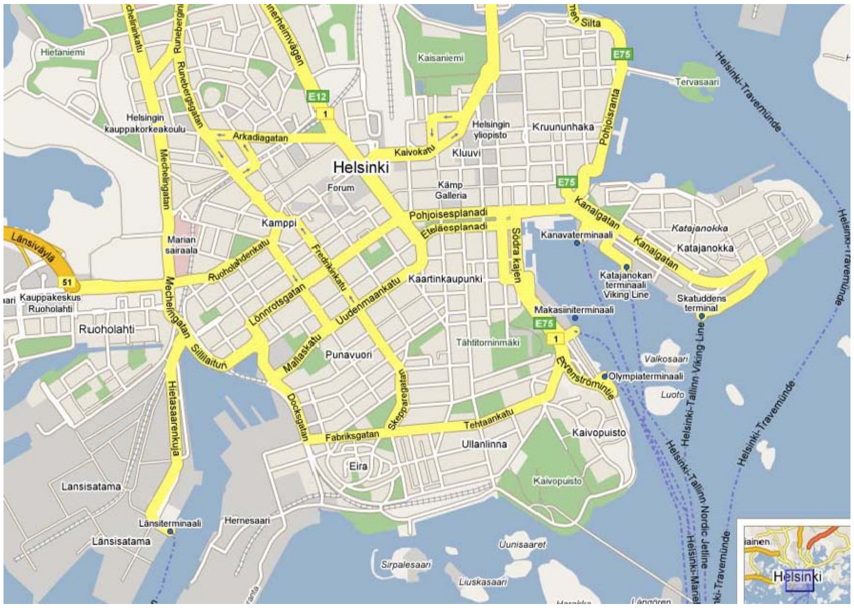


Figure 4: Helsinki simulation area (map data provided by Maanmittauslaitos, 2007)

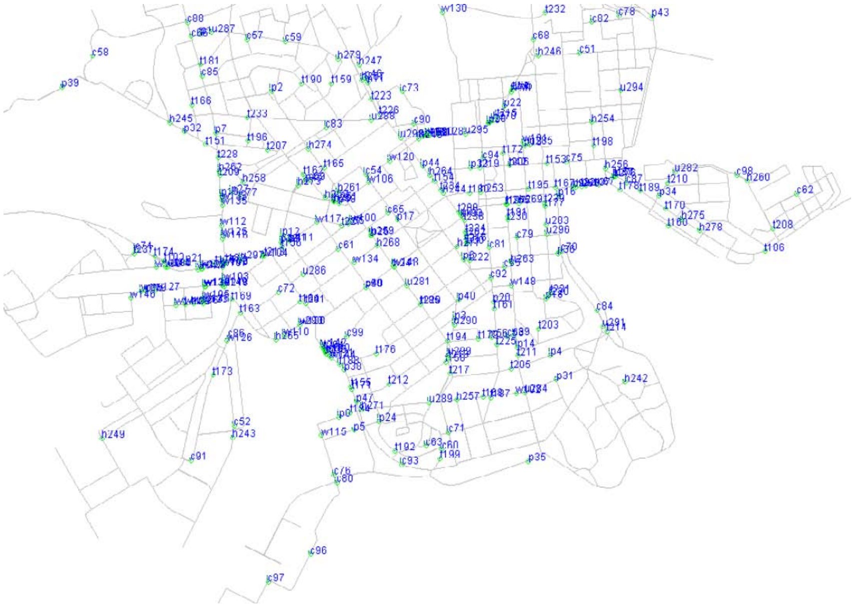


Figure 5: Simulation scenario

5 Related Work

In this section we summarize trust management schemes that have been developed for WSNs. We describe trust management schemes based on specific design purposes such as secure routing, authentication,and key management.

A. Secure Routing

In [24], the authors proposed a CONFIDANT protocol based on the traditional routing, Dynamic Source Routing(DSR). In this trust model, every node monitors the behavior of its next hop neighbors in

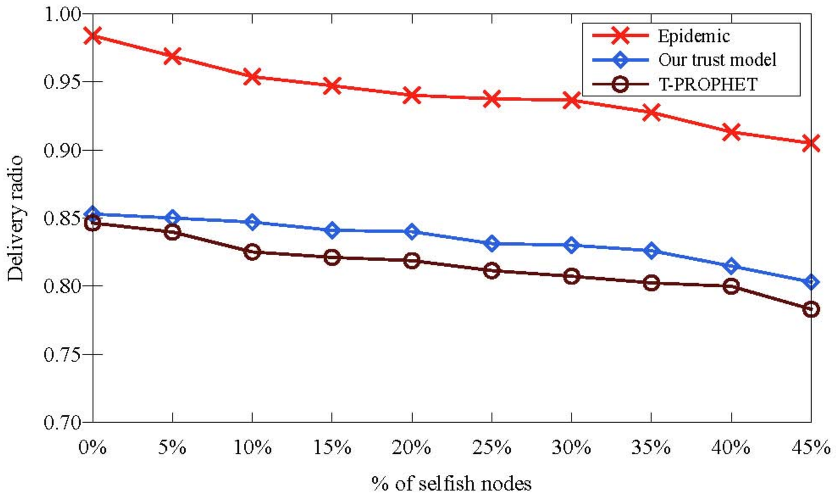


Figure 6: Delivery ratio with different numbers of selfish nodes. The number of nodes in the network is $N = 300$.

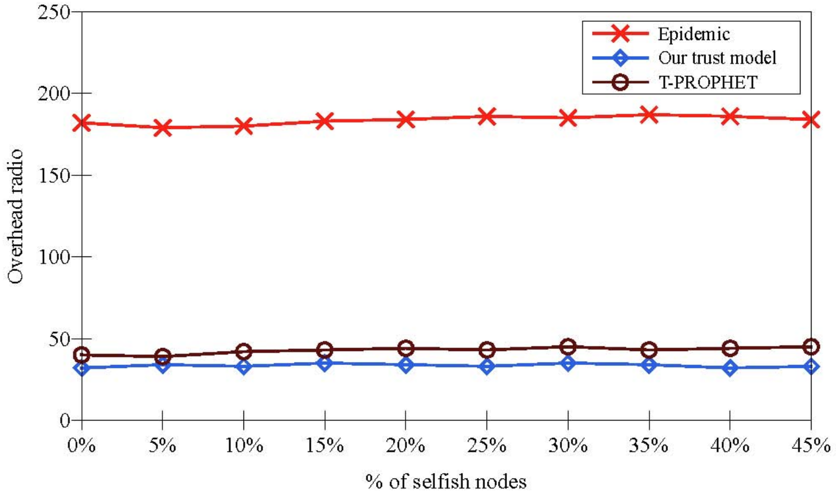


Figure 7: Overhead with different numbers of selfish nodes. Here overhead represents the number of copies propagated per message.

a the same way of watchdog. Then the information is given to the reputation system which will update the trust value of each user. A reputation-based trust management scheme is proposed in [15]. The scheme consists of a watchdog that monitors node behaviors and a pathrater to collect reputation information. This trust management is based on the DSR (Dynamic Source Routing).

In [20], a reputation-based trust management scheme called SORI (Secure and Objective Reputation-based Incentive) is proposed. This trust scheme isolates selfish behaviors by using quantified objective measures and reputation propagation. In [22], authors proposed a distributed mechanism to distinguish selfish nodes in MANETs. Although this work considers more aspects of trust such as transitivity and subjectivity, it used only packet forwarding behaviors to calculate trust values. In [10], the authors concern with the formation of reputation rather than with the detection and response components. The scheme first formulate a stochastic process based on certain assumptions and then derive the ”mean” ordinary differential equation by averaging the dynamics. Furthermore, it evaluates a system's tolerance to untrusted nodes;

In [9], a SocialTrust framework for aggregating trust in online social networks is proposed to guarantee the safety management of credible social information. They made use of three key factors for trust establishment in online social networks C trust group feedback, distinguishing the users relationship quality from trust, and tracking user behavior to describe a principled approach for assessing each component.

In [25], authors used small word characteristics to improve the traditional trust aware recommendation system TARS, and to reduce the time complexity. Based on small world theory, in [26], a MSN trust model is proposed. Furthermore the scheme used share character factors, such as credible feedback of digital content, feedback weighting factor and user share similarity to identify the trust value for every user.

B. Authentication

[5], a secure public key authentication service is proposed. This authentication service is based on trust model and network model to prevent nodes from obtaining false public keys of the others when there are malicious nodes in the network. And the trust is evaluated based on both direct monitoring and recommendation.

[2], the authors proposed a security model for low-value transactions which focus on authentication in ad-hoc networks. This scheme makes use of recommendations and references to derive a trust relationship and is scalable with respect to security.

C. Key Management

In [18],authors proposed a fully distributed public key certificate management system based on trust graphs and threshold cryptography. Trust relationship is developed based on the trust graph in order to protect normal users against malicious nodes, which may sign false public key certificates for other nodes in the network. In [7], a trust management protocol for mission-driven group communication systems was proposed. Hierarchical modeling techniques is used based on stochastic Petrinets.

6 Conclusion

In this paper, we have proposed a fuzzy-based trust model for WSNs. When there are selfish nodes in the network, the trust model allow nodes to rank their neighbors, based on the direct and indirect information obtained from other users. Furthermore instead of using only one metric, we combine three trust metrics to evaluate the trust value. We have analyzed and evaluated our proposed trust model through simulations. Our results have demonstrated that our fuzzy-based trust model designed to maximize delivery ratio can effectively trade off message overhead for a significant gain in delivery ratio.

Acknowledgement

This research is sponsored in part by the National Natural Science Foundation of China (contract/grant number: No. 61173179 and No.61202441). This research is also sponsored in part supported by the Fundamental Research Funds for the Central Universities (No. DUT13JS10) and by the Major National Science and Technology Special Projects High-Nuclear-Based Project of China under Grant No. 2012ZX01039-004-21.

References

[1] C. Alcaraza, J. Lopeza, R. Romanb, and H.-H. Chenc. Selecting key management schemes for WSN applications. *Computers Security*, 31(8):956–966, November 2012.

[2] W. Andre and G. Thonet. A distributed light-weight authentication model for ad-hoc networks. In *Proc. of the 4th International Symposium on Information Security and Cryptology (ICISC'01), Seoul, Korea, LNCS*, volume 2288, pages 341–354. Springer-Verlag, December 2001.

[3] K. Ari, J. Ott, and T. Karkkainen. The ONE simulator for DTN protocol evaluation. In *Proc. of the 2nd International Conference on Simulation Tools and Techniques (SIMUTools'09), Rome, Italy*, pages 55–64. ACM, March 2009.

[4] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis. The role of trust management in distributed systems security. *Secure Internet Programming*, 1603(1):185–210, January 1999.

[5] N. E. CH and M. R. Lyu. Trust and clustering-based authentication services in mobile ad hoc networks. In *Proc. of the 24th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS 2004 Workshops), Tokyo, Japan*, pages 582–587. IEEE, March 2004.

[6] J.-H. Cho, S. A., and I.-R. Chen. A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys and Tutorials*, 13(4):562–583, October 2004.

[7] J.-H. Choa, A. Swamia, and I.-R. Chenb. Modeling and analysis of trust management with trust chain optimization in mobile ad hoc networks. *Network and Computer Applications*, 35(3):1001–1012, May 2012.

[8] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava. Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 4(15):1–12, May 2008.

[9] C. James, L. Liu, and S. Webb. The socialtrust framework for trusted social information management: Architecture and algorithms. *Information Sciences Special Issue on Collective Intelligence*, 180(1):95–112, January 2008.

[10] M. Jochen and J.-Y. L. Boudec. Analysis of a reputation system for mobile ad hoc networks with liars. *Performance Evaluation*, 65(3):212–22, March 2008.

[11] L. Junhai, X. Liu, and M. Fan. A trust model based on fuzzy recommendation for mobile ad-hoc networks. *Computer Networks*, 53(14):2396–2407, September 2009.

[12] P. Kamat, Z. Y, and T. W. Enhancing source-location privacy in sensor network routing. In *Proc. of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05), Columbus, Ohio, USA*, pages 5996–608. IEEE, June 2005.

[13] Koutsonikolas, Dimitrios, and C.-C. Wang. Effcient network-coding-based opportunistic routing through cumulative coded acknowledgments. *IEEE/ACM Transactions on Networking (TON)*, 19(5):1368–1381, December 2011.

[14] Y. L, L. Bing, W. Guowei, Y. Kai, and W. Jia. A biometric key establishment protocol for body area networks. *Distributed Sensor Networks*, 2011(1):1–10, May 2011.

[15] S. Marti, T.J.Giuli, Kevin.Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proc. of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), Boston, Massachusetts, USA*, pages 255–265. ACM, August 2000.

[16] M. Musolesi and C. Mascolo. A community based mobility model for ad hoc network research. In *Proc. of the 2nd International Workshop on Multi-hop Ad Hoc Networks: From Theory to Reality (REALMAN'06), Florence, Italy*, pages 31–38. ACM, May 2006.

[17] L. Na and S. K. Das. A trust-based framework for data forwarding in opportunistic networks. *Ad Hoc Networks*, 11(4):1497–1509, June 2013.

[18] M. Omara, Y. Challalb, and A. Bouabdallahb. Reliable and fully distributed trust model for mobile ad hoc networks. *Computers and Security*, 28(3):199–214, May 2009.

[19] H. Pan and J. Crowcrof. Bubble rap: Social based forwarding in delay-tolerant networks. *IEEE Transactions on Mobile Computing*, 10(11):1576–1589, November 2011.

[20] H. Qi, D. Wu, and P. Khosla. SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks. In *Wireless Communications and Networking Conference (WCNC'04), Atlanta, Georgia, USA*, pages 825–830. IEEE, March 2004.

[21] V. R and P.T.Vanathi. Energy aware routing for wireless sensor networks. In *Proc. of the 7th International Conference on Signal Processing, Communications and Networking (ICSPCS'09), Chennai, India*, pages 545–550. IEEE, February 2009.

[22] S. Soltanali, S. Pirahesh, S. Niksefa, and M. Sabaei. An efficient scheme to motivate cooperation in mobile ad hoc networks. In *Proc. of the 3rd International Conference on Networking and Services (ICNS'07), Athens, Greece*, pages 98–103. IEEE, June 2007.

[23] A. Vahdat and D. Becker. Epidemic routing for partially connected ad hoc networks. Technical Report 200006, Department of Computer Science, Duke University, 2000.

[24] Y.Rebahi, V.Mujica, and D.Sisalem. A reputation-based trust mechanism for ad hoc networks. In *Proc. of the 10th IEEE Symposium on Computers and Communications (ISCC'05), Murcia, Cartagena, Spain*, pages 37–42. IEEE, June 2005.

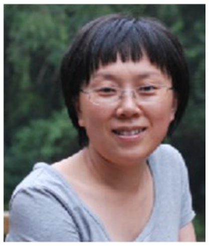
[25] W. Yuana, D. Guana, Y.-K. Leea, and S. Leea. Improved trust-aware recommender system using small-worldness of trust networks. *Knowledge-Based Systems*, 23(3):232–238, April 2011.

[26] Z. Zhang and K. Wang. A trust model for multimedia social networks. *Social Network Analysis and Mining*, 18(1):1–11, July 2012.

Author Biography

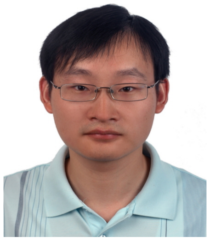
Guowei Wu received B.E. and Ph.D. degrees from Harbin Engineering University, China, in 1996 and 2003, respectively. He was a Research Fellow at INSA of Lyon, France, from September 2008 to March 2010. He has been an Associate Professor in School of Software, Dalian University of Technology (DUT), China, since 2003. Dr. WU has authored three books and over 20 scientific papers. His research interests include embedded real-time system, cyber-physical systems (CPS), and wireless sensor networks.

Zuosong Liu received B.E. degree from Dalian University of Technology, China. Currently she is a M.E. Candidate in School of Software, Dalian University of Technology. Her research interests include wireless sensor networks security and cyber-physical systems (CPS).



Lin Yao received B.E. and Master degrees from Harbin Engineering University, China, in 1998 and 2001, respectively, and received Ph.D. degree from Dalian University of Technology, China in 2011. She has been a lecturer in School of Software, Dalian University of Technology (DUT), China, since 2004. She has co-authored one book and over ten scientific papers. Her research interests include pervasive computing, cyber-physical systems (CPS), and wireless sensor networks.

Zhenzhen Xu received B.E. degree from Nanjing Normal University, China, in 2002 and received Ph.D. degree in Shenyang Institute of automation, Chinese Academy of Sciences, China, in 2008. She has been a lecturer in School of Software, Dalian University of Technology (DUT), China, since 2003. Her research interests include Scheduling algorithms and intelligent optimization algorithms.



Wei Wang received B.E. degree form Northeast Normal University, China, in 2002 and received Ph.D. degree in Dalian University of Technology in 2008. He has been an associate professor in The Institute of Mathematics, Dalian University of Technology (DUT), China since 2008. His research interests include nonlinear partial differential equation.