2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems

Trust Models in Wireless Sensor Networks and Online Social Networks: A Comparative Study

Wenjun Jiang† and Jie Wu‡
†*School of Information Science and Engineering, Hunan University, P. R. China*
‡*Department of Computer and Information Sciences, Temple University, USA*

***Abstract*—Wireless sensor networks (WSNs) are networks based on on the cooperation of small-sized nodes. Those nodes are mainly characterized by their low energy consumption, low cost, and wireless communication; Meanwhile, online social networks (OSNs) are becoming a popular way to meet people and keep in touch with friends. To improve the security performance in WSNs and the service quality in OSNs, trust models are commonly incorporated in both network environments. In this article, we present the first comparative study of trust models in WSNs and OSNs. We first provide a comparison of the features of WSNs and OSNs, and we provide a simple discussion of trust management in WSNs and OSNs. Next, we review and compare existing trust models for WSNs and OSNs in the literature. Finally, we conduct some discussion and point out the future directions, especially on how to enhance the trust management in a network by learning from the other type.**

***Keywords*-online social networks (OSNs), trust models, Wireless Sensor Networks (WSNs)**

I. Introduction

Wireless sensor network (WSN) is an emerging class of systems made possible by cheap hardware, advanced programming tools, complex algorithms, long lasting power sources, and energy efficient radio interfaces [1]. WSN is a new paradigm in designing fault-tolerant mission critical systems, used to enable varied applications like threat detection, environmental monitoring, traditional sensing and actuation, and much more. It is an emerging area of interdisciplinary research among people in electrical engineering, computer science, and various other disciplines. Meanwhile, online social networks (OSN) provide a basis for maintaining social relationships, for finding users with similar interests, and for locating content and knowledge that has been contributed or endorsed by other users [2].

Security is one of the most important topics in both WSNs and OSNs, for which trust management is found to be a necessity. The conventional view of security based on cryptography alone is not sufficient for the unique characteristics and novel misbehavior encountered in WSNs and OSNs. Fundamental to this is the observation that cryptography cannot prevent the malicious or non-malicious insertion of data from internal adversaries or faulty nodes [3]. In this paper, we conduct a comparative study of trust models in WSNs and OSNs, with the goal of benefiting both.

A number of research groups are working on WSNs, since this kind of network has broad applications ranging from the military to the environment, passing through sanitary applications, domestics, Intelligent Transportation Systems (ITS) [4], [5], etc. Similarly, OSNs have attracted a large amount of users and the broad attention of researchers. Facebook has billions of users; More than 200 millions of users are using Tencent QQ at the same time; Twitter has more than 100 million users. All of them indicate the popularity of OSNs.

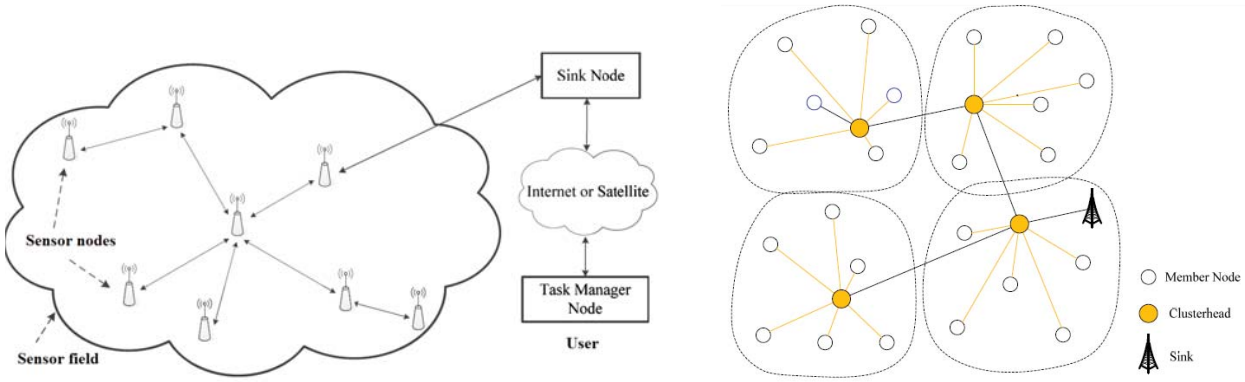
WSNs are susceptible to many security threats. Furthermore, because of communication, computation, and delay constraints of WSNs, traditional security mechanisms cannot be used [6]. Trust management models have been recently suggested as an effective security mechanism for WSNs. Similarly, trust becomes an essential and important element of a successful social network [7]. Trust is a multidimensional, complex, and context-dependent concept [8]. Considerable research has been done on modeling and managing trust. In this paper, we present a brief survey on various trust models that are geared towards WSNs and OSNs, respectively. We try to conduct a comparative study, as to better understand trust models and their effects on different network environments.

Our contributions are threefold:

- We analyze the features of WSNs and OSNs, respectively.
- We conduct a comparative study of trust models in WSNs and OSNs.
- We provide discussions on enhancing trust management in one network by learning from that of the other.

Note that there are already some review articles providing surveys on different aspects of trust. Just to mention a few: Yu et al. [6] analyze how to resist attacks with a trust scheme, and they categorize various types of attacks and countermeasures related to trust schemes in WSNs. Cho et al. [8] provide a survey of trust management schemes developed for mobile ad hoc networks (MANETs) and discuss generally accepted classifications, potential attacks, performance metrics, and trust metrics in MANETs. Marmol et al. [9] present a pre-standardization approach for trust and/or reputation models in distributed systems, including

978-1-4799-6036-1/14 $31.00 © 2014 IEEE
DOI 10.1109/MASS.2014.71



(a) (b)

Figure 1. The structure of (a) a typical wireless sensor network; (b) a cluster-based wireless sensor network.

P2P, ad-hoc networks, multi-agent systems, or Wireless Sensor Networks. There has been a wide review of them carried out, involving the extraction of common properties and the providing of some pre-standardization recommendations. Jøsang et al. proposed an important survey on the notions, categories, and applications of trust and reputation systems for online service provisioning [10]. Sherchan et al. [7] presented a comprehensive review of trust in social networks, in which they surveyed the literature of existing reviews, and examined the definitions and measurements of trust through the prisms of sociology, psychology, and computer science. There are more works on reputation, a concept that is closely related with trust. We recommend [10], [11], and [12] for the comprehensive review in the reputation system (or hybrid system of trust and reputation).

The remainder of this paper is organized as follows: Section II summarizes the features of WSNs and OSNs, respectively. Section III surveys some representative trust models in WSNs and OSNs, respectively. Section IV introduces validation approaches used by trust models in WSNs and OSNs. Finally, Section V concludes this paper and discusses some open challenges that deserve more attention in the future.

II. Features of WSNs and OSNs

In this section, we summarize the features of WSNs and OSNs, respectively. We mainly consider their construction, their network structures, network scales, and the meanings of trust in them. These features can be taken as a basis for trust model designs and implementations.

A. Features of WSNs

Construction: WSNs are composed with several sensors that are usually small, with low cost and low power. Moreover, those sensors can be left unattended. In WSNs, the nodes are physically accessible by other people including adversaries, and have been known to expose cryptographic materials such as the encryption keys and other important data.

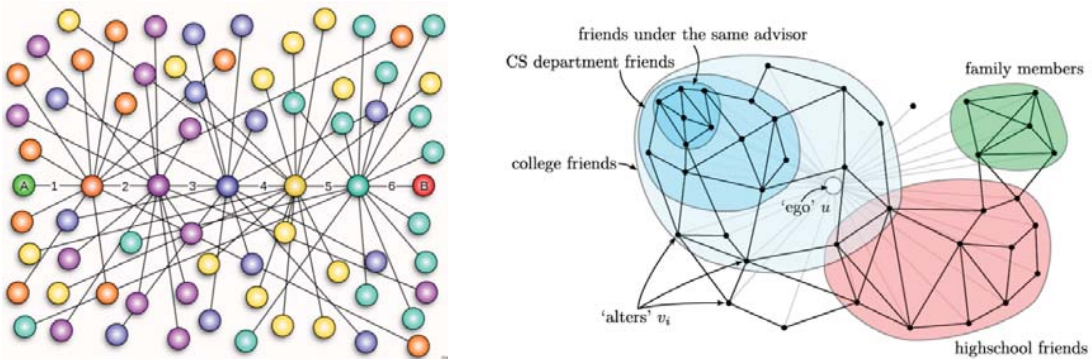
Structure: Fig. 1 shows the typical structure of a WSN, and a cluster-based WSN. Clustering provides one of the best solutions for communication in WSNs, due to its inherent energy saving qualities and its suitability for highly scalable networks [13]. Clustering naturally facilitates data aggregation, an energy efficient technique where nodes forwards data to a cluster head for processing and fusion before transmitting to base station. Therefore, many WSNs have a hierarchical structure, which has several small groups (called clusters), and each group has a cluster head.

Trust and Trust Management in WSNs. Trust has different meanings in different contexts, even in WSNs only. For instance, in sensor network security, trust is a level of assurance about a key's authenticity that would be provided to the sensor node by some centralized trusted body [14], [15]. In wireless sensor network reliability, trust is used as a measure of a node's competence in providing a required service [16]–[18]. In this paper, we mainly consider the latter meaning.

From some point, trust management in WSNs is much more challenging than in OSNs, which can be taken as centralized environments. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to changes in the topology induced by node mobility or node failure. Also, resource limitations lead to a higher requirement on the efficiency and communication/memory cost. For instance, due to resource limitations, trust scales in WSNs are usually represented as integers, e.g., from 1 to 100 [19].

B. Features of OSNs

Construction: OSNs are organized around users. Generally, the scale of an OSN is much larger than that of a WSN. Therefore, although it has fewer limitations on resources, the efficiency and scalability are also facing challenges.



(a) (b)

Figure 2. The illustration of (a) small-world network; (b) an example online social network. (We get the two figures online.)

Table I
COMPARISON OF EXISTING GRAPH-BASED TRUST MODELS IN OSNS.

Model	Category	Computation Model	Trust Value	Dimension	Trust Information	Test data set
TidalTrust [20]	simplification	linear model	discrete, [1, 10]	1	trust	FilmTrust
SWTrust [21]	simplification	linear model	continuous, [0, 1]	1	trust	Epinions
RN-Trust [22]	analogy	resitive network	continuous, [0, 1]	1	trust	-
FlowTrust [23]	analogy	network flow	continuous, [0, 1]	2	confidence, trust	-

Structure: From the view of network structure, OSNs fall into the range of complex networks. It has been studied to bear the characteristics of small-world networks [24], [25]: higher clustering and short distances between any two nodes. Based on these features, searching proper trust evidence in large OSNs can be completed. Fig. 2 illustrates the small-world network property, and shows an example OSN which consists several communities.

Trust and Trust Management in OSNs. Trust in OSNs also has many definitions and categories, such as those mentioned in [7], [10]. If not specified, we take the one defined in [20] as a default, saying that, trust in a person is a commitment to an action, based on a belief that the future actions of that person will lead to a good outcome.

Unlike WSNs, in which a node usually has limited resources, a node in an OSN is usually supposed to own enough resources. There is, typically, also a centralized platform which can be taken as a server of an OSN that has enough storage and computation capabilities. Therefore, trust models in OSNs can focus more on the accuracy and the real effects.

III. TRUST MODELS IN WSNS AND OSNS

In this section, we review some representative trust models in WSNs and OSNs, respectively.

A. Trust Models in WSNs

Traditional trust management schemes developed for wired networks are not well suited for sensor networks due to their higher consumption of resources such as memory and power. A few comprehensive trust management schemes have been proposed for WSNs. E.g., Reputation-based Framework for Sensor Networks (RFSN) [3], Agent-based Trust and Reputation Management (ATRM) [26], Parameterized and Localized trUst management Scheme (PLUS) [27], and Group-based Trust Management Scheme (GTMS) [19].

RFSN. Ganeriwal et al. [3] proposed RFSN, where nodes maintain reputations for other nodes and use it to evaluate their trustworthiness. RFSN provides a scalable, diverse, and generalized approach for countering all types of misbehavior resulting from malicious and faulty nodes. The authors employ a Bayesian formulation, specifically, a beta reputation system for reputation representation, updates, and integration.

ATRM. Boukerche et al. [26] proposed an ATRM scheme. The objective of the scheme is to manage trust and reputation locally with minimal overhead in terms of extra messages and time delay. They present extensive performance evaluation results, which clearly show that trust and reputation can be computed in WSNs with minimal overhead.

PLUS. Yao et al. [27] proposed PLUS, where each sensor node maintains highly abstracted parameters, rates the trustworthiness of its interested neighbors to adopt appropriate cryptographic methods, identify the malicious nodes, and share the opinion locally. Results of a serious of simulation experiments show that the proposed scheme can maximize security as well as minimize energy consumption for WSNs.

GTMS. Shaikh et al. [19] proposed a new lightweight group-based trust management scheme (GTMS) for WSNs, which employs clustering. GTMS evaluates the trust of a group of sensor nodes, instead of evaluating a single node at a time. This approach requires less memory to store trust records at each sensor node in the network, so as to reduce the cost of trust evaluation. Moreover, GTMS works on two topologies: intragroup topology, where distributed trust management approach is used, and intergroup topology, where the centralized trust management approach is adopted. This methodology helps to drastically reduce the cost associated with the trust evaluation of distant nodes. Theoretical and simulation results show that GTMS demands less memory, energy, and communication overheads, as compared to other trust management schemes. Therefore, it is more suitable for large-scale WSNs.

Observations in WSNs: We can see that, all of the above models pay special attention to the resource overhead of their models, which is a common requirement for all the other trust models in WSNs. Besides the above models, some work incorporated bio-inspired algorithm. For instance, the models in [4], [28] are based on a bio-inspired algorithm called Ant Colony System (ACS).

B. Trust Models in OSNs

Various approaches have been applied to trust management in OSNs. Typically, they are based on a trusted graph, which consists of a source node *trustor*, a target node *trustee*, and several intermediate recommenders. Based on a trusted graph, the trust level can be estimated by either a graph analogy-based approach, or a graph-simplicity approach. Here, we only mention two representative models for each approach. Table I shows a brief comparison.

RN-Trust: Taherian et al. [22] proposed RN-Trust, where they emulated a trusted graph with a resistive network, using a logarithmic function to map between the trust value t and the resistance values r, i.e., $r = \log_{10} t$. They first computed the equivalent resistance value, R_{ab}^{eq}, between two nodes a and b. Then they can get trust value using $t_{ab} = 10^{R_{ab}^{eq}}$.

FlowTrust. Wang and Wu [23] presented FlowTrust, where they apply network flow theory into trust evaluation. They use the trust value and confidence level as two trust factors, and deduce four trust metrics from these two trust factors: maximum flow of trust value, maximum flow of confidence level, minimum cost of uncertainty with maximum flow of trust value, and minimum cost of untrust with maximum flow of confidence level. They also propose three FlowTrust algorithms to normalize these four trust metrics.

SWTrust. To generate small trusted graphs for large OSNs, Jiang et al. [21] proposed SWTrust. They proposed a *user-domain-based trusted acquaintance chain discovery* algorithm to preprocess an OSN, by using its small-world network characteristic and taking advantage of "weak ties [29]." Then, they generate a trusted graph with the adjustable width breadth-first search algorithms. They use Epinions.com as the test bed to validate the effectiveness of their work. The work is the first to focus on generating small trusted graphs for large OSNs, and to explore the stable and objective information (such as $domain$) for inferring trust.

TidalTrust. Golbeck [20] proposed TidalTrust. The calculations sweep forward from the source to the target in the network, and then pull back from the target to return the final value to the source. Using a recursive search with weighted averages, TidalTrust can take two people in the network and generate a recommendation about how much one person should trust the other, based on the trusted paths. Note that only the shortest strongest trusted paths are used.

Observations in OSNs: Taking an overview on the trust models in OSNs, we can see that their focus is mainly on the interpretation of trust itself, including evidence collection and aggregation; since there is no strict resource-limitation in OSNs. Moreover, based on trust evaluation schemes, many interesting models can be flexibly incorporated and many applications can be conducted. For instance, [30] proposes a rating prediction scheme in trust-based recommendation system, using fluid dynamics theory.

IV. Validation Approaches

A. Simulations in WSNs

WSNs typically consist of hundreds or even thousands of sensor nodes deployed in a geographical region to sense events. Using actual sensor networks in the case of developing a new scheme or experimenting with functionalities may consume too much time and cost. Therefore, researchers have developed several simulators as the test beds for simulation in WSNs (comprehensive surveys can be found in [31], [32]). Some of them have been used in simulating trust models in WSNs, e.g., Sensor Network Simulator and Emulator (SENSE) [33], OPNET [34], Trust and Reputation Models Simulator for Wireless Sensor Networks (TRMSim-WSN) [35], and SensorMaker [36]. Among them, TRMSim-WSN is well-suited for trust models.

TRMSim-WSN is a Java-based simulator aiming at testing Trust and Reputation models for WSNs. It provides several Trust and Reputation models, and new ones can be easily added. It allows researchers to test and compare their trust and reputation models against a wide range of WSNs. They can decide whether they want static or dynamic networks, the percentage of fraudulent nodes, the percentage of nodes acting as clients or servers, etc. It has been designed to easily adapt and integrate a new model within the simulator. Only a few classes have to be implemented in order to carry out this task. Fig. 3 shows the GUI of TRMSim-WSN.

Metrics. Besides accuracy, resource costs including communication overhead and memory consumption are considered.

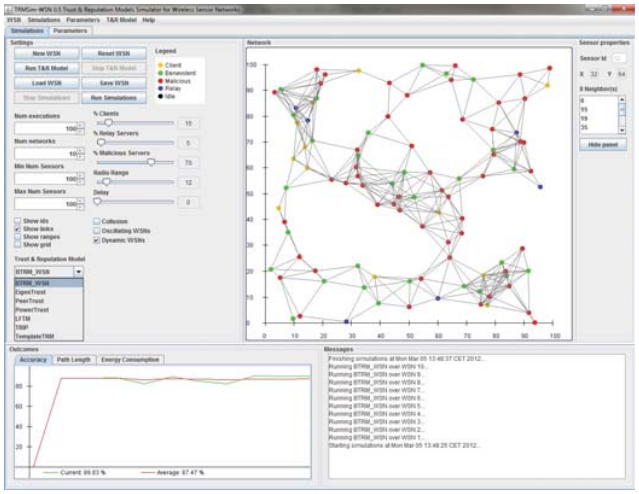


Figure 3. The TRMSim-WSN simulator.

B. Simulations in OSNs

To test the effects of trust models in OSNs, researchers usually use a standard evaluation technique in machine learning: leave one out [37]. If there is an edge between two nodes, that edge is masked, and trust is calculated through algorithms. Then, they compare the calculated value with the masked value. Moreover, various real social network data sets are available for use. Two commonly used data sets are from Epinions (www.epinions.com) and Advogato (www.advogato.org).

Advogato is an online social networking site dedicated to free software development. Because Advogato was the first website to use a robust, attack-resistant trust metric and to release the underlying code for that trust mechanism under a free software license, it has been the basis of numerous research papers on trust metrics and social networking. Taking the snapshot collected in June 2012 for instance, it contains 7,436 users and 56,667 links. On Advogato, users can certify each other on 4 different levels: Observer, Apprentice, Journeyer, and Master, which can be assigned 0.4, 0.6, 0.8, and 1.0, respectively, to numerate the level of trust.

Epinions is a good test bed that is widely used in the research of trust evaluation and trust-based recommendation [38]. The main reason is that it includes both the information of user trust relationships and user/item ratings. Users can review items and assign them numeric ratings in the range of [1, 5]. They can also build their own trust network by adding the people whose reviews they think are valuable. One data set of Epinions.com is published by Massa [38]. It consists of 49,290 users who rated a total of 139,738 different items at least once. The total number of reviews is 664,824. The total number of issued trust statements is 487,181.

Metrics. Two metrics are commonly used, i.e., the *coverage* and *trust accuracy* [21]. The former represents how many users can be predicted, and the latter represents the ability to predict whether a user will be trusted or not, respectively: (1) Precision: $A_t \cap B_t / B_t$, (2) Recall: $A_t \cap B_t / A_t$, (3) FScore: 2· Recall $\cdot Precision$/(Recall+Precision).

V. Discussions and Conclusion

Discussions: We are interested in how the trust models in WSNs can benefit those in OSNs, and vice versa. Therefore, we summarize their common features as follows: (1) Time sensitivity and dynamic topology. Both WSNs and OSNs are dynamically updated. Trust relations, node behaviors, and network topology are changing over time. (2) Efficiency requirement. As we have mentioned before, WSNs require high efficiency due to their resource limitations; While OSNs also require high efficiency, due to its very large scale. (3) Validation requirement. Trust models in WSNs and OSNs need to be tested, to show their effects and performance. Different simulators are developed for WSNs, and different data sets are available for OSNs. Could we collect some real world data sets for WSNs? Or, could we develop simulators for OSNs? We think the answer is yes. However, it may require the cooperation of researchers among the two fields.

Conclusion. We present a comparative study of trust models in WSNs and OSNs. We first provide a comparison of the features of WSNs and OSNs. Next, we review and compare existing trust models in the literature. Finally, we analyze the common features of trust models in WSNs and OSNs, and conduct some discussion on how to enhance the trust management in a network by learning from the other type.

References

[1] http://en.wikipedia.org/wiki/Category:Wireless_sensor_network.

[2] A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee. Measurement and analysis of online social networks. *Proc. IMC*, pages 29–42, 2007.

[3] S. Ganeriwal and M.B. Srivastava. Reputation-based framework for high integrity sensor networks. *Proc. SASN*, pages 66–67, 2004.

[4] F. G. Mrmol and G. M. Prez. Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication Systems*, 46(2):163–180, 2011.

[5] F. Li and Y. Wang. Routing in vehicular ad hoc networks: a survey. *IEEE Vehicular Technology Magazine*, 2(2):12–22, 2007.

[6] Y. Yu, K. Li, W. Zhou, and P. Li. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications*, 35(3):867 – 880, 2012. Special Issue on Trusted Computing and Communications.

[7] W. Sherchan, S. Nepal, and C. Paris. A survey of trust in social networks. *ACM Computing Surveys*, 45(4):47:1–47:33, 2013.

[8] J. Cho, A. Swami, and I. Chen. A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys Tutorials*, 13(4):562–583, Fourth 2011.

[9] F. G. Mrmol and G. M. Prez. Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. *Computer Standards & Interfaces*, 32:185–196, 2010.

[10] A. Jøsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision. *Decision Support System*, 43(2):618–644, March 2007.

[11] Z. Noorian and M. Ulieru. The state of the art in trust and reputation systems: a framework for comparison. *J. Theor. Appl. Electron. Commer. Res.*, 5(2):97–117, August 2010.

[12] Y. Yao, S. Ruohomaa, and F. Xu. Addressing common vulnerabilities of reputation systems for electronic commerce. *J. Theor. Appl. Electron. Commer. Res.*, 7(1):1–20, April 2012.

[13] G.V. Crosby and N. Pissinou. Cluster-based reputation and trust for wireless sensor networks. In *Proc. CCNC*, 2007.

[14] H. S. Ng, M. L. Sim, and C. M. Tan. Security issues of wireless sensor networks in healthcare applications. *BT Technology J.*, 24(2):138–144, 2006.

[15] E. Shi and A. Perrig. Designing secure sensor networks. *IEEE Wireless Comm.*, 11(6):38–43, 2004.

[16] A. A. Pirzada and C. McDonald. Establishing trust in pure ad-hoc networks. *Proc. ACSC*, pages 47–54, 2004.

[17] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y.J. Song. Trust management problem in distributed wireless sensor networks. *Proc. RTCSA*, pages 411–414, 2006.

[18] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu. Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 24(2):305–317, 2006.

[19] R. A Shaikh, H. Jameel, B.J. d'Auriol, Heejo Lee, Sungyoung Lee, and Young-Jae Song. Group-based trust management scheme for clustered wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*, 20(11):1698–1712, Nov 2009.

[20] J. Golbeck. Computing and applying trust in web-based social networks. *PhD thesis, University of Maryland*, 2005.

[21] W. Jiang, G. Wang, and J. Wu. Generating trusted graphs for trust evaluation in online social networks. *Future Generation Computer Systems*, 31:48–58, 2014.

[22] M. Taherian, M. Amini, and R. Jalili. Trust inference in web-based social networks using resistive networks. *Proc. ICIW*, pages 233–238, 2008.

[23] G. Wang and J. Wu. FlowTrust: Trust inference with network flows. *Frontiers of Computer Science in China*, 5(2):181–194, 2011.

[24] D. J. Watts. Small worlds: The dynamics of networks between order and randomness. *Princeton University Press*, 1999.

[25] W. Yuan, D. Guan, and Y. Lee. Improved trust-aware recommender system using small-worldness of trust networks. *Knowledge-Based Systems*, 23:232–238, April 2010.

[26] A. Boukerche, X. Li, and K. EL-Khatib. Trust-based security for wireless ad hoc and sensor networks. *Computer Comm.*, 30:2413–2427, 2007.

[27] Z. Yao, D. Kim, and Y. Doh. Plus: Parameterized and localized trust management scheme for sensor networks security. *Proc. MASS*, pages 437–446, 2006.

[28] H. Marzi and M. Li. An enhanced bio-inspired trust and reputation model for wireless sensor network. *Proceedings of The 4th International Conference on Ambient Systems, Networks and Technologies*, pages 1159–1166, 2013.

[29] M. Granovetter. The strength of weak ties. *American Journal of Sociology*, 78(6):1360–1380, 1973.

[30] W. Jiang, J. Wu, G. Wang, and H. Zheng. Fluidrating: Time-evolving rating prediction in trust-based recommendation systems using fluid dynamics. *Proc. IEEE INFOCOM*, 2014.

[31] B. Musznicki and P. Zwierzykowski. Survey of simulators for wireless sensor networks. *International Journal of Grid and Distributed Computing (IJGDC)*, 5(3):23–50, 2012.

[32] M. Imran, AM. Said, and H. Hasbullah. A survey of simulators, emulators and testbeds for wireless sensor networks. In *Proc. ITSim*, volume 2, pages 897–902, June 2010.

[33] B.K. Szymanski. Sense: Sensor network simulator and emulator. http://www.ita.cs.rpi.edu/sense/index.html, 2008.

[34] www.opnet.com.

[35] F. G. Mrmol and G. M. Prez. Trmsim-wsn, trust and reputation models simulator for wireless sensor networks. *Proc. ICC*, pages 1–5, 2009.

[36] S. Yi, H. Min, Y. Cho, and J. Hong. Sensormaker: A wireless sensor network simulator for scalable and fine-grained instrumentation. In *Computational Science and Its Applications (ICCSA 2008)*, volume 5072, pages 800–810. 2008.

[37] R. Kohavi. A study of cross-validation and bootstrap for accuracy estimation and model selection. In *Proc. IJCAI*, pages 1137–1143, 1995.

[38] P. Massa and P. Avesani. Trust-aware recommender systems. In *Proc. ACM RecSys*, pages 17–24, 2007.