Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.5, No.2, 2014

A Survey of Provenance Leveraged Trust in Wireless Sensor Networks

Gulustan Dogan[1,*] and Ted Brown[1]
[1]City University of New York, Graduate Center, 365 5th Ave, New York, NY 10016
[*] E-mail of the corresponding author: dogangulus@gmail.com

Abstrat
A wireless sensor network is a collection of self-organized sensor nodes. WSNs have many challenges such as lack of a centralized network administration, absence of infrastructure, low data transmission capacity, low bandwidth, mobility, lack of connectivity, limited power supply and dynamic network topology. Due to this vulnerable nature, WSNs need a trust architecture to keep the quality of the network data high for a longer time. In this work, we aim to survey the proposed trust architectures for WSNs. Provenance can play a key role in assessing trust in these architectures. However not many research have leveraged provenance for trust in WSNs. We also aim to point out this gap in the field and encourage researchers to invest in this topic. To our knowledge our work is unique and provenance leveraged trust work in WSNs has not been surveyed before.
Keywords: Provenance, Trust, Wireless Sensor Networks

1. Introduction

In a wireless sensor network, nodes communicate with each other via radio links. Radio links have limited transmission range, so nodes transmit data via a multi-hop strategy. Each node acts as a router and as a host (Momani & Challa, 2010). There is a very low data transmission capacity and bandwidth between nodes. One other property of wireless sensor networks is they have a limited power supply and their energy is exhausted easily. Lastly, nodes join or leave a network at any given time and their position change frequently, this results in a dynamic network topology. They have the same challenges that a MANET have. In addition to challenges a MANET have such as absence of infrastructure, mobility, lack of connectivity, there is also computation constraint. This is why a trust model for WSNs have to be designed (Momani & Challa, 2010). WSN technology is a newly emerging concept. Tiny and cheap nodes are employed in large numbers in difficult environments such as military fields for many purposes such as surveillance. Small low cost sensors collect and relay environmental data (Akyildiz, et al., 2002). Originally WSNs were motivated by surveillance in battlefields for military however in time the they were used in many areas (Momani & Challa, 2010). Some examples of these areas are monitoring an active volcano(Werner-Allen, et al., 2006; Werner-Allen, et al., 2005), monitoring the microclimate throughout the volume of redwood trees (Culler, et al., 2004), to building and bridge monitoring (Glaser, 2004; Paek, et al., 2006), to health-care monitoring (Gao, et al., 2006), and some other applications such as (Tubaishat & Madria, 2003; Akyildiz et al., 2002; Yoneki & Bacon, 2005; Callaway, 2004).
Trust is quite important for self-configurable and autonomous systems such as WSN (Fernández-Gago, et al., 2007). WSNs are very vulnerable environmensts due to computational and energy constraints. In addition WSNs are very open to physical world effects such as a person walking on a field can step on a sensor and make it dysfunctional. A trust management scheme can make a WSN tolerant to node failures and misbehaviours by assisting decision making process. For example a node can decide to cooperate with

a node or not based on the feedback it will receive from the trust model. Trust research on WSN is very new, few systems have considered it (Ganeriwal, et al., 2008; Yao, et al., 2005). More research has been done on Trust in Ad-hoc and P2P networks. although these network types have many similarities to WSN, still a seperate trust management system has to be developed for WSN because of their specific characteristics such as energy and computation constraints. For example most of the trust models for ad-hoc networks use a central reputation mechanism that needs a manager overseeing the trust of the network (Rebahi, et al., 2005). This approach is not very applicable to sensor networks because of energy and scalability issues.

One of the biggest constraints in developing a trust model for WSNs is the overhead that can be caused by
the trust model. Trust model should be as lightweight as possible (Fernández-Gago et al., 2007). Moreover data collection is very important in the process of designing a trust management system. The system should be history aware, past behaviors should be taken into consideration (Fernández-Gago et al., 2007). Moreover, every node should keep their past behavior statistics regarding the data they produce such as average error of the created data in the past time intervals. This is where provenance comes into the picture. There are many different data that can be used as input of the trust model. For example, a node that is not alive for a long time or a node that appears or disappears randomly many not be trusted. On the communication layer, a node which is misreporting will not be trusted. For instance a node which is giving a fire alarm when conditions are calm should be given a low trust value (Fernández-Gago et al., 2007).
In Section II, we give some background information on Provenance. We present background information on Trust in Section III. Section IV surveys the trust architectures in Social Sciences, E-Commerce, Ad-hoc and Peer-to-peer networks. Section V surveys the WSN trust architectures. Section VI concludes the paper.

2. Background on Provenance

In the study of fine art, provenance refers to the documented history of some art object (Moreau, et al., 2008a). Provenance of a painting is a history of its ownership. Based on the documented history, the object is considered authentic or fake. For instance if it cannot be verified that Mona Lisa was created by Leonardo Da Vinci then the painting is considered invaluable.
In the first place, database community has addressed the issue of provenance. Cui et al.(Cui, et al., 2000)
were among the first researchers to formalize provenance of data in the context of relational databases calling it *lineage* of a tuple. Each tuple present in the output of a query is associated with a set of tuples present in the input. The associated tuples are called lineage. Basically the lineage of a tuple is defined as the input data that contributed to the tuple.
Although provenance was first addressed by database community, later it was used by many research com-
munities such as network(Zhou, et al., 2010), internet (Carroll, et al., 2005), trust(Golbeck, 2006), file systems(Sar & Cao, 2005).
Computing divides provenance into data provenance and workflow provenance (Moreau, et al., 2008b). Data
provenance gives a detailed record of the derivation of a piece of data that is the result of a transformation step (Tan, 2007) whereas workflow provenance is the information or metadata that characterizes the pro- cessing steps of information from input to output (Davidson & Freire, 2008).
Research is being done for assessing trust using provenance in sensor networks. However we still examine the trust associated with routing messages between nodes (binary events). Wireless sensor network stream both continuous and discrete data or monitor events. New trust models are needed to address the continuous data issue and to combine data trust with communication trust(Momani & Challa, 2010).
In WSNs provenance should be validated in order to prevent spoofing of messages from malicious attack-
ers. For instance nodes can have digital signatures to validate the authenticity of the computed provenance (Zhou, et al., 2008). There should be some kind of access control for securing data (Lange, 2010). Making provenance records trustworthy is a challenge (Hasan, et al., 2009). Cost of digital signatures and cryptogra- phy techniques is too high. Therefore light-weighted digital signature techniques should be used for handling security and privacy in data provenance systems (Lim, et al., 2009).

3. Background on Trust

Josang et al. (Jsang & Presti, 2004) defines trust and trustworthiness based on the definitions of Gambetta (Gambetta, 2000). Solhaug et al. (Solhaug, et al., 2007) defines trustworthiness as objective probability that the trustee performs a particular action on which interests of the trustor

depend. Trust is a subjective probability varying from 1 (complete trust) to 0 (complete distrust) (Jsang & Presti, 2004).
As trust is the believed probability and trustworthiness is the actual probability, there can be a difference between them. This difference introduces the risk factor (Cho, et al., 2010). Risk increases if the trust is misplaced.
Reputation is also a concept that is very related to trust. Sometimes reputation and trust is used in the same context however they have different meanings. Reputation is the opinion of an entity such a node, a person about the other. However trust is derivation of reputation of an entity. Trust is calculated based on the reputation.
Uncertainty is also related to trust. Trust is a mechanism to cope with uncertainty. If the information that
is used as trust evidence is uncertain then the trust is inaccurate too (Walker, et al.,
2003).
Information trust or data trust refers to the trust placed on data produced by objects or processes. Infor- mation trust in a network is important because it can prevent erroneous data to accumulate in the network. In a network, a node can (i) create data (ii) process the data such as fusion (iii) pass the data along. The trust of data depends on the trust of the node that creates the data and the trust of the nodes the data has visited. Information trust in a network can be categorized into three : (i)creator node's subjective view of the trust (ii)objective trust assessment of the data by the neighbouring nodes (iii) changes in information trust as the data travels along the network

4. Trust in Different Domains

Below we give information about trust literature in different domains based on the survey of Momani and Challa.

4.1 Trust in Distributed and Peer-to-Peer Systems

In distributed systems, there is no central authority for assessing the trust of entities. Hence entities form their own opinions of trust by exchanging information with their peers. Generally methods from game theory (Xiong & Liu, 2003), bayesian networks (Wang & Vassileva, 2003a) are used for trust calculation distributedly.
Aberer and Despotovis were one of the first researchers to propose a reputation management system for P2P systems (Aberer & Despotovic, 2001). They employe algorithms and data structures that require no knowledge from a central authority. The trust model is based on the past interactions between the nodes. One drawback of their method is that only the negative feedbacks are considered and the system is sensitive to misbehaviour of peers. The resurrecting duckling model in (Stajano & Anderson, 2000) and its descendants (Balfanz, et al., 2002) use out-of-band channels to authenticate key exchange. The established trust between the nodes is binary, either secure or not secure.
There are other trust models for peer-to-peer systems which we do not want to go into details of as we
are interested in trust models for sensor networks. Other trust mechanisms surveyed by Momani and Challa(Momani & Challa, 2010) are SECURE(Cahill, et al., 2003), Distributed Trust Model(Abdul-Rahman
& Hailes, 1998), Bayesian Network Model (Wang & Vassileva, 2003a), UniTec(Kinateder, et al., 2005), BambooTrust(Kotsovinos & Williams, 2006), B-trust model(Quercia, et al., 2006).

4.2 Trust in Ad-hoc Networks

In ad-hoc networks, nodes join to networks or move networks very often. There are no trusted nodes to support the network functionality. Trust relationship between the nodes is also dynamic as the network is constantly changing (Zhou, 2003).
A majority of the trust mechanisms in ad-hoc networks use game theory and bayesian network approaches. Two examples of these systems are CONFIDANT (Buchegger & Le Boudec, 2002) and CORE (Michiardi

& Molva, 2002). Recently Bayesian analytics methods are most widely deployed than game theory methods (Buchegger et al., 2003a; Buchegger, et al., 2003b).

5. Trust in WSNs

Trust has been a research area in social sciences for a long time however it is a new area in computing motivated by trust models for e-commerce (McKnight & Chervany, 2001). Trust in WSNs is an open and challenging research area. Although extensive efforts have been carried out for trust management in Ad-hoc and P2P networks, very little has been done on Trust management in WSN domain (Fernández- Gago et al., 2007). Some of the reputation and trust systems in the context of sensor networks can be listed as follows (Srinivasan, et al., 2006; Crosby, et al., 2006; Hur, et al., 2005; Chen, et al., 2007; Xiao, et al., 2007; Crosby & Pissinou, 2007; Krasniewski, et al., 2005; Shaikh, et al., 2006; Yao et al., 2005; Hung, et al., 2007; Mundinger & Le Boudec, 2006; Ma, et al., 2006; Zhang, et al., 2008; Yao, et al., 2006; Momani, et al., 2006).

Security and trust are very related concepts and sometimes they are used interchangeably (Pirzada & Mc- Donald, 2004). However security is different than trust. It is broader than trust and overhead is higher in security. Trust is used in restructuring a WSN such as omitting nodes, adding nodes, merging clusters. Trust establishment is a must because WSN depends on cooperative and trusting nature of its nodes. However due to limited resources in WSN, it is not possible to use the traditional cryptographic approaches (Eschenauer, et al., 2004). Different trust mechanisms are needed for wireless sensor networks.

The most common methodologies in trust calculation in WSNs are ratings, weighting, probability, bayesian
network, neural network, game theory, fuzzy logic, swarm intelligence, directed undirected graph. Clusters are also very important for sensor networks because if clusters are malicious, the network will quickly become dysfunctional. A trust based decision making in selecting cluster heads should be used.

A WSN faces different kinds of attacks such as eavesdropping, fabrication, injection, modification of packets, node capturing and many others (Momani & Challa, 2010). These attacks rise issues such as privacy, account- ability, data integrity, data authentication and data freshness. Some research has been done on security of WSN as surveyed by Momani and Challa (Wang, et al., 2006; Papadimitratos & Haas, 2002; Zhou, 2003; Wal- ters, et al., 2007; Newsome, et al., 2004; Zia & Zomaya, 2006; Perrig, et al., 2004; Stajano & Ander- son, 2000; Zhou & Haas, 1999; Przydatek, et al., 2003). Cryptographic mechanisms do not completely solve the problems. System faults, erroneous data, bad routing by malicious nodes can cause network break- downs. Cryptography is not sufficient to solve the security problems, cryptographic approaches should be integrated with tools from domains such as statistics, e-commerce, social sciences. A secure routing protocol (SRP) is needed. Some nodes can behave maliciously or selfishlessly. SRP has to discover and isolate these nodes.

Trust establishment in sensor networks is a must because the survival of a WSN depends on cooperative and trusting nature of its nodes. Due to resource limitation of sensor nodes, using traditional methods such as cryptography to generate trust is not possible (Eschenauer et al., 2004). Therefore new methods for secure communication and distribution of trust values between nodes are needed. Provenance can play an important role in eliminating the challenges faced in developing trust architectures by keeping the historical behavior of nodes. Some trust models in WSNs make use of provenance but some of them do not. Below we have surveyed both directions.

5.1 Standard Trust Models

There are some trust models for sensor networks which do not make use of provenance. In this subsection, we have surveyed them and briefly summarized their approaches.

One example of a trust model for sensor networks is TIBFIT (Krasniewski et al., 2005). In TIBFIT, a trust index based fault tolerance system, they keep a trust index as a quantitative measure of fidelity of previous event reports (Krasniewski et al., 2005). Their notion of trust is closely related to error rate of data produced by nodes. They keep historical correctness of nodes without calling it provenance. Bayesian network (Wang
& Vassileva, 2003a; Wang & Vassileva, 2003b) and game theory techniques (Xiong & Liu, 2003) are two other examples of the models used for building trust in networks (Momani & Challa, 2010).

Ganeriwal and Srivastava were the first to introduce a reputation model for sensor networks

(Ganeriwal
et al., 2008). Their system is called RFSN (Reputation-based Framework for High Integrity Sensor Networks). Their model uses beta distribution to represent and continuously update trust and reputation. Their model uses direct and indirect information (second hand information) to calculate reputation. Their notion of trust is binary. Nodes are classified as cooperative or uncooperative based on their trust values. Trust is calculated as an expected value of reputation. If node's trust is below a threshold, it is considered uncooperative. RFSN use a watchdog mechanism to monitor the nodes, to calculate the reputation and to calculate trust (Ganeriwal et al., 2008). Bayes theorem is used to describe the binary events as succesful and unsuccesful. They do not make use of second hand information and they do not mention about trust updates.

Dai et al. calculate trust scores based on four factors: 1) path similarity 2) data similarity 3) data conflict 4) data deduction (Dai, et al., 2008). For data similarity they calculate distance between two numerical values, distance between two categorical values and distance between two string values.

DRBTS (Distributed Reputation-based Beacon Trust System) is a system that is primarily modeled for sensor networks which it is crucial to know the location of a sensor (Srinivasan et al., 2006). They use beacon nodes to find the nodes that are misreporting their places. Every beacon node is distributedly monitoring the 1-hop neighborhood for misbehaving nodes and updating the reputation of the misreporting nodes in the Neighbor-Reputation-Table (NRT). Sensor nodes use the information in NRT tables to decide about trustworhiness of a node based on simple majority voting scheme.

One of the most important breaches of sensor networks is that cluster heads can be malicious (Crosby
et al., 2006). Garth et al. proposes a distributed trust based framework for election of trustworthy cluster heads. Direct and indirect information coming from trusted nodes is used. Trust is calculated as the weighted calculation of the packet drop rate, data packets and control packets. Every node is keeping a trust table of the nodes around it and they report to the cluster head upon request. The second-hand information is not used so the bad mouthing effect is prevented.

Hur et al. has proposed a trust model for assessing trustworthiness of sensor data and to remove the
data from malicious nodes (Hur et al., 2005). Their work has many similarities to a work of ours (Dogan, et al., 2011). However their model does not make use of provenance, the historical data. Each node evaluates trustworthiness of its neighbor nodes by crosschecking the neighbor nodes redundant sensing data with its own result. More accurate results are found out by disregarding the data coming from malicious nodes. Chen et al. (Chen et al., 2007) propose a reputation-based trust which borrows tools from probability, statistics and mathematics analysis. They have suggested a new term certainty used in trust system and they argued that the positive or negative outcomes for a certain event is not enough information to make a decision in WSNs. They build up a reputation space and trust space in WSNs, and define a transformation from reputation space to trust space. Finally, they discuss some important properties of them and point out some open problems in reputation system in WSNs.

Xiao et al. use a Trust Voting algorithm, a sensor node consults with its neighbors to validate if its reading is true or not (Xiao et al., 2007). Faulty nodes do not participate in voting algorithm.

Tanachaiwiwat et al. (Tanachaiwiwat, et al., 2004) has built a trust routing model (TRANS) for sensor
networks. In their model, nodes send probing messages to neighbours and wait for ACK messages. Nodes that are maliciously routing the message or dropping the message are blacklisted by the sink node. Traffic flow is from/to the sink.

One of the models using beta reputation system is Connected Dominating Set (CDS)-based reputation monitoring system by Srinivasan et al. (Srinivasan, et al., 2008). The nodes obtain direct information about other nodes and store it as a beta distribution parameters tuple.

Momani et al. build a Gaussian Reputation System for WSN (Momani, et al., 2007). Each node's reported data is evaluated by its neighbour nodes. They introduce a Bayesian probabilistic approach for mixing second hand information from neighbouring nodes with directly observed information.

RDAT uses a beta reputation system and base station evaluates trustworthiness of nodes based on sensing, routing and aggregation behaviours (Ozdemir, 2008). Reliability of the system is increased in presence of compromised nodes.

GTMS is a group-based trust management scheme developed by Shaikh et al. (Shaikh et al., 2006).

They combine centralized and distributed approaches. Their work has very similarities to our approach. However they do not consider faulty data sent by malicious nodes. Every group has a trust value which is kept at a small database at the base station.
In Agent Based Trust and Reputation Management Sytem (ATRM) nodes store the trust and reputation information locally (Boukerch, et al., 2007). The network model is based on a clustered WSN with backbone where its core is a mobile agent system.

5.2 Provenance Leveraged Trust Models

In many sensor network applications, provenance can be used for assessing trust. In this subsection, we surveyed the work in literature. However not many research leveraging provenance for computing trust in wireless sensor networks has been done. One of the main aims of this research is to point out this gap in the field and encourage more researchers to invest in this topic.
Two example wireless sensor network applications are a battlefield monitoring system and a supervisory control data acquisition system. A battlefield system gathers target locations from multiple sources such as cameras, satellite images, vehicles, proximity sensors. Critical decisions are taken based on the data hence trustworthiness is a concern and can be assessed by using provenance. A Supervisory Control and Data Acquisition (SCADA) system collects real-time information from data collection points such as sensors, based on this data it performs critical tasks. A failure can affect the whole system. Therefore provenance is a key in preventing failures beforehead by finding out untrusted sources (Lim et al., 2009).
In a multihop network, data goes through many nodes. Some techniques have been introduced in order to
make sure data is not changed such as digital signature. However errors in network can be due to intentional misbehavior such as attacks or unintentional errors such as exhausted batteries (Wang, et al., 2010). In our previous work, we estimate the trustworthiness of information based on trustworthiness of its provider (Govindan, et al., 2011). Then we further assess the trustworthiness of this information based on similarity of information received from multiple paths. Our approach is unique in the sense that we consider both path and information correlation in trust assessment. Our trust model works in three steps (1)*initial trust computation* (2) *information trust adjustment* (3) *reputation feedback* (Govindan et al., 2011). In another work of us, we have designed a trust enhancing architecture based on provenance which restructures the network for a higher trust value (Dogan et al., 2011). Our system is unique in the sense that network restructuring is done based on provenance records.
Orchestra is a system assessing trust and authority based on provenance. It is not specifically designed for wireless sensor networks. It is a data integration engine using provenance to accept or reject updates from neighboring nodes by examining the provenance of updates (Ives, et al., 2005). In the path-vector protocol used in BGP, whole path is carried during route advertisement. Nodes in the network trace the origins of data and accept or reject that data based on origins.
Lim et al. has work on using provenance to compute trustworthiness in streaming environments (Lim,
et al., 2010). They implement a framework for computing trust scores of nodes and data in a network. Both network nodes and data items have trust values. Trust value of a network node is computed as the weighted sum of trust score of the node and the average of the trust values of the data items of this node (data items that are originated from or visiting this network node). The first score of data item is calculated based on the trust scores of network nodes that is in its provenance graph. It is assigned the minimum trust score of the nodes in the provenance graphs. This trust score is the initial score, later trust score is updated. The intermediate trust score is calculated both using the value and provenance similarity. The distribution of values for all the data items in the network is modeled. If the value is the data item is close to mean, it is given a bigger trust score. It is determined by value similarity and adjusted by provenance similarity. They

assume that items in the same event should have similar provenance graphs, they do adjustments according to the provenance graph similarity. They do intuitive changes on the trust scores according to provenance similarity results. For instance if values are similar and if also provenance graphs are similar, the trust score is increased. If values are different and if also provenance graphs are different, the trust score is increased. If values are different but provenance graphs are same than the trust score is decreased. Because it means that the items are in the same event but they are generating different

data values. They have ran experiments on the implementation they have done. The trust scores are decreasing when faulty data is injected to the system.
Zhou et al. use provenance for enforcing distributed trust management policies in networks and they also explore the general applicability of these techniques to sensor networks (Zhou, et al., 2007). They use provenance tables to trace the origins of networked data and to enforce trust policies to accept or reject data based on source origins.

6. Conclusion

Trust in WSNs is still an open and challenging field due to the dynamic nature of sensor networks. However it is a very rewarding area as most of the WSN applications are deployed in hostile environments such as military fields. A solid trust architecture leveraging provenance for WSNs will be a valuable intellectual contribution to both research and industry as WSN applications are very widely used in real world applications.

References

A. Abdul-Rahman & S. Hailes (1998). 'A distributed trust model'. In *Proceedings of the 1997 workshop on New security paradigms*, pp. 48–60. ACM.

K. Aberer & Z. Despotovic (2001). 'Managing trust in a peer-2-peer information system'. In *Proceedings of the tenth international conference on Information and knowledge management*, pp. 310–317. ACM.

I. Akyildiz, et al. (2002). 'Wireless sensor networks: a survey'. *Computer networks* 38(4):393–422.

D. Balfanz, et al. (2002). 'Talking to strangers: Authentication in ad-hoc wireless networks'. In *Proceedings of the 9th Annual Network and Distributed System Security Symposium (NDSS)*, pp. 7–19.

A. Boukerch, et al. (2007). 'Trust-based security for wireless ad hoc and sensor networks'. *Computer Communications* 30(11-12):2413–2427.

S. Buchegger et al. (2003a). 'Coping with false accusations in misbehavior reputation systems for mobile ad-hoc networks' .

S. Buchegger, et al. (2003b). 'The effect of rumor spreading in reputation systems for mobile ad-hoc networks'.
In *WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*.

S. Buchegger & J.-Y. Le Boudec (2002). 'Performance analysis of the CONFIDANT protocol'. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, pp. 226–236. ACM.

V. Cahill, et al. (2003). 'Using trust for secure collaboration in uncertain environments'. *Pervasive Com- puting, IEEE* 2(3):52–61.

E. Callaway (2004). *Wireless sensor networks: architectures and protocols*, vol. 3. CRC press.

J. Carroll, et al. (2005). 'Named graphs, provenance and trust'. In *Proceedings of the 14th international conference on World Wide Web*, pp. 613–622. ACM.

H. Chen, et al. (2007). 'Reputation-based trust in wireless sensor networks'. In *Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on*, pp. 603–607. IEEE.

J. Cho, et al. (2010). 'A survey on trust management for mobile ad hoc networks'. *Communications Surveys& Tutorials, IEEE* (99):1–22.

G. Crosby & N. Pissinou (2007). 'Cluster-based reputation and trust for wireless sensor networks'. In *Proc.4th Consumer Communications and Networking Conference (CCNC 2007)*.

G. Crosby, et al. (2006). 'A framework for trust-based cluster head election in wireless sensor networks'. In *Dependability and Security in Sensor Networks and Systems, 2006. DSSNS 2006. Second*

IEEE Workshop on, pp. 10–pp. IEEE.

Y. Cui, et al. (2000). 'Tracing the lineage of view data in a warehousing environment'. *ACM Transactions on Database Systems (TODS)* 25(2):179–227.

D. Culler, et al. (2004). 'Overview of Sensor Networks'. *Computer Journal* pp. 41–49.

C. Dai, et al. (2008). 'Trust evaluation of data provenance'. *Computer* .

S. Davidson & J. Freire (2008). 'Provenance and scientific workflows: challenges and opportunities'. In*SIGMOD Conference*, pp. 1345–1350. Citeseer.

G. Dogan, et al. (2011). 'Evaluation of Network Trust Using Provenance Based on Distributed Local Intel- ligence'. In *Military Communications Conference, 2011. MILCOM 2011. IEEE*. IEEE.

L. Eschenauer, et al. (2004). 'On trust establishment in mobile ad-hoc networks'. In *Security Protocols*, pp.47–66. Springer.

M. Fernández-Gago, et al. (2007). 'A survey on the applicability of trust management systems for wireless sensor networks'. In *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. SECPerU 2007. Third International Workshop on*, pp. 25–30. IEEE.

D. Gambetta (2000). 'Can we trust trust'. *Trust: Making and breaking cooperative relations* pp. 213–237.

S. Ganeriwal, et al. (2008). 'Reputation-based framework for high integrity sensor networks'. *ACM Trans- actions on Sensor Networks (TOSN)* 4(3):15.

T. Gao, et al. (2006). 'Vital signs monitoring and patient tracking over a wireless network'. In *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, pp. 102–105. Ieee.

S. Glaser (2004). 'Some real-world applications of wireless sensor nodes'. In *Proceedings of SPIE Symposium on Smart Structures and Materials/NDE*, p. 344.

J. Golbeck (2006). 'Combining provenance with trust in social networks for semantic web content filtering'. In *Provenance and Annotation of Data*, pp. 101–108. Springer.

K. Govindan, et al. (2011). 'PRONET: Network Trust Assessment Based on Incomplete Provenance'. In *Military Communications Conference, 2011. MILCOM 2011. IEEE*. IEEE.

R. Hasan, et al. (2009). 'Preventing history forgery with secure provenance'. *ACM Transactions on Storage (TOS)* 5(4):1–43.

K. Hung, et al. (2007). 'A trust-based geographical routing scheme in sensor networks'. In *Wireless Com- munications and Networking Conference, 2007. WCNC 2007. IEEE*, pp. 3123–3127. IEEE.

J. Hur, et al. (2005). 'Trust evaluation model for wireless sensor networks'. In *Advanced Communication Technology, 2005, ICACT 2005. The 7th International Conference on*, vol. 1, pp. 491–496. IEEE.

Z. Ives, et al. (2005). 'ORCHESTRA: Rapid, collaborative sharing of dynamic data'. *CIDR, January* .

A. Jsang & S. L. Presti (2004). 'Analysing the Relationship between Risk and Trust'.

M. Kinateder, et al. (2005). 'Towards a generic trust model–comparison of various trust update algorithms'. *Trust Management* pp. 119–134.

E. Kotsovinos & A. Williams (2006). 'BambooTrust: Practical scalable trust management for global public computing'. In *Proceedings of the 2006 ACM symposium on Applied computing*, pp. 1893–1897. ACM.

M. Krasniewski, et al. (2005). 'Tibfit: Trust index based fault tolerance for arbitrary data faults in sensor networks'. In *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International*

Conference on, pp. 672–681. IEEE.

R. Lange (2010). *Provenance aware sensor networks for real-time data analysis*. Ph.D. thesis, University of Twente, Netherlands.

H. Lim, et al. (2009). 'Research issues in data provenance for streaming environments'. In *Proceedings of the 2nd SIGSPATIAL ACM GIS 2009 International Workshop on Security and Privacy in GIS and LBS*, pp. 58–62. ACM.

H. Lim, et al. (2010). 'Provenance-based trustworthiness assessment in sensor networks'. In *Proceedings of the Seventh International Workshop on Data Management for Sensor Networks*, pp. 2–7. ACM.

R. Ma, et al. (2006). 'Fault-intrusion tolerant techniques in wireless sensor networks'. In *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*, pp. 85–94. IEEE.

D. McKnight & N. Chervany (2001). 'Conceptualizing trust: A typology and e-commerce customer relation- ships model'. In *System Sciences, 2001. Proceedings of the 34th Annual Hawaii International Conference on*, pp. 10–pp. IEEE.

P. Michiardi & R. Molva (2002). 'Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks'. In *Advanced Communications and Multimedia Security*, pp. 107–121. Springer.

M. Momani, et al. (2007). 'RBATMWSN: recursive Bayesian approach to trust management in wireless sensor networks'. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pp. 347–352. IEEE.

M. Momani, et al. (2006). 'A New Algorithm of Trust Formation in Wireless Sensor Networks'. In *Proceedings of the 1st IEEE International Conference on Wireless Broadband and Ultra Wideband Communications*.

M. Momani & S. Challa (2010). 'Survey of trust models in different network domains'. *Arxiv preprint arXiv:1010.0168* .

L. Moreau, et al. (2008a). 'The provenance of electronic data'. *Communications of the ACM* 51(4):52–58.

L. Moreau, et al. (2008b). 'Special issue: The first provenance challenge'. *Concurrency and Computation: Practice and Experience* 20(5):409–418.

J. Mundinger & J. Le Boudec (2006). 'Reputation in self-organized communication systems and beyond'.
In *Proceedings from the 2006 workshop on Interdisciplinary systems approach in performance evaluation and design of computer & communications sytems*, p. 3. ACM.

J. Newsome, et al. (2004). 'The sybil attack in sensor networks: analysis & defenses'. In *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pp. 259–268. ACM.

S. Ozdemir (2008). 'Functional reputation based reliable data aggregation and transmission for wireless sensor networks'. *Computer Communications* 31(17):3941–3953.

J. Paek, et al. (2006). 'A programmable wireless sensing system for structural monitoring'. In *4th World Conference on Structural Control and Monitoring (4WCSCM)*.

P. Papadimitratos & Z. Haas (2002). *Securing mobile ad hoc networks*. CRC Press.

A. Perrig, et al. (2004). 'Security in wireless sensor networks'. *Communications of the ACM* 47(6):53–57.

A. Pirzada & C. McDonald (2004). 'Establishing trust in pure ad-hoc networks'. In *Proceedings of the 27th Australasian conference on Computer science-Volume 26*, pp. 47–54. Australian Computer

Society, Inc.

B. Przydatek, et al. (2003). 'SIA: Secure information aggregation in sensor networks'. In *Proceedings of the 1st international conference on Embedded networked sensor systems*, pp. 255–265. ACM.

D. Quercia, et al. (2006). 'B-trust: Bayesian trust framework for pervasive computing'. *Trust Management* pp. 298–312.

Y. Rebahi, et al. (2005). 'A reputation-based trust mechanism for ad hoc networks'. In *Computers and Communications, 2005. ISCC 2005. Proceedings. 10th IEEE Symposium on*, pp. 37–42. IEEE.

C. Sar & P. Cao (2005). 'Lineage file system'. *Online at http://crypto. stanford. edu/cao/lineage. html* .

R. Shaikh, et al. (2006). 'Trust management problem in distributed wireless sensor networks'. In *Em- bedded and Real-Time Computing Systems and Applications, 2006. Proceedings. 12th IEEE International Conference on*, pp. 411–414. IEEE.

B. Solhaug, et al. (2007). 'Why Trust is not proportional to Risk'. In *Proceedings of The 2nd International Conference on Availability, Reliability and Security (ARES)*, pp. 11–18.

A. Srinivasan, et al. (2008). 'A Novel CDS-based Reputation Monitoring System for Wireless Sensor Net- works'. In *Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on*, pp. 364–369. IEEE.

A. Srinivasan, et al. (2006). 'DRBTS: Distributed reputation-based beacon trust system'. In *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*, pp. 277–283. IEEE.

F. Stajano & R. Anderson (2000). 'The resurrecting duckling: Security issues for ad-hoc wireless networks'. In *Security Protocols*, pp. 172–182. Springer.

W.-C. Tan (2007). 'Provenance in databases : Past, Current, and Future'. *IEEE Data Engineering Bulletin* 30:3–12.

S. Tanachaiwiwat, et al. (2004). 'Location-centric isolation of misbehavior and trust routing in energy- constrained sensor networks'. In *Performance, Computing, and Communications, 2004 IEEE International Conference on*, pp. 463–469. IEEE.

M. Tubaishat & S. Madria (2003). 'Sensor networks: an overview'. *Potentials, IEEE* 22(2):20–23.

W. Walker, et al. (2003). 'Defining uncertainty: a conceptual basis for uncertainty management in model- based decision support'. *Integrated Assessment* 4(1):5–17.

J. Walters, et al. (2007). 'Wireless sensor network security: A survey'. *Security in distributed, grid, mobile, and pervasive computing* p. 367.

X. Wang, et al. (2010). 'Provenance based information trustworthiness evaluation in multi-hop networks'. *IEEE Globecom, Florida, USA* .

Y. Wang, et al. (2006). 'A survey of security issues in wireless sensor networks' .

Z. Y. Wang & J. Vassileva (2003a). 'Bayesian network-based trust model'. In *Web Intelligence, 2003. WI 2003.*
Proceedings. IEEE/WIC International Conference on, pp. 372–378. IEEE.

Y. Wang & J. Vassileva (2003b). 'Trust and reputation model in peer-to-peer networks'. In *Peer-to-Peer Computing, 2003.(P2P 2003). Proceedings. Third International Conference on*, pp. 150–157. IEEE.

G. Werner-Allen, et al. (2005). 'Monitoring volcanic eruptions with a wireless sensor network'. In *Wireless Sensor Networks, 2005. Proceeedings of the Second European Workshop on*, pp. 108–120. IEEE.

G. Werner-Allen, et al. (2006). 'Deploying a wireless sensor network on an active volcano'. *Internet Com- puting, IEEE* 10(2):18–25.

X. Xiao, et al. (2007). 'Using sensorranks for in-network detection of faulty readings in wireless sensor networks'. In *Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access*, pp. 1–8. ACM.

L. Xiong & L. Liu (2003). 'A reputation-based trust model for peer-to-peer e-commerce communities'. In
E-Commerce, 2003. CEC 2003. IEEE International Conference on, pp. 275–284. IEEE.

Z. Yao, et al. (2006). 'PLUS: Parameterized and localized trust management scheme for sensor networks security'. In *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on*, pp. 437–446. IEEE.

Z. Yao, et al. (2005). 'A security framework with trust management for sensor networks'. In *Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on*, pp. 190–198. IEEE.

E. Yoneki & J. Bacon (2005). 'A survey of Wireless Sensor Network technologies: research trends and middlewares role'. *University of Cambridge TR* 646.

Q. Zhang, et al. (2008). 'A framework for identifying compromised nodes in wireless sensor networks'. *ACM Transactions on Information and System Security (TISSEC)* 11(3):12.

D. Zhou (2003). 'Security issues in ad hoc networks'. In *The handbook of ad hoc wireless networks*, pp.
569–582. CRC Press, Inc.

L. Zhou & Z. Haas (1999). 'Securing ad hoc networks'. *Network, IEEE* 13(6):24–30.

W. Zhou, et al. (2007). 'Provenance-aware Declarative Secure Networks'. *Technical Reports (CIS)* p. 764.

W. Zhou, et al. (2008). 'Provenance-aware secure networks'. In *Data Engineering Workshop, 2008. ICDEW 2008. IEEE 24th International Conference on*, pp. 188–193. IEEE.

W. Zhou, et al. (2010). 'Efficient querying and maintenance of network provenance at internet-scale'. In
Proceedings of the 2010 international conference on Management of data, pp. 615–626. ACM.

T. Zia & A. Zomaya (2006). 'Security issues in wireless sensor networks'. In *Systems and Networks Com- munications, 2006. ICSNC'06. International Conference on*, pp. 40–40. Ieee.