Trust Models in Wireless Sensor Networks: A Survey

Mohammad Momani

Faculty of Engineering and Information Technology, School of Computing and Communications, University of Technology, Sydney, Australia
Mohammad.Momani@uts.edu.au

Abstract. This paper introduces the security and trust concepts in wireless sensor networks and explains the difference between them, stating that even though both terms are used interchangeably when defining a secure system, they are not the same. The difference between reputation and trust is also explained, highlighting that reputation partially affects trust. The methodologies used to model trust and their references are presented. The factors affecting trust updating are summarised and some examples of the systems in which these factors have been implemented are given. The survey states that, even though researchers have started to explore the issue of trust in wireless sensor networks, they are still examining the trust associated with routing messages between nodes (binary events). However, wireless sensor networks are mainly deployed to monitor events and report data, both continuous and discrete. This leads to the development of new trust models addressing the continuous data issue and also to combine the data trust and the communication trust to infer the total trust.

Keywords: Trust, model, wireless, sensor, networks, survey.

1 Introduction

Wireless sensor networks (WSNs) in recent years, have shown an unprecedented ability to observe and manipulate the physical world, however, as with almost every technology, the benefits of WSNs are accompanied by a significant risk factors and potential for abuse. So, someone might ask, how can a user trust the information provided by the sensor network?

Sensor nodes are small in size and able to sense events, process data, and communicate with each other to transfer information to the interested users. Typically, a sensor node consists of four sub-systems [1, 2].

- Computing sub-system (processor and memory): responsible for the control of the sensors and the execution of communication protocols.
- Communication sub-system (transceiver): used to communicate with neighbouring nodes and the outside world.
- Sensing sub-system (sensor): link the node to the outside world.
- Power supply sub-system (battery): supplies power to the node.

WSNs are a collection of self-organised sensor nodes that form a temporary network. Neither pre-defined network infrastructure nor centralised network administration

N. Meghanathan et al. (Eds.): CNSA 2010, CCIS 89, pp. 37–46, 2010.

exists. Wireless nodes communicate with each other via radio links and since they have a limited transmission range, nodes wishing to communicate with other nodes employ a multi-hop strategy for communicating and each node simultaneously acts as a router and as a host.

It should be noted that bandwidth available between communicating wireless nodes is restricted. This is because wireless networks have a significantly lower data transmission capacity compared to fixed-line data networks. Furthermore, wireless nodes only have a limited power supply available, as power supplied by batteries is easily exhausted. Lastly, wireless nodes may join or leave a network at any given time and frequently change their location in a network; this results in a highly dynamic network topology.

Due to impressive technological innovations in electronics and communications, small low-cost sensor nodes are available, which can collect and relay environmental data [3, 4]. These nodes have sensing, computing and short-range communication abilities and can be deployed in many environments. Such deployment can be in controlled environments, such as sensing the atmosphere in buildings and factories, where the mobility of the nodes is of interest. Or they can be spread in hazardous and hostile environments and left unattended. Originally motivated by surveillance in battlefields for the military, interest in WSNs spread over a wide range of applications, from scientific exploration and monitoring, for example, the deployment of a WSN on an active volcano [5, 6], to monitoring the microclimate throughout the volume of redwood trees [7], to building and bridge monitoring [8, 9], to health-care monitoring [10] and a number of other applications presented in [2, 3, 11, 12].

The rest of the paper is organised as follows: Section 2 discusses security in WSNs and section 3 introduces the notion of trust. Trust and reputation models in WSNs are presented in section 4 and section 5 concludes the paper.

2 Security in WSNs

In general, the key security goals of any network are to protect the network against all sorts of attacks, such as eavesdropping, fabrication, injection and modification of packets, impersonation; node capturing and many others, and to address other issues, like privacy, availability, accountability, data authentication, data integrity and data freshness. All these issues apply to traditional and wireless networks, but can have different consequences in WSNs, due to the open transmission medium, the resource constraints and the mass unattended deployment, especially in difficult and dangerous environments.

Research continues to be conducted into the design and optimisation of WSNs, as the use of these networks is still in its infancy phase. The security issue has been raised by many researchers [13-23], and, due to the deployment of WSN nodes in hazardous and/or hostile areas in large numbers, such deployment forces the nodes to be of low cost and therefore less reliable or more prone to overtaking by an adversary force. Some methods used, such as cryptographic authentication and other mechanisms [24-31], do not entirely solve the problem. For example, adversarial nodes can have access to valid cryptographic keys to access other nodes in the network. The reliability issue is certainly not addressed when sensor nodes are subject to system

faults. These two sources of problems, system faults and erroneous data or bad routing by malicious nodes, can result in the total breakdown of a network and cryptography by itself is insufficient to solve these problems. So new tools from different domains — social sciences, statistics, e-commerce and others — should be integrated with cryptography to completely solve the unique security attacks in WSNs, such as node capturing, Sybil attacks, denial of service attacks, etc.

3 Notion of Trust

Due to the nature of WSN deployment being prone to the surrounding environment and suffering from other types of attacks in addition to the attacks found in traditional networks, other security measurements different from the traditional approaches must be in place to improve the security of the network. The trust establishment between nodes is a must to evaluate the trustworthiness of other nodes, as the survival of a WSN is dependent upon the cooperative and trusting nature of its nodes.

Security and trust are two tightly interdependent concepts and because of this interdependence, these terms are used interchangeably when defining a secure system [32]. However, security is different from trust and the key difference is that, it is more complex and the overhead is high.

Trust has been the focus of researchers for a long time [33], from the social sciences, where trust between humans has been studied to the effects of trust in economic transactions [34-36]. Although intuitively easy to comprehend, the notion of trust has not been formally defined. Unlike, for example, reliability, which was originally a measure of how long a machine can be trustworthy, and came to be rigorously defined as a probability, trust is yet to adopt a formal definition.

Along with the notion of trust, comes that of reputation [37], which is occasionally treated by some authors as trust. Reputation is not to be confused with trust: the former only partially affects the latter. Reputation is the opinion of one person about the other, of one internet buyer about an internet seller, and by construct, of one sensor node about another. Trust is a derivation of the reputation of an entity. Based on the reputation, a level of trust is bestowed upon an entity. The reputation itself has been built over time based on that entity's history of behaviour, and may be reflecting a positive or negative assessment. It is these quantities that researchers try to model and apply to security problems in WSNs.

Among the motivating fields for the development of trust models is e-commerce, which necessitated the notion of judging how trusted an internet seller can be [37, 38]. This was the case for peer-to-peer networks and other internet forums where users deal with each other in a decentralised fashion [39-43]. Recently, attention has been given to the concept of trust to increase security and reliability in ad-hoc [32, 44-51] and sensor networks [52-54]. WSNs are open to unique problems, due to their deployment and application nature. The low cost of the sensor nodes of a WSN prohibits sophisticated measures to ensure data authentication. Some methods used, such as cryptographic, authentication and other mechanisms [24-28, 30], do not entirely solve the problem. In the following section a brief survey, introducing only the methodology used to formulate trust and how is it being updated, of existing research on trust in WSNs is presented in order to easily understand the concept of trust.

4 Trust in Sensor Networks

Trust in WSN networks plays an important role in constructing the network and making the addition and/or deletion of sensor nodes from a network, due to the growth of the network, or the replacement of failing and unreliable nodes very smooth and transparent. The creation, operation, management and survival of a WSN are dependent upon the cooperative and trusting nature of its nodes, therefore the trust establishment between nodes is a must. However, using the traditional tools such as cryptographic tools to generate trust evidence and establish trust and traditional protocols to exchange and distribute keys is not possible in a WSN, due to the resource limitations of sensor nodes [44]. Therefore, new innovative methods to secure communication and distribution of trust values between nodes are needed. Trust in WSNs, has been studied lightly by current researchers and is still an open and challenging field.

Reputation and trust systems in the context of sensor networks prior to this research have received little attention from researchers, however, recently researchers have started to make efforts on the trust topic, as sensor networks are becoming more popular. Ganeriwal and Srivastava were the first to introduce a reputation model specific to sensor networks in [52]; the RFSN (Reputation-based Framework for High Integrity Sensor Networks) model uses the Beta distribution, as a mathematical tool to represent and continuously update trust and reputation. The model classifies the actions as cooperative and non-cooperative (binary) and uses direct and indirect (second-hand) information to calculate the reputation. The second-hand information is weighted by giving more weight to the information coming from very reliable nodes. Trust is calculated as an expected value of the reputation and the behaviour of the node is decided upon a global threshold; if the trust value is below a threshold, the node is uncooperative, otherwise it is cooperative. The system propagates only the positive reputation information about other nodes [52], and by doing so, it eliminates the bad-mouthing attack, but at the same time it will affect the system's efficiency, as nodes will not be able to exchange their bad experience with malicious nodes. The aging factor is also introduced to differently weight the old and new interactions; more weight is given to recent interactions.

The DRBTS (Distributed Reputation-based Beacon Trust System) presented in [53] is an extension to the system introduced in [55], which presented a suite of techniques that detect and revoke malicious beacon nodes that provide misleading location information. It is a distributed security protocol designed to provide a method in which beacon nodes can monitor each other and provide information so that sensor nodes can choose to trust, using a voting approach. Every beacon node monitors its one hope neighbourhood for misbehaving beacon nodes and accordingly updates the reputation of the corresponding beacon node in the neighbour-reputation table. Beacon nodes use second-hand information for updating the reputation of their neighbours after the second-hand information passes a deviation test. A sensor node uses the neighbour-reputation table to determine whether or not to use a given beacon's location information based on a simple majority voting scheme. The DRBTS models the network as an undirected graph, uses first-hand and second-hand information to build trust.

Garth et al., [56] proposed a distributed trust-based framework and a mechanism for the election of trustworthy cluster heads in a cluster-based WSN. The model uses direct and indirect information coming from trusted nodes. Trust is modelled using

the traditional weighting mechanism of the parameters: packet drop rate, data packets and control packets. Each node stores a trust table for all the surrounding nodes and these values are reported to the cluster head only and upon request. This approach is not based on second-hand information, so it reduces the effect of bad-mouthing. Hur et al., proposed a trust model in [57], to identify the trustworthiness of sensor nodes and to filter out (remove) the data received from malicious nodes. In their model, they assume that each sensor node has knowledge of its own location, time is synchronised and nodes are densely deployed. They computed trust in a traditional way, weighting the trust factors (depending on the application) and there is no update of trust.

The proposed reputation-based trust model in WSNs by Chen et al., in [58], borrows tools from probability, statistics and mathematical analysis. They argued that the positive and/or negative outcomes for a certain event are not enough to make a decision in a WSN. They built up a reputation space and trust space in WSNs, and defined a transformation from the reputation space to the trust space [58]. The same approach presented in RFSN [52] is followed; a watchdog mechanism to monitor the other nodes and to calculate the reputation and eventually to calculate trust, and Bayes' theorem is used to describe the binary events, successful and unsuccessful transactions, with the introduction of uncertainty. Initially, the trust between strangers is set to (0) and the uncertainty is set to (1). The model does not use second-hand information, and how to refresh the reputation value is an issue. Xiao et al., in [59] developed a mechanism called SensorRank for rating sensors in terms of correlation by exploring Markov Chains in the network. A network voting algorithm called TrustVoting was also proposed to determine faulty sensor readings. The TrustVoting algorithm consists of two phases: self diagnose (direct reading) and neighbour diagnose (indirect reading), and if the reading is faulty then the node will not participate in the voting.

Crosby and Pissinou, in [60], proposed a secure cluster formation algorithm to facilitate the establishment of trusted clusters via pre-distributed keys and to prevent the election of compromised or malicious nodes as cluster heads. They used Beta distribution to model trust, based on successful and unsuccessful interactions. The updating occurs through incorporating the successful/unsuccessful interactions at time $t+1$ with those of time t. Their trust framework is designed in the context of a cluster-based network model with nodes that have unique local IDs. The authors of [61] proposed the TIBFIT protocol to diagnose and mask arbitrary node failures in an event-driven wireless sensor network. The TIBFIT protocol is designed to determine whether an event has occurred or not through analysing the binary reports from the event neighbours. The protocol outperforms the standard voting scheme for event detection.

A few other systems related to trust in WSNs, have been proposed in the literature such as [62-68], which use one or more of the techniques mentioned before to calculate trust. The proposed model in [62] uses a single trust value for a whole group (cluster), assuming that sensor nodes mostly fulfil their responsibilities in a cooperative manner rather than individually. In [63], the model is based on a distributed trust model to produce a trust relationship for sensor networks and uses the weighting approach to combine trust from different sources. In [64], a trust-based routing scheme is presented, which finds a forwarding path based on packet trust requirements, also using the weighting approach. In [65], a stochastic process formulation based on a number of assumptions is proposed to investigate the impact of liars on their peers' reputation about a subject. In [66], the authors proposed a new fault-intrusion tolerant

routing mechanism called MVMP (multi-version multi-path) for WSNs to provide both fault tolerance and intrusion tolerance at the same time.

The proposed model in [67] is an application-independent framework, built on the alert-based detection mechanisms provided by applications, to identify the malicious (compromised) nodes in WSNs. In [68], a parameterised and localised trust management scheme for sensor networks security (PLUS) is presented, whereby each sensor node rates the trustworthiness of its interested neighbours, identifies the malicious nodes and shares the opinion locally.

It is also worth mentioning that almost all the work undertaken on trust is based on successful and unsuccessful (binary) transactions between entities, that is, trust has been modelled in networks in general from a communication point of view, with no exception for WSNs, which is characterised by a unique feature: sensing events and reporting data. This unique characteristic is the basis of our research, which is focusing on modelling and calculating trust between nodes in WSNs based on continuous data (sensed events) and will eventually introduce the communication as a second factor of trust. Accordingly, a trust classification for WSNs has been introduced in [69] and in [70, 71] a new framework to calculate trust in WSNs has been introduced, using the traditional weighting approach to combine direct and indirect trust. In [72], the sensed data was introduced as the decisive factor of trust, that is, trust in WSNs was modelled from the sensor reliability perspective. The RBATMWSN model introduced in [73], represents a new trust model and a reputation system for WSNs, based on sensed continuous data. The trust model establishes the continuous version of the Beta reputation system applied to binary events and presents a new Gaussian Trust and Reputation System for Sensor Networks (GTRSSN), as introduced in [74], which introduces a theoretically sound Bayesian probabilistic approach for mixing second-hand information from neighbouring nodes with directly observed information to calculate trust between nodes in WSNs, and finally a Bayesian fusion approach was introduced in [75], to combine continuous data trust based on sensed events and binary communication trust based on successful and unsuccessful transactions between nodes.

References

1. Bharathidasan, A., Ponduru, V.A.S.: Sensor Networks: An Overview, Technical Report, Dept. of Computer Science, University of California at Davis (2002)
2. Tubaishat, M., Madria, S.: Sensor networks: an overview. IEEE Potentials 22, 20–23 (2003)
3. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless Sensor Networks: a Survey. Computer Networks 38, 393–422 (2002)
4. Rajaravivarma, V., Yang, Y., Yang, T.: An Overview of Wireless Sensor Network and Applications. In: The 35th Southeastern Symposium on System Theory (2003)
5. Werner-Allen, G., Lorincz, K., Ruiz, M., Marcillo, O., Johnson, J., Lees, J., Welsh, M.: Deploying a Wireless Sensor Network on an Active Volcano. IEEE Internet Computing (2005)
6. Werner-Allen, G., Johnson, J., Ruiz, M., Lees, J., Welsh, M.: Monitoring Volcanic Eruptions with a Wireless Sensor Network. In: Second European Workshop on Wireless Sensor Networks (EWSN 2005), Istanbul, Turkey (2005)

7. Culler, D., Estrin, D., Srivastava, M.: Overview of Sensor Networks. IEEE Computer Journal 37, 41–49 (2004)
8. Glaser, S.D.: Some Real-world Applications of Wireless Sensor Nodes. In: Proceedings of the SPIE Symposium on Smart Structures and Materials NDE, San Diego, CA, USA (2004)
9. Paek, J., Gnawali, O., Jang, K.-Y., Nishimura, D., Govindan, R., Caffrey, J., Wahbeh, M., Masri, S.: A Programmable Wireless Sensing System for Structural Monitoring. In: The 4th World Conference on Structural Control and Monitoring (4WCSCM), San Diego, CA (2006)
10. Gao, T., Greenspan, D., Welsh, M., Juang, R., Alm, A.: Vital Signs Monitoring and Patient Tracking over a Wireless Network. In: The 27th Annual International Conference of the Engineering in Medicine and Biology Society, IEEE-EMBS 2005 (2005)
11. Yoneki, E., Bacon, J.: A Survey of Wireless Sensor Network Technologies: Research Trends and Middlewares Role, Computer Laboratory. University of Cambridge, Cambridge (2005)
12. Callaway, E.H.: Wireless sensor networks: architectures and protocols. CRC Press LLC, Boca Raton (2004)
13. Wang, Y., Attebury, G., Ramamurthy, B.: A Survey of Security Issues in Wireless Sensor Networks. IEEE Communications Surveys and Tutorials 8, 2–23 (2006)
14. Stajano, F., Anderson, R.: The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In: Malcolm, J.A., Christianson, B., Crispo, B., Roe, M. (eds.) Security Protocols 1999. LNCS, vol. 1796, pp. 172–182. Springer, Heidelberg (2000)
15. Perrig, A., Stankovic, J., Wagner, D.: Security in Wireless Sensor Networks. Communications of the ACM 47, 53–57 (2004)
16. Chan, H., Perrig, A.: Security and Privacy in Sensor Networks. IEEE Computer Journal 36, 103–105 (2003)
17. Zia, T., Zomaya, A.: Security Issues in Wireless Sensor Networks. In: International Conference on Systems and Networks Communication (ICSNC 2006), Tahiti, French Polynesia (2006)
18. Newsome, J., Shi, E., Song, D., Perrig, A.: The Sybil Attack in Sensor Networks: Analysis & Defenses. In: The 3rd International Symposium on Information Processing in Sensor Networks, New York (2004)
19. Walters, J.P., Liang, Z., Shi, W., Chaudhary, V.: Wireless Sensor Network Security: A Survey. In: Xiao, Y. (ed.) Security in Distributed, Grid, and Pervasive Computing. Auerbach Publications/CRC Press (2006)
20. Zhou, D.: Security Issues in Ad-hoc Networks. In: The Handbook of Ad-hoc Wireless Networks, pp. 569–582. CRC Press, Inc., Boca Raton (2003)
21. Papadimitratos, P., Haas, Z.J.: Securing Mobile Ad-hoc Networks. In: The Handbook of Ad-hoc Wireless Networks. CRC Press LLC, Boca Raton (2003)
22. Zhou, L., Haas, Z.J.: Securing Ad-hoc Networks. IEEE Network Magazine (1999)
23. Przydatek, B., Song, D., Perrig, A.: SIA: Secure Information Aggregation in Sensor Networks. In: The 1st International Conference on Embedded Networked Sensor Systems Los Angeles, California, USA (2003)
24. Karlof, C., Wagner, D.: Secure Routing in Sensor Networks: Attacks and Countermeasures. In: First IEEE International Workshop on Sensor Network Protocols and Applications (2003)
25. Bohge, M., Trappe, W.: An Authentication Framework for Hierarchical Ad-hoc Sensor Networks. In: 2003 ACM Workshop Wireless security (WiSe 2003), San Diego, CA, USA (2003)

26. Karlof, C., Sastry, N., Wagner, D.: TinySec: A Link Layer Security Architecture for Wireless Sensor Network. In: Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, Baltimore, MD, USA (2004)
27. Perrig, A., Zewczyk, R., Wen, V., Culler, D., Tygar, D.: SPINS: Security Protocols for Sensor Networks. Wireless Networks 8, 521–534 (2002)
28. Ye, F., Luoa, H., Lu, S., Zhang, L.: Statistical En-route Filtering of Injected False Data in Sensor Networks. Selected Areas in Communications of the ACM 23 (2005)
29. Zhu, S., Setia, S., Jajodia, S.: LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. In: The 10th ACM Conference on Computer and Communications Security, Washington D.C., USA (2003)
30. Zhang, Y., Liu, W., Lou, W., Fang, Y.: Location-based Compromise Tolerant Security Mechanisms for Wireless Sensor Networks. IEEE Journal on Selected Areas in Communications 24, 247–260 (2006)
31. Zhang, W., Cao, G.: Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach. In: The 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2005), Miami, USA (2005)
32. Pirzada, A.A., McDonald, C.: Establishing Trust in Pure Ad-hoc Networks. In: The 27th Australasian Conference on Computer Science, Dunedin, New Zealand (2004)
33. McKnight, D.H., Chervany, N.L.: The Meanings of Trust: MIS Research Center, Carlson School of Management. University of Minnesota (1996)
34. Ba, S., Pavlou, P.A.: Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior. MIS Quarterly 26, 243–268 (2002)
35. Dasgupta, P.: Trust as a Commodity. In: Ingram, D. (ed.) Trust: Making and Breaking Cooperative Relations, electronic edn., pp. 49–72. Department of Sociology, University of Oxford (2000)
36. McKnight, D.H., Cummings, L.L., Chervany, N.L.: Trust Formation in new Organaizational Relationships: MIS Research Center, Carlson School of Management. University of Minnesota (1996)
37. Resnick, P., Kuwabara, K., Zeckhauser, R., Friedman, E.: Reputation systems. Communications of the ACM 43, 45–48 (2000)
38. McKnight, D.H., Chervany, N.L.: Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model. In: The 34th Hawaii International Conference on System Sciences (2001)
39. Aberer, K., Despotovic, Z.: Managing Trust in a Peer-2-Peer Information System. In: The Tenth International Conference in Information and Knowledge Management, Atlanta, Georgia, USA (2001)
40. Blaze, M., Feigenbaum, J., Ioannidis, J., Keromytis, A.: The KeyNote Trust Management System. University of Pennsylvania, Philadelphia (1999)
41. Xiong, L., Liu, L.: A Reputation-based Trust Model for Peer-to-Peer E-Commerce Communities. In: IEEE International Conference on E-Commerce Technology (CEC 2003), pp. 275–284 (2003)
42. Blaze, M., Feigenbaum, J., Lacy, J.: Decentralized Trust Managament. In: IEEE Symposium on Security and Privacy (1996)
43. Chen, R., Yeager, W.: Poblano: A Distributed Trust Model for Peer-to-Peer Networks. Sun Microsystems (2001)
44. Eschenauer, L.: On Trust Establishment in Mobile Ad-hoc Networks. In: Department of Electrical and Computer Engineering, vol. Master of Science, p. 45. University of Maryland, College Park (2002)

45. Baras, J.S., Jiang, T.: Dynamic and Distributed Trust for Mobile Ad-hoc Networks. University of Maryland, Orlando (2004)
46. Liu, Z., Joy, A.W., Thompson, R.A.: A Dynamic Trust Model for Mobile Ad-hoc Networks. In: The 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, FTDCS 2004 (2004)
47. Davis, C.R.: A Localized Trust Management Scheme for Ad-hoc Networks. In: The 3rd International Conference on Networking, ICN 2004 (2004)
48. Buchegger, S., Boudec, J.Y.L.: Performance analysis of the CONFIDANT protocol (Cooperation of Nodes- Fairness in Dynamic Ad-hoc NeTworks). In: The 3rd ACM Internationa Symposium Mobile Ad-hoc Networking & Computing (MobiHoc 2002), Lausanne, CH (2002)
49. Michiardi, P., Molva, R.: CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad-hoc Networks. In: The IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security Portoroz, Slovenia (2002)
50. Capra, L.: Towards a Human Trust Model for Mobile Ad-hoc Networks. In: The 2nd UK-UbiNet Workshop. Cambridge University, Cambridge (2004)
51. Serugendo, G.D.M.: Trust as an Interaction Mechanism for Self-Organising Systems. In: International Conference on Complex Systems (ICCS 2004). Marriott Boston Quincy, Boston (2004)
52. Ganeriwal, S., Srivastava, M.B.: Reputation-based Framework for High Integrity Sensor Networks. In: The 2nd ACM Workshop on Security of Ad-hoc and Sensor Networks, Washington, DC, USA (2004)
53. Srinivasan, A., Teitelbaum, J., Wu, J.: DRBTS: Distributed Reputation-based Beacon Trust System. In: The 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, DASC 2006 (2006)
54. Ganeriwal, S., Balzano, L.K., Srivastava, M.B.: Reputation-based Framework for High Integrity Sensor Networks. ACM Transactions on Sensor Networks v (2007)
55. Liu, D., Ning, P., Du, W.: Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks. In: The 25th IEEE International Conference on Distributed Computing Systems, ICDCS 2005 (2005)
56. Crosby, G.V., Pissinou, N., Gadze, J.: A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks. In: The Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS 2006), Columbia, Maryland (2006)
57. Hur, J., Lee, Y., Yoon, H., Choi, D., Jin, S.: Trust Evaluation Model for Wireless Sensor Networks. In: The 7th International Conference on Advanced Communication Technology (ICACT 2005), Gangwon-Do, Korea (2005)
58. Chen, H., Wu, H., Zhou, X., Gao, C.: Reputation-based Trust in Wireless Sensor Networks. In: International Conference on Multimedia and Ubiquitous Engineering (MUE 2007), Seoul, Korea (2007)
59. Xiao, X.-Y., Peng, W.-C., Hung, C.-C., Lee, W.-C.: Using SensorRanks for In-Network Detection of Faulty Readings in Wireless Sensor Networks. In: The 6th ACM International Workshop on Data Engineering for Wireless and Mobile Access Beijing, China (2007)
60. Crosby, G.V., Pissinou, N.: Cluster-based Reputation and Trust for Wireless Sensor Networks. In: The 4th IEEE Consumer Communications and Networking Conference (CCNC 2007), Las Vegas, Nivada (2007)
61. Krasniewski, M., Varadharajan, P., Rabeler, B., Bagchi, S.: TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks. In: The 2005 International Conference on Dependable Systems and Networks, Yokohama, Japan (2005)

62. Shaikh, R.A., Jameel, H., Lee, S., Rajput, S., Song, Y.J.: Trust Management Problem in Distributed Wireless Sensor Networks. In: The 12th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA 2006), Sydney, Australia (2006)
63. Yao, Z., Kim, D., Lee, I., Kim, K., Jang, J.: A Security Framework with Trust Management for Sensor Networks. In: The 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks (2005)
64. Hung, K.-S., Lui, K.-S., Kwok, Y.-K.: A Trust-Based Geographical Routing Scheme in Sensor Networks. In: The IEEE Wireless Communications and Networking Conference (WCNC 2007), Hong Kong (2007)
65. Mundinger, J., Boudec, J.-Y.L.: Reputation in Self-Organized Communication Systems and Beyond. In: The 2006 Workshop on Interdisciplinary Systems Approach in Performance Evaluation and Design of Computer & Communications Sytems, Pisa, Italy (2006)
66. Ma, R., Xing, L., Michel, H.E.: Fault-Intrusion Tolerant Techniques in Wireless Sensor Networks. In: The 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (2006)
67. Zhang, Q., Yu, T., Ning, P.: A Framework for Identifying Compromised Nodes in Sensor Networks. ACM Transactions on Information and System Security (TISSEC) 11 (2008)
68. Yao, Z., Kim, D., Doh, Y.: PLUS: Parameterized and Localized trUst Management Scheme for Sensor Networks Security. In: The Third IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS). IEEE, Vancouver (2006)
69. Momani, M., Agbinya, J., Navarrete, G.P., Akache, M.: Trust Classification in Wireless Sensor Networks. In: The 8th International Symposium on DSP and Communication Systems (DSPCS 2005), Noosa Heads, Queensland, Australia (2005)
70. Momani, M., Agbinya, J., Navarrete, G.P., Akache, M.: A New Algorithm of Trust Formation in Wireless Sensor Networks. In: The 1st IEEE International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2006), Sydney, Australia (2006)
71. Momani, M., Agbinya, J., Alhmouz, R., Navarrete, G.P., Akache, M.: A New Framework of Establishing Trust in Wireless Sensor Networks. In: International Conference on Computer & Communication Engineering (ICCCE 2006), Kuala Lumpur, Malaysia (2006)
72. Momani, M., Challa, S., Aboura, K.: Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective. In: Sobh, T., Elleithy, K., Mahmood, A., Karim, M. (eds.) Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications. Springer, Netherlands (2007)
73. Momani, M., Aboura, K., Challa, S.: RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks. In: The Third International Conference on Intelligent Sensors, Sensor Networks and Information, Melbourne, Australia (2007)
74. Momani, M., Challa, S.: GTRSSN: Gaussian Trust and Reputation System for Sensor Networks. In: International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE 2007). University of Bridgeport (2007)
75. Momani, M., Challa, S., Alhmouz, R.: Can we Trust Trusted Nodes in Wireless Sensor Networks? In: The International Conference on Computer and Communication Engineering (ICCCE 2008), Kuala Lumpur, Malaysia (2008)