A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks

M. Carmen Fernández-Gago, Rodrigo Román, Javier Lopez
Department of Computer Science, University of Malaga, 29071, Málaga, Spain
{mcgago,roman,jlm}@lcc.uma.es

Abstract

Trust plays an important role in human life environments and virtual organizations. In the context of a network, trust may help its elements to decide whether another member of the same network is being uncooperative or malicious. Trust becomes quite important in self-configurable and autonomous systems, such as wireless sensor networks (WSN). However, very little effort has been done in the field of trust management in WSN. On the other hand, some efforts have been made in quite related fields such as Ad-hoc and P2P networks. In this paper we give an overview of existing trust management solutions, mainly those developed for Ad-Hoc and P2P networks and, more importantly, investigate their suitability to WSN. We also provide some guidelines to aid the development of trust management systems for WSN according to the nature of these networks.

1 Introduction

The Wireless Sensor Networks paradigm has been shown as a growing area of research. One of the main reasons for this growth is its usefulness in many real-life situations such as environmental, healthcare or Ambient Intelligence scenarios. All of these scenarios require of specific services that WSN can help to provide due to their autonomous capabilities and their potential to self-configure. However, security problems inherent to WSN also arise. WSN are usually very accessible within the physical world, what makes them very vulnerable. Also, due to their computational or energy constraints, an attack could make the network partially or totally unusable. Thus, providing WSN with security mechanisms becomes very important. Trust, or the trust on the behaviour of the elements of the network, is a key aspect for WSN. A trust management system can be useful for detecting a node which is not behaving as expected (either faulty or maliciously) or it can assist in the decision-making process, for instance, if a node needs a partner in order to achieve a common goal. Even though trust is an important feature for WSN few systems have considered it [12, 23]. However, more efforts have been made on the fields of Ad-hoc and P2P networks, which are somehow similar to WSN. In this paper we provide an overview of the existing trust management approaches for some kind of networks, more specifically for Ad-hoc and P2P networks, and analyse how these approaches can be applied to WSN. As a result, it becomes possible to extract what are the requirements that a trust management system should fulfill in a WSN environment, and to provide new directions for future works in this area. The structure of the paper is as follows. The notions of trust and trust management are given in Section 2. The existing solutions of trust management for Ad-hoc and P2P networks are also given in this section. Section 3 is devoted to sensor networks, paying special attention to the importance of trust for these networks. The applicability to WSN of the existing trust management methods mentioned earlier is analyzed in Section 4. Section 5 gives some directions for future research and Section 6 concludes the paper.

2 Trust Management

2.1 Trust Management Solutions

The term *trust management* was first coined by Blaze et. al in [7] as an attempt to define a coherent framework for the study of security policies, credentials and trust relationships. One of the first implementations of a trust management system was PolicyMaker [8, 6, 9]. KeyNote [5] appeared as an improvement of PolicyMaker and REFEREE [10] as a trust management system for web services.

There are have been many attempts to specify trust for different domains. Our interest focus on trust management for WSN. Very little has been done on this field, but some efforts have been carried out in quite related areas such as Ad-hoc and P2P networks. Most of the trust management systems developed for these kind of networks consist of collection of data and the application of a certain engine in order to compute that data. Most of these systems are based,

or take into consideration, the concept of *reputation*. Once the reputation ratings of a system are collected, they should be computed. There exist different reputation engines. A classification of them can be found in [13].

Trust management and reputation methods for Ad-hoc and P2P networks can be classified into two types- basing the notion of trust on the values obtained from peers behaviour and certificate-based trust establishment methods. The work in [2] presents a classification of these methods for Ad-Hoc and sensor networks. Most of the methods presented in this paper correspond to behaviour-based trust establishment frameworks, where each node performs trust evaluation based on continuous monitoring of the behaviour of its neighbours in order to evaluate how trustable they are. In certificate-based trust establishment methods trust decisions are mainly based on the provision of a valid certificate that proves that the target node is considered trusted either by a certification authority or by other nodes that the issuer trusts.

Ad-hoc Networks. In [15] the authors present a trust model for mobile Ad-hoc networks that can be used in a dynamic context within the routing process. Initially, each node is assigned a trust value according to its identity. For instance, if no information is available about the trustworthiness of a node the assigned value will be *unknown*. Each node records the trust levels about their neighbours. Then, by using simple, logical calculations similar to averages a node i can derive the trust level of node j, $TL_i(j)$. In [21] secure routing is also considered but the way of assigning the trust levels is carried out by evaluation of nodes over other nodes. Trust is evaluated considering factors such as statistics, data value, intrusion detection or personal reference to other nodes. The trust evaluation values, $TE(i, j)$, are stored in a matrix. The final trust value is calculated via a linear function that uses the values stored in the matrix. Reputation is considered in [16] as a way for building trust. The mechanism builds trust through an entity called the *trust manager*. An important part of the trust manager is the reputation handling module. Each node monitors the activities of its neighbours and sends the information to the reputation manager. Then, the information is passed to the reputation handling module and the reputation values are obtained via simple metrics. Zhu *et al* [22] provide a practical approach to compute trust in wireless networks by viewing any individual mobile device as a node of a delegation graph G and mapping a delegation graph from the source node S to the target node T into an edge in the correspondent transitive closure of the graph G, from which the trust value is computed.

P2P Networks. PET [14] is a personalized trust model that evaluates risk and reputation separately in order to derive trust values. Reputation is also used as a way to obtain trust in [1]. In this work, when an agent wants to evaluate the trustworthiness of another agent, it starts to search for complaints on it. Once the data about the complaints is collected trust can be assessed by an algorithm proposed by the authors. Bayesian networks have also been used [3, 20]. Other approaches [18] use statistics methods such as standard deviation and mean in order to detect anomalies or malicious behaviour of peers.
TrustMe [17] is a secure protocol for anonymous trust management that uses public-key cryptography. A similar approach is presented in [11] where the authors introduce a protocol based on a polling mechanism. This protocol also uses public key cryptography.

3 Sensor Networks and Trust

3.1 The Importance of Trust in Sensor Networks

It is possible that the emerging importance of sensor networks could be hindered by their inherent security problems. It is then imperative to provide a set of security primitives and services that can protect those network and improve their robustness and reliability. Trust management, which models the trust on the behavior of the elements of the network, can be specially useful for a sensor network environment. Not only it can help the nodes of the network to self-configure themselves against any change in their neighbourhood, but it can also assist and/or take advantage of the other security protocols, as shown in the following paragraphs.

The first step towards a robust and reliable sensor network is to properly secure the node as a physical entity, by using code and data obfuscation schemes or software attestation mechanisms. The outputs of these schemes can be easily integrated into a trust management system that can also be used as a tool launched by the trust system for testing the integrity of a suspected node. After protecting the node, it is time to protect the communication channel against eavesdroppers and other adversaries using cryptographic primitives. These primitives need a Key Management System (KMS) for distributing and maintaining their security credentials. The existence of a trust management system can assist the activities of such KMS by, for example, pointing out which nodes are completely untrusted for the purpose of revoking their keys.

Protecting the channel is not enough for assuring the security of the network. The functionality of the network relies on a minimal set of core protocols required for providing services, which are routing, data aggregation and time

synchronization. Finally, a sensor network may also require the assistance of other services like secure location for creating services of greater complexity. All these services, core or not, can benefit from the existence of a trust management system, either by using the output of the trust system as an assistant in their decision-making process, or by providing useful inputs for the trust system that could be of use for any other service.

3.2 Current State of Trust Management Solutions in Sensor Networks

As we have mentioned in previous sections very little has been done in the field of trust management for WSN, and in those that consider this topic, the approaches are quite similar, if not the same, as those proposed for Ad-hoc and P2P networks. However, as we will see in coming sections there are differences among these type of networks and, consequently adapting the trust management for Ad-hoc and P2P networks may not be suitable for WSN.

In [12] the authors introduce a reputation framework for high integrity sensor networks based on bayesian formulation. The architecture of the framework considers watchdog mechanism, reputation, trust, behaviour and second hand information. Reputation is stored in a table where the entries are built by the nodes through the Watchdog mechanism. Nodes not only use their own direct observations but they also exchange information with other nodes (second hand information). Reputation is calculated by using the beta reputation distribution and trust is obtained as a function of reputation. Then the behaviour of a node is given by *cooperate* and *don't cooperate* according to whether the trust values are respectively above or below a given threshold. Tanachaiwiwat *et al* [19] propose a location-centric architecture for isolating misbehaviour and establishing trust routing in sensor networks. Trust values are calculated as a function of cryptography, availability and packet forwarding. If a value is below a specific threshold the node is considered insecure and it is isolated. In this work the traffic flow is from/to the sink (or base station). One of the latest approaches of trust management for wireless sensor networks is introduced in [23]. They propose a framework similar to existing approaches for Ad-hoc networks where trust values are assigned to each node. A trust evaluation process is carried out based on the localized trust model and two kinds of knowledge: *p*ersonal reference obtained by direct interaction with the node to be evaluated (*suspect* node) and *r*eference or reputation sent by the *juries* (specific nodes which are given this role). The trust value is obtained as a simple summation between the personal reference and the reference as $T_i = T_{pr(i)} \times W_{pr} + T_{r(i)} \times W_r$, where $W_{pr} + W_r = 1$ and $pr(i)$ denotes personal reference of node i and r denotes the reference. N.B. that obtaining $T_{pr(i)}$ and $T_{r(i)}$ involves the use of some algorithms which are not as simple as the formula above. The evaluation of the suspect node is done by the *judge*.

4 Analysis of Trust Management Systems for Wireless Sensor Networks

WSN present some constraints due to their nature (computational power, energy-consuming, etc). For this reason, the applicability of the methods outlined in the previous sections might not be trivial or even possible for this kind of networks. In the following we will try to analyse the applicability of such a methods to WSN from the point of view of *data collection* (cf. Section 4.1) and *system features* (cf. Section 4.2).

For *data collection* we refer to the data collected from the nodes' behaviour. This forms the basis for most of the trust management frameworks. Our belief is that the type of behavioral data collected from Ad-hoc and P2P nodes is not enough for WSN, thus it is necessary to point out what are the primary sources of behavioral data for sensor nodes. Regarding *system features*, we refer to the overall features of the trust system, such as initialization procedures, hierarchy, trust evolution, and others. It is also our belief that the solutions mentioned in this paper for Ad-hoc and P2P networks do not satisfy the special requirements of a sensor network, and that existing solutions for WSN do not adequately fulfill such needs.

4.1 Data Collection

One of the most important aspects of trust management solutions is the process of data collection. In general, for the development of the trust management systems mentioned in this work, data related to the nodes behaviour is collected and then analyzed depending on how the system works. Therefore, it is essential to point out what type of data will be more relevant for these systems, and which are the sources that can provide a useful feedback to the system. Notice that a node should not only collect data about other devices, but also about itself.

From the perspective of the hardware, a node that is not detected as alive for a long period of time [4], or that appears and disappears from the network under normal conditions, should not be considered trusted. Such mistrust comes from the belief that the node is being tampered, or is starting to malfunction and cannot properly provide services to the other nodes.

On the communication layer, there are plenty of situations where one node should start to mistrust another. A node creating alarms (e.g. temperature sensors reporting a

fire) when the physical surroundings are calm, or reporting an answer to a non-existent query of the base station, should be mistrusted. Another possible reason of mistrust is when a node starts creating packets outside the "burst time", i.e. when the periodic sensor readings are forwarded to the base station. Also, important issues such as selective forwarding and packet delaying, which can be detected thanks to the broadcast nature of communications, have to be taken into account.

As for the sensor readings, the inherent redundancy of the network can help on detecting values, which can be either external or internal to a sensor node, that significantly differ from the average of a certain neighbourhood. Finally, misbehavior in the core protocols and application services, such as lying in a negotiation process or exchanging false or delayed data, is another reason for mistrusting a certain node. Note that a node should not only take into consideration the reports produced by itself while observing other nodes, but also the reports produced by its neighbouring nodes, taking into account the possible existence of malicious reports.

Summarizing, there is a large set of network events, ranging from hardware-related situations to behaviour in the application layer, that can be used as inputs for the trust management system. Nevertheless, the existing trust systems for sensor networks do not take all of them into account. For example, only data consistency and forwarding issues are considered by Ganeriwal and Srivastava [12]. Tanachaiwiwat et. al. [19] also considers the availability of a node, but other aspects are left behind. At last, Yao et. al. [23] consider the lack of cryptographic operations as a source of mistrust. The existence of malicious behaviour in some, but not all, node interactions is also considered as a source of mistrust.

4.2 System Features

In this section we will analyse the applicability of the methods presented in Section 2.1 to WSN. In particular we will analyse the applicability of the methods for Ad-hoc and P2P networks. We will also analyse the methods presented in Section 3.2. This analysis will be done from the point of view of the overall features of the trust system.

4.2.1 Advantages and Disadvantages of Trust Management Frameworks for Ad-Hoc and P2P networks

In general, the solutions designed for Ad-Hoc and P2P networks are not suitable for sensor networks environments. The main reason is essentially the differences among these network architectures in terms of infrastructure and functionality. Among these features power constraint which is much more restricted in WSN than on P2P or Ah-Hoc networks.

Scalability and lifetime of the network are other issues to be taken into account. In Ad-Hoc networks, the number of members is usually not high, while in sensor networks it is likely to have a community of thousands of nodes. In P2P networks cab be even higher than in WSN. Regarding the lifetime of the network, a sensor network could offer its services for much longer periods of time than Ad-Hoc and P2P networks, where nodes enter and exit the network periodically offering their functionality for a short period of time. This may affect the way trust evolves on the network and how trust values should be updated.

A final difference between Ad-Hoc, P2P and sensor networks is the behaviour of the nodes. Any deviation in the behaviour of a single node should be reason enough to start suspecting of the integrity of that node, as seen in Section 4.1. As a result, the mechanisms and rules that dictate the evolution of trust for a single sensor node have to be calibrated for these kind of situations.

It is possible to identify the previously presented issues in the trust management solutions developed for Ad-Hoc and P2P networks introduced in Section 2.1. For example, the approach presented in [16] considers reputation in order to build trust for Ad-hoc networks. This is done through a reputation manager. This method might not be very applicable to sensor networks due to several reasons. Using an entity such as a reputation manager that controls all the traffic information and distribute it might be very high energy-consuming for sensor networks. Scalability might also be a problem. Other approaches for Ad-hoc networks [15, 21] might not be suitable for sensor networks. These methods consider that an initial trust value is given to each node according to their identity. This could be considered a bit contradictory with the nature of sensor networks, as initially all nodes in the WSN are preloaded with identification information created by the user. Assigning initial trust values to each node might not be very accurate in order to compute the final trust value. However, Yao *et.al* [23] follow this approach for WSN.

4.2.2 Analysis of the Existing Approaches for WSN

In section 3.2 we gave an outline of the existing approaches to trust management for wireless sensor networks. To the best of our knowledge only these few works have been done so far in this area.

In all of these approaches the observations or data used in order to derive trust or reputation values only take into account one or two specific aspects, and as we have mentioned in Section 4.1 the nature of the data collected is essential for the development of a trust management system. Thus, in [19] the observations are based on forwarding and routing process and in [23] observations only consider correctness of forwarding. Ganeriwal et al [12] do realise that not all the

events should be given the same importance for their reputation system, however they only consider forwarding and data consistency when calculating reputation.

An interesting approach is followed by Tanachaiwiwat where the base station (or sink, as they called it) is in charge of storing the trust values obtained by itself or other nodes and distributing the blacklisting. In the other approaches the nodes are in charge of using their observations. Even further, Yao et al consider for their trust system self-confidence of nodes as a very important factor. They give more weight to the personal reference trust. We believe this does not correspond to the nature of WSN. In particular, we believe that the approach followed by the authors does not reflect in general the nature of WSN and this approach could be used in a general sense for any kind of network.

5 Research Directions

It is clear that any trust management system has to be specially designed and prepared for reacting against the particular issues, such as autonomy, decentralization, and initialization, that can be found in wireless sensor network environments. Although there are some existing architectures for WSN that partially solve these problems, it is still possible to point out the neglected aspects that can be considered crucial for creating a satisfactory trust system.

Regarding the initialization of the trust model, initial trust is not a very important value, since all nodes are usually initialized in a controlled environment, and the events that occur during the lifetime of the network are more indicative of their behaviour. Such events, as pointed out by Ganeriwal and Srivastava [12], are not equally important for calculating the reputation of a node. However, the existence of a certain event does not mean that the node is going to misbehave in all its activities. Therefore, it should be necessary to deduce different trust values for every distinct behaviour of the nodes.

Sensor nodes should also be aware of the trust history of their neighbourhood. Since all sensor nodes have to perform almost the same tasks continuously on time, a node that is intermittently uncooperative should be completely untrusted. The consistence in the trust readings is also significant. A normal sensor network environment should produce very few reports regarding malicious activities. Therefore, the existence of different and contradictory reports should be evidence enough of malicious activity and source of mistrust.

Note that all the important decisions taken by the nodes, such as node exclusion, should be notified to the base station for logging, monitoring and maintenance purposes. However, as mentioned by Tanachaiwiwat *et. al.* [19], it is possible for the base station to have its own trust model. Going further into that assumption, the base station can be considered as a special, more powerful node that receives the most significant data created inside the network. Therefore, it can be possible to create a valid trust model that can monitor the behavior of the nodes using such huge volume of data.

As a final matter, one of the biggest constraints regarding trust management for sensor networks is the overhead that the existence of this system may impose over the constrained elements of the network. It is then imperative to balance the overhead of the data collection process, and to make both these processes and the trust and reputation models as lightweight as possible. Due to the broadcast nature of the communications, the simplicity of the data collection processes, and the inherent redundancy of sensor networks, we think it is still probable to have a functional trust management system for sensor networks.

6 Conclusions

Trust is an important factor in any kind of social or computing network environment. In particular, we are interested in developing trust management systems for WSN. Thus, in order to achieve our goal we have firstly investigated the existing approaches for Ad-hoc and P2P networks and then their applicability to WSN. In this work, we intend to set the basis for a future research line and therefore, we have identified some features of the existing trust management methods that could be suitable for WSN and some others that could not be applied to WSN at all. We have also identified the main problems and the possible solutions in order to develop trust management systems for WSN. Thus, we consider that data collection is a very important factor in the process of designing a trust management system. Not all the data is equally relevant and their relevance may evolve with time. The systems should be history-aware, meaning that newer information is more relevant to the system, but past behaviour shall also be taken into account. We have also highlighted the importance of the role of the base station. A good trust management solution should be an essential part of it.

References

[1] K. Aberer and Z. Despotovic. Managing trust in a peer-2-peer information system. In Henrique Paques, Ling Liu, and David Grossman, editors, *Proceedings of the Tenth International Conference on Information and Knowledge Management (CIKM01)*, pages 310–317. ACM Press, 2001.

[2] E. Aivaloglou, S. Gritzalis, and C. Skianis. Trust Establishment in Ad Hoc and Sensor Networks. In J. López, editor, *1st International Workshop on Critical Information Infrastructure Security, CRITIS'06*,

volume 4347 of *Lectures Notes in Computer Science, LNCS*, pages 179–194, Samos, Greece, 2006. Springer.

[3] T. Bearly and V. Kumar. Expanding Trust Beyond Reputation in Peer to Peer Systems. In *15th International workshop on Database and Expert Systems Applications (DEXA'04), IEEE Computer Society*, 2004.

[4] A. Becher, Z. Benenson, and M. Dornseif. Tampering with Motes: Real-world Physical Attacks on Wireless Sensor Networks. In *3rd International Conference on Security in Pervasive Computing (SPC 2006)*, York, UK, April 2006.

[5] M. Blaze, J. Feigenbaum, and A. D. Keromytis. KeyNote: Trust Management for Public-Key Infrastructures (position paper). *Lecture Notes in Computer Science*, 1550:59–63, 1999.

[6] M. Blaze, J. Feigenbaum, and A. D. Keromytis. The Role of Trust Management in Distributed Systems Security. In *Secure Internet Programming*, pages 185–210, 1999.

[7] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized Trust Management. In *IEEE Symposium on Security and Privacy*, 1996.

[8] M. Blaze, J. Feigenbaum, and M. Strauss. Compliance Checking in the PolicyMaker Trust Management System. In *Financial Cryptography*, pages 254–274, 1998.

[9] M. Blaze, J. Ioannidis, and A. D. Keromytis. Trust Management and Network Layer Security Protocols. In *Proceedings of the 7th International Workshop on Security Protocols*, pages 103–118, London, UK, 2000. Springer-Verlag.

[10] Y.-H. Chu, J. Feigenbaum, B. LaMacchia, P. Resnick, and M. Strauss. REFEREE: Trust Management for Web Applications. *Computer Networks and ISDN Systems*, 29:953–964, 1997.

[11] F. Cornelli, E. Damiani, S. Paraboschi, and P. Samarati. Choosing Reputable Servents in a P2P Network. In *Eleventh International World Wide Web Conference*, Honolulu, Hawaii, May 2002.

[12] S. Ganeriwal and M. B. Srivastava. Reputation-Based Framework for High Integrity Sensor Networks. In *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks.*, pages 66–77, Washington, DC, USA, 2004.

[13] A. Josang, R. Ismail, and C. Boyd. A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, 2006.

[14] Z. Liang and W. Shi. PET: A Personalized Trust Model with Reputation and Risk Evaluation for P2P Resource Sharing. In *38th Hawaii International Conference on System Sciences*, 2005.

[15] Z. Liu, A. W. Joy, and R. A. Thompson. A Dynamic Trust Model for Mobile Ad-hoc Networks. In *10th IEEE International Workshop on Future Trends of Distributed Computing Systems*, pages 80–85, Suzhou, China, May 2004.

[16] Y. Rebahi, V. E. Mujica-V, and D. Sisalem. A Reputation-Based Trust Mechanism for Ad-hoc Networks. In *10th IEEE Symposium on Computers and Communications (ISCC 2005)*, 2005.

[17] A. Singh and L. Liu. TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems. In *Third International Conference on Peer-to-Peer Computing (P2P'03)*. IEEE, 2003.

[18] N. Stakhanove, S. Basu, J. Wong, and O. Stakhanov. Trust Framework for P2P Networks using Peer-Profile based Anomaly Technique. In *25th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'05)*. IEEE, 2005.

[19] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy. Location-centric Isolation of Misbehavior and Trust Routing in Energy-Constrained Sensor Networks. In *IEEE COnference on Performance, Computing and Communications*, pages 463–469, 2003.

[20] Y. Wang and J. Vassileva. Trust and Reputation Model in Peer-to- Peer Networks. In *Third International Conference on Peer-to-Peer Computing (P2P'03)*, 2003.

[21] Z. Yan, P. Zhang, and T. Virtanen. Trust Evaluation Based Security Solutions in Ad-hoc Networks. In *NordSec 2003, Proceedings of the Seventh Nordic Workshop on Security IT Systems*, 2003.

[22] H. Zhu, F. Bao, and K. Kim. Computing of Trust in Wireless Networks. In *60th IEEE Vehicular Technology Conference*, Los Angeles, California, September 2004.

[23] Z.Yao, D. Kim, I. Lee, K. Kim, and J. Jang. A Security Framework with Trust Management for Sensor Networks. In *Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, pages 190–198, 2005.