Trust classification in wireless sensor networks

Mohammad Momani, Johnson Agbinya, Gina Paola Navarrete and Mahmood Akache
University of Technology, Information Communication Technology Group
1 Broadway, Sydney 2007, Australia
{mmomani, agbinya, gina, makache}@eng.uts.edu.au

Abstract

Wireless sensor network as an emerging technology has received a great attention recently from researchers, due to the need of tiny and cheap nodes to be distributed in high volumes and in difficult environments, such as military zones. However trust as a major role player in building and continue functioning of such networks has received very little attention from research groups, due to the lack of proper definition and classification of trust. In this paper we present a trust classification and introduce a wireless sensor network relationships trust model based on a general trust construct.

1. Introduction

Wireless sensor network (WSN) is an emerging technology and has received an increasing attention due to the advancement in wireless communications in the last few years. The need also of having very tiny and cheap nodes to be deployed in large numbers and in difficult environment such as military zones gave WSN increased focus from researchers.

Trust in WSN plays an important role in constructing the network and making the addition or deletion of sensor nodes from a network very smooth and transparent. Trust in WSN has been studied lightly by current researchers and is still an open and challenging field.

Trust in nodes is based on the fact that the trusted node will not act maliciously in a particular situation [1]. A wireless sensor network however closely resembles a human behaviour model, where a number of nodes just met are able to communicate with each other based on mutual trust levels developed over a period of time.

Most of the definitions of trust in the literature are focussing on what trust is used for in a static fashion and not on the dynamic aspects of trust such as the formation, evolution and propagation of trust [2]. Trust formation in wireless sensor networks is the process of establishing the initial trust of each node. The main sources of trust information about another node are: the node observations of the other node's behaviour, the recommendations from trusted third parties provide the possibility for trust to be propagated between unknown nodes and the reputation of a node in the absence of experience or recommendation.

The presence of some optimistic nodes willing to take risks is required in the case of forming trust with new nodes with no evidence of past behaviour. The level of trust must be modified as additional evidence becomes available and that will change the risk assessment of the node. For successful interactions, the higher the risk, the greater the increase in trust value and vice versa and for unsuccessful interactions, the higher the risk, the lower the penalty and vice versa [2].

In this paper we classify trust in WSN based on the trust model given in [3], we also created a trust typology of the related trust constructs in WSN. The rest of the paper is organised as follows: In section 2, we classify trust in WSN and introduce trust constructs in WSN based on the general trust constructs model. Section 3 provides characteristics of WSN as a self organising network. Section 4 explains the trust typology and introduces the typology of related trust constructs in WSN and finally section 5 concludes the paper.

2. Classification of Trust

Trust in general is categorised by [3] into two categories, a classification system for types of trust and a set of related trust constructs that forms a model. The first category is a sensible method of differentiating one conceptual type from another and the second category is a group of constructs that are conceptually distinguishable, but relate to each other in specified ways. However in this paper we modified the construct model to apply to wireless sensor networks as shown in figure 1.

2.1 Types of Trust

There are three types of trust according to [4], basic, general and situational trust, which we can apply to WSN as follows:

Basic Trust: It is based on the previous experience of the node in all situations. If two sensor nodes (A and B) are to communicate with each other, then the basic trust is not the amount of trust node A has in node B, rather it is the general dispositional trust node A has on other nodes. It has a value in the range [-1, +1] and the higher the value the more trusting is the node.

General Trust: It is the amount of trust node A has in node B, not specific to a particular situation. It also has a value in the range of [-1, +1].

Situational trust in nodes: It represents the amount of trust node A has in node B in a particular situation, and again it has a value in the range between [-1, +1]

2.2 Trust Constructs

The six most important trust constructs of a node in WSN driven from the general trust constructs given in [3] are: Trusting Intention of a node, Trusting Behaviour of a node, Trusting Beliefs in nodes, System Trust in nodes, Dispositional Trust of a node and Situational Decision to Trust a node. Figure 1 shows the relationships between these constructs and a description of these constructs is given below.

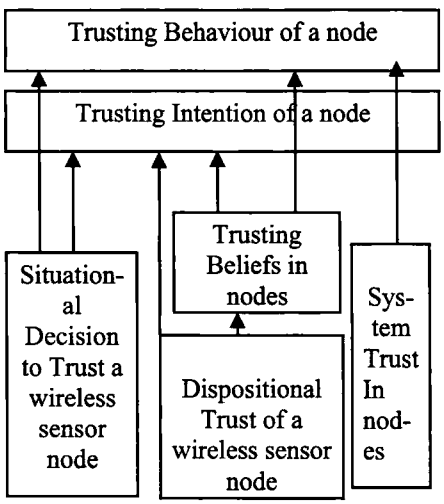

Figure 1. Relationships among Trust Constructs [3]

Trusting intention of a node is the willingness of one node to depend on another node in a specific situation even though the risk is there. This means when node A is willing to depend on node B in a WSN. The trusting intention consists of essential elements such as, experience of reliability, evidence of security, recommendation from another trusted node or entity.

Trusting behaviour of a node is a voluntarily dependence of one node on the other in a specific situation with the existence of risk. It means, when entity A voluntarily depends on entity B in a WSN. Figure 1 shows that trusting intention of a node supports trusting behaviour, which means willingness to be dependent leads one node to actually depend (behaviourally) on the other node.

Trusting beliefs in nodes is the confidence and belief of one node that the other node is trustworthy in a specific situation, that is, when node A believes node B is trustworthy. Therefore trusting beliefs in nodes consist of four categories:

- Benevolence – the node acting in the other node's interests
- Ability of the node to fulfil any promises made. Promises can be expressed for example as a function of the following, quality of services (q), a specific distance (x), data rate (d) and error rate (e).
  $P= f(q,x,d,e)$ (1)
- Competence or the ability of the node to do what is expected or required of it. Competence can be expressed as a function of, power (p), processing speed (s), and memory (m) as follows in equation 2.
  $C=f(p,s,m)$ (2)
- Predictability is the ability to forecast what a node will do in a specific situation.

System trust in nodes is when nodes believe that proper impersonal structures are in place to encourage successful interactions such as monitoring and dealing with improper behaviour. That is when node A trusts impersonally the structure node B is part of. Thus system trust can depend strongly on the network structure and which nodes are part of it.

Dispositional trust of a node is the node's general expectations about the trustworthiness of other nodes across different situations, that is, when node A is naturally inclined to trust (has a general trust in other nodes). It is

normally the risk a node takes initially in trying to trust an unknown node.

Situational decision to trust a node occurs when the node intends to depend on non-specific other node in a given situation. It means that node A trusts a particular situation or scenario. As illustrated in Figure 2, if node B wants to communicate with node A, then it should communicate with a third party trusted management system (TMS), which is also trusted by node A. Therefore the TMS acts as a trust broker for the nodes.

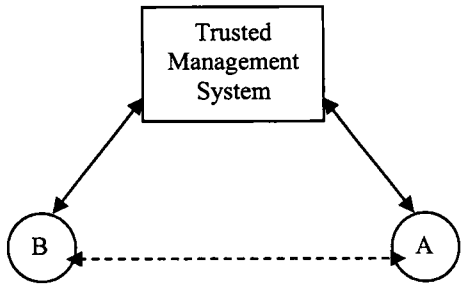

Figure 2. Situational Decision to Trust

Trust as a self organising mechanism in WSN has specific requirements on nodes. These requirements are discussed further.

3. Self-organising characteristics of wireless sensor networks

Wireless sensor networks as a special type of ad-hoc networks are organised on the fly, that is, without any infrastructure. For such self organising networks to be built and work there must be some sort of trust between nodes to communicate and exchange information. Trust in such networks is regarded as a self organising mechanism that has specific requirements on nodes. According to [5, 6], these are:

- Mutual Causality
  Interactions between nodes influence their behaviour and leads to updating their trust value by recommendations exchange and direct observation.
- Autocatalysis
  Nodes exchange references about other nodes affects the trust and the number of interactions between them. Positive evidence reinforces trust, and increases number of interactions and negative evidence decreases trust, and decreases number of interactions.
- Far-from equilibrium condition
  Nodes as part of a highly changing environment need a trust based network to integrate new nodes and update information and trust about leaving nodes to free resources such as power supply, network links and memory.
- Morphogenetic change
  Networks with no infrastructure are always confronted with random conditions affecting the environment and the resources such as broken network links, join/leave nodes, power supply, memory and others.

Based on the above mentioned information regarding trust and from other works in [4, 7], trust can be characterised by the following in wireless sensor networks:

1. Trust is subjective;
   It is based on observations made by a node and evidence made available to the node in a specific situation.
2. Trust is linked with risk;
   Although the benefits of interaction are often worth the risk, the higher the risk the less cooperation is likely to occur.
3. Trust is intransitive;
   Suppose we use <=> to indicate the mutual trust between nodes then if (A <=> B) and (B <=> C) this does not necessarily imply node A trusts node C (A <≠> C). However, this does not rule out the possibility of the transfer of trust information.
4. Trust is self-reinforcing;
   It means above a threshold, trust will not decrease below that threshold and below a threshold, trust will not increase above that threshold [7]. While [7] has advocated this, it is not naturally true because trust is built based on past events and new and positive events will alter this threchold.
5. Trust is dynamic;
   It may decrease or increase by the time based on new evidence or experience [6].

Creating a trust typology from trust constructs is the key issue in building a trust relationship model, which is discussed in the following section.

4. Trust Typology

Due to the broad concept of trust and because of the so many trust definitions in current literature, the key to move the trust research forward is to build a good theoretical and conceptual view of trust specific to a discipline through a typology of trust constructs.
The authors of [5] analysed the existing trust definitions to produce an acceptable typology.

They found two broad groupings of definitions. The first group could be categorized into different conceptual types such as attitudes, beliefs, behaviours and dispositions. This research is not based on this group. The second group could be categorized as reflecting different referents such as trust in something, in someone or in a specific characteristic of someone or something. We are more interested in this group.

From the mapping of the two groups and from the analysis of how trust types relate to each other, the authors of [5] built an interdisciplinary model of trust types as shown below in Figure 3. It is almost the same as the relationships model given in Figure 1 with two changes. First, system trust construct and situational decision to trust constructs are merged into one construct as they are related to each other. Second, trusting behaviour construct was dropped due to endless duplicate that is likely to happen as trusting behaviour depends on trusting intentions. We will use the same model to build our WSN relationships trust model. The two groups of trust definitions seemed relatively exclusive but not overlapping, in that the first refers to what type of construct trust is, while the second refers to the object of trust [5]. We will use this model to create our typology of related constructs in WSN as described in the following section.

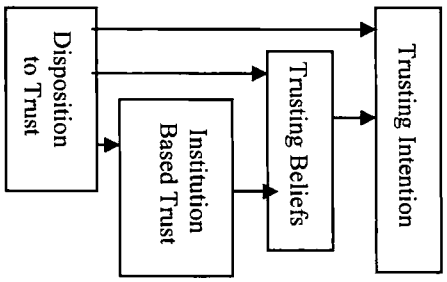

Figure 3. Interdisciplinary Trust Constructs Model [5]

4.1 Typology of related trust constructs in wireless sensor networks

In this section we discuss a topology of related trust in wireless sensor networks which we developed. It is based on the interdisciplinary trust constructs (ITC) model shown in Figure 3. We build our sensor network relationship model and link trust variables to two sensor network trust constructs as illustrated in Figure 4. The trust model in Figure 4 uses six constructs which are, disposition to trust, institution based trust, trusting beliefs, trusting intention, trust-related sensor node behaviour and sensor network interventions. The first four constructs of Figure 4 are identical to those in Figure 3 and were discussed in section 2.2 in this paper.

The main link is from trusting intentions and trusting beliefs to trust-related sensor node behaviours. This construct is defined as behaviours that demonstrate a node is willing to communicate with other nodes in the sensor networks, share resources with them, cooperate with them and exchange information or interact with them. Trust-related sensor node behaviour is not a trust construct, but it is a following consequent of the trust constructs [5]. Trusting beliefs and intentions will influence nodes to actually communicate and share resources with other nodes in the sensor network.

The actual network can also try to influence nodes to collaborate and share resources through the network interventions as shown in Figure 4. These are actions or characteristics the network may take to provide assurance to nodes about the network itself such as reputation building, security policies, quality of services, network reliability and internetworking (links to other networks). The relationship between trust constructs and the sensor network constructs are described bellow.

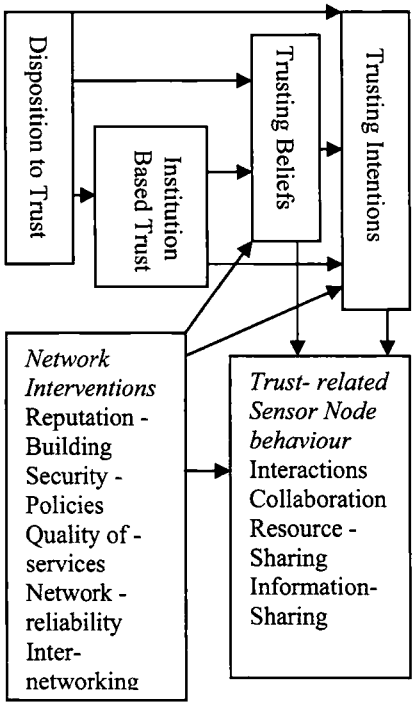

Figure 4. Sensor Network Relationships Trust Model

Reputation is one of the three main sources of trust information about another node or entity

[2] (observation experience, recommendations and reputation). In the absence of experience or recommendation, the reputation of a node or entity can be consulted.

Reputation building - is based on the information about the entity or from the observations experience of its past behaviour. Reputational information is not just based on the opinion of others but it also includes an individual agent's own personal experiences, that is a reputation information is a combination of personal opinions and opinions of others for the same subject [8]. Propagating reputation is a form of social control, where the behaviour of a node in a network is influenced by other nodes acting collaboratively. Improving the network reputation will also improve the trusting beliefs and the trusting intention and will encourage other nodes to join and cooperate and share resources and information.

Network reputation can be improved through security policies, Quality of Service, network reliability and internetworking.

Security policies - good security policies in the sensor network will keep the network available (protected against the denial of service attacks), the integrity of the message is intact, and the confidentiality and privacy protected, which will raise the trusting beliefs in the security of the network and as a consequence increase the willingness to depend on that network.

Quality of services - high quality of service assured by the WSN will provide guarantees on the ability of a network to deliver predictable results and will encourage other nodes to have high trusting intention towards the network and improve their behaviours.

Network Reliability - The trusting beliefs in the network will rise if the network is reliable generating a willingness to depend on that network, that is, persuades nodes to interact with the network and share resources and information.

Internetworking - Links to other reputable sensor networks will broaden the services of the network and will provide assurance of enabling collaboration or other node behaviours.

In summary, each sensor network trust-building intervention tends to influence and produce trust related sensor node behaviours by building trusting beliefs and intentions.

5. Conclusion

This paper has classified trust in WSN based on the general trust constructs. It discusses the self-organising characteristics of trust in WSN and introduces a trust typology of related trust constructs in WSN based on the interdisciplinary trust construct model. This typology will help researchers and developers to build an effective trust relationship model between nodes in such networks and will lead to advancement of research in this area.

References

[1] A. A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad-hoc Networks," presented at ACM International Conference Proceeding Series, Dunedin, New Zealand, 2004.

[2] C. English, P. Nixon, S. Terzis, A. McGettrick, and H. Lowe, "Dynamic Trust Models for Ubiquitous Computing Environments," presented at Ubicomp2002 Security Workshop, 2002.

[3] D. H. McKnight and N. L. Chervany, "The Meanings of Trust," MIS Research Center, Carlson School of Management, University of Minnesota, 1996.

[4] S. Marsh, "Formalising Trust as a Computational Concept," in *Departmet of Computer Science and Mathematics*, vol. PhD: University of Stirling, 1994, pp. 184.

[5] D. H. McKnight and N. L. Chervany, "Conceptualizing Trust: A Typology and E-Commerce Customer Relationships Model," presented at Proceedings of the 34th Hawaii International Conference on System Sciences - 2001, 2001.

[6] G. D. M. Serugendo, "Trust as an Interaction Mechanism for Self-Organising Systems," presented at International Conference on Complex Systems (ICCS'04), 2004.

[7] P. Nixon, W. Wagealla, C. English, and S. Terzis, "Security, Privacy and Trust Issues in Smart Environments," University of Strathclyde, Computer and Information Sciences, Smartlab Technical Report 2004.

[8] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities," presented at Proceedings of the 33rd Hawaii International Conference on System Sciences, 2000.