A New Algorithm of Trust Formation 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

This paper introduces a new algorithm for calculating trust in Wireless Sensor Networks based on the quality of services characteristics expected to be fulfilled by nodes. Figure 3 shows the algorithm being proposed as a flowchart. The flowchart shows the three main sources for computing trust; the previous experience with the nodes, the recommendations from the surrounding nodes and the dispositional trust in nodes (the amount of risk the node is ready to take in the absence of the previous experience and/or the recommendations). Wireless Sensor Networks as an emerging technology has received a great attention from both, researchers and the industry due to the need of tiny and cheap nodes to be distributed in large scales and in difficult environments. The creation, operation, management and survival of Wireless Sensor Networks as a special type of ad hoc network is dependent upon the cooperative and trusting nature of its nodes.

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 has been formalized as a computational model, but the term trust means different things in different research communities, for example it may relate to trust in the underlying technology or to trust between entities when they have to collaborate. End-to-end trust according to [1] includes both types of trust, trust between parties and trust in the underlying infrastructure. 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.

WSN is a special kind of mobile ad hoc networks (MANET) that include sensor nodes with limited computation and communication capabilities deployed by large numbers especially in hostile areas. Addition and deletion of sensor nodes due to the growth of the network or the replacement of failing and unreliable nodes is an aspect of the dynamic characteristic of such networks. This means the design of a secure communication between nodes of a sensor network is even much harder than of a typical ad hoc network and therefore the trust establishment between nodes is a must [2]. However using the traditional tools of doing things such as cryptographic tools to generate trust evidence and establish trust and traditional protocols to exchange and distribute keys is not possible in WSN due to the resource limitations of sensor nodes [2]. Therefore new innovative methods to secure communication and distribution of trust values between nodes are needed.

This paper is focused on trust formation in WSN and is organised as follows. Section 2 presents trust modelling and trust metrics. We present our new trust formation algorithm in section 3 and section 4 concludes the paper.

2. Trust modelling

A trust model can be defined as the representation of the trustworthiness of each node in the opinion of another node, thus each node associates a trust value with every other node [3]. As illustrated in Figure 1, node A might believe that node B will fulfil 40% of the promises made, while node C might believe that node B will fulfil 50% of the promises made.

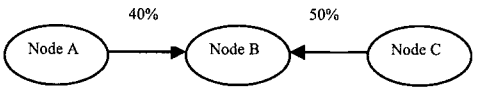


Figure 1. A simple trust map [3]

The calculation of these values is discussed in details in section 3. Trust modelling in WSN hasn't been addressed by anyone yet, however a number of people addressed the issue in MANET. Some of the models we think that are most relevant to our work are presented below.

The trust model presented in [4] is based on the work of Marsh [5], but it uses weight variable instead of utility and importance variables used in Marsh's model [5] for simplicity. The model is simple and operates passively so it has minimal energy and computational requirements as the authors claim. But suffers from the following drawbacks: The model is still under investigation by the authors to determine the precise amount of trust established. It is not taken the previous interactions or the reputations of the entities into account, not even the risk entities are prepared to take in the events of new entities joining the network. Finally the model lapses a mechanism to discover or report malicious nodes. The model might be suitable for small networks with specific mission and predefined protocols but not for networks deployed in a large scale of entities such as WSN without modifying the model to compensate some of its drawbacks.

The trust model proposed in [6] is used to determine and maintain dynamic trust relationships and then make routing decisions. The model is based on the assumptions that every node deployed possesses an Intrusion Detection System (IDS) that can detect and report the behaviour of malicious nodes, and that nodes are stimulated to cooperate adequately on the network. The model assumes that each node is authenticated initially if possible and is assigned a trust value according to its identity but doesn't say how it is authenticated. It also does not say what is going to happen if it is not possible to be authenticated. These assumptions actually limit the module to be used in mission specific small networks. The model seems to be flexible and generic but it uses discrete values similar to Pretty Good Privacy (PGP) model [7], which we think is not sufficient to represent trust that has a continuous trend especially when the node is new to the network.

Trust levels can be represented in different schemes such as continuous values in the range of (-1, +1) or discrete values with labels rather than numbers, such as very low trust, low trust, medium trust, high trust, very high trust and blind trust depends on the environment it is implemented in. According to [4], trust degrees can be represented as simple values, such as trusted and distrusted or as structured values of at least two elements, where the first element represents an action, say access a file, and the second element represents the trust level associated to that action. "Trust levels can also be computed based on the effort that one node is willing to expend for another node. This effort can be in terms of battery consumption, packets forwarded or dropped or any other such parameter that helps to establish a mutual trust level" [8]. Even though someone might think of representing degrees of trust as some probability measurements in the range of (0, 1), the probability values will be meaningless according to [9] unless it is based on well-defined repeatable experiments, which is very difficult to achieve when dealing with dynamic environments such as WSN. The second problem with probability is that it is inherently transitive while trust is not necessarily so.

In his work Marsh, represented trust as a continuous variable over a specific range (-1, +1). We modified the proposed values to reflect our description of trust formation as given in Figure 3. Table 1 shows the new modified trust values.

Table 1: Possible trust values

Value	Label	Description
+1	Blind trust	Based on previous experience.
> .75	Very high trust	Based on experience and recommendation.
.5 to .75	High trust	Based on recommendation.
.25 to .5	Medium trust	Based on recommendation and risk.
0 to .25	Low trust	Dispositional trust (risk)
-.25 to 0	Low distrust	Dispositional trust (risk).
-.5 to -.25	Medium distrust	Based on recommendation and risk
-.75 to -.5	High distrust	Based on recommendation.
< -.75	Very high distrust	Based on experience and recommendation.
-1	Complete distrust	Based on previous experience.

The benefit of using values for trust is that it reflects the continuous nature of trust in WSN and it allows easy implementation and experimentation. The drawback is that the subjectivity is more difficult to understand and the sensitivity may be a problem because small differences in individual values may produce relatively large differences in the overall result.

Establishing trust between nodes in WSN is the most important dynamic aspect of trust. In the following section we propose a new algorithm for trust formation in WSN.

3. Trust Formation Algorithm

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, revocation and propagation of trust [10]. Trust formation in WSN is the process of establishing the initial trust between nodes. There are three main sources of trust calculation in WSN; the node's previous experience with the other node (direct trust), the recommendations from the surroundings nodes (indirect trust) and the dispositional trust (the amount of risk the node is ready to take in the absence of the experience and the recommendation - the case of forming trust with new nodes). Figure 2 shows a general trust computational model used to calculate trust values in WSN.

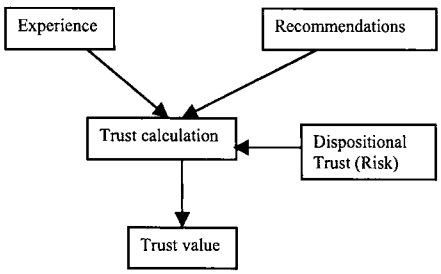


Figure 2. General trust computational model

Trust values regarding other nodes should be maintained locally and updated periodically as new evidence (direct or indirect observation) becomes available. Thus, trust evolves with time as a result of evidence, and allows to adapt the behaviour of entities consequently [11].

The evolution process as another dynamic aspect of trust can be regarded as iterating the process of trust formation as additional evidence becomes available. The level of trust must be modified as additional evidence becomes available and that will change the risk assessment of the node [10].

In order for nodes in a network to receive updates regarding the trusted behaviours of nodes or even threats, a mechanism for trust reporting is necessary. Calculations of trust levels and trust relationship establishment depend on trust reports. This paper is focused on trust formation in WSN, trust evolution and trust reporting are out of the scope of this paper and will be discussed in future work.

The proposed trust formation algorithm is presented in figure 3 as a flowchart. We compute trust in our model based on the QoS characteristics offered by nodes in WSN such as data rate, error rate, distance, power consumption, processing speed and memory. These characteristics are classified in different categories and trust values are assigned to these categories. The assignment of these trust values is based upon the nodes own criteria, circumstances and the situations they are in. Each node will calculate trust for all its surrounding nodes and store these values for later use; these values should be updated in a specific time period based on new interactions.

The illustration of the algorithm given in Figure 3 is as follows. Initially when a node X for example needs to interact with another node Y, the first thing node Y will do is to check, if it had any previous experience with node X. If that's the case then it will check if the amount of trust node Y has on node X (A as shown in equation 1) is enough to do the required interactions (it might require 70% trust value to forward a message for example and 30% trust value to calculate or store something for the node) and if A is enough then they will interact with each other, otherwise node Y will proceed to the next step. If the trust value A is not enough or in case of no previous experience, then node Y will look for any recommendations about node X from the surrounding nodes and if there is, then it will check again to see if the trust value (C given in equation 4) is enough to interact. If C is enough, then they will interact with each other, otherwise node Y will proceed to the following step. If trust value C is not enough or in case of a new node (no experience or recommendations available for node X), then node Y will check the amount of dispositional trust value on node X (E as shown in equation 5). If E is enough, then node X and node Y

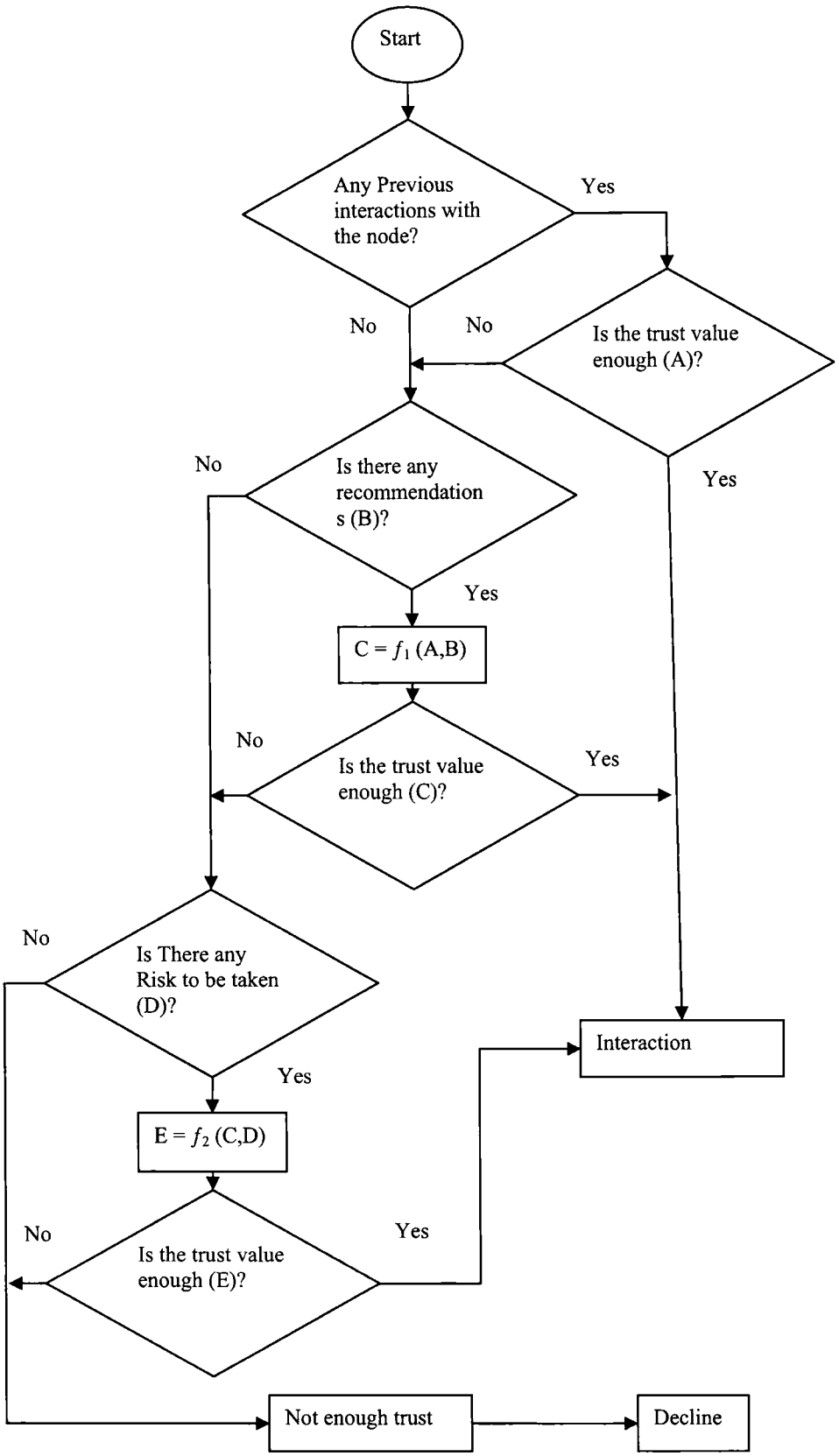


Figure 3. Algorithm for calculating trust in WSN

will interact with each other, otherwise the whole process will be declined. From the above description and by referring to the actual algorithm given in Figure 3, the trust value of node Y in node X - $T_y(x)$ - can be any of the following values (A, B, C, D, E).

$$T_y(x) = \begin{cases} \text{A, if the trust from previous interactions is enough} \\ \text{B, if the trust from recommendations is enough} \\ \text{C, if } f(\text{A,B}) \text{ value is enough} \\ \text{D, if the Dispositional trust is enough} \\ \text{E, if } f(\text{C,D}) \text{ value is enough} \end{cases}$$

Each of these values can be calculated as follows:

$$A = \sum_{i=1}^{n} T_y(i) \qquad (1)$$

Where:
$T_y(i)$ – trust value of the ith trust category.
n – number of trust categories.

$$B = \frac{\sum_{j=1}^{n} T_j(x)}{n} \qquad (2)$$

Where:
$T_j(x)$ – trust value of node J on Node X.
n – number of the surrounding nodes.

$$D = \sum_{k=1}^{n} T_k(x) \qquad (3)$$

Where:
$T_k(x)$ - the risk value of k^{th} trust category.
n – number of trust categories.

$$C = f_1(A,B) \qquad (4)$$

$$E = f_2(C,D) = f_2(f_1(A,B),D) \qquad (5)$$

Functions C in equation (4) and E in equation (5) represent a data fusion and methods of calculating them will be investigated in future work.

4. Conclusion and Future Work

In this paper we presented a new algorithm for trust formation in WSN based on the QoS and experience characteristics offered by nodes. The model is simple, flexible and easy to be implemented. At this stage, the proposed model is being developed and we are in a process of simulating the model to gain further insight. In the future we will extend the model to have new algorithms for the other dynamic aspects of trust (evolution, revocation and propagation).

References

[1] J.-M. Seigneur, S. Farrell, C. D. Jensen, E. Gray, and Y. Chen, "End-to-end Trust Starts with Recognition," presented at The First International Conference on Security in Pervasive Computing, Boppard, Germany, 2003.

[2] L. Eschenauer, "On Trust Establishment in Mobile Ad-Hoc Networks," in *Department of Electrical and Computer Engineering*, vol. Master of Science: University of Maryland, College Park, 2002, pp. 45.

[3] B. N. Shand, "Trust for resource control: Self-enforcing automatic rational contracts between computers," University of Cambridge UCAM-CL-TR-600, 2004.

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

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

[6] Z. Liu, A. W. Joy, and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks," presented at Distributed Computing Systems, 2004. FTDCS 2004. Proceedings, 2004.

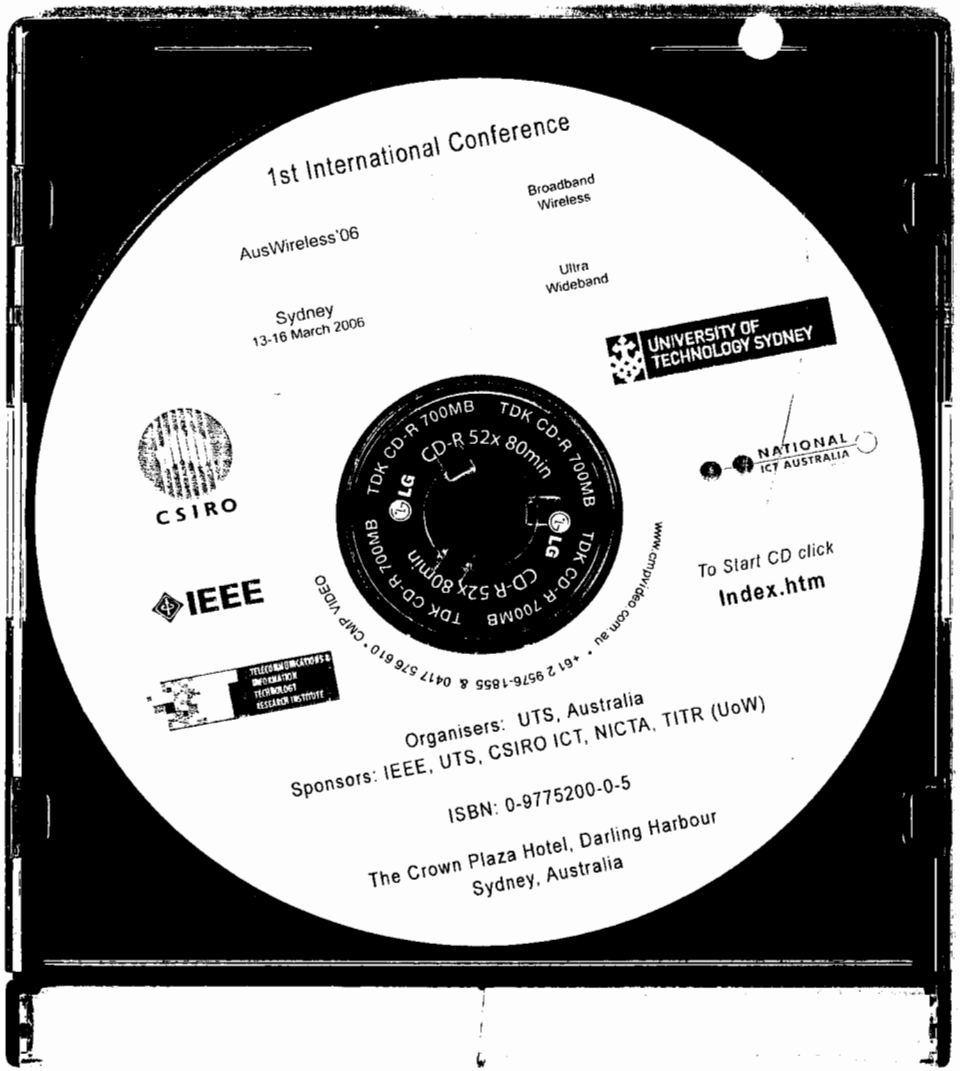
[7] P. Zimmermann, "PGP User's Guide," vol. 2005, 1994, pp. available at http://www.pgpi.org/doc/guide/.

[8] S. Marsh and J. Meech, "Trust in design," in *CHI '00 extended abstracts on Human factors in computing systems*. The Hague, The Netherlands: ACM Press, 2000, pp. 45-46.

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

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

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


1st International Conference
AusWireless'06
Sydney
13-16 March 2006
Broadband
Wireless
Ultra
Wideband
UNIVERSITY OF TECHNOLOGY SYDNEY
CSIRO
NATIONAL ICT AUSTRALIA
IEEE
TDK CD-R 700MB
CD-R 52x 80min
LG
www.cmpvideo.com.au • +61 2 9576-1855 & 0417 576 610 • CMP VIDEO
To Start CD click
Index.htm
Organisers: UTS, Australia
Sponsors: IEEE, UTS, CSIRO ICT, NICTA, TITR (UoW)
ISBN: 0-9775200-0-5
The Crown Plaza Hotel, Darling Harbour
Sydney, Australia