RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks

#Mohammad Momani [1], Khalid Aboura [1], Subhash Challa [2]
[1] *Engineering Department, University of Technology, Sydney*
Sydney 2007, Australia, mmomani@eng.uts.edu.au, kaboura@eng.uts.edu.au
[2] *Engineering Department, University of Melbourne*
VIC, 3010, Australia, Subhash.Challa@nicta.com.au

Abstract

This paper introduces a new trust model and a reputation system for wireless sensor networks based on a sensed continuous data. It establishes the continuous version of the beta reputation system introduced in [1] and applied to binary events and presents a new Gaussian Reputation System for Sensor Networks (GRSSN) . We introduce a theoretically sound Bayesian probabilistic approach for mixing second-hand information from neighbouring nodes with directly observed information.

1. Introduction

Wireless Sensor Network (WSN) has an additional function to the traditional functions of an ad hoc network, which is monitoring events and reporting data. This additional function is the foundation of our new approach to model trust in WSN [2]. While wireless communication is already introduced in almost all aspects of the daily life, WSNs have yet to step beyond the experimental stage. There is a strong interest in the deployment of WSNs in many applications, and the research effort is significant. Due to impressive technological innovations in electronics and communications, small low-cost sensor nodes are available, which can collect and relay environmental data [3]. These nodes have sensing, computing and short range communication abilities and can be deployed in many environments. Such deployment can be in controlled environment such as the sensing of 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 application, from scientific exploration and monitoring, for example the deployment of a wireless sensor network on an Active Volcano [4], to monitoring the microclimate throughout the volume of redwood trees [5], to buildings and bridges monitoring [6], to health care monitoring [7] etc.

In this paper we extend our previous work presented in [2] and we look at applying the Trust notion to WSNs providing data. Most studies of Trust in WSNs focused on the trust associated with the routing and the successful performance of a sensor node in some predetermined task. This resulted in looking at binary events. The trustworthiness and reliability of the nodes of a WSN, when the sensing data is continuous has not been addressed. We look at the issue of security in WSNs using the trust concept, in the case of sensed data that is of continuous nature. We extend an existing trust model for binary events, the Beta Reputation System [1], and introduce a theoretically sound Bayesian probabilistic approach for modelling trust in a wireless sensor network. The rest of the paper is organised as follows: Section 2 presents the notion of trust based on the research work done in the area. We introduce Beta reputation system in section 3. Section 4 introduces the expert opinion theory. Gaussian reputation system is presented in section 5. In section 6 we present some of the simulation results and section 7 concludes the paper.

2. Notion of Trust

Trust has been the focus of researchers for a long time. It started in social sciences where trust between humans was studied. The effect of trust was also analysed in economic transactions [8, 9], and Marsh [10] was one of the first to introduce a computational model for trust in his thesis. Then e-commerce necessitated a notion to judge how trusted an internet seller can be [11, 12]. So did Peer-to-Peer networks and other internet forums where users deal with each other in a decentralized fashion [13, 14]. Recently, attention has been given to the concept of trust to increase security and reliability in Ad Hoc [15, 16] and sensor networks [17, 18]. Although intuitively easy to comprehend, the notion of Trust has not been formally defined unanimously. Unlike *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. Reputation is the opinion of one person about the other, of one internet buyer about an internet seller, and by construct, of one WSN node about another. Trust is a derivation of the reputation of an entity. Based on a reputation, a level of trust is bestowed upon an entity. The reputation itself has been build over time based on that entity's history of behaviour, and may be reflecting a positive or negative assessment. The trust problem is a *decision problem under uncertainty*, and the only coherent way to deal

with uncertainty is through *Probability*. There are several frameworks for reasoning under uncertainty, but it is well accepted that the probabilistic paradigm is the theoretically sound framework for solving decision problems with uncertainty. Some of the trust models introduced for sensor networks employ probabilistic solutions mixed with ad-hoc approaches. None of them produces a full probabilistic answer to the problem.

In this work, we derive a Bayesian probabilistic reputation system and trust model for wireless sensor network. The problem of assessing a reputation based on observed data is a statistical problem. Some trust models make use of this observation and introduce probabilistic modelling such as the trust model RFSN developed by Ganeriwal and Srivastava [17]. The RFSN model presented in [17] uses a Bayesian updating scheme known as the Beta Reputation System [1] for assessing and updating the nodes reputations. The use of the Beta distribution is due to the binary form of the events considered. The observable nodes transactions data is referred to as *first-hand information*. A second source of information in trust modelling is information gathered by other nodes about a node of interest to an entity assessing its reputation. This second source of information is referred to as *second-hand information*. It consists of information gathered by nodes as first-hand information and converted into an assessment of that node. Due to the limitations of a WSN, the second-hand information is summarized before being shared. For example, RFSN uses a probability model in the form of a reputation system to summarize the observed information, and share the values of the parameters of the probability distributions as second-hand information. This shared information is soft data, requiring a proper way to incorporate it with the observed data into the trust model. The step of combining both sources of information is handled differently by different trust models. RFSN uses Dempster-Shafer belief theory. Although a reputation system is designed to reduce the harmful effect of an unreliable or malicious node, such system can be used by a malicious node to harm the network. Systems such as RFSN and DRBTS, a Distributed Reputation and Trust-based Beacon Trust System proposed by Srinivasan, Teitelbaum and Wu [18], are confronted with the issue of what second-hand information is allowed to be shared. For example, some prohibit negative second-hand information to be shared, in order to reduce the risk of a negative campaign by malicious nodes. We propose a full probabilistic way to incorporate all the second-hand information into a reputation system. To resolve the issue of the validity of the information source, the information is modulated using the reputation of the source. This probabilistic modelling answers rigorously the question of how to combine the two types of data in the exercise of assessing reputations in a sensor network. It is based on work done in modelling Expert Opinion in past decades [19-21]. The expert opinion is soft data that is merged with the hard data according to the laws of probability. Opinions provided by knowledgeable sources are known as experts opinions. Such opinions are modulated by existing knowledge about the experts themselves, to provide a calibrated answer.

3. The Beta Reputation System

The Beta Reputation System was proposed by Josang and Ismail [1] as a model to derive reputation ratings in the context of e-commerce. It was presented as a flexible system with foundations in the theory of statistics. Ganeriwal and Srivastava [17] use the work of Josang and Ismail in their trust model for wireless sensor networks. Srinivasan, Teitelbaum and Wu [18] mention the possibility of use of the Beta reputation system. The Beta reputation system is based on the Beta probability density function, *Beta* (α, β) as shown in equation (1)

$$f(p \mid \alpha, \beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \qquad (1)$$

Where $0 \le p \le 1$, $\alpha > 0$, $\beta > 0$ and p is the probability that the event occurs, that is $\theta = 1$. If we observe a number of outcomes where there are r occurrences and s non occurrences of the event, then using a Bayesian probabilistic argument, the probability density function of p can be expressed as a Beta distribution, where $\alpha = r + 1$ and $\beta = s + 1$. This probabilistic mechanism is applied to model the reputation of an entity using events of completion of a task by the assessed entity. The reputation system counts the number r of successful transactions, and s the number of failed transactions, and applies the Beta probability model. This provides for an easily updatable system, since it is easy to update both r and s in the model. Each new transaction results either in r or s being augmented by 1. RFSN uses this probability model in its reputation system. For each node n_j, a reputation R_{ij} can be carried by a neighbouring node n_i. The reputation is embodied in the Beta model and carried by two parameters α_{ij} and β_{ij}. α_{ij} represents the number of successful transactions node n_i had with, or observed about n_j, and β_{ij} the number of unsuccessful transactions. The reputation of node n_j maintained by node n_i is $R_{ij} = Beta\ (\alpha_{ij} + 1, \beta_{ij} + 1)$.

The trust is defined as the expected value of the reputation, $T_{ij} = E(R_{ij})$. Second hand information is presented to node n_i by another neighbouring node n_k. Node n_i receive the reputation of node n_j by node n_k, R_{kj} , in the form of the two parameters α_{kj} and β_{kj}. Using this new information, node n_i combines it with its current assessment R_{ij} to obtain a new reputation

$$R_{ij}^{new} = Beta(\alpha_{ij}^{new}, \beta_{ij}^{new}) \qquad (2)$$

Where node n_i uses its reputation of node n_k in the combination process. The authors of RFSN follow the approach of [1], by mapping the problem into a Dempster-Shaffer belief theory model [22], solving it using the concept of belief discounting, and doing a reverse mapping from

belief theory to continuous probability. We find it unnecessary to use the Belief theory. Rather, the probabilistic theory provides for a way to combine these two types of information.

4. Expert Opinion Theory

The use of expert opinion received much attention in the statistical literature. It allows for the formal incorporation of informed knowledge into a statistical analysis. The probabilistic approach adopted is to consider the opinion given by the expert as data and treat it according to the laws of probability [20]. If θ is a random variable, and μ represents an opinion from an expert that relates to the value of θ, then $P(\theta|\mu)$ obtains, using Bayes theorem.

$$P(\theta \mid \mu) = \frac{P(\mu \mid \theta)P(\theta)}{P(\mu)} \tag{3}$$

Bayes theorem inverses the probability, so that the evidence μ highlights that value of θ that is most likely. The likelihood function $L(\theta) = P(\mu \mid \theta)$ is what allows the expert opinion to be incorporated into the prior knowledge using the coherent laws of probability. The core problem at the heart of the expert opinion solution is the modelling of this likelihood in which, the analyst also introduces a modulation to include his opinion of the expert, leading to a calibrated solution. The analyst may not only have prior knowledge but also some observed data y about the random variable of interest, θ. In such case, Bayes theorem is applied to combine the three sources of information:

$$P(\theta \mid y, \mu) = \frac{P(y \mid \theta, \mu)P(\mu \mid \theta)P(\theta)}{P(y, \mu)} \tag{4}$$

This seemingly simple operation can effectively combine many sources of information. In this work, we use it to model the reputation of a node when opinions about that node are provided by other nodes.

5. GRSSN: The Gaussian Reputation System

Let $\{A_1, A_2, \ldots, A_N\}$ be the nodes of a wireless sensor network. Let the corresponding matrix be $\Gamma = [\Gamma_{i,j}]$, where $\Gamma_{i,j} = \Gamma_{j,i} = 1$ if A_i is connected to A_j, 0 otherwise. X is a field variable of interest which is of a continuous nature. This variable such as temperature, chemical quantity, atmospheric value, is detected and sensed by the nodes of the WSN and is reported only at discrete times t = 0, 1, 2, …, k, the random variable $X_{Ai} = X_i$ is the sensed value by node A_i. i = 1, …, N. $xi(t)$ is the realization of that random variable at time t. Each node A_i, i = 1, …, N has a time series $\{x_i(t)\}$. These time series are most likely different, as nodes are requested to provide a reading at different times, depending on the sources of the request. It could also be that the nodes provide such readings when triggered by some events. We assume that each time a node provides a reading, its one-hop neighbours see that report and can evaluate the reported value. For example if node A_j reports $x_j(t_0)$ at some time t_0, then node A_l obtains a copy of that report, and has its own assessment $x_l(t_0)$ of the sensed variable, say temperature.

Let $y_{i,j}(t) = x_j(t)$-$x_i(t)$. From node A_i's perspective, $X_i(t)$ is known, and $Y_{i,j}(t) = X_j(t) - X_i(t)$ represents the error that node A_j commits in reporting the sensed field value $X_j(t)$ at time t. $Y_{i,j}(t)$ is a random variable modelled as a Normal (Gaussian).

$$Y_{i,j}(t) \sim N(\theta_{i,j}, \tau^2) \tag{5}$$

τ is assumed known, and is the same for all nodes. If we let

$$\overline{y}_{i,j} = \sum_{t=1}^{k} y_{i,j}(t)/k \tag{6}$$

to be the mean of the observed error, as observed by A_i about A_j's reporting, then

$$(\theta_{i,j} \mid y_{i,j}) \sim N(\overline{y}_{i,j}, \tau^2/k) \tag{7}$$

Where $y_{i,j} = \{(y_{i,j}(t)\,;$ for all t values at which a report is issued by $A_j\}$. This is a well known straightforward Bayesian updating where a diffuse prior is used. We let $\mu_{i,j} = \overline{y}_{i,j}$ and $\sigma^2_{i,j} = \tau^2/k$. Recall that k is nodes dependent. It is the number of reports issued by node j, and differs from node to node. We define the reputation as being

$$R_{i,j} = N(\mu_{i,j}, \sigma^2_{i,j}) \tag{8}$$

where $\mu_{i,j} = \overline{y}_{i,j}$ and $\sigma^2_{i,j} = \tau^2/k$ are the equivalent of α_{ij} and β_{ij} in RFSN.

Trust is defined differently, since we want it to remain between 0 and 1. In this case, we define the trust to be the probability as shown in equation (9).

$$T_{i,j} = \text{Prob}\{|\theta_{i,j}| < \varepsilon\} \tag{9}$$

$$T_{i,j} = \text{Prob}\{-\varepsilon < \theta_{i,j} < +\varepsilon\} = \phi\left(\frac{\varepsilon - \overline{y}_{i,j}}{\tau/\sqrt{k}}\right) - \phi\left(\frac{-\varepsilon - \overline{y}_{i,j}}{\tau/\sqrt{k}}\right) \tag{10}$$

The bigger the error θ_{ij} is, meaning its mean shifting to the right or left of 0, and the more spread that error is, the less the trust value is. Each node A_i maintains a line of reputation assessments composed of $T_{i,j}$ for each j, such that $\Gamma_{i,j} \neq 0$ (one-hop connection). $T_{i,j}$ is updated for each time period t for which data is received for some connecting node j.

In addition to data observed in form of $y_{i,j} = \{(y_{i,j}(t)$ for all t values at which a report is issued by $A_j\}$, node A_i uses second hand information in the form of $(\mu_{l_s,j}, \sigma_{l_s,j})$, s = 1, …, m from the m nodes connected to A_j. This is an "expert opinion", that is soft information from external sources. Each of these m nodes has observed node A_j's reports and produced assessments of its error in the form of $(\mu_{l_s,j}, \sigma_{l_s,j})$, s = 1, …, m and consequently $T_{ls,j}$, s = 1, …, m. In using expert opinion/external soft information, one needs to modulate it.

Node A_i uses its own assessment of the nodes $A_{l_1},...,A_{l_m}$, in the form of $(\mu_{i,l_s},\sigma_{i,l_s})$, $s = 1, \dots, m$ and consequently $T_{i,ls}$, $s = 1, \dots, m$. Using Bayes theorem, the probability distribution of $\theta_{i,j}$ is obtained, that uses the observed data along with the second hand, modulated information.

$$P(\theta_{i,j} \mid y_{i,j},(\mu_{l_1,j},\sigma_{l_1,j}),...,(\mu_{l_m,j},\sigma_{l_m,j}),$$
$$(\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})) \quad (11)$$

is proportional to the product of three terms:

$$P(y_{i,j} \mid \theta_{i,j},(\mu_{l_1,j},\sigma_{l_1,j}),...,(\mu_{l_m,j},\sigma_{l_m,j}),$$
$$(\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})) \quad (12)$$

$$P((\mu_{l_1,j},\sigma_{l_1,j}),...,(\mu_{l_m,j},\sigma_{l_m,j}) \mid \theta_{i,j},$$
$$(\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})) \quad (13)$$

and

$$P(\theta_{i,j} \mid (\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})) \quad (14)$$

The first term (equation 12) reduces to $P(y_{i,j} \mid \theta_{i,j})$ through conditional independence, and is equal to the product of the likelihoods

$$\prod_{t=1}^{k} N(\theta_{i,j},\tau^2) \quad (15)$$

The third term (equation 14), due to the conditional independence of $\theta_{i,j}$ from $(\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})$, further reduces to $P(\theta_{i,j})$. It is the prior distribution of $\theta_{i,j}$ which we model as a diffuse prior $N(0,\infty)$. The second term (equation 13) models the use of the second hand information. This term requires some elaboration:

$$P((\mu_{l_1,j},\sigma_{l_1,j}),...,(\mu_{l_m,j},\sigma_{l_m,j}) \mid \theta_{i,j},$$
$$,(\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})) \quad (16)$$

can be reduced to the product

$$\prod_{s=1}^{m} P((\mu_{l_s,j},\sigma_{l_s,j}) \mid \theta_{i,j},(\mu_{i,l_s},\sigma_{i,l_s})) \quad (17)$$

through conditional independence arguments. To derive

$$P((\mu_{l_s,j},\sigma_{l_s,j}) \mid \theta_{i,j},(\mu_{i,l_s},\sigma_{i,l_s})) \quad (18)$$

for each $s = 1, \dots, m$, we observe the following:
for some t's,

$$\theta_{i,j} = x_j(t) - x_i(t) \quad (19)$$

$$\theta_{l,j} = x_j(t) - x_l(t) \quad (20)$$

if all t's were the same, then

$$\theta_{i,j} = x_j(t) - x_i(t) = (x_j - x_l) + (x_l - x_i) =$$
$$= \theta_{l,j} + \theta_{i,l} \quad (21)$$

But not all t's are the same, so all data is not used at the same times. But we inspire ourselves from this relationship to model the expert opinion likelihood. As a model, we assume that

$$\theta_{l,j} \simeq \theta_{i,j} - \theta_{i,l} \quad (22)$$

$$\mu_{l,j} \simeq \theta_{i,j} - \mu_{i,l} \quad (23)$$

and we model

$$\mu_{l,j} \sim N(\theta_{i,j} - \mu_{i,l}, var) \quad (24)$$

where we choose *var* to be inversely related to node A_i assessment of the reputation of node A_l. That is

$$var = \left(\frac{1}{T_{i,l}} - 1\right)\alpha \quad (25)$$

where α is a model parameter.

$$\mu_{l,j} \sim N(\theta_{i,j} - \mu_{i,l}, \left(\frac{1}{T_{i,l}} - 1\right)\alpha) \quad (26)$$

leads to

$$\prod_{s=1}^{m} P((\mu_{l_s,j},\sigma_{l_s,j}) \mid \theta_{i,j},(\mu_{i,l_s},\sigma_{i,l_s})) =$$
$$= \prod_{s=1}^{m} N(\theta_{i,j} - \mu_{i,l_s}, \left(\frac{1}{T_{i,l_s}} - 1\right)\alpha) \quad (27)$$

and consequently

$$P(\theta_{i,j} \mid y_{i,j},(\mu_{l_1,j},\sigma_{l_1,j}),...,$$
$$(\mu_{l_m,j},\sigma_{l_m,j}),(\mu_{i,l_1},\sigma_{i,l_1}),...,(\mu_{i,l_m},\sigma_{i,l_m})) \quad (28)$$

is a Normal (Gaussian) distribution with mean and variance

$$\mu_{i,j}^{new} = \frac{\sum_{s=1}^{m} \frac{(\mu_{l_s,j} + \mu_{i,l_s})}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k\bar{y}/\tau^2)}{\sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k/\tau^2)} \quad (29)$$

$$\sigma_{i,j}^{2\ new} = \frac{1}{\sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k/\tau^2)} \quad (30)$$

These values $(\mu_{i,j}^{new},\sigma_{i,j}^{2\ new})$ along with $(\mu_{i,j},\sigma_{i,j}^2)$ are easily updatable values that represents the continuous Gaussian version of the $(\alpha_{i,j},\beta_{i,j})$ and $(\alpha_{i,j}^{new},\beta_{i,j}^{new})$ of the binary approach in [17], as derived from the approach in [1]. The network topology and protocols follow those of [17, 18]. The solution presented is simple, and easily computable. This is with keeping in mind that the solution applies to networks with limited computational power. Some would object to the use of a diffuse prior, which in effect, forces a null prior trust

value, regardless of the ε value. A way to remedy to this is to start with a $N(\mu_0, \sigma_0^2)$ prior distribution for all θ_{ij}, such that the prior trust is 1/2. This choice not only answers the diffuse prior issue, but also allows the choice of the parameters involved. ε can be determined, given μ_0 and σ_0. μ_0 is most likely to be set to 0. Therefore, σ_0 and ε determine each other. With a proper prior

$$\theta_{i,j} \sim N(\mu_0, \sigma_0^2) \tag{31}$$

the reputation parameters are:

$$\mu_{i,j} = \frac{(\mu_0 / \sigma_0^2) + (k\overline{y}_{i,j} / \tau^2)}{(1/\sigma_0^2) + (k/\tau^2)} \tag{32}$$

$$\sigma_{i,j}^2 = \frac{1}{(1/\sigma_0^2) + (k/\tau^2)} \tag{33}$$

and

$$\mu_{i,j}^{new} = \frac{(\mu_0 / \sigma_0^2) + \sum_{s=1}^{m} \frac{(\mu_{l_s,j} + \mu_{i,l_s})}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k\overline{y}_{i,j} / \tau^2)}{(1/\sigma_0^2) + \sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k/\tau^2)} \tag{34}$$

$$\sigma_{i,j}^{2\ new} = \frac{1}{(1/\sigma_0^2) + \sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k/\tau^2)} \tag{35}$$

6. Simulation and Results

In a simulated experiment, we calculate the trust between 4 nodes (1,6,7,13) in a sub-network of 15 nodes as shown in Figure 1.

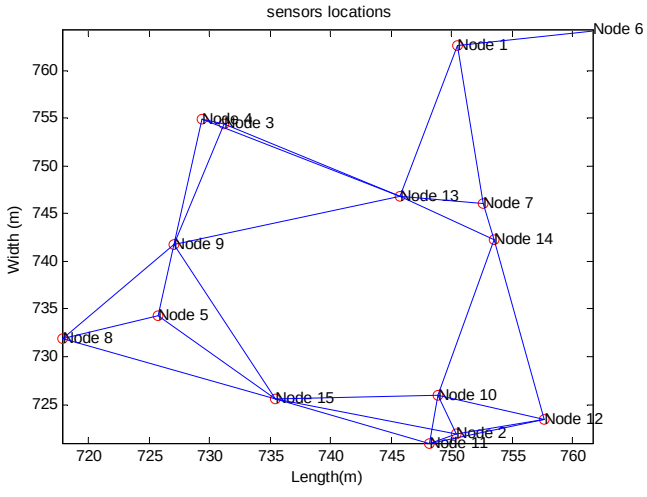

Fig. 1: Wireless Sensor Network Diagram

First, we assume that all nodes are working properly and report the sensed event with only a small reading error. Simulation showed that the trust values of node 1 for the other nodes (6,7,13) are slightly different but converge to 1 as can be seen in Figure 2.

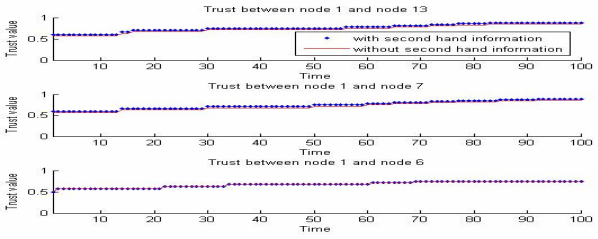

Fig. 2: All nodes are normal

In other experiments, we assume that nodes 7 and 13 are faulty. The results of the simulation are presented in Figure 3 and show the trust value for nodes 7 and 13 dropping to zero. Node 6 is assumed reliable, and its corresponding trust value follows a growing path that eventually reaches 1.

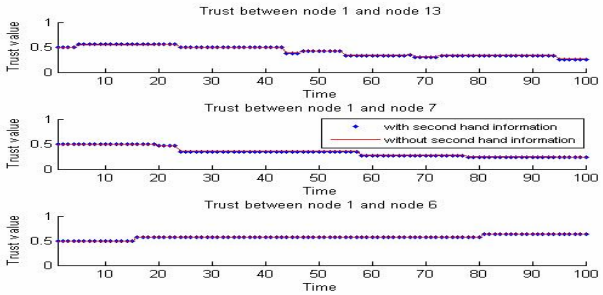

Fig. 3: Node7 and node 13 are faulty

As can be seen from Figure 4, the trust value from the direct information reaches zero for both nodes 7 and 13. This is because node 1 is faulty, and contradicts nodes 7 and 13 based only on direct information. However, using second information, the trust for these two nodes is high. This is an interesting case as both nodes (13,7) are assessing node 1 as a faulty node. The trust value for node 6 is set to the initial value of (0.5) and will decrease to zero as there is no second hand information available about node 6.

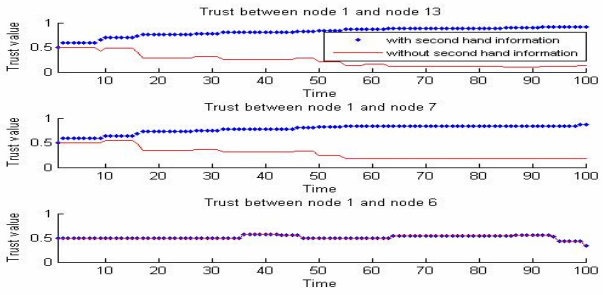

Fig. 4: Node 1 is a malicious node

In the last example shown in Figure 4, we do know that node 1 is faulty, since it is a simulation exercise. The results clearly should indicate to the network that node 1 is faulty. However, it could also be the case that nodes 7 and 13 are malicious. The trust system works on the assumption that a majority of

nodes in a neighbourhood are reliable. This principle helps purge the system of bad elements. In our case, at this point in time, we observe that the trust system we developed is effective in distinguishing among nodes.

7. Conclusion and Future Work

In this paper we introduced a new Gaussian Reputation System for Sensor Networks (GRSSN). We introduced a theoretically sound Bayesian probabilistic approach for calculating trust and reputation systems in WSN. In future research, we will address the issue of how to decide on the deleting or keeping of WSN nodes using Bayesian Networks.

ACKNOWLEDGEMENT

We acknowledge funding for this research through a postgraduate scholarship from the University of Technology, Sydney and partial funding from Thales Australia through the ARC Linkage Grant LP0561200.

References

[1] A. Jøsang and R. Ismail, "The Beta Reputation System," in *15th Bled Electronic Commerce Conference*. Bled, Slovenia, 2002.

[2] M. Momani, S. Challa, and K. Aboura, "Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective," presented at International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CIS2E 06) University of Bridgeport, USA, 2006.

[3] I. F. Akyildiz, Y. S. W. Su, and E. Cayirci, " Wireless sensor networks: a survey," *Computer Networks*, vol. 38, pp. 393-422, 2002.

[4] G.Werner-Allen, K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, and M. W. . "Deploying a wireless sensornetwork on an active volcano," *IEEE Internet Computing*, 2005.

[5] D. Culler, D. Estrin, and M. Srivastava, "Overview of sensor networks. Special Issue in Sensor Networks,," *IEEE Computer*, vol. 37, pp. 41-49, 2004.

[6] S. D. Glaser, "Some real-world applications of wireless sensor nodes," presented at Proceedings of the SPIE Symposium on Smart Structures and Materials NDE, San Diego, CA, USA, 2004.

[7] T. Gao, D. Greenspan, M. Welsh, R. R. Juang, and A. Alm., "Vital signs monitoring and patient tracking over a wireless network.," presented at Proceedings of the 27th IEEE EMBS Annual International Conference, 2005.

[8] S. Ba and P. A. Pavlou, "Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior," *MIS Quarterly*, vol. 26, 2002.

[9] P. Dasgupta, "Trust as a commodity," in *n Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations*, vol. electronic edition, D. Ingram, Ed.: Department of Sociology, University of Oxford,, 2000, pp. 49-72.

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

[11] 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.

[12] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: empirical analysis of eBays reputation system," presented at NBER: workshop on empirical studies of electronic commerce, 2000.

[13] K. a. D. Aberer, Z. , "Managing trust in a peer-2-peer information system," presented at Ninth Int. Conf. Information and Knowledge Management, 2001, 2001.

[14] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer e-commerce communities," presented at IEEE conference on E-commerce, 2003.

[15] S. Buchegger and J. L. Boudec, "Performance analysis of the CONFIDANT protocol," presented at 3rd ACM int. symp. Mobile ad hoc networking & computing, 2002.

[16] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks," 2001.

[17] S. Ganeriwal and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," presented at the 2nd ACM workshop on Security of ad hoc and sensor networks Washington DC, USA 2004.

[18] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed Reputation-based Beacon Trust System," in *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06)*, 2006.

[19] P. A. Morris, "Bayesian expert resolution," in *Department of Engineering-Economic Systems*, vol. Ph.D: Stanford University, 1971.

[20] D. V. Lindley and N. D. Singpurwalla, "Reliability (and fault tree) analysis using expert opinions. ," *Journal of the American Statistical Association*, vol. 81, pp. 87-90, 1986.

[21] M. West, "Bayesian aggregation," *Journal of Royal Staistical Society Series A*, vol. 147, pp. 600-607, 1984.

[22] G. Shafer, "A mathematical theory of evidence," *Princeton University*, 1976.