GTRSSN: Gaussian Trust and Reputation System for Sensor Networks

Mohammad Momani[1], Subhash Challa[2]
[1]*Engineering Department, University of Technology Sydney, Australia*
[2] *NICTA, VRL, University of Melbourne, Australia*
mmomani@eng.uts.edu.au , Subhash.Challa@nicta.com.au

***Abstract*- This paper introduces a new Gaussian trust and reputation system for wireless sensor networks based on sensed continuous events to address security issues and to deal with malicious and unreliable nodes. It is representing a new approach of calculating trust between sensor nodes based on their sensed data and the reported data from surrounding nodes. It is addressing the trust issue from a continuous sensed data which is different from all other approaches which address the issue from communications and binary point of view.**

I. INTRODUCTION

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 as presented in [1, 2], and Marsh in [3] was one of the first to introduce a computational model for trust. Then e-commerce necessitated a notion to judge how trusted an internet seller can be as in [4, 5]. So did Peer-to-Peer networks and other internet forums where users deal with each other in a decentralized fashion as in [6, 7]. Recently, attention has been given to the concept of trust to increase security and reliability in Ad Hoc as in [8, 9] and sensor networks as in [10, 11]. 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 wireless sensor network (WSN) node about another node in the same network.

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 paper we extend our previous work presented in [12, 13] 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. The rest of the paper is organised as follows: Section 2 presents the related work, which covers only the very specific related work which we extended before. Section 3 introduces the Beta reputation system. We introduce our new model in section 4. In section 5 we present some of the simulation results and section 6 concludes the paper.

II. BACKGROUND

In this paper, we derive a Bayesian probabilistic reputation system and trust model for wireless sensor network. We argue that 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 in [10]. The RFSN model presented in [10] uses a Bayesian updating scheme known as the Beta Reputation System introduced in [14] 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. “Reference [10] uses Dumpster-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 in [10] and [11] 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.

III. Related Work

The Beta Reputation System was proposed by Josang and Is mail in [14] 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 in [10] use the work of Josang and Ismail in their trust model for wireless sensor networks. Srinivasan, Teitelbaum and Wu in [11] 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).

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

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. "Reference [10] 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} as in equation (2).

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

Where node n_i uses its reputation of node n_k in the combination process. The authors of [10] follow the approach of [14], by mapping the problem into a Dempster-Shaffer belief theory model [15], 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.

IV. GTRSSN Trust Model

Trust modelling represents the trustworthiness of each node in the opinion of another node, thus each node associates a trust value with every other node as in [16], and based on that trust value a risk value required from the node to finish a job can be calculated. As illustrated in Fig. 1, node X might believe that node Y will fulfil 40% of the promises made, while node Z might believe that node Y will fulfil 50% of the promises made.

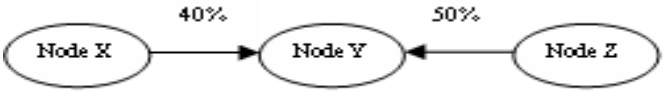

Fig.1: A simple trust map [16]

In other words trust modelling is simply the mathematical representation of a node's opinion in another node in a network. In our model we are calculating trust based on the continuous sensed data (temperature) as opposed to all previous related works which are calculating trust based on binary events.

Let $\{A_1, A_2, \ldots, A_N\}$ be the nodes of a wireless sensor network. Let the corresponding matrix (Γ) be as shown in equation (3).

$$\Gamma = [\Gamma_{i,j}] = \begin{pmatrix} 1 & . & . & . \\ . & 1 & . & . \\ . & . & 1 & . \\ . & . & . & 1 \end{pmatrix} \quad (3)$$

If node A_i is connected to node A_j then $\Gamma_{i,j} = \Gamma_{j,i} = 1$ otherwise it is equal to 0. 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) shown in equation (4).

$$Y_{i,j}(t) \sim N(\theta_{i,j}, \tau^2) \qquad (4)$$

τ is assumed known, and is the same for all nodes. If we let $\overline{y}_{i,j}$ to be the mean of the observed error, as observed by A_i about A_j's reporting as in equation (5),

$$\overline{y}_{i,j} = \sum_{t=1}^{k} y_{i,j}(t) / k \qquad (5)$$

then

$$(\theta_{i,j} \mid y_{i,j}) \sim N(\overline{y}_{i,j}, \tau^2 / k) \qquad (6)$$

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 $R_{i,j}$ as in equation (7)

$$R_{i,j} = N(\mu_{i,j}, \sigma^2_{i,j}) \qquad (7)$$

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} as in [10].

Trust is defined differently, since we want it to remain between 0 and 1, we define the trust to be the probability as shown in equations (8) and (9).

$$T_{i,j} = \text{Prob}\{|\theta_{i,j}| < \varepsilon\} \qquad (8)$$

$$T_{i,j} = \text{Prob}\{-\varepsilon < \theta_{i,j} < +\varepsilon\} = \phi\left(\frac{\varepsilon - \overline{y}_{i,j}}{\tau / \sqrt{k}}\right) - \phi\left(\frac{-\varepsilon - \overline{y}_{i,j}}{\tau / \sqrt{k}}\right) \qquad (9)$$

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, … , m and consequently $T_{i,ls}$, s = 1, …, 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 as shown in equation (10).

$$P(\theta_{i,j} \mid y_{i,j}, (\mu_{l_1,j}, \sigma_{l_1,j}), ..., (\mu_{l_m,j}, \sigma_{l_m,j}), (\mu_{i,l_1}, \sigma_{i,l_1}), ..., (\mu_{i,l_m}, \sigma_{i,l_m})) \qquad (10)$$

Equation (10) is proportional to the product of three terms, which represents the likelihood, the prior distribution and the second hand information. By elaborating the second hand information we proved that it is a Normal (Gaussian) distribution with mean and variance as shown in equations (11) and (12) consequently.

$$\mu_{i,j}^{new} = \frac{\sum_{s=1}^{m} \frac{(\mu_{l_s,j} + \mu_{i,l_s})}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k\overline{y} / \tau^2)}{\sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k / \tau^2)} \qquad (11)$$

$$\sigma_{i,j}^{2\ new} = \frac{1}{\sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k / \tau^2)} \qquad (12)$$

These values $(\mu_{i,j}^{new}, \sigma_{i,j}^{2\ new})$ along with $(\mu_{i,j}, \sigma^2_{i,j})$ 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 [10], as derived from the approach in [14]. The network topology and protocols follow those of [10, 11]. 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 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 $\theta_{i,j}$ as shown in equation (13),

$$\theta_{i,j} \sim N(\mu_0, \sigma_0^2) \tag{13}$$

the reputation parameters $\mu_{i,j}$ and $\sigma_{i,j}^2$ are presented in equations (14) and (15) consequently.

$$\mu_{i,j} = \frac{(\mu_0 / \sigma_0^2) + (k\overline{y}_{i,j} / \tau^2)}{(1/\sigma_0^2) + (k/\tau^2)} \tag{14}$$

$$\sigma_{i,j}^2 = \frac{1}{(1/\sigma_0^2) + (k/\tau^2)} \tag{15}$$

and the updated values are presented in equations (16) and (17).

$$\mu_{i,j}^{new} = \frac{(\mu_0 / \sigma_0^2) + \sum_{s=1}^{m} \frac{(\mu_{l_s,j} + \mu_{i,l_s})}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k\overline{y}_{i,j} / \tau^2)}{(1/\sigma_0^2) + \sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k/\tau^2)} \tag{16}$$

$$\sigma_{i,j}^{2\ new} = \frac{1}{(1/\sigma_0^2) + \sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k/\tau^2)} \tag{17}$$

V. Simulation Results

To verify our theory we developed several simulation experiments and we present in this section the results from 2 different scenarios conducted on the network shown in Figure 2. In both simulation experiments, we calculate the trust between 4 nodes (1, 6, 7 and 13) in a sub-network of 15 nodes as shown in Figure 2. In the first scenario we assumed that only a random region is selected to report data on every time series and the result is represented first in Figures 3, 4 and 5, while in the second scenario we assumed that the entire network is reporting for every time series and the result is represented in the second figure of Figures 3, 4 and 5.

First, we assume that all nodes are working properly and report the sensed event with only a small reading error. Simulation results show that the trust values of node 1 for the other nodes (6, 7 and 13) are slightly different but converge to 1 as can be seen in Figure 3. The results presented in Figures 3, 4 and 5 show that the second scenario is giving more precise results as the trust is updated for all nodes at each time series.

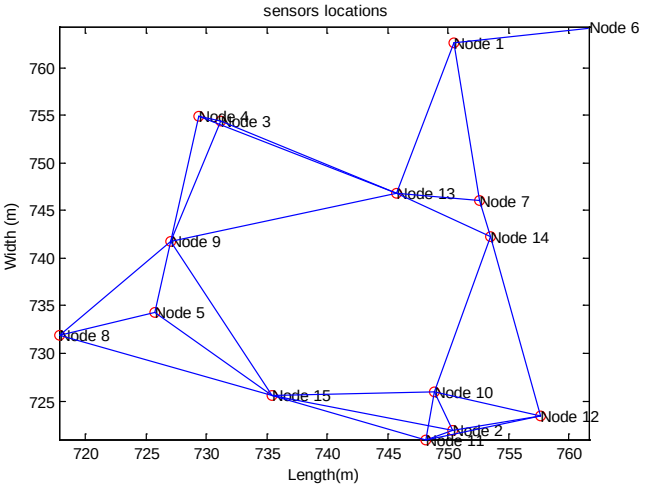

Fig. 2: Wireless Sensor Network Diagram

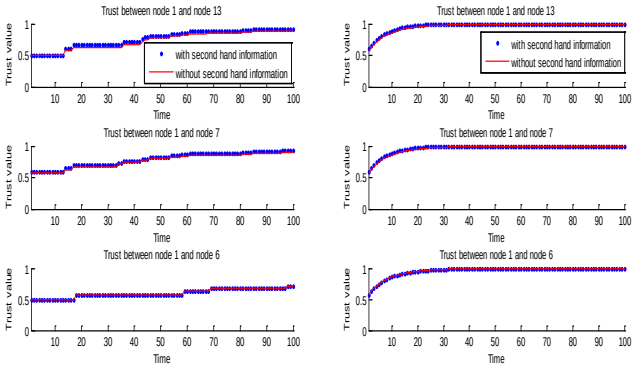

Fig. 3: All nodes are normal

In other experiments, we assume that nodes 7 and 13 are faulty or malicious nodes, the results from the simulation are presented in Figure 4 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.

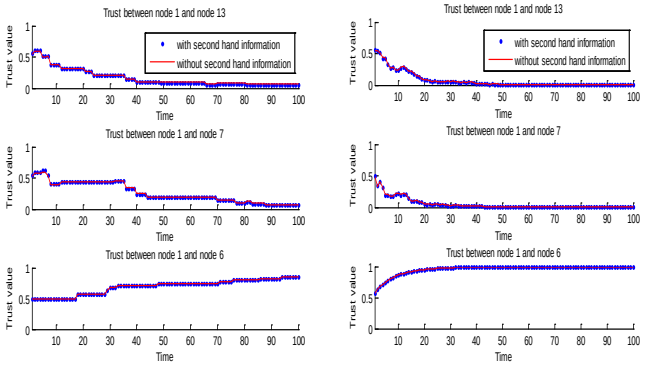

Fig. 4: Node7 and node 13 are faulty

Figure 5 shows 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.

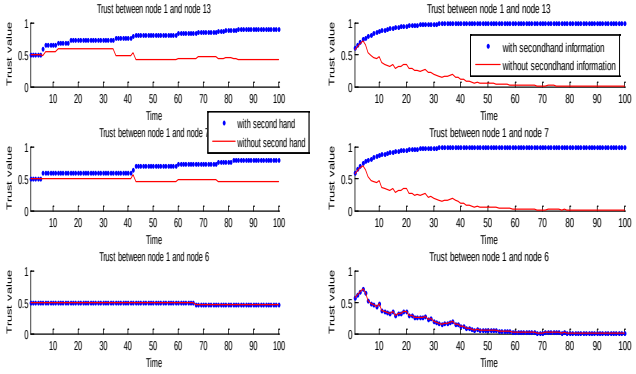

Fig. 5: Node 1 is a malicious node

In the last example shown in Figure 5, 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.

VI. Conclusion And Future Work

In this paper we introduced a new Gaussian Trust and Reputation System for Sensor Networks (GTRSSN). We introduced a theoretically sound Bayesian probabilistic approach for calculating trust and reputation systems in WSN. We also presented simulation experiment results conducted on different scenarios. In future research, we will try to map the trust network model to a Bayesian network model to address the issue of how to decide on the deleting or keeping nodes in wireless sensor networks.

Acknowledgement

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

References

[1] 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.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

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

[10] 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.

[11] 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.

[12] M. Momani, S. Challa, and K. Aboura, "Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective," in *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*, T. Sobh, K. Elleithy, A. Mahmood, and M. Karim, Eds.: Springer Netherlands, 2007.

[13] M. Momani, K. Aboura, and S. Challa, "RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks," presented at The Third International Conference on Intelegent Sensors, Sensor Networks and Information Processing, Melbourne, Australia, 2007.

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

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

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