Can we Trust Trusted Nodes in Wireless Sensor Networks?

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

Abstract

In this paper we extend our previously designed trust model in wireless sensor networks to include both; communication trust and data trust. Trust management in wireless sensor networks is predominantly based on routing messages; whether the communication has happened or not (successful and unsuccessful transactions). The uniqueness of sensing data in wireless sensor networks introduces new challenges in calculating trust between nodes (data trust). If the overall trust is based on just the communication trust, it might mislead the network, that is; untrustworthy nodes in terms of sensed data can be classified as trusted nodes due to their communication capabilities. Hence we need to develop new trust models to address the issue of the actual sensed data. Here we are comparing the two trust models and proving that one model by itself is not enough to decide on the trustworthiness of a node, so new techniques are required to combine both data trust and communication trust.

I. INTORUCTION

Trust as an essential attribute in building a relationship between entities has been studied for long time by scientists from almost all different sciences. Every field is looking at modelling and calculating trust using different techniques and one of the most prominent and promising techniques is the use of statistics; mainly probabilities to solve the problem especially in dynamic networks, where the topology is changing very rapidly.

Even though researchers started to look into the issue of trust in wireless sensor networks, they still follow almost the same approaches used by researchers from other fields. In this paper we are trying to prove that approaching the problem from one angle is not enough to decide on whether or not to trust a specific node in a wireless sensor network (WSN); as not only routing or communication is involved like in the other types of networks, but also a sensed data, which is a unique characteristic to sensor networks. So new techniques are required to examine the actual sensed data; That is, more than one criteria should be merged together to produce a combined trust in WSN. The rest of the paper is organised as follows: Section 2 presents trust in WSN. We introduce the communication trust in WSN in section 3. Section 4 introduces the data trust in WSN. Simulation results are presented in section 5 and section 6 concludes the paper.

II. TRUST IN WIRELESS SENSOR NETWORKS

Building a trust in any entity in general depends on the direct (observation, first hand information) and the indirect (recommendations, second hand information) interactions between entities. The uniqueness of WSN from other networks in sensing events introduces new extra challenges to be dealt with in addition to the existing ones in the ad hoc or peer to peer networks. Prior to our introduction of data (continuous) trust as proposed in [1, 2], most of trust models in literature such as [3-8] were dealing with trust from a communication (binary) point of view; that is; successful and unsuccessful transactions, ratings and/or routings between nodes. In this paper we will simulate and compare our work presented in [1, 2] with the work presented in [3], and we will prove that looking at the trust in WSN from a communication point of view might not be enough to decide on whether or not to trust a specific node in a network.

Let us consider the following scenario, which will differentiate between the communication trust and the data trust as mentioned before. Suppose we have the following WSN consists of three nodes (1,2, 3) and a fusion centre (FC) as shown in Figure 1, nodes are deployed to monitor an event and report the sensed data to the (FC). Nodes can communicate (send and receive information (routing)) even if some of them are adversary, but for some reason they don't report their sensed data and vice versa, they can report their data but not routing messages from other nodes.

For example, node 3 in Figure 1, is forwarding all messages from node 1 and node 2 to the (FC), which means it is very trustful in terms of communication, but for some reason it is not reporting it is actual data to other nodes in the network (node 3 for ex. is an adversary node and there is an intruder personnel from the same group entering and leaving the battle field). And the same thing is valid when all three nodes are sending their sensed data (temperature for ex.) but because the communication is very expensive in such networks, node 3 is not routing messages from nodes 1 and 2, and that way node 3 is trusted from the data point of view but not from the communication point of view. So a mechanism to discover that situation and report it to the other nodes and/or to the (FC) is needed.

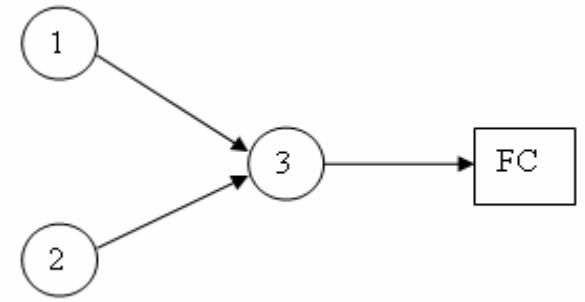

Figure 1: Wireless sensor network scenario

Based on the above illustration, we will extend our trust computational model for WSN presented in [9, 10] to reflect the new changes as shown in Figure 2.

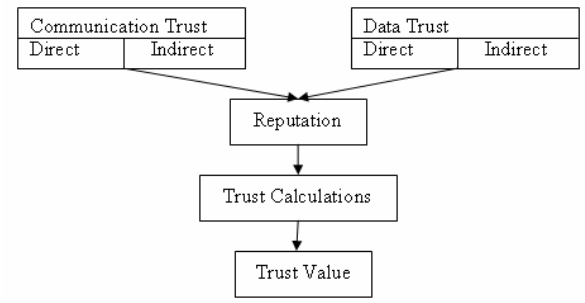

Figure 2: Trust computational model in WSN

According to Figure 2, trust in WSN is a combination of communication trust and data trust, which are presented in sections 3 and 4 respectively.

III COMMUNICATION TRUST IN WSN

Communication trust here means the trust value calculated between nodes based on their cooperation of routing messages to other nodes in the network.

In their trust model for sensor networks Ganeriwal and Srivastava in [3] use the work of Josang and Ismail presented in [4] as a model to derive reputation ratings in the context of e-commerce. Srinivasan, Teitelbaum and Wu in [6] also 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 [3] 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 shown in equation (2).

$$R_{ij} = Beta(\alpha_{ij} + 1, \beta_{ij} + 1) \quad (2)$$

Trust is defined as the expected value of the reputation and is given in equation (3)

$$T_{ij} = E(R_{ij}) = E\{Beta(\alpha_{ij} + 1, \beta_{ij} + 1)\} = \frac{(\alpha_{ij} + 1)}{(\alpha_{ij} + \beta_{ij} + 2)} \quad (3)$$

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 (4).

$$R_{ij}^{new} = Beta(\alpha_{ij}^{new}, \beta_{ij}^{new}) \quad (4)$$

Where node n_i uses its reputation of node n_k in the combination process. α_{ij}^{new} and β_{ij}^{new} shown in equations (5) and (6) respectively, are the updated values for α_{ij} and β_{ij} given by the authors of [3] by mapping the problem into a Dempster-Shaffer belief theory model [11], solving it using the concept of belief discounting, and doing a reverse mapping from belief theory to continuous probability. For more details on all these equations we refer the readers to [3, 4, 12]. T_{ij}^{New}, given in equation (7) is the updated trust value based on α_{ij}^{new} and β_{ij}^{new} values.

$$\alpha_{ij}^{New} = \alpha_{ij} + \frac{2 * \alpha_{ik} * \alpha_{kj}}{(\beta_{ik}+2)*(\alpha_{kj}+\beta_{kj}+2)+(2*\alpha_{ik})} \quad (5)$$

$$\beta_{ij}^{New} = \beta_{ij} + \frac{2 * \alpha_{ik} * \beta_{kj}}{(\beta_{ik}+2)*(\alpha_{kj}+\beta_{kj}+2)+(2*\alpha_{ik})} \quad (6)$$

$$T_{ij}^{New} = E(R_{ij}^{New}) = E\{Beta(\alpha_{ij}^{New}+1, \beta_{ij}^{New}+1)\} = \frac{(\alpha_{ij}^{New}+1)}{(\alpha_{ij}^{New}+\beta_{ij}^{New}+2)} \quad (7)$$

IV. DATA TRUST IN WSN

Data trust is a new concept introduced by us to calculate the trust in WSN based on the actual sensed data of the sensors as presented in [1], and to differentiate it from the communication trust as discussed in the previous section. If we let $\{A_1, A_2, ..., A_N\}$ be the nodes of a WSN and the corresponding matrix (Γ) be as shown in equation (8), and if node A_i is connected to node A_j, then $\Gamma_{i,j} = \Gamma_{j,i} = 1$ otherwise it is equal to 0.

$$\Gamma = [\Gamma_{i,j}] = \begin{pmatrix} 1 & . & . & 1 \\ . & 1 & . & . \\ 1 & . & 1 & . \\ . & 1 & . & 1 \end{pmatrix} \quad (8)$$

Let X be 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 $t = 0, 1, 2, \ldots, k$, the random variable $X_{Ai} = X_i$ is the sensed value by node A_i. $i = 1, \ldots, N$. $xi(t)$ is the realization of that random variable at time t. Each node A_i, $i = 1, \ldots, N$ 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 (9).

$$Y_{i,j}(t) \sim N(\theta_{i,j}, \tau^2) \quad (9)$$

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 (10),

$$\overline{y}_{i,j} = \sum_{t=1}^{k} y_{i,j}(t) / k \quad (10)$$

then

$$(\theta_{i,j} \mid y_{i,j}) \sim N(\overline{y}_{i,j}, \tau^2 / k) \quad (11)$$

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 $\sigma_{i,j}^2 = \tau^2 / k$. 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 (12)

$$R_{i,j} = N(\mu_{i,j}, \sigma_{i,j}^2) \quad (12)$$

where $\mu_{i,j} = \overline{y}_{i,j}$ and $\sigma_{i,j}^2 = \tau^2 / k$ are the equivalent of α_{ij} and β_{ij} as given in [3].

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 (13) and (14).

$$T_{i,j} = \mathrm{Prob}\{|\theta_{i,j}| < \varepsilon\} \quad (13)$$

$$T_{i,j} = \mathrm{Prob}\{-\varepsilon < \theta_{i,j} < +\varepsilon\} = \\ = \phi\left(\frac{\varepsilon - \mu_{i,j}}{\sigma_{i,j}}\right) - \phi\left(\frac{-\varepsilon - \mu_{i,j}}{\sigma_{i,j}}\right) \quad (14)$$

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 (15).

$$P(\theta_{i,j} \mid y_{i,j}, (\mu_{l_1,j}, \sigma_{l_1,j}),...,(\mu_{l_m,j}, \sigma_{l_m,j}), \\ (\mu_{i,l_1}, \sigma_{i,l_1}),...,(\mu_{i,l_m}, \sigma_{i,l_m})) \quad (15)$$

Equation (15) 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 (16) and (17) consequently. We encourage the readers to refer to our model presented in [1] for detailed analysis of equation (15) as of lack of space to present it in here.

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

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

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 [3], as derived from the approach in [4]. The network topology and protocols follow those of [3, 6]. 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 (18), the reputation parameters $\mu_{i,j}$ and $\sigma_{i,j}^2$ are presented in equations (19) and (20) respectively and the updated values for them $\mu_{i,j}^{New}$ and $\sigma_{i,j}^{New}$ are presented in equations (21) and (22). $T_{i,j}^{New}$ in equation (23) is the newly updated trust based on $\mu_{i,j}^{New}$ and $\sigma_{i,j}^{New}$.

$$\theta_{i,j} \sim N(\mu_0, \sigma_0^2) \quad (18)$$

$$\mu_{i,j} = \frac{(\mu_0/\sigma_0^2) + (k\bar{y}_{i,j}/\tau^2)}{(1/\sigma_0^2) + (k/\tau^2)} \quad (19)$$

$$\sigma_{i,j}^2 = \frac{1}{(1/\sigma_0^2) + (k/\tau^2)} \quad (20)$$

$$\mu_{i,j}^{new} = \frac{(\mu_0/\sigma_0^2) + \sum_{s=1}^{m} \frac{(\mu_{l_s,j} + \mu_{i,l_s})}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k\bar{y}_{i,j}/\tau^2)}{(1/\sigma_0^2) + \sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k/\tau^2)} \quad (21)$$

$$\sigma_{i,j}^{2\ new} = \frac{1}{(1/\sigma_0^2) + \sum_{s=1}^{m} \frac{1}{\left(\frac{1}{T_{i,l_s}} - 1\right)\alpha} + (k/\tau^2)} \quad (22)$$

$$T_{i,j}^{New} = \phi\left(\frac{\varepsilon - \mu_{i,j}^{New}}{\sigma_{i,j}^{New}}\right) - \phi\left(\frac{-\varepsilon - \mu_{i,j}^{New}}{\sigma_{i,j}^{New}}\right) \quad (23)$$

In the following section we will present some of the simulation results received by simulating the two trust models on the same network.

V. SIMULATION RESULTS

To verify our theory we conducted several simulation experiments to calculate communication trust and data trust between 4 nodes (1,6,7, and 13) in a sub-network of 15 nodes as shown in Figure 3.

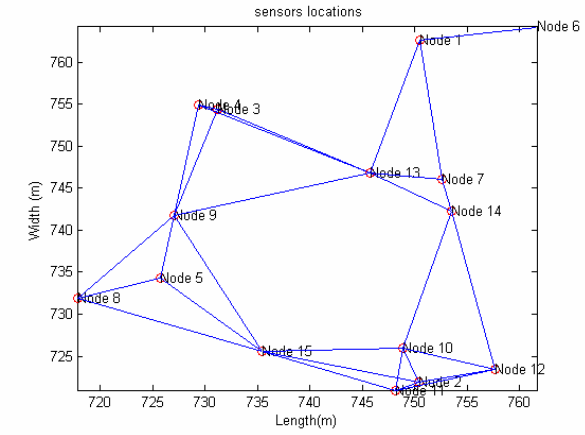

Figure 3: Wireless sensor network Diagram

First of all we assume that all nodes are normal (no faulty or malicious nodes) in terms of communication and data sensing. The results presented in Figure 4, show that all nodes trust each other and trust value is increasing gradually until it reaches 1 for both; data trust (DT) and communication trust (CT).

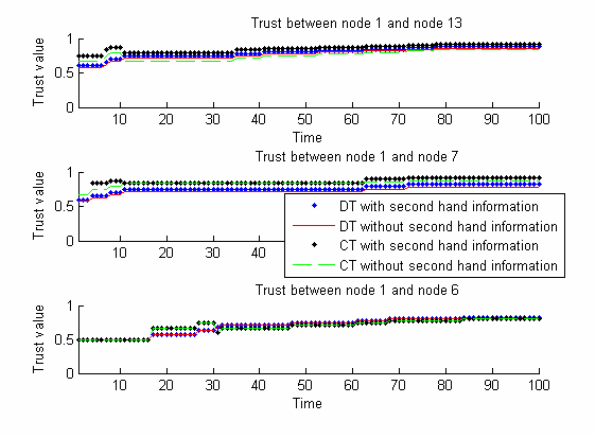

Figure 4: All nodes are normal

The results presented in Figure 5 below, show that the CT is gradually increasing to 1 between all nodes (there is no communication error between nodes), while the DT trust is decreasing to 0 for node 13 as it is a malicious node (not reporting its sensed data to other nodes).

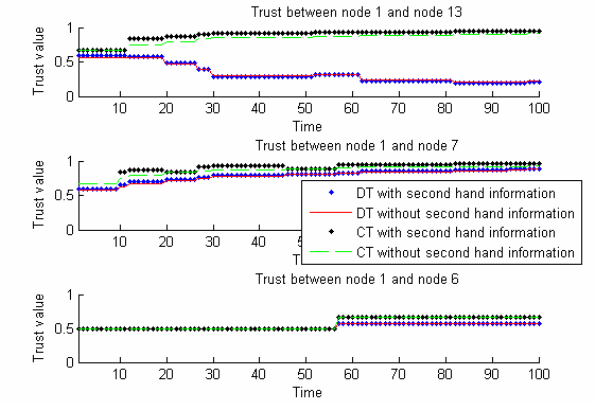

Figure 5: node 13 is faulty

In another simulation experiment we introduced a communication error between nodes and the results presented in Figure 6 below, show that the CT is gradually decreases to 0 between all nodes and the DT is gradually increasing to 1 as all nodes are reporting their sensed data.

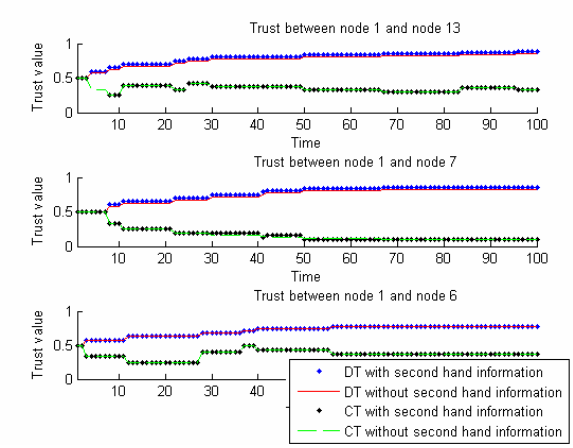

Figure 6: Nodes with communication error

VI. CONCLUSION AND FUTURE WORK

From the above illustration and as can be seen from our simulation results, we proved that trusted nodes from a communication point of view can be un-trusted from data point of view and vice versa. That is, examining the trust in WSN from a traditional communication point of view only is not going to work in some scenarios, which means introducing some techniques to examine the actual reported data is required. In the future we are planning to combine the data trust and the communication trust using Bayesian networks to come up with a fine tune solution to calculate trust in WSN.

REFERENCES

[1] 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.

[2] M. Momani and S. Challa, "GTRSSN: Gaussian Trust and Reputation System for Sensor Networks," presented at International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CIS2E 07), 2007.

[3] 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.

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

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

[6] 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.

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

[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] 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.

[10] M. Momani, J. Agbinya, R. Alhmouz, G. P. Navarrete, and M. Akache, "A New Framework of Establishing Trust in Wireless Sensor Networks," in *International Conference on Computer & Communication Engineering, (ICCCE '06)*. Kuala Lumpur, Malaysia, 2006.

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

[12] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor networks," *ACM Transactions on Sensor Networks,*, vol. v, 2007.