Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks

Mohammad Momani
Faculty of Engineering and Information Technologies, University of Technology Sydney, Australia
Email: mmomani@eng.uts.edu.au

Subhash Challa and Rami Alhmouz
NICTA, VRL, University of Melbourne, Australia
Engineering Faculty, Al-isra University, Amman, Jordan
Email: {subhash.challa@nicta.com.au, ralhmouz@gmail.com}

***Abstract*—This paper introduces a new Bayesian fusion algorithm to combine more than one trust component (data trust and communication trust) to infer the overall trust between nodes. This research work proposes that one trust component is not enough when deciding on whether or not to trust a specific node in a wireless sensor network. This paper discusses and analyses the results from the communication trust component (binary) and the data trust component (continuous) and proves that either component by itself, can mislead the network and eventually cause a total breakdown of the network. As a result of this, new algorithms are needed to combine more than one trust component to infer the overall trust. The proposed algorithm is simple and generic as it allows trust components to be added and deleted easily. Simulation results demonstrate that a node is highly trustworthy provided that both trust components simultaneously confirm its trustworthiness and conversely, a node is highly untrustworthy if its untrustworthiness is asserted by both components.**

***Index Terms*—Trust, Bayesian, Fusion, Sensor, Network, Data, Communication**

I. INTRODUCTION

Trust is an old yet important issue in any networked environment that can solve some problems which lies beyond the power of traditional cryptographic security. Generally, trust plays a major role in establishing relationship between entities which has been studied mainly by social scientists for a long time. Trust is something humans use every day to promote interactions and accept risk; exchanging information with others, buying and selling and all the other interactions with the environment involve some form of trust.

Trust and trust establishment between nodes in wireless sensor networks (WSNs) are the starting point for constructing the network. Even though trust has been formalised as a computational model, it still means different things for different research communities. Therefore, it is argued in this paper that trust in WSNs can assume more than one definition, depending on the applications and/or the attributes involved in trust evaluation. Hence, trust is defined in this context as "*The subjective probability by which node A depends on node B to fulfil its promises in performing an action and at the same time being reliable in reporting its sensed data".*

Trust management in WSNs is predominantly based on routing messages regardless of the fact that communication has occurred or not [1-5]. This is known as "Communication Trust". The introduction of sensed data, as discussed in [6] and [7], as a new core component when deciding to trust nodes in WSNs, represents a new challenge on "how much trust is enough, and which components should be included to decide on trust". This new core component is called "Data Trust".

This paper argues that if the overall trust is solely based on communication trust, then the network might be misled, hence, untrustworthy nodes in terms of data trust might be classified as trusted nodes due to their communication capabilities and the same argument holds for the other case. That is, approaching the trust problem from one angle is not enough to decide on whether or not to trust a specific node in a WSN. Therefore, new trust models need to be developed in order to answer the questions of which components are to be involved when calculating trust and, how to combine these components to achieve overall trust given different scenarios and applications.

In this paper, the previously designed trust model for WSNs, as discussed in [6] and [7], is extended to include both communication trust and data trust. The data trust model presented in [6, 7], is simulated and compared with the communication trust model presented in [1], and the results have proven that modelling trust using only one component might not be enough to decide the trustworthiness of nodes in a WSN. As a result of this, a

doi:10.4304/jnw.5.7.815-822

new Bayesian fusion algorithm is introduced to address this issue by combining both data and communication trust to infer the overall trust. The proposed algorithm is generic and allows more trust components to be plugged into the model to infer the total trust for different scenarios. The rest of the paper is organised as follows: Section 2 presents the problem statement and section 3 discusses the trust components (communication trust and data trust). The Bayesian fusion algorithm is presented in section 4. In section 5 we present some of the simulation results and section 6 concludes the paper.

II. Problem Statement

The problem addressed in this paper can be stated as: "Given a network of large number of sensor nodes deployed in some area distant from a fusion centre, as presented in Fig. 1. Sensor nodes perform measurements and the fusion centre would like to query statistics of the measured values. However, sensor nodes cannot report the measurements directly to the fusion centre, due to their power and range capability, so they employ a multi-hop strategy for communicating with other nodes in the network to deliver the data to the fusion centre. That is, each node in the network acts as a host (senses events) and as a router (routes messages for other nodes) simultaneously. As there is no guarantee that all nodes in the discovered route are trusted nodes and will behave as expected, some malicious or selfish nodes might exist, and that can lead to network malfunctioning or even to a total breakdown of the network. So, how can we exclude the malicious sensor nodes that do not route messages and/or provide correct or reliable sensed data?"

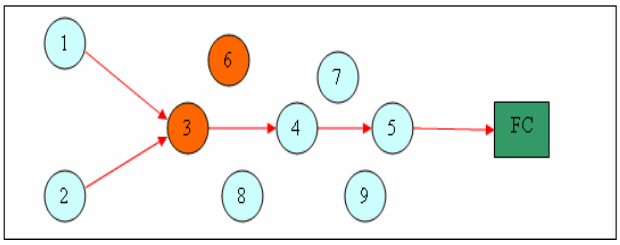

Figure 1. Wireless sensor network example

To further illustrate the problem, let us consider the following scenario for the network presented in Fig. 1, which assumes that a WSN consists of several sensor nodes and a fusion centre (FC). Nodes are deployed to monitor an event and to report the sensed data to the FC. Nodes can communicate, send and receive messages, even if some of them are malicious, but for unseen reasons (being faulty or malicious), they do not report their own sensed data and, vice versa, nodes do report their sensed data but do not route messages for other nodes. In other words, node (3) in Figure 1, for example, is forwarding all messages from node (1) and node (2) to the FC using a multi-hop route through nodes (4) and (5), which means that node (3) is very trustworthy from the communication point of view. On the other hand, node (3) is not reporting its actual data to other nodes in the network. For example, if node (3) is a malicious (having been captured by an enemy) node and because the reported data will affect it somehow, imagine that the sensed data are pointing to intruder personnel from the same group as node (3) entering and leaving a battle-field: of course node (3) is not going to report it, so node (3) is untrustworthy from the data point of view. That is, node (3) is trustworthy from a communication point of view and at the same time it has been proven that it is untrustworthy from the data point of view. The same situation is valid when all three nodes are sending their sensed data, temperature, for example, but due to the high cost of communication in such networks and because of node (3) being selfish, it is not routing messages from nodes (1) and (2). In this situation, node (3) is trusted from the data point of view but not from the communication point of view. So a mechanism to judge and predict the behaviour of node (3) and to notify the other nodes and/or the FC about node (3)'s trustworthiness is needed, in order for appropriate actions to be taken.

III. Trust Components

Based on the above illustration, the trust computational model for WSNs presented in [8, 9], is extended to reflect the new challenges, using more than one criterion to decide on trust. The extended trust computational model for WSNs, presented in Fig. 2, is a generic trust model, that is, new trust components affecting nodes' trustworthiness in a network can be added to or removed from the model and the overall trust can be recalculated very easily.

As can be seen from Fig. 2, trust in WSNs is a combination of communication trust and data trust, which are presented in the following sub-sections.

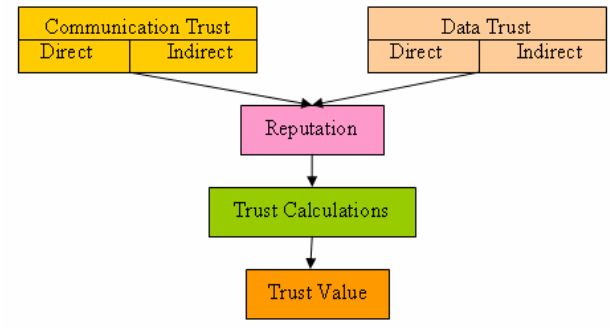

Figure 2. Extended trust computational model for WSNs

A. Communication Trust in WSNs

Communication trust (CT), here, means the trust value calculated between nodes based on their cooperation in routing messages to other nodes in the network. In their trust model for sensor networks, Ganeriwal and Srivastava, in [1], extended the work of Josang and Ismail presented in [10] as a model to derive reputation ratings in the context of e-commerce. The Beta reputation system

is based on the Beta probability density function, *Beta* (α, β), and is given in (1),

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

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 (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 (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 receives 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 (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 (5) and (6) respectively, are the updated values for α_{ij} and β_{ij} given by the authors of [1] by mapping the problem into a Dempster-Shaffer belief theory model [11], solving it using the concept of belief discounting, and undertaking a reverse mapping from belief theory to continuous probability. For more details on all these equations, readers are encouraged to refer to [1, 10, 12]. T_{ij}^{New}, given in (7), is the updated CT value based on α_{ij}^{new} and β_{ij}^{new} values.

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

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

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

B. Data Trust in WSNs

Data trust (DT) is a new concept introduced in [13] to calculate trust in WSNs based on the actual sensed data of the sensors, and it is recommended that readers refer to [14] for a detailed explanation on the equations presented here, in order to avoid repetition. Reputation $R_{i,j}$ and trust $T_{i,j}$ between node n_i and node n_j are defined as discussed in the previous chapter and given in (8) and (9) respectively,

$$R_{i,j} = N(\mu_{i,j}, \sigma_{i,j}^2) \quad (8)$$

$$\begin{aligned} T_{i,j} &= \mathrm{Prob}\{|\theta_{i,j}| < \varepsilon\} \\ &= \mathrm{Prob}\{-\varepsilon < \theta_{i,j} < +\varepsilon\} \\ &= \phi\left(\frac{\varepsilon-\mu_{i,j}}{\sigma_{i,j}}\right) - \phi\left(\frac{-\varepsilon-\mu_{i,j}}{\sigma_{i,j}}\right) \end{aligned} \quad (9)$$

where $\mu_{i,j}$ and $\sigma_{i,j}^2$, represent the mean and variance as shown in (10) and (11),

$$\mu_{i,j} = \frac{(\mu_0/\sigma_0^2)+(k\bar{y}_{i,j}/\tau^2)}{(1/\sigma_0^2)+(k/\tau^2)} \quad (10)$$

$$\sigma_{i,j}^2 = \frac{1}{(1/\sigma_0^2)+(k/\tau^2)} \quad (11)$$

It is also argued that the second-hand information represents a Normal, Gaussian distribution with updated mean $\mu_{i,j}^{new}$ and variance $\sigma_{i,j}^{2\ new}$, given in (12) and (13) respectively,

$$\mu_{i,j}^{new} = \frac{(\mu_0/\sigma_0^2)+\sum_{s=1}^{m}\frac{(\mu_{s,j}+\mu_{i,l_s})}{\left(\frac{1}{T_{i,l_s}}-1\right)\alpha}+(k\bar{y}_{i,j}/\tau^2)}{(1/\sigma_0^2)+\sum_{s=1}^{m}\frac{1}{\left(\frac{1}{T_{i,l_s}}-1\right)\alpha}+(k/\tau^2)} \quad (12)$$

$$\sigma_{i,j}^{2\ new} = \frac{1}{(1/\sigma_0^2)+\sum_{s=1}^{m}\frac{1}{\left(\frac{1}{T_{i,l_s}}-1\right)\alpha}+(k/\tau^2)} \quad (13)$$

based on the above discussion, the newly updated DT value $T_{i,j}^{New}$ between node n_i and node n_j will be calculated as in (14),

$$T_{i,j}^{New} = \phi\left(\frac{\varepsilon - \mu_{i,j}^{New}}{\sigma_{i,j}^{New}}\right) - \phi\left(\frac{-\varepsilon - \mu_{i,j}^{New}}{\sigma_{i,j}^{New}}\right) \quad (14)$$

Simulation experiments to verify the argument "one trust component might mislead nodes in a WSN, and distrusted nodes can be seen as very trustworthy", were developed and conducted to calculate CT and DT between four nodes (1, 6, 7, and 13) in a sub-network of fifteen nodes, as shown in Fig. 3.

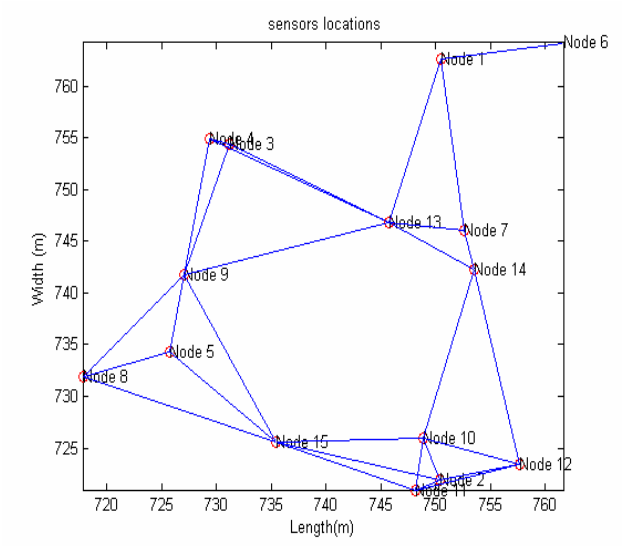

Figure 3. Wireless sensor network diagram

Initially, it is assumed that all nodes are normal; no faulty or malicious nodes exist in the network, so all nodes report their sensed data and route messages normally. The results presented in Fig. 4, demonstrate that all nodes in the sub-network trust each other and the trust value is increasing gradually until it reaches the maximum value for both DT and CT.

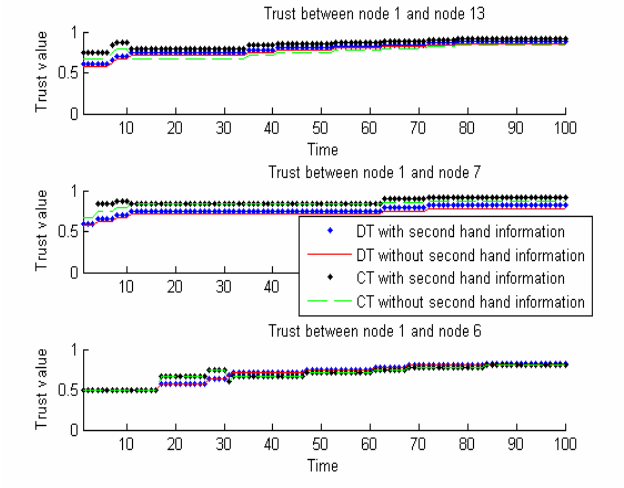

Figure 4. All nodes are normal

In a second simulation, whose results are presented in Fig. 5, node (13) is assumed to be malicious, not reporting data, so it is noticeable that the CT is gradually increasing to the maximum value between all nodes, as there is no communication error between nodes, while the DT trust is decreasing to the minimum value for node (13) as it is a malicious node, not reporting its sensed data to other nodes. In other words, node (13) is assumed to be a trusted node from a communication point of view, but in reality it is not, as can be seen from the data point of view.

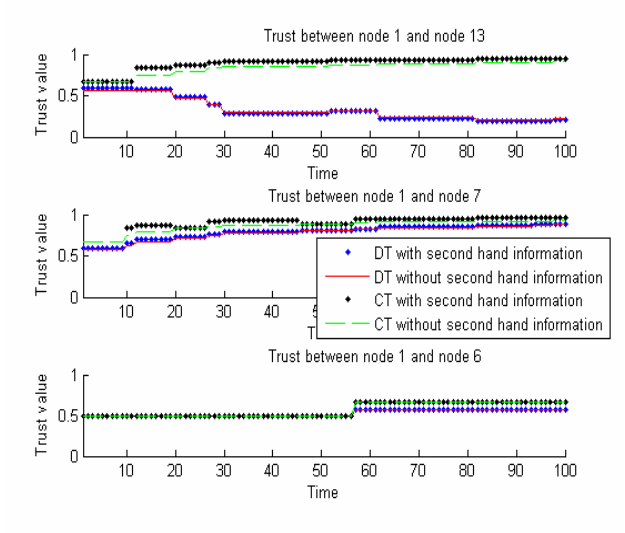

Figure 5. Node 13 is not reporting data

In a third simulation experiment, it is assumed that a communication error exists between nodes, so nodes can report their sensed data but are not routing messages between themselves, and the results presented in Fig. 6, below indicate that the CT is gradually decreasing to the minimum value between all nodes and the DT is gradually increasing to the maximum value, as all nodes are reporting their sensed data. Similarly in this case, nodes are assumed to be trusted from the data point of view, while in reality they are not, as they are not routing messages between themselves and the communication trust is decreasing to the minimum value.

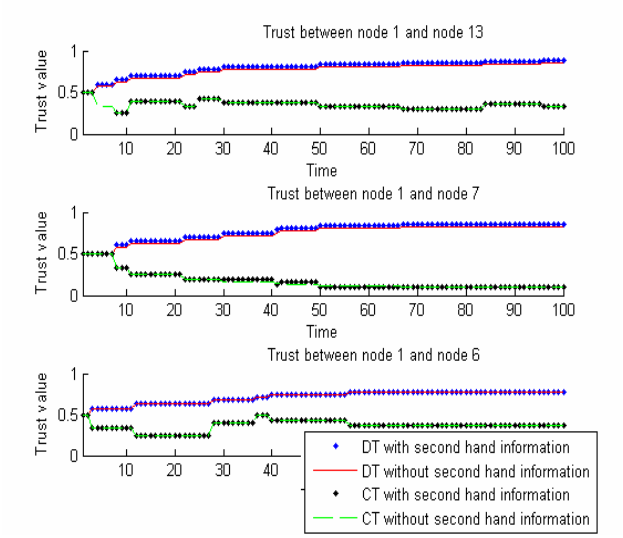

Figure 6. All nodes have a communication error

From the previous simulation results, it has been proven that one component for calculating trust in WSNs might not be enough, as it could mislead the whole network, so a new technique is required to combine more than one trust component to achieve the overall trust. It has been argued that Bayesian fusion algorithms are the most suitable tools to combine trust components, as discussed in the following section.

IV. Bayesian Fusion Algorithm

The Bayesian fusion structure illustrated in Fig. 7, is a representation of the newly created trust model given in Fig. 2; which is a substitution to the Bayesian network structure given in [14]; where C represents the communication trust, D represents the data trust and T represents the total trust.

Using Bayes' theorem, the probability of the total trust, given the data trust and communication trust, can be presented, as shown in (15),

$$P(T|D,C)=\frac{P(D|T,C)*P(T|C)}{P(D|C)} \tag{15}$$

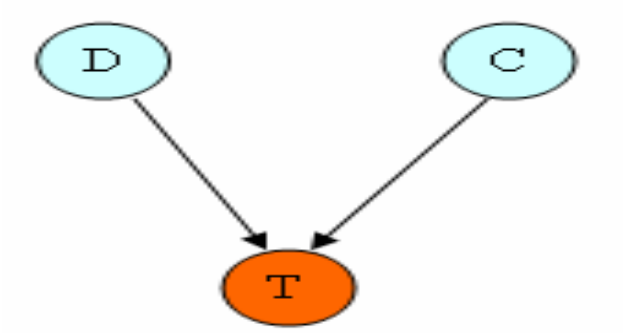

Figure 7. Bayesian fusion structure

As discussed previously in the intrusion detection scenario illustrated in Fig. 1, in the case of a node always communicating but not reporting the data, C and D are independent. Because of that independence, the likelihood function $P(D|T,C)$ in (15) can be presented, as in (16),

$$P(D|T,C)=P(D|T) \tag{16}$$

By substituting equation (16) in equation (15), the probability of the total trust will be as given in (17),

$$P(T|D,C)=\frac{P(D|T)*P(T|C)}{P(D|C)} \tag{17}$$

Applying Bayes' theorem, $P(D|T)$ can be calculated as in (18),

$$P(D|T)=\frac{P(T|D)*P(D)}{P(T)} \tag{18}$$

By substituting (18) in (17), the result is given in (19),

$$P(T|D,C)=\frac{P(T|D)*P(T|C)*P(D)}{P(D|C)*P(T)} \tag{19}$$

Equation (19), after ignoring the normalising factor and the other constants, it can be seen that the probability of the combined trust T is mainly equal to the multiplication of the probabilities of both trust components, C and D, as shown in (20),

$$P(T|D,C)=P(T|D)*P(T|C) \tag{20}$$

In other words, the resulting distribution of both distributions – the Beta distribution used to calculate communication trust and the Normal distribution used to calculate data trust – is equal to the multiplication of both distributions, as illustrated in Fig. 8.

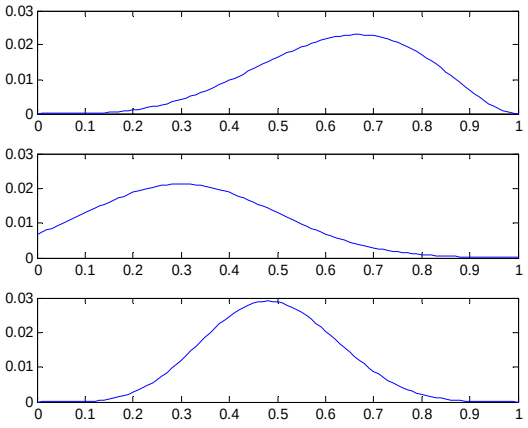

Figure 8. Multiplication of Beta and normal distributions

The first distribution represents a Beta distribution, the second distribution represents a normal distribution and the third distribution represents the resulting distribution, the multiplication of the Beta and normal distributions.

V. Simulation Results

To verify the theory given in the previous section, several simulations were conducted on the same sub-network of nodes (1, 6, 7 and 13) from the network diagram presented in Figure 3.

A. All Nodes are Normal

Fig. 9, below displays the results when all nodes in the sub-network are normal from both the communication and data point of view. The total trust value is increasing to the maximum value of one, as for the other trust values: data trust and communication trust.

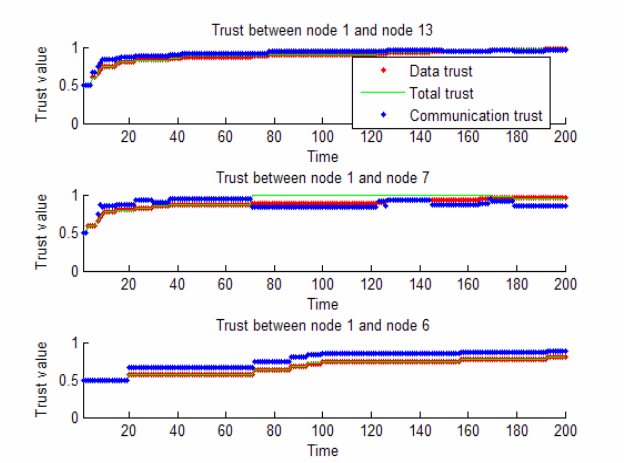

Figure 9. All nodes in the sub-network are normal

B. Node 13 is not Reporting Data

Fig. 10, shows the results when node 13 is faulty from the data point of view, That is, node 13 is routing messages but not reporting sensed data. The data trust is decreasing to zero and the communication trust is increasing to one, the total trust is in between, which is reasonable; the total trust stays on the initial trust value assigned to the node. In other simulations the total trust might be higher or lower, depending on how long the node stays in the same situation.

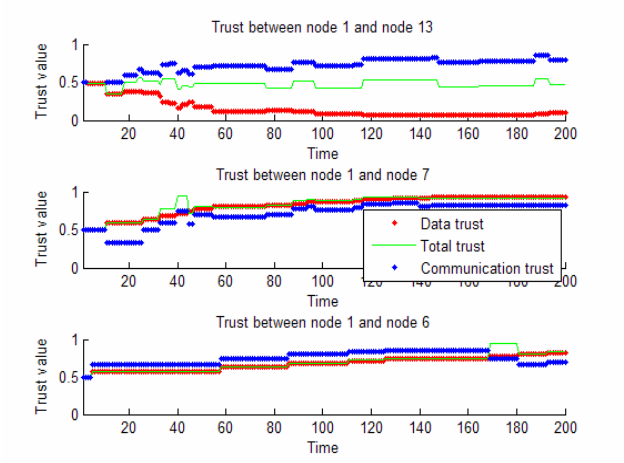

Figure 10. Node 13 is faulty (data error)

C. All Nodes have a Communication Error

Fig. 11, below shows the results when nodes are not routing messages. It explains the situation when there is a communication error but there is no data error, that is, all nodes are reporting their sensed data, but not routing messages for other nodes. As can be seen, the communication trust value for all nodes is decreasing towards the value of zero, while the data trust value is increasing towards the value of one. The total trust is again in the reasonable range, around the initial assigned value, which is better than being completely trusted or distrusted.

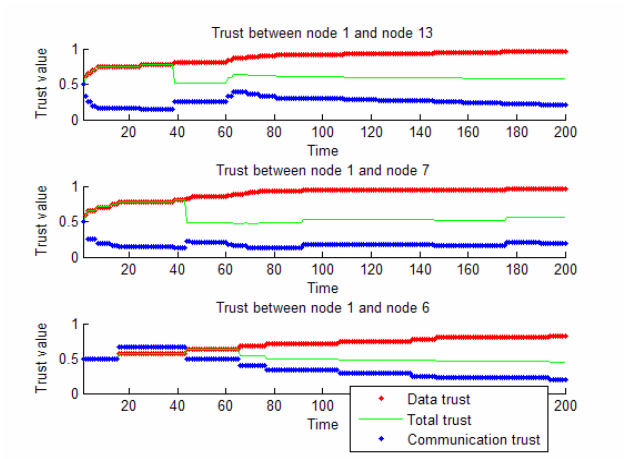

Figure 11. All nodes have a communication error

D. All Nodes with Communication Error and Node 13 has also a Data Error

Fig. 12, below explains when there is a communication error between all nodes and a data error in node 13, that is, all nodes are not routing messages and node 13 is also not reporting its sensed data properly. As can be seen from Fig. 12, the communication trust value for all nodes is decreasing towards the value of zero, the data trust values for node 7 and node 6 are increasing towards the value of one, and the total trust value is around the initial assigned trust value. The interesting case here is that, for node 13, the communication trust value and the data trust value are decreasing towards the value of zero and this is also the case for the total trust value.

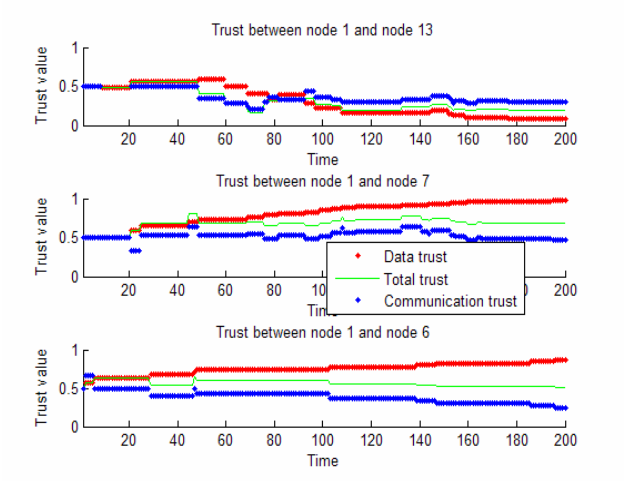

Figure 12. All nodes have a communication error and node 13 has also a data error

In summary and as can be seen from the above illustrations, it has been proven that nodes in a WSN can be trusted from a communication point of view but distrusted from a data point of view, and vice versa. In other words, the node can be trusted and distrusted at the same time if only one trust component is considered. Therefore a new Bayesian fusion algorithm is introduced to combine both trust values – data trust and communication trust – and to produce the total trust which defines the node as a trusted or distrusted node.

VI. CONCLUSION

It has been argued that using one trust component to decide the trustworthiness of nodes in WSNs is not enough and can mislead the network. Therefore, more than one component should be considered when evaluating trust. Therefore, the two different trust components, the data trust and the communication trust, were reconsidered and a simulation comparison between them was conducted. It has been proven that a trusted node from the data point of view can be distrusted from a communication point of view and vice versa. This led to the extension of the trust computational model in WSNs to reflect the new challenges and to include both trust components – data trust and communication trust – as decisive factors regarding the trustworthiness of nodes.

This paper has also presented a new Bayesian fusion algorithm to combine both trust components. The algorithm is generic and allows trust components to be added to and/or deleted from very smoothly and transparently. The simulation results for the newly introduced algorithm show that, if a node is trusted on one component and distrusted on the other component, then the combined trust value will be around the initially assigned trust value. In other words, one trust component by itself cannot fully decide the trustworthiness of nodes in WSNs. The results have also demonstrated that the node is very trustworthy if it is trusted by both components at the same time and, vice versa, the node is very untrustworthy if it is distrusted by both components.

REFERENCES

[1] S. Ganeriwal and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks", in *The 2nd ACM Workshop on Security of Ad-hoc and Sensor Networks* Washington DC, USA 2004.

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

[3] D. Liu, P. Ning and W. Du, "Detecting Malicious Beacon Nodes for Secure Location Discovery in Wireless Sensor Networks", in *The 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05)*, 2005.

[4] G. V. Crosby, N. Pissinou and J. Gadze, "A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks", in *The Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS '06)*, Columbia, Maryland, 2006.

[5] H. Chen, H. Wu, X. Zhou and C. Gao, "Reputation-based Trust in Wireless Sensor Networks", in *International Conference on Multimedia and Ubiquitous Engineering (MUE '07)*, Seoul, Korea, 2007.

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

[7] M. Momani and S. Challa, "GTRSSN: Gaussian Trust and Reputation System for Sensor Networks", in *International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE '07)*, University of Bridgeport 2007.

[8] 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. Mahmoodand M. Karim, Eds.: Springer Netherlands, 2007.

[9] 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.

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

[11] G. Shafer, *A Mathematical Theory of Evidence*: Princeton University Press, 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.

[13] M. Momani, S. Challa and R. Alhmouz, "Can we Trust Trusted Nodes in Wireless Sensor Networks?" in *The International Conference on Computer and Communication Engineering (ICCCE '08)*, Kuala Lumpur, Malaysia, 2008.

[14] M. Momani, S. Challa and R. Alhmouz, "BNWSN: Bayesian Network Trust Model for Wireless Sensor Networks", in *Mosharaka International Conference*

on Communications, Computers and Applications (MIC-CCA '08), Amman, Jordan, 2008.

Mohammad Momani is a sessional lecturer at the University of Technology, Sydney, Faculty of Engineering and Information Technologies. His research interests are trust management and security issues in mobile ad hoc networks and wireless sensor networks. He graduated with a PhD in Computer Engineering from the University of Technology, Sydney in 2009, a M.Sc. in Internetworking from the University of Technology, Sydney in 2003 and a M.Sc. in Computer Engineering from Bulgaria in 1986 and. He is also a CCNI, CCNA, MCSE and a CNE certified with almost 20 years of experience in the computer industry.

Prof. Subhash Challa is the Senior Principal Scientist at NICTA, Victorian Research Lab, Melbourne, Australia. Prior to this he was the Professor of Computer Systems at the University of Technology, Sydney, and lead the Networked Sensor Technologies (NeST) Lab.

He was a senior research fellow at the University of Melbourne where he led a number of tracking and data fusion projects in collaboration with DSTO, DARPA, BAE, Raytheon, Tenix Defense, Thales, RTA, NSW Police and others. He received his PhD from QUT, Brisbane, Australia in 1999. Part of his PhD was completed at Harvard Robotics Lab, Harvard University, Boston, USA.

Subhash was a Tan-Chun-Tau Fellow at Nanyang Technological University, Singapore 2002-2003. He has been the plenary, tutorial and invited speaker at various information fusion and sensor network conferences worldwide, including IDC 2007 (Adelaide, Australia), Sensors Expo 2006 (Chicago, USA), ISSNIP conferences (2005, 2004) and Fusion Conferences (2003, 2005, 2006). He is co-authoring of reference text "Fundamentals of Object Tracking," to be published by Cambridge University Press, UK. He is also the associate editor of the Journal of Advances in Information fusion. He has published about 70 papers in various International journals and conferences.

Rami Al-Hmouz was born in 1975, He received a B.Sc. degree in from Mutah university 1998, a MSc. from university of Western Sydney, 2003 and PhD degree from University of Technology, Sydney,2008. Currently he is an Assistance professor at Alisra private university (Jordan). His research interests are in computer vision, computer Networks and sensor networks.