Trust and Reputation Analysis in Fading Wireless Sensor Network Channel

Rami Al-Hmouz [1], Mohammed Momani [2], Maen Takruri [3]

[1.] King Abdulaziz University, Saudi Arabia
[2.] University of Technology, Sydney, Australia
[3.] American University of Ras Al Khaimah, UAE
ralhmouz@kau.edu.sa

Abstract: This paper introduces a Trust model and a Reputation System for wireless sensor nodes in fading multi paths channel. The proposed model establishes the continuous version of the Beta Reputation System applied to binary events. In doing so, we introduce a theoretically sound Bayesian probabilistic approach for mixing second hand information from neighboring nodes with directly observed information. A Trust model in a wireless sensor network addresses the security issue and how to deal with possibly malicious and unreliable nodes. Although encryption and cryptography keys are used, these deterministic approaches fail to answer the problem of securing the routing and content of information through a network. Reputation systems are developed to combine with deterministic measures to secure the integrity of a network. Previous research focused on binary transactions in a network, such as routing. This paper introduces Trust model for continuous data in multi paths fading channel.

[Al-Hmouz R, Momani M, Takruri M. **Trust and Reputation Analysis in Fading Wireless Sensor Network Channel**. *Life Sci J* 2013;10(4):310-318] (ISSN:1097-8135). http://www.lifesciencesite.com. 41

Keywords: Trust management; fading channel Sensor network.

1. Introduction

Wireless Sensor Network (WSN) technology is relatively new concept. While wireless communication is already in all sectors 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 (Akyildiz et al., 2002), (Rajaravivarma et al, 2003). 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. Also 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 WSN on an Active Volcano (Werner-Allen et al., 2005), to monitoring the microclimate throughout the volume of redwood trees (Culler et al., 2004), to buildings and bridges monitoring (Glaser., 2004), to health care monitoring (Gao, 2005), to security of oil and water supply pipelines (Alsaade, 2011).

Research continues to be conducted in the design and optimization of WSNs, as the use of these networks is still in its infancy phase. The security issues in WSNs have been raised in (Stajano and Anderson, 1999), (Wang et al., 2006), (Perrig et al., 2004), (Zaman et al., 2012), however as WSN nodes can be deployed in hazardous or hostile areas in large numbers. Such deployment forces the nodes to be of low cost and therefore less reliable or more prone to overtaking by an adversary force. Some methods used such as cryptographic, authentication and other mechanisms (Karlof et al., 2003), (Bohge and Trappe, 2003), (Karlof et al., 2004) do not solve the problem entirely. For example, adversarial nodes can have access to valid cryptographic keys. It certainly does not address the reliability issue where sensor nodes are subject to system faults. These two sources of problems, system faults and erroneous data or bad routing by malicious nodes, can result in the total breakdown of a network. A statistical approach to the problem was introduced in the notion of Trust, formerly applied in social networks and web based commercial exchanges.

In this article, we look at applying the Trust notion to WSNs providing data in multi path fading channel. 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. Momani and Challa (2008), Momani et al. (2007) introduced a theoretical Bayesian probabilistic approach for modeling trust in a wireless sensor network by modeling the noise as additive white Gaussian noise (AWGN). We extend an existing trust model for binary events, the Beta Reputation System (Josang and Ismail, 2002) and Bayesian probabilistic approach (Momani and Challa, 2008) and introduce a probabilistic approach for modeling trust in a wireless sensor networks that experience a multi path fading.

2. The Trust Concept

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 analyzed in economic transactions (Dasgupta, 2000), (Ba and Pavlou, 2002). Marsh (1994) was one of the first to introduce a computational model in his thesis. Then e-commerce necessitated a notion to judge how trusted an internet seller can be (Ba and Pavlou., 2002), (Marsh., 1994). So did Peer-to-Peer networks and other internet forums where users deal with each other in a decentralized fashion (Aberer et al., 2001), (Xiong and Liu., 2003), (Blaze et al., 1999). Recently, attention has been given to the concept of trust to increase security and reliability in Ad Hoc (Michiardi and Molva, 2002), (Buchegger and Boudec, 2002) and sensor networks (Srinivasan et al., 2006), (Ganeriwal and Srivastava, 2004). 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 reflection of the reputation of an entity. Based on reputation, a level of trust is bestowed upon an entity. The reputation itself has been built over time based on that entity's history of behavior, 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.

3. Uncertainties and Decision Problem

The trust problem in wireless networks is characterized by uncertainty in a decision problem. The purpose of a WSN is to detect and report events and data. Initially, the primary focus of the research on trust was on whether a node will detect appropriately, will report or not the detected event(s), and will route information. The uncertainty in these actions warranted the development of reputation systems and corresponding trust models. A node would observe a neighboring node's behavior and build a reputation for that node based on the observed data. By their nature, the considered events are binary, and most trust models developed so far for WSNs are for binary events related node transactions. 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 modeling. For example the WSN trust model RFSN. RFSN stands for Reputation-based Framework for Sensor Networks and was developed by Ganeriwal and Srivastava (2004). This model uses a Bayesian updating scheme known as the Beta Reputation System (Josang and Ismail, 2002) for assessing and updating the nodes reputations. The use of the Beta distribution is due to the binary form of the statistical events considered. The observable nodes transactions data is referred to as first-hand information.

A second source of information in trust modeling 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 consist of information gathered by nodes as first-hand information that is 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 into the trust model and combine it with the observed data or first-hand information. While some trust models build reputation purely on the basis of observations, most attempt to use the second-hand information for obvious reasons. The step of combining both sources of information is handled differently by different trust models. RFSN uses Dempster-Shafer belief theory.

There is a further issue in using second-hand information. 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 et al. (2006) 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. However, this is sub-optimal as information is lost. 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 modeling 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 modeling Expert Opinion in past decades (Lindley and Singpurwalla, 1986), (West, 1984). 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 expert's opinions. Such opinions are modulated by existing knowledge about the experts themselves, to provide a calibrated answer. Momani and Challa (2008), Momani et al. (2007) model trust using Bayesian method in WSN in Gaussian channel.

4. The Beta Reputation System

The Beta Reputation System was proposed by Josang and Ismail (2002) 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 (2004) use the work of Josang and Ismail (2002) in their trust model for wireless sensor networks. Srinivasan et al. (2006) mentioned the possibility of use of the Beta reputation system in their development of DRBTS. The Beta reputation system is based on the Beta probability density function, Beta(α,β):

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

where $0 \leq p \leq 1$; $\alpha > 0$; $\beta > 0$, 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 Rij can be carried by a neighboring node n_i. The reputation is embodied in the Beta model and carried by two parameters α_{ij} and β_{ij}. αij 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 nj maintained by node n_i is R_{ij} = Beta(α_{ij} + 1; β_{ij} + 1). The trust is defined as the expected value of the reputation

$$\begin{aligned} T_{ij} &= E(R_{ij}) = E(Beta(\alpha_{ij}+1, \beta_{ij}+1)) \\ &= \frac{\alpha_{ij}+1}{\alpha_{ij}+\beta_{ij}+2} \end{aligned}$$

Second hand information is presented to node n_i by another neighboring 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 $R_{ij}^{new} = Beta(\alpha_{ij}^{new}, \beta_{ij}^{new})$, where:

$$\begin{aligned} \alpha_{ij}^{new} &= \alpha_{ij} + \frac{2\alpha_{ik}\alpha_{kj}}{(\beta_{ik}+2)(\alpha_{kj}+\beta_{kj}+2)+(2\alpha_{ik})} \\ \beta_{ij}^{new} &= \beta_{ij} + \frac{2\alpha_{ik}\beta_{kj}}{(\beta_{ik}+2)(\alpha_{kj}+\beta_{kj}+2)+(2\alpha_{ik})} \end{aligned}$$

Note that node ni uses its reputation of node nk in the combination process. The authors of RFSN follow the approach of (Josang and Ismail, 2002), by mapping the problem into a Dempster-Shafer belief theory model (Shafer, 1976), 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.

5. 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. Expert opinion, or informed judgment, is often available in the form of vendor information, engineering knowledge, manufacturer knowledge, or simply an opinion formed over time. It is often a subjective opinion based on knowledge. Its main departure from hard data is that it cannot be claimed as objectively observed data. Nevertheless, it is often valuable information that has been formed over the course of time. In our case, the reputation is offered to neighboring nodes as an opinion. The node making the assessment has not observed that reputation, and therefore treats it as an opinion. The probabilistic approach developed for the use of expert opinion applies in the context of second-hand information in reputation modeling.

The probabilistic approach adopted in the elicitation and use of expert opinion is to consider the opinion given by the expert as data and treat it according to the laws of probability Lindley and Singpurwalla, 1986). If θ is a random variable, and μ represents an opinion from an expert that relates to the value of θ, then P(θ/μ) obtains, using Bayes theorem

$$P(\theta|\mu) = \frac{P(\mu|\theta)P(\theta)}{P(\mu)} \qquad (2)$$

Bayes theorem inverses the probability, so that the evidence μ highlights that value of θ that is most likely. The likelihood function $L(\theta) = P(\mu/\theta)$ 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 modeling of this likelihood. In it, the analyst also introduces a modulation to include his expert opinion, leading to a calibrated solution. The analyst may not only have prior knowledge but also some observed data y about a random variable of interest, θ. In such case, Bayes theorem is applied to combine the three sources of information:

$$P(\theta|y,\mu) = \frac{P(y|\theta,\mu)P(\mu|\theta)P(\theta)}{P(y,\mu)} \qquad (3)$$

One often writes

$$P(\theta|y,\mu) \propto P(y|\theta,\mu)P(\mu|\theta)P(\theta),$$

The denominator being a normalizing constant that does not affect the combination occurring in the numerator. 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.

3. Trust and Reputation System in multi paths fading channel

Let $\{A_1, A_2, \dots\dots A_N$ }be the nodes of a wireless sensor network. Let the corresponding matrix be $C = [C_{ij}$], where $C_{ij}= C_{ji}= 1$ if A_i is connected to A_j, 0 otherwise. X is a field variable of interest. This variable such as temperature, chemical quantity, atmospheric value, is detected and sensed by the nodes of the WSN. X is of a continuous nature, but the nodes can report only at discrete times t = 0; 1,2,……….k. $X_{Ai} =X_i$ is the sensed value (random variable) by node A_i; i = 1,…,N. $x_i(t)$ 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 neighbors see that report, and can evaluate the reported value. A_j reports $s_j(t_0)$ at some point of time t_0 then node A_l obtains a modified copy of the report as $x_j(t_0)$ because of the transmission in multi path fading channel. A_l also has its own self-assessment $x_l(t_0) = s_l(t_0)$ (as no transmission is involved). In WSN, the noise generated in the sensor and effect of the fading channel will affect the values reported by the sensors, the multi path fading channel system is modeled as shown in the equation below:

$$x_j(t_0) = hs_j(t_0) + n; \qquad (4)$$

where:

- h is a complex scalar
- s_j is the actual sensor report
- n is AWGN with zero mean and σ^2 variance.

Consequently, reports form sensors $s_j(t_0)$ will suffer from the effect of multi fading channel and it will be received at sensor Ai as $x_j(t_0)$. This will effect on the trust values among sensors. Figure 1 shows a descriptive model of WSN in a fading channel.

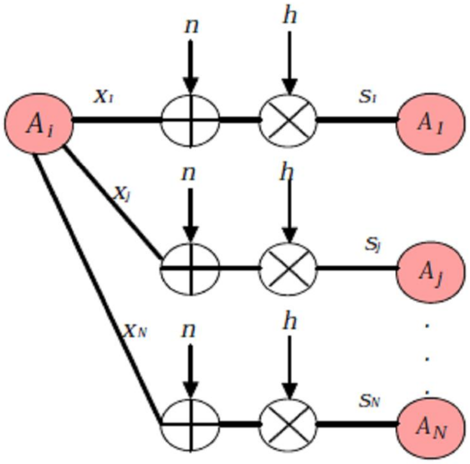


Figure 1. Sensor models in fading channel

In Wireless sensor network the most frequently assumed model for a transmission channel is the additive white Gaussian noise channel (Bohge and Trappe, 2003), (Karlof et al., 2004), (Momani and Challa, 2008). However, the AWGN channel is inadequate model, and it is necessary to adopt a model that imitates the real world. One typical type of such model that occurs in practice is the fading channel. The fading channel is a mobile radio channel, where the sensors receive multi path reflections.

The fading reports $x_j(t_0)$ can be modeled by a Rician or a Rayleigh distribution, depending on the presence or absence of the direct path between A_i and A_j. Fading is Rayleigh if the multiple reflective paths are large in number and there is no dominant or direct line-of-sight (LOS) propagation path. If there is also a dominant LOS path, then the fading is Rician distributed. The Rayleigh probability density function (pdf) can be described by the following formula:

$$p(x) = \begin{cases} \frac{x}{b^2}\exp(-\frac{x^2}{2b^2}) & x \geq 0 \\ 0 & otherwise \end{cases} \quad (5)$$

The mean μ and variance σ^2 of Rayleigh probability density function is given by:

$$\mu = b\sqrt{\frac{\pi}{2}} = 1.233b$$

$$\sigma^2 = b^2(2 - \frac{\pi}{2}) = 0.4292b^2$$

The Rayleigh distribution is a special case of the Ricean distribution, when there is not a dominant signal in the channel, this distribution is characterized by the following probability density function:

$$p(x) = \begin{cases} \frac{x}{b^2}\exp(-\frac{x^2+\nu^2}{2b^2})I_0(\frac{x\nu}{b^2}) & x \geq 0, A \geq 0 \\ 0 & x \prec 0 \end{cases} \quad (6)$$

where υ is the maximum amplitude of the dominant signal and I_0 is the Bessel function of first kind and zero-order. As υ= 0, the Ricean distribution reduces to a Rayleigh distribution. Let $y_{i,j}(t) = x_j(t) - x_i(t)$. From node A_i's perspective, $X_i(t)$ is known and approximates as Gaussian distribution with mean μ_i and variance σ_i^2. Sensors are spread in random and in most case no direct path between them. Therefore, $x_j(t)$ is approximated as Rayleigh distribution with mean μ_j and variance σ_j^2as described above. $Y_{i,j}(t) = X_j(t) - X_i(t)$ represents the error that node A_j commits in reporting the sensed field value $X_j(t)$ at time t. $Y_{ij}(t)$ is a random variable is approximated and modeled as a Normal (Gaussian) with mean μ_{ij} and variance σ_{ij}^2. $Y_{i,j}(t)$ is obtained from the convolution sum between the signal $X_j(t)$ and the signal $X_i(-t)$. At each time instant Y is:

$$Y_{i,j}(t) \sim N(\mu_{i,j}, \sigma_{i,j}^2)$$

$\mu_{ij}(t_0) = \mu_i - \mu_j$ and $\sigma_{ij}^2 = \sigma_{ij}^2 + \sigma_{ij}^2$ is assumed to be known, and it is the same for all nodes. If we let $\bar{y} = \sum_{t=1}^{k} \frac{y_{ij}(t)}{k}$ $y_{i,j}(t)=k$ be the mean of the observed error, as observed by A_i about A_j 's reporting, then:

$$p(\theta_{i,j}|y_{i,j}) \sim N(\mu_{i,j}, \sigma_{i,j}^2)$$

where $y_{i,j} = \{(y_{i,j}(t)$; for all t values at which a report is issued by $Aj\}$. This is a well-known straightforward Bayesian updating where a diffuse prior is used. We let $\mu_{ij} = y_{i,j}$. 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:

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

These are the equivalent of αij and βij of 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 $T_{i,j} = \text{Prob}\{|\theta_{i,j}| < \varepsilon\}$.

$$\begin{aligned} T_{i,j} &= \text{Prob}\{-\epsilon < \theta_{i,j} < \epsilon\} \\ &= \phi\left(\frac{\epsilon-\mu_{i,j}}{\sigma_{i,j}}\right) - \phi\left(\frac{-\epsilon-\mu_{i,j}}{\sigma_{i,j}}\right) \end{aligned} \quad (7)$$

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

6.1 Second Hand Information

In addition data observed in form of $y_{ij} = \{(y_i;j(t)$; for all t values at which a report is issued by $A_j\}$, node Ai uses is proportional to the product of three terms:

$$P(\mathrm{y}_{i,j}|\theta_{i,j}, (\mu_{l_1,j}, \sigma_{l_1,j}), \ldots, (\mu_{l_m,j}, \sigma_{l_m,j}), (\mu_{i,l_1}, \sigma_{i,l_1}), \ldots \\ \ldots, (\mu_{i,l_m}, \sigma_{i,l_m})),$$

$$P((\mu_{l_1,j}, \sigma_{l_1,j}), \ldots, (\mu_{l_m,j}, \sigma_{l_m,j})|\theta_{i,j}, (\mu_{i,l_1}, \sigma_{i,l_1}), \ldots \\ \ldots, (\mu_{i,l_m}, \sigma_{i,l_m}))$$

and

$$\prod_{s=1}^{m} P((\mu_{l_s,j}, \sigma_{l_s,j})|\theta_{i,j}, (\mu_{i,l_s}, \sigma_{i,l_s})) \quad (8)$$

Through conditional independence arguments, To derive $P((\mu_{ls,j}, \sigma_{ls,j})|\theta_{i,j}, (\mu_{i,ls}, \sigma_{i,ls}))$ for each s = 1,….., m, we observe the following:

$$\begin{aligned} \theta_{i,j} &= x_j(t) - x_i(t) \text{ for some } t\text{'s} \\ \theta_{l,j} &= x_j(t) - x_l(t) \text{ for some } t\text{'s} \end{aligned}$$

if all t's were the same, then $\theta i,j = \theta_{lj} + \theta_{i,l}$. 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. since Ai can listen *Aj* and A_l, however since *Xj* and X_l are modeled as Rayleigh distribution with parameters b_j and b_l consecutively. $Y_{l,j}(t) = X_l(t) - X_i(t)$ is approximates as Gaussian distribution. So as a model, assume that:

$$\begin{aligned} \theta_{l,j} &\simeq \theta_{i,j} - \theta_{i,l} \\ \mu_{l,j} &\simeq \theta_{i,j} - \mu_{i,l} \end{aligned}$$

and we model $\mu_{l,j} \sim N(\theta_{i,j} - \mu_{i,l}; var)$, where we choose *var* to be inversely related to node A_i assessment of the reputation of node A_l, that is:

$$var = \sigma_{lj}^2 = \sigma_l^2 + \sigma_j^2$$

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

leads to

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

and consequently,

$$P(\theta_{i,j} | \mathbf{y}_{i,j}, (\mu_{l_1,j}, \sigma_{l_1,j}), \ldots, (\mu_{l_m,j}, \sigma_{l_m,j}), (\mu_{i,l_1}, \sigma_{i,l_1}), \ldots, (\mu_{i,l_m}, \sigma_{i,l_m}))$$

is a Normal (Gaussian) distribution with mean and variance:

$$\begin{aligned} \mu_{i,j}^{new} &= \frac{\sum_{s=1}^{m} \frac{\mu_{l_s,j}}{(\sigma_{l_s,j}^2)} + \mu_{i,j}/\sigma_{i,j}^2}{\sum_{s=1}^{m} \left(\frac{1}{\sigma_{l_s,j}^2}\right) + 1/\sigma_{i,j}^2} \\ \sigma_{i,j}^{2\ new} &= \frac{1}{\sum_{s=1}^{m} \left(\frac{1}{\sigma_{l_s,j}^2}\right) + 1/\sigma_{i,j}^2} \end{aligned}$$

These values $(\mu_{ij}^{new}, \sigma_{ij}^{2\ new})$, along with $(\mu_{ij}, \sigma_{ij}^2)$ are easily updatable values that represent the continuous Gaussian version of the $(\alpha_{ij}\ ; \beta_{ij})$ and $(\alpha_{ij}^{new}, \beta_{ij}^{new})$ of the binary approach in (Buchegger and Boudec, 2002), as derived from the approach in (Josang, and Ismail, 2002). The network topology and protocols follow those of (Ganeriwal and Srivastava, 2004), (Srinivasan et al., 2006). 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 $\theta_{i,j}$, such that the prior trust is 0.5. 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 andσ_0. μ_0 is most likely to be set to 0. Therefore, σ_0 and *ε* determine each other. Once one is set, the other is automatically deducted. With a proper prior $\theta_{i,j} \sim N(\mu_0; \sigma_0)$, the reputation parameters are:

$$\begin{aligned} \mu_{i,j} &= \frac{\mu_0/\sigma_0^2 + \mu_{i,j}/\sigma_{i,j}^2}{1/\sigma_0^2 + 1/\sigma_{i,j}^2} \\ \sigma_{i,j}^2 &= \frac{1}{1/\sigma_0^2 + \sigma_{i,j}^2} \end{aligned}$$

and

$$\begin{aligned} \mu_{i,j}^{new} &= \frac{\mu_0/\sigma_0^2 + \sum_{s=1}^{m} \frac{\mu_{l_s,j}}{(\sigma_{l_s,j}^2)} + \mu_{i,j}/\sigma_{i,j}^2}{1/\sigma_0^2 + \sum_{s=1}^{m} \left(\frac{1}{\sigma_{l_s,j}^2}\right) + 1/\sigma_{i,j}^2} \\ \sigma_{i,j}^{2\ new} &= \frac{1}{1/\sigma_0^2 + \sum_{s=1}^{m} \left(\frac{1}{\sigma_{l_s,j}^2}\right) + 1/\sigma_{i,j}^2} \end{aligned}$$

7. Simulation and Results

In a simulated experiment, we calculate the trust between 4 nodes (5,8,9,15) in a network of 15 nodes, as shown in figure 2. First, we assume that all nodes are working properly and report the sensed event with minimum error, usually a reading error, the parameter b = 1.5 for multi path effect, and ε = 0.25 to calculate the direct trust. The initial trust is assumed to be 0.5. Simulation showed that the trust values of node 5 for the other nodes (8,9,15) are slightly different but almost the same, in both cases with and without second hand information (Figure 3 c). In other experiments, we assume that nodes 9 and 15 are faulty. The results of the simulation are presented in Figure 3 and showed the trust value for both nodes (15, 9) by node 5 dropped to zero. Node 8 is assumed reliable, and its corresponding trust value follows a growing path that eventually reaches 1.

Note that the trust without second hand information is labeled as (o), and the trust assessed using second hand information is labeled as (+). In the experiment of figure 4, we assume that node 5 is faulty. We exaggerated the experiment so that the changes are dramatic and can be seen without waiting too long. As can be seen, the trust value from the direct information reaches zero for both nodes 9 and 15. This is because node 5 is faulty, and therefore contradicts nodes 9 and 15 based only on direct information. However, using second information (+ in figure 4), the trust for these two nodes is high, leaving the two nodes to assess each other indirectly. This is a very interesting case again as both nodes (15, 9) are now assessing node 5 as a faulty node. The trust value for node 8 is set to the initial value 0.5 and will decrease to zero as there is no second hand information available to node 8. This last example shows precisely the reason the trust system is instituted. It allows the classification of nodes into separate sets according to their trustworthiness. In the last example, we do know that node 5 is faulty, since it is a simulation exercise. Results clearly should indicate to the network that node 5 is faulty. However, it could also be the case that the node 9 and 15 are malicious.

In comparison with work by Momani et al. (2007), the results of multipath fading channel don't show major difference that of (AWGN) as multipath fading can approximated as Gaussian for this particular scenario.

8. Conclusions

The trust system works on the assumption that the majority of nodes in a neighborhood are reliable. This principle helps purge the system of bad elements. In our case, we modeled trust in wireless sensor network taking into consideration the effect of multi path channel. Results show that the multi path can be approximated as Gaussian distribution when interacting with direct trust as well as the second hand information.

Corresponding Author:
Dr. Rami Al-Hmouz
King Abdulaziz University, Saudi Arabia
E-mail: ralhmouz@kau.edu.sa

Acknowledgements:

This article was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah. The authors, therefore, acknowledge with thanks DSR technical and financial support.

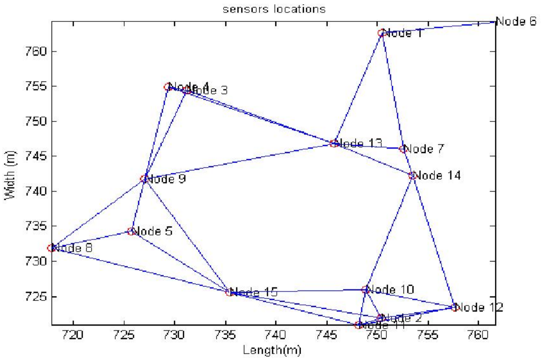
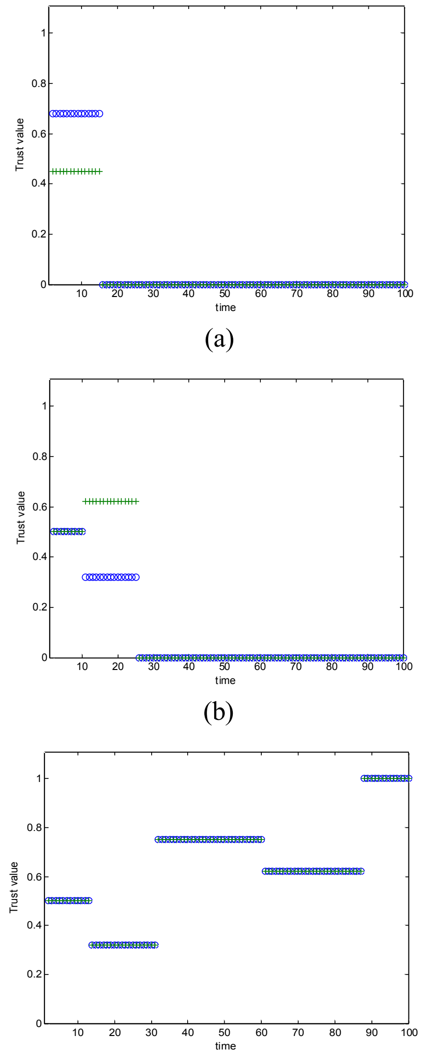


Figure 2: Wireless Sensor Network diagram

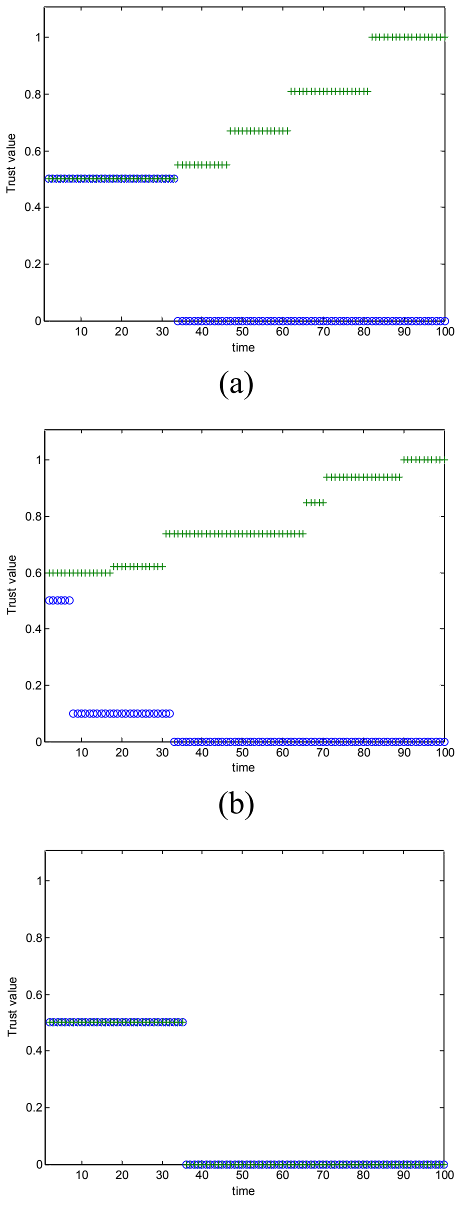


(a)

(b)

(c)

Figure 3: Trust values between node 5 (assuming 9 and 15 are faulty)and: (a) node 15, (b) node 9 and (c) node 8



(a)

(b)

(c)

Figure 4: Trust values between the faulty node 5 (assuming 9 and 15 are faulty) and: (a) node 15, (b) node 9 and (c) node 8

References

1. Akyildiz, I. F., W. Su, Y. Sankarasubramaniam and E. Cayirci. Wireless sensor networks: a survey. Computer Networks 2002: 38(4): 393-422.
2. Rajaravivarma, V., Y. Yang and T. Yang. An overview of Wireless Sensor Network and applications. Proceedings of the 35th Southeastern Symposium on System Theory, March 2003: 432-436.
3. Werner-Allen, G., K. Lorincz, M. Ruiz, O. Marcillo, J. Johnson, J. Lees, M. Welsh. Deploying a Wireless Sensor Network on an Active Volcano. IEEE Internet Computing, March-April 2005: 23 -25.
4. Culler, D. D., Estrin and M. Srivastava. Overview of Sensor Networks. Special Issue in Sensor Networks, IEEE Computer 2004: 37(8):41-49.
5. Glaser, S. D. Some Real-world Applications of Wireless Sensor Nodes. Proceedings of the SPIE Symposium on Smart Structures and Materials NDE, San Diego, CA, USA 2004.
6. Gao, T. D. Greenspan, M. Welsh, R. R. Juang and A. Alm. Vital Signs Monitoring and Patient Tracking Over a Wireless Network. Proceedings of the 27th IEEE EMBS Annual International Conference, September 2005: 102-105.
7. Alsaade, F. Proposing a Secure and Reliable System for Critical Pipeline Infrastructure Based on Wireless Sensor Network. Journal of Software Engineering 2011: 5: 145-153.
8. Stajano, F. Anderson R. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks wireless networks. 7th International Workshop on Security Protocols. 1999.
9. Wang, Y., Attebury, G. Ramamurthy, B. A survey of Security Issues in Wireless Sensor Networks. IEEE Communications Surveys & Tutorials 2006: 8(2):2-23.
10. Perrig, A. Stankovic, J. Wagner, D. Security in Wireless Sensor Networks. Communications of the ACM 2004: 47(6): 53-57.
11. Zaman, N. Jung, L. T. Alsaade, F. Alghamdi, T. Wireless Sensor Network (WSN): Routing Security, Reliability and Energy Efficiency. Journal of Applied Sciences 2012. Available: http://scialert.net/abstract/?doi=jas.0000.42944.42944.
12. Karlof, C. Wagner, D. Secure routing in sensor networks: Attacks and countermeasures. Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.
13. Bohge, M. Trappe, W. An Authentication Framework for Hierarchical Ad Hoc Sensor Networks. Wireless Security, Proceedings of the 2003 ACM workshop on Wireless security, San Diego, CA, USA, 2003: 79 - 87.
14. Karlof, C. Sastry, N. Wagner, D. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. Conference On Embedded Networked Sensor Systems, Proceedings of the 2nd International Conference on Embedded Networked Sensor sSstems, Baltimore, MD, USA, 2004: 162-175.

15. Momani, M. Challa, S. GTRSSN: Gaussian Trust and Reputation System for Sensor Networks Book Title: Advances in Computer and Information Sciences and Engineering. Springer Netherlands, 2008.
16. Momani, M. Aboura, K. Challa, S. RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks, The Third International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Melbourne, Australia, 2007:347-352.
17. Josang, A. Ismail, R. The beta reputation system. Proceedings of the 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 2002:618-644.
18. Dasgupta, P. Trust as a Commodity. In Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, chapter 4, 2000: 49-72.
19. Ba, S. Pavlou, P. A. Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior, MIS Quarterly 2002: 26: 243–268.
20. Marsh, S. Formalising Trust as a Computational Concept, Department of Computer Science and Mathematics, vol. PhD: University of Stirling. 1994.
21. Aberer, K.. Despotovic, Z. Managing Trust in a Peer-2-Peer Information System. In Proceedings of the Ninth International Conference on Information and Knowledge Management (CIKM2001), 2001.
22. Xiong, L. Liu, L. A reputation-based trust model for peer-topeer e-commerce communities”, IEEE conference on E-commerce, June 2003: 275–284.
23. Blaze, M. Feigenbaum, J. Ioannidis, J. Keromytis, A. RFC2704 - The KeyNote Trust Management System Version 2, 1999. available from: http://www.ietf.org/rfc/rfc2704.txt.
24. Michiardi, P. Molva, R. CORE: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, 2002:107–121.
25. Buchegger, S. Boudec, J. L. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, 2002: 226–236.
26. Srinivasan, A. Teitelbaum, J. Wu, J. DRBTS: Distributed Reputation based Beacon Trust System. The 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC06), Indianapolis, USA, 2006.
27. Ganeriwal, S. Srivastava, M. Reputation-based framework for high integrity sensor networks. Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN 04), 2004:66-7.
28. Lindley, D. V. Singpurwalla, N. D. Reliability (and Fault Tree) Analysis Using Expert Opinions. Journal of the American Statistical Association, 1986:81(393): 87–90.
29. West, M. Bayesian Aggregation. Journal of Royal Statistical Society Series A, 1984: 147: 600-607.
30. Shafer, G. A mathematical theory of evidence, Princeton University, 1976.

9/21/2013