Trustworthiness assessment of cow behaviour data collected in a wireless sensor network

L. Gomez[1], R.M. de Mol[2], P.H. Hogewerf[2] and A.H. Ipema[2]
[1] *SAP Research France, Sophia Antipolis, France*
[2] *Wageningen UR Livestock Research, P.O. Box 65, 8200 AB Lelystad, The Netherlands*
rudi.demol@wur.nl

Abstract
Wireless sensor networks can be used for automated cow monitoring, e.g. for behaviour and locomotion monitoring. Sensor data should only be used when they can be trusted. The trustworthiness of sensor data can be assessed in a framework, from the acquisition at the node to their delivery to business applications, including any intermediary routing and processing. The trustworthiness assessment method has been evaluated with sensor data collected during one of the experiments within the WASP project. Sensor data are not trusted when the trustworthiness gets below a threshold. An alert is generated then and it is possible to find the cause by tracing back the trust of composing elements. The trustworthiness assessment method results in the detection of problems with nodes (e.g. detached node or exhausted battery). Most of these problems can be classified as true and most of them were not notified on the farm. Therefore trustworthiness assessment is worthwhile to improve automated cow status monitoring.

Keywords: Wireless Sensor Networks, behaviour, dairy cows.

Introduction

Application of wireless sensor networks (WSN) is a new method to collect data that can be used for automated cow monitoring (Wang *et al.*, 2006). The application of WSNs is especially useful for behaviour and locomotion monitoring. Sensor data should only be used when they can be trusted. Trustworthiness is defined as the probability that sensor data really corresponds to the measurement in the physical world. Sensor data may be erroneous due to intentional misbehaviour and unintentional errors. Intentional misbehaviour is expected to be less relevant in cow monitoring applications. Unintentional errors are caused by malfunction of the hardware (broken or obstructed sensors), mispositioning of the node (untied or incorrectly attached node) or exhausted battery (Gomez *et al.*, 2010).
The trustworthiness of sensor data can be assessed in a framework, from the acquisition at the node to their delivery to business applications, including any intermediary routing and processing (Gomez *et al.*, 2009).
Possible applications of WSNs have been investigated in the Wirelessly Accessible Sensor Populations (WASP) project (www.wasp-project.org). One of the applications was 'Detection of health problems with focus on claw health and locomotion' (De Mol *et al.*, 2007, *Lokhorst et al.*, 2008). The trustworthiness assessment using the framework has been evaluated with sensor data collected during one of the experiments within the WASP project.
In this paper the focus will be on the evaluation results. The framework will be described in short, as well as the experimental conditions.

Material and methods

The trust model

Three states are identified in the sensor data life cycle (for a more detailed description see (Gomez *et al.*, 2010): raw, routed and processed (Figure 1). A sensor produces raw data. The data is processed by data manipulation such as filtering, fusion or aggregation. The data is routed when it is sent to another node in the network (or delivered to the business application). There are specific trust assessment mechanisms for each state:

- for raw data it is based on the trustworthiness of several available attributes (e.g. node battery level and measurement accuracy);
- for routed data it is based on the trust relationship between the sender and the receiver;
- for processed data it depends on the information used for the processing mechanism, that is the type of processing services and the input sensor data used.

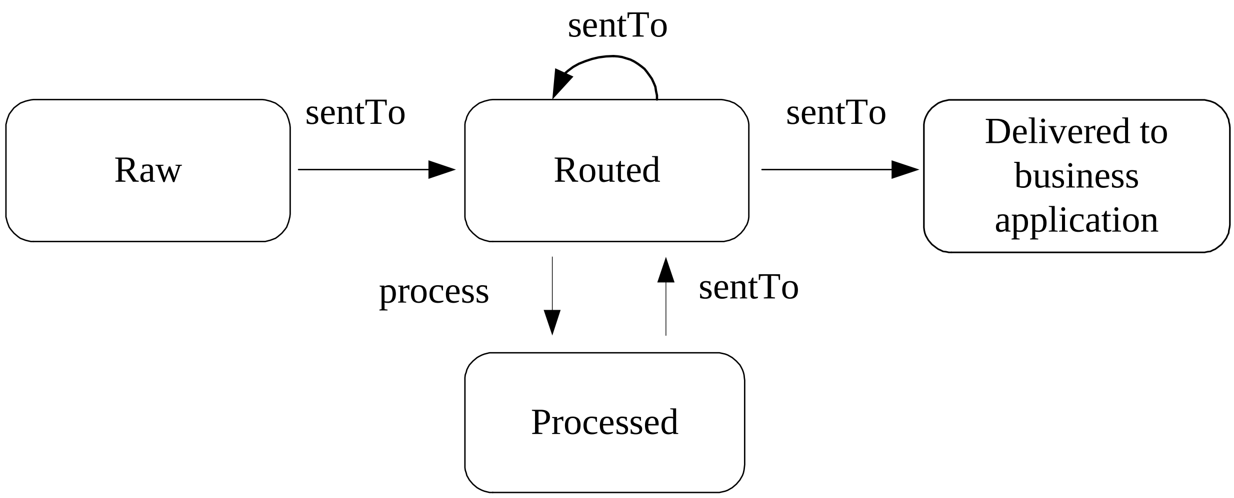

Figure 1. Sensor data life cycle, figure reproduced from Gomez et al. (2010).

In Gomez *et al.*, (2010), the trustworthiness is formalised as the opinion in the theoretical framework of subjective logic, based on Dempster-Schafer theory of evidence (Josang, 2001). An opinion is a 4-tuple (b, d, u, a) where b represent belief, d disbelief, u uncertainty and a the a priori probability. The range of all four values b, d, u, a is [0, 1] and b + d + u = 1. The subjective logic framework provides a set of operators for combining opinions. Gomez *et al.* define operators to evaluate the trust in sensor data attributes and a combine operator to determine the overall trustworthiness of sensor data.

Attributes of the raw data are battery and value. The battery operator is used to asses the trust in a battery given the current battery level. The trust decreases as the battery level decreases. The trust is always lower than the battery level and the difference depends on a parameter in the battery operator model.

The value operator is used to determine the trustworthiness of the sensor value. The trust decreases when an abnormal sensor data value is detected, based on the difference with the forecasted value found (e.g. with exponential smoothing). A sudden change in the measurement results in a decrease in the trust.

Gomez *et al.* (2010) also define a combine operator that fulfils the following requirements:

- a combination of close opinions is rewarded, it results in an increase of opinion;
- a combination of distant opinions is penalized.

The combine operator is based on formulas for combined belief and combined uncertainty of the underlying opinions. The same operator is used for raw and processed data.

Experimental conditions

In de Mol *et al.* (2009), the authors monitored daily behaviour of dairy cows during 50 days. The goal of this experiment was to evaluate in real-time the health and well-being status of cows, indoor and outdoor. The cows were indoor the first 36 days, and had access to pasture the last 14 days. Six cows were equipped with two tilt sensors to measure the acceleration in X and Y direction of their neck and right hind leg every half a minute (Figure 2). Each sensor device on the cow represents a mobile node in the network. Based on calibration measurements, raw acceleration from neck and leg were processed in order to determine cow behaviour (e.g. standing, lying). Applied to this scenario, our approach enables farmers to evaluate the trustworthiness of cow's acceleration and derived cow behaviour, which is the trustworthiness of the calculated lying and standing behaviour. Abnormal status should be detected at an early stage. In this scenario, erroneous acceleration is due to multiple factors (e.g. detached nodes, exhausted battery). During the experiment, few nodes have been detached from the cow, and found in the pasture. Farmers recorded in a logbook different events occurring to the nodes (see Table 1). The trustworthiness assessment should make it possible to detect in real-time such events. The value of trustworthiness assessment follows from the impact of erroneous data on the processing over cow activity.

Figure 2. Node attached to the leg (in circle in left picture) and node attached to the back of the neck (in ellipse in right picture).

Table 1. Description of events in the logbook during the first month of the experiment.

Date	Description of event
May 7, p.m.	Nodes allocated to cows
May 7, p.m.	Node 3 (Cow 428) replaced by Node 5
May 9, a.m.	Node 5 at the inner side of the leg of Cow 428, node turned back
May 9, a.m.	Node 15 detached and found by a farm worker, attached again to Cow 507
May 14, p.m.	Node 5 at the inner side of the leg of Cow 428, node turned back
May 14, p.m.	All nodes with transmission problems were restarted and attached again to the cows
May 14, p.m.	Node 7 detached and found in the feeding passage, attached again to Cow 74
May 20, p.m.	Node 4 replaced by node 1 on Cow 445

Results

<u>Worked-out example of one event</u>

The trustworthiness was calculated for the six cows during the experimental period. The data should not be trusted when the trustworthiness is below a threshold. The cause of such incidents can be tracked by following the trustworthiness assessment in the opposite direction:

- the trustworthiness per cow is a combination of the trustworthiness per node of that cow;
- the trustworthiness per node is a combination of the trustworthiness of acceleration X and acceleration Y;
- the trustworthiness in acceleration X (or Y) is a combination of the trustworthiness of value and battery.

For example a drop in the trust of a battery will give a trust decrease of the acceleration, and subsequently a trust decrease for the node and the cow.

Some results of Cow 507 are given in Figure 3 through 12 to illustrate this. The trust evaluation of Cow 507 during the first month in the experiment is shown in Figure 3. Drops in trust occur on May 9, May 11 and May 19. The first drop coincides with an event mentioned in Table 1. The trust in Cow 507 is based on the acceleration trustworthiness on Node 10 and 15; these are depicted in Figure 4 and 5.

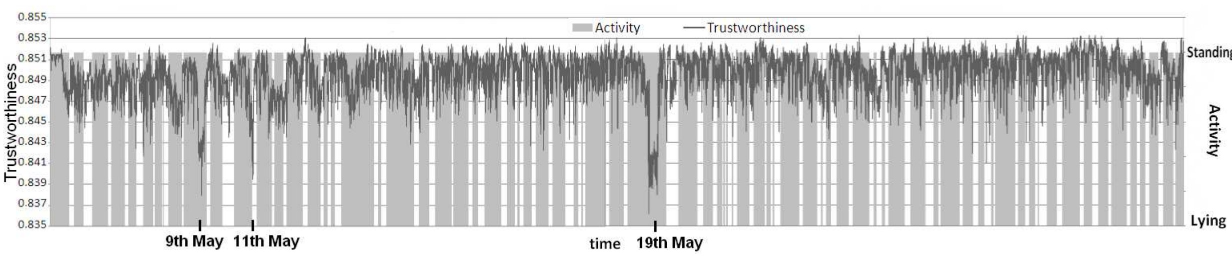

Figure 3. Trustworthiness evaluation and activity of Cow 507 during the month of May 2008.

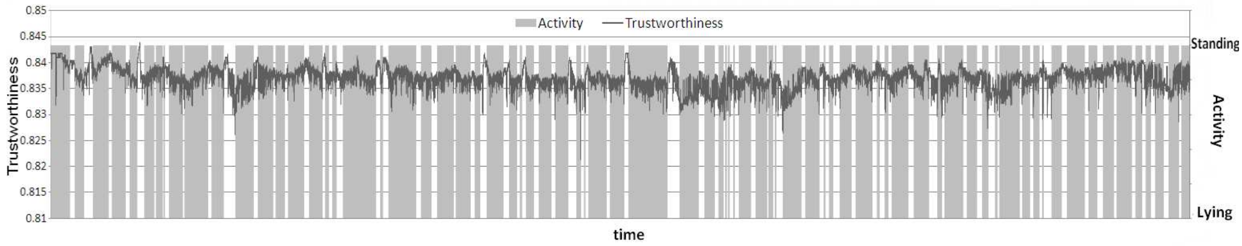

Figure 4. Trustworthiness evaluation and activity of Node 10 (attached to the right hind leg of Cow 507) during the month of May 2008.

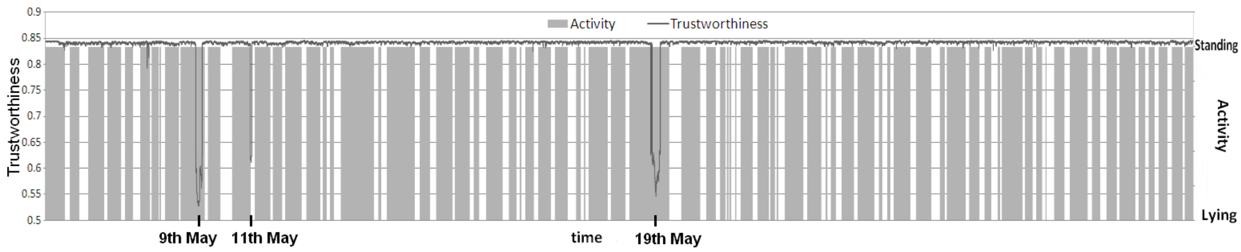

Figure 5. Trustworthiness evaluation and activity of Node 15 (attached to the neck collar of Cow 507) during the month of May 2008.

The trustworthiness around the third drop (May 19) is depicted in Figure 6 (trust of Cow 507), and the trust evaluation of Node 10 and Node 15 in the same period is shown in Figure 7 and 8. The trust in Node 10 remains at the same level, around 83%. Apparently the drop is caused by the drop in trust for 15 (below 55%, Figure 8). The trust in Node 15 is a combination of the trust in acceleration X and acceleration Y of Node 15. Therefore this is worked out further in Figure 9 and 10 where the trust evaluation around May 19 of acceleration X and Y of Node 15 are shown. The trust in Y (Figure 10) is decreasing which can be explained by a decrease in trust in the value of Y acceleration (Figure 11) while the trust in battery remains roughly at the same level (Figure 12). The trust in Y values gets below 20%; and the cause for this drop is unknown as there is no event given in the logbook on that date.

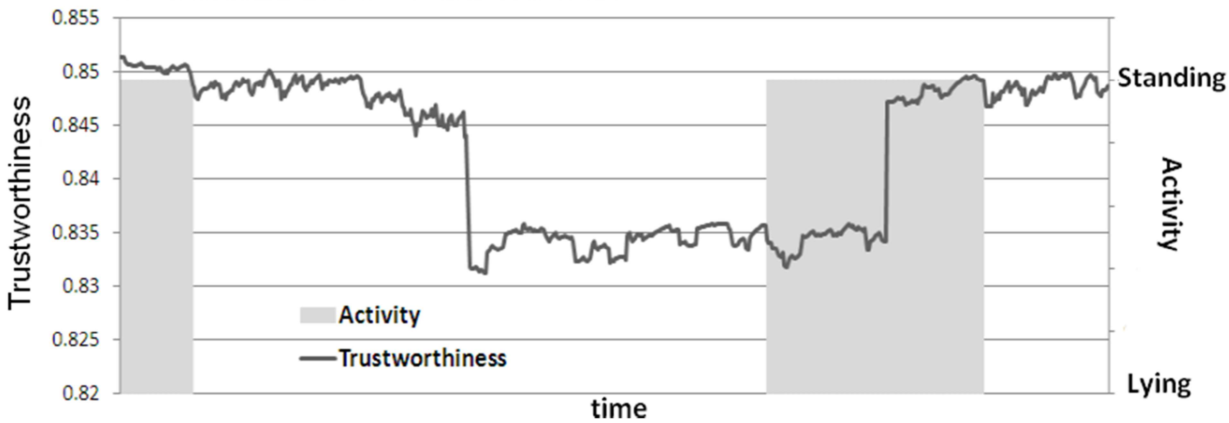

Figure 6. Trustworthiness evaluation and activity of Cow 507 around May 19.

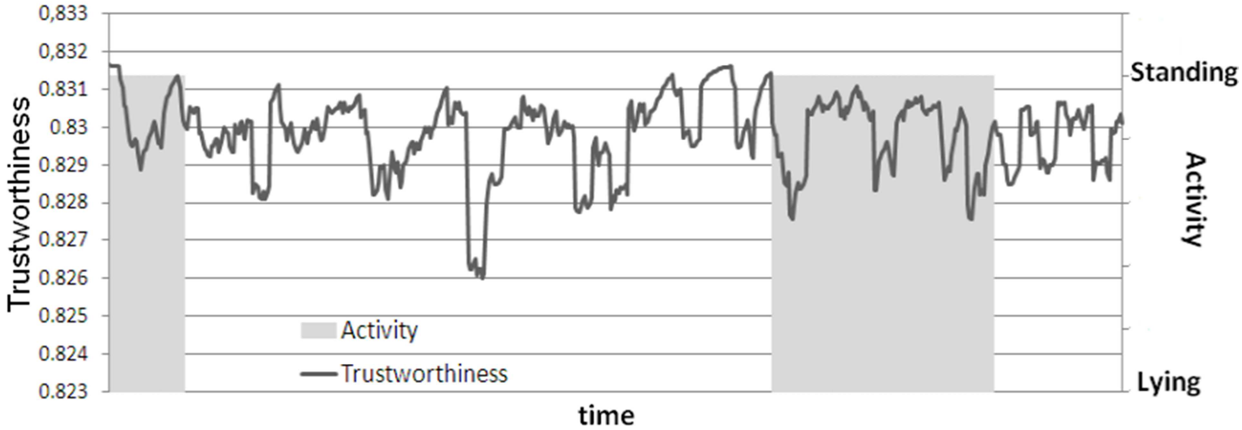

Figure 7. Trustworthiness evaluation and activity of Node 10 (attached to the right hind leg of Cow 507) around May 19.

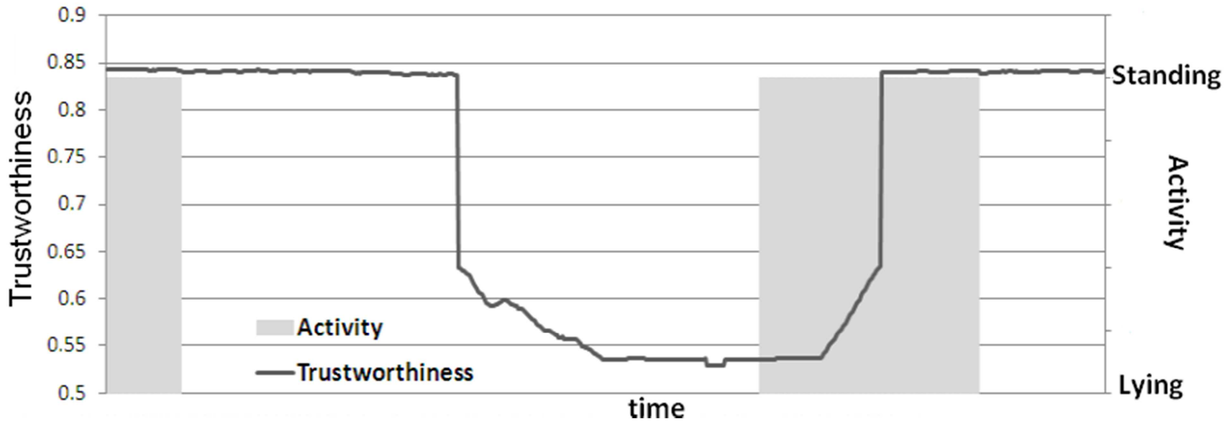

Figure 8. Trustworthiness evaluation and activity of Node 15 (attached to the neck collar of Cow 507) around May 19.

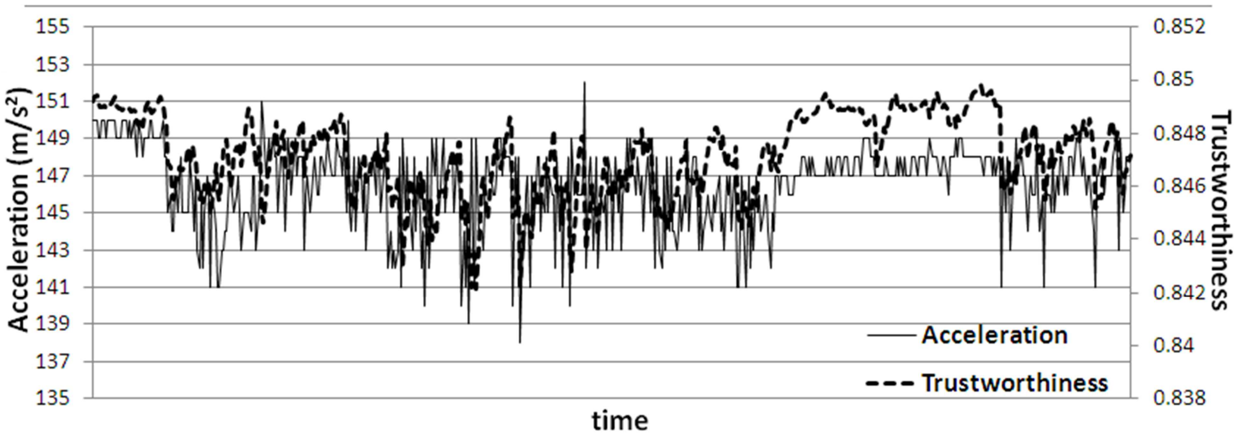

Figure 9. Acceleration and trustworthiness evaluation of acceleration X on Node 15 (attached to the neck collar of Cow 507) around May 19.

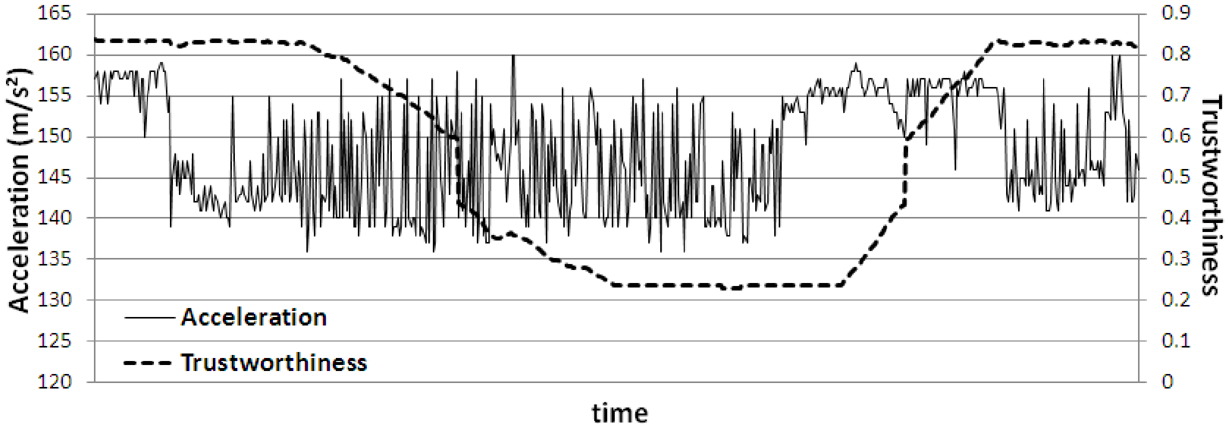

Figure 10. Acceleration and trustworthiness evaluation of acceleration Y on Node 15 (attached to the neck collar of Cow 507) around May 19.

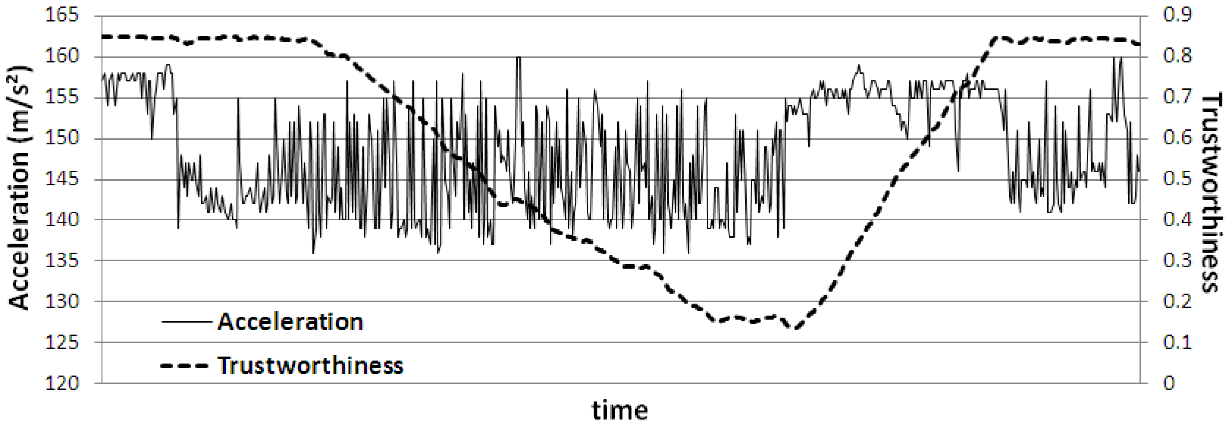

Figure 11. Acceleration and trustworthiness evaluation of acceleration Y value (left) and battery level (right) of Node 15 (attached to the neck collar of Cow 507) around May 19.

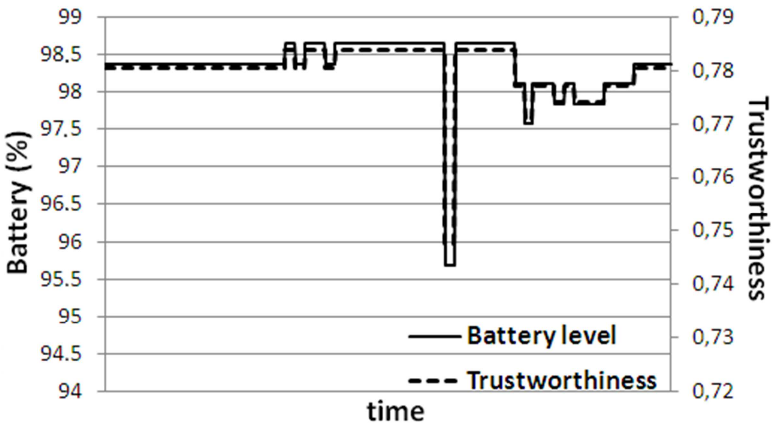

Figure 12. Battery level and trustworthiness evaluation of battery level of Node 15 (attached to the neck collar of Cow 507) around May 19.

In general, measured acceleration values and battery levels are used to calculate the trust in X or Y acceleration, both are combined for the trust in a node. The trust in both nodes is combined to get the trust per cow. This also works the other way round: when the trustworthiness is decreased for a cow, the cause can be detected by following the mechanism backwards.

Experimental results

Fifteen nodes have been used in the experiment to measure the behaviour of the six cows. Six nodes have been discarded for the trustworthiness analysis because they did not produce enough data. Three nodes did not produce any abnormal measurements. On the remaining six nodes, 73 events have been detected by the trust model (based on a threshold 83.5% for trustworthiness). On the farm only 19 events have been recorded in the logbook (Table 1), that is one out of four events was also detected by the farmer.

Whenever an incident occurs, (e.g. detached node, out of battery), it is important to consider three phases:

(i) the time when the problem occurs;
(ii) the time when the farmer detects the problem (reaction time);
(iii) the time when the farmer fixes the problem and everything goes back to normal (response time).

The trustworthiness model detects an event when the trust gets below a threshold. The higher the threshold, the more events will be detected. An event is classified as False Positive when the trustworthiness does not get below 40%. For the 85.5% threshold 73 events were detected, 10 of these 73 events were FP (14%). Results for other thresholds are included in Table 2. A higher threshold results in decreased reaction time as the alert will be generated earlier. But it is also more likely that the alert is FP (when the trust deceases but not far enough). Therefore a higher threshold is not attractive as the number of FP alert increases strongly.

Table 2. Event detection results for three threshold levels.

threshold	83.5%	84.0%	84.5%
average reaction time (min)	20.0	12.5	7.5
percentage of false positives	14%	40%	88%

Discussion

The results of the trustworthiness assessment depend on the threshold setting. It may be worthwhile to adapt this threshold automatically based on the generated results (true positives vs. false positives based on the minimum trust level reached per event).

It is assumed that intentional misbehaviour is not an issue in automated cow status monitoring. Otherwise the method should be adapted to detect such cases.

There might be some overlap in the results of trustworthiness assessment and the results of automated detection as both are looking for deviating measurement values. In trustworthiness assessment values are deviating when they cannot be trusted any longer. In automated detection values are deviating when the cow's behaviour is different because of a case of illness or oestrus. Alerts from the detection model should be generated when the values are deviating (higher temperature, lower milk yield) but still trusted. Values are not trusted when they are outside the acceptable range. In practice these alerts might be combined because in both cases the farmer should inspect the cow or the cow's nodes.

Conclusions

Measured values should only be used in business applications when they can be trusted. Therefore a method for trustworthiness assessment as described in this paper is worthwhile. Erroneous sensor data hamper automated cow status monitoring. Trustworthiness assessment is useful for data collection in WSN because erroneous data is detected and should not be used as input for the detection model. This will lead to a lower number of false positive alerts. It is possible to find the cause of the problem (e.g. defect sensor or flat battery) by analysing the drop in trustworthiness backwards in the trustworthiness assessment procedure.

Acknowledgements

This work was partially financed by the European Commission under the Framework 6 IST Project Wirelessly Accessible Sensor Populations (WASP).

References

de Mol, R.M., Bleumer, E.J.B., Hogewerf, P.H., A.H.Ipema, 2009. Recording of dairy cow behaviour with wireless accelerometers. In: Lokhorst, C., Koerkamp, P.W.G.G. (Eds.), 4th European Conference on Precision Livestock Farming, Wageningen. Wageningen, pp. 349-356.

De Mol, R.M., van Eijk, O.N.M., Goense, D., Hogewerf, P.H., Ipema, A.H., Lokhorst, C., Frumento, E., Mazzu, M., Wells, H., Savio, W., Wrona, K., 2007. WASP, Scenario choice, Deliverable 6.1.

Gomez, L., Laube, A., Sorniotti, A., 2009. Trustworthiness assessment of wireless sensor data for business applications. In: Proceedings - International Conference on Advanced Information Networking and Applications, AINA. pp. 355-362.

Gomez, L., Gentile, X., Riveill, M., 2010. Trustworthiness assessment of sensor data: evaluation. In: IFIP NTMS’11

Josang, A., 2001. A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems 9, 279-311.

Lokhorst, C., de Mol, R.M., Wells, H., Mazzu, M., Frumento, E., Corongiu, A., Savio, W., Ipema, A.H., Sorniotti, A., Gomez, L., 2008. WASP, Specified application requirements and prototype selection, Deliverable D6.2.

Wang, N., Zhang, N., Wang, M., 2006. Wireless sensors in agriculture and food industry - Recent development and future perspective. Computers and Electronics in Agriculture 50, 1-14.