ICT YOUNG 2012

TRUST MANAGEMENT IN WSN – CASE STUDY EVALUATION

Janusz Górski[1], Alan Turower[1]

[1]Gdańsk University of Technology, Faculty of Electronics, Telecommunications and Informatics, Department of Software Engineering

Abstract

The paper presents a case study related to WSN application in the e-health domain. It was assumed that the network implements the method of distributed trust management which leads to detection and isolation of sensors violating the network policies. To measure the effectiveness of such detection a set of metrics was derived in a systematic way, using Goal-Question-Metrics approach. The network was simulated with the help of a dedicated simulator and the resulting data were used to obtain values of the metrics which demonstrate how effectively the broken nodes are eliminated from the network.

1. INTRODUCTION

Wireless sensor networks (WSN) increase their role in application areas with high dependability expectations, including healthcare, transport, environment monitoring and others. Sensor nodes are distributed, (often) mobile and subjected to severe limitations of their resources which call for specialized, resource-economic solutions addressing various aspects of network dependability.

To cope with this problem we proposed a distributed trust management model that provides uniform distribution of the responsibility for trust assessment and related decision making [1, 2]. Such decisions can eventually lead to exclusion of the untrustworthy nodes from the network. A dedicated simulator provides for experimenting with this model with respect to wireless sensor networks of different size and topology.

The objective of this paper is to introduce a set of metrics targeted at evaluating the effectiveness of the proposed trust management method. First we explain how we used the common Goal-Question-Metrics (GQM) methodology [3] to select a set of metrics. Next, we present a case study where our trust management method is applied. Network simulator is applied to investigate network behaviours and the set of selected metrics is used to assess the effectiveness of our trust management method in removing broken nodes from the network.

2. RELAED WORKS

Different approaches to assess effectiveness of detecting and removing distrusted nodes have been proposed so far. It implies the results are often incomparable.

Zia [4] in the experiments uses nodes, that transfers one packet every *n* seconds. When a node receives a packet not intended for it, it first checks the destination to see whether it is for one of the neighbouring nodes. If not, it discards the packet. Time (in seconds) needed to detect all distrusted nodes is used to assess the method effectiveness.

Momani et al. [5] do not precisely describe their experiments conditions. To assessment and comparison their method they use the change of trust value between two observed nodes in time. However, this measure is relative, non-general and enforces the knowledge about the two observed nodes.

Maroti et al. [6] examine the number of errors in a period of time and create histograms using real time of simulation.

Also Loscri et al. [7] use the real time in their simulation experiments. They present numbers of nodes (e.g. alive nodes) or amounts of data (sent / received) in a period of time. They also use other metrics not connected with time, e.g. number of nodes in number of data signals.

In comparison, Heinzelman et al. [8] measure numbers of nodes in time steps (simulation rounds), as called *system lifetime*.

Interesting metrics are used by Handy et al. [9]. They introduce three metrics: *First Node Dies* (FND), *Half of Nodes Alive* (HNA) and *Last Node Dies* (LND). These metrics are used to measure energy usage. The results are presented in simulation rounds.

Our approach differs from the above in that our metrics allow to measure effectiveness of nodes detection in wide context and asses many aspects. Moreover our metrics can be used both in simulator experiments (measurement in simulator turns) as well as in laboratory experiments (measurement in real time).

3. CASE STUDY – PATIENT IN HOME ENVIRONMENT

Health care is an important area of WSN application. There are many benefits that can be achieved such as freeing the patient from uncomfortable wires what make him/her feel better or treating easier sick patients at their homes, thus reducing the cost of medical care and causing less stress to patients.

Example use of WSN in the patient's home was presented in the demonstration scenario of the ANGEL project [10]. Illustrative representation of this scenario is shown in Figure 1.

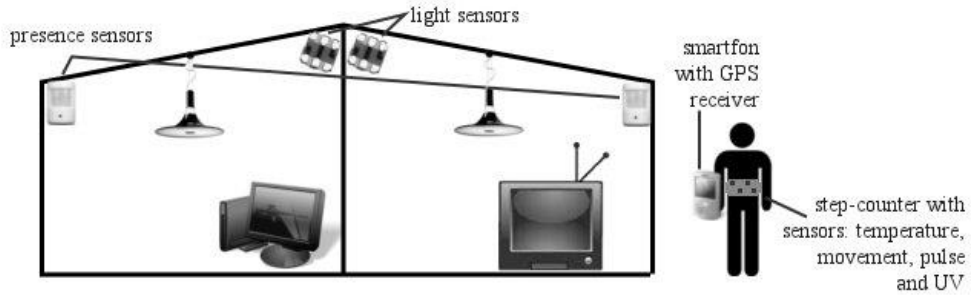

Fig.1. Patient in home environment

Bob has bought the Angel platform, and owns a TV set and a mobile phone, both acting as an Angel compliant Gateway. Bob wants to keep his ideal weight, but the results

achieved so far with different diets where not completely satisfactory, because anyway he has a tendency to gain weight during autumn, while during spring he cannot fully recover his shape. So every year he accumulates some kilos that he is not able to lose.

When Bob went to a healthcare professional to have assistance on his diet he has been told that he could have been easily supported by the Angel Platform. Through this platform, indeed, he can benefit of a Light Therapy service and of a Training Monitoring service. To follow the Light Therapy, Bob buys some wireless light sensors and special wireless lamps, all compliant with the ZigBee Home Automation Profile [11]. Bob needs just to place the devices in his house where he prefers.

Now Bob is ready to use the platform. In particular during winter and autumn, at wakeup moment the lights of the house, in the room that Bob occupies, are set to simulate the dawn with the time and speed of the summer season. If Bob changes the room during the simulated dawn the light follows him in the different rooms of the house.

To be supported in doing his physical exercises, Bob bought also a special step-counter, which embeds also a movement and UV (Ultraviolet) sensor, able to detect whether Bob is exercising indoor or outdoor. Considering in fact that Bob wears his step-counter all day long, not all the activities measured by the Step-Counter are real exercises, some of them are just steps done during the daily life (i.e. from one room to another, stairs etc.).

After the initial configuration, Bob can live his normal life, bringing always with him his step-counter. If Bob wants to, he can connect to a web site and design a training plan that he is willing to follow, or he can eventually ask to a professional to fill it for him (i.e. the personal trainer, the nutritionist, the doctor etc.). The platform can send some messages to Bob to remind him to follow his exercises, as well as some messages of positive or negative feedbacks about the compliance with the decided plan.

The step-counter is worn by Bob during the whole day and always sends the training data to the gateway owned by Bob, transparently to the user. If during an outdoor training session a heart attack is identified, using temperature, movement and pulse sensors in step-counter, the platform will immediately notify the emergency and inform about the whereabouts of Bob using data from the GPS receiver in Bob’s smartfon.

The solution adopted in the project ANGEL consists in the fact that Bob is able to transfer to the platform information about the context in which it currently is (called *profile*) [12]. Based on this information platform reveals or hides the data which appearing could prejudice the privacy of Bob. For example data on health status are displayed on the TV screen, which is located in the home, if Bob chooses profile "I'm alone". However, when he selects "I'm with friends", the screen shows only the information about the environmental conditions in his apartment, and health status information is hidden. Bob is also able to authorize devices other than its own TV and a smartphone – for example he can redirect the data to Sarah's TV, if he is in her house.

The entire platform consists of multiple cooperating sensors. Creating such a platform using wired sensors would not be possible. However, use of WSN enters a number of requirements, e.g. sensors must be small enough not to affect the comfort and be energy efficient to avoid the frequent battery replacement. The range of radio signal from the sensors is also restricted.

4. DISTRIBUTED TRUST MANAGEMENT

Trust management models are becoming popular, because they offer uniform distribution of the responsibility for trust assessment and related decision making. They allow reducing expensive data transmission and using fewer resources than cryptographic calculations.

Our model [1, 2] assumes that each node in the network evaluates trust to other nodes. The network is composed of clusters and has tree structure. There are three types of nodes:

— *sink* – a node with significant computational capabilities, connected to a constant energy source, which processes all received data;
— *leaves* – nodes, which main task is to measure and send the measured data;
— *routers* – nodes, which in addition to measurement and sending of measured data also forward data from leaves that are too far from the sink.

The nodes from a cluster communicate among themselves and with the cluster head creating the lower tier. The sink and the heads of the clusters form the higher tier of the network. We propose a mechanism which enables each node to make autonomous decisions about trust based on its own experiences and the trustworthiness assessments. We assume that all nodes cooperate in evaluation of trust. The objective of the trust management system is to distinguish between trustworthy network nodes and untrustworthy ones. Then the untrustworthy nodes can be excluded from the network.

A node has two roles in the network – for outgoing communication other nodes judge if it can be trusted; for incoming communication, a node makes a real-time decision if the sender can be trusted. We assume that sink is always trustable as long as it is available.

Decision about trust is based on two factors:

— evidence about trustee's conformance to agreed security policies;
— the evidence resulting from the recommendations received from the neighbour nodes (reputation).

Depending on the result of trustworthiness assessment, the node can proceed with message processing and raise reputation of the trustee or discard the message and decrease the reputation of the trustee.

Each new node receives a *neutral level* of reputation – the other nodes do not have any information relating to his reputation yet. Then, depending on his behaviour, its reputation may change. If the reputation value falls below the *cut-off point*, the node is seen as unreliable and messages received from that node are discarded without verification of their compliance with the policy of the network. Depending on the nodes' trust also routes of messages are changed so that data is not transmitted by distrusted nodes. If the reputation of a node falls below the cut-off point, it cannot regain trust, unless by special recovery procedure (this could include, for example, manual inspection of the node, its replacement, etc.).

Below we present two sample scenarios that demonstrate the usefulness of trust management in this system.

4.1. Unfair services supplier

Bob may want insert to the system another device, or to add new services to existing ones. There is a risk that software embedded in such new device could have a harmful effect on the system, and thereby endanger the health and, in extreme situations, even the

Bob's life. With some level of authorization the new could also have access to Bob's personal information which could lead to violation of Bob's privacy. However, with the trust management functionality on, if the device attempts to perform actions not permitted by its role and / or prohibited by the network policies and this fact is detected by other nodes, its trustworthiness in the eyes of its neighbours will drop down and consequently the device will be excluded from the network. Adequate notice may be sent to the sink and then appears on Bob's interface, so he quickly learns about the risk associated with the new device.

4.2. Broken nodes

A sensor can fail and stop transferring data or it transmits incorrect data. Lack of transmission can be detected relatively easily. We assume that the network nodes are equipped with testing capabilities sufficient to detect incorrect data before the data reaches the sink of the network. As a result the sender's trustworthiness will be reduced what can eventually result in cutting the source of incorrect data off. For example, if the light sensor sends information about light intensity exceeding the values set in the network policy, it will be detected before the lamps in Bob's apartment are set incorrectly. Adequate notice sent to the sink and displayed on the TV or on Bob's smartphone will result in initiating some repair action. The data from the failed sensor will be blocked until the repair is performed and the repaired sensor restores its trust in the network.

5. OBTAINING THE METRICS SYSTEM

A set of metrics to assess effectiveness of the trust management method was identified using the Goal-Question-Metrics (GQM) methodology [3]. GQM offers systematic approach which allows obtaining a set of metrics starting from an explicit statement of a measurement goal. Next, there is the intermediate layer of questions, which links the goal and metrics. Answering these questions helps to decide which metrics support the stated goal.

We defined the overall goal of our experiment as follows:

Analyze WSN trust management method applied in the case study for the purpose of improvement with respect to effectiveness of broken nodes detection without isolating properly working nodes.

At lower decomposition level of GQM, the following questions were identified:

— Q1: What is the effectiveness of broken nodes detection?
— Q2: What is the effectiveness of detecting broken nodes without isolating properly working nodes?

The third level of GQM decomposition involves identification of metrics which are used to answer a particular question. The metrics answering the questions are given in Table 5.1.

Table 5.1

Metrics associated with questions Q1 and Q2

Question	Metric name	Metric description
Q1	First Node Detected (FND)	Number of simulation rounds needed to detect the first broken node
	All Nodes Detected (AND)	Number of simulation rounds needed to detect all broken nodes
	Cut-off Quality (CQ)	Inverse of the distance (measured as the number of intermediate router nodes) from detected node to the detecting node (1/distance)
Q2	Orphans Number (ON)	Number of nodes which detected a broken node, but are not able to send proper information to the sink, because the only route to the sink is through the node assumed as distrusted.

All metrics are expressed in numeric values; FND, AND and ON as integers and CQ as a real number between 0 and 1. We assume a node as *detected* when one of its routers (or the sink) considers it as untrustworthy (so information about detection can be send to the sink).

6. MEASURING THE TRUST MANAGEMENT EFFECTIVENESS

In the previous papers [1, 2] we presented the proposed trust management model and the related WSN simulator together with some simulation results In this section we give the results related to simulations of the scenario described above. We assume that the network consists of 20 nodes. Some nodes cannot send their data directly to the sink and have to use other nodes as routers. The distances between nodes vary from a few centimetres to several meters. The whole network is divided into four clusters. Bob's smartphone is the sink. It is assumed that the network covers a square ***S*** with dimensions 30 × 30 meters.

In the simulator, time is measured in *simulation rounds*. During one round, each node asynchronously:

- sends a message to the sink,
- forwards messages received from other nodes (if it is a router),
- receives a message broadcasted by the sink,
- updates its local data related to trustworthiness assessment of other nodes.

We assume that the range of each node does not exceed 10 meters (the sensors are communicating using ZigBee protocol [13]). We also assume that the sink is in the middle of ***S***.

Under these assumptions, we conducted two experiments:

EI: new nodes are inserted to the network sending data that do not conform to the network policies;

EII: some nodes already in the network are damaged.

For each experiment, we distinguished the following three cases:

C1: a leaf from some cluster is broken;

C2: a cluster-head and a leaf from another cluster are broken;

C3: a cluster-head and two leaves from another cluster are broken.

During the experiments it was assumed that the messages that do not conform to the network policy are 70% of the transmission from broken node, and every other node can send broken message with a 2% probability (due to the possible transmission errors). In each simulation round the sink broadcasts a message to all nodes in the network. Initially, all nodes are considered to be fully trustworthy. In experiment EI, broken nodes start with initial trust equals half of the full trust and in the experiment EII damaged nodes start with initial trust equals full trust.

Table 6.1 shows the results of the experiments. All results are the average taken from 100 simulations. In all simulations the distribution of nodes remains unchanged.

Table 6.1

Experiments results

Experiment - case	FND	AND	CQ	ON
EI-C1	5	5	1	0
EI-C2	1	6	1	0
EI-C3	2	6	0,92	0,01
EII-C1	12	12	1	0
EII-C2	2	16	1	0
EII-C3	3	13	0,9	0,14

Table 6.1 shows that the broken nodes cumulated in one cluster (case C3) slightly influence the quality of trust management detection – not all nodes were detected by their nearest neighbours (in router hops) and therefore some orphans occurred in the network. Table 6.1 also shows that a broken cluster head can be detected fast, because it sends (forwards) multiple messages during each simulation round.

7. CONCLUSIONS

In the paper we presented a scenario of wireless sensor network application in the e-health domain and considered two associated threat scenarios. We explained how the resulting risks can be mitigated by applying the trust management mechanism proposed in [1, 2]. To measure the effectiveness of broken nodes detection and isolation we selected a set of metrics, following the GQM approach [3], which seems to be a useful method of sufficient deriving metrics in a systematic way. A series of experiments was performed during which we used a dedicated simulator to investigate network behaviours. The data resulting from these experiments were used as an input to our metrics. The results show that detecting a single broken leaf node is much slower than detecting a cluster head. Moreover if there are more broken nodes in one cluster, the trust management mechanisms can cause some orphan nodes appear.

BIBLIOGRAPHY

[1] Górski J., Turower A., Wardziński A.: *Distributed Trust Management Model for Wireless Sensor Networks*, Sixth International Conference on Dependability and Computer Systems DepCoS-RELCOMEX, 2011
[2] Górski J., Turower A.: *Two-tier distributed trust management model for wireless sensor networks*, Forum Innowacji Młodych Badaczy, 2011
[3] van Solingen R., Berghout E.: *The Goal/Question/Metric method: A practical guide for quality improvement of software development*, McGraw-Hill Publishing Company, England, 1999
[4] Zia T. A.: *Reputation-based Trust Management in Wireless Sensor Networks*, International Conference on Multimedia and Ubiquitous Engineering, 2007, pp. 603-607
[5] Momani M., Challa S.: *Trust Management in Wireless Sensor Networks*, proc. of 5th ACM Conference on Embedded Networked Sensor Systems, 2007
[6] Maroti M. et al.: *The Flooding Time Synchronization Protocol*, proc. of 2nd ACM Conference on Embedded Networked Sensor Systems, 2004
[7] Loscri V. et al.: *A Two-Levels Hierarchy for Low-Energy Adaptive Clustering Hierarchy (TL-LEACH)*, Vehicular Technology Conference, 2005, pp. 1809-1813
[8] Heinzelman W.R. et al.: *Energy-Efficient Communication Protocol for Wireless Microsensor Networks*, Proc. of the Hawaii International Conference on System Sciences, 2000
[9] Handy M.J. et al.: *Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection*, 4th International Workshop on Mobile and Wireless Communications Network, 2002, pp. 368-372
[10] Description of Final ANGEL Demonstrator w ANGEL Project Report; Deliverable D5.2, ANGEL Project, 2007
[11] ZigBee Alliance: *ZigBee Home Automation Public Application Profile* specification, 2007
[12] Gołaszewski G., Górski J.: *Context sensitive privacy management in a distributed environment, Lecture Notes in Computer Science*, 2010, LNCS 6426, Springer, pp. 639-655
[13] IEEE: Standard 802.15.4