ZESZYTY NAUKOWE WYDZIAŁU ELEKTRONIKI,
TELEKOMUNIKACJI I INFORMATYKI POLITECHNIKI GDAŃSKIEJ
Nr 9 Seria: ICT Young 2011

USING TRUST MANAGEMENT MODEL FOR DETECTION OF FAULTY NODES IN WIRELESS SENSOR NETWORKS

Janusz Górski[1], Alan Turower[1]

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

Abstract

Wireless Sensor Networks are used in applications which require high dependability, like healthcare, environmental monitoring, defence and others. Deployed sensors are often left unattended which make them vulnerable to physical damage, shortage of energy supply or intentional attacks. Trust management helps to differentiate between trustworthy and untrustworthy sensors without excessive investment in sophisticated network diagnostic and protection mechanisms which can be too costly comparing to the limited computational and energy resources of the sensors. Distributed trust management models provide for uniform distribution of the responsibility for trust assessment and related decision making. The paper presents the model of distributed trust management in wireless sensor networks, and the simulation results aiming at evaluating the effectiveness of this mechanism in detecting faulty nodes in the network.

1. INTRODUCTION

The role of wireless sensor networks (WSN) increases in many application areas, e.g. in healthcare, defence, environment monitoring and others. More complicated networks which provide more sophisticated services require better targeted and more effective security mechanisms. However, not all security solutions suitable for traditional networks are appropriate for WSN. Sensor nodes are subjected to severe limitations of their resources and cannot afford running sophisticated security mechanisms which are often significantly resource consuming. Dependability of such networks becomes a difficult issue as in addition to technical imperfections and human faults, malicious actions have to be taken into account.

To cope with this problem we employ the concepts of trust and trustworthiness. We understand trust management as collecting the evidences about the behaviour of network nodes and based on these making decisions about trust in these nodes. The collected evidence enables distinguishing between trustworthy and untrustworthy nodes which in turn allows excluding from the network the nodes which are distrusted.

The objective of this paper is to introduce a model of distributed trust management in wireless sensor networks and to present some results related to assessment of its effectiveness in faulty nodes detection. The presented results are based on simulations performed with the help of a dedicated simulator.

The rest of the paper is organized as follows: in section 2 we summarize related works. Next, in section 3 we describe the proposed model. This is followed by the simulation results presented in section 4. We finalize with conclusions in section 5.

2. RELATED WORKS

Distributed trust models are recommended for large-scale sensor networks. Zhiying et al [1] find such models appropriate for sensor network security design because each node focuses on the trustworthiness of its neighbours and can assess if these nodes obey agreed security policies. They propose a corresponding security framework with different security schemes. However, their work does not take into consideration limited resources of nodes in sensor networks.

Zia [2] proposes the security framework to provide a comprehensive security solution against the known threats by integrating the reputation and trust management mechanism. In this concept nodes monitor their neighbouring nodes and rank the neighbours to execute a trust vote.

Momani et al [3] introduce a trust model and a reputation system for WSNs based on sensing continuous data. The trust model establishes the continuous version of the Beta reputation system [4], and a Bayesian probabilistic approach for mixing second-hand information from neighbouring nodes. Directly observed information is used to calculate trust between nodes in WSNs.

Chen et al [5] propose a distributed agent-based trust management scheme where each agent node independently monitors the behaviour of the nodes within its radio range and broadcasts their trust ratings. They also introduce a reputation based trust model using probability, statistics and mathematical analysis and have suggested a trust system to create a reputation space and trust space in WSNs [6].

3. THE PROPOSED MODEL

A dictionary definition states that trust is a belief or confidence in the honesty, goodness, skill or safety of a person, organization or thing [7]. We assume that such a belief is based on explicit assessment of trustworthiness of the trusted party. Our model assumes that a distributed network is composed of clusters, each cluster having its head node and the nodes of a cluster communicating among themselves and with the cluster head. We propose a mechanism which enables each node to make autonomous decisions about trust based on the trustworthiness assessment of its neighbours. We see this model as applicable for the networks applying the LEACH protocol [8] at the lower tier as well as at the higher tier (the backbone cluster). We assume that all nodes should cooperate in evaluation of trust of other nodes in the network [1, 9]. The objective of trust management system is to distinguish between trustworthy network nodes and untrustworthy ones. Then the trustworthy nodes can cooperate to provide trustworthy network services and the untrustworthy nodes are excluded from the network [10].

For this paper we assume the following definition: trust is an act of acceptance of a message received from a network node which results from the assessment of the trustworthiness of the message and its source.

A network node acts as a trustor and a trustee:

— for outgoing communication, the node acts as a trustee – other nodes judge if it can be trusted;
— for incoming communication, a node acts as a trustor – it makes a real-time decision if the sender can be trusted.

Decision about trust is made each time the trustor receives a message from any other node (the trustee). This decision is based on trustworthiness assessment of the sender of the message. The assessment is based on two pillars of evidence: the evidence resulting from the application of agreed security mechanisms (policy-based approach) and the evidence resulting from the recommendations received from the neighbour nodes (reputation-based approach). Each node maintains data on the reputation of other nodes. The corresponding data structure is called *reputation table*. The above mechanism is implemented in each network node and the nodes collectively perform the trust management process of the network. Depending on the trust assessment result the trustor performs appropriate actions:

— if the trustee is trusted:
  a) proceed with message processing,
  b) raise reputation of the trustee;
— if the trustee is not trusted:
  a) discard the message (do not process the data),
  b) decrease the reputation of the trustee,
  c) inform about the event if it is required.

Recommendation is an entry of a local reputation table sent to another node. A node can recommend any other node except itself.

4. SIMULATION EXPERIMENTS

All simulation results are obtained using a simple simulator we developed [10].

During experiments we were considering networks with faulty nodes occurring during the simulation course. The objective of the experiments is to verify how many *simulation turns* are needed to detect faulty nodes in networks of different sizes.

Simulation turn is a basic step of the simulation process. During a simulation turn, each node sends a message to the sink with probability $\boldsymbol{p}$ (and resends the messages from other nodes, if this is a router node). At the end of the turn, the nodes exchange their reputation tables with their neighbours and update own reputation tables accordingly. For each turn, the sink sends a broadcast message to all nodes with probability $\boldsymbol{r}$.

During experiments, the nodes were distributed in the rectangle of the size X×X', where X = X' = 100 points (a point is a distance unit) and the node signal range was set to Y = 30 points. All nodes are fixed (they cannot change their position). The trust scale was the interval of real numbers [0..1] where:

— distrust = 0;
— full trust = 1;
— cut off point = 0,2;
— initial trust = 0,5.

For the experiments we set p = 80% and r = 80%. It was assumed that each non-faulty node sends an incorrect or broken message (it is called *a spoiled message*) with probability z = 2% and faulty nodes send spoiled messages with probability w = 70%. Each node detects spoiled messages with probability c.

The parameters of the experiments are summarized in Table 4.1. The first column gives the probability that the receiving node detects a spoiled message sent by other node (some spoiled messages can stay undetected). This reflects the 'strength' of the mechanisms applied for detection (which in turn may indicate how much resources have been locally devoted to this task). The second column indicates the frequency with which faulty nodes occur in the network. This frequency may indicate design or material imperfections or the environmental stress imposed on the nodes.

Table 4.1

Simulation parameter values for the experiments

	c	*Faulty nodes rate*
Experiment I	90%	every 5 turns
Experiment II	50%	every 5 turns
Experiment III	90%	every 1 turn
Experiment IV	50%	every 1 turn
Experiment V	90%	3 in a row every 10 simulation turns
Experiment VI	50%	3 in a row every 10 simulation turns

The results of experiments for a network containing 50 nodes are shown in Figure 1. On the horizontal axis we have numbers of subsequent faulty nodes injected to the network. On the vertical axis we have numbers of simulation turns necessary to detect a given faulty node.

We can observe that for Experiment I (probability of spoiled message detection 90% and faulty nodes occurring rate 1/5) the first faulty node is detected relatively fast and detecting the next faulty nodes takes slightly longer. The explanation is that initial trust level is well below the maximum (the nodes are more 'suspicious' mutually) and therefore detection is faster. Later, with low rate of faulty nodes occurrence, the level of mutual trust increases and therefore more time is needed to detect the node which departs from the agreed policies.

Experiment II shows how the situation changes if the spoiled message detection weakens. In such case much longer simulation time is needed to detect subsequent faulty nodes. And because many spoiled messages remain undetected, the mutual trust increases and therefore detection of subsequent faulty nodes takes much longer.

Experiments II and IV show how the situation changes when the faulty node occurrence rate increases. Now, with so many faulty nodes the mutual trust level drops and the detection time shortens.

Experiments V and VI refer to the situation where faulty nodes occur in groups. We can observe that is such case the detection time varies and after detecting the current group, the detection time of the first node of the next group shortens. This can be explained by the drop of the mutual trust resulting from the previous group detection – the nodes become more suspicious with respect to their neighbours and the detection is faster.

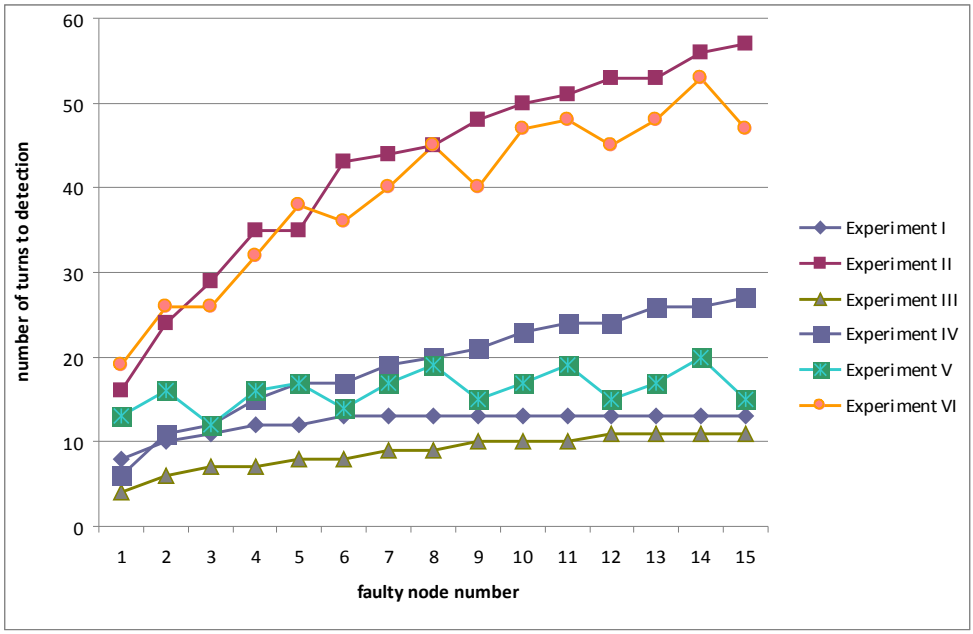

Fig.1. Number of simulation turns needed to detect all faulty nodes in the network of 50 nodes

5. CONCLUSIONS

Trust and trust management is an important issue in distributed wireless sensor networks. Distributed trust management can help in detecting faulty nodes while evenly distributing the detection effort and maintaining the investment of the precious resources (computation time, memory) of nodes in reasonably limits.

In this paper we propose an innovative trust management mechanism and demonstrate, with the help of a dedicated demonstrator, its potential to detect and isolate faulty nodes in a sensor network.

All experiments were carried out for one network cluster. In further research we will investigate the behaviour of a network build from many clusters and a backbone network. We will also investigate how the proposed model can protect the network against more sophisticated attacks, where nodes can modify their behaviour or cooperate to achieve their goals.

BIBLIOGRAPHY

[1] ZHIYING Y., DAEYOUNG K., INSUN L., KIYOUNG K., JONGSOO J., A Security Framework with Trust Management for Sensor Networks, IEEE SecureComm, 5–9 September 2005.
[2] ZIA T. A: Reputaton-based Trust Managmenet in Wireless Sensor Networks, Intelligent Sensors, Sensor Networks and Information Processing, 2008.
[3] MOMANI M., CHALLA S.: Trust Management in Wireless Sensor Networks, Proc. of 5th ACM Conf. on Embedded Networked Sensor Systems, Sydney, Australia, 6 – 9 November, 2007.
[4] JOSANG A., ISMAIL R.: The BetaReputation System, in 15th Bled Electronic Commerce Conference, Bled, Slovenia, 2002.
[5] CHEN H., WU H., ZHOU X., GAO C.: Agent-based Trust Model in Wireless Sensor Networks, in 8th ACIS Int.Conf. on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Qingdao, China, 2007.
[6] CHEN H., WU H., ZHOU X., GAO C.: Reputation-based Trust in Wireless Sensor Networks, in International Conference on Multimedia and Ubiquitous Engineering MUE'07, 2007.
[7] Cambridge Advanced Learner's Dictionary, http://dictionary.cambridge.org/
[8] HANDY M. J., HASS M.: Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection, in Proc. 4th IEEE International Workshop on Mobile and Wireless Communications Network (MWCN '02), pp. 368-372, Stockholm, Sweden, 2002.
[9] GÓRSKI J. et al.: WSN Trust Management Model, in "Angel project report: WSN trust architecture and security protocols", Deliverable 3.2., ANGEL Project, 2007.
[10] GÓRSKI J. et al.: Distributed Trust Management Model for Wireless Sensor Networks, Sixth International Conference on Dependability and Computer Systems DepCoS-RELCOMEX 2011.