Exploiting Malicious Node Detection for Lifetime Extension of Sensor Networks

R. Behnke, J. Salzmann, D. Lieckfeldt, K. Thurow, F. Golatowski, and D. Timmermann

Abstract—**Wireless Sensor Networks (WSN) have attracted considerable research effort in the community during the past couple of years. One of the most challenging issues so far is the extension of network lifetime with regards to small battery capacity and self-sustained operation. Endeavors to save energy have been made on various frontiers, ranging from hardware improvements over medium access and routing protocols to network clustering and role changing strategies. In addition some authors studied failures in communication regarded as error detection. Yet, only weak attention has been paid to the detection of malicious nodes and its potential for lifetime extension. In this work, we present a short overview of detection and classification of malicious nodes in WSN and describe its potential in terms of network lifetime and reliability.**

***Index Terms*—Wireless Sensor Networks, Lifetime prolongation, Malicious Node Detection**

I. Introduction

Recent technological advances have led to the development of tiny wireless devices, which are able to sense the environment, compute simple tasks and exchange data among each other. Interconnected assemblies of such devices, called Wireless Sensor Networks (WSN), are commonly used to observe large inaccessible areas. A key issue to be solved before WSNs can be deployed in a wide range of applications is limited battery capacity which constrains the operational time of sensor nodes. This has been addressed by hardware manufacturers as well as research groups developing energy efficient protocols on various layers, e.g. routing, medium access and clustering. However, only few investigations have been conducted in the field of malicious node detection. From our point of view, this topic becomes more and more important. We focus on the potential of detecting malicious nodes to save energy by supporting network management with additional information. In particular in the field of life science automation, more and more different kinds of sensors, i.e physical and even chemical sensors, are used in WSNs [2]. Specifically those sensors have a higher risk of malfunction due to limited lifetime of used chemicals or any kind of attrition constitute additional error sources. Furthermore, such specialized sensors are less power efficient than, for example, light detectors. Knowledge of such faulty sensors, i.e. malicious nodes, opens the door for improved network management and increased lifetime of affected WSNs. Dealing with potentially faulty measurements and high cost of sensing are the main design and implementation issues.

The remainder of the paper is organized as follows. Section II covers related work in terms of error detection and role changing. In Section III we illustrate our ideas to improve lifetime by malicious node detection. Finally in Section IV we shortly summarize our work and identify future research topics.

II. Related Work

A. Lifetime

Existing approaches for lifetime extension range from specialized medium access protocols over effective routing protocols and data aggregation and compression to role changing and clustering mechanisms. To name only few examples, S-MAC [11] and Z-MAC [9] reduce cost for medium access compared to former protocols by smarter scheduling and reduced idle listening. Special routing protocols avoid costly routing tables or shorten the routing path by bypassing obstacles, holes or dead ends [1]. Data aggregation approaches concatenate and combine messages from adjacent nodes to reduce data transmissions as well as length of data packets. 2-MASCLE [10], as an example of clustering approaches, uses location based square cells to build clusters within which only one node has to be active at a time. In addition, only every second cluster has to be active, which prolongs the lifetime by 80%. Other clustering approaches assign roles to cluster members, e.g. routing nodes, cluster head, sensing node.

B. Error detection

Many approaches concerning detection and management of errors or faults, respectively, have been published during the last years. Surveyed approaches in [8] all focus on routing, transportation and application layers as well as data dissemination. Faults are seen as packet loss or total loss of (routing) nodes. Faulty readings are identified as a source of errors but not investigated in detail. In [6], detecting faulty nodes was identified as important research topic, but only as diagnostic tool for human networkers, further insides are not provided. The author's approach is based on comparisons between neighboring nodes, performed on a central server, to

R. Behnke, J. Salzmann, D. Lieckfeldt and D. Timmermann are with University of Rostock, Institute of Applied Microelectronics and Computer Engineering, Germany (e-mail: {ralf.behnke;jakob.salzmann; dominik.lieckfeldt;dirk.timmermann}@uni-rostock.de)

F. Golatowski and K. Thurow are with Center For Life Science Automation - CELISCA, Rostock, Germany (e-mail: {frank.golatowski; kerstin.thurow}@celisca.de)

detect malicious nodes. Another example that focuses solely on connectivity is [5], which, in addition, only differentiate between alive and dead nodes. A similar problem is addressed by [7], which focuses on attacks on routing activities.

In [3], SASHA is described as a self-healing architecture inspired by human lymph system. Pattern recognition techniques and neuronal networks are used to mitigate the effects of various types of faults. Therefore, non battery driven nodes, i.e. embedded computers, with higher capabilities, supported by PC class servers, are proposed to be used to monitor normal nodes. In [4], a type of self-management is presented which adapts sleep and sense cycles of neighboring nodes and is able to identify and exclude nodes with alternating readings.

III. Our Idea

In contrast to earlier mentioned conceptions, our notion of malicious node detection is to detect when a node physically measures wrong values. This may be caused by faulty sensors, converters, exceeded sensor lifetime or even manipulations.

As a consequence and in contrast to former approaches, we divide the node functionality into functional, inoperable and partly functional. We also identify different types of faults. We define faults to be significant discrepancies of measurements in comparison to those of neighboring nodes, i.e. spatial correlation, and as unusual behavior over time, e.g. strong leaps or alternating values. Beside this temporal correlation also full-scale or out of range measurements can be detected as failures.

Another classification of detection schemes can be self-detection and cooperative detection, i.e. neighbors of a node or a central instance are to determine its functionality.

Irrespective of whether such detection will be performed on each node in the network or on a central instance, we see a variety of benefits by utilizing this knowledge. Beside the simple diagnostic information of malicious readings, we believe, that using this information nodes can save a lot of energy and therefore prolong network lifetime. Firstly a node, being aware of its malfunction, can save energy he would otherwise spend for sensing. Especially WSNs in the field of chemistry, equipped with catalytic or optic sensors, will profit from this approach. Secondly, nodes do not have to send faulty measurements. This exculpates not only the node itself but mainly the whole network as the number of packet transmissions is reduced. A third advantage would be that network management in terms of role assignment can be significantly improved, as a node, once depicted as only partly functional, can be assigned non-sensing tasks like routing or aggregation. Consequently, a fully functional node should not be used for this work. As a result, we believe that the network will stay functional for longer time. In addition such a functionality-based role assignment opens the door to use cheaper components, accepting some faulty sensors, for large area observations.

We already obtained first insides in in-network fault detection with our 2-MASCLE clustering approach. This approach ensures that each node in a cluster is able to observe the same phenomena, which allows the cluster members to control each other. Also adjacent clusters are able to control themselves because a phenomenon within a cluster can also be detected by at least one neighboring cluster.

IV. Conclusion

We reviewed several publications about error and fault detection respectively. Only a small part of these works consider fault detection, also referred to as malicious node detection, in terms of identifying nodes whose measurements are erroneous. The few existing approaches often rely on centralized techniques instead of in-network detection and do not pursue network lifetime extension as a benefit. In contrast, our goal is to disburden the fully functional nodes of a network from non-sensing tasks, improve role changing and therefore prolong network lifetime. Future work will use geographic clustering as base for spatial correlation tests and will strive to use cluster free approaches relying only on pure neighborhood detection. In particular, the amount of energy saving and lifetime extension have to be analyzed.

References

[1] J.N. Al-Karaki and A.E. Kamal. Routing techniques in wireless sensor networks: a survey. *Wireless Communications, IEEE*, 11(6):6–28, Dec. 2004.

[2] R. Behnke, F. Golatowski, K. Thurow, and D. Timmermann. Wireless sensor networks for life science automation. In *International Forum Life Science Automation*, 2007.

[3] T. Bokareva, N. Bulusu, and S. Jha. Sasha: Toward a self-healing hybrid sensor network architecture. *Embedded Networked Sensors, 2005. EmNetS-II. The Second IEEE Workshop on*, pages 71–78, May 2005.

[4] P. Boonma, P. Chamnprasert, and J. Suzuki. A biologically inspired architecture for self-managing sensor networks. *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on*, 3:734–739, Sept. 2006.

[5] Xiaojiang Du, Ming Zhang, K. Nygard, M. Guizani, and Hsiao-Hwa Chen. Distributed decision making algorithm for self-healing sensor networks. *Communications, 2006. ICC '06. IEEE International Conference on*, 8:3402–3407, June 2006.

[6] Chaiporn Jaikaeo, Chavalit Srisathapornphat, and Chien-Chung Shen. Diagnosis of Sensor Networks. In *IEEE International Conference on Communications (ICC 2001)*, Helsinki, Finland, June 2001.

[7] Waldir Ribeiro Pires Junior, Thiago H. de Paula Figueiredo, Hao Chi Wong, and Antonio A. F. Loureiro. Malicious node detection in wireless sensor networks. *ipdps*, 01:24b, 2004.

[8] Paradis, Lilia, Han, and Qi. A survey of fault management in wireless sensor networks. *Journal of Network and Systems Management*, 15(2):171–190, June 2007.

[9] Injong Rhee, A. Warrier, M. Aia, Jeongki Min, and M.L. Sichitiu. Z-mac: A hybrid mac for wireless sensor networks. *Networking, IEEE/ACM Transactions on*, 16(3):511–524, June 2008.

[10] J. Salzmann, R. Behnke, D. Lieckfeldt, and D. Timmermann. 2-mascle - a coverage aware clustering algorithm with self healing abilities. *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pages 739–744, Dec. 2007.

[11] Wei Ye, J. Heidemann, and D. Estrin. An energy-efficient mac protocol for wireless sensor networks. *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, 3:1567–1576 vol.3, 2002.