ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 2 Issue 1 January-February 2014

International Manuscript ID : 23482001V2I101022014-28

AN EFFECTIVE ALGORITHMIC APPROACH FOR WIRELESS SENSOR NETWORKS RECONFIGURATION AND REDEPLOYMENT

Dr. Su Kan

China University of Technology

ABSTRACT

Originally, each group of many sensor nodes are deployed for one special application. Nowadays and especially in the future, sensor nodes are used for multi-purposes. They are set for a certain configuration, but may adapt to the dynamic environment and flexible specification. The user such as e.g. administrator controls the whole network and organizes a reconfiguration if necessary. A reconfiguration could be topology changes, task re-assignments, software updates, etc. The network receives a new configuration and immediately manages the update process. The sensor nodes perform the adaptation automatically. Therefore, human intervention is not needed at sensor nodes. In this work, tools of the trade are classified into reconfiguration objects and goals. A survey on reconfiguration in wireless sensor networks gives an overview about possible approaches from the literature. Thereby, for each class, typical scenarios describe the requirement of reconfiguration of some application and system parts. Various approaches are compared to represent the sub-classes. In this paper, an empirical algorithmic approach is proposed for reconfigurability and redeployment of the wireless sensor nodes using digital imaging devices.

Keywords – Wireless Sensor Networks, Redeployment, Reconfiguration

INTRODUCTION

A reconfigurable wireless sensor network (WSN) consists of many sensor nodes, which are deployed for multiple purposes and dynamic environments. The sensor nodes are installed on tiny and resource-constraint devices, because more than hundreds of them are used to sense data in one area.

Due to resource constraints, the sensor nodes are originally fixed for some certain applications. Nowadays, it is desired to use the same WSN for different applications such as multiple monitoring. Thus avoids activating too much nodes. Another important reason for flexible deployment of the nodes comes from the dynamic environments. The natural environment leads to detection of disasters and protection of moving objects.

The number of deployed sensor nodes or involved sensing objects is not fixed. Saving energy, the performance of each WSN is scalable. The more performance is required, the more powerful approaches are used, which often consume more energy. Furthermore, the topology in a WSN is important. It decides about the efficiency of the data gathering and communication. The communication model influences the robustness of such network. Normally, sensor nodes may often fail. Thus needs adapting the participation of those. Secure applications such as sensing sensible data require more protection. Attacks to WSNs are reduced by providing security approaches, but they are selected with regard to their necessity. Consequently, the setting of WSNs in all environments should be easily changeable.

Reconfiguring the WSN, the initial setting will be adapted to the desired specification. Hence, new applications or configurations are needed. Clearly, the network administrator can go the nodes and install new software and hardware manually. However, the intervention is too high due to the large amount of nodes or the environment may be dangerous or not possible to enter. Thus leads to reconfigurations over the network. Existing tools for standard computers are not appropriate, because they are not such aware to the constrained resource.

There are surveys, which refer to the same topic. However, each paper explains one reconfiguration. Furthermore, it explains why reconfiguration is needed by referring to the scenarios. Finally, own ideas show new possible reconfigurations or proposals for improvements.

RECONFIGURABLE NETWORKS

Reconfigurable WSNs means that sensor nodes in such networks receive initial settings and applications. Adapting to the current specification of the user and natural environment, the settings and applications are changeable. In the followed sub-sections, the characteristics of WSNs are described. They lead to necessity of reconfiguration. Examples show some real cases where WSNs should be reconfigurable. Afterwards, the generic steps describe one reconfiguration procedure in general.

CHARACTERISTICS AND ASPECTS

The resource in WSNs is very constraint. The hardware installing for sensor nodes is much more limited than standard personal computers. The nodes run on some small batteries. That is why they sometimes deplete energy and fail. Furthermore, they have slow processors and some MB of memory. Their size varies from shoebox to grain of sand. Normally, they cost under $1. Consequently, more than hundreds or even thousand nodes can be deployed for one area. In some networks, they are closely together. With that, each detail of such area will not be left out. However, the performance of such systems is restricted. Processing of sensing data is left out. The nodes should only sense and collect data. Then, they transmit the data toward the target. Thus, nodes near the target consume more energy than the other ones. Furthermore, the target is often a base station, which has no such limitations, and can evaluate the data.

RECONFIGURATION AND REDEPLOYMENT

Reconfiguration contains topology change, task management, software update and adapting system parameters to the flexible environments. WSNs are aware to different applications and scalable to the necessary level of performance, dependability and security.

Some concrete examples show when reconfiguration is required. Initially, sensor nodes monitor one building and collect sensing data of temperature measure. The task for one group of sensor nodes may be changed from time to time. With the same nodes, the user sometimes wants to monitor e.g. the movement in this building and the pressure near the windows. Otherwise, in a huge area like a piece of land, the nodes measure the rainfall, but are able to send warning signals if flooding possibly happens. Becoming active, the nodes may restrict nature disasters by sending warning signals. Especially in military, intrusion should be detected by providing appropriate security mechanisms. However, the memory does not allow so many applications stored on the nodes. Thus, it leads to software update or activating new nodes for certain tasks. The topology is crucial for the efficiency of disseminations. If nodes may fail or move, the topology will be changed.

Reconfiguring, the heterogeneity are cared, because all nodes should be compatible to the new settings and applications. Furthermore, human intervention and duration of reconfiguration process are to be minimized.

Reconfiguration can be initialized either by the user, by the network or by the nodes. Normally, at the beginning the user specifies the reconfiguration. The user differs from case to case. It can be network administrator, software developer, robots or end users. Reconfigurations require human intervention at initialization, because human can set rules for reconfiguration. If some decisions are easy to be made and robots are deployed, robots can take over the control. If applications run, the network will control the data distribution and provides other useful network functions (e.g. communication). Finally, the nodes execute their sensing tasks according to the applications. Especially in self-organizing networks, they should be able to reconfigure themselves.

PROPOSED ALGORITHMIC APPROACH

1. Deployment of Sensor Nodes Vector DSV[i] {i<=n}
2. Activation Matrix of Digital Imaging Camera Devices Ci
3. C_i->WSN_i (Position) => Monitoring of nodes by the camera
4. Investigation of Camera[i] Vector to analyze the recorded vector
5. Vehicle based redeployment of the sensor nodes captured by the camera.
6. Final Generation of the overall network performance and reconfiguration vector

CONCLUSION

This work contains a survey and future works on reconfiguration in WSNs. It defines the term reconfiguration as followed. Reconfiguration is to modify the setting of the network and sensor nodes. After an initial configuration, if the environment or specification for the applications changes, the involving sensor nodes should be adapted. They are desired to perform their tasks as before. Due to the complexity of this work, there are many sub-classes. Each sub-class presents another goal (objectives) and reconfiguring object (capabilities), whereby the classification prefers the objectives. Objectives are functionality, dependability and security. Capabilities are node properties, network, software, middleware and hardware. The appropriate scenarios are described in detail to lead to those reconfiguration possibilities. For each possibility, we have one or more options, how we can reconfigure. These approaches, which refer to according papers, are described in a general way. The similarities are reported and the differences are explained in the paper summaries. Therefore, the reader can have a better overview. For details of one certain reconfiguration, he can read the description in the paper summaries.

Evaluating the tools of the trade, the discussion contains opinions to their fulfilment. They are able to provide necessary reconfiguration technologies in efficient and robust manner. However, future works on data compression, routing protocols, frameworks for heterogeneity, etc. are important to enhance the efficient use of less sensor nodes for multiple purposes. Furthermore, some improvements such as by using other reconfiguration options can be taken into account. For example, multiple topology formats such as multiple trees or clusters may reduce the system failure rate due to failed node. Additionally, they may increase the dissemination rate up to nearly flooding. However, the node participation becomes higher. Therefore, hardware capabilities and the current environment should be regarded carefully.

Consequently, there are more reconfiguration possibilities for the future works. The most important fact is that WSNs should be designed for re-configurability, but they are.

FUTURE WORK

- Currently using digital imaging devices, the situation, location and placement of the sensor nodes can be monitored
- There is no policy of including the temperature detector so far so that the temperature based on the threshold can be detected.
- In future work, the inclusion of threshold based temperature detector and air vehicle based redeployment can be done.

REFERENCES

[1] Hang Su; Xi Zhang, “Energy-Efficient Clustering System Model and Reconfiguration Schemes for Wireless Sensor Networks”, Information Sciences and Systems, 2006 40th Annual Conference !!

Perf Extended analy. Model to derive optimal number of clusters to max. The netw. Lifetime and preserve energy

[2] S. Capkun, J.-P. Hubaux, “Secure positioning in wireless networks”, IEEE

Journal on Selected Areas in Communications, 2006

[3] L. Lazos and R. Poovendran, “Serloc: Robust localization for wireless sensor networks”, ACM Trans. Sensor Networks, 2005

[4]] Geoff Coulson, Richard Gold, Manish Lad, Cecilia Mascolo, Luca Mottola, Gian Pietro Picco and Stefanos Zachariadis, “Dynamic Reconfiguration in the RUNES Middleware”, 2006

[5] Paolo Costa, Geoff Coulson, Cecilia Mascolo, Luca Mottola, Gian Pietro Picco and Stefanos Zachariadis, “Reconfigurable Component-based Middleware for Networked Embedded Systems”, 2005

[6] M. S. Vieira, N. S. Rosa, “A Reconfigurable Group Management Service for Wireless Sensor Neworks”, MPAC 05, 2005

[7] D. J. Malan, M. Welsh, and M. D. Smith, “A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography“, In First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004

[8] P. Hu, J. Indulska, R. Robinson, “Reconfigurable middleware for sensor based applications”, CM International Conference Proceeding Series; Vol. 185, Proceedings of the 3rd international Middleware doctoral symposium Melbourne, Australia, 2006

[9] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz, “Comparing elliptic curve cryptography and rsa on 8-bit cpus“, In In 2004 workshop on CryptographicHardware and Embedded Systems, 2004

[10] Kai-Wei Fan, Sha Liu, Prasun Sinha, “Storage and abstractions: Scalable data aggregation for dynamic events in sensor networks“, Proceedings of the 4th international conference on Embedded networked sensor systems SenSys '06, 2006

[11] http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[12] Anthony D. Wood, Lei Fang, John A. Stankovic, Tian He, “Secure routing: SIGF: a family of configurable, secure routing protocols for wireless sensor networks“, Proceedings of the fourth ACM

workshop on Security of ad hoc and sensor networks SASN ′06, October 2006

[13] J. Reich, E. Skar, “Toward Automatic Reconfiguration of RobotSensor Networks for Urban Search and Rescue“, 2006

[14] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[15] SensorWare: “Design and Implementation of a Framework for Efficient and Programmable Sensor Neworks”, Open Architectures and Network Programming Proceedings, 2002 IEEE, 2002

[16] Adam Dunkels, Niclas Finne, Joakim Eriksson, Thiemo Voigt, “Operating systems: Run-time dynamic linking for reprogramming wireless sensor networks“, Proceedings of the 4th international conference on Embedded networked sensor systems SenSys ′06, October 2006