International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 3 Issue: 1 26-Jun-2014,ISSN_NO: 2321-3337

INFORMATION SECURITY ON ENERGY-EFFICIENT WIRELESS NETWORKS

C.Thangamalar[1] Dr.K.Ravikumar[2]

(Research Scholar,Research & Development Center,
Bharathiar University,Coimbatore[1]
Asst.Professor,Dept.of.Computer Science,Tamil University,Thanjavur[2])

ABSTRACT--*An wireless energy-efficient, reliable and timely data transmission is essential for wireless sensor networks (WSNs) employed in scenarios. To reach a maximum efficiency, cross layer interaction is a major design paradigm to exploit the complex interaction among the layers of the protocol stack. This is challenging because latency, reliability, and energy are at odds, and resource constrained nodes support only simple algorithms. The adaptive protocol Breath is proposed for control applications. Breath is designed for WSNs where nodes attached to plants must transmit information via multi-hop routing to a sink. Breath ensures a desired packet delivery and delay probabilities while minimizing the energy consumption of the network. The protocol is based on randomized routing, medium access control, and duty-cycling jointly optimized for energy efficiency. The design approach relies on a constrained optimization to solve this problem,*

Keywords: A*daptive routing,packets*

I. INTRODUCTION

Function is the energy consumption and the constraints are the packet reliability and delay. The challenging part is the modeling of the interactions among the layers by simple expressions of adequate accuracy, which are then used for the optimization by in-network processing. The optimal working point of the protocol is achieved by a simple algorithm, which adapts to traffic variations and channel conditions with negligible overhead. The protocol has been implemented and experimentally evaluated on a test-bed with off-the-shelf wireless sensor nodes, and it has been compared with a standard solution. Analytical and experimental results show that Breath is tunable and meets reliability and delay requirements. Breath exhibits a good distribution of the working load, thus ensuring a long lifetime of the network. Therefore, Breath is a good candidate for efficient, reliable, and timely data gathering for control applications

II. Wireless Sensor Networks:

Wireless sensor networks (WSNs) are networks of tiny sensing devices for wireless communication, monitoring, control, and actuation. Given the potential benefits offered by these networks, e.g., simple deployment, low installation cost, lack of cabling, and high mobility, they are specially appealing for control and industrial applications. The variety of application domains and theoretical challenges for WSNs has attracted research efforts for more than a decade. Although WSNs provide a great advantage for process, manufacturing and industry, they are not yet efficiently deployed. This is because the software for these applications is usually written by process and software engineers that are expert in process control technology, but know little of the network and sensing infrastructure that has to be deployed to support control applications. On the other side, the communication infrastructure is designed by communication engineers that know little about process control technology. Moreover, the adoption of wireless technology further complicates the design of these networks. Being able to satisfy high requirements on communication performance over unreliable communication channels is a difficult task.

III. WIRELESS SENSORE PROCESSING:

Reliability:

Sensor information must be sent to the sink of the network with a given probability of success, because missing these data could prevent the correct execution of control actions or decisions concerning the phenomena sensed. However, maximizing the reliability may increase substantially the network energy consumption. Hence, the network designers need to consider the tradeoff between reliability and energy consumption. Delay: Sensor information must reach the sink within some deadline. A probabilistic delay requirement must be considered instead of using average packet delay since the delay jitter can be too difficult to compensate for, especially if the delay variability is large. Retransmission of old data to maximize the reliability may increase the delay and is generally not useful for control applications.

Energy efficiency: The lack of battery replacement, which is essential for affordable WSN deployment, requires energy-efficient operations. Since high reliability and low delay may demand a significant energy consumption of the network, thus reducing the WSN lifetime, the reliability and delay must be flexible design parameters that need to be adequate for the requirements. Note that controllers can usually tolerate a certain degree of packet losses and delay. Hence, the maximization of the reliability and minimization of the delay are not the optimal design strategies for the control applications we are concerned within this paper.

Application requirements may change dynamically and the communication protocol must adapt its design parameters according to the specific requests of the control actions. To support changing requirements, it is essential to have an analytical model describing the relation between the protocol parameters and performance indicators.

Scalability: Since the processing resources are limited, the protocol procedures must be computationally light. These operations should be performed within the network, to avoid the burden of too much communication with a central coordinator. This is particularly important for large networks. The protocol should also be able to adapt to size variation of the network, as, for example, caused by moving obstacles, or addition of new nodes. In this paper, we offer a complete design approach that embraces all the factors mentioned above. We propose the Breath protocol, a self-adapting efficient solution for reliable and timely data transmission. Since the protocol adapts to the network variations by enlarging or shrinking next-hop distance, sleep time of the nodes, and transmit radio power, we think that it behaves like a breathing organism.

Computations Of adaptive process

we allocate the more sensors in different places, that used to collect the temperature details of the particular place, here we are using the temperature sensor to observes the temperature of the place. These sensors are collecting the temperature of the several places these details are send to the cluster head.

International Journal of Advanced Research in
Computer Science Engineering and Information Technology
Volume: 3 Issue: 1 26-Jun-2014,ISSN_NO: 2321-3337

Receive sensor value

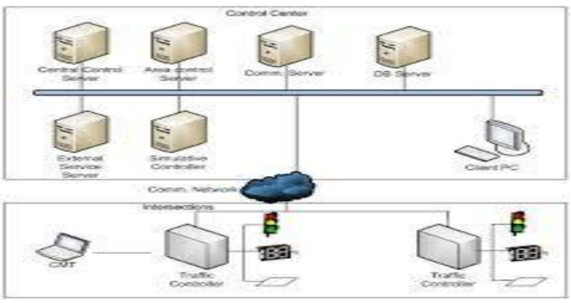
Here the cluster head system receive the various sensor's temperature values from the various sensors using sensor ID and cluster header name, then cluster the given values.

Controller

Controller gets the values from the cluster head, that values are get from the various sensor nodes. Then the controller display higher temperature values with the particular place. Controller analyze the given various temperature and find the.

Adaptation:

The network operation should adapt to application requirement changes, varying wireless channel and network topology. For instance, the set of higher temperature in which node. Then display the higher temperature in which place



Wireless topology transmitted

Adoptive approach for topology management Large and Dense Real time wireless sensor networks

Topology management protocols play an important role in WSNs, managing the sleep transitions of the nodes to make data transmissions occur in an energy-efficient way, thus prolonging network lifetime. However, classical topology management protocols are not suitable for real-time WSNs, as they may introduce unbounded delays. In a previous work, we presented a static topology management protocol specifically designed for real-time WSNs which is able to provide bounded delay and routing fidelity. This paper extends such work, presenting a dynamic topology management protocol that surpasses the static approach introducing support for event-driven data transmissions and node joining at runtime and providing a novel adaptive technique for energe.

IV. CONCLUSION

We designed and implemented Breath, a protocol that is based on a system-level approach to guarantee explicitly reliability and delay requirements in wireless sensor networks for control and actuation applications. The protocol considers duty-cycle, routing, MAC, and physical layers all together to maximize the network lifetime by taking into account the tradeoff between energy consumption and application requirements for control applications. We provided a complete test-bed implementation of the protocol, building a wireless sensor network with Tiny OS and Tmote sensors. An experimental campaign was conducted to test the validity of Breath in an indoor environment with both AWGN and Rayleigh fading channels. Experimental results showed that the protocol achieves the reliability and delay requirements, while minimizing the energy consumption. We are currently investigating the extension of the design methodology to consider mesh networks such as coexisting ad-hoc and wireless sensor networks.

V. REFERENCES

[1]. Appelbaum, P.S., "*Threats to the Confidentiality of Medical Records – No Place to Hide*", JAMA; (283:6), pp. 795-797, Feb 2000.

[2]. Benbasat I., Goldstein D.K., and Mead M.,**"***The Case Research Strategy in Studies of Information Systems"*, MIS Quarterly; (11:3), pp. 369-386, Sept. 1987

[3]. Biotech Business Week, "*Electronic Medical Records: Medical Identity Theft Survey Shows Consumers Concerned about Privacy, Protection of Records*", Jan 8, 2007.

[4]. Boyd, A.D., Hosner, C., Hunscher, D.A., Athey, B.D., Clauw, D.J., and Green L.A., *"An Honest Broker" mechanism to Maintain Privacy for Patient Care and Academic Medical Research"*,
International Journal of Medical Informatics; (76); pp. 407-411, 2007,.

[5]. Conn, J., *"A Real Steal. Patients, Providers Face Big Liabilities as Medical Identity Theft Continues toRise, and in Many Cases it's an Inside Job,"Mod Healthc;* (36), pp. 26-28, 2006.Computing Technologies for Healthcare, 2008.Pervasive Health 2008.

[6] Ng, J., Lo, B., Wells, O., and Sloman, M. (2004). Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon).*In Proceedings of the International Conference onUbiquitous Computing (Ubicomp)*.