DISTRIBUTED SENSOR NETWORKS: LIFETIME AND SECURITY

Zdravko Georgiev Karakehayov

MCI-CPD, University of Southern Denmark, Grundtvigs Alle 150, DK-6400 Sønderborg, Denmark, phone: +45 6550 1696, e-mail: zdravko@mci.sdu.dk

Niels Lervad Andersen

MCI-CPD, University of Southern Denmark, Grundtvigs Alle 150, DK-6400 Sønderborg, Denmark, phone: +45 6550 1614, e-mail: nla@mci.sdu.dk

Zdravko Todorov Monov

Faculty of German Engineering Education and Industrial Management, Technical University of Sofia, 8 Kliment Ohridski St, Sofia-1000, Bulgaria, phone +359 2 855 9277, e-mail: ztm@tu-sofia.bg

This paper describes a routing algorithm for distributed sensor networks. The algorithm attempts to satisfy the conflicting needs of power efficiency and security. The method can be applied for sensor networks designed for energy scavenging. The nodes of the network communicate in a multihop manner. The best candidate for the next hop is the node closest to the destination. At the same time, nodes in process of scavenging have ample amount of energy and become suitable replacements for well located nodes. This feature makes the network more vulnerable in case of black hole attacks. Malicious nodes may attract traffic and drop packets. The proposed algorithm is based on the assumption that the environment will influence several nodes simultaneously. We discuss the CPU architectures used in the domain of sensor networks and provide simulation results for three of them. The simulation results indicate the algorithm execution time and memory requirements for different density of the network.

Keywords: Sensor networks, low-power routing, secure routing

1. INTRODUCTION

Distributed sensor networks consist of hundreds or thousands tiny, low-cost nodes, possibly mobile but more likely at fixed locations. The functionality of distributed sensor networks can be broken down into four major tasks: sensing, computation, communication and actuation. Since a large number of nodes cooperatively perform complex tasks, the most effective malicious influence is to attack the communication. A node can simply consume the packets and block the forwarding. This type of malicious behavior is termed a black hole. Since the energy is a scarce resource, the network's functionality must be viewed from a low-power perspective. Security requires extra processing. Communication has security

overhead as well. The resulting energy drawn from the battery is increased and low-power design becomes a vital issue.

The network nodes have a limited radio footprint and packets are forwarded in a multihop manner. When a node receives a packet, it applies a routing algorithm to select a neighbor for forwarding. Different criteria can guide the local decision. A common approach is to choose the closest to the destination neighbor.

The greater than linear relationship between transmit energy and distance promises to reduce the energy cost when the radio link is partitioned. Nodes calculate the distance and tune their transmit power accordingly. Consequently, it would be beneficial to use several hops to reach a node within the transmission radius instead of a direct link. Algorithms for multihop optimization select the neighbor which offers the most power efficient forwarding of the packet.

2. RELATED WORK

Many sensor networks applications need to run for several months or even years. The lifetime of a network depends on the daily energy budget and the energy the battery can supply. For example, if the daily energy budget is 4 mAh and the nodes have coin cells, 1000 mAh, the resulting lifetime is 250 days. The Great Duck Island project was planed for 8.15 mAh daily energy budget [1].

The individual nodes are comprised of a microcontroller, sensors and a radio transceiver. The largest part of the energy budget goes for radio transmission. Multihop optimization has been studied for simple linear settings with the assumption that equally spaced nodes might be available for retransmissions [2, 3, 4].

One way to mitigate the problem of limited energy sources is to apply scavenging [5, 6]. Along with solar cells, an excellent solution, vibration, air flow, temperature differences and electromagnetic fields can be used to scavenge energy. Naturally, nodes in process of scavenging are good candidates for a next hop target. However, malicious nodes may use this to attract traffic and wage black hole attacks [7].

Routing algorithms, such as REWARD, are capable of declining the network's vulnerability in face of black hole attacks. REWARD detects black hole attacks and organizes a distributed data base for suspicious nodes and areas [8, 9, 10]. The algorithm utilizes two types of broadcast messages, MISS and SAMBA, to recruit nodes to act as security servers. Security servers keep records for detected black hole attacks and provide security services when forward packets. Another protocol for secure routing, called cluster key grouping, helps to balance between the conflicting requirements of power efficiency, memory size and security [11].

In this paper we provide a modification of the routing protocol which declines the network vulnerability when the life time is increased via scavenging.

3. NOTATION

Assume that the nodes of a wireless ad hoc network are members of the following set:

$$N = \left\{N_1, N_2, N_3, \ldots N_{n(N)}\right\}$$

Alternatively, the nodes can be represented by the natural numbers of their IDs.

$N = \{1,2,3,...\}$

The nodes are placed in a rectangular region of *X* by *Y*. The distance between node i and node j is *d*(i,j). Routing algorithms are employed to determine the next hop node of N_i, N_i^{+1}. A set N_i^R includes all neighbours of N_i that are within its communication range. A subset of N_i^R, $N_i^{R,S}$, represents neighbour nodes in process of scavenging.

4. THE ALGORITHM

The method is based on the assumption that the environment will influence several nodes simultaneously. For example, solar power may be available not only for a single node, but most likely for a set of nodes. All these nodes will periodically broadcast their status of scavenging. If a single node or very few nodes report a status of scavenging, they will be excluded from the routing.

Algorithm 1 $N_i^{+1} \leftarrow \text{NextHop}\left(N_i, N_D, N_i^R, N_i^{R,S}\right)$

1: **if** $N_D \in N_i^R$
2: **return** N_D
3: **end if**
4: $N_i^{+1} = 0$
5: **if** $n(N_i^{R,S}) > \text{SMIN}$
6: $s = d(i, D)$
7: **for** $1 \le j \le n(N),\ j \ne i$ **do**
8: **if** $N_j \in N_i^{R,S}$ and $d(j, D) < s$
9: $N_i^{+1} = N_j,\ s = d(j, D)$
10: **end if**
11: **end for**
12: **end if**

Algorithm 1 describes the procedure to determine the next hop of N_i, N_i^{+1}. If the destination, N_D, is a neighbour, it is selected for the next hop. The algorithm checks if the number of neighbours in process of scavenging is higher than a threshold, SMIN. We can choose SMIN according to the density of the network, the environmental conditions and the type of the energy source. Furthermore, we can modify SMIN to adjust the security capability of the algorithm. The procedure checks in line 8 if the current node is in process of scavenging and if it makes progress toward the destination. In case the number of neighbours reported scavenging is

below the limit or the number is sufficient, but none of them makes progress, the procedure ends up with $N_i^{+1} = 0$. Then a standard procedure is performed to find the next hop.

5. ARCHITECTURES

Since the nodes are resource-constrained devices, a single processor architecture is the most logical approach. Simple hardware and simple software accord well with the requirements for price, power consumption and size. At the same time, the CPU must be fast enough to perform the real-time operations with enough capacity to provide a reasonable operating margin. Simulations may be needed to prove the timing properties of the network nodes.

As far as the instruction set architecture (ISA) is concerned, quite a few ISAs vie for attention in the embedded systems domain today [12]. The same applies for distributed sensor networks as well. Three CPUs dominate the sensor networks platforms: 8051, Atmel AVR and ARM [13, 14, 15]. The lack of architecture diversity simplifies the modelling of algorithms for distributed sensor networks.

The power consumption of the network node embedded computer is an important design metric. Along with the efficiency of the ISA to execute a set of algorithms, the availability of power management via energy saving modes and voltage/clock scaling is a fundamental design issue. Manufacturers extend the power management to the embedded peripherals. In order to save energy nodes should stay in a sleeping mode as long as possible. Periodically, nodes must wake up and receive the packets buffered for them. Wireless networks use beacons to synchronize internode communications. The beacon periods impose deadlines for the node functionality.

6. SIMULATION RESULTS

Real-time operation of sensor networks requires more than just having short execution times on average - it requires proper timing for the worst-case scenario. Consequently, we must consider the density of the network when evaluate the execution time.

We have used C language to code Algorithm 1. The C code has been compiled for the following ISAs: 8051, Atmel AVR, ARM and ARM-THUMB. Fig. 1 shows simulation results for the execution time.

Different numbers of neighbouring nodes lead to different execution times. Also, the data type used for nodes coordinates has a significant impact on the execution time. The simulation results have been obtained for an 8051 microcontroller running at 24 MHz, an Atmel AVR microcontroller at 20 MHz and an Atmel ARM microcontroller clocked at 33 MHz.

The memory size, a companion simulation result, is shown in Fig. 2. Again, the algorithm utilizes as input neighbouring nodes within the range 4 through 16. While the execution time is a strong function of the number of neighbours, the memory size is increased slightly from sparse to dense networks.

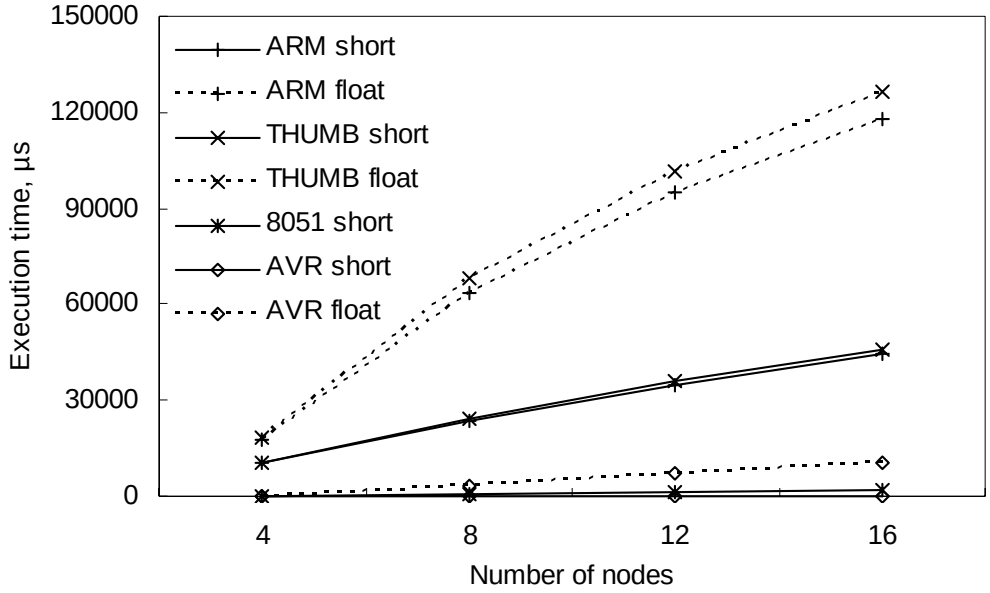

Fig. 1. Execution time for different CPUs and two data types

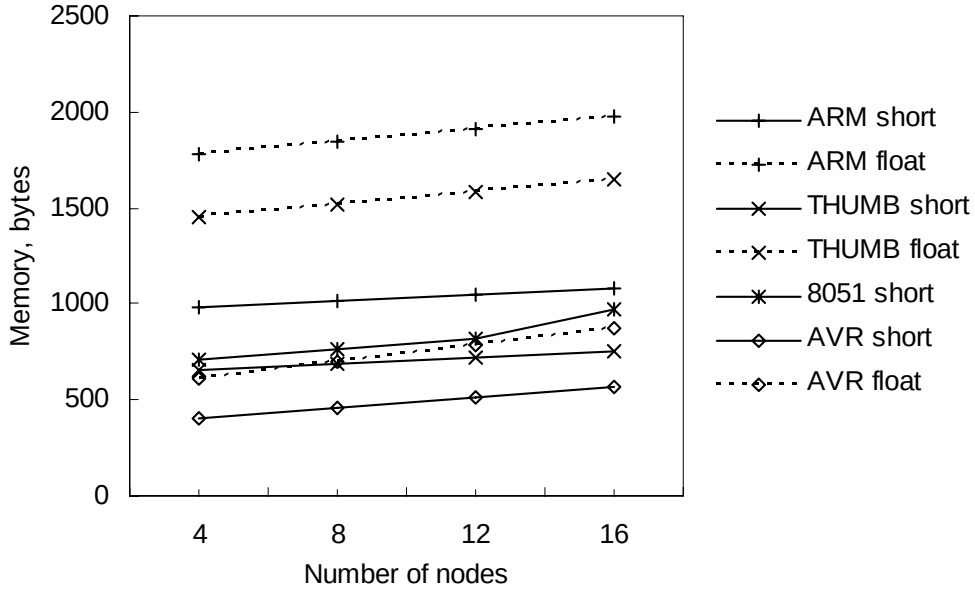

Fig. 2. Memory requirements for different CPUs and two data types

7. CONCLUSION

We have presented a routing algorithm for distributed sensor networks. The algorithm strikes the balance between network lifetime and security. The method can be applied for sensor networks designed for energy scavenging. The algorithm has an adjustable security capability. We discussed CPU architectures popular in the domain

of sensor networks and provided simulation results for three of them. The simulation results indicate the algorithm execution time and memory requirements for different density of the network.

8. REFERENCES

[1] Mainwaring A., D. Culler, J. Polastre, R. Szewczyk, J. Anderson, *Wireless Sensor Networks for Habitat Monitoring*, Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, Atlanta, 2002, pp. 88-97.

[2] Stojmenovic I., X. Lin, *Power aware localized routing in wireless networks*, IEEE Transactions on Parallel and Distributed Systems, Vol. 12, No. 11, November 2001, pp. 1122-1133.

[3] Karakehayov, Z., *Low-power communication for wireless ad hoc networks*, Proc. ELECTRONICS'2003 International Conference, Sozopol, 2003, pp. 77-82.

[4] Karakehayov, Z., Low-power design for Smart Dust networks, in *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, edited by Mohammad Ilyas and Imad Mahgoub, CRC Press LLC, 2005, pp. 37-1 - 37-12.

[5] Voigt T., H. Ritter, J. Schiller, *Solar-Aware Routing in Wireless Sensor Networks*, Personal Wireless Communication, pp. 847-852, 2003.

[6] Yeatman E., M., *Advances In Power Sources For Wireless Sensor Nodes*, Proceedings of The 1st Int. Workshop on Body Sensor Networks, London, 2004, pp. 108-113, 1998.

[7] Karlof C., D. Wagner. *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures.* Proceedings of The First IEEE International Workshop on Sensor Networks, Protocols and Applications, 2003, pp. 113-127.

[8] Karakehayov Z., *Design of Distributed Sensor Networks for Security and Defense*, In Proceedings of the NATO Advanced Research Workshop on Cyberspace Security and Defense: Research Issues, (Gdansk, September 6-9, 2004), edited by J. S. Kowalik, J. Gorski and A. Sachenko, Springer, NATO Science Series II, Vol. 196, 2005, pp. 177-192.

[9] Karakehayov Z., *Using REWARD to Detect Team Black-hole Attacks in Wireless Sensor Networks*, Workshop on Real-World Wireless Sensor Networks, REALWSN'5, June, Stockholm, 2005.

[10] Karakehayov Z., I. Radev, *REWARD: A Routing Method for Ad-hoc Networks with Adjustable Security Capability*, NATO Advanced Research Workshop "Security and Embedded Systems", Patras, August, 2005, pp. 180-187.

[11] Hwang D. D., B. C. Lai, I. Verbauwhede, *Energy-Memory-Security Tradeoffs in Distributed Sensor Networks*, Proceedings Third International Conference Ad-Hoc, Mobile, and Wireless Networks, Vancouver, 2004, pp. 70-81.

[12] Wolf W., *How Many System Architectures?*, IEEE Computer, March, 2003, pp. 93-95.

[13] Karakehayov Z., K. S. Christensen, O. Winther, *Embedded Systems Design with 8051 Microcontrollers*, Dekker, 1999.

[14] Atmel Corporation, *ATmega128 AVR 8-Bit RISC Microcontroller*. Available at www.atmel.com.

[15] Atmel Corporation, *ARM7TDMI (Thumb) Datasheet*, 1999. Available at www.atmel.com.