Polygonal Broadcast for Sensor Networks

(Extended Abstract)

Shlomi Dolev Ted Herman Limor Lahiani

***Abstract*— This work considers communication among sensors that are spread in a geographic region. Each sensor is a computing device with severe resources limitations, low power, slow processing and small memory. The devices are distributed (uniformly) in the geographic region. In this work we present self-stabilizing broadcast, flooding and sense of direction procedures that fit the special characteristics of the system. Imaginary polygons tilings are presented as a general scheme for supporting communication in sensor networks. The broadcast procedures are used by a sensor for distributing secrets that activate the sensors simultaneously at a particular time without revealing the nature of the upcoming activity.**

I. Introduction

There is a great interest and attention of industry and research communities in the capabilities of small computing devices, called *sensors*, that use wireless communication among themselves [1], [7]. The applications for such devices in creating a global computing environment [6] may change our view on computers and computing.

The new special settings of such systems require careful examination, and rethinking concerning the methodologies and technologies used for coordination. Energy limitation is a concern in sensor networks. Message transmission is much more expensive, in energy terms, than message receiving. Moreover, energy required for transmission can grow more than quadratically with the distance imposing locality of transmission [8]. One would like to broadcast a message while *ensuring that most of the sensors will not have to transmit messages*. In a sense, a backbone of the network should be constructed, such that local broadcasts of some radius r of the backbone sensors will ensure global coverage of the geographic region in which the sensors are located. The geographic coverage requirement is a consequence of the possibility for having passive sensors that only receive messages (perhaps in a mode used to harvest more energy) such that other sensors are not aware of their existence. Moreover, the backbone may not be a fixed back-bone, but could be an ad-hoc defined back-bone for each particular broadcast. The existence of several back-bones, spanned by different set of representative sensors, distributes the energy usage in a balanced fashion among the sensors.

We present several schemes based on imaginary (or virtual) partition of the plane into (all possible) regular polygons: triangles, squares and hexagons; we call this an imaginary tiling because no permanent tiling or clustering of the sensors is established. Each polygon in the tiling has a representative sensor who is responsible for local-broadcasting the message to all the sensors in its polygon region, the representative can be elected according to different parameters such as, its relative location in the polygon, the maximum available power, the minimum transmitting energy, etc. The polygons representatives form the ad-hoc back-bone, they are the only transmitting sensors of a broadcast/flood, while all the others are receiving. The scheme abstracts the specific transmission radius of the devices, by allowing the length of a polygon edge to be a parameter.

Our broadcast schemes are extended to the case in which the sensors are not uniformly distributed. We use polygonal flooding in order to cope with empty or hardly populated areas. The polygonal flooding requires (an additional constant factor) more transmissions and storage of arriving messages in the sensors memory. Then we turn to the cases in which only portions of the network should be notified by presenting polygonal local broadcast and polygonal local flooding. We show that it is possible to send a message to a particular geographic relative location. The combination of polygonal send and polygonal local broadcast/flooding enables a remote broadcast to a particular region. We also demonstrate the way the imaginary tiling can be used to provide sense of direction.

*The first and the last authors are with the Department of Computer Science, of Ben Gurion University of the Negev, Beer-Sheva, Israel, Ted Herman is with the Department of Computer Science University of Iowa, Iowa City, Iowa, USA. Partially supported by IBM faculty award, NSF grant, the Israeli ministry of defense, Rita Altura trust chair in computer sciences and DARPA award. An extended version including details and references appears in [4]. Emails: {dolev,lahiani}@cs.bgu.ac.il and herman@cs.uiowa.edu.

Sense of direction is useful in many applications; for instance, sensors could direct an audience to building exits. Our sense of direction schemes are based on polygonal (backbone) flooding.

At last we examine a specific application of the polygonal broadcast/flooding schemes. Namely, we study the case in which an initiator would like to activate the sensors simultaneously and securely. An adversary that can observe the entire activity of every sensor including the initiator (see, e.g., [3] for similar settings), immediately after the initiator starts the broadcast and until the sensors are actually activated. In other words, we would like the sensors not to know what is the command (or if there is a command at all) in the arriving message.

To achieve the above we propose to use puzzles in the form of public key, transmitted by a satellite, used by the initiator to encrypt the command (the command decided upon sensing-an-event/user-request, is immediately eliminated from the initiator memory). Then the command is broadcast with the time the puzzle will be solved by the satellite. The command is decrypted and executed simultaneously, succeeding to cope with the inherent information flood initiator-receivers delay. Our sensor activation schemes uses unidirectional communication from a satellite. The sensors are not capable of transmitting messages to the satellite, therefore the satellite serves as a one way oracle that supplies puzzles and later the solutions. In addition, we allow the command itself to be encrypted by a (time) puzzle, in a way that a predefined period of computation time will be required by the sensors for decryption. In this way the end-to-end delay will be eliminated by the first (unidirectional satellite) scheme, while the flexibility in activation time will be tuned and controlled by the (sensor that is the) command initiator.

Related work and our contribution: We are the first to present (imaginary) polygonal broadcast, where no (global) location information is a must. There are several broadcast, flooding and message transmission schemes for sensor networks e.g., [1], [2], [7], [12]. Most schemes are based on flood, and therefore require that most of the sensors or even all of the sensors will actively participate in sending messages, which in turn uses a large amount of energy for each broadcast/flood.

Sense of direction in communication networks is an important paradigm that is extensively studied (e.g., [10]). We show ways to achieve this important task in sensor networks using the imaginary tiling.

Self-stabilization [5], using *time initializing* where timers reset flags and thus initiate the system, is suggested to make the system fault tolerant. Roughly speaking, the sensors change state to an initial state following a predefined period of time in which no (communication) activity is detected. Thus, the system reaches a predefined initial global state in which new (communication) activities are handled correctly. In the case one would like a fixed (i.e., sense of direction) output a floating (direction) output can be rewritten after each repeated computation (see [5] section 2.8). Thus, from every (possibly corrupted) initial configuration the system eventually recompute the (direction) output and every subsequence computation results with the same output, therefore the output is eventually fixed and correct.

There are several criteria to choose the specific tiling, the overhead the of transmission, the efficiency of the in-polygon broadcast (is it similar to a circle), the way broadcast propagates (say in relation to a breadth first search broadcast), and the next hop coordinates calculations. Our study shows that hexagons and squares tiling are better than triangles tiling for many of the above aspects. Hierarchical imaginary polygonal tiling structure is naturally defined, tuning the transmission radius using an approach similar to the one used for *topology control*. Finally, we note that our schemes can be easily extended to the case of three dimensions instead of a two dimension plane.

II. Polygonal Broadcast and Flooding

We propose schemes for broadcasting information. We try to minimize the *transport overhead* defined by the number of bits used to implement a header of the *polygonal transport layer*. The *polygonal transport layer* is defined by means of polygons rather than sensors, while the *data link* concerns include communication between particular (possibly polygon representatives) sensors. We present several examples in the sequel that clarify the transport overhead notion.

The initiator location defines the center of a regular polygon such as triangle, square or hexagon. The imaginary tiling is then inferred from the initiator's polygon (and the arbitrary orientation of the initiator's polygon chosen by the initiator). The initiator does not need to calculate the coordinates of the tiling; it only needs to use some convention among sensors concerning the type of polygon used and the length of the polygon's edge. In our schemes the initiator sends the message to a representative of neighboring polygons (to simplify the presentation, we suppose a sensor is at the center of each polygon, however in implementation a sensor elsewhere in the polygon simulates the actions of the center). The (relative) direction from which a broadcast arrives and additional bit(s)

of broadcast information control the behavior at the receiving polygon. Formally:

Definition II.1: A *polygonal broadcast scheme* S is a tuple $\langle \mathcal{T}, \mathcal{I}, \mathcal{F} \rangle$, where $\mathcal{I}$ is the algorithm of the initiator that specifies to the broadcast initiator how to initiate a broadcast, meaning, to which neighboring polygon it should send messages and what should be the broadcast bit(s) (transport overhead) attached to each of these messages; $\mathcal{F}$ specifies to each sensor how to forward a received message according to the broadcast bit(s) attached to it, meaning, to which neighboring polygons it should forward the message and what are the broadcast bit(s) that should be attached to that message in order to reach each polygon representative exactly once.

Note that the broadcast scheme considers the information (data) that should be broadcast as a black-box that accompanies each message that is sent (and hence received) by a sensor (thus, the additional bits can be viewed as a polygonal transport layer header [11]).

One potential application of a broadcast is to establish global orientation, establish a coordinate system, or carry local information to correct coordinate values.

The broadcast schemes presented in Figures 1, 2, 3 and 4 minimize the number of transmitting sensors and the *transport overhead* defined by the number of bits used to implement a header of the *polygonal transport layer* (defined by means of polygons rather than sensors). In the case of square or hexagon tiling, only one bit transport overhead is required for implementing the broadcast scheme, two bits are required in the case of triangle tiling.

In case of irregular distribution a flood is used, Figure 5 demonstrates a flood in a square tiling. More details, including impossibility results for more efficient schemes, can be found in [4].

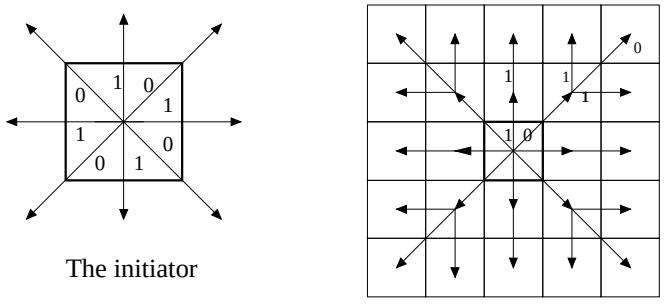

Fig. 1. One-bit broadcast scheme for square tiling

III. Sense of Direction

Sense of direction to several locations can be achieved by flooding the system as proposed in Section II leaving a pointer to the direction in which the first flood message arrived to every polygon. It can be useful for data queries [2]. A query initiator floods the system with a query and a sensor who has data relevant to that query, sends it along the path to the flood initiator on the fastest path defined by the flood-tree.

Another application based on sense of direction is finding a path to the nearest emergency exit in case of fire (or any other emergency event). In that case, we assume that

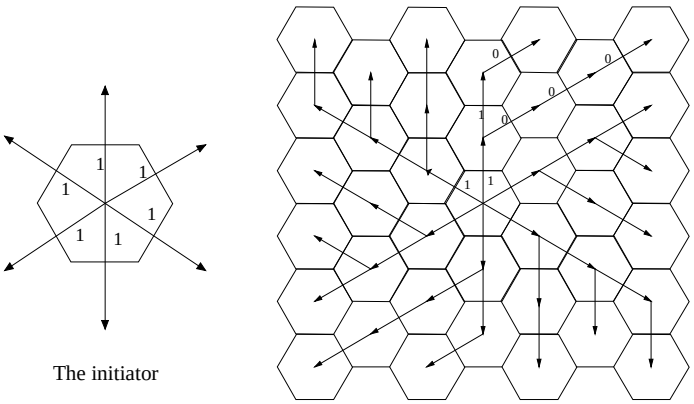

Fig. 2. One-bit broadcast scheme for hexagon tiling

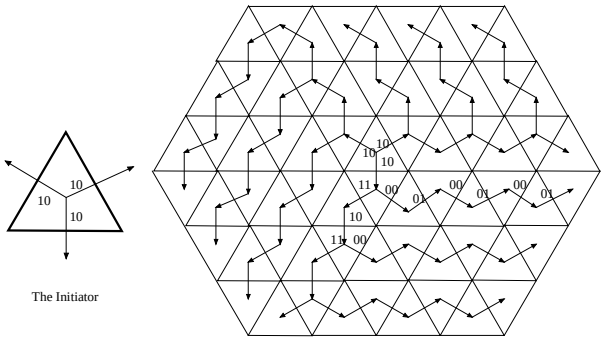

Fig. 3. Two-bits broadcast scheme for triangles tiling

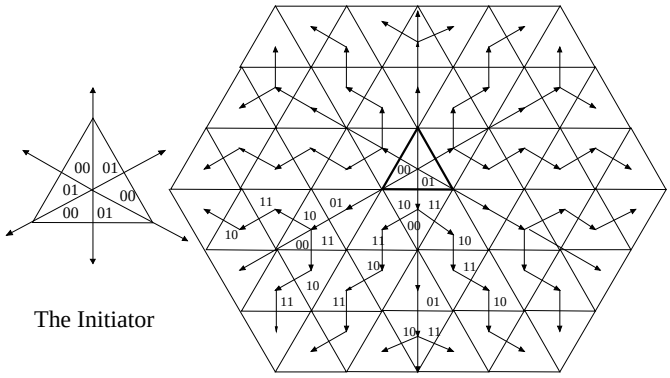

Fig. 4. Improved broadcast scheme for triangles tiling

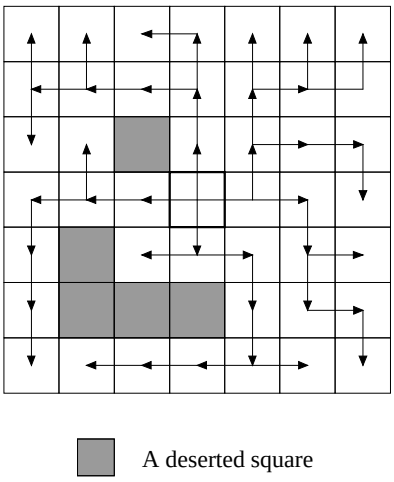

Fig. 5. Nondeterministic flood for square tiling

the fastest path from each sensor to any emergency exit e_i defines shortest (minimal distance) path to that exit. This application requires every flood message to be uniquely identified, so that every sensor would be able to identify flood messages from different emergency exits.

An emergency exit sensor s_{e_i}, representing an emergency exit e_i initiates a flood, the independent flood-trees are maintained by different pointers π_i each points to the direction in which the first flood message initiated by s_{e_i} arrived. Note that floods from different exits may start at different times, thus we propose to use the time difference between the flood initialization and the flood arrival as a criteria for choosing the direction to the closest exit. Δ_i denotes the time it took the flood message to arrive since it was sent by the flood initiator s_{e_i}. The flood messages carries the flood initialization time (or the amount of time elapsed since the flood initialization), thus every sensor records the shortest time required to reach each exit, later arriving messages from this exit are eliminated, as defined by the flood schemes. Note that we assume that there exists an average time for forwarding a message from a polygon to its neighbor, and the variance in the transmission time (say, due to retransmissions) is canceled along the message path. The path from sensor s_j to the nearest emergency exit is defined by the pointers π_i with the minimal Δ_i value. We note that the time decreases in a traversal defined by the π_i of the sensors, and thus the closest exit is reached.

IV. Secret Maturity and Sensor Activation

One of the main issues in sensor networks is the (simultaneous) activation of the sensors. We propose a scheme that activates the sensor in a secure way. The main idea is to flood the system with triggering information (encrypted) and use clock synchronization or satellite signal to activate the sensors. Secret maturity can be achieved by enforcing calculation of certain length (e.g., [9]), this however will still allow a gap of the flooding time in revealing the secret. Another option is to have outside entity (satellite) broadcasting a public key with promise to reveal the private key in Δt time units (where Δt is larger than the broadcast propagation time).

A satellite transmits a public key Ke_i and a private key Kd_i every Δt time units (we note that it is possible to have finer time granularity, we use Δt for simplifying the presentation). Ke_i is used to encrypt secrets, sent in time t_i and Kd_i for decrypting secrets encrypted (at time t_{i-1}) with Ke_{i-1}. Assume that a sensor s wants to initiate a synchronized activation, at time t_{i+1}, it encrypts the secret using Ke_i, throws away the original secret and floods the system (or uses local flooding), with its encrypted secret. At time t_{i+1}, all the sensors had received that secret, and received the private key Kd_{i+1}. Thus the sensors can decrypt the secret and execute the decrypted command. More details can be found in [4].

References

[1] I. F. Akylidz, W. Su, Y. Sankarasubramanian, and E. Cayirci. "Wireless sensor networks: a survey." *Computer Networks* (Elsevier), 38(4):393-422, 2002

[2] D. Braginsky and D. Estrin, "Rumor Routing Algorithm For Sensor Networks", *First Workshop on Sensor Networks and Applications* (WSNA), 2002.

[3] H. Chan, A. Perrig, D. Song, "Random Key Predistribution Schemes for Sensor Networks", *IEEE Symposium on Security and Privacy*, 2003.

[4] S. Dolev, T. Herman, L. Lahiani, TR #03-04 Department of Computer Science, Ben-Gurion University, Beer-Sheva, Israel, 2003. `http://www.cs.bgu.ac.il/~lahiani/tr0304.ps`.

[5] S. Dolev, *Self-Stabilization*, MIT Press, 2000.

[6] K. S. J. Pister, J. M. Kahn, and B. E. Boser, "Smart Dust: Wireless networks of millimeter-scale sensor nodes", Electronic Research Laboratory Research Summary, UC Berkeley, 1999

[7] H. Qi, P. T. Kurganti, and Y. Xu, "The Development of Localized Algorithms in Wireless Sensor Networks", Sensors 2002, 2, 286-293.

[8] V. Rodoplu, and T. H. Meng, "Minimum Energy Mobile Wireless Networks," *Proc. of the IEEE International Conference on Communication*, vol. 3, pp. 1633-1693, 1998.

[9] R. L. Rivest, A. Shamir, and D. A. Wagner. "Time-lock puzzles and timed-release Crypto", Technical Report, MIT/LCS/TR-684, 1996.

[10] N. Santoro, J. Urrutia and S. Zaks, "Sense of direction and communication complexity in distributed networks", *Proc. of the 1st International Workshop on Distributed Algorithms*, pp. 123-132, 1985.

[11] A. S. Tanenbaum, *Computer Networks*, Prentice Hall, 2000.

[12] F. Yen, H. Luo, J. Cheng, S. Lu, and L. Zhang, "A Two-Tier Data Dissemination Model for Large-scale Wireless Sensor Networks", MOBICOM 2002.