

Environmental Notification Support Using Passage Detecting Sensor Nodes

Daniel Reißner and Wolfram Hardt
Technische Universität Chemnitz, Germany

Abstract—Interconnected sensor nodes can be used for a long term monitoring of widely spread ecosystems. Individual nodes can be unavailable during the runtime due to a lack of energy, disruption of communication channels, or physical damages of nodes. In this paper, a new approach to transfer messages from nodes to gateways (and optional to flood gate nodes) in such dynamically disturbed networks is presented. The focus is the routing in branched line-structures, e.g. flood barriers. The usage of gradient structures in each node allow tree routing, tree propagation, energy-efficient exploring broadcast, exploitation of line-structures, and collection of position information. Additionally, a generic preference evaluation and decision making concept allows energy or signal quality evaluation, routing decision, structure setup decision, position estimation, synchronization adaption, and randomization of security approaches. It can be extended by further rules.

Index Terms—energy-efficient, gradient routing, preference-based, flood water, barrier, spread-broadcast

I. INTRODUCTION

In order to maintain and monitor barriers, sensor nodes can be placed in dykes and on walls to track water and saturation level. The gained information can be used to detect dangerous water levels or saturations mainly during flooding times. Since it is important to collect all information about the sensor states at central points, the wireless interconnection of nodes is useful. It helps to transfer all information even in the case of massive disruptions. Furthermore, costs for the installation along the coast of waters are saved. For low effort maintaining, energy-autarkic nodes are appropriate, e.g. by solar panels.

As shown in previous projects, flood water monitoring can be done using water pressure sensors [1], humidity sensors and certain node architecture [2] able to deal with half water immersed antennas [3]. Due to the distribution of the nodes along a coast line or river, the resulting structure of the sensor network will last in a line of nodes with less number of neighbors. The nodes can be equipped with wake-up receivers to allow energy efficient sleeping modes and asynchronous communication.

An approach for routing maintenance and alert message in this dedicated network structure is presented in this paper. During normal operation mode, the energy efficiency of the network structure and routing strategies are prioritized. In case of flooding, the probability of disturbances in the structure increases. In this case, the reliable transmission of alert messages to central nodes along the coast line is focused.

Basic idea of the approach is the *Passage*. It bases up on the line structure of the coast line or river and defines the different

shortest network paths to the gateways that can be reached without passing another gateway. Furthermore, in order to avoid plain text transfer of safety relevant data or to attack the network with manipulated data, a combination of variable key and variable encryption architecture is presented.

II. STATE OF THE ART

Trickle routing [4] increases the probability of successful transmission by multi-path routing. Each packet is transmitted on different routes. Obviously, this approach generates a lot of communication overhead and wastes a lot of energy. General gradient based routing allows routing from node to node using gradient mesh structures [5]. Messages are forwarded to neighbours according to some increasing or decreasing gradient value. In some cases, the sensor data can be used as gradient itself [6].

Clustering based approaches allow the grouping of nodes according to dedicated node properties, e.g. solar radiation [7]. Each cluster elects a cluster head. It works as a gateway between each node in the cluster and the heads of other clusters. Additional energy or resources are required for cluster head selection or maintaining and the transfer to final target nodes.

Existing gradient routing approaches introduce a cost function to keep messages in a certain band by sending a signal strength message during each forwarding step [8]. Accordingly, a message is sent via the strongest neighbours. Redundant messages can occur so that the reliability is increased but the energy efficiency is decreased.

Homogeneous Object Binding structure introduces flexible group-value messages able to transfer gradient information as energy-efficient attachment [9] without additional header overhead. In sensor nodes group-value format allows for flexible neighbor and management information tables simplifying data access.

Existing security mechanisms expect HW support of microcontroller, introducing additional key layer in software. In [10] such keys are generated by the server and distributed in messages throughout the network.

Most of the sensor network approaches do not consider concrete applications and the resulting influences to the structure of network. In opposite, preference based routing bases up on the concept of gradient based routing but introduces dedicated adaptations to application dependent network structures [11]. It introduces spatial and temporal relations between the

nodes and the measurements. The wake-up and communication schedules are adapted as well as the routing strategy. The approach presented in this paper adapts to the concrete structure of nodes along a coast line or river as well and introduces optimised routing approaches.

III. GENERAL PREFERENCE CONCEPT

The preference P is a general concept for qualitative integration of parameter values (p_i). In combination with a weighting (w_i) of each parameter, a quantitative cost is determined. Additionally, the resulting costs realise an activation to perform an associated action or decision. The combination of cost value and cost label associated action is called Preference. Each node implements a preference controller that determines all necessary values (p_i) and calculates the preference based on the weightings. For different applications or application modes, different preferences can be calculated.

A homogeneous object binding structure [9] is used in order to allow a light weighted implementation of the preference controller. The parameters p_i , w_i and the preference P_j are stored in several tables. Group parameters are attached to the entries. Hence, parameters can be accessed easily during runtime. Group attributes provide decision support for selection of parameter sets in the actual preference mode. For example, the group sizes of dynamic group-value pairs enable automated transmissions of measured values after scanning a complete set of values. Hence, packets of fixed length can be transferred more reliable considering static group length indicator.

In order to express the integration, the dependency Operator $\xrightarrow{\square}$ is proposed allowing for weighted sum, comparisons of measure boundaries and intervals, weightings or order relations. The control information (stating which operation to perform) as well as the parameters and sub-preferences are grouped in an Application Gradient Object. The resulting interaction between group structure, dependency operator and action realizable preference measure are illustrated in following figure 1.

Depending on configuration information in current group, preference controller may contain additional stages for reweighting of parameters by error checking. Dependency operator allows for design of program loops for wakeup, measuring, checking receive queue, processing, sending and sleep. Dependency operator is used as max operator to choose best preference from neighbour groups comparison. Furthermore a count operator is used to allow detection of passages described in next chapter.

Furthermore dependency Operator allows for definition of shortcut boundary check and activation using preference.

$P \xrightarrow{a, >} b_i$:
 If $P > b_i$: $P = p1*w1 + p2*w2 + \dots + pn*wn$ else $P=0$;
 If $P > 0$: perform action a ;
 return P ;

where $\xrightarrow{a, >}$ operator returns the evaluation result of Preference integration and in case of activated action performs associated action on reaching the boundary. This allows for a generic

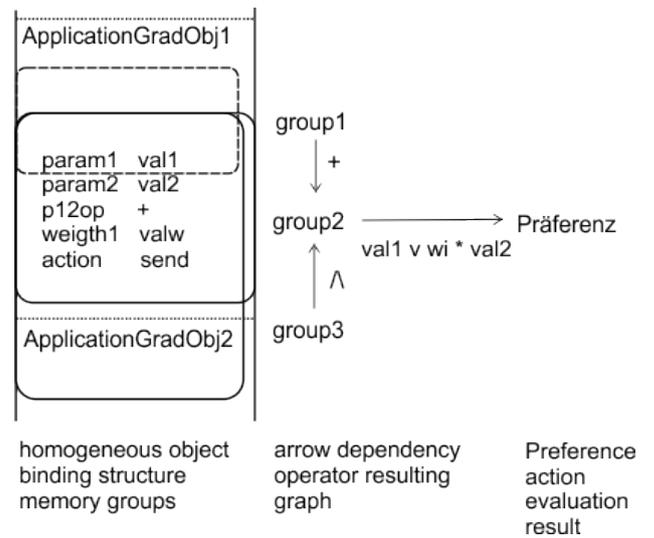


Fig. 1. General Preference Controller operates with dependency operator on application object groups generating a preference; in case action control information is available, action will be performed

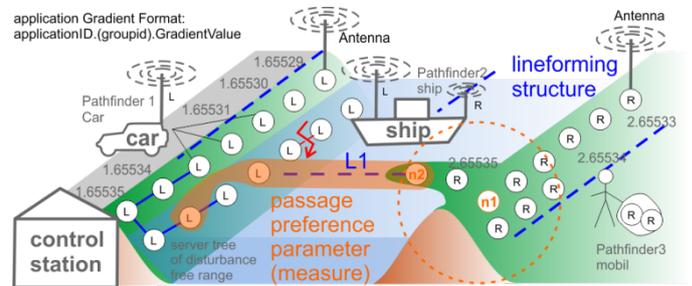


Fig. 2. flood water disturbances in dike line forming network; barrier preference weightable special nodes (car, control stand, antenna gateway, ship, dike side L/R, rough oder/groups from embedding in barrier); passage detect

short representation of intervals for a hierarchical controllable controller realization.

$P_k \xrightarrow{a, >} (P_i \xrightarrow{a, >} b_i) \xrightarrow{\square} (P_j \xrightarrow{a, >} b_i)$
 $\xrightarrow{a, >}$ expresses $P_i > b_i$ and $\xrightarrow{a, <=}$ expresses $P_j < b_i$. Hence, $\xrightarrow{a, >}$ results in a value unequal to zero only if both conditions fit. An implicit logical “and” operation of $\xrightarrow{\square}$ Operator can be expressed by multiplication. Open intervals are expressible by $+$ operator allowing logic “or” expressions. Boundaries, intervals, and logic selections are expressed by hierarchically applying cut and union sets on sub preferences.

The preference evaluates these expressions to an action and allows implicit error adaptation during the runtime by changing the according weights w_i .

IV. PASSAGE ROUTING PREFERENCE

Several servers are provided for the sensor network along the coast lines or dikes fig. 2. Each server maintains a gradient based network in order to improve routing and to estimate the position of the nodes. Mobile servers, e.g. in cars or ships, provide gradient networks for a restricted period. Nodes can belong to several gradient networks.

4 different message types are supported and managed. Alert Messages need to reach its destination with maximal probability. Data Messages have to be transmitted in energy efficient routes; messages losses are acceptable. Maintenance Messages are used for setup and maintenance of the network. The transmission reliability is less for this kind of messages. The server is the typical destination or source for all this messages. In opposite, node-to-node messages can be transmitted between 2 nodes in the network with high transmission reliability.

Alert messages are transmitted from one node to every server. Typically, it is sent along the 2 lines (up and down the coast line). The alert message is duplicated at every bridge or crossing point of the network and addressed to every available server. The forwarding decisions base up on the gradients, the signal quality, the available energy of alternative nodes, and the distance to the nodes of some gradients.

Server initiated gradient propagation allows shortest paths between nodes and the estimation of initial positions. The advantage is that the uniquely distributed gradient provides globally optimal distance information. It allows nodes to send along shortest path to server without requiring path recalculations. The disadvantage is that the redistribution in the complete network is necessary in case of disturbances.

In opposite, the presented approach uses spread broadcasts in the case of broken paths or missing gradients. In case of missing node gradient information, this information is distributed with first transmission attached as group-value pair to data message. If a node receives a message from a neighbour with bigger broadcast-source-gradient it will not redundantly relay this message. The relaying to the original source of the message is avoided by gradient comparison. If a broadcasted message reaches a node with gradient information the broadcast is stopped and the message is routed along the gradient structure. The according node propagates the gradient to the forwarder of the broadcast message. Hence the size of the gradient based network is increased. In order to save transmissions the back propagated gradient is encoded in the acknowledge message.

Line structured networks result by the installation of nodes along linear expanding dikes or coasts. The structures are characterized by contiguous nodes and allow stable connections due to the node denseness. Additionally, line structures realise direct routing to the server and prevent routing cycles along local neighbours.

A concept that extends the gradient routing by so called Passages nodes needs to be introduced in order to use the line structures.

A node n1 calls another node n2 as passage node if n2 has a connection to the maximal number of foreign nodes and if n2 has the maximal distance (hops) to n1 (fig. 2). The inductive comparison in next node, with maximal number of foreign nodes results in a line L1. Hence, passage neighbours are the start of a logic Routing Passage directing to dedicated nodes and using real line structures.

Dedicated nodes are servers, gateways, connected cars, or

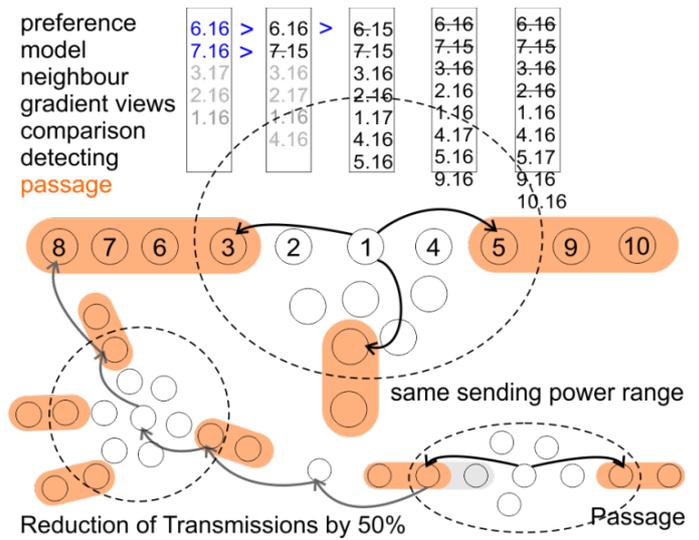


Fig. 3. top: passage detection starting node by comparison of neighbour gradient views in node 1; bottom: short cut by 50% by skipping one node per passage detection

ships. A passage neighbour knows the maximal number of unknown nodes due to a distributed gradient of forwarding nodes.

A Passage is a segment of a route from the passage neighbour to the dedicated node. The length of the segment depends on the transmission distance of the neighbour. Energy efficient local decisions are possible based on the global knowledge of the gradients.

Routing along all passages increases the probability of successful transmission of critical alert messages in the case of temporarily disturbed connections. Tracing messages of less priority are transmitted automatically to the efficient nodes by preference-based node evaluation. This evaluation is adopted dynamically considering the connectivity of each node.

A node n1 compares the gradient information of its neighbours and selects a neighbour, which knows most non-neighbourhood (foreign) nodes and has a shorter distance to the server (fig 3).

Parameters, like the number of foreign nodes, the server bonus, or the initially obtained gradient, are used for the calculation of preferences and is considered to build up a Passage Routing Preference.

The passage routing preference results in energy-saving by 50% of messages/pathlength in the case of a sending range of two neighbour hops per node (fig 3 bottom).

Groups of nodes are introduced in order to manage the handling and storage of gradient values of neighbored nodes. A node needs to store only the gradients of the neighbours in its own group. Additionally, information about the connection to other groups is necessary.

The gradients decrease from the server to the nodes of different layers iteratively. A node becomes a relay node if it has a gradient of 0. In this case, it opens a new group and increase its gradient. The propagation is continued in the new

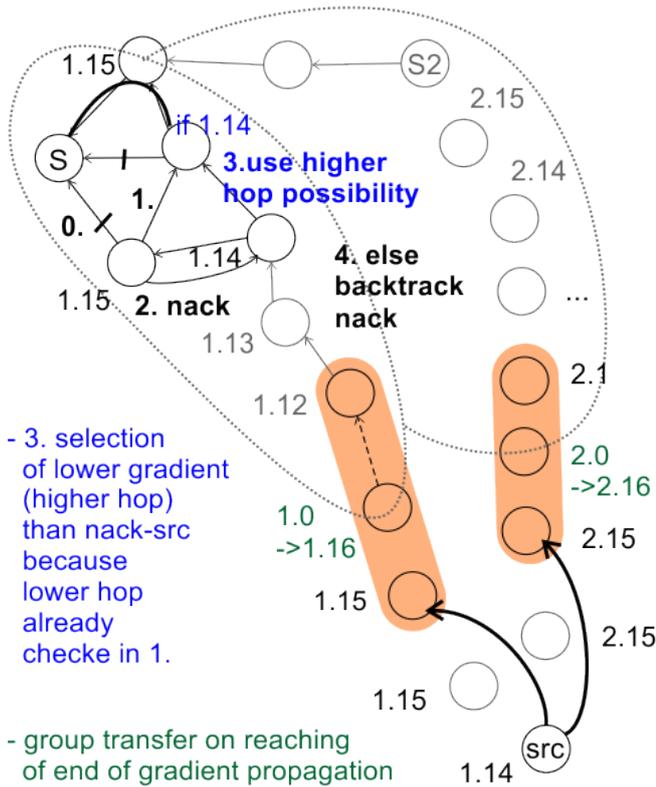


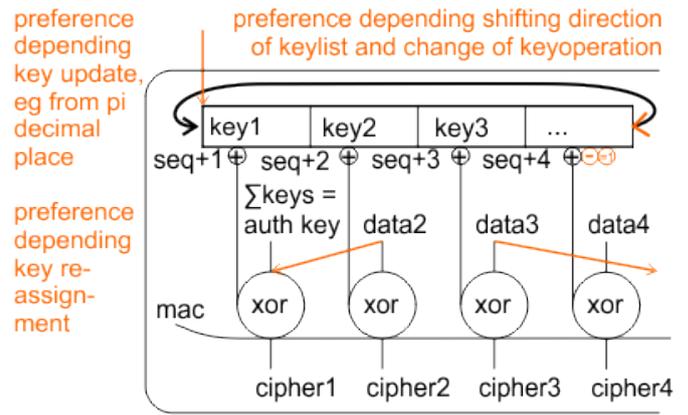
Fig. 4. lineforming groups network; top: disturbance adaption for medium reliability messages; bottom group-gradient transfer for reduced gradient memory overhead

group. Nodes of a group send messages always to this relay node so that it acts as some kind of local server.

The relay extends the actual group by a groupTransferFlag to realise the transition during the preference determination. Hence, gradient values can be stored with less memory. Additionally, the number of assigned gradients is decreased by the number of relayed groups and the number of available servers.

Data messages have to reach the destination with an average reliability. In case of transmission disturbances, a new node is searched according to the preference approach. A "NACK" message is backpropagated to the forwarder of a message if no new node can be found. If a node receives a NACK, it takes the according message from its cache and tries to resend to another node on the route to the destination (fig. 4). Nodes with greater or equal gradient for the same server are not considered as new forwarding targets. These nodes were excluded already due to the signal quality consideration. The backpropagation is executed only for one level if the messages are alert messages or less prioritised maintenance messages.

A special kind of messages are node-to-node messages. This can be routed directly between different types of sensor nodes, e.g. water level sensors, water pressure sensors, etc. To in-



Ciphering-Example:	key1	key2	key3
basekeys:	1011	0011	0010
preference operand:	0010	0001	0011
eg from seq cnt, shift, +, xor			
pref operation eg add:	1101	0100	0101
data:	0000	1111	1010
auth Key $11+3+2 \text{ mod } 16 = 0$		data0	data1
Ciphering prefkey xor data:	1101	1011	1111
Decoding-Example:	1101	1011	1111
using same pref calculation:	1101	0100	0101
data from xor:	0000	1111	1010

Fig. 5. preference-randomized node data ciphering and authentication, integrating cbr approach in ciphering preference; top: encryption of message HW Realization also realizable in software in microcontroller; bottom: decryption and authentication verification for sample with three keys

crease the transmission reliability, a confirmation message has to be send from the receiver to the sender. If this confirmation is not received after a dedicated time, the sender retransmit the message ones.

The approach of preferences allows the extention or adaptation of the parameter modelling by using weights. Furthermore, the preference value (implicitly associated with sender address) can be transmitted easily and energy efficiently between nodes.

The introduction of further paramerts for the calculation of the preference is possible. Properties like node mobilites (car, ship, etc.), positions (side of dike, etc.), or the node hierarchy type (server, antenna, gateway) can be used to improve the quality of the calculated preference. Gradient information gives hop distance measure and can be integrated with travel time and installation time group and node orders to give more accurate position estimate.

Finally, the security of the transmission can be increased by the integration of preferences to a varying keys and chipering schema (fig. 5).

A new variable encryption preference needs to be repeated until the sender has received an acknowledge by the receiver of it. After this, the new preference is used for transmission. A flag indicates that message has to be decrypted with the new preference.

$$rtfactor = \frac{myHPG}{fRtCnt(maxuseRtCnt)} //base\ value$$

$$rssifactor = \frac{hpg(level-1) - hpg(mylevel)}{maxRssi} //one\ hop\ level\ dec$$

$$SignalQuality = \frac{curRtCnt * rtfactor * rssifactor}{-(curRtCnt - 1) * rssifactor * curmeasrssi}$$

Fig. 6. overview of Signal Quality Calculations

$$Energy = (U) * I * t = I * t = I * numChars * chartime$$

$$= I * numChars * \frac{1s}{numChars} = I * numChars * \frac{1}{datarate}$$

$$Energy = \begin{cases} 174 * \frac{numChars}{250kbps} & | \text{Message received} \\ 188 * \frac{numChars}{250kbps} & | \text{Message send} \\ 3 & | \text{wake //asumed 0.3ma for 1s} \end{cases}$$

Fig. 7. overview of Sending and receiving Energy Model

An array of similar keys per node and a random basic preference is used to prohibit attackers from scanning initial keys. The receiver can determine the basic preference of a sender by its knowledge of the initial key array. In opposite, an attacker receives only randomised data so that he cannot reconstruct keys from equal messages.

V. WEIGHTING MECHANISM

The presented approach has been simulated and compared to another approach.

In the simulation model, the signal quality is considered to change one hop level by scaling definition and includes the scaled retransmission count RtCnt as well as the RSSI-Quality (fig. 6). myHPG is the hop-power-gradient [10] - a gradient value with squared function interval. It maps the power values to provide more server-near resolution for distinguishing far away nodes in global order.

Initially, the energy (fig. 7) scales within the complete range of the hop-power-gradient to allow drain node in global gradient network order to zero. The supply voltage is assumed as constant and therefore not integrated. The scaling of units was done to get small integer values that can be implemented efficiently on microcontrollers:

The hop-power-gradient is calculated by equations from [11]. The RtCnt follows the equation $fRtCnt = (2 * rtcount)^2$ as scaling with hop relevant impact. Furthermore, rtfactor scales to a parameter depending maximal value RtCnt.

The tree update parameter "nodeUpdateRate" results from applicational parameters, e.g. from the frequency of requests to get humidity data.

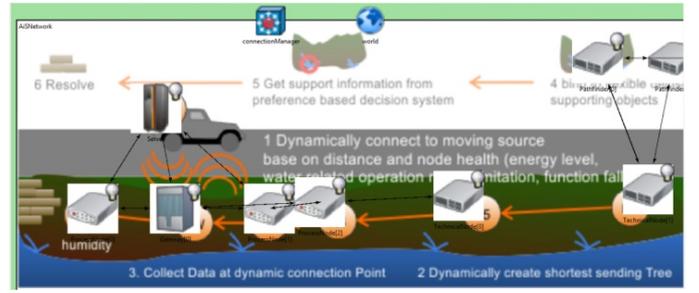


Fig. 8. flood water disturbances in network basic spreaded broadcast exploration of way to possibly moving server.

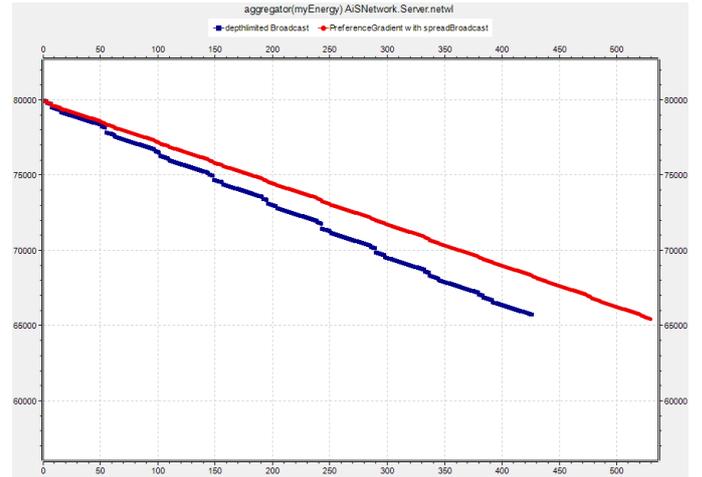


Fig. 9. Energy saving of preference-based gradient routing (red) compared to depth limited broadcast (blue); despite additional acknowledge messages in the preference-based gradient approach

VI. RESULTS

In order to test the routing approach, a flood water scenario - as shown in Fig. 8 - was simulated in Omnet++. The implemented routing approaches allow forwarding of data in the case of missing gradients. A basic realisation of a spreading broadcast approach is used in this case.

With increasing number of nodes energy is saved over time for each broadcast cell. As soon as structure information about the gradient tree is available, preference gradient improves the structure. The depth limited broadcast does not consider additional structure or other parameter information and broadcasts in all systems per message (not limited by tree structure as with preference gradient).

The depth limited broadcast transmits messages efficiently in all directions. But due to the attached sequence number of each message, the energy consumption for the transmission of each message is increased. Hence, more energy is needed compared to the gradient-based broadcast of the preference-based routing. The gradient-based broadcast uses the gradient information of the initial server-driven gradient distribution. Hence, it does not generate overhead in the messages.

The Leach approach of reaching destination addresses directly is not performable in huge distributed networks. It is

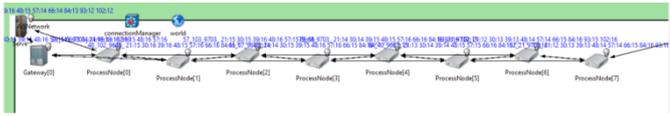


Fig. 10. line forming network with overlapping sending ranges for passage detection; using server, gateway, sensor nodes and activating node

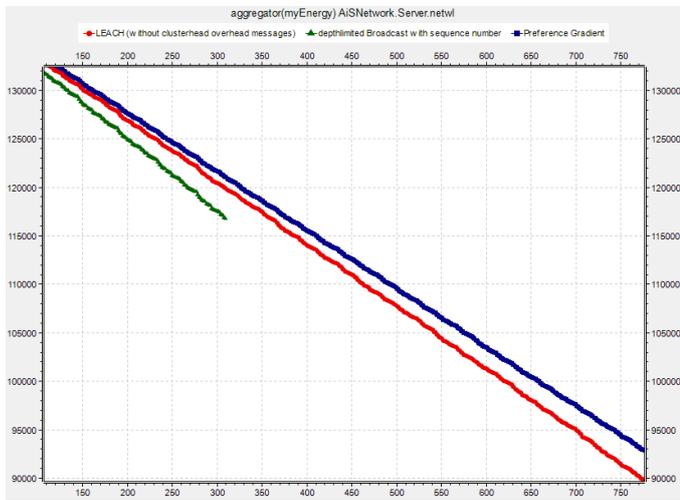


Fig. 11. reduction of network energy over time by message transfer to server; sequence number broadcast wastes most energy; optimistic view on gradient routing requires more energy by indirection to cluster head than energy-efficient preference gradient routing

even not suitable for small networks if restricted bands are used. Additional transmissions are necessary, e.g. to restrict the cluster heads. The energy consumption is higher as compared to the preference-based routing due to temporarily insufficient cluster heads.

The line forming network in fig. 10, 11 was used for a second simulation to compare broadcast, LEACH and the preference gradient optimised approach of this paper. For comparison, an external node simulated periodic activations at the end of the network line and in the middle of it. Cluster heads were iterated sequentially (randomisation, energy-distribution) over all nodes, requiring additional transmissions from node to

clusterhead and clusterhead to server for indirections not using directly shortest gradient path.

VII. CONCLUSION AND OUTLOOK

In this paper, a routing approach was presented. It allows the exploitation of situational parameters and enables shortest paths from nodes to the server even in disturbance situations. Therefore, an optimised broadcast is used. It keeps the resource consumption as low as possible by considering available gradient information. Preference based decision making is used for routing decision, and adaptive node synchronisation. Additionally, it is extended to pattern randomization for cipher generation. Thereby, only disturbance free and group relevant messages are transferred by authentication in order to save energy resources.

It is planned as future work to realise the observer mechanism. Actually, it is conceptual approach to enable the autonomous weighting of parameters.

REFERENCES

- [1] Microsoft Research, <http://research.microsoft.com/en-us/collaboration/focus/e3/sensornetwork.aspx>, September 2014
- [2] Zainah Md. Zain and M.N.M.Khalid, *Development of Flood Detector System Using MC68HC11 Microcontroller*, SCORED Dec. 2007
- [3] M. F. Farooqui, Christian Claudel, and Atif Shamim, *An Inkjet-Printed Buoyant 3-D Lagrangian Sensor for Real-Time Flood Monitoring*
- [4] P. Levis, *Trickle: a self-regulating algorithm for code propagation and maintenance in wireless sensor networks*, NSDI'04 V. 1 P. 2-2
- [5] T. Watteyne, *Implementation of Gradient Routing in Wireless Sensor Networks*, GLOBECOM 2009. IEEE , pp.1,6, Nov. 30 2009
- [6] C. Buchhorsts, *Natural Gradient Routing: Sink convergence using data as guide*, LATINCOM 2013 IEEE pp.1,6,24 Nov. 2013
- [7] T. Voigt, *Solar-aware Clustering in Wireless Sensor Networks*, ISCC 2004
- [8] Fan Ye, Gargy Zhong, *GRAdient Broadcast: A Robust Data Delivery Protocol for Large Scale sensor networks*, Journal Wireless Networks, Volume 11 issue 3, May 2005, Pages 285 - 298 Sensor Networks
- [9] Daniel Reißner, Wolfram Hardt *In Process Homogeneous Object-Binding Structure for Preference Zone Based Decision Making*, Knowledge-Based Software Engineering 11th Joint Conference JCKBSE 2014, Volgograd Russia, September 17-20, 2014
- [10] Morten Tranberg Hansen, *Asynchronous group key distribution on top of the cc2420 security mechanisms for senso networks*; Second ACM Conference on Wireless Network Security, WISEC 2009, Zurich, Switzerland, March 16-19, 2009
- [11] D. Reissner, F. Strakosch, *Energy-efficient adaptive communication by preference-based routing and forecasting*, SSD 11-14 Feb. 2014