In Proc. of the European Workshop on Wireless Sensor Networks, IEEE, Jan 2005
Pages 226--235, ISBN: 0-7803-8802-X

Using energy where it counts: Protecting important messages in the link layer

Andreas Köpke, Holger Karl, Marc Löbbers
Telecommunication Networks Group, Technische Universität Berlin
Sekr. FT5-2, Einsteinufer 25, 10587 Berlin, Germany

Email: {koepke|loebbers}@tkn.tu-berlin.de, holger.karl@uni-paderborn.de

***Abstract*— Saving energy is the most important goal in a sensor network. But shortsighted optimization for energy can lead to sensor networks that can not fulfill their task. Hence, this goal must be balanced with task related goals. One such task related goal is to transmit messages in a sufficiently reliable way. For instance for a monitoring sensor network this means that the messages that arrive at the sink node allow a good overview of the monitored area, while at the same time no energy resources are wasted. In this paper we define a "good overview" as the "informational value" that arrives at the sink node and adapt the reliability of the link layer such that the overall system efficiency is maximized. The system efficiency is defined as the informational value arriving at the sink put into relation with the energy spent by the network to get it there. Our major result is that there exists a rule that describes how to adapt the reliability of the link layer, which can be evaluated by each node using only locally available information. When the reliability of the link layer is adapted according to this rule, the system efficiency can be increased (sometimes by more than 20%) compared to the best performing non-adaptive link layer.**

I. Introduction

Saving energy is an important goal in Wireless Sensor Network (WSN). It is used as the main optimization objective, while other objectives like throughput, delay and reliability are less important. But saving energy alone does not lead to a system that can fulfill a task; because it is very energy-efficient not to do anything at all. As an example, consider the case of a sensor network that monitors a forest for beginning fires or changes in the probability for a fire. To fulfill its task, it can report the temperature and humidity periodically and beginning fires using alarm messages. The alarm messages occur very rarely, but if they occur they are very important and must be transmitted reliably. The periodic reports, on the other hand, consume a large amount of energy, hence their transmission should be optimized to save energy. Furthermore, the periodic reports are less important, because they can be extrapolated either using past sensor readings or readings from other sensors. In this sense, they carry less informational value than the alarm messages. It seems to be a good idea to transmit more important messages more reliably than less important messages, in order to achieve an optimal balance between energy expenditure and reliability. In this paper, we deal with the question how an optimal balance can be found by adapting the reliability of the link layer using the informational value of a message.

The distinction between two classes of messages (periodic reports and alarm messages) is not general enough and does not capture some important cases in sensor networks. In sensor networks, often aggregation mechanisms are used to lower the number of transmitted messages. Such a case is shown in Figure 1.

In this aggregation example, the nodes report their sensor readings to their parents in the tree. When all children of a node have answered, the messages are combined into a single one and forwarded to the next node. This convergecast is a suitable scheme to transmit the periodic reports in an energy-efficient way. During the convergecast, some messages contain the aggregated readings of more and more nodes. These messages carry more informational value and should therefore be sent more reliably. In this case, it seems to be easy to define a measure for the informational value of a message: just count the number of contributing nodes. While this approach is simple, it is not general enough. We will present other measures for the informational value in Section III.

Holger Karl is now full professor at University of Paderborn

This work has been partially sponsored by the European Commission under the contract IST-2001-34734 – Energy-efficient sensor networks (EYES).

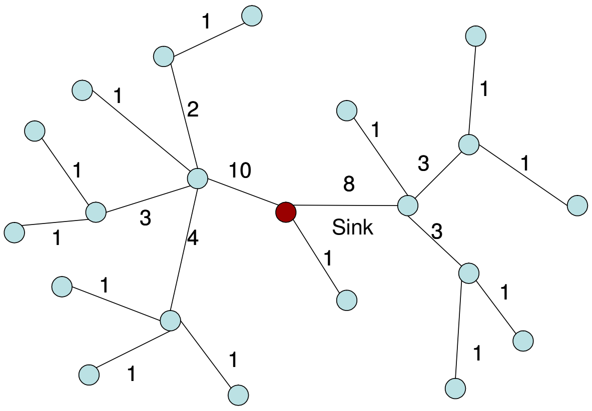

Fig. 1. Convergecast tree with number of aggregated sensor readings communicated over each link

Using the (suitably defined) informational value, the link layer of a node chooses a sufficiently reliable way to transmit the message. One way to transmit a message reliably is the transmission using an Automatic Repeat reQuest (ARQ) protocol[1]. An ARQ protocol has at least the overhead of the Acknowledgments (ACKs) plus the retransmissions. The higher the number of possible retransmissions the higher the probability that a message arrives at the parent node, but the higher also the energy spent to send the message.

In the tradeoff between energy expenditure and reliability the overall system efficiency should be maximized. System efficiency is defined as the informational value arriving at the sink node (v_r) put into relation with the energy spend to get it there (η_r). To maximize the system efficiency ($L = v_r/\eta_r$), each node has to decide how reliably a message should be transmitted. Ideally, each node decides locally, without any additional communication. Otherwise the communication overhead may easily exceed the energy savings of a link layer that adapts the reliability of the transmission.

Before we present a local rule to choose the optimal reliable way (maximizing the system efficiency defined above) to transmit a message – the optimal protection of the message by the link layer – in Section VI, we start with a strict mathematical formulation of the optimization problem. The mathematical formulation allows the computation of the system efficiency for a specific way of choosing the protection given the message value. However, the formulation does not easily lead to a rule that can be used by each node to make a decision on the protection it should use. As a major result of this work, we present a rule that every node can evaluate *locally* that approximates the optimal system efficiency very closely.

II. Related work

In this paper, which can be seen as a continuation of [1], we concentrate on the reliable transmission of data from the source to the sink, where each node on the route contributes. More generally, we concentrate on end-to-end reliability with an energy constraint. A similar goal is investigated by Stathopoulos and Estrin [2]. In their approach, the sink node decides which source node should be asked to retransmit its message. This question is closely related to our approach, however, we concentrate on the question how *each node on the route* can contribute to the reliability, instead of leaving this decision to the sink node. The other direction, from the sink to the sensors is examined by Park et al. [3]. It remains part of future work to see how their approach can be fitted into a system with messages with different informational value.

If the correlation between the sensor readings is used, a different notion of reliability is more appropriate: the event to sink reliability, introduced in [4]. They assume that sensor readings are by nature correlated and it is sufficient for at least one message to arrive at the sink. From an energy point of view, it might be better not to send the redundant messages at all, but to compress the messages into a single, high valued one.

At first glance the work done to optimize energy expenditure by building optimal convergecast trees and clusters seems to be related. It is not; aggregation is just used as an example. Optimizing the aggregation structure with some clever clustering or tree building algorithm is not considered in this paper. Furthermore, the local rule that we propose here is completely oblivious to the underlying aggregation structure, therefore we conjecture[2] that an optimal aggregation structure comes as an additional benefit, but has no influence on how reliable a node forwards a message. The specific measure for the informational value that is used as an example has some relation with an aggregation structure, however, our approach is much more general as we will exemplify in the next section.

III. Informational value

The definition of the informational value is not an easy task, since it can not easily be defined without

[1] Error Correcting Codes (ECCs) are also evaluated in this paper, but omitted here for clarity reasons.

[2] Computation results for other graphs support this claim.

application specific knowledge. In sensor networks, this knowledge is available and the protocol stack can be designed such that this information can be passed to the link layer. This is a unique feature for sensor networks and explains why the “Quality of Service” of conventional networks research is not directly related.

Application specific measures are – when suitably defined – probably the best possible measures for the informational value. Their disadvantage is that someone has to define them carefully, which can be a tedious work. We present some measures for the informational value that are more general, and can be used by more than one application.

A. *Count-based measure*

For the aggregation example, we have already introduced a very simple and readily available measure for the informational content: the count based measure. The informational value of a packet is defined as the number of sensor readings aggregated into a forwarded packet. It is easy to compute and does not need any additional information or support from the network, the convergecast tree is sufficient. In this paper, we use it to compute the system efficiency, a necessary step to find the maximum. But this measure has its shortcomings, especially when the sensors are distributed randomly and some areas are observed by many sensors and some are observed by just a few.

B. *Area-based measures*

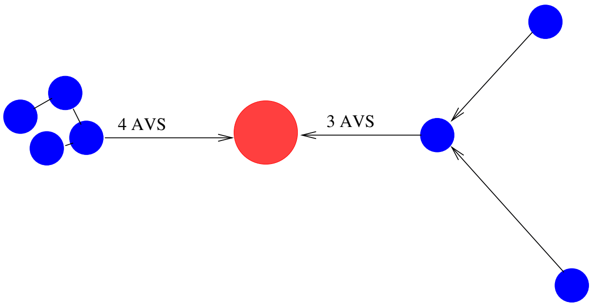

Fig. 2. Unequally distributed sensors

Figure 2 shows such a case where sensors are unevenly distributed. Here, the left side will contribute more informational value if simply contributing sensors are counted. However, the left side covers a much smaller area than the right side and this should have an influence on the value.

A possible way to measure the impact of the covered area on the informational value is to assign each sensor an area that it observes and use the area of the circumscribing circle as the measure of the informational value. This is shown in Figure 3. The problem with this measure is that it grows rapidly. Also it does not reflect the fact how the sensors are distributed in it – if all sensors are in a small area on the left and one is on the far right, it will still assign a large value to the message.

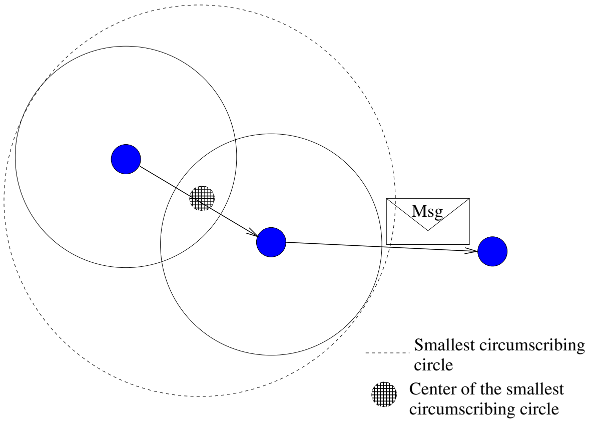
Msg
Smallest circumscribing circle
Center of the smallest circumscribing circle

Fig. 3. Circumscribing circle

A third possible measure tries to account for that fact and assigns an area to the circle that increases by the area a new sensor contributes. If the sensors are packed in a small area, each sensor will contribute only a small additional area, because its area is already observed by other sensors. Compared to the simple count based measure, the area based measures reflect reality better, but need geographical information.

C. *Entropy-based measures*

What the area based measures try to compute is the additional information that a new sensor contributes. This additional information is actually the best possible measure and is at the heart of entropy based measures. If a sensor is the only one that observes an area, it contributes much information and lowers the entropy by a large amount for this area. In the forest monitoring example, sensors within a region that has only a few sensors contribute much information, compared to sensors in regions with many sensors. In addition, the sensor that reports a starting fire first provides much information, because this is a surprising and unexpected event. Entropy based measures are able to capture also the latter case. Therefore, we believe such measures are the most appropriate. In future work, we will examine several measures from statistics and coding theory and tailor them to the needs of an adaptive link layer.

IV. Protection mechanisms

These measures enable an operational definition of the informational value of a message. Using this informational value, a link layer has to decide which protection mechanism it should use. Some conceivable mechanisms include Forwad Error Correction (FEC), transmission power control, data rate adaptation, packet length adaptation, and ARQ protocols.

FEC: Forward Error Correction allows to add some redundancy to a packet so that the packet can be correctly received even if it encountered a (limited) number of bit errors during transmission. Different forward error control codes exist so that proper choices for packet size, channel condition, and intended protection are feasible. The trade-off is between reduced packet error rate and longer packet length.

ARQ: ARQ protocols enable retransmission of failed packets by sending acknowledgements and detecting missing acknowledgements. The trade-off here is the required overhead for acknowledgements in the correct case against the (compared to FEC) shorter packet length.

Transmission power adaptation:
Higher transmission power reduces the packet error rate by improving the signal to noise ratio, but increases energy consumption. This mechanism has to be supported by the radio front end to make sense.

Data rate adaptation:
Closely related to the FEC approach, controlling the data rate reduces the time necessary to transmit a given packet for the price of an increased bit error rate. This mechanism has to be supported by the radio front end to make sense.

The goal for an adaptive link layer is to choose these mechanisms (typically in combination) depending on the informational value of a message that is to be forwarded in such a way that the system efficiency is maximized.

V. Trading Energy for Value

In order to arrive at a maximum system efficiency, it is important to know the protection mechanism influences the probability that a packet arrives as well as its energy consumption. This enables the computation of the system efficiency, defined as $L = v_r/\eta_r$; the value arriving at the sink node (v_r) put into relation with the energy used to get it there (η_r); and this relation should be maximized. The two variable v_r and η_r depend on each other: the value arriving at the root depends on the way how the protection is chosen (the mapping of informational value to protection), because a higher protection increases the probability that a message is transmitted correctly. The chosen protection mechanism influences the consumed energy (η_r) to get the information to the sink node.

To gain an understanding of the problem, a specific system has to be defined. First of all, a measure for informational value is chosen, here the count based measure is used. Each sensor reading adds “1” to the informational value. This choice is not essential for the problem formulation, in fact any expression for the informational value could be used; the mapping of informational value to protection is independent of the measure. Just for convenience it is assumed that a message that is “worth sending” has at least an informational value of “1” and every measure is scaled in such a way that it keeps this property.

Secondly, a relation between the informational value and the chosen protection is defined: $v \rightarrow p(v)$, where $p(v)$ denotes the protection chosen, given a certain informational value v. The problem is that nothing about the properties of p is known. To keep it is general as possible, a table is used. The table is defined in pairs $v \rightarrow p$. When a message with an informational value of v arrives, the link layer looks into the table, and protects the message against e.g. p bit errors per block. The entries in this table must be chosen such that the maximum system efficiency is achieved.

A. Computing the value arriving at the sink

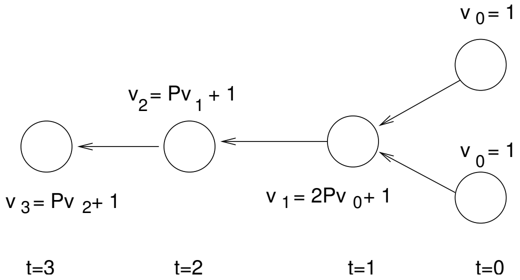

Fig. 4. Example problem sketch

Using the definition of the value and the definition of how the protection is chosen, it is possible to compute the system efficiency. The system in Figure 4 is used to derive the computation of the value arriving at the sink node v_r. The computation is done recursively, v_t denotes the value that arrives at tree depth t.

In WSNs messages do not always arrive correctly, but with a certain probability P. Messages are lost due to independent bit errors that appear with a certain probability b. This probability is not constant but depends on the protection $p(v)$ of the message transmitted, because messages with higher values are possibly given a higher protection; which implies that they arrive with a higher probability.

Thus, the expected informational value of a message that a certain node at tree depth $t+1$ has to forward is:

$$v_{t+1} = \begin{cases} a + \sum_{j=1}^{c} P(v_{t,j}) v_{t,j} & \text{if } c > 0 \\ a & \text{if } c = 0 \end{cases} \tag{1}$$

where $c \in \mathbb{N}_0$ denotes the number of children of the node, and a denotes the value that the node at three depth $t+1$ adds. Throughout this paper a count based measure is used, which means that $a = 1$. The forwarded value depends on the probability that a certain value arrives from a subtree that is rooted in the child j.

With this value, it is possible to compute the energy spent for the transmission of the message

$$\eta_{t+1} = f[p(v_{t+1})], \tag{2}$$

but this is specific for each protection mechanism, and discussed in the next sections.

B. Forward Error Correction

1) Fixed length codes: In this paper, three ways to protect a packet against bit errors are evaluated. The first class are Bose-Chaudhuri-Hocquenghem (BCH) codes with fixed block length. This means that the l information bits are spread across multiple blocks. Each of these blocks of length n can contain i information bits, the $n - i = k$ control bits are necessary to correct a certain amount of bit errors.

For the computation of the system efficiency a BCH code with a block length n of 63 bit is used. The protection $p(v) = e$ is the number of bit errors in a block e that can be corrected. This requires an overhead, namely the number of control bits in a block. The number of control bits k necessary to be able to correct e bit errors were taken from [5], [6] and are shown in Table I.

If the maximum protection is used, only two information bits per block can be transmitted. For a message that would have fitted into a single 63 bit block when no protection is used, 33 blocks or 2079 bit have to be transmitted when the maximum protection is used.

2) Optimal length codes: The fixed block length codes (esp. those with small block sizes like $n = 15\,\text{bit}$) have the advantage that they can be kept in a table, simplifying encoding and decoding to table lookups. But they are not the most efficient way to protect a message against independent bit errors. It is more efficient to make the block so large that it contains all information bits and the control bits in a single block.

The number of control bits k necessary to correct e bit errors in an n bit long block can be approximated using the Hamming distance $d = 2e + 1$ and the Varshamov-Gilbert bound

$$k(d) \geq \log_2 \left(\sum_{j=0}^{d} \binom{n}{j} \right). \tag{3}$$

The transmitted packet is $n = i + k$ bits long. For this protection mechanism the protection p is the number of bit errors e that can be corrected in such a packet. The energy spent to transmit the message is related to the length of the packet, and computed in bits.

3) Probability of successful transmission: The energy spent to transmit a message is only one side of the protection mechanism. It also influences the probability that a packet arrives. The probability that a block is successfully transmitted, which means it contains at most the number of bit errors that can be corrected, is given by the Bernoulli distribution:

$$P(X \leq e) = \sum_{j=0}^{e} \binom{n}{j} b^x (1-b)^{n-j} \tag{4}$$

The probability that a packet with l information bits is successfully transmitted using blocks of length n is

$$P(S) = P(X \leq e)^{\lceil l/n \rceil}, \tag{5}$$

since each block in it must be transmitted correctly.

C. ARQ

A completely different approach to add error protection is the use of an ARQ protocol. Basically, the ARQ protocol sends an ACK for every correctly received packet. The computation of energy consumption and success probability is more complex, as several cases have to be discerned.

The first case considered here is a successful transmission; the packet and the ACK are received correctly. The probability that a packet consisting of l bits is received without errors is

$$P(A) = (1-b)^l, \tag{6}$$

e	1	2	3	4	5	6	7	10	11	13	15	17	20
i	57	51	45	39	36	30	24	18	16	10	7	3	2
k	6	12	18	24	27	33	39	45	47	53	56	60	61

TABLE I

OVERHEAD FOR A 63 BIT BCH CODE

whereas the probability that an ACK of length l_a is received successfully is

$$P(B) = (1-b)^{l_a}. \tag{7}$$

For a successful transmission it is necessary that at least one of the transmission attempts is successful. If t denotes the maximum number of retransmissions, the probability of a successful transmission $P(S)$ is given by

$$P(S) = P(A) \sum_{i=0}^{t} [1 - P(A)]^{li} \tag{8}$$

The expected energy used for one transmission attempt consists of the energy spend for the packet and the energy spend for the ACK. However, the ACK is only send if the packet was received correctly. Hence, the expected energy per transmission attempt $\mathrm{E}(E)$ is

$$\mathrm{E}(E) = P(A)(l + l_a) + [1 - P(A)]l \tag{9}$$

The ARQ retries to send a packet when either the packet or the ARQ is lost. This has implications on the expected number of transmissions $\mathrm{E}(T)$:

$$\mathrm{E}(T) = 1 + \sum_{i=1}^{t} [1 - P(A)P(B)]^{i} \tag{10}$$

These formulas allow the computation of the expected value that arrives at the root node and the energy that is on average spend to achieve this:

$$\eta_{t+1} = \mathrm{E}(T)\mathrm{E}(E). \tag{11}$$

D. Computing the system efficiency

With the definition of the informational value and the spent energy it is possible to compute the system efficiency:

$$L = \frac{v_r}{\nu} \cdot \frac{(\nu-1)l}{\eta_r} \approx \frac{v_r l}{\eta_r} \tag{12}$$

where v_r is the value arriving at the sink (the root of the spanning tree) and ν is the total value, which is equal to the number of nodes in the tree. Hence v_r/ν is the value arriving at the root compared with the maximum possible value. The second term $(\nu-1)l/\eta_r$ represents the energy consumption, measured in sent bits (η_r) compared with the minimal number of bits that must be sent: $(\nu - 1)l$. The minimal energy that has to be spent is equal to the number of edges in the tree $\nu - 1$ times the number of information bits l that must be transmitted.

VI. CHOOSING THE RIGHT PROTECTION

The formulas presented in the preceding sections are difficult to evaluate symbolically, hence they were evaluated numerically using a network with 400 nodes in a unit disc graph, where each node had 14 neighbors on average. The spanning tree was built using Dijsktra's shortest path algorithm[3]. To compute the overall system efficiency, the system efficiencies obtained for each of the 400 possible sink nodes were averaged.

In this setup, we tried to find the maximum system efficiency for a number of Bit Error Rates (BERs) using different ways to map the informational value to protection level ($v \rightarrow p(v)$). Several ways to find such a mapping are presented in the following sections.

A. Using a function

One way to allow a link layer to find a certain protection given the informational value of a messages is a formula like:

$$v \rightarrow p(v) = \alpha + \beta v \tag{13}$$

By applying this formula, the link layer could compute for a message with a value of $v = 1$ a protection of, say $p(v) = 2$, or expressed in the shorthand notation: $1 \rightarrow 2$. This means for instance for a BCH code that each block should be able to correct two bit errors, or for an ARQ protocol that at most two retransmissions should be attempted.

But this approach faces severe difficulties. First of all, it is unknown whether such a functional relationship is a sensible approach. It could also be a relationship like $p(v) = \alpha + \beta v^{\gamma}$ or even something completely different. Even if the functional relationship of Eq. (13) is reasonable, the question remains what values to assign to the constants α and β.

[3] For comparison the computations were also done for random graphs, where the spanning tree was built with Prim's algorithm. The results are similar and therefore not shown here.

B. Using a table

Finding the right formula and fitting the constants such that the system efficiency is maximized is difficult. Hence, we did not try to fit such a function, but rather tried to find points on such a curve. Before transmitting a message, a link layer can look up the protection to use in a table using the informational value of the message.

Consider the case of a BCH Code with a block length of 63 bit. This code can correct up to 20 bit errors. Thus we can choose 20 informational values at which the protection is increased. For instance, we can choose to protect all messages against at least a single bit error ($1 \rightarrow 1$), all messages with a value of three or higher against 2 bit errors ($3 \rightarrow 2$) and all messages with a value of 200 and above against 20 bit errors ($200 \rightarrow 20$). For the simplifying assumption[4] that for each additional bit that can be corrected a different informational value has to be chosen, for a 400 node network we end up with

$$\binom{399}{20} \approx 2.6 \cdot 10^{33}$$

ways to choose 20 from the 399 informational values to mark a point where the protection is increased. This complexity rules out a brute force approach to find the mapping that maximizes system efficiency. The situation is further aggravated by the fact that the number of possible protections to choose from has no upper bound for ARQ approaches or for the approach based on the Varshamov-Gilbert bound.

Fortunately, full enumerations for smaller systems provide strong evidence for the assumption that the entries in the mapping table are independent. If there is only one entry, it is sufficient to find the optimal solution for this entry. In next step, this entry is kept fixed (say $1 \rightarrow 1$) and the next entry is tried. If the optimum is found (say $3 \rightarrow 2$), this entry is also kept and the next entry is tried. This way, the optimal mapping can be found in an iterative fashion. In our example, this involves less than $20 \cdot 399 = 7980$ steps. This approach was used to find the global optimum i.e. the mapping table that maximizes the system efficiency.

C. Using a heuristic

In a deployed sensor network it is not possible to find the optimal mapping of informational value to protection in such an iterative way. It imposes a prohibitively large communication overhead, as not only many mappings have to be tried but also each mapping has to be kept for a certain time to gain an understanding of its performance.

Listing 1. Pseudo-code of local rule

```
current protection = no protection;
oldPs = P(S) using current protection;
newPs = P(S) using increased protection;
oldEnergy = energy consumption using current
          protection;
newEnergy = energy consumption using increased
          protection;

while((newPs−oldPs)∗value >=
     (newEnergy − oldEnergy)/newEnergy)
{
  current protection = increased protection;
  oldPs = newPs;
  oldEnergy = newEnergy;
  increase protection;
  compute values for newPs and newEnergy
    for this new, increased protection;
}
transmit using current protection;
```

In order to adapt the reliability of the link layer given the informational value of a message, it is necessary that each node on the route can choose the protection with locally available information. We propose the following rule, which allows a very good approximation of the globally optimal mapping: increase the protection as long as the increase in value outweighs the relative increase in energy. Listing 1 shows the rule in pseudo-code.

This local rule allows a very close approximation of the maximum system efficiency and has several interesting features. First of all, it is completely independent of the protection mechanism used (BCH, ARQ, transmission power adaptation, data rate adaptation, etc.) as long as each mechanism can be expressed in increased energy expenditure. Secondly, it is completely oblivious of the underlying network topology. This suggests that it is useful under a wide range of conditions and thus provides a valuable starting point for anyone searching the right tradeoff between energy and the value that arrives at the root node.

VII. Results

A link layer that adapts the reliability of transmission to the informational value of a message implies an increased complexity in the protocol stack. This complexity has to pay off, and in this section we present the maximum achievable system efficiencies for each of the

[4] This is a conservative assumption. It is also possible to choose the same informational value twice, hence protecting it against two more bit errors. This increases the number of choices beyond a simple permutation.

three approaches (globally optimum, local rule and fixed protection) for the three protection mechanisms (FEC with fixed block length, FEC with optimal block length and an ARQ protocol) for different BERs.

The results are shown in Table II. The column "Algo." denotes the protection algorithm used, VG stands for an FEC with optimal block lengths, BCH for a BCH code with a block length of 63 bit. For ARQ an ACK of 80 bits was used. The column "size" denotes the packet size in bits. The next column contains the BER.

The next column (G. Map.) contains the mapping of values to the number of bit errors that the BCH codes should be able to correct, or the number of *re*transmissions for an ARQ protocol. This mapping was obtained in the iterative fashion described in section VI-B.

Column L. Map. is the mapping obtained with the local rule presented in the previous section. A comparison with the global optimum shows that the mappings differ only marginally – this can also be seen by comparing the values of L for these mappings, presented in columns G. Opt and L. Opt. The maximum possible value is $400/399 \approx 1$. The last column shows the value of L if the link layer with the best fixed protection is used. The best fixed protection is also contained in the table, using the independence of table entries: if the mapping contains an entry $1 \rightarrow p$ this is the best fixed protection, if the table does not contain such an entry, the best fixed protection scheme is to use no protection at all. We decided to compare against the best possible fixed protection, assuming that the designer of a link layer chooses the reliability of the link layer carefully with the application in mind. Other choices for the fixed protection are always somewhat arbitrary, as it is possible to choose a scheme that yields a system efficiency close to zero.

The table shows that the optimal mapping and the mapping computed with the local rule yield practically the same performance. It also shows that an adaptive link layer can be nearly twice as good compared to one with fixed protection. If an adaptive link layer can not be implemented, the application of the local rule leads to link layers with fixed protection that perform usually nearly as good as the adaptive ones.

Another interesting fact is that the ARQ protocol should not be used if a packet has only a value of one. Put differently, if ARQ is used as a mechanism, the network should never retransmit messages from leaf nodes.

The results can be summarized in two points: if possible, use a FEC with long blocks and choose a fixed protection with the help of the local rule. Although the fixed protection with block codes performs poorly under some scenarios, an adaptive scheme may not be worth the effort. The reason for the often negligible difference between the fixed protection scheme and the adaptive ones is the granularity how the protection mechanism can be adjusted. The optimal block length FEC allows the most granular increase. Protecting the packet against on more bit error increases the overall packet length slightly. But even this small increase is often too large and a considerable increase in the value (e.g. from 4 to 47) is needed before it pays off. The effect becomes even more pronounced when a less granular scheme like the BCH code with 63 bit block size is used. Here, choosing a fixed basic protection with a block code is the optimal strategy for many BERs.

The second point is that an ARQ protocol performs considerable worse than the other schemes. However, it is often built into the link layer, for instance in many Carrier Sense Multiple Access (CSMA) type Medium Access Control (MAC) protocols it is used to detect collisions of data packets; ARQ protocols are also necessary for hop-by-hop flow control, which also explains why they are used so often in link layers. In addition, an ARQ protocol should perform better when the bit errors are not independent but appear in bursts. It remains part of future work to evaluate performance for transmission channels with bursty bit errors. It seems to be interesting to make a more in depth simulation for ARQ protocols because the results in Table II suggest that it is possible to find an adaptive ARQ protocol that works reasonably well under a wide range of conditions.

VIII. Conclusion and future work

The evaluation of different ways to adapt the reliability of a link layer to the informational value of a message lead to a number of interesting insights. Using the system efficiency it is possible to define an optimal balance between energy expenditure and the informational value that arrives at the sink node. The local rule presented in this paper shows that each node can decide how reliable it should transmit a message just based on the informational value of the message and some channel information. The adaptation of the reliability of a link layer is nonetheless challenging, because the available protection mechanisms do not allow a sufficiently fine grained control of the reliability. It is therefore often optimal to choose a fixed protection scheme with the local rule at design time.

A slightly different conclusion has to be drawn for ARQ protocols. ARQ protocols are used very often in link layers, esp. when a CSMA type MAC is used. In addition, they allow hop-by-hop flow control and thus provide an added value. Although they perform poorly under the conditions examined in this paper, they should perform better for more realistic assumptions for the bit error behavior. Hence, the performance of adaptive ARQ protocols should be studied in depth for different channel assumptions as well as different ways to measure the informational content, at the very least the ARQ protocols should be analyzed for more aggregation structures and other channel conditions.

REFERENCES

[1] H. Karl, M. Löbbers, and T. Nieberg, "A data aggregation framework for wireless sensor networks," in *Proc. Dutch Technology Foundation ProRISC Workshop on Circuits, Systems and Signal Processing*, Nov. 2003. [Online]. Available: http://www.tkn.tu-berlin.de/tkn/publications/papers/prorisc.pdf

[2] T. Stathopoulos and D. Estrin, "An information-driven reliability mechanism for wireless sensor networks," Center for embedded networked sensors (CENS), Tech. Rep. 16, June 2003. [Online]. Available: http://deerhound.ats.ucla.edu:7777/pls/portal/docs/PAGE/CENS_REPOSITOR%IES/CENS_TECH_REPORTS/16_IDR[1].PDF

[3] S.-J. Park, R. Vedantham, R. Sivakumar, and I. F. Akyildiz, "A scalable approach for reliable downstream data delivery in wireless sensor networks," in *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*. ACM Press, 2004, pp. 78–89.

[4] Y. Sankarasubramaniam, B. Akan, and I. F. Akyildiz, "ESRT: event-to-sink reliable transport in wireless sensor networks," in *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*. ACM Press, 2003, pp. 177–188.

[5] C. Wilhelm, *Datenübertragung*. Berlin: Militärverlag der DDR, 1976.

[6] J. P. Stenbit, "Table of generators for Bose-Chaudhuri codes," *IEEE Trans. Inf. Theory*, vol. IT, no. 10, pp. 390–391, 1964.

TABLE II: Value to protection mappings

Algo.	**Size**	**BER**	**G. Map.**	**L. Map.**	**G. Opt.**	**L. Opt.**	**F. Opt**
VG	300	0.0005	1 → 1 4 → 2 47 → 3	1 → 1 4 → 2 44 → 3	0.91	0.91	0.90
VG	300	0.001	1 → 1 2 → 2 7 → 3 86 → 4	1 → 1 2 → 2 7 → 3 81 → 4	0.89	0.89	0.83
VG	300	0.005	1 → 4 2 → 5 4 → 6 12 → 7 41 → 8	1 → 4 2 → 5 4 → 6 11 → 7 38 → 8 145 → 9	0.80	0.80	0.76
BCH	300	0.0005	2 → 2	2 → 2	**0.81**	**0.81**	**0.63**
BCH	300	0.001	1 → 2	1 → 2	0.80	0.80	0.80
BCH	300	0.005	1 → 2 8 → 3 85 → 4	1 → 2 7 → 3 66 → 4	0.76	0.76	0.74
ARQ	300	0.0005	2 → 2 3 → 4 4 → 5 5 → 7 6 → 8	2 → 3 3 → 5 4 → 6 5 → 7 6 → 8	**0.70**	**0.70**	**0.55**
ARQ	300	0.001	2 → 2 3 → 4 4 → 6 5 → 7	2 → 3 3 → 5 4 → 7 5 → 8	**0.61**	**0.61**	**0.39**
ARQ	300	0.005	3 → 11 4 → 15 5 → 18 6 → 21	3 → 15 4 → 19 5 → 22 6 → 24	0.17	0.17	0.06