A Review of Energy Conservation in Wireless Sensor Networks

Vamsee P S, Dr Syed Umar
Department of ECM,
KL University, A.P.,INDIA.

Abstract— **In a previous paper a novel forwarding scheme for wireless sensor networks has been proposed by the same authors [3]. The authors showed that the proposed technique, mainly based on the Chinese Remainder Theorem (CRT), outperformed more traditional approaches in terms of both energy efficiency and fair distribution of energy consumption. Furthermore, only few changes to the commonly used forwarding schemes are needed for its implementation. However, although the advantages of the method were clear, all reported results were only empirical and obtained through simulations on ideal sensor networks. In this paper some analytical results regarding the proposed method are introduced and it is shown how to extend the proposed forwarding method on a more realistic wireless network where unreliable erasure channels are considered. Furthermore, a trade-off between reliability and energy saving is investigated.**

Keywords— **Security, Wireless, Conservation, Energy, Sensor networks.**

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of a large number of sensor nodes distributed over a geographic area Each node is usually powered by an energy-limited battery, therefore the energy budget is a critical design constraint in WSNs and energy saving is the key issue in order to increase the network lifetime. Several works [1],[8], have shown that energy consumption is mainly due to data transmission, consequently, energy conservation schemes have been proposed aimed at minimizing the energy consumption of the radio interface. In particular, two main approaches can be found in the literature: Duty Cycling and In-Network Aggregation see [2] and [5] respectively, for a survey. The first approach consists in putting the radio transceiver in the sleep mode (also known as power saving mode) whenever communications are not needed. Although this is the most effective way to reduce energy consumption, a sleep/wakeup scheduling algorithm is required (which implies solving critical synchronization issues) and energy saving is obtained at the expense of an increased node complexity and network latency. The second approach is intended to merge routing and data aggregation techniques and it is primarily aimed at reducing the number of transmissions. In particular, in order to improve robustness, multipath routing algorithms are usually employed. However, multiple paths could remarkably consume more energy than the shortest path because several copies of the same packet could reach the destination [7].

With the aim of reducing the energy consumption, in [3] we proposed a novel approach which splits the original messages in several packets such that each node in the network will forward only small sub-packets. The splitting procedure is realized applying the Chinese Remainder Theorem (CRT) algorithm [9], which is characterized by a simple modular division between integers. The sink node, once all sub-packets (called CRT components) are received correctly, will recombine them, thus reconstructing the original message. The simple splitting procedure is particularly helpful for those forwarding nodes that are more solicited than others, due to their position inside the network. As regards the complexity of the algorithm, in the proposed approach almost all nodes operate as in a classical forwarding algorithm and, with the exception of the sink, few low complex arithmetic operations are needed. If we consider that usually the sink node is computationally and energetically more equipped than the other sensor nodes, the overall complexity of the algorithm remains low and therefore suitable for a WSN. However, although the advantages of the proposed method were clear, all results reported in [3] were empirical only and obtained by considering simulations on a sensor network where it is assumed that an ideal communication among neighbor sensors exists, and all the CRT components can be received correctly. Obviously this hypothesis is not valid in a real network. In this paper some analytical results regarding the method are obtained and it is shown how to extend the proposed forwarding scheme on a more realistic WSN scenario where erasure channels are considered. Furthermore the trade-off between reliability and energy saving of the method is investigated. It is worth mentioning that the idea of using a multipath approach together with erasure codes to increase the reliability of a WSN was already proposed in [4]. However, in that work, the authors suggested to use disjoint paths. As compared to our proposed forwarding technique, the use of disjoint paths has two main drawbacks. First, a route discovery mechanism is needed. Second, because the number of disjoint paths is limited, the number of splits (and therefore the achievable energy reduction factor) is limited too. Furthermore in [4] the authors considered general FEC techniques without investigating on their complexities and/or their impact on energy consumption. The rest of the paper is organized as follows. Section II describes the CRT theorem, the metrics used across the paper and describes the proposed forwarding technique. In Section III we derive some analytical results. In Section IV the performance of the proposed approach is discussed and the analytical model is validated. Finally, in Section V some concluding remarks are drawn.

II. Forwarding Technique Based On The Chinese Remainder Theorem

In this Section we briefly outline the Chinese Remainder Theorem (CRT) and we show how to use it to implement a new forwarding technique that is both reliable and energy efficient.

A. Chinese Remainder Theorem

Basically, in its simpler form, the CRT can be formulated as follows [9]: *Given* N *primes* pi > 1, *with* i ∈ {1...N}, *by assuming* M *their product, i.e.* M = _ipi, *then for any set of given integers* {m1,m2, ..., mN} *there exists a unique integer* m < M *that solves the system of simultaneous congruencies* m = mi (mod pi) *and it can be obtained by* m = (PN i=1 ci mi) (mod M). *The coefficients* ci *are given by* ci = Qiqi, *where* Qi = M
Pi *and* qi *is its modular inverse, i.e.* qi *solves*
qiQi = 1 (mod pi).

For instance let us consider the system:
m = 1 (mod 3)
m = 4 (mod 5)
m = 1 (mod 7)

It is simple to prove that m = 64 solve the system and that it can be obtained by the above equations. According to the CRT, the number m can be alternatively identified with the set of numbers mi provided that pi are known. However, it is worth noting that in the above example 7 bits are needed to represent m, while no more than 3 bits are needed to represent each mi. Therefore if, instead of m, mi numbers, with mi = m (mod pi), are forwarded in a wireless sensor network, the maximum energy consumed by each node for the transmission can be substantially reduced. For instance, consider Fig. 1. If X, Y, and Z receive a message mA from A, each of them, applying the procedure shown above, can transmit a message mi, with i ∈ {1, 2, 3}, to the sink instead of mA. Furthermore, the sink, knowing pi, with i ∈ {1, 2, 3}, and using the CRT approach, will be able to reconstruct mA.

B. Metrics for energy efficiency

In general, if we consider that the energy consumption is proportional to the number of bits transmitted then, assuming w the number of bits in the original message m, and ω_{CRTmax} the maximum number of bits of a CRT component, i.e. $\omega_{CRTmax} = \max([\log_2(pi)])$,

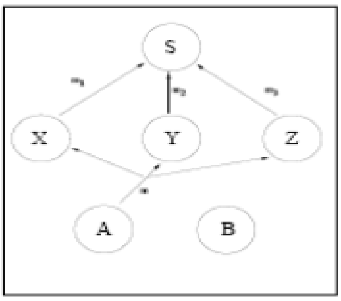


Fig. 1. Example of forwarding after splitting.

we can consider a theoretical maximum energy reduction factor (MERF) given by

$$MERF = \frac{w - w_{CRTmax}}{w}$$

For instance, in the previous example is MERF = $7-3/7 \approx .57$, this means that about 57% of the energy could be saved by considering the proposed forwarding scheme. The previous energy reduction factor can be obtained for high ode densities, i.e. when there are a sufficient number of disjoint paths so that it is highly probable that all the CRT components are forwarded by different nodes. However, it is worth noting that in the above example the total number of bits transmitted has been reduced too (i.e. only 1+3+1=5 bits are need to forward m instead of the original 7 bits). Therefore, even in the worst case where all the components of the previous example have to be forwarded by the same node, we have an energy reduction factor equal to $7-5/7 \approx 0.29$. Although this last result is dependent on the particular value of m, on the basis of the above example, we can roughly state that CRT-based splitting is more efficient than a simple splitting (i.e. packet chunking) or other FEC-based splitting techniques (where redundancy have to be added to the original packet by increasing the total number of bits). It is pointed out that, with the aim of obtaining simulation results that are not dependent on the particular message m, all reported simulation results are carried out for the worst case message, i.e. by considering the maximum number of bits for all CRT components (for instance 2,3,3, for the mi in the previous example). In a real scenario, where the CRT components are not forwarded through disjoint paths, the MERF is rarely obtained and the expected energy reduction factor (ERF) have to be expressed taking into account both the actual number of bits forwarded by a normal forwarding algorithm and our proposed CRT-based forwarding algorithm. In particular, for comparison purposes, the Shortest Path with Load Balancing (SP) is considered by assuming that a sensor node having a packet to forward chooses randomly as next-hop a node belonging to the shortest path towards the sink. The expected energy reduction factor can be expressed by considering the mean energy consumed by a node in the case of the proposed CRT-based and the SP forwarding technique, i.e. ECRT = nc $\bar{\omega}_{CRT}$ and ESP = npw respectively, where nc and np are the mean number of forwarded packets with the above forwarding schemes and $\bar{\omega}_{CRT}$ is the mean number o bits needed to represent the CRT components:

$$ERF = \frac{E_{SP} - E_{CRT}}{E_{SP}} = 1 - \frac{n_c \bar{w}_{crt}}{n_p w}. \qquad (1)$$

The above metrics well be used throughout the paper. Obviously the primes set should be chosen in order to maximize MERF and ERF.

C. On the choice of the prime numbers

It is important to observe that the set of prime numbers pi > 1, with i ∈ {1...N}, can be arbitrarily chosen provided that m < M, therefore, the number of bits needed to represent mi can be reduced by choosing the prime numbers as small as possible. As a consequence of this choice, the MERF is maximized. Throughout the paper we indicate with Minimum Primes Set (MPS) the set of the smallest consecutive primes that satisfy the condition M ⩾ 2w. For instance, if N = 4 and m is a 40- bits word (w = 40), the MPS will be {1019, 1021, 1031, 1033} (this is the set of smallest 4 consecutive primes that satisfies the condition M ⩾ 240). The MERF in this case is 0.725. However, when the primes set is chosen as above, the message can be reconstructed if and only if all the CRT components are correctly received by the sink. This was the main hypothesis (and limit) of our previous paper [3]. Let us consider another primes set {10313, 10321, 10331, 10333}. These are the smallest consecutive primes that satisfy the condition _ipi ⩾ 240 even if one of primes is removed. We call this set as the Minimum Primes Set with one admissible failure (the name will be better clarified below) and we will indicate it as MPS-1. In general, throughout the paper we will indicate with MPS-f the Minimum Primes Set with f admissible failures. When compared with the previous MPS it is possible to observe that

- the number of components in MPS-1 is not changed (i.e. the same number of nodes is needed to forward the message).
- the MERF obtained with the new set is 0.65 i.e. MERF is reduced by about 11%. However with this choice it is possible to reconstruct the original message m even if a component is lost (i.e. if we have one failure). In fact, whatever is the lost component mj , the product of the primes associated with the received components satisfies the condition M′ = _i6=jpi > 240 and therefore it respects the hypothesis of the CRT theorem. For instance if the last component m4 is not received it is again possible to obtain m as m = P3 i=1 ci mi (mod M′)= where M′ = _3 i=1pi is the product of the first three primes, and c1, c2, c3 are the first three CRT coefficients computed for the MPS-1 on the basis of the CRT algorithm. The previous example can be extended in order to consider a greater number of failures f. Therefore, the parameter f allows a trade-off between reliability and energy saving that will be investigated in this paper. Let us observe that by fixing w, N and the number of admissible failures f the MPS-f is unique.

D. The Forwarding Algorithm

Let us consider a sensor network where sensor nodes periodically send messages to a sink through a multi-hop transmission. The basic idea of the paper is to split the messages sent by each source node so that a reduced number of bits could be transmitted by each forwarding node in the network. The forwarding algorithm is based on two temporal phases. The first phase is called *Initialization phase* and guarantees two necessary conditions:

1) The sink should know the prime numbers pi in order to reconstruct the original packet;

2) Different pi ∈ MPS-f should be chosen by each next hop of the source.

This phase organizes the network in clusters and also has the advantage of minimizing the number of hops needed to reach the sink. Once the network has been organized, it follows the

Forwarding phase where the forwarding procedure is actually applied. Note that when the procedure is applied to a WSN, the number NX of primes corresponds to the number of forwarding nodes for each source X.

1) Initialization phase: Let us consider a non-initialized network where CLID identifies the cluster number. We assume that the sink is the only node in CLID= 1 and it sends an initialization message (IM) with the sequence number SN=2 at the start-up (see Fig. 2.a). Note that the sequence number SN=1 is reserved to reset an already initialized network. Furthermore, we assume that the number of admissible failures f is decided by the sink and sent in a proper field of the IM

All the nodes that receive the IM with SN= 2 assume to belong to CLID= 2 and consider the sink as their next hop. Nodes in CLID= 2 will retransmit both the IM with an increased sequence number (SN= 3) and their addresses (see Fig. 2.b). Any node receiving this message assumes to belong to CLID= 3 and considers as possible next-hops the nodes from which it has received the IM with SN= 3 (or a subset of these nodes to reduce memory requirements). Nodes on CLID= 3 will retransmit the IM with SN= 4 together with the list of addresses of nodes on CLID= 2 from which they have received the IM and that will be used afterward as next-hops to reach the sink (see Fig. 2.c). Thanks to this procedure, nodes on CLID= 2 will know how many next-hops can be used by the nodes in CLID= 3 to forward a packet. For instance, consider Fig. 2.c, node X knows that A will use X and Y as next-hops and therefore that all packets originated by A can be splitted in NA = 2 parts. This procedure can be repeated until all the nodes of the sensor network are reached. At the end of the procedure each node in the network will know its next-hops, who will use itself as next-hop and in how many parts the received packets can be splitted. In order to obtain the prime numbers to be used to split a packet, a node can proceed as follows. Let us assume that all the nodes know the size of the packets, K w, where w is the word size in bits and K is the number of words carried inside a packet. The message size can be considered either constant in the network or its value can be specified in the packet header.

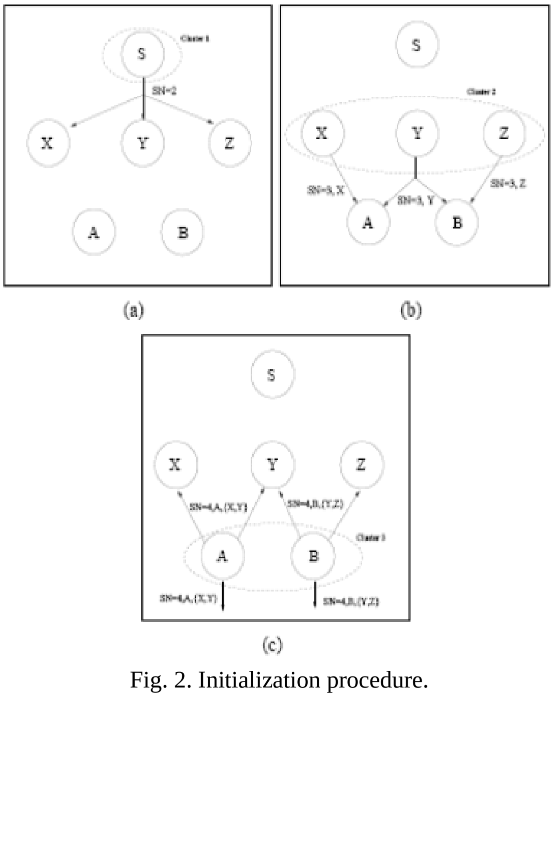


Fig. 2. Initialization procedure.

As observed in the previous section, knowing NX, w and f it is possible to determine (for each source X) a unique set of primes (MPS-f). Considering the previous example shown in Fig. 2.c, knowing NA, w and f, X and Y can derive independently the same MPS-f to be used to split the packets originating by A (i.e. without further communications). Furthermore, they can select different prime numbers of the MPS-f by considering the order of the addresses specified in the IM. If we consider the previous example, X and Y receive from A the IM:[SN=4,A,{X,Y}] so that X will select the first prime number of the MPS-f and Y the second one. It is worth mentioning that because there is a unique MPS- f for each NX, it is not necessary for the sink to receive the prime numbers used to split the packet but only the number of components used to split the packet (i.e. NX). However, the sink, in order to reconstruct the messages, needs also to know the index of the received component (i.e. i for each mi). For this purpose we will assume that in the header of each packet there is a field called *mask*. The mask could be the binary representation of the index i followed by the number of components (i.e. a pair (i,NX)) or a "one-hot" coding bit sequence followed by a tail bit, i.e. a sequence of N + 1 bits where the i-th bit is 1 if the packet contains in the payload the i-th component, mi, and the last bit is always 1. In this manner, the length of the mask, i.e. the number of components, and the component index, can be easily identified. For instance, if the mask is 101, this means that the original packet has been splitted in two components and the current packet contains the first of the two components, i.e. m1. Moreover, the mask will be 011 for the second component m2 of the same packet and 11 if the packet is not splitted (i.e. m). Despite the one-hot coding could be less efficient than a simple binary index, throughout the paper we will use it for the sake of clarity. Furthermore, we will assume that the overhead introduced by the mask is negligible. This is reasonable if we consider that a mask is composed by a few bits while a packet is composed by several words of w bits each. It is worth mentioning that the initialization procedure is performed only when the network is activated for the first time and it is not needed to run it when either a new node joins the network or a node belonging to a certain cluster goes out of energy. In both cases it is sufficient that few IMs (one for each node) are exchanged between the node and its neighbors belonging to the near clusters.

2) Forwarding phase: Let us consider the network shown in Fig. 3 where clusters are obtained according to the initialization procedure already described in the previous section. The figure shows the messages and masks sent by each node when the source node H sends a message m to the sink S.

In particular H specifies the mask 11 to indicate that the message is unsplitted. According to the initialization procedure, node G knows that it is the only next-hop of node H and therefore it must forward the packet without performing a splitting procedure.

It is worth mentioning that it is not needed for G to specify the list of the destination addresses {C,D,E,F} in the packet. In fact, in the initialization phase, nodes {C,D,E,F} have already received the IM message IM:[SN=5,G,{C,D,E,F}] and therefore they know that node G has 4 next-hops and that all of them have to split in NG = 4 parts the messages received from G. Therefore, when they receive the packet, according to both the packet size, w, and NG, they select independently the prime numbers and send the components mi = m (mod pi), together with a proper mask, to one of the possible next-hops. For instance if w = 40 and f = 1, the MPS 1 is {10313,10321,10331,10333} and therefore {10313,10321,10331,10333} are used as prime numbers for {C,D,E,F} respectively. Nodes A and B know that the received messages were already splitted (by checking the mask) and therefore they simply forward the received packets to one of the potential next-hops (in this case the sink). When the sink receives a component mi, it identifies the number of expected components on the basis of the mask and therefore it calculates the MPS-f. Then, according to the CRT algorithm, the sink nodes calculate the coefficients ci needed to reconstruct the original message. Finally, when the sink receives at least N–f components of the original message, it can reconstruct the message by m = Pi cimi (mod M′) as shown before1. Concerning the complexity of the algorithm, it is worth mentioning that in our proposed approach only the next hop nodes of the source perform a splitting procedure, while the other sensor nodes in the network will just forward the sub-packets. Moreover, only the sink node will reconstruct the original message through more complex operations as described above, but this can be neglected if we consider that usually the sink node is computationally and energetically more equipped than the other sensor nodes. Obviously, in the case of very big packets it is possible to split the packets recursively but in this case a trade-off between complexity, energy efficiency and mask overhead should be taken into account. In order to keep the complexity of the proposed algorithm very low, throughout the paper we will consider that a packet can be splitted only one time.

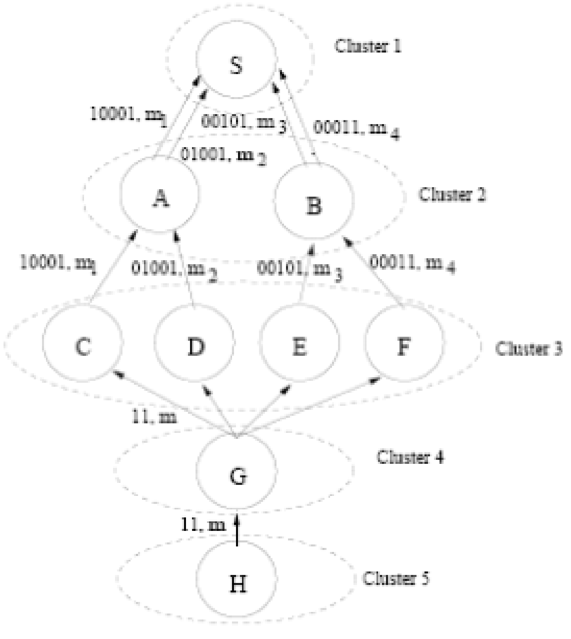


Fig. 3. Forwarding Example.

III. PERFORMANCE EVALUATION

In this Section we show a comparison between the results obtained through the analysis reported in the previous section and those obtained through a custom MATLAB simulator. For the sake of space we report simulation results for a specific case study but several simulations have been carried out with similar results. We consider a sensor network where nodes are randomly distributed in a square area of size Grid Size = [300m × 300m] with density _ = 0.03. Sensor nodes are considered static as usual in most application scenarios [1]. In each simulation the sink node is located in the center of the square grid and each sensor node has a transmission range equal to R= 60m. As described in section II-D, the network is organized in clusters numbered in ascending order starting from the cluster where is located the sink node, which is identified with CLID = 1. Moreover, nodes have a unique address, ID ⩾ 2, assigned during the initialization phase (ID = 1 is assigned to the sink node). A certain number of events, called E_v = 15, happens randomly in the sensor network. We assume that each event happens in cluster CLID(TX) ⩾ 5. After an event has occurred, all the nodes that recognize to be close to the event generate a message having the sink node as destination. More precisely, we assume that only nodes inside the circular area of radius, r = 20 m, with center in the location of the event, will send a message to the sink. Each source X generates a message, mX, whose word size in bits is equal to w = 100 bits if not differently specified. Therefore, for each event Ev, the number of messages generated is in the order of π r2 ρ, i.e. Nm ≈ E_v π r2 ρ, First, we verify the results discussed in Section III-A regarding the number of CRT components. Accordingly to Table I, for the considered packet size (w = 100), the maximum number of CRT components to be used is N_{max}=22. To prove the above statements, in Fig. 4 we report the ERF considering 100 different topologies (US=[1,100]) for three values of NCRT (i.e. 15, 21 and 25). For the sake of clarity we have sorted the topologies (S=[1,100]) so that the ERF values are ordered from the highest to the smallest value.

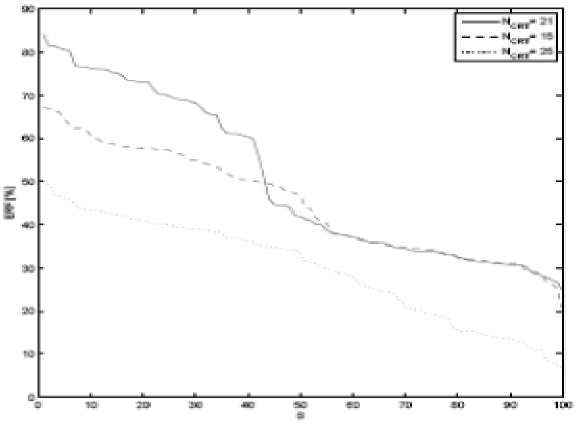


Fig.4. ERF vs. sorted topologies, S, with different values of NCRT

.

As anticipated by our model, it is not convenient to choose a value of NCRT greater than N_{max} = 22. Furthermore, simulation results for NCRT = 15 and NCRT = 21 confirm that increasing NCRT we can obtain better performance (due to the fact that we have smaller packets). Moreover, for some simulations, almost the same ERF is achieved due to the fact that the products NCRT $\bar{\omega}_{CRT}$ are very close. Some results regarding the impact of the number of admissible failures f on the ERF are shown in Fig. 5. For some of the above topologies (i.e. 10, 50, 90) the experimental values of ERF_f are reported in Table II together with the estimated values of ERF_f evaluated according to eq. (4). As it can be observed, the experimental results match with the model.

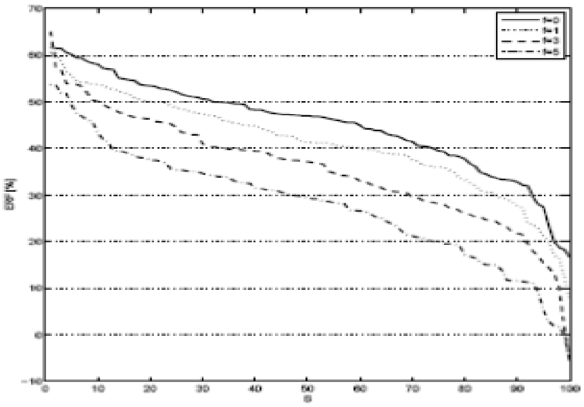
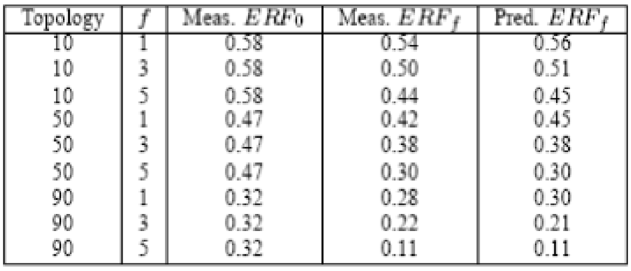


Fig. 5. ERF vs. sorted topologies, S, with different values of f.



Topology	f	Meas. ERF_0	Meas. ERF_f	Pred. ERF_f
10	1	0.58	0.54	0.56
10	3	0.58	0.50	0.51
10	5	0.58	0.44	0.45
50	1	0.47	0.42	0.45
50	3	0.47	0.38	0.38
50	5	0.47	0.30	0.30
90	1	0.32	0.28	0.30
90	3	0.32	0.22	0.21
90	5	0.32	0.11	0.11

TABLE II

MEASURED AND PREDICTED ERF_f FOR DIFFERENT VALUES OF f.

Fig. 6 shows the experimental and estimated values of the ERF obtained by means of eq. (9). More precisely, the nodes of the cluster 2 of 100 different topologies are considered and the following values are used for the simulations: NCRT = 21 (i.e. $\bar{\omega}_{CRT}$ = 5.28) and Nm ∈ [100, 500]. As can be observed, the model provides the exact value of ERF in most cases and a conservative estimation in the other cases. Finally, in Fig. 7 we show the number of bits forwarded from the nodes belonging to CLID = 2. Results show that applying the CRT approach the number of bits forwarded from these nodes is reduced (i.e. 400 vs 600), moreover, we observe a more fair distribution of the forwarded bits among all nodes.

V. CONCLUSIONS

In this paper an analytical model for a recently proposed forwarding algorithm based on the Chinese Remainder Theorem has been introduced. Because the energy consumption per node is proportional to the amount of bits received and subsequently forwarded, by applying the proposed technique it is possible to reduce significantly the energy consumed for each node and consequently to increase the network lifetime of the wireless sensor network. Furthermore, the trade-off between energy consumption and reliability of the method has been investigated. As a future work we plan to study analytically the optimal number of components, NCRT , related to the network density.

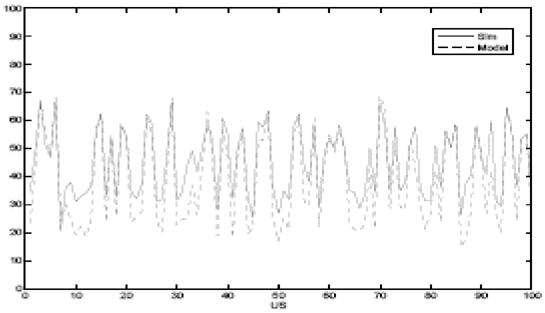


Fig. 6. Experimental and estimated values of the ERF vs unsorted topologies (US).

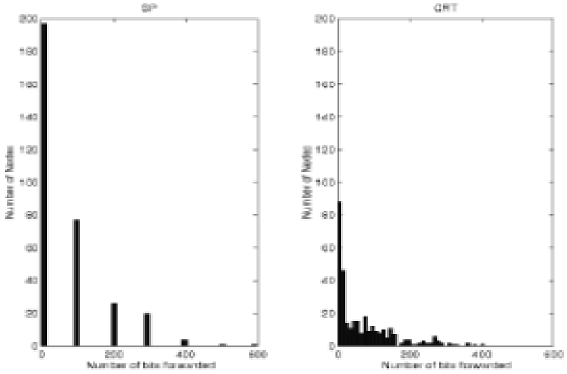


Fig. 7. Number of bits forwarded from nodes belonging to CLID = 2, when GridSize= [300m x 300m], w = 100 bits and _ = 0.03.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. A Survey on Sensor Networks. *IEEE Communications Magazine*. Vol. 40 , No. 8, pp. 102-114, August 2002.

[2] G. Anastasiii, M. Conti, M. Di Francesco, A. Passarella. How to Prolong the Lifetime of Wireless Sensor Network. *Handbook of Mobile Ad Hoc and Pervasive Communications*. Chapter 6 in Mobile Ad Hoc and Pervasive Communications, (M. Denko and L. Yang, Editors), American Scientific Publishers, 2007.

[3] G. Campobello, A. Leonardi, S. Palazzo. On the Use of Chinese Remainder Theorem for Energy Saving in Wireless Sensor Networks. *Proc. Of IEEE International Conference on Communications (ICC 2008)*, Beijing, China, May 2008.

[4] S. Dulman, T. Nieberg, J. Wu, P. Havinga. Trade-Off between Traffic Overhead and Reliability in Multipath Routing for Wireless Sensor Networks. *Proc. of WCNC Conference*, New Orleans, USA, March 2003.

[5] E. Fasolo, M. Rossi, J. Widmer, M. Zorzi: In-Network Aggregation Techniques for Wireless Sensor Networks: A Survey. *IEEE Wireless Communications*, Vol.14, No. 2, pp. 70-87, April 2007.

[6] A.M. Gittelsohn. An Occupancy Problem. *The American Statistician*, Vol. 23, No. 2, pp. 11-12, April 1969.

[7] D. Ganesan, R. Govindan, S. Shenker, D. Estrin. Highly Resilient, Energy Efficient Multipath Routing in Wireless Sensor Networks. *Mobile Computing and Communications Review (MC2R)*. Vol. 1, No. 2, 2002.

[8] J. Haapolai, Z. Shelby, C. Pomalaza-Raez, P. Mahonen. Cross-Layer Energy Analysis of Multihop Wireless Sensor Networks. *Proc. of the 2nd European Workshop on Wireless Sensor Networks (EWSN '05)*, Istanbul, Turkey, January 2005.

[9] J.-H. Hong, C.-H. Wu, C.-W. Wu. RSA Cryptosystem Based on the Chinese Remainder Theorem. *Proc. of Asia and South Pacific Design Automation Conference (ASP-DAC)*, Yokohama, Japan, January 2001.

[10] A. Menezes, et al., *Handbook of Applied Cryptography*, CRC Press, Oct. 1996