ISSN 2278-7763

MAXIMIZING THE LIFETIME OF WIRELESS SENSOR NETWORKS USING CRT BASED PACKET SPLITTING ALGORITHM

Sridhar Manda, Archana N,Umarani N.

Sridhar Manda asst.prof.CJITS, Jangaon, email:mandasridhar550@gmail.com.

Archana nagelli asst.prof. CJITS, Jangaon, email:archana.nagelli@gmail.com.

Umarani nagavelli asst.prof. CJITS, Jangaon, email:umarani.nagavelli@gmail.com.

Abstract**:** *Each node is usually powered by an energy limited battery, therefore energy budget and life time is a critical design constraint in WSNs and energy saving is the key issue in order to increase the network the network lifetime. There are many approaches found like duty cycling and in network aggregation, sleep wake scheduling algorithm which is used especially in solving critical synchronization and saving is obtained. The approach called multi path routing algorithm is also employed which consumes more energy. Apart from all these we aim at reducing energy consumption and increasing lifetime of WSN. So, here a proposed 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 based on Chinese Remainder Theorem (CRT) algorithm which is done by a simple modular division between integers. At sink node, once all sub packets are received correctly will recombine them, thus constructs the original message. The overall complexity of algorithm remains low complex arithmetic operations. Hence maximizes the lifetime of wireless sensor networks.*

Key words: WSN, Energy saving, maximization of lifetime, packets,CRT.

I.INTRODUCTION

A wireless sensor network 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 energy consumption is mainly due to 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,[2] 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-wake 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 mere 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

Copyright © 2013 SciResPub.

ISSN 2278-7763

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 $p_i > 1$, with $i \in \{1 \ldots N\}$, by assuming M their product, i.e. $M = \pi_i p_i$, then for any set of given integers $\{m_1, m_2, m_3, \ldots, m_N\}$ there exists a unique integer $m < M$ that solves the system of simultaneous congruence's $m = m_i \ (mod\ p_i)$ and it can be obtained by $m = \left(\sum_{i=1}^{N} c_i \, . m_i\right)(mod\ M)$. The coefficients c_i are given by $c_i = Q_i q_i$, where $Q_i = \frac{M}{p_i}$ and q_i is its modular inverse, i.e. q_i solves $q_i Q_i = 1 \ (mod\ p_i)$.

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 $m = 64$ solves 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 m_i provided that p_i 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 eachm_i. Therefore if, instead of m, m_i numbers, with $m_i = m \ (mod\ p_i)$, are forwarded in a wireless sensor network, the maximum energy consumed by each node for the transmission can be substantially reduced.

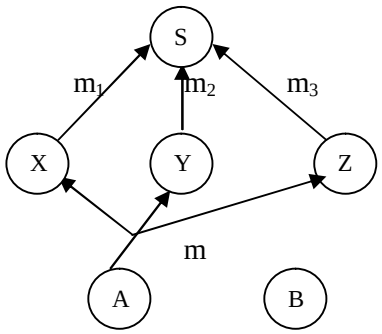


fig. 1. Forwarding after splitting.

For instance, consider Fig. 1. If X, Y, and Z receive a message m_A from A, each of them, applying the procedure shown above, can transmit a message m_i, with $i \in \{1, 2, 3\}$, to the sink instead of m_A. Furthermore, the sink, knowing p_i, with $i \in \{1, 2, 3\}$,

Copyright © 2013 SciResPub.

ISSN 2278-7763

and using the CRT approach, will be able to reconstruct m_A .

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 the maximum number of bits of a CRT component, i.e. $w_{CRTmax} = \max([\log_2(p_i)])$, 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 $MERF = \frac{7-3}{7} \approx 0.57$, 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 node 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 $\frac{7-3}{7} \approx 0.29$.

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 m_i 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. $E_{CRT} = n_c \bar{w}_{crt}$ and $E_{SP} = n_p w$ respectively, where n_c and n_p are the mean number of forwarded packets with the above forwarding schemes and $\bar{w}_{CRT}$ is the mean number of bits needed to represent the CRT components:

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

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

B. On the choice of the prime numbers

It is important to observe that the set of prime numbers $p_i > 1$, with $i \in \{1 \dots N\}$, can be arbitrarily chosen provided that $m < M$, therefore, the number of bits needed to represent m_i 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$M \geq 2^w$. 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 $\geq 2^{40}$). The MERF in this case is 0.725. However, when the primes set are 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 $\pi_i p_i \geq 2^{40}$ 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).

Copyright © 2013 SciResPub.

ISSN 2278-7763

- 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 componentm_j, the product of the primes associated with the received components satisfies the condition $M' = \pi_{i \neq j} p_i > 2^{40}$ and therefore it respects the hypothesis of the CRT theorem.

For instance if the last component m_4 is not received it is again possible to obtain m as $m = \sum_{i=1}^{3} c_i . m_i \ (mod\ M')$ where $M' == \prod_{i=1}^{3} p_i$ 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.

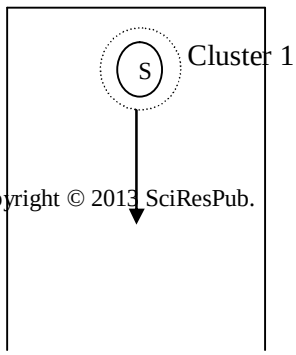
C. The Forwarding Algorithm

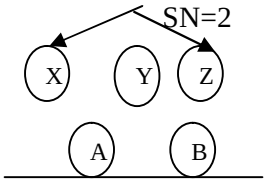
Let us consider a sensor network where sensor nodes periodically send messages to a sink through a multihop transmission. The basic idea of the paper is to split the messages sent by each source node so that a reduced number of bits could be transmitted by each forwarding node in the network. The forwarding 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 p_i in order to reconstruct the original packet.
2) Different $p_i \in MPS - f$ should be chosen by each nexthop of the source.

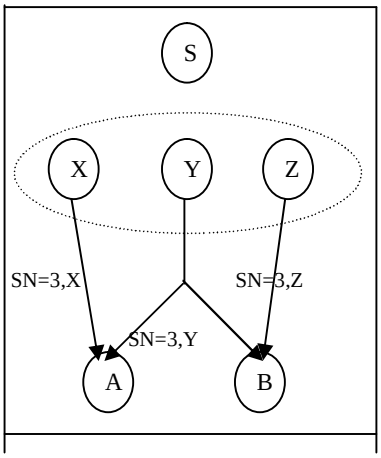
This phase organizes the network in clusters and also has the advantage of minimizing the number of hops needed to reach the sink. Once the network has been organized, it follows the

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

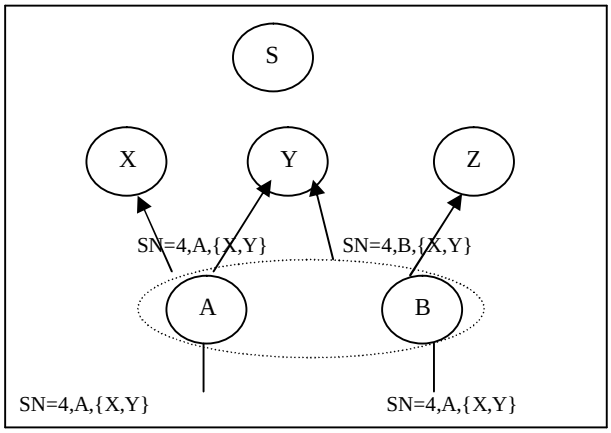




(a)



(b)



(c)

Fig.2. Initialization procedure.

Copyright © 2013 SciResPub.

ISSN 2278-7763

1) Initialization phase: Let us consider a non-initialized network where CL_{ID} identifies the cluster number. We assume that the sink is the only node in $CL_{ID} = 1$ 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 $CL_{ID} = 2$ and consider the sink as their nexthop. Nodes in $CL_{ID} = 2$ 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 $CL_{ID} = 3$ 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 $CL_{ID} = 3$ will retransmit the IM with SN= 4 together with the list of addresses of nodes on $CL_{ID} = 2$ 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 $CL_{ID} = 2$ will know how many next-hops can be used by the nodes in $CL_{ID} = 3$ 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 $N_A = 2$ 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. As observed in the previous section, knowing N_X, w and f it si possible to determine (for each source X) a unique set of primes (MPS-f). Considering the previous example shown in fig. 2.c, knowing N_A , 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 prime number the MPS-f and Y the second one.

It is worth mentioning that because there is a unique MPS-f for each N_X , 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. N_X). However, the sink, in order to reconstruct the messages, needs also to know the index of the received component (i.e.i for each m_i). 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, N_X)) 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 m_i, 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. m_1. Moreover, the mask will be 001 for the second component m_2 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.

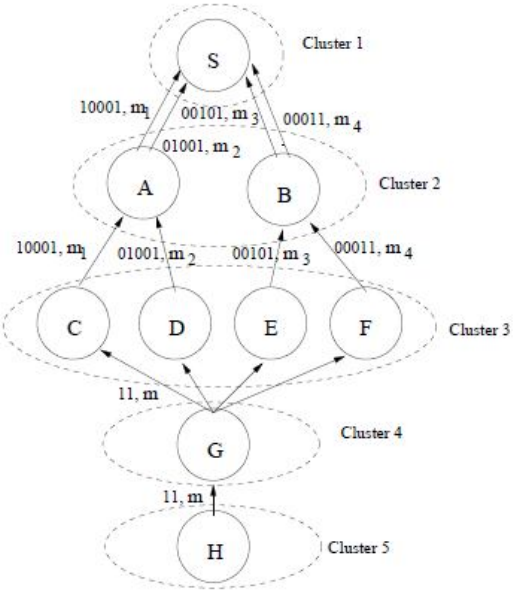
It is worth mentioning that the initialization procedure is performed only when the network is activated for the first time and it is not needed to run it when either a new node joins the network or a node belonging to a certain cluster goes out of energy. In both cases it is sufficient that few IMs(one 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

Copyright © 2013 SciResPub.

ISSN 2278-7763

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 $N_G = 4$ parts the messages received from G. therefore, when they receive the packet, according to both the packet size, w, and N_G, they select independently the prime numbers and send the components $m_i = m \pmod{p_i}$, 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 m_i , 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 c_i 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 $m = \sum_i c_i m_i \pmod{M'}$.

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 in account. In order to keep the complexity of the proposed algorithm very low, throughput the paper will consider that a packet can be splitted only one time.

III. ANALYTICAL RESULTS

Some analytical results were derived regarding the proposed method. The main results are:

1) It will be shown that by fixing w, a value of N exists above which the energy reduction factor starts to decrease. We explain the reason of this behavior and how to obtain this threshold, N_{max}, which corresponds to the maximum number of CRT components that should be used for a given value of w .
2) The impact of the number of admissible failures f on the network reliability will be evaluated analytically.
3) The impact of the number of admissible failures f on the energy reduction factor will be evaluated analytically.
4) An analytical model that can be used to estimate the mean energy reduction factor achievable with the proposed forwarding scheme is derived and it is proved that, under proper conditions, the proposed forwarding algorithm is able to

Copyright © 2013 SciResPub.

ISSN 2278-7763

reduce the mean energy consumption by about the 37%.

A. On the choice of the number of CRT components

Here some considerations about the choice of the number of CRT components. Obviously, the maximum number of components is limited by the node density of the network. But in this subsection its proved that, by fixing w, a maximum number of CRT components, N_{max}, exists above which the ERF decreases and therefore, even for high node densities, it is not convenient to use a number of CRT components greater than this value.

According eq.(1) it is possible to state that the ERF is maximized if the product $n_c . \overline{w}_{CRT}$ is minimized.

Intuitively, when the number of CRT components for each message, N_{CRT}, increases the number of CRT components that can be received by a node, n_c increases too. The amount of this increment could be more or less negligible on the basis of the node density but the proportionality law between n_c and N_{CRT} always holds. Therefore an increment of N_{CRT} can be justified only of $\overline{w}_{CRT}$ decreases. For a specific MPS={p_1,…, pN_{CRT} }, if we consider that number of bits of the *i*-th component is $[\log_2(pi)]$, the mean number of bits for the CRT components can be evaluated as

$$\overline{w}_{CRT} = \frac{\sum_{i=1}^{N_{CRT}} [\log_2(pi)]}{N_{CRT}} \quad 2.$$

Let us consider another MPS obtained by adding a new prime p_0 to the previous MPS.

It is straightforward to prove that the mean number of bits of this second MPS, $\overline{w}'_{CRT}$, is greater than $\overline{w}_{CRT}$ if $p_0 > pN_{CRT}$(i.e. if the MPS is extended toward the right) and smaller than $\overline{w}_{CRT}$ if $p_0 < p_1$ (i.e. if the MPS is extended toward the left).

However, observe that if the minimum prime number of the first MPS is $p_1 = 2$ a left extension cannot be done and therefore any increase of the N_{CRT} increases the $\overline{w}_{CRT}$ too.

Thus according to the previous statements, it can be conclude that it is convenient to increase the number of CRT components until the MPS does not contain the prime number 2 and therefore for a specific value of w the maximum value to be used for N_{CRT} is the minimum value N that satisfies $\prod_{i=1}^{N} p_i \geq 2^w$, with $p_1 = 2$. The values of $N_{max}$for different values of w arereported. Mean number of bits does not consider the actual number of bits in each CRT component but the maximum number of bits. When the actual number of bits is considered, it can be proved that the number of bits is reduced by about one bit for each component.

B. On the relation between reliability and admissible failures

Basically the reliability of a WSN can be defined as the probability that the sink is able to reconstruct the message.

Let see the analytical model with the aim of relating , with the probability of erasure, for a single hop, . This model, even if quite simple, allows us to obtain the value of to be chosen to achieve a desired . Let us assume that each node fails to forward a packet (i.e. a CRT component) with a know probability, . Therefore if is the number of hops needed to reach the sink, the probability that a CRT component is not received successfully is $= 1 - (1 -$) .According to the proposed forwarding algorithm, the sink will not be reconstruct the original message of more than components are not received, consequently, if we consider components, this happens with probability $P_N = \sum_{i=f+1}^{N_{CRT}} \binom{N_{CRT}}{i} p_n^i (1 - p_n)^{N_{CRT}-i}$ .Therefore the reliability can be related to both the erasure probability, p_e, and the number of failures f. as

$$P_R = 1 - P_N = \sum_{i=0}^{f} \binom{N_{CRT}}{i} p_n^i (1 - p_n)^{N_{CRT}-i} \quad 3.$$

$$P_R(with\ p_0 = 0.01, L = 5)$$

Copyright © 2013 SciResPub.

ISSN 2278-7763

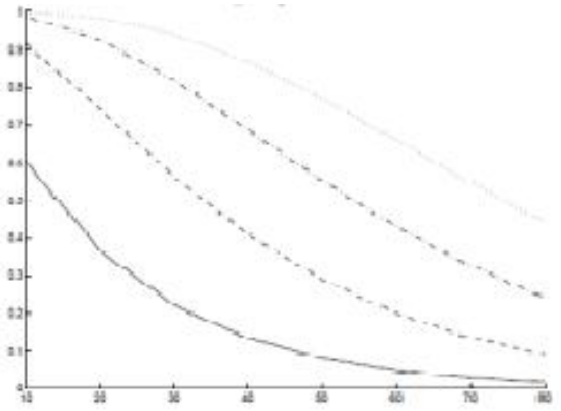


Fig.4.Reliability function: $p_e = 10^{-2}, L = 5, f \in \{0, \dots, 3\}$

As it observed that low values of are sufficient to increase the reliability.

In general according to eq.3 if the desired reliability is fixed and the parameters p_c and L are known, we can obtain the proper value of f.

C. *On the relation between ERF and admissible failures*

According to the previous results, it is possible to state that we can increase the reliability by increasing$f$. However this has a counter consequence the reduction of ERF.In fact in order to increase f (by maintaining the same number of CRT components, N_{CRT}) , The prime numbers p_i of the MPS must be increased too. Assuming eq.(2), when a greater value of prime numbers is chosen, the mean number of bits $\overline{w}_{CRT}$ increases and therefore, according to eq. (1)., the ERF decreases.

In this section we use the notation ERF_f and $\overline{w}_{CRTf}$ and highlight that ERF and $\overline{w}_{CRT}$are related to the specific value of admissible failures $f$and we show that ERF_f can be estimated analytically if the ERF_0 is known.Let us observe that eq. (1) can be rewritten as $ERF_f = 1 - \alpha_{\overline{w}_{CRTf}}$. where $\alpha=\frac{n_c}{n_p w}$. The factor $\overline{w}_{CRTf}$ can be obtained knowing , N_{CRT} and w (for instance, if $w = 100$ and $N_{CRT} = 20$, the MPS-f can be obtained and then, using eq.(2),it follows $\overline{w}_{CRT0} = 5.65$, $\overline{w}_{CRT1} = 5.85$, $\overline{w}_{CRT3} = 6.55$, $\overline{w}_{CRT5} = 7.40$).

Instead, the factor α does not change with f. In fact, when the number of transmitted packets and the number of CRT components are not changed, the number of forwarded packets (n_c, n_p) remains the same. It follows that α can be obtained from $ERF_0 = 1 - \alpha_{\overline{w}_{CRT0}}$ as $\alpha=\frac{1-ERF_0}{\overline{w}_{CRT0}}$ and it can be used to analytically evaluate ERF_f *as*

$$ERF_f = 1 - \frac{1-ERF_0}{\overline{w}_{CRT0}} \overline{w}_{CRTf} \qquad 4.$$

D. *Analytical model*

Here its derived analytical model that can be used to estimate the mean energy reduction factor achievable with the proposed forwarding scheme and in comparison of an usual forwarding algorithm, when a large number of nodes and messages are considered, the proposed algorithm is able to reduce the mean energy consumption by about the 37%.Eq.(1) can be rewritten by considering that n_c and $n_p$can be expressed on the basis of the number of sent messages n_m and the mean number of nodes used to forward the messages to the next cluster in the case of CRT and SP schemes, N_{Hcrt} and N_{Hsp} respectively. In fact, the mean number of packets forwarded by a node is $n_p \frac{n_m}{N_{Hsp}}$ for the SP forwarding algorithm (considering N_{CRT}packets for each message), so that $\frac{n_c}{n_p} = N_{CRT} \frac{N_{Hsp}}{N_{Hcrt}}$.

Accordingly, the ERF can be evaluated as $\frac{n_c}{n_p} = N_{CRT} \frac{N_{Hsp}}{N_{Hcrt}}$.Below we derive N_{Hcrt}, N_{Hsp} analytically.

We briefly review a classical "occupancy problem"[6]: " A group contains N persons, any w of whom can be selected at random form a committee. If r committees are formed, find the probability that exactly m persons will be committee members ". In [6] the probability distribution of $X = N - m$ is derived and it is proved that the expected number of persons who are not represented on a committee is $B_1 = N(1 - \frac{w}{N})^r$. Obviously, the expected number of persons who are

Copyright © 2013 SciResPub.

ISSN 2278-7763

represented on a committee is $E(m) = N - B_1 = N\left[\left(1 - \frac{w}{N}\right)^r\right]$.

We can re-read the above problem as follows: "given $N_T$possible nodes that can be used as next-hops, any N_{CRT} of whom can be selected at random to send a splitted message (i.e. its CRT components). If $N_m$messages are sent, find the probability that exactly N_{Hcrt} nodes will be used as next-hops". According to the above rules, the mean number of nodes used as next-hops is

$$N_{Hcrt} = N_T[1 - \left(1 - \frac{N_{CRT}}{N_T}\right)^{N_m}] \qquad 6.$$

Lets observe that, to obtain the mean number of nodes when an usual forwarding technique is used, it is sufficient to consider the above formula with $N_{CRT} = 1$ i.e.

$$N_{Hsp} = N_T[1 - \left(1 - \frac{1}{N_T}\right)^{N_m}] \qquad 7.$$

It is worth noting that the eq. 6 is valid only if all the CRT components are sent by the same node (i.e. for the first hop).

If the CRT components are sent independently (i.e. from different nodes), we have to consider each CRT component as a different packet so that the above formula have to be used also for the CRT-based forwarding technique considering a number of sent packets equal to $N_{CRT}N_m$ i.e.

$$N_{Hcrt} = N_T[1 - \left(1 - \frac{N_{CRT}}{N_T}\right)^{N_{CRT}N_m}]. \quad .8$$

However, if $N_{CRT} \ll N_T$ the equations 8 and 6 return the same values.By substituting equations 8 and 7 into eq. 5 we obtain:

$$ERT = 1 - N_{CRT}\frac{[1-\left(1-\frac{1}{N_T}\right)^{N_m}]}{[1-\left(1-\frac{1}{N_T}\right)^{N_{CRT}N_m}]}\frac{\overline{w}_{CRT}}{w} \qquad 9$$

If we restrict our analysis to the nodes of the second cluster $N_T$can be easily obtained by $N_T = \rho\pi R^2$where R is the transmission range of the sink and ρ is the network density. It should be noted that these nodes are the most important because represent the sink's neighbors: if these nodes run out of energy, the sink remains isolated from the rest of network preventing any message to reach it.

Finally, it is worth noting that

1) If $N_m$is fixed $N_T$tends to infinity if follows that ERF=MERT;
2) If both N_T and N_m tend to infinity and $N_{CRT}\,\overline{w}_{CRT} \approx w$, then ERF$\approx 1 - \frac{1-e^{-1}}{1-e^{-N_{CRT}}} \approx e^{-1}$ i.e. the ERF is about 0.37.

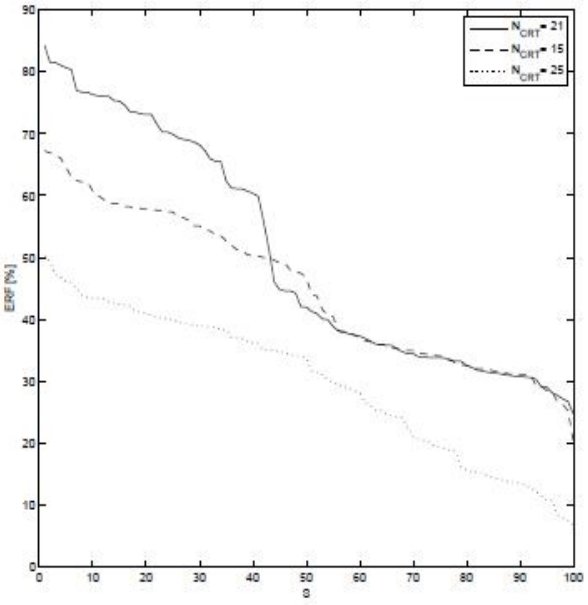


Fig.5. ERF vs. sorted topologies, S, with different values of

Copyright © 2013 SciResPub.

ISSN 2278-7763

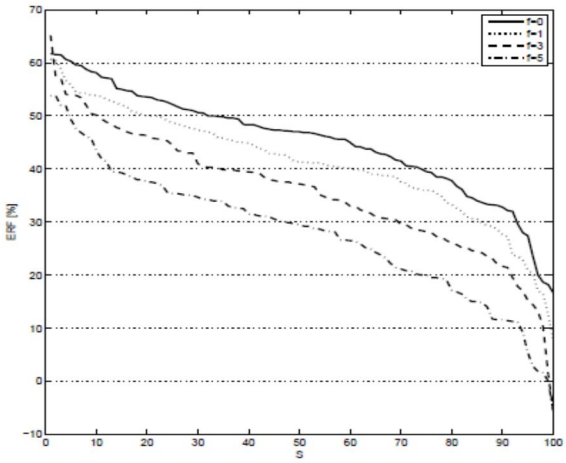


Fig. 6. ERF vs. sorted topologies, S, with different values of f.

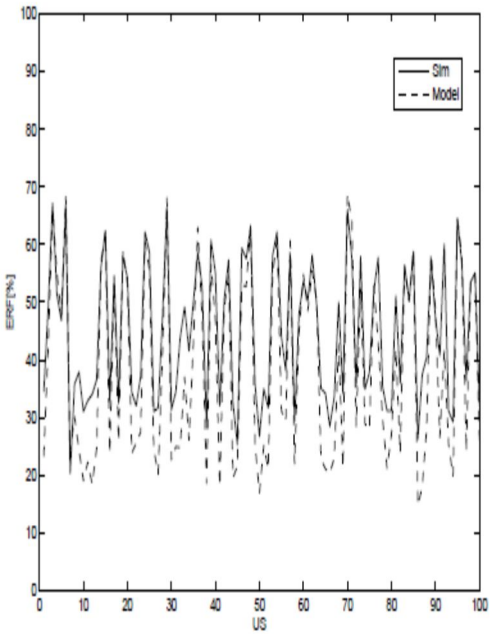
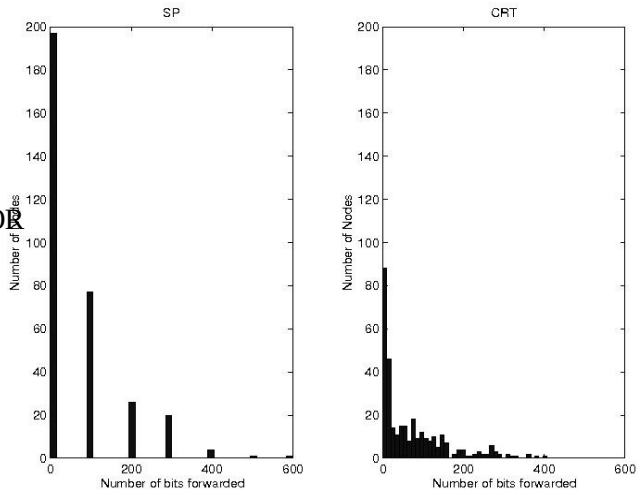


Fig. 7. Experimental and estimated values of the ERF vs unsorted
topologies (US).

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 ERFf FOR DIFFERENT VALUES OF f .



Copyright © 2013 SciResPub.

ISSN 2278-7763

Fig. 8. Number of bits forwarded from nodes belonging to $CLID = 2$, when $= [300m \; x \; 300m], w = 100 \; bits \; and \; \rho = 0.03$.

V. CONCLUSION

In this paper an analytical model for a recently proposed forwarding algorithm based on the Chinese Remainder theorem has taken. 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 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 its planned to study analytically the optimal number of components, N_{CRT} related to the network density.

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. Anastasi, 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 Remain-der 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 Netwo rks. *Mobile Computing and Communications Review (MC2R)*. Vol. 1, No. 2, 2002.

[8] J. Haapola, 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

Copyright © 2013 SciResPub.