

Innovative Packet Routing Solutions for improved Energy saving and Reliability in Wireless Sensor Networks

Kamana Singh¹, Ankur Goyal²

M. Tech student, Yagyavalkya Institute of Technology, Jaipur
Assistant Professor, Yagyavalkya Institute of Technology, Jaipur
Email: ¹er.kamnasingh@gmail.com

Abstract - Sensor networks offer a powerful combination of distributed sensing, computing and communication. In this paper an analytical model for 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.

Keywords - CRT (Chinese Remainder Theorem), GCD (Greatest Common Divisor), MERF (Maximum Energy Reduction Factor), MPS (Minimum Primary Set), RSA Algorithm (Ron Rivest, Adi Shamir and Leonard Adleman).

I. INTRODUCTION

Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors to co-operatively monitor physical or environmental conditions such as temperature, sound, vibration, pressure, motion or pollutants". WSNs have various applications that are widely used by researchers, exploration teams, military etc. The lifetime of the networks can be increased by efficiently using the energy and increasing the message transfer reliability. Protocols already proposed for ad hoc networks do not fully fit the requirements of the sensor networks, and several modifications or new approaches have been introduced [1-2]. At the network layer a significant subset of routing protocols for wireless sensor networks is based on a multipath approach [3]. However, multiple paths could remarkably consume more energy than the shortest path and several copies of the same packet could reach the

destination. In order to reduce the overhead introduced with multipath routing, authors in [4] have proposed a new mechanism that splits the original data packets into a number of subpackets equal to the number of disjoint paths from source to destination. With the aim of reducing energy consumption while taking the algorithmic complexity into account, we propose a novel approach that splits the original messages into several packets such that each node in the network will forward only small sub packets. The CRT technique is well known in cryptography [5], number theory, signal processing and channel coding [6]. The sensors are battery-operated with diverse capabilities and types and are empowered with limited data processing engines. The mission for these sensors is dynamically changing to serve the need of one or multiple command nodes. Command nodes can be stationary or mobile.

II. MOTIVATION FOR RESEARCH

This work can be summarized as these solutions are not suitable for applying to any networks without event loss and same time improved reliability and reduced energy usage. The followings are the limitations noticed in the literature review.

1. There algorithms proposed are not suitable for execution in Wireless sensor network because they consume more time.
2. Movement of sensor nodes or nodes is proposed which is not practical in all networks.

So the new innovative idea is proposed by authors Giuseppe Campobello, Alessandro Leonardi and Sergio Palazzo, that is Improving Energy Saving and Reliability in Wireless Sensor Networks Using a Simple

CRT-Based Packet-Forwarding Solution has been implemented in this paper work.

III. RELATED WORK

Splitting techniques are used for splitting the original message and they are carried out in a simple manner to reduce the energy consumption of the system. Reliability should be taken in account as the possibility that the original message cannot be obtained when the packets are spitted into too many small packets. In this section, the implementation of the system is done by using CRT based packet forwarding technique which includes GCD as a part of it and few approaches of RSA algorithm are also used.

A. The Chinese Remainder Theorem

Packets are split into sub packets using Chinese Remainder Theorem. Let x_1, x_2, \dots, x_k be the prime numbers. (pair wise relatively prime integers) [5]. If y_1, y_2, \dots, y_k are any integers, then there exist a unique integer p modulo $Z = x_1 * x_2 * \dots * x_k$ that satisfies the system of linear Congruencies,

$$\begin{aligned} A &\cong y_1 \pmod{x_1} \\ A &\cong y_2 \pmod{x_2} \\ &\dots \\ A &\cong y_k \pmod{x_k} \end{aligned}$$

Moreover $p \cong x_1 Z_1 b_1 + x_2 Z_2 b_2 + \dots + x_k Z_k b_k \pmod{Z}$ where $Z_i = Z/x_i$ and $Z_i b_i = 1 \pmod{x_i}$ for $i=1,2,\dots,k$. There are conditions where x_i 's are not pairwise coprime. In such a case the simultaneous congruencies of p exists iff $y_i \cong y_j \pmod{\gcd(x_i, x_j)}$

for all i and j . For instance It is considered that the system:

$$\begin{aligned} m &= 1 \pmod{3} \\ m &= 4 \pmod{5} \\ m &= 1 \pmod{7} \end{aligned}$$

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 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 each m_i . Therefore if, instead of m , m_i numbers, with $m_i = m \pmod{p_i}$, are

forwarded in a wireless sensor network, the maximum energy consumed by each node for the transmission can be substantially reduced.

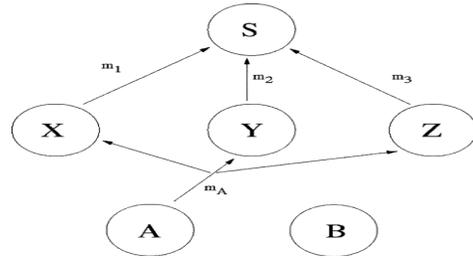


Fig .1 Example of Splitting and forwarding

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 $i \in \{1, 2, 3\}$, and using the CRT approach, will be able to reconstruct m_A .

B. GCD Algorithm

In CRT algorithm when there are conditions where no pair wise co prime exists GCD algorithm is taken into account [7]. The algorithm is stated as :

Begin algorithm

Function greatest common divisor (x, y) While value of x is not equal to y ($x \neq y$) Thenif value of x is greatest than that of y ($x > y$)

$x := x - y$

else

$y := y - x$

The value of x or y obtained is taken as output.

The recursive version of the GCD algorithm of successive remainders can be stated as: function greatest common divisor (a, b).if the value of $y = 0$ then return the value of x as output elsereturn greatest common divisor (y, $x \pmod{y}$)

C. RSA Algorithm

RSA algorithm is developed Ron Rivest, Adi Shamir and Leonard Adleman in the year 1977. RSA is used as an internet authentication and encryption system which is used as a part of web browsers.

The algorithm mainly involves two large prime numbers which are multiplied and constitutes of public key and private key operations [8] [6]. The originally randomly considered prime numbers can be discarded once the two keys are developed. The encryption and decryption procedure uses these public and private keys in order to transmit the confidential data. Concept of RSA algorithm is used to find random numbers:

1. Choose two distinct prime numbers p and q
2. Compute $n = pq$. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length
3. Compute $z = (p - 1)(q - 1)$.
4. Choose an integer e such that $1 < e < z$
5. Determine d as $(d * e) \bmod z = 1$.

Finally,

Encryption: $c = m^e \bmod n$

Decryption: $c^d \bmod n$

D. Metrics for energy efficiency

According to CRT algorithm, with the specified set of numbers that are provided, a number can be alternatively identified. To find the number i.e., a prime number which are randomly generated concepts of RSA algorithms are considered and used. 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 W_{CRTmax} the maximum number of bits of a CRT component, i.e. $W_{\text{CRTmax}} = \max(\lceil \log_2(\pi_i) \rceil)$, we can consider a theoretical maximum energy reduction factor (MERF) given by

$$\text{MERF} = w - W_{\text{CRTmax}}/w.$$

For instance, in the previous example is $\text{MERF} = 7 - 3/7 \approx 0.57$, this means that about 57% of the energy could be saved by considering the proposed forwarding scheme. 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 casewhere 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). 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. $\text{ECRT} = n_c \bar{w}_{\text{CRT}}$ and $\text{ESP} = n_p w$ 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:

$$\text{ERF} = \frac{\text{ESP} - \text{ECRT}}{\text{ESP}} = 1 - \frac{n_c \bar{w}_{\text{CRT}}}{n_p w} \quad (1)$$

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

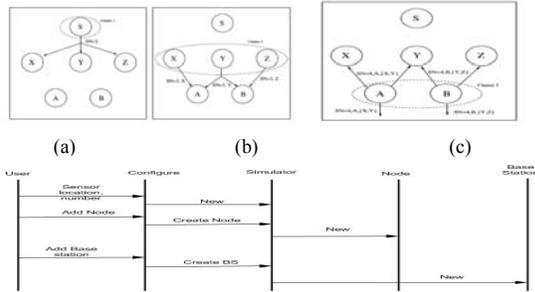
E. Choosing Prime Numbers

The number of bits needed is represented using the prime numbers. Prime numbers are selected as small as possible and primary numbers are chosen arbitrarily. The MERF may be maximized as the result of selecting small prime numbers. The set of smallest consecutive primes are used to indicate throughout the paper that satisfies the condition, the set is called as Minimum Primes Set (MPS).

It is considered that primes set $\{10313, 10321, 10331, 10333\}$. These are the smallest consecutive primes that satisfy the condition $\pi_i \pi_i \geq 2^{40}$ 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, following observations have been found:

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



(d) Sequence diagram of initialization phase

Fig. 2 Initialization procedure

For instance if the last component m_4 is not received it is again possible to obtain m as $m = \sum_{i=1}^3 c_i m_i \pmod{M'}$ where $M' = \prod_{i=1}^3 p_i$ is the product of the first three primes, and c_1, c_2, c_3 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.

F. Phases of Algorithm

There are two phases in this algorithm which are temporal. The initialization phase and the forwarding phase.

1. Initialization

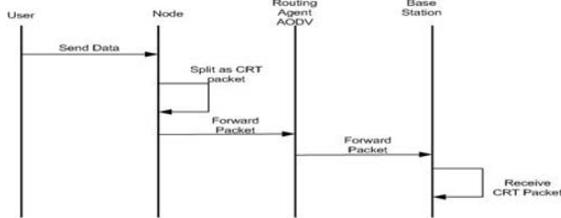
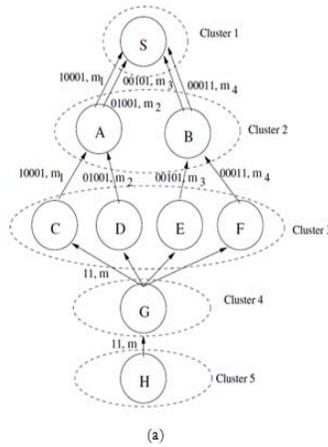
The Initialization phase organizes the networks in the clusters and has the advantage of minimizing the number of hops needed to reach the sink. The initialization message is exchanged where the cluster number is identified. The initialization messages are received by the nodes from its neighbours, they are named with the sequence numbers. They belong to the clusters and the initialization messages starts from the sink. The procedure is as follows, the sink sends the first initialization message. They are split and sent to the neighbouring nodes and are received by the nodes X, Y and Z . The nodes X and Y are used as next-hops and the messages from the A are split into several packets and the initialized messages are retransmitted. The source address is specified in the received messages and they will be used as forwarders.

It is considered that 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.2a). Note that the sequence number $SN= 1$ is reserved to identify a failure or to reset an already initialized network. All the nodes that receive the IM with $SN= 2$ assume to belong to $CLID = 2$ and consider the sink as their nexthop. Nodes in $CLID = 2$ will retransmit both the IM with an increased sequence number ($SN= 3$) and their addresses (see Fig.2b). 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.2c). 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.4.3.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. 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.

2. Forwarding phase

In this paper the forwarding procedure is actually applied. When the procedure is applied to a wireless sensor network, the number N_x of primes corresponds to the number of forwarding nodes for each source X . It is considered that the network shown in Fig. 3(a) where clusters are obtained according to the initialization procedure already described in the previous section.



(b) Sequence Diagram of forwarding phase

Fig. 3 Forwarding Example

The figure shows the messages and masks sent by each node when the source node H sends a message m to the sink S. because there is a unique MPS (unique set of primes) 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 on which it is splitted (i.e. N_x).

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 [9].

Finally, when the sink receives at least $N-f$ components of the original message, it can reconstruct the message by $m = \sum_i c_i m_i \pmod{M'}$.

IV. RESULT

A. Analytical Result

In this section we will derive some analytical results regarding the proposed method. The main results are briefly summarized below:

- 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 reduce the mean energy consumption by about the 37%.

1) On the choice of the number of CRT components

In this subsection we report some considerations about the choice of the number of CRT components.

Table I
W V/S Nmax

W	Nmax
32	10
40	12
64	16
100	22
150	30
200	37

Obviously, the maximum number of components is limited by the node density of the network, but in this subsection we intend to prove 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 to eq. (1) it is possible to state that the ERF is maximized if the product $n_c \cdot \bar{w}_{CRT}$ is minimized. Intuitively, when the number of CRT components for each message, $NCRT$, 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 $NCRT$ always holds. Therefore an increment of $NCRT$ can be justified only if \bar{w}_{CRT} decreases. For a specific MPS= $\{p_1, \dots, p_{NCRT}\}$, if we consider that the number of bits of the i -th component is $\lceil \log_2(p_i) \rceil$, the mean number of bits for the CRT components can be evaluated as

$$\bar{w}_{CRT} = \prod_{i=1}^{NCRT} [\log_2(p_i)] / NCRT \quad (2)$$

It is considered that 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, \bar{w}'_{CRT} , is greater than \bar{w}_{CRT} if $p_0 > p_{NCRT}$ (i.e. if the MPS is extended toward the right) and smaller than \bar{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 $NCRT$ increases the \bar{w}_{CRT} too. Thus, according to the previous

statements, we can 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 $NCRT$ is the minimum value N that satisfies $\prod_{i=1}^N p_i \geq 2$, with $p_1 = 2$. In Table I the values of N_{max} for different values of w are reported.

According to the proposed forwarding algorithm, the sink will not be able to reconstruct the original message if more than f components are not received, consequently, if we consider $NCRT$ components, this happens with probability $PN = \sum_{i=f+1}^{NCRT} \binom{NCRT}{i} p_n^i (1-p_n)^{NCRT-i}$. Therefore, the reliability can be related to the erasure probability, p_e , and the number of failures, f , as follows:

$$PR = 1 - PN = \sum_{i=f+1}^{NCRT} \binom{NCRT}{i} p_n^i (1-p_n)^{NCRT-i} \quad (3)$$

2) 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 as a counter consequence the reduction of ERF. In fact, in order to increase f (by maintaining the same number of CRT components, $NCRT$), 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 \bar{w}_{CRT} increases and therefore, according to eq. (1), the ERF decreases. In this section we use the notation ERF_f and \bar{w}_{CRT}^f to highlight that ERF and \bar{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 $ERF_f = 1 - \alpha \bar{w}_{CRT}^f$, where $\alpha = n_c / n_p w$. The factor \bar{w}_{CRT}^f can be obtained knowing f , $NCRT$ and w (for instance, if $w = 100$ and $NCRT = 20$, the MPS- f can be obtained and then, using eq. (2), it follows $\bar{w}_{CRT}^0 = 5.65$, $\bar{w}_{CRT}^1 = 5.85$, $\bar{w}_{CRT}^3 = 6.55$, $\bar{w}_{CRT}^5 = 7.40$). 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 $ERF_0 = 1 -$

$\alpha \bar{\omega}_{\text{CRTf}} 0$ as $\alpha = 1 - \text{ERF}_0 / \bar{\omega}_{\text{CRTf}0}$ and it can be used to analytically evaluate ERFf as

$$\text{ERFf} = 1 - \frac{1 - \text{ERF}_0}{\bar{\omega}_{\text{CRTf}}} \bar{\omega}_{\text{CRTf}} \quad (4)$$

3) Analytical Model

In this subsection we derive an analytical model that can be used to estimate the mean energy reduction factor achievable with the proposed forwarding scheme. Furthermore, we prove that, 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 $n_p = N_m / N_{\text{Hsp}}$ for the SP forwarding algorithm and $n_c = N_m N_{\text{CRT}} / N_{\text{Hcrt}}$ for the proposed CRT-based forwarding algorithm (considering N_{CRT} packets for each message), so that $N_c/n_p = N_{\text{CRT}} (N_{\text{Hsp}}/N_{\text{Hcrt}})$. Accordingly, the ERF can be evaluated as

$$\text{ERF} = 1 - N_{\text{CRT}} \frac{N_{\text{Hsp}} \bar{\omega}_{\text{CRT}}}{N_{\text{Hsp}} w} \quad (5)$$

Below we derive N_{Hcrt} , N_{Hsp} analytically. We briefly review a classical ‘‘occupancy problem’’ [10]: ‘‘A group contains N persons, any w of whom can be selected at random to form a committee. If r committees are formed, find the probability that exactly m persons will be committee members’’. In [10] 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 $B1 = N(1 - w/N)^r$. Obviously, the expected number of persons who are represented on a committee is $E(m) = N - B1 = N[1 - (1 - w/N)^r]$. According to the above results, the mean number of nodes used as next-hops is

$$N_{\text{Hcrt}} = NT [1 - (1 - N_{\text{CRT}} / NT)^{N_m}] \quad (6)$$

Let us 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 $N_{\text{CRT}} = 1$, i.e.

$$N_{\text{Hsp}} = NT [1 - (1 - 1/NT)^{N_m}] \quad (7)$$

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 $N_{\text{CRT}} N_m$, i.e.

$$N_{\text{Hcrt}} = N_T [1 - (1 - 1/NT)^{N_{\text{CRT}} N_m}] \quad (8)$$

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

$$\text{ERF} = 1 - N_{\text{CRT}} \{ [1 - (1 - 1/N_T)^{N_m}] / [1 - (1 - 1/N_T)^{N_{\text{CRT}} N_m}] \} \bar{\omega}_{\text{CRT}} / w \quad (9)$$

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. Finally, it is worth nothing that

- if N_m is fixed and NT tends to infinity it follows that $\text{ERF} = \text{MERF}$
- if both NT and N_m tend to infinity and $N_{\text{CRT}} \bar{\omega}_{\text{CRT}} \approx w$, then $\text{ERF} \approx 1 - 1 - e^{-1} / 1 - e^{-N_{\text{CRT}}} \approx e^{-1}$, i.e. the ERF is about 0.37.

B. Performance Evaluation

We consider a sensor network where nodes are randomly distributed in a square area of size $\text{GridSize} = [300\text{m} \times 300\text{m}]$ with density $\rho = 0.03$. 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 $R = 60\text{m}$., the network is organized in clusters numbered in ascending order starting from the cluster where is located the sink node, which is identified with $\text{CLID} = 1$. Moreover, nodes have a unique address, $\text{ID} \geq 2$, assigned during the initialization phase ($\text{ID} = 1$ is assigned to the sink node). A certain number of events, called $\text{Ev} = 15$, happens randomly in the sensor network. We assume that each event happens in cluster $\text{CLID}(\text{TX}) \geq 5$. 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. 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, m_X , whose word size in bits is equal to $w = 100$ bits if not differently specified. Therefore, for each event E_v , the number of messages generated is in the order of $\rho \cdot r^2$, i.e. $N_m E_v \cdot r^2$. First, we verify the results 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).

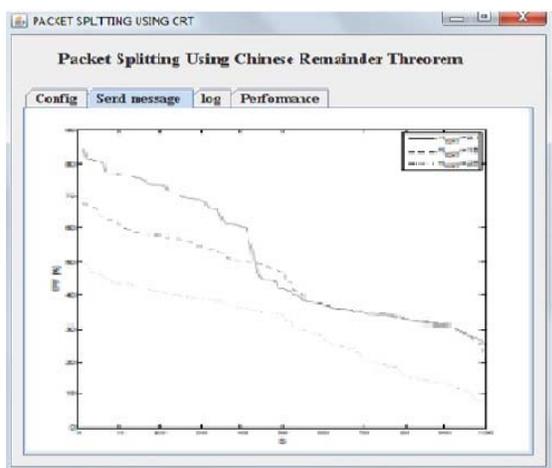


Fig. 4 ERF vs. sorted topologies, S , with different value of NCRT (21,15,25)

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. 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 $NCRT \cdot r_{CRT}$ are very close.

Finally in Fig. 5 and 6, we observe the number of bits forwarded from the nodes belonging to $CLID = 2$ and

Comparison of energy levels of both CRT and NON CRT (sorted path topology).

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. In this paper an analytical model for proposed forwarding algorithm based on the Chinese Remainder Theorem has been introduced.

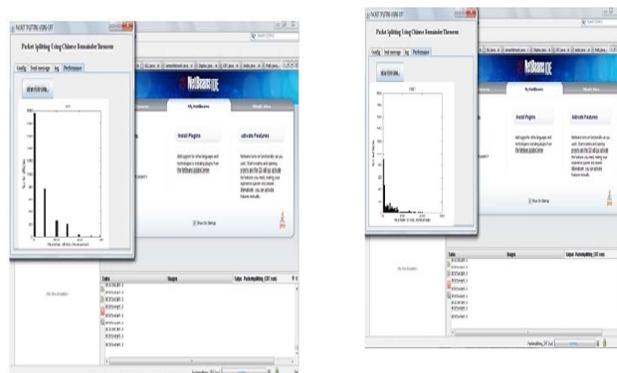


Fig.5 Number of bits forwarded from nodes belonging to $CLID=2$, when Grid Size = [300m, 300m], $w=100$ bits and $\rho=0.03$

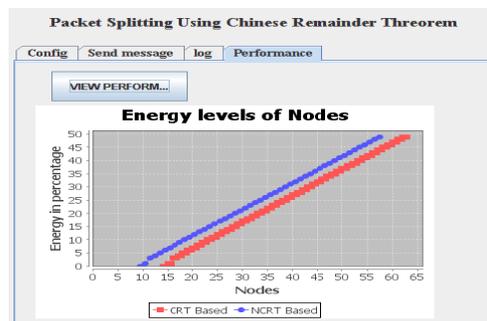


Fig.6 Comparison of CRT and Non CRT graph

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.

V. CONCLUSION

In this paper, we have provided with a novel forwarding technique based on the Chinese Remainder Theorem (CRT) in WSN's. We have provided a method in which there is minimum energy consumption and remarkable improvement in performance. Starting from choosing the CRT algorithm parameters in order to keep the processing complexity low, then we have derived trade-offs between energy consumption and reliability. The prime numbers are obtained and the algorithm is run and the resulting output is shown. The obtained output clearly shows that the performance of the CRT based algorithm is better than Non-CRT based algorithm.

VI. REFERENCES

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp.102–114, Aug. 2002.
- [2] K. Akkaya, M. Younis. A Survey of Routing Protocols in Wireless Sensor Networks. Elsevier Ad Hoc Network Journal. Vol. 3, No. 3, pp. 325-349, May 2005.
- [3] Parallel Extended GCD Algorithm Pou-Yah Wu and Julian Chuen-Liang Chen Dept. of Information Management, Kaohsiung Polytechnic Institute.
- [4] S. Dulman, T. Nieberg, J. Wu, P. Havinga. Trade-Off between Traffic Overhead and in Multipath Routing for Wireless Sensor Networks. Proc. Of WCNC Conference, New Orleans, USA, March 2003.
- [5] 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.
- [6] O. Goldreich, D. Ron, M. Sudan. Chinese remaindering with errors. Proc. of the thirty-first annual ACM symposium on Theory of computing (STOC '99), Atlanta, USA, May 1999.
- [7] Comparing Several GCD Algorithms T. Jebelean RISC-Linz, A-4040 Austria.
- [8] File encryption and decryption system based on RSA algorithm Suli Wang Ganlai Liu School of Information Engineering Support Center Jingdezhen Ceramic Institute Jingdezhen Telecom Jingdezhen, Jiangxi Province, China Jingdezhen, Jiangxi Province, China.
- [9] A. Menezes, et al., *Handbook of Applied Cryptography*, CRC Press, Oct.1996.
- [10] A.M. Gittelsohn. An Occupancy Problem. *The American Statistician*, Vol.23, No. 2, pp. 11-12, April 1969.