Implementation of Modified CRT Algorithm for Packet Routing Evaluation to Improved Energy Saving and Reliability in Wireless Sensor Networks

Kamana Singh[#1], Ankur Goyal[*2]
[#]*M. Tech student, Yagyavalkya Institute of Technology, Jaipur*
[*]*Assistant Professor, Yagyavalkya Institute of Technology, Jaipur*

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 [5]. 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 [7] 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 [9], number theory, signal processing and channel coding [3].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[1].

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 x1, x2,…, xk be the prime numbers. (pair wise relatively prime integers)[9]. If y1,y2 ,…,yk are any integers, then there exist a unique integer p modulo Z = x1*x2*…*xk that satisfies the system of linear Congruencies,

A ≅y1 (mod x1)

A ≅ y2 (mod x2)

…

A ≅ yk (mod xk)

Moreover p ≅ x1Z1b1 + x2Z2b2 + … + xkZkbk (mod Z) where Zi = Z/xi and Zibi = 1 (mod xi) for i=1,2,…,k .There are conditions where xi's are not pairwise coprime. In such a case the simultaneous congruencies of p exists iff yi ≅ yj (mod gcd(xi,xj))

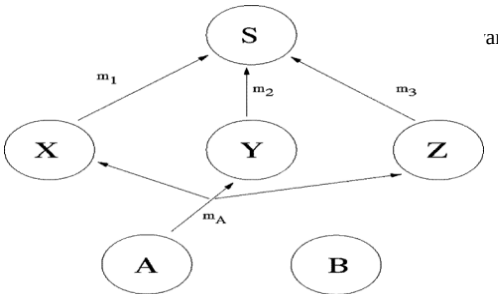
for all i and j.For instance It is considered that the system:

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.



arding

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. GCD Algorithm

In CRT algorithm when there are conditions where no pair wise co prime exists GCD algorithm is taken into account[4][5]. The algorithm is stated as :

Begin algorithm

Function greatest common divisor (x, y) While value of x is not equal to y (x ≠ 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 mod 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[7].

The algorithm mainly involves two large prime numbers which are multiplied and constitutes of public key and private key operations[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 $(d*e) mod\ z = 1$.

Finally,

Encryption: c=m^e mod n

Decryption: c^d mod 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 Wcrtmax the maximum number of bits of a CRT component, i.e. Wcrtmax = max(⌈log2(pi)⌉), we can consider a theoretical maximum energy reduction factor (M ERF) given by

MERF =w – Wcrtmax/w.

For instance, in the previous example is MERF =7−3/7≈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 case where all the components of the previous example have to be forwarded by the same node, we have an energy reduction factor equal to7−5/7≈ 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. 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 of bits needed to represent the CRT components:

$$ERF = \frac{ESP - ECRT}{ESP} = 1 - \frac{nc\ \bar{\omega} CRT}{npw} \quad (1)$$

The above metrics(equation) well be 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 πipi $\geq 2^{40}$ 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).
- 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' = $\prod_{i \neq jpi} > 2^{40}$ and therefore it respects the hypopaper of the CRT theorem.

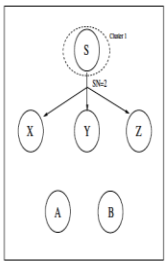
For instance if the last component m4 is not received it is again possible to obtain m as m = $\sum_{i=1}^{3} ci.mi\ (mod\ M')$ where M' = $\prod_{i=1}^{3} pi$ is the product of the first three primes, and c1, c2, c3 are the first three CRT coefficients computed for the MPS-1 on the basis of the CRT 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.

F. Phases of Algorithm

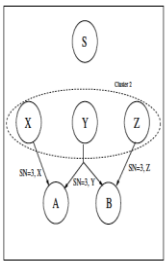
There are two phases in this algorithm which are temporal. The initialization phase and the forwarding phase.

1) Initialization

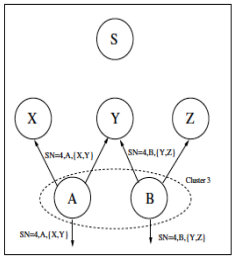
The Initialization phase organizes the networks in the clusters and has the advantage of minimizing the number of hops needed to reach the sink.The initialization message is exchanged where the cluster number is identified. The initialization messages are received by the nodes from its neighbours, they 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. Step by step initialization process is shown in fig 2(a), 2(b), 2(c) and 2(d).



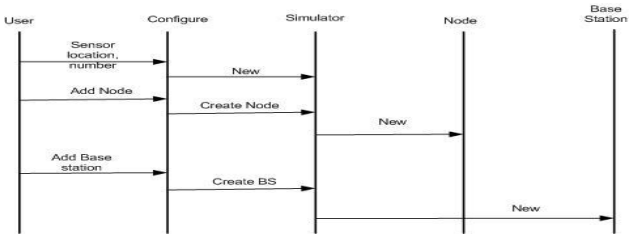
(a) Sink node sends IM with SN=2



(b) Nodes CLID=2 retransmit both IM and address



(c) Nodes CLID=2 retransmit both the IM with increased SN=3 and their address



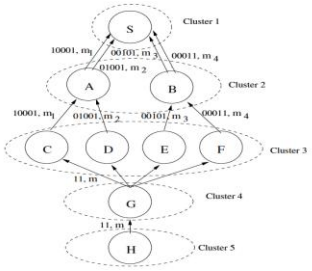
(d) Sequence Diagram of initialization phase

Fig. 2 Initialization procedure

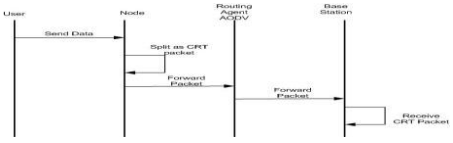
The initialization procedure is performed only when the network is activated for the first time and it is not needed to run it when either a new node joins the network or a node belonging to a certain cluster goes out of energy.

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



(a) Messages and masks sent by each



(b) Sequence Diagram of forwarding phase

Fig. 3 Forwarding Example

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.
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 example if w=40 and f=1, the MPS-1 is {10313,10321,10331,10333}so that these are also 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.
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 calculates the coefficients ci needed to reconstruct the original message[8].
Finally, when the sink receives at least N−f components of the original message, it can reconstruct the message by m = $\sum_i cimi$(mod M').

IV. Result (Output)

A. Analytical Result

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

1)In this section we consider choice of the number of CRT components.

TABLE 1:
Nmax vs w

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

the maximum number of components is limited by the node density of the network, but in this section we prove that, by fixing w, a maximum number of CRT components, Nmax, means ERF decreases from eq.(1)we know that, it is possible to state that the ERF is maximized if the product nc · $\bar{\omega}_{CRT}$ is minimized.When the number of CRT components for each message, NCRT , increases, the number of CRT components that

can be received by a node, nc, increases.if we consider that the number of bits of the i-th component is ⌈log2(pi)⌉, the mean number of bits for the CRT components can be evaluated as

$\bar{\omega}_{CRT} = \prod_{i=1}^{NCRT} [log2\ (pi)] / N_{CRT}$ (2)

if the minimum prime number of the first MPS is p1 = 2 a left extension cannot be done and therefore any increase of the NCRT increases the $\bar{\omega}_{CRT}$ too. Thus, fron 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 2and therefore, for a specific value of w, the maximum valueto be used for NCRT is the minimum value N that satisfies $\prod_{i=1}^{N} pi >= 2$, with p1 = 2. In Table 1shows the values of Nmax for different values of w.

According to our 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

$PN = \sum_{i=f+1}^{NCRT} \left(\frac{NCRT}{i}\right) p_n^i (1\text{-}p_n) N_{CRT} - i$

Therefore, the reliability can be related to both the erasure probability, pe, and the number of failures, f, as follows:

$PR = 1 - PN = \sum_{i=f+1}^{NCRT} \left(\frac{NCRT}{i}\right) p_n^i (1\text{-}p_n) N_{CRT} - I$ (3)

2) analytical model is used to estimate the mean energy reduction factor i.e achieved by using proposed forwarding scheme.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%.From the Eq.(1) we considering that nc and np can be expressed on the basis of the number of sent messages Nm and the mean number of nodes used to forward the messages to the next cluster in the case of CRT and SP schemes, NHcrt and NHsp respectively. In fact, the mean number of packets forwarded by a node is np = Nm / NHsp for the SP forwarding algorithm and nc = NmNCRT / NHcrt for the proposed CRT-based forwarding algorithm (considering NCRT packets for each message), so that Nc/np = NCRT (NHsp/NHcrt) Accordingly, the ERF can be evaluated as

$ERF = 1 - NCRT \frac{NHsp}{NHsp} \frac{\bar{\omega} CRT}{W}$ (5)

If we considered only 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 we say that:

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

3) 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%.

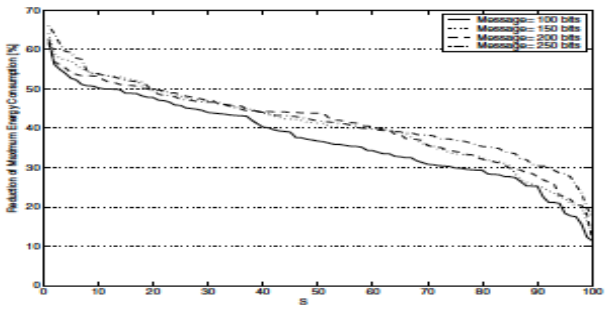
B. Performance Evaluation

We consider a sensor network where nodes are randomly distributed in a square area of size GridSize = [300m × 300m] with density ρ = 0.03. we evaluate the reduction of maximum energyconsumption in percentage, calculated as

$ERF=(E_{SP}-E_{CRT})/E_{SP}$or

$ERF = (1- NcW_{CRT})/ N_PW$ or by directly using eq(5).

considering three different values of ρ. We haveconsidered 100 different topologies, S=[1, 100], and we havesorted them so that the corresponding values of E(S) resultordered from the highest to the smallest value. We observethat CRT achieves better results if compared to SP in 90% ofthe different topologies considered. In the remaining 10% oftopologies CRT shows worse performance.In fig: 4 we see that if MNN=20 When w increases, CRT achieves a higher reduction of energyconsumption if compared to SP and the effect of CRT splittingis more evident.Sensor nodes are considered static as usual in most application scenarios[1].



Fi g . 4Reduction of maximum energy consumption (SP - CRT) vs. sorted
topologies, S, with different values of w.

Finally to evaluate the effectiveness of the CRT algorithm, in Fig. 5 and 6 we show 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. Because

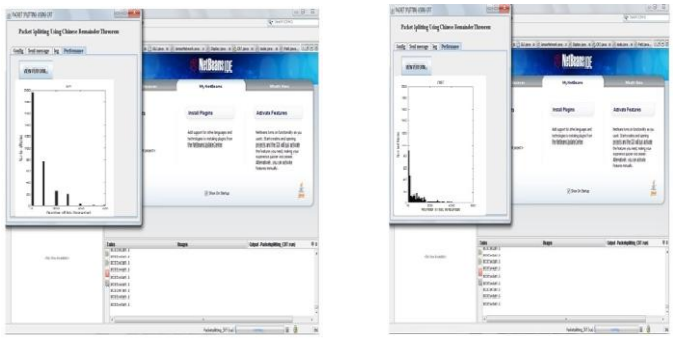


Fig.6 Comparison of CRT and Non CRT graph

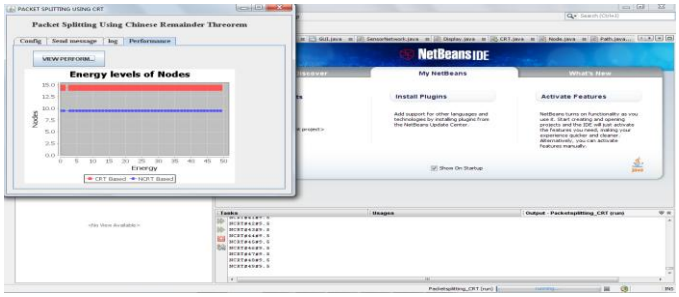


Fig.5 Number of bits forwarded from nodes belonging to CLID=2, when Grid Size = [300m, 300m], w=100 bits and ρ=0.03

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. ACKNOWLEDGEMENTS

First we thank God Almighty for his blessings for this paper. I would like to thank my HOD and paper Guide Mr. Ankur Goyal for taking me under his wing and providing constant support and motivation during the term of the paper and for his time, valuable input and feedback during the different phases of the paper. Without their vision and versatility, this report and its implementation would not have been feasible right from the formulation of the report. We thank this opportunity to express my hearty thanks to my parents and friends for the moral support, encouragement to make this as a success.

VII. 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] *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.*

[4] *Comparing Several GCD Algorithms T. Jebelean RISC-Linz, A-4040 Austria.*

[5] *Parallel Extended GCD Algorithm Pou-Yah Wu and Julian Chuen-Liang Chen Dept. of Information Management, Kaohsiung Polytechnic Institute.*

[6] *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.*

[7] *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.*

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

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