Improving Reliability in WSN by Collaborating Robust Data Aggregation and CRT-based Packet Forwarding Technique

Navnit Kumar Singh, Archana Singh, Pushpendra foujdar
Mail id: navnits8@gmail.com, archanasingh0786@yahoo.com, level4newlife@gmail.com

Abstract

Aimed at combination of high performance and low computational complexity having reliability and energy efficiency as the main goal this paper provides a novel packet forwarding scheme for wireless sensor networks. This packet-splitting algorithm is based on the Chinese Remainder Theorem (CRT) which is characterized by simple modular division between numbers of integers. Simplified protocol architecture is designed to make communication simple and efficient. The solutions elaborated for these network must be aimed at fair distribution or minimizing the energy and delay which determines the reliability of the system.

Key Words: 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. To make the communications efficient and simple, simple protocol architecture can be designed as their processing capabilities are low. The solutions derived for these networks are aimed at reducing the energy consumption. The power unit of the networks is based on the battery which saves energy. The data transmission consumes more energy in these networks and so the energy conservation methodologies are based on reducing the energy consumed by the radio interface.

A new approach is proposed to reduce the consumption of energy and considering the complexity of the algorithm by splitting the original message into packets such that the node forwards only the sub-packets. The Chinese Remainder Theorem algorithm (CRT) which uses a simple modular division is applied to split the packets.

The split messages are received by the sink node and they are combined to form the original message. Almost all nodes operated through classical forwarding algorithm except sink nodes as they need low complex arithmetic operations to be operated. The more the nodes are solicited from the other nodes; the splitting procedure is more efficient for such nodes. The sink node should be considered as more equipped energetically and computationally than the other nodes, they become suitable for a WSN and the complexity remains low. The energy consumption and complexity can be derived using a analytical framework model that makes the results more accurate. The analytical study of the tradeoff between reliability, energy saving and complexity has been done

Forwarding Examples:

Consider the examples of various message transmission methods.

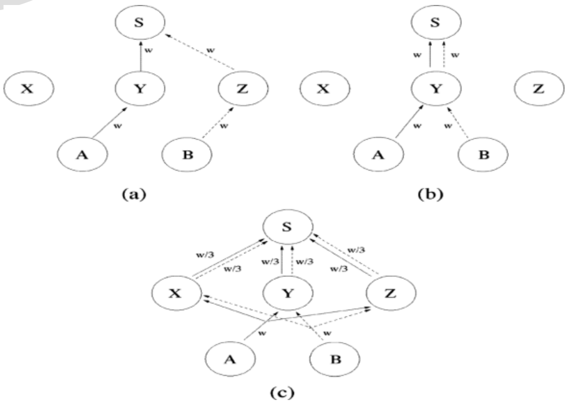


Fig (a) represents the message forwarding with next hops. Fig (b) the same next hop message forwarding. Fig (c) The messages are split and forwarded. The sink S and can do it through nodes X, Y, and Z, Fig (a)

represents the message forwarding with next hops. Fig (b) the same next hop message forwarding. Fig (c) The messages are split and forwarded.
The sink S and can do it through nodes X, Y, and Z, which are all in the coverage range of A and B.
Two cases can be differentiated when the normal forwarding scheme is adopted.

Case a) Nodes A and B select different next-hop nodes using probability. [See Fig. 1(a)].
Case b) Nodes A and B select the same next-hop nodes using probability. [See Fig. 1(b)].

The maximum number of bits transmitted by a node belonging to the set is the number of bits in both the cases (a) and (b). Let us Consider that each node in the set knows that A and B have three possible next-hops and a different forwarding scheme is adopted, as shown in Fig(c). When X, Y, and Z receive a packet, they split it and sub-packets are sent to the sink. The nodes X, Y and Z have to transmit at most bits each. By comparing the two forwarding methods the second one has maximum number of bits transmitted. The reduction factor is obtained by comparing the splitting procedure as shown in the cases a and b. The average reduction factor of value 4/9 is obtained.
If the energy consumption is distributed among the nodes, the maximum number of bits transmitted per node is reduced and the mean energy consumed is also reduced by splitting the packets. When the energy is distributed among the nodes the lifetime of a sensor network increases.
For example, Consider Fig (c) the messages of b are sent. X,Y,Z will forward six messages without forwarding, after using splitting technique messages are split into three components and forwarded from b. While splitting maximum number of transmitted bits per node is reduced. The more number of bits are reduced as the node keeps splitting forward.

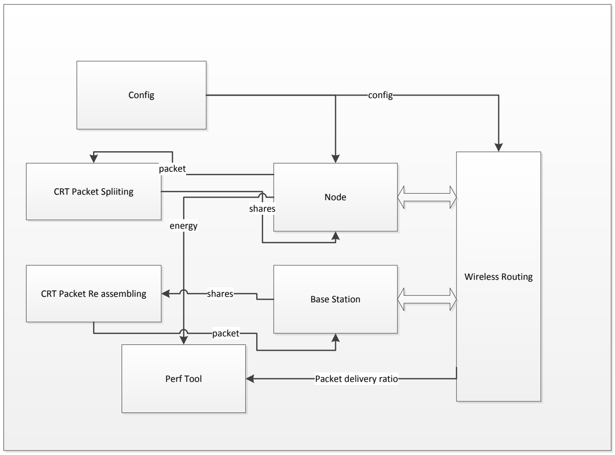
II. Basic idea

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. To reduce the risk of losing the original message and maintain reliability several measures can be taken. The sensor networks are created with the configurable number of nodes and the CRT based packet forwarding can be implemented to send the packets. The original message is reconstructed in the base station where the sub packets are assembled. The path taken by each sub packet can be displayed using the simulator.

The non functional requirements includes the project includes usability, maintainability and scalability. The configurations of the project must be easy and the output obtained must be easy to visualize. The implementation of the project should be carried out without any faults. The project is classified into different modules so that the maintenance of the modules will be easier in order to reduce the number of faults. When modules are separated from each other they can be added or removed irrespective of functions of each other. Each modules should be maintained in such a way that a small alteration in a module should not implement any visual changes in the end result. The project which includes many numbers of nodes should be a scalable one in order to obtain a fault-free reliable system. The output of the system should be independent of number of nodes and it should not affect the performance of the system when there are considerably large numbers of nodes.

III. Design phase:w

The system is configured in such a way that packet splitting and reassembling is a part of the system. Packets are split and recombined using CRT (Chinese Remainder Theorem) Algorithm. Initially once the nodes are created the packet forwarding begins from source to base station. A method of wireless routing is involved in the delivery of packet ratio to the performance tool so that the work performed by each node is distributed among each other. Once the packets are split and sent to the base station the energy consumption by the system is reduced as the work is divided between the nodes. Once the message from all the nodes arrives at the base station it is reassembled and the original message is obtained.



To make the system reliable the algorithm is efficiently used. Reliability will also mean internal consistency of the system. Some of the reliable measures have to be taken like test-retest or stability, alternate form and internal consistency. Reliability can also be performed as a parallel form where the result from two systems working simultaneously on different administrative versions of an assessment tool can be correlated to evaluate the consistency of the results. Once the system is reliable it is required to know about the accuracy of its validation. In order to prove that the system is valid, the measures like, the extent to which the result of the test are productive or concurrent and the to extend which the system meets a instructional objectives once the content present in it has best matching to the test. The construction and the criterion also play a very important role in order to make the system reliable.

IV. CRT-Based forwarding technique

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). 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

$A \cong y1 \ (\text{mod } x1)$

$A \cong y2 \ (\text{mod } x2)$

…

$A \cong yk \ (\text{mod } xk)$

Moreover $p \cong x1Z1b1 + x2Z2b2 + \ldots + xkZkbk \ (\text{mod } Z)$

where $Zi = Z/xi$ and $Zibi = 1 \ (\text{mod } xi)$ for $i=1,2,\ldots,k$.

There are conditions where xi’s are not pairwise coprime. In such a case the simultaneous congruencies of p exists iff

$yi \cong yj \ (\text{ mod gcd}(xi,xj))$ for all i and j.

GCD Algorithm:

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

Begin algorithm

```
Function greatest common divisor (x, y)
  While value of x is not equal to y (x ≠ y)
  Then
  if 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
else return greatest common divisor (y, x mod y)
```

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. 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 $(d*e) \text{mod } z = 1$.

   Finally,

   Encryption: c=m^e mod n

   Decryption: c^d mod n

B. Energy Efficiency criterion

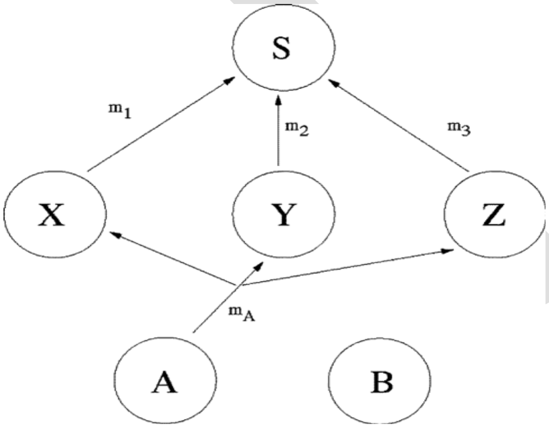
According to CRT algorithm, with the specified set of numbers that are provided, a number can be alternatively identified. To find the number i.e., a prime number which are randomly generated concepts of RSA algorithms are considered and used.

As a result of using such a concept where packets are split a reduction in the maximum energy consumption can be noticed and hence performance of the system consistently improved.

For instance, consider Figure, If A sends message to X, Y, and Z, each of them will transmit the message using procedure explained above, to the sink instead. Furthermore, the sink will reconstruct the message by using CRT algorithm again.

In general, if we consider that the maximum number of bits transmitted is proportional to the energy consumption, and assuming as the number of bits in the original message , and as the maximum number of bits of a CRT component, i.e., , we can consider a theoretical maximum energy reduction factor (MERF).

By considering this disjoint packet forwarding frame more than about 57% of the needed energy could be saved. In a real scenario, paths are not always distinct when forwarding the CRT components. MERF can be only obtained as a virtual result but in a real system both our proposed CRT-based forwarding algorithm and the actual number of bits forwarded by a traditional forwarding algorithm under the same conditions are tahen into consideration. In order to compare, the Shortest Path with Load Balancing is considered.



The Shortest Path approach is almost same as the probabilistic routing. The number of hops needed to reach the sink is minimized as a random choice of neighbors is made be sensor nodes having the packet. By avoiding overload of nodes the lifetime of a network is prolonged by this Random choice of re-layer which also means load balancing. In this paper we consider that the CRT based splitting of packets can be applied by considering that shortest path is composed by words of bits each. Here we also consider that for all words present in the same packet the same prime number which is randomly generated is used. As the splitting procedure produces the same number of bits for all the words in the generated packet there length is obtained by the prime number that is used to split it. In CRT when the packet are generated from different nodes then different lengthened packets may be generated.

Its known that the energy reduction factor and maximum energies are related to each other therefore In this paper we consider the maximum energy consumed by the system node is taken into account as the network lifetime is directly proportional to the time until first node is destroyed.

Obviously, the choice of set of primes should be proper order to maximize the above metrics.

C. Choosing Prime Numbers

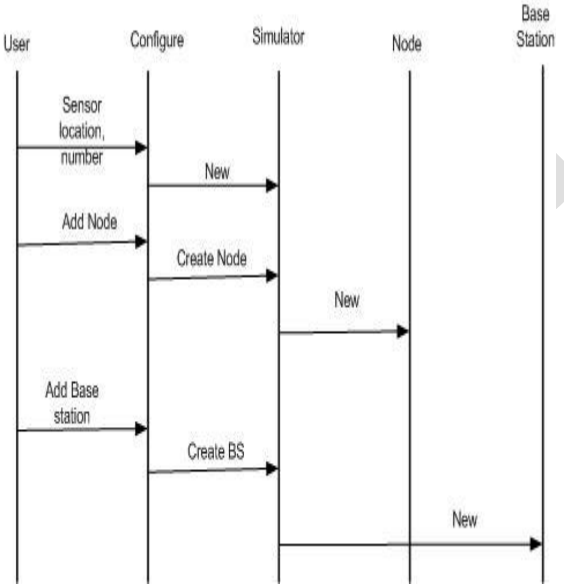
The number of bits needed is represented using the prime numbers. Prime numbers are selected as small as possible and primary numbers are chosen arbitrarily. The MERF may be maximized as the result of selecting small prime numbers. The set of smallest consecutive primes are used to indicate throughout the paper that satisfies the condition, the set is called as Minimum Primes Set (MPS). For example, if there is a 40-b word, the MPS will be formed by selecting four consecutive primes that satisfies the condition. The MERF in this condition will be 0.725. The sink receives all the CRT packets where the messages will be reconstructed into the original message. Consider another set of primes with smallest consecutive prime number such that even one of it is removed and the numbers still satisfies the condition. This kind of set is called as Minimum Primes Set with one acceptable failure and it is indicated as MPS-1. The Minimum Primes Set with one acceptable failure will be used to indicate throughout. The prime numbers are chosen consecutively due to the implementation issues in the system. When the second set of the primes are chosen the number of components in the previous set is same as the current set of primes and not changed. The same number of forwarders is needed in the second primes set. The value of the MERF is reduced by about 11% in the second set and the value obtained is 0.65. It is possible to reconstruct the original message even if one component has a failure. The conditions are satisfied by the rest of the components other than the one which has failure this follows the hypothesis of the CRT algorithm. It is also possible to obtain MPS even if the last component is not received using the first three primes the product is calculated and coefficients are computed for MPS. This can be extended to calculate if more number of failures is present in the set and how that condition could be satisfied. The tradeoff between the energy saving and reliability of the system is discussed in the following. The acceptable number of failures can be fixed and it is observed that the MPS obtained is unique. The sensor nodes usually have simple processing units and low complex procedure for obtaining the MPS. Lookup-tables (LUT) store the ordered list of prime numbers for each possible input value and return a pointer to the first prime number. The procedure is very fast and the memory requirements are low.

D. Phases of Algorithm

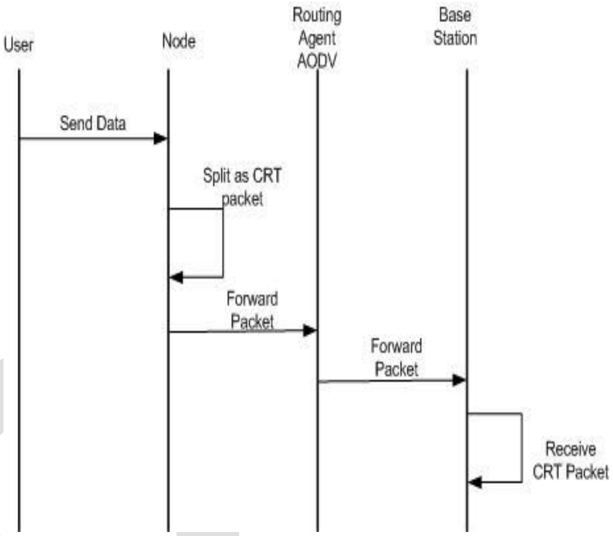
There are two phases in this algorithm which are temporal. The initialization phase and the forwarding phase.

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 neighbors, 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.



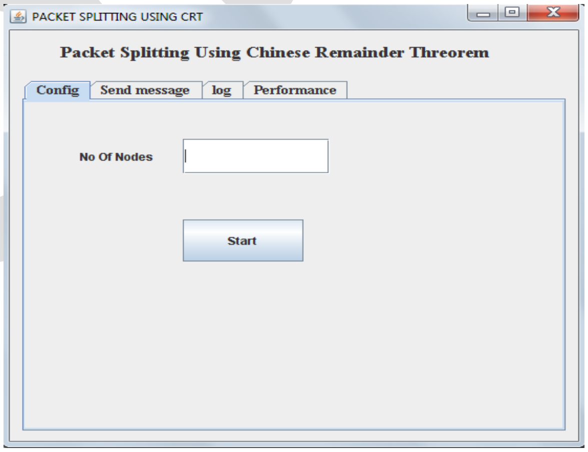
Packet Forward:



V. Implementation Using CRT And NON-CRT Based Algorithm:

RUN

Initially,

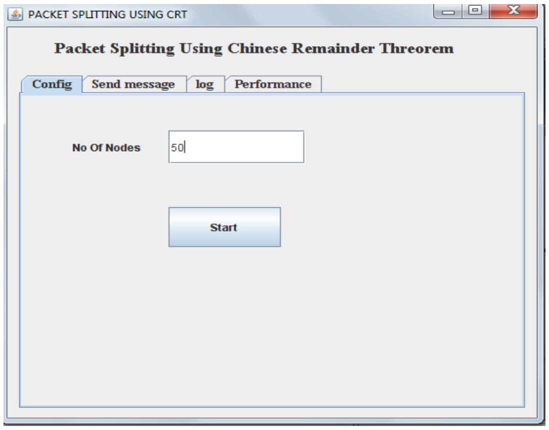


PACKET SPLITTING USING CRT

Packet Splitting Using Chinese Remainder Threorem

No Of Nodes

1. Enter the number of nodes:

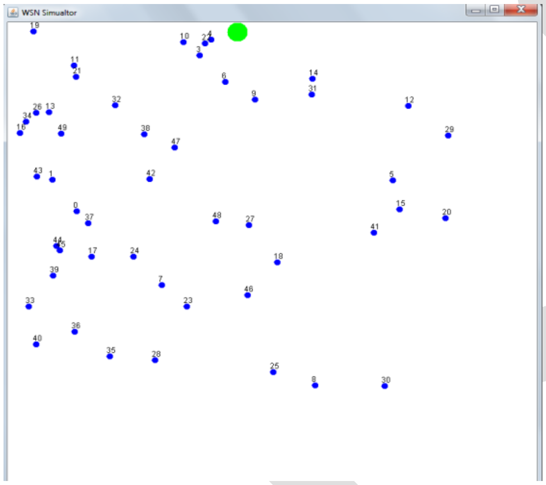


PACKET SPLITTING USING CRT

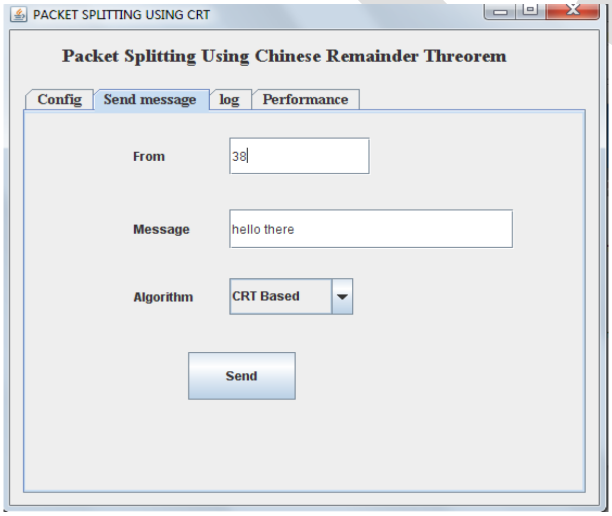
Packet Splitting Using Chinese Remainder Threorem

No Of Nodes: 50

2. Nodes generated



3. Message transmission:



PACKET SPLITTING USING CRT

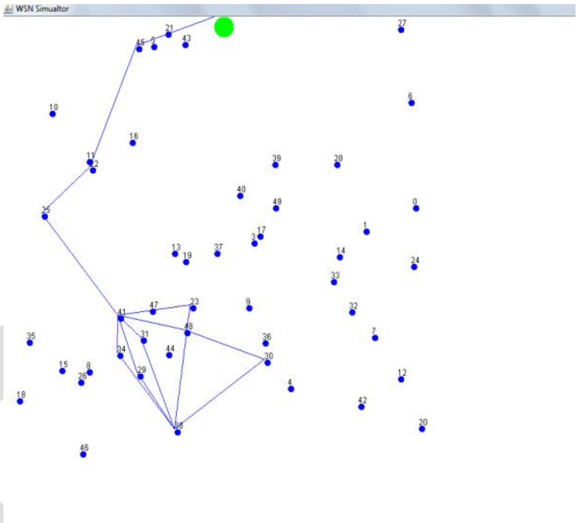
Packet Splitting Using Chinese Remainder Threorem

From: 38

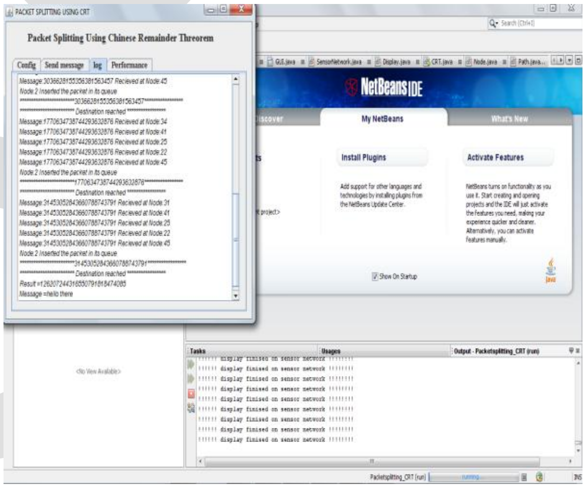
Message: hello there

Algorithm: CRT Based

4. Split data is sent to base station using CRT based Algorithm:



5. Log:



PACKET SPLITTING USING CRT

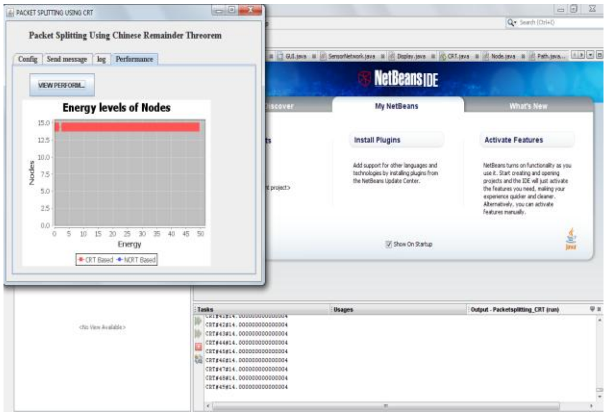
Packet Splitting Using Chinese Remainder Threorem

```
Message:3036628155356381563457 Recieved at Node:45
Node:2 Inserted the packet in its queue
************************3036628155356381563457*****************
************************ Destination reached *****************
Message:1770634738744293632876 Recieved at Node:34
Message:1770634738744293632876 Recieved at Node:41
Message:1770634738744293632876 Recieved at Node:25
Message:1770634738744293632876 Recieved at Node:22
Message:1770634738744293632876 Recieved at Node:45
Node:2 Inserted the packet in its queue
************************1770634738744293632876*****************
************************ Destination reached *****************
Message:31453052843660788743791 Recieved at Node:31
Message:31453052843660788743791 Recieved at Node:41
Message:31453052843660788743791 Recieved at Node:25
Message:31453052843660788743791 Recieved at Node:22
Message:31453052843660788743791 Recieved at Node:45
Node:2 Inserted the packet in its queue
************************31453052843660788743791*****************
************************ Destination reached *****************
Result =126207244316550791818474085
Message =hello there
```

NetBeans IDE
Discover
My NetBeans
What's New
Install Plugins
Add support for other languages and technologies by installing plugins from the NetBeans Update Center.
Activate Features
NetBeans turns on functionality as you use it. Start creating and opening projects and the IDE will just activate the features you need, making your experience quicker and cleaner. Alternatively, you can activate features manually.
Show On Startup
<No View Available>
Tasks
Usages
Output - Packetsplitting_CRT (run)
Packetsplitting_CRT (run)
running...

```
!!!!!! display finised on sensor network !!!!!!!
!!!!!! display finised on sensor network !!!!!!!
!!!!!! display finised on sensor network !!!!!!!
!!!!!! display finised on sensor network !!!!!!!
!!!!!! display finised on sensor network !!!!!!!
!!!!!! display finised on sensor network !!!!!!!
!!!!!! display finised on sensor network !!!!!!!
!!!!!! display finised on sensor network !!!!!!!
!!!!!! display finised on sensor network !!!!!!!
!!!!!! display finised on sensor network !!!!!!!
```

6. Performance graph for CRT based packet splitting:

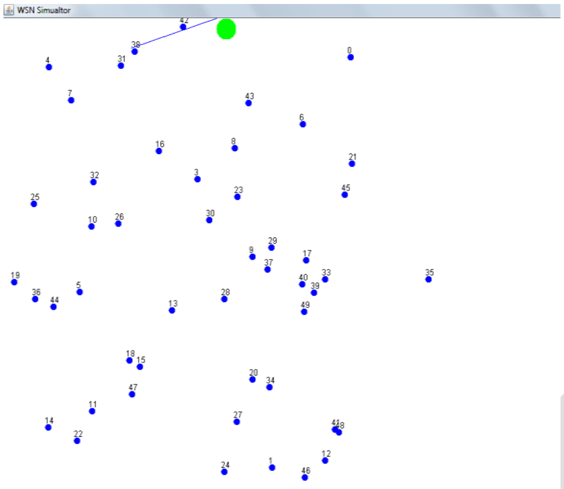


PACKET SPLITTING USING CRT

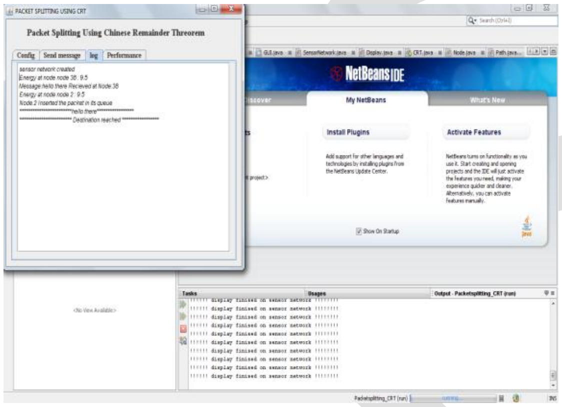
Packet Splitting Using Chinese Remainder Threorem

```
CRT#42#14.000000000000004
CRT#43#14.000000000000004
CRT#44#14.000000000000004
CRT#45#14.000000000000004
CRT#46#14.000000000000004
CRT#47#14.000000000000004
CRT#48#14.000000000000004
CRT#49#14.000000000000004
```

7. Data is sent to base station using Non-CRT based algorithm:



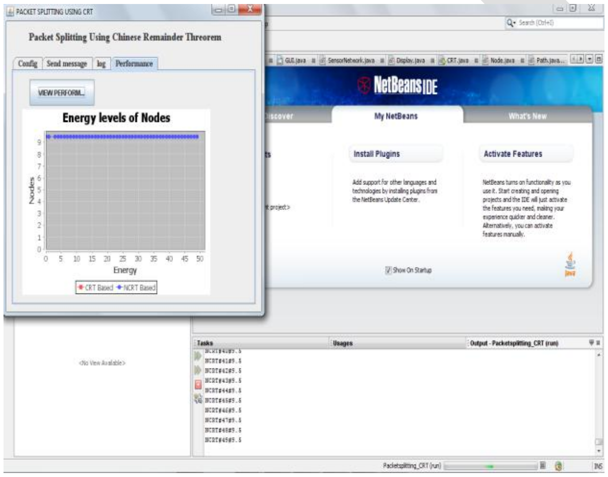
8. Log:



```
sensor network created
Energy at node node 38 : 9.5
Message:hello there Recieved at Node:38
Energy at node node 2 : 9.5
Node.2 inserted the packet in its queue
***********************hello there*****************
*********************** Destination reached *****************
```

```
!!!!!! display finised on sensor network !!!!!!!!
!!!!!! display finised on sensor network !!!!!!!!
!!!!!! display finised on sensor network !!!!!!!!
!!!!!! display finised on sensor network !!!!!!!!
!!!!!! display finised on sensor network !!!!!!!!
!!!!!! display finised on sensor network !!!!!!!!
!!!!!! display finised on sensor network !!!!!!!!
!!!!!! display finised on sensor network !!!!!!!!
!!!!!! display finised on sensor network !!!!!!!!
!!!!!! display finised on sensor network !!!!!!!!
```

9. Performance graph for Non-CRT based packet transmission:

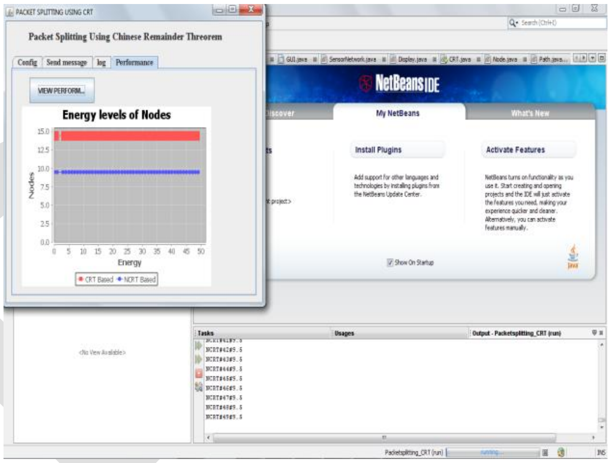


```
NCRT#40#9.5
NCRT#41#9.5
NCRT#42#9.5
NCRT#43#9.5
NCRT#44#9.5
NCRT#45#9.5
NCRT#46#9.5
NCRT#47#9.5
NCRT#48#9.5
NCRT#49#9.5
```

VI. Result (OUTPUT):

"The CRT Algorithm is used to prove through simulation that there Is further reduction in energy consumption with minimum delay making the system more reliable"

Comparison of both Performance graph:



```
NCRT#41#9.5
NCRT#42#9.5
NCRT#43#9.5
NCRT#44#9.5
NCRT#45#9.5
NCRT#46#9.5
NCRT#47#9.5
NCRT#48#9.5
NCRT#49#9.5
```

VII. Conclusion:

In this paper, we have provided with a novel forwarding technique based on the Chinese Remainder Theorem (CRT) in WSN's. In particular, 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 tradeoffs 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.

References:

[1]Improving Energy Saving and Reliability in Wireless Sensor Networks Using a Simple CRT-Based Packet-Forwarding SolutionGiuseppe Campobello, Alessandro Leonardi, and Sergio Palazzo, Senior Member, IEEE

[2] A CRT-RSA algorithm secure against hardware fault attacks
Sining Liu, Brian King, Member, IEEE, and Wei Wang, Member, IEEE.

[3] 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

[4] Design and Implementation of an Improved RSA Algorithm

Yunfei Li School of Information Science and Engineering Yunnan University Kunming, China, Qing Liu, Tong Li National Pilot School of Software Yunnan University Kunming, China

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

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

[7] Fault Attacks and Countermeasures on Vigilant’s RSA-CRT Algorithm Jean-S´ebastien Coron_, Christophe Giraudy, Nicolas Moriny, Gilles Piretz and David.

[8] A CRT-RSA algorithm secure against hardware fault attacks Sining Liu, Brian King, Member, IEEE, and Wei Wang, Member, IEEE.

[9] The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip_ Johann Großsch¨adl.

[10] 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.

[11] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, “How to prolong the lifetime of wireless sensor network,” in Handbook of Mobile Ad Hoc and Pervasive Communications. Valencia, CA: American Scientific Publishers, 2007.

[12] G. Campobello, A. Leonardi, and S. Palazzo, “On the use of Chinese Remainder Theorem for energy saving in wireless sensor networks,” in Proc. IEEE ICC, Beijing, China, May 2008

[13] R. Crepaldi, A. F. Harris, III, M. Rossi, G. Zanca, andM.Zorzi, “Fountain reprogramming protocol: A reliable data dissemination scheme for wireless sensor networks using fountain codes, demo abstract,” in Proc. ACM SenSys, Sydney, Australia, Nov. 2007, pp. 389–390.