Crt Based Rsa Algorithm For Improving Reliability And Energy Efficiency With Kalman Filter In Wireless Sensor Networks

B.Arutselvan*, R.Maheswari**

*PG Scholar, **Assistant Professor-ECE Department

Loyola Institute of Technology, Chennai-600 123, Tamilnadu, India.

***Abstract*— Broadcast authentication is a critical security service in wireless sensor networks (WSNs). However, due to resource constrained of sensor nodes, providing an authentication mechanism for broadcast message is difficult. This paper deals with the forwarding scheme for wireless sensor networks aimed at combining low computational complexity and high performance in terms of energy efficiency with RSA Cryptosystem. The proposed approach relies on a packet-splitting algorithm based on the Chinese Remainder Theorem (CRT) and is characterized by a simple modular division between integers and a Kalman filter is used to reduce the noise and find the shortest path to reach the receiving end. RSA uses the Chinese Remainder Theorem to associate the authenticating procedure of the authentication key and the Message Authentication Code of broadcast messages together. The reliability in the network and use it to allocate network resources to minimize energy while the reliability of the network is guaranteed. The Simulation is done through MATLAB which provides the data authentication using RSA cryptosystem and shows that the proposed algorithm outperforms traditional approaches in terms of energy saving with practical issues such as the effect of unreliable channels and topology changes, reliability, simplicity and fair distribution of energy consumption among all nodes in the network and finds the shortest path and also reduces the noise in the receiver end.**

***Keywords*— RSA Algorithm, Chinese Remainder Theorem (CRT), Packet splitting, Energy Efficiency, Kalman filter.**

I. INTRODUCTION

Wireless sensor networks (WSNs) usually consist of a large number of tiny sensor nodes and several base stations. Broadcast authentication is an essential security service in wireless sensor networks, because it is usually desirable for base station to broadcast commands and data to sensor nodes. The authenticity of such commands and data is critical for the normal operation of sensor nodes. If convinced to accept forge or modified commands or data, sensor nodes may perform unnecessary or incorrect operation and can't fulfill the intended purposes of the network. Thus, in a hostile environment, it is necessary to enable sensor nodes to authenticate broadcast messages received from the base station. However, due to the resource constraints on sensor nodes, traditional broadcast authentication techniques such as public key based digital signatures are not desirable. Symmetric schemes and hash functions have lower computational requirements and are more widely used in sensor networks.

Moreover, usually the power supply unit is based on an energy-limited battery; therefore solutions elaborated for these networks should be aimed at minimizing the energy consumption. For this purpose, several works have shown that energy consumption is mainly due to data transmission, and accordingly energy conservation schemes have been proposed aimed at minimizing the energy consumption of the radio interface. 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 subpackets. The splitting procedure is achieved applying the Chinese Remainder Theorem (CRT) algorithm, which is characterized by a simple modular division between integers. The sink node, once all subpackets (called CRT components) is received correctly, will recombine them, thus reconstructing the original message. The splitting procedure is especially helpful for those forwarding nodes that are more solicited than others due to their position inside the network.

In this paper, we develop an efficient scheme for broadcast authentication in wireless sensor networks, which allows sensor nodes to authenticate broadcast messages from the base station immediately. The main contribution of this paper uses the Chinese Remainder Theorem in broadcast authentication in wireless sensor networks. Although there are many applications of the Chinese Remainder Theorem in cryptography, best of our knowledge this work is the first apply design theory to broadcast authentication in wireless sensor networks. A comprehensive framework in which we provide a thorough analytical model that allows us to derive some accurate results regarding energy consumption and reliability by using packet forwarding technique CRT and Kalman filter for tracing the shortest path of nodes and to precise the noise of each node.

II. RSA CRYPTOSYSTEM

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large numbers, the factoring problem. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors are kept secret.

A. *Key Generation*

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
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 φ (n) = φ (p) φ (q) = (p − 1) (q − 1), where φ is Euler's totient function.
4. Choose an integer e such that 1 < e < φ (n) and gcd (e, φ (n)) = 1; i.e., e and φ (n) are coprime.
   - e is released as the public key exponent.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller value of e (such as 3) have been shown to be less secure in some settings. [4]
5. Determine d as $d^{-1} \equiv e$ (mod φ (n)), i.e., d is the multiplicative inverse of e (modulo φ (n)).
   - This is more clearly stated as solve for d given de ≡ 1 (mod φ (n))
   - This is often computed using the extended Euclidean algorithm.
   - d is kept as the private key exponent.

By construction, d·e ≡ 1 (mod φ (n)). The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ (n) must also be kept secret because they can be used to calculate d.

III. CHINESE REMAINDER THEOREM

The Chinese remainder theorem is a result about conruence's in number theory and its generalizations in abstract algebra. In its basic form, the Chinese remainder theorem will determine a number *n* that when divided by some given divisors leave given remainders.

Suppose n_1, n_2, …, n_k are positive integers which are pairwise co-prime. Then, for any given sequence of integers a_1, a_2, …, *ak*, there exists an integer *x* solving the following system of simultaneous congruence's.

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Furthermore, all solutions' *x* of this system is congruent modulo the product, $N = n_1 n_2 \ldots n_k$.

Hence $x \equiv y \pmod{n_i}$ for all $1 \le i \le k$, if and only if $x \equiv y \pmod{N}$.

Sometimes, the simultaneous congruences can be solved even if the n_i's are not pairwise coprime. A solution *x* exists if and only if:

$$a_i \equiv a_j \pmod{\gcd(n_i, n_j)} \qquad \text{for all } i \text{ and } j.$$

All solutions' *x* are then congruent modulo the least common multiple of the n_i. We can construct a solution as follows:

1. Let m = m1m2 · · ·mn.
2. Let $M_k = m/m_k$, for all k = 1, 2, . . . , n.
3. For all k = 1, 2, . . . , n, find integers y_k such $M_k y_k \equiv 1 \pmod{m_k}$.

Since gcd $(M_k, m_k) = 1$, we know that y_k exists. The extended Euclidean algorithm can be used to find y_k.

4. The integer $a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n$ is a solution of the system.

The integer $x = (a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n) \bmod m$ is the unique solution with $0 \le x < m$.

IV. ENERGY EFFICIENCY

A sensor network is a static ad hoc network consisting of hundreds of sensor nodes deployed on the fly for unattended operation. Each sensor node is equipped with a sensing device, a low computational capacity processor, a short-range wireless transmitter-receiver and a limited battery-supplied energy. Sensor nodes monitor some surrounding environmental phenomenon, process the data obtained and forward this data towards a base station located on the periphery of the sensor network. Base station(s) collect the data from the sensor nodes and transmit this data to some remote control station.

A. *Energy Reduction Factor*

Consider, the Shortest Path with Load Balancing (SP), which is very similar to the probabilistic routing. A sensor node having a packet to forward, randomly chooses a neighbor node as next-hop so that the number of hops needed to reach the sink is minimized. Load balancing (i.e., a random choice of the next hop) allows to prolong the network lifetime avoiding that some nodes can be overloaded.

An SP packet is composed of *K* words of *w*-bits each and that the CRT based splitting procedure can be applied to each word by considering that the same prime number is used for all the words of the same packet. As already described in [1], 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, that is, $E_{CRT} = n_c w_{\mathrm{CRT}} * \varepsilon_b$ and $E_{\mathrm{SP}} = n_p w * \varepsilon_b$, respectively, where, n_c and n_p are the mean number of forwarded packets with the above forwarding schemes, w_{CRT} is the mean number of bits needed to represent the CRT components, and ε_b is the energy needed to transmit a bit. More precisely, the expected energy reduction factor can be defined as follows:

$$\mathrm{ERF} = \frac{E_{\mathrm{SP}} - E_{\mathrm{CRT}}}{E_{\mathrm{SP}}} = 1 - \frac{n_c w_{\mathrm{CRT}}}{n_p w} \qquad (1)$$

It is worth noting that we are considering the average value of the components, w_{CRT} , because in the case of CRT, a node transmits packets that can have components of different length due to the fact that the packets may be generated by different nodes. However, if a large number of packets are considered, the expected total number of bits is $\sum_{i=1}^{n_c} K w_i \approx n_c K \bar{w}_{\mathrm{CRT}}$.

In several papers about WSNs, the network lifetime is related to the time until the death of the first node [2]. In this case, the maximum energy consumed by a node should be also considered. Therefore, in this paper we also investigate the energy reduction factor related to the maximum energies

$$\mathrm{ERF}_{\mathrm{max}} = \frac{\mathrm{E}_{\mathrm{SPmax}} - \mathrm{E}_{\mathrm{CRTmax}}}{\mathrm{E}_{\mathrm{SPmax}}} = 1 - \frac{\mathrm{n}_{\mathrm{cmax}}\bar{\mathrm{w}}_{\mathrm{CRT}}}{\mathrm{n}_{\mathrm{pmax}}\mathrm{w}} \qquad (2)$$

V. RELIABILITY

Basically, the reliability of a WSN can be defined as the probability *PR* that the sink is able to reconstruct the message. In this section, we introduce an analytical framework which allows to relate *PR* to the probability of erasure for a single hop, *pe*. Moreover, we investigate the relation between *PR* and a possible duty-cycle mismatch. These relationships allow us to obtain the value of *f* (the number of admissible failures) to achieve a target *PR*.

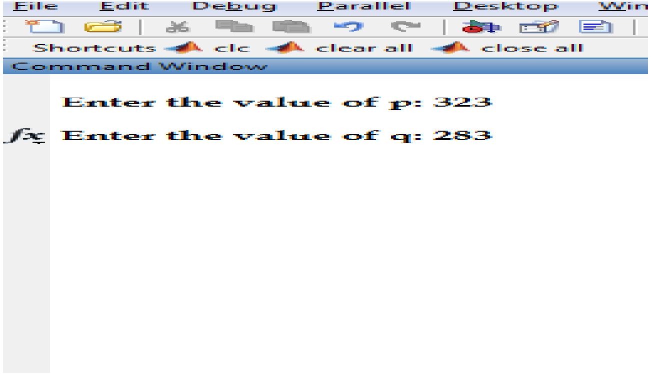
It is worth noting that the possibility to obtain different trade-offs between energy saving and reliability by choosing different values of *f* is one of the main advantages of using the CRT as splitting technique, and that this is not possible with other simple splitting techniques (e.g., simple chunk). Furthermore, considering the limited energy and computation capability of sensor nodes, the very low complexity of the CRT allows it to be more suitable to achieve reliability in WSN's in comparison to other techniques (e.g.,FEC techniques based on RS and LT codes) commonly used for other types of wireless networks.

VI. RESULTS AND DISCUSSION

The authentication is provided for broadcasting the messages through the sensor nodes for safer transmission by tracing the shortest path between the transmitter and receiver. While transmitting the messages through nodes, the energy efficiency of overall node is given to the transmitting node for faster transmission and the energy is saved by changing the inactive nodes to sleep mode. The overheads and Topology changes are analyzed and the simulated results are obtained as follows:

A. RSA Cryptosystem

RSA is an algorithm for public-key cryptography, that is based on the presumed difficulty of factoring large numbers, the factoring problem (as discussed in section-II). The Key has to be generated with the help of two prime numbers for security purposes. The two prime numbers are represented as p and q. This p and q values must be chosen randomly and should be of similar bit-length. The p and q values are entered as shown in fig-2.



```
Enter the value of p: 323
Enter the value of q: 283
```

Fig-2 choosing the p and q value for key generation.

After choosing the p and q values, the results for the following steps are obtained. The transmitter encrypts the data with the public key and transmits the data as shown in Fig-3.

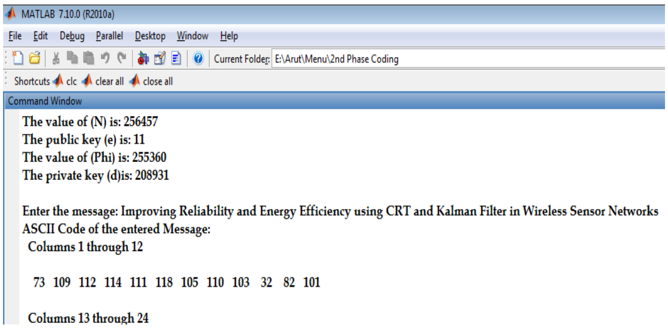
Step-1: Compute N=pq. N is the modulus for both the private and public keys.

Step-2: Compute φ (n) = φ (p) φ (q) = (p − 1) (q − 1), where φ is Euler's totient function.

Step-3: Choose an integer e such that 1 < e < φ (n) and gcd (e, φ (n)) = 1; i.e., e and φ (n) are coprime.

Where, e is an encrypted message.

Step-4: Determine d as $d^{-1} \equiv$ e (mod φ (n)), i.e., d is the multiplicative inverse of e (modulo φ (n)).



```
The value of (N) is: 256457
The public key (e) is: 11
The value of (Phi) is: 255360
The private key (d)is: 208931

Enter the message: Improving Reliability and Energy Efficiency using CRT and Kalman Filter in Wireless Sensor Networks
ASCII Code of the entered Message:
 Columns 1 through 12


  73  109  112  114  111  118  105  110  103   32   82  101


 Columns 13 through 24
```

Fig-3 Public Key and Private Key are obtained with p and q.

B. Input Data Transmission

After obtaining the public and private keys, the transmitter will type a message to be transmitted. Depending upon the length of the message to be transmitted, the input data are plotted against Packet size and Transmission per bit, as shown in Fig-4.

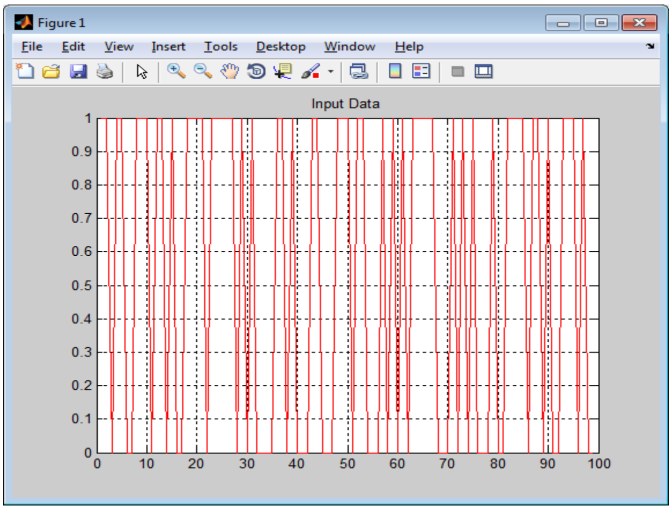


Fig-4 Input Data Transmission

The total size of the input data is segmented and modulated with the QAM-64 modulation technique and the data are processed as shown in the Fig-5 & 6.

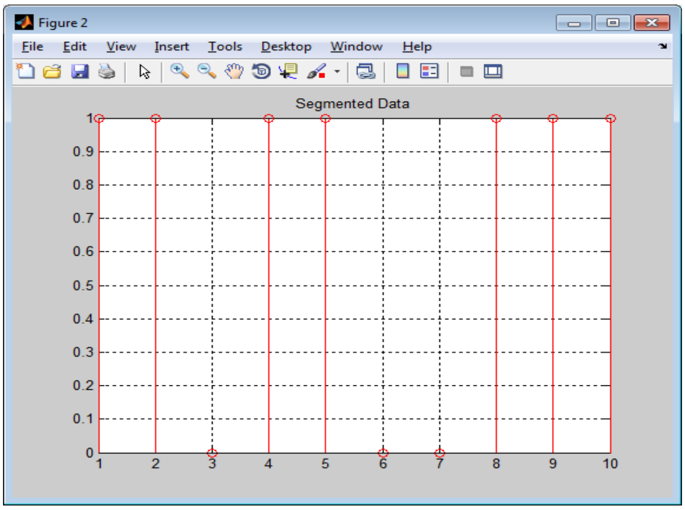


Fig-5 Segmented Data Process

The modulated input data are then splitted into sub-packets with the CRT process and each splitted sub-packets are transmitted through different nodes in a wireless network. The error rate during the transmission of packets are plotted at different nodes in Fig-7.

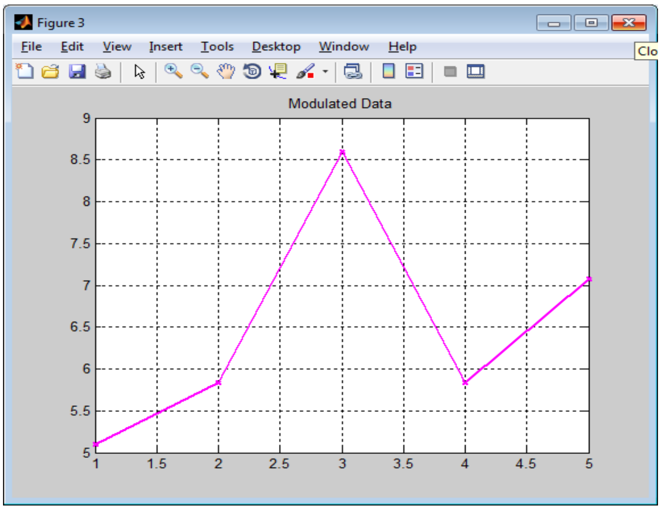


Fig-6 Modulated Data Process

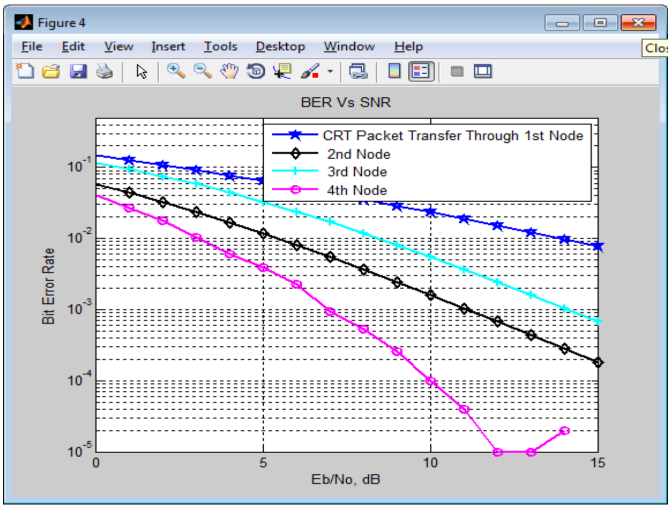
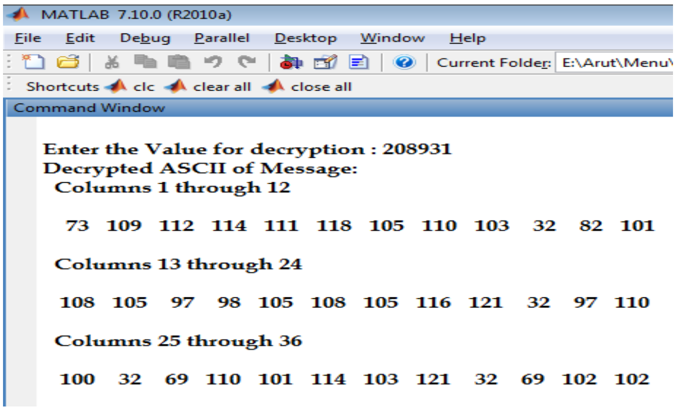


Fig-7 CRT subpacket transmission through different nodes

The splitted sub-packets are retrieved at the receiving end and the data has to be decrypted with the transmitter's private key. If the private key is not authenticated one, then the data process will be stopped at the receiver side. So, the receiver needs to provide the key to decrypt the data as shown in Fig-8.


MATLAB 7.10.0 (R2010a)
File Edit Debug Parallel Desktop Window Help
Current Folder: E:\Arut\Menu\
Shortcuts clc clear all close all
Command Window

```
Enter the Value for decryption : 208931
Decrypted ASCII of Message:
 Columns 1 through 12

  73  109  112  114  111  118  105  110  103   32   82  101

 Columns 13 through 24

 108  105   97   98  105  108  105  116  121   32   97  110

 Columns 25 through 36

 100   32   69  110  101  114  103  121   32   69  102  102
```

Fig-8 Obtaining Private key for decryption

By entering the private key, the data are decrypted and the error rate in receiving the packets is plotted at different nodes as shown in Fig-9.

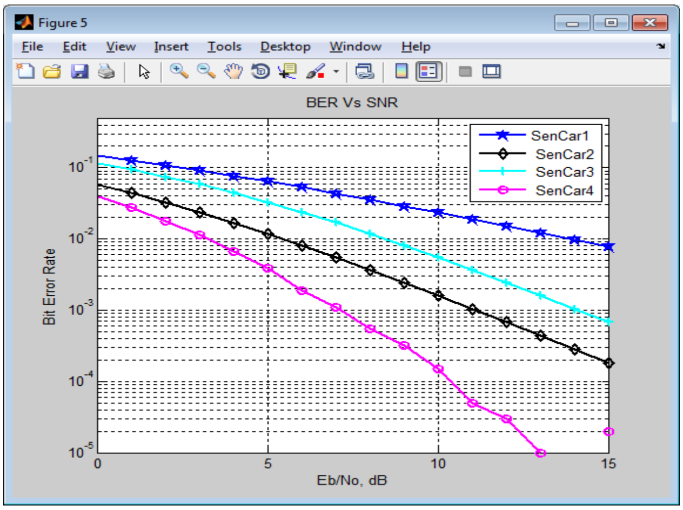


Fig-9 Retrieving sub-packets through different nodes

C. *Comparison Results*

The flow of data in the normal transmission with the throughput is shown in Fig-10. The position of each node is far away through which the data are delayed and the energy provided for each node is wasted.

By normal transmission, the node energies are wasted in transmission. In order, to reduce the energy for transmission, the shortest path between each node are to be traced with the help of Kalman filter. The data sent through different nodes after CRT and Kalman filter process is traced as shown in Fig-11. In this, the nodes are placed nearby after the Kalman filtering process, the path is made smoothened when compared to the Fig-10

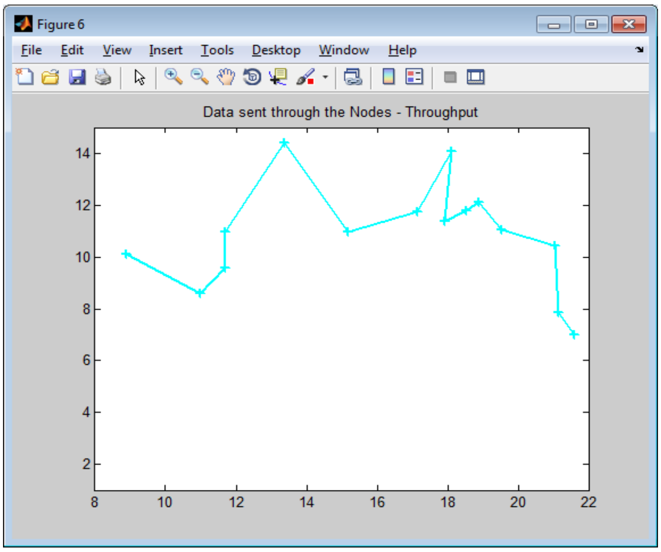


Fig-10 Data sent with a throughput at different nodes.

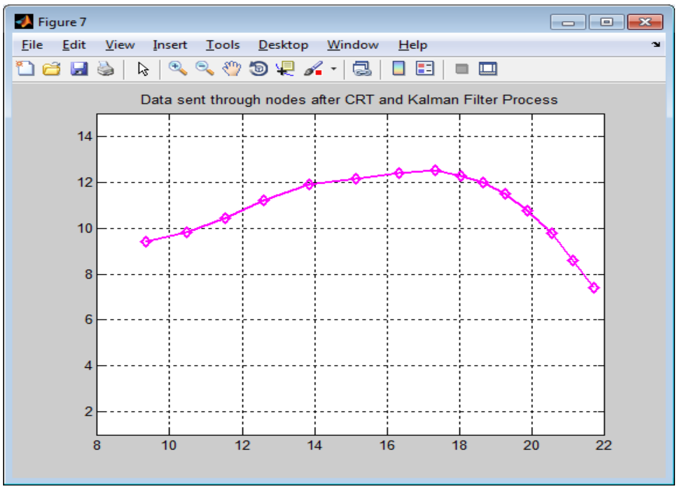


Fig-11 Energy Efficient by tracing a shortest path

The accuracy of the proposed model comparing the analytical results on reliability obtained through simulation as shown in Fig-13.

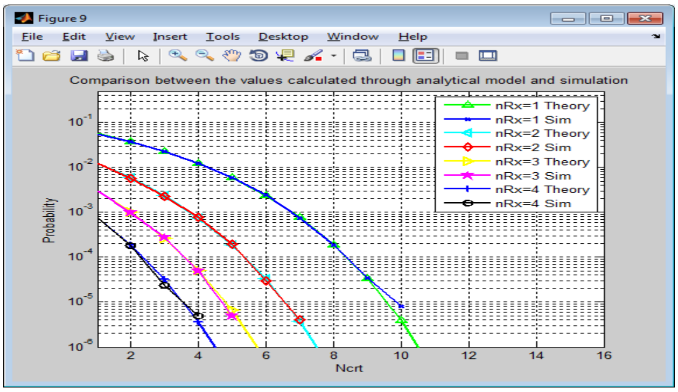


Fig-13 Comparison of Anaytical and Simulation model

In the proposed system, both the unicast and multicast systems are combined together and the blocking probability of the system is calculated by the service request rate. The comparison of the proposed system is made with the other systems ans shown in Fig-14.

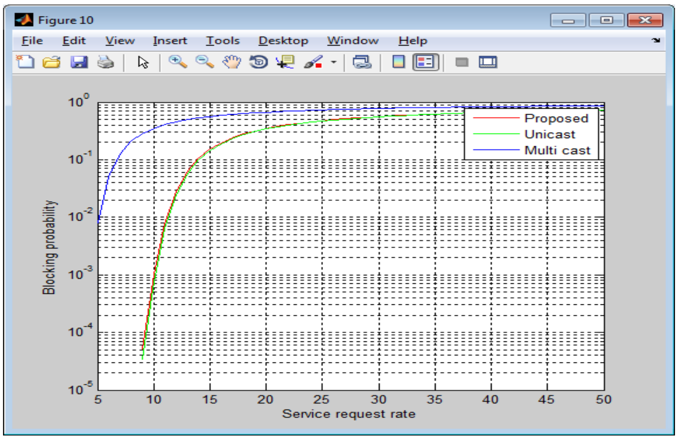


Fig-14 Comparison of different systems

The position of nodes through which the data are passed through is traced by using the interactive gaming concept as shown in Fig-15. This concept is used to trace the movement of each node in the wireless network.

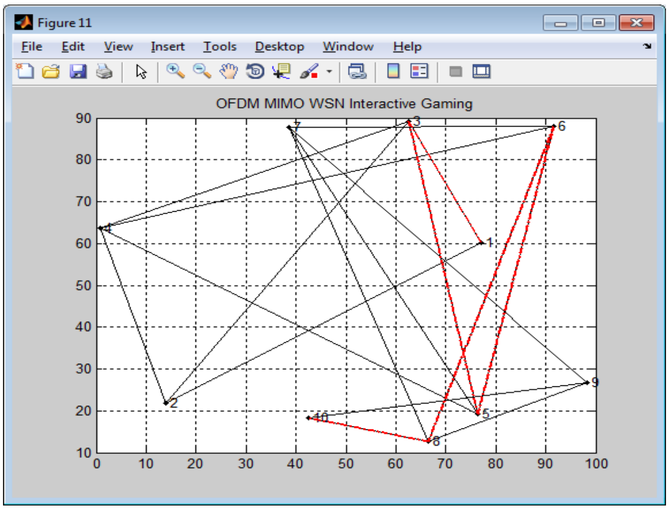


Figure 11
File Edit View Insert Tools Desktop Window Help
OFDM MIMO WSN Interactive Gaming
90
80
70
60
50
40
30
20
10
0
10
20
30
40
50
60
70
80
90
100
1
2
3
4
5
6
7
8
9
10

Fig-15 Node path traced using Interactive Gaming

After each process of transmitting data from one node to another the existing node moves to a new location. The movement of each node before and after is traced and shown in Fig-16. The node location changes for every execution.

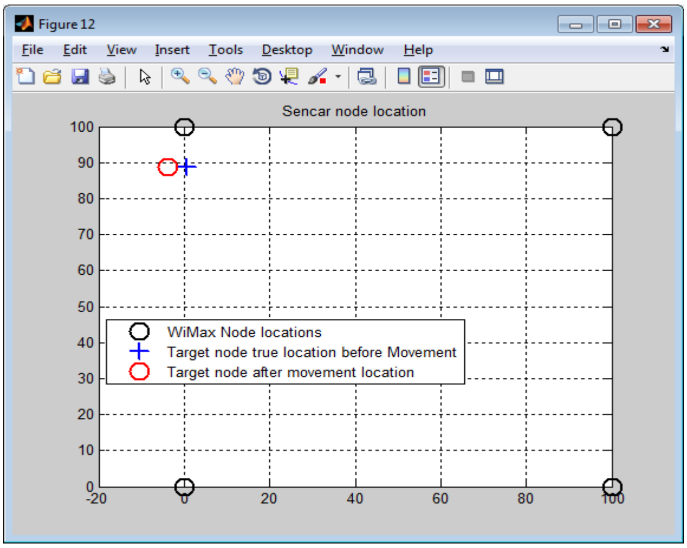


Figure 12
File Edit View Insert Tools Desktop Window Help
Sencar node location
100
90
80
70
60
50
40
30
20
10
0
-20
0
20
40
60
80
100
WiMax Node locations
Target node true location before Movement
Target node after movement location

Fig-16 Node movements traced using sencar

VII. CONCLUSIONS

In this Paper, we proposed an efficient broadcast authentication scheme for wireless sensor networks. We analyzed the security of two provably secure RSA-CRT algorithms and also proposed an energy efficient usage to increase the lifetime of wireless sensor networks. Using a rigorous approach to optimize energy utilization leads to significant increase in network lifetime. The analysis shows that the system has low overhead in computation, communication and storage, immune to DoS attack.

Simulation results using MATLAB, have confirmed the results obtained analytically and have shown that applying the CRT-based technique significantly reduces the energy consumed for each node.

REFERENCES

[1]. Arutselvan.B and Maheswari.R (2013), "Improving reliability and energy efficiency using packet splitting based on the CRT forwarding technique and Kalman filter in wireless sensor networks", ICICES, 2013 International conference, Pg. 701-705.

[2]. Giuseppe Campobello, Alessandro Leonardi, and Sergio Palazzo (2012), "*Improving Energy Saving and Reliability in Wireless Sensor Networks Using a Simple CRT-Based Packet-Forwarding Solution*", IEEE/ACM transactions on networking, vol. 20, no. 1, pp. 191-205, February.

[3]. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci (2002), "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, August.

[4]. P. Djukic and S. Valaee (2004), "Minimum energy reliable ad hoc networks," in *Proc. 22nd Bienni. Symp. Commun.*, Kingston, ON, Canada, June, pp. 150–152.

[5]. Campobello, A. Leonardi, and S. Palazzo (2008), "On the use of Chinese Remainder Theorem for energy saving in wireless sensor networks," in *Proc. IEEE ICC*, Beijing, China, May, pp. 2723–2727.

[6]. Anastasi, M. Conti, M. Di Francesco, A. Passarella (2007), "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.

[7]. Campobello, A. Leonardi, and S. Palazzo (2009), "A novel reliable and energy-saving forwarding technique for wireless sensor networks," in *Proc. ACM MobiHoc*, New Orleans, LA, May 18–21, pp. 269–278.

[8]. Fasolo, M. Rossi, J. Widmer, and M. Zorzi, (2007), "In-network aggregation techniques for wireless sensor networks: A survey," *IEEEWireless Commun.*, vol. 14, no. 2, pp. 70–87, April.

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