**I J C T A**, 9(28) 2016, pp. 289-300


# SURVEY ON HYBRID CRYPTOGRAPHY ALGORITHMS IN WSN USING ZIGBEE

**S. Aruna* D. Anitha** Promit Roy*** and Riddhi Datta******

***Abstract :*** In today's world, network security is the bottleneck of communicating important and vulnerable data across the internet. The more the networking facilities are being upgraded, the more the data are vulnerable to outside exposure as hackers try their best to retrieve and modify important information which may prove to be fatal to any individual, organization or the nation. This is where the concept of cryptography comes into use. Symmetric and Asymmetric cryptography were indeed helpful in providing network security. Hybrid cryptography came later, which enhanced the security level while reducing the disadvantages of the symmetric as well as asymmetric cryptography. In this paper we have given the survey of various security protocols for hybrid cryptography algorithms in WSN's.

## 1. INTRODUCTION

Security and cryptography are very vital part of computer networks. This also can means that for any computer network assurance of secure data transfer is as important as transmission of the data itself. The attributes of cryptographic algorithms to secure any kinds of networks are Authentication, Confidentiality, Integrity and Non-repudiation.

- **Authentication**: Assurance of identity of a person or originator of data.
- **Confidentiality:** safeguard from revelation to illicit persons.
- **Integrity:** Confirms the receiver that the received data is not altered in transit by an opponent.
- **Non-repudiation:** non-repudiation refers to the ability to ensure that a person to a contract or a message cannot decline the realism on a document or the sending of a message that they originated.

The basic kinds of cryptographic algorithms are symmetric, asymmetric and hybrid cryptography algorithms. An encryption scheme is a procedure in which the sender and recipient of a message share a common key that is used to encrypt and decrypt the text. Benefit of symmetric encryption scheme are: faster, cipher text can be transferred on the communication channel is secure , no key is transferred with the cipher text hence the conversion between cipher text and plain text by the hackers is less, secret key to decrypt the plain text .Limitations of symmetric cryptographic algorithms are: not secure while transmitting the secret key between the sender and the receiver, The shared secret key is to be transferred to the receiver prior to the cipher is to be transmitted, all way of electronic contact is timid as it is not possible to assurance that no one will be capable to faucet communication channel. [3]

* **Email:** aruna809@gmail.com
** **Email:** avrlaksha@gmail.com
*** Student, **Email:** royp04330@gmail.com@gmail.com
**** Student, **Email:** toriddhi.datta@gmail.com

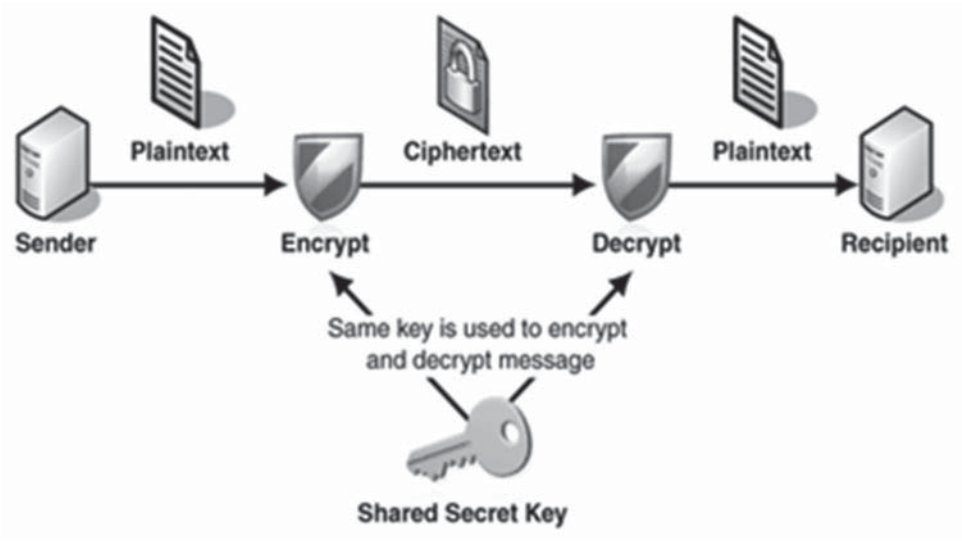


**Fig 1. Block Diagram of Symmetric Key Encryption**

Figure 1 depicts the diagrammatic representation of symmetric key encryption [20]. Asymmetric encryption technique makes use of two keys: a public key and a private key. One key in the pair can be shared with everyone and it is called the public key.. The private key is kept secret and is used to decrypt received messages. In asymmetric encryption there is no need for exchanging keys, and thus it eliminates the key distribution problem. The main benefit of public-key cryptography is increased security: the private keys do not ever need to be transmitted or revealed to anyone. It provides digital signatures that can be repudiated. A problem of using public-key cryptography for encryption is speed since there are popular secret-key encryption methods which are considerably faster than other available public-key encryption method.[3]Hybrid encryption scheme is a method of encryption that merge both symmetric and asymmetric encryption schemes to increase the influence of both type of encryption.

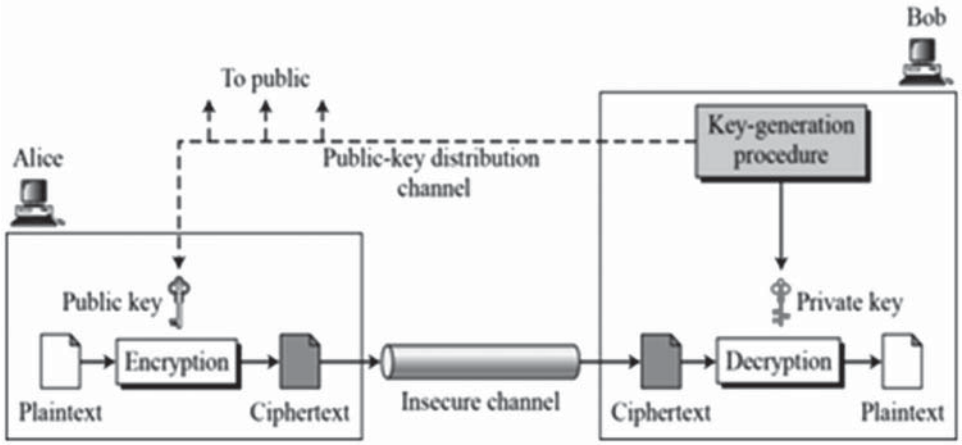


**Figure 2. Block diagram of asymmetric key encryption**

Figure 2 depicts the diagrammatic representation of asymmetric key encryption. [22] Hybrid cryptography is a set of rules using several ciphers of different types together, each to its best advantage. Hybrid cryptography try to take advantages of both types of algorithm module, while evading their weakness.[3] Main focus of this paper is in securing the data so, we go through a existing hybrid cryptography algorithms in which we find that the most reliable way to secure the data is by implementing a simple system which includes the properties of network security as well size of cipher text, time of encryption process, time of decryption process ,throughput, measuring energy consumption in WSN's.

## 2 STATE-OF-THE-ART SURVEY:

### 2.1 Hybrid security protocol Architecture I (Subasree)

The Plain text is encrypted with the Elliptic Curve cryptography and concurrently hash value is determined using MD5 for the plain text, to make secure the hash value is encrypted with the DUAL RSA since RSA can be broken down by taking factors of N. DUAL RSA is added secure than RSA. It is complex to derive the plain text from the cipher text as the hash value of plain text is encrypted with the Dual RSA and elliptic curve cryptography is used to encrypt the plain text. Two drawbacks are there in this security protocol. The first, two symmetric encryption algorithms is used which becomes more time-consuming. Asymmetric algorithms require less time. The second, if private key is known the entire message can be read.

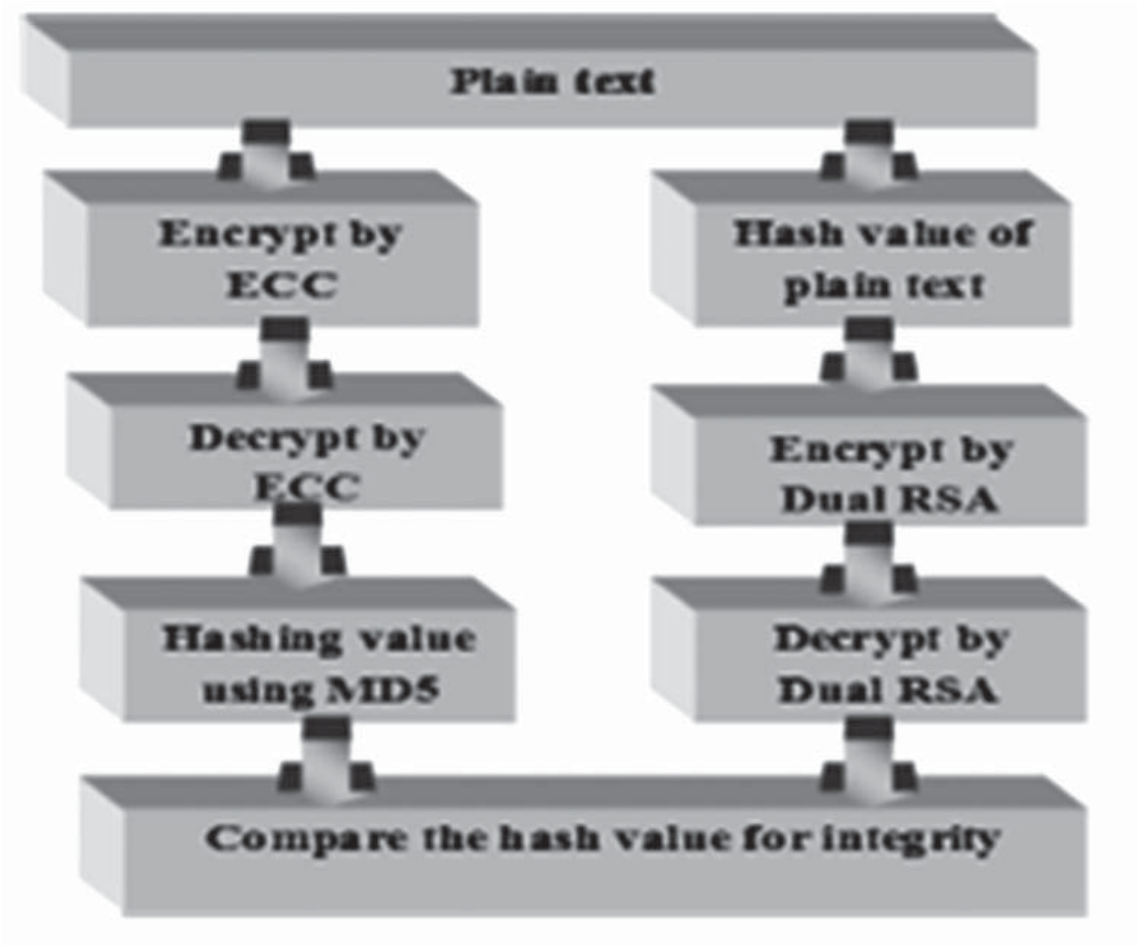


**Figure 3. Subasree security protocol architecture [10]**

### 2.2 Hybrid security protocol Architecture II (Dubal):

In Dubal's Security protocol architecture the plain text is encrypted with the Dual RSA and the keys used for encryption is derived from Elliptic Curve Diffie Hellman (ECDH), for authentication signature generated by the Elliptic Curve Digital Signature Algorithm(ECDSA) is add on with the cipher text. Simultaneously the hash value of MD5 for cipher text and the digital signature is sent to the receiver through secure channel. At decryption side the hash value is derived using MD5 from the received cipher text and it is compared with the received hash value. If there is no change in both the hash values, there is no modification in the plain text and hence the integrity is proved.

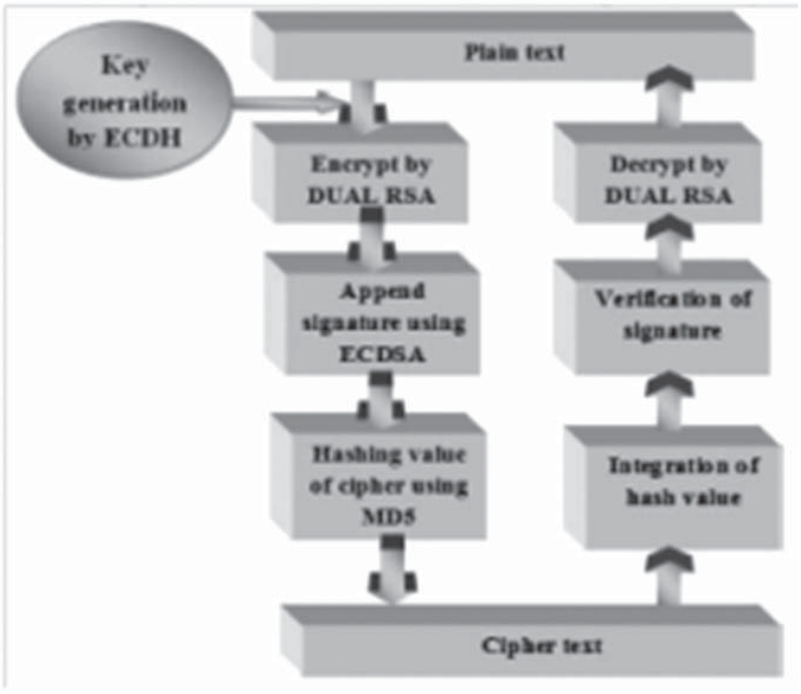


**Figure 4. Dubal security protocol architecture [11]**

### 2.3 Hybrid security protocol Architecture III (Kumar)

This is the architecture. The plaintext is encrypted first with AES and then with ECC. The encrypted cipher's hash value is passed through MD5 algorithm. The hash value is first evaluated and integrated on the other side. The decryption of cipher text is performed by AES and ECC. Hence, plaintext is derived. It is a combination of both Symmetric and Asymmetric Cryptographic techniques. Execution time is more because AES and ECC have been used sequentially.

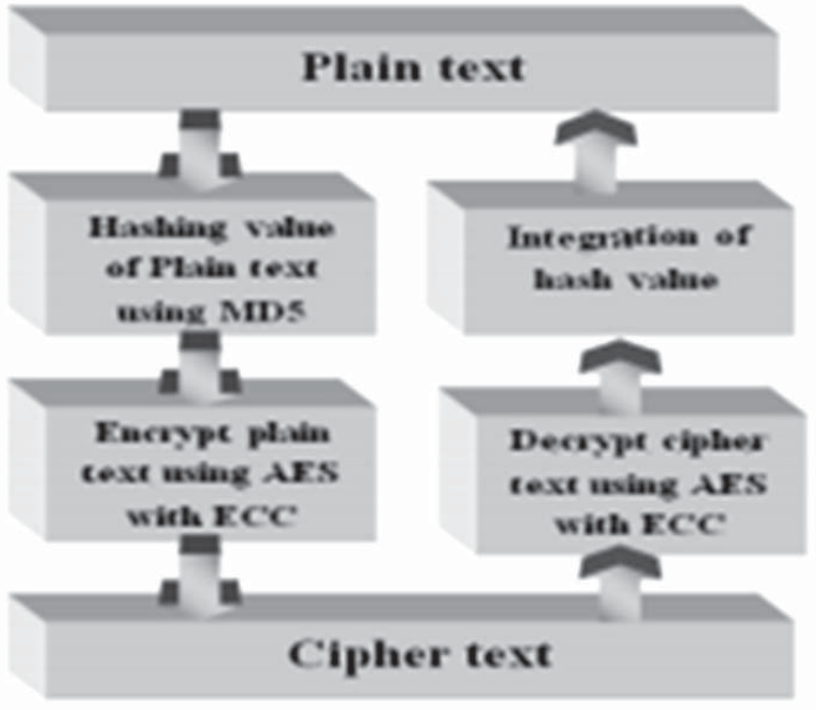


**Figure 5. Kumar security protocol architecture [13]**

### 2.3 Hybrid security protocol Architecture IV (Ren)

DES has a higher efficiency rate in block encryption and is hence used for transmission. RSA has got management advantages and is so used for the encryption of the DES. During encryption phase, the random number generator uses a DES session key once which is 64 bits. The plaintext is encrypted to produce the cipher text. Public key is received from the public key management center. RSA is used for encryption of session key. The RSA encrypted session key and cipher text from DES encryption are combined and sent [15]. The decryption is just the reverse process. Using DES with RSA affects the security level. Thus, this protocol is weak.

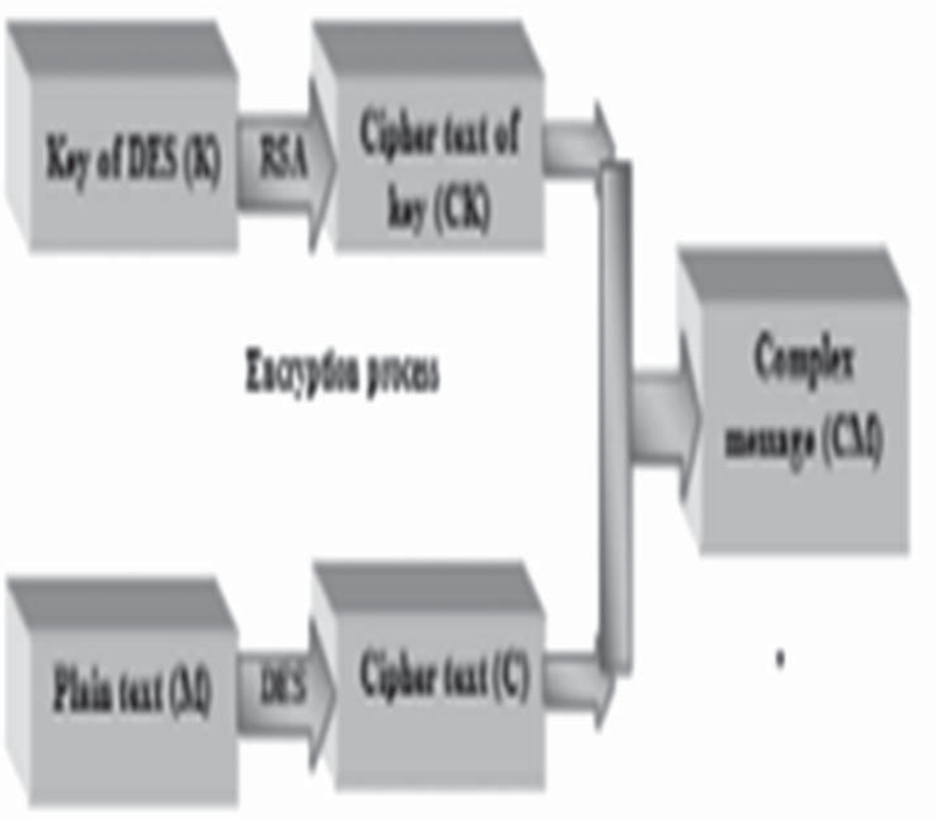


**Figure 6. Ren security protocol architecture [14]**

***Hybrid security protocol Architecture V (Zhu):***

The figure shows the Zhu security protocol. Symmetric cipher algorithm is used for the encryption process. The key and digital signature belonging to symmetric encryption is encrypted with asymmetric encryption. Plaintext P is encrypted with key $K_{AES}$ (belonging to AES algorithm). To ensure security sender uses $K_{AES}$ algorithm only once. Original information P is obtained after signature verification. There is very low security level in this protocol because the message is encrypted only in a single phase. This leads to less complexity.


**Figure 7. Zhu security protocol architecture [16]**

## 2.4 Hybrid security protocol Architecture VI (Alkady)

***Encryption phase***

This is the encryption phase. The plaintext that has been provided is divided into n blocks. Each of the blocks contains 128 bits. This text is divided into two parts-say, P($a$) and P($b$); P($a$) contains $0 \rightarrow n/2-1$ blocks and P($b$) contains $n/2 \rightarrow n-1$ blocks.

Now, let us consider the first $n/2$ blocks. This is encrypted using hybrid encryption algorithm, i.e. using AES and ECC. ECC is used for the purpose of protecting the secret key, using most secure public key algorithm. Mathematically, ECC algorithm can be solved by fully exponential instead of sub exponential. ECC requires smaller key size than other algorithm thus requiring less memory size. As a result the communication nodes can handle larger number of requests and also dropping minimum number of packets. Now, ECC consumes more power than symmetric algorithm; AES has less power consumption, hence, increasing the life of the system. AES along with ECC helps us to save power, achieving 25% of speed during the process of encryption and about 20% during the decryption phase. Let us take the first $n/2$ blocks into account.

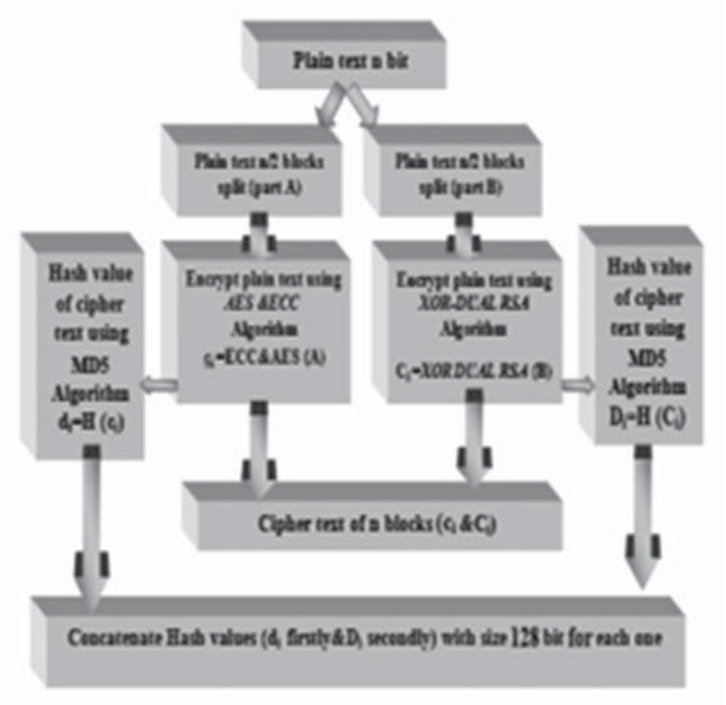


**Figure 8. Encryption Phase [22]**

P($a$) is encrypted by using AES. A key $k_i$ is taken which is the secret key for the AES encryption phase. The size is 128 bits. $k_i$ is encrypted by ECC to give $K_j$

$$\begin{aligned} M &= {}^{i=n/2}\textstyle\sum_{i=1}(B_1) && 0 < i \le n/2-1 \\ K_i &= ECC_{enc}(TC_{PK}, k_{j=1}) && 0 < j \le n/2-1 \end{aligned} \quad (1) \text{ and } (2)$$

In the above equation, ECCenc is the elliptic curve encryption function. The input is ciphered with the trust center public key (TCPK) and this is used as a function to authenticate the key.

$$C_i = (E_{AES})K_j(B_i) \quad (3)$$

where $E_{AES}$ is the AES encryption function.

At the same time the remaining $n/2$ blocks are implemented by using XOR-DUAL RSA principle. The main advantage of DUAL RSA is that it allows extremely fast encryption and decryption; almost four times that of standard RSA. The XOR encryption is a symmetric encryption algorithm, i.e. same key is used for both encryption as well as decryption.

For a resultant stronger algorithm XOR-DUAL principle uses the algorithm stated below:

$$M = {}^{i=n/2}\textstyle\sum_{i=m+1}(B_i)\ n/2 < i \le n-1 \quad (4)$$

Let us choose two very large prime numbers, say $p$ and $q$. Take another variable $n = p*q$ and $\varnothing(n) = (p-1)*(q-1)$. Now, we have to choose a number which is relatively prime to $\varnothing$, say $d$. Find a value e such that $e*d = 1 \bmod \varnothing(n)$. The public key $(e, n)$ is used for encryption.

$$Ri = (Bi)e \bmod n \quad (5)$$

We have to get the ASCII of Bi and convert it into binary.

$$Li = ASCII(Bi) \quad (6)$$

Here, Li is the the function that is required to convert message block to ASCII. Ri is the cipher text which is using DUAL RSA.

$$Ci = (Ri)XOR(Li) \tag{7}$$

MD5 encryption algorithm is applied to cipher texts ci and Ci. This is the performance which is best for hashing function security.[17]

$$di = MD5(ci) \tag{8}$$

$$Di = MD5(Ci) \tag{9}$$

At the last stage of the encryption phase, the two $n/2$ blocks that were divided initially, are integrated to generate cipher text of n blocks. The hash values (di and Di) having size 128 bits each are concatenated. Then they are sent to the sink node simultaneously.

$$C = ci + Ci \tag{10}$$

$$D = di + Di \tag{11}$$

***Decryption phase***

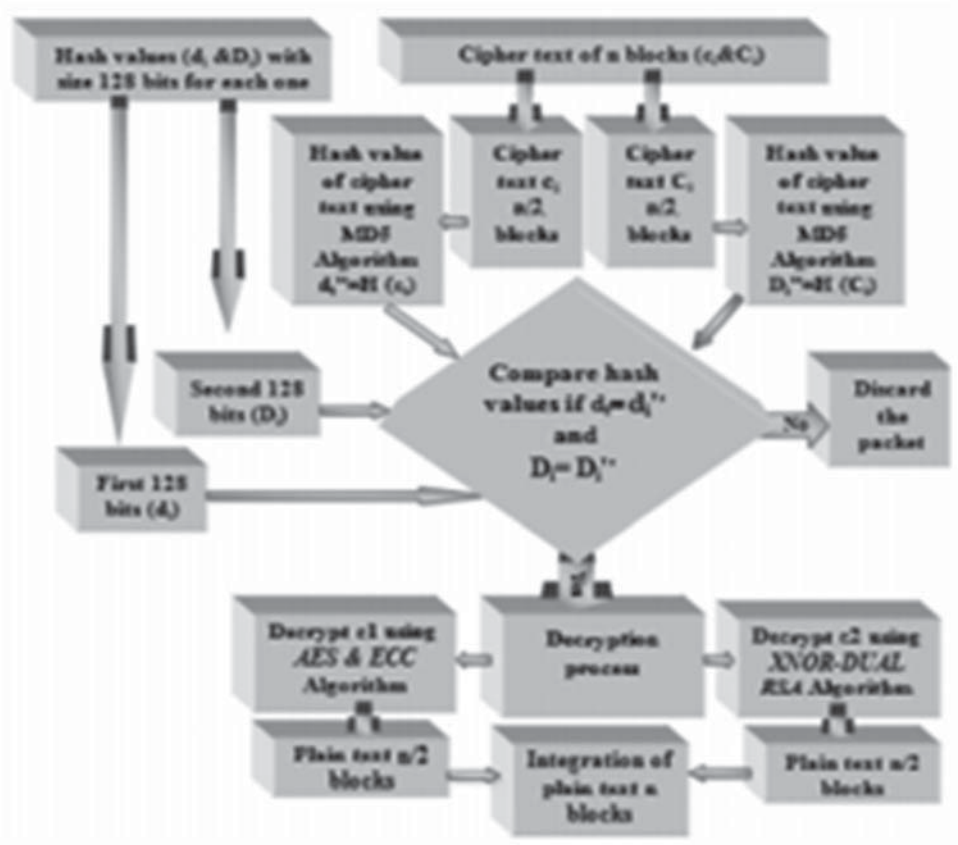


**Figure 9. Decryption phase [22]**

In the decryption phase, the cipher text is divided into n blocks of 128 bits each. It is then divided into 2 parts, $c_i$ (0: $n/2 - 1$) blocks and $C_i$ ($n - 1$) blocks. The hashed value of the cipher is used to check the integrity of the message, the protocol processing only the messages whose hash values are same in both the phases and discarding the rest. For messages that are processed, the first $n/2$ blocks are decrypted using AES and ECC algorithms as the following:

$$C = {}^{i=n/2}\Sigma_{i=1}(B_i) \qquad 0 < i \le n/2\text{-}1 \tag{12}$$

$$k_i = ECC_{dec}(TC_{PK}, K_{j-1}) \qquad 0<i\le n/2\text{-}1 \tag{13}$$

*k* is produced by decryption of $K_j$ using ECC, which is again used to decrypt the cipher text using AES decryption scheme ($D_{AES}$ – AES decryption function).

$$m_i = (D_{AES})_{Kj}(c_i)$$

$m_i$ is the first part of the plain text, P1.

**XNOR DUAL RSA** is applied to decrypt the remaining *n*/2 blocks.

$$C = {}^{i=n/2}\Sigma_{i=n-1}(B_i) \qquad n/2 < i \leq n\text{-}1 \tag{14}$$

The private key (*d*, *p*, *q*) is used for decryption as follows:

First parameters $dp = d \bmod (p-1)$, $dq = d \bmod (q-1)$, $R_{pi} = R_i\ dp \bmod p$, $R_{qi} = R_i\ dq \bmod q$ are computed

$$S_0 = (R_{qi} - C_{pi}).\ p - 1 \bmod q \tag{15}$$

$$S_i = R_{pi} + S_0.\ P \tag{16}$$

Get ASCII for (Ci) and convert ASCII to binary.

$$W_i = \text{ASCII}\ (C_i)$$

Where $L_i$ is a function used to convert block of cipher text to ASCII.

$$M_i = Si \text{ XNOR } Wi \tag{17}$$

$M_i$ is P2, the second part of the plaintext.

In the final stage, the two parts are integrated into the plain text of *n* blocks.

$$M = m_i + Mi \tag{18}$$

$$M = m_i + M_i \tag{18}$$

## 3. NUMERICAL RESULT

### 3.1 Based on the size of Cipher Text

The first categorization that we have done is on the size of the cipher text. Values from all hybrid cryptographic standards have been used to show the comparison between the encryption processes.

### 3.2 Based on time of encryption/decryption

It is known that the time required for an encryption algorithm to convert to the cipher text is called *encryption time*. Similarly, *decryption time* is the amount of time that is required to convert cipher text to plaintext. From obtained values it can be said that Zhu protocol and the proposed hybrid cryptographic protocol require minimum time for encryption. Also, Zhu protocol and the proposed hybrid standard have the least decryption time.

### 3.3 Based on throughput

The throughput of an encryption scheme can be calculated by finding the encryption time of that particular algorithm. In other words, it indicates the speed of encryption. It can be calculated by using the formula:

$$\text{Throughout of encryption} = T_p(\text{bytes})/E_t(\text{seconds}) \tag{19}$$

Where, $T_p$ is the total plaintext represented in bytes and $E_t$ is the encryption time.

In this case both Zhu and the required protocol achieve the largest values.

### 3.4 Based on consumption of energy in WSN

The energy consumption rate varies greatly in WSNs. It totally depends on the protocols being used by the sensors for communication. We take a basic assumption here and it is that the primary source of power of sensors is batteries. It is very difficult to change the batteries or recharge them when there are hundreds of them together. In order to increase the life of the sensors the power consumption must be decreased.

One of the most well known sensor networks is Zigbee. The power consumption for 24 bytes of data is 0.035706(W). Hence,

$$\text{Bits per sec} = 24*8=192 \text{ bits}$$

$$\text{Power per bit} = 0.0357061192 = 185.9 \text{ uW/bit} = 1487.75$$

$$\text{Energy} = p*t = 0.035706 \text{ w x t (Joules)}$$

It is clear that Kumar encryption standard consumes most power.

**Table 1.**
**Table showing the comparison between various HCPs [22]**

| | Size of plain text (bytes) | Subasree protocol | Dubal protocol | Kumar protocol | Ren Protocol | Zhu protocol | HCP |
|---|---|---|---|---|---|---|---|
| Size of cipher text (bytes) | 609 | 609 | 673 | 846 | 602 | 609 | 641 |
| | 25615 | 25615 | 25645 | 35142 | 25610 | 25615 | 25647 |
| | 35080 | 35080 | 35192 | 48226 | 35070 | 35080 | 35112 |
| | 61386 | 61386 | 61486 | 84340 | 61369 | 61386 | 61418 |
| | 184162 | 184162 | 184262 | 253008 | 184143 | 184162 | 184194 |
| Time of encryption (ms) | 609 | 2063 | 2032 | 1500 | 1432 | 998 | 998 |
| | 25615 | 3683 | 6305 | 1518 | 1490 | 1022 | 1022 |
| | 35080 | 5651 | 15643 | 1526 | 1468 | 1059 | 1059 |
| | 61386 | 15351 | 120608 | 4219 | 3019 | 3143 | 3143 |
| | 184162 | 105889 | 198700 | 5752 | 4970 | 3814 | 3814 |
| Time of decryption (ms) | 609 | 1078 | 1016 | 966 | 756 | 562 | 562 |
| | 25615 | 1085 | 4053 | 972 | 821 | 713 | 713 |
| | 35080 | 1082 | 13227 | 980 | 953 | 824 | 824 |
| | 61386 | 1197 | 13227 | 991 | 864 | 891 | 891 |
| | 184162 | 2087 | 18578 | 1099 | 1075 | 907 | 907 |
| Throughput | 609 | 295.20 | 299.70 | 406.00 | 425.28 | 610.2 | 610.2 |
| | 25615 | 6954.93 | 4062.65 | 6874.18 | 17191.2 | 12063.6 | 12063.6 |
| | 35080 | 6207.75 | 2242.54 | 22988.2 | 23896.5 | 33125.6 | 33125.6 |
| | 61386 | 3998.83 | 508.97 | 14549.9 | 20333.2 | 19531.0 | 19531.0 |
| | 184162 | 1739.20 | 926.83 | 32017.0 | 37054.7 | 48285.8 | 48285.8 |

## 4. SIMULATION

The security protocol of the proposed system is tested in the WSN. Network simulator ns2 is used for the simulation. Twenty nodes have been taken and are located randomly in the network. Node 0 is transmitting a data to node 18.

Each node must know about the other nodes. First, the information will be sent in form packets. This packet has information about the source packet. Finally, when the packet reaches the final node, all addresses present in the packet is checked. After that, it sends a reply to the source node. The size of the packet keeps on increasing as other nodes in between add their addresses to that packet. Once the transmission is done, all the nodes will have knowledge about the location of every sensor node that are present in the network. Hence, communication is possible.

It may be possible that due to some situation, the link between nodes fail or their location can change. Thus, the link gets disconnected. Improper packets may also be sent between two networks.

Hybrid algorithm deletes some of the packets because of time-out. If insecure packets are deleted from a link, then it will not be used for a certain amount of time.

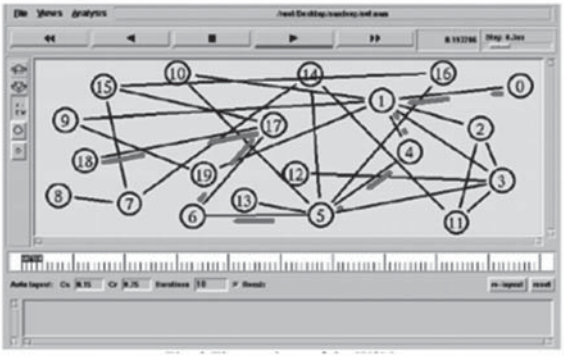

**Figure 10. WSN topology**

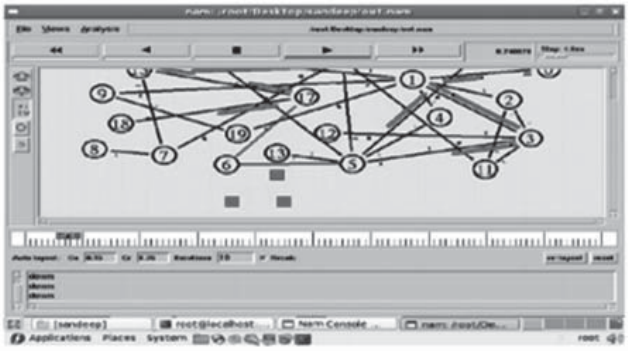

**Figure 11. Packets dropped using proposed protocol**

## 5. CONCLUSION

A robust hybrid protocol has been proposed in this paper. It has been used to solve several problems and also exhibit the strength of cryptosystem. The intruder will face extreme difficulty to get back the plaintext from the cipher that has been generated. This is because in the same plaintext two different encryption techniques have been used. In this case, we are using both symmetric and asymmetric encryption standards. However, we have been successfully been able to eliminate all the disadvantages of both of them. Also, MD5 cryptographic scheme has been used to make sure that there is no way in which the original data can be changed. This encryption standard has proved in all the ways that it is better than most other hybrid encryption techniques. Also, the longevity of the devices will be more if such an encryption standard is used. Thus, we can say that this hybrid encryption technique can easily be used in everyday application without any problem.

### *References:*


1. S. Faye, and J. F. Myoupo, “Secure and energy-efficient geocast protocols for wireless sensor networks based on a hierarchical clustered structure,” International Journal of Network Security, vol. 15, no. I, pp. 121-130, January 2013.
2. T. Bin, Y. Yi-Xian, L. Dong, L. Qi and X. Yang, “A security framework for wireless sensor networks,” The Journal of China Universities of Posts and Telecommunications, vol. 17, pp.118 122, 2010 .
3. G. Singh, Supriya, “A Study of encryption algorithms (RSA, DES, 3DES and AES) for Information Security,” International Journal of Computer Applications, vol. 67, no. 19, pp. 33-38, April 2013.
4. W. Burr, “Selecting the Advanced Encryption Standard,” IEEE, vol. I , no. 2, pp. 43-52, 2003.
5. R. Kodali and N. Sarma, “Energy efficient ECC encryption using ECDH,” Springer-Verlag, vol. 248, pp. 471-478, 2013.
6. M. Balitanas, “Wi Fi protected access-pre-shared key hybrid algorithm,” International Journal of Advanced Science and Technolog, vol. 12, November 2009.

7. D. Johnson, A. Menezes, and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA),” International Journal of Information Security, vol. I, no. I, pp. 36-63, August 2001.

8. M. Frunza and Gh. Asachi, “Improved RSA encryption algorithm for increased security of wireless networks,” ISSCS International Symposium, vol. 2, July 2007.

9. Md. A. Hossain, Md. K. Islam, S. K. Das and Md. A. Nashiry “Cryptanalyzing of message digest algorithms MD4 and MD5”, International Journal on Cryptography and Information Security (lJClS), vol. 2, no. I, March 2012.

10. S. Subasree and N. K. Sakthivel, “Design of a new security protocol using hybrid cryptography algorithms,” lJRRAS, vol. 2, no. 2, pp. 95-103, February 2010.

11. M. J. Dubal, T. R. Mahesh, and P. A. Ghosh, “Design of a new security protocol using hybrid cryptography architecture,” In Proceedings of 3rd International Conference on Electronics Computer Technology (ICECT), vol. 5, 2011.

12. H. Sun, and et aI., “Dual RSA and its security analysis”, IEEE Transaction on Information Theory, pp. 2922 -2933, August 2007.

13. N. Kumar, “A Secure communication wireless sensor networks through hybrid (AES+ECC) algorithm”, von LAP LAMBERT Academic Publishing, vol. 386, 2012.

14. W. Ren, and Z. Miao, “A hybrid encryption algorithm based on DES and RSA in bluetooth communication,” In Proceedings of the 2nd International Conference on Modeling, Simulation and Visualization Methods, pp. 221-225 , 2010.

15. D. Boneh and G. Durfee, “Cryptanalysis of RSA with private key d less than N,” IEEE Trans. In! Theory, vol. 46, no. 4, pp. 1339- 1349, Jul. 2000.

16. S. Zhu,” Research of hybrid cipher algorithm application to hydraulic information transmission,” In Proceedings of International Conference on Electronics, Communications and Control (ICECC), 2011.

17. A. Lenstra, “Unbelievable security matching AES security using public key systems,” Advances in Cryptology -ASIA CRYPT, vol. 2248, pp. 67-86, December 2001.

18. S. Ti11ich, J. Gro13schadl ,”Accelerating AES using instruction set extensions for Elliptic Curve cryptography,” Computational Science and Its Applications - ICCSA, vol. 3481, pp. 665-675, 2005.

19. S. AI-alak, Z. Ahmed, A. Abdullah and S. Subramiam,” AES and ECC Mixed for ZigBee Wireless Sensor Security”, World Academy of Science, Engineering and Technology, 2011.

20. www. islab.csie.ncku.edu.tw/course/slide/ch_10.ppt

21. Komal D Patel , Sonal Belani,” Image Encryption Using Different Techniques: A Review””,IJETAE Volume 1, Issue 1, November 2011

22. Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk.” A New Security Protocol Using Hybrid Cryptography Algorithms”, 2013 IEEE.