ISSN 2277-3061

Developing and Evaluation of New Hybrid Encryption Algorithm

Hatem M. Abdul Kader[1] , Mohie M. Hadhoud[2] , Salah M El-Sayed[3] , Diaa Salama AbdElminaam[4]

Information Systems Department , Faculty of Computers and Informatics, Menofyia University, Egypt
hatem6803@yahoo.com
Information Technology Department , Faculty of Computers and Informatics, Menofyia University, Egypt
mmhadhoud@yahoo.com
Scientific Computing Department , Faculty of Computers and Informatics, Banha University, Egypt
ms4elsayed@fci.bu.edu.eg
Information Systems Department , Faculty of Computers and Informatics, Banha University, Egypt
Diaa.salama@fci.bu.edu.eg

ABSTRACT

Wireless Sensor networks consist of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed. As wireless sensor networks continue to grow, so does the need for effective security mechanisms because sensor networks may interact with sensitive data. Encryption algorithms play good roles in information security systems (ISS). Those algorithms consume a significant amount of computing resources such as battery power. Wireless Sensor networks are powered by a battery which is a very limited resource. At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. The present asymmetric encryption methods and symmetric encryption methods can offer the security levels but with many limitations. For instance key maintenance is a great problem faced in symmetric encryption methods and less security level is the problem of asymmetric encryption methods even though key maintenance is easy. To improve the strength of these algorithms, we propose a new hybrid cryptographic algorithm in this paper. The algorithm is designed using combination of two symmetric cryptographic techniques and two Asymmetric cryptographic techniques. This protocol provides three cryptographic primitives, integrity, confidentiality and authentication. It is a hybrid encryption method where elliptical curve cryptography (ECC) and advanced encryption (AES) are combined to provide node encryption. RSA algorithm and Blowfish are combined to provide authentication and (MD5) for integrity. The results show that the proposed hybrid cryptographic algorithm gives better performance in terms of computation time and the size of cipher text.

This paper tries to present a fair comparison between the new protocols with four existing different hybrid protocols according to power consumption. A comparison has been conducted for those protocols at different settings for each protocol such as different sizes of data blocks, and finally encryption/decryption speed. Experimental results are given to demonstrate the effectiveness of each algorithm.

Indexing terms/Keywords

Wireless Sensor networks (WSN), Information Security Systems (ISS), Advanced Encryption Standard (AES), Cryptography, Elliptic Curve (ECC), Message Digest-5, hybrid cryptographic algorithm.

Council for Innovative Research

Peer Review Research Publishing System

Journal: INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Vol 13, No. 1

editor@cirworld.com

www.cirworld.com, www.ijctonline.com

1. INTRODUCTION

As the important of the data on Wireless Sensor Networks (WSNs) increase so does the need to protect them. The Security has become very important in Wireless Sensor Networks (WSNs) [1]. There are many different cryptographic algorithms to achieve the security services such as Authentication, Confidentiality, and Integrity.

- ***Authentication***: means preventing unauthorized parties from participating in the network.
- ***Confidentiality***: means keeping information secret from unauthorized parties.
- ***Integrity***: ensures the receiver that the received data is not altered in transit by an adversary. Note that data authentication can provide data integrity also.

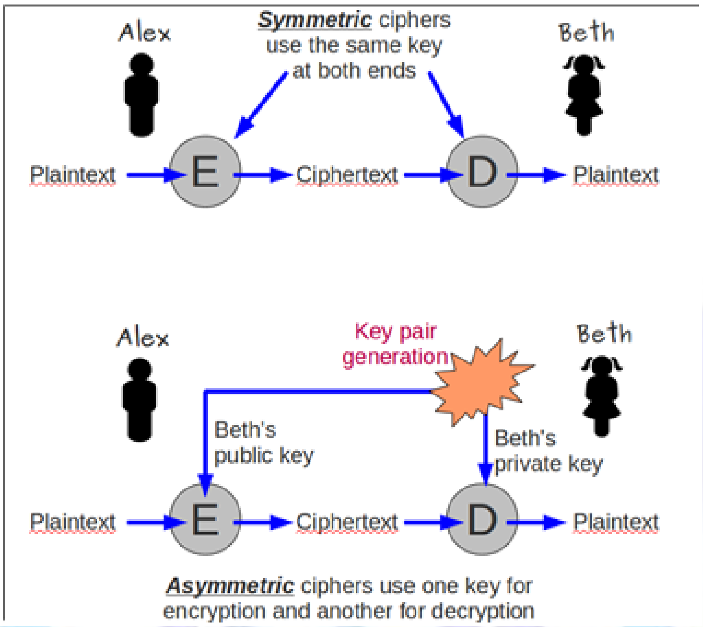

Fig. 1 : Overview of the field of cryptography

There are two essential problems related to security protocols arise in WSNs. Firstly, the overload that security protocols introduce in messages should be reduced at a minimum; every bit the sensor sends consumes energy and, consequently, reduces the life of the device. Secondly, the memory size which refers to size of encrypted message and key size should also be reduced [2].

Security can be provided at different settings with different security algorithms. The security settings can be different in many factors, but the main factors are the choice of ciphers used to prove security functions, packet size.

Cryptography algorithm can be classified into category (Fig.1). The two categories are: Symmetric and Asymmetric keys encryption. In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. The key should be distributed before transmission between entities. Keys play an important role. If weak key is used in algorithm then everyone may decrypt the data. Strength of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. There are many examples of cryptography algorithms like Blowfish, DES, RC6,and AES.Blowfish uses various (32-448); default 128bits while AES is used various (128,192,256) bits keys [3-8].

Asymmetric key encryption is used to solve the problem of key distribution. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption .Because users tend to use two keys: public key, which is known to the public and private key which is known only to the user. There is no need for distributing them prior to transmission. Common asymmetric encryption algorithms include RSA and Elliptic Curve Cryptography (***ECC***) [9]. ***ECDSA*** - Elliptic Curve Digital Signature Algorithm [10] is used for authenticating a device or a message sent by the device. ***ECDH*** – Elliptic Curve Diffie Hellman [11] is a key agreement protocol that allows two parties to establish a shared secret key that can be used for private key algorithms. Both parties exchange some public information to each other. ***RSA*** [8]is based on the presumed difficulty of factoring large integers, the factoring problem.

Both Symmetric and Asymmetric cryptographic algorithms offer advantages and disadvantages. Asymmetric algorithms provide more functionality than Symmetric algorithms, at the expense of speed and hardware cost. On the other hand Symmetric encryption provides cost-effective and efficient methods of securing data without compromising security and should be considered as the correct and most appropriate security solution for many applications. In some instances, the best possible solution may be the complementary use of both Symmetric and Asymmetric encryption.

Hybrid encryption attempts to exploit the advantages of both kinds of algorithm classes, while avoiding their disadvantages.

Hashing creates a unique, fixed-length signature for a message or data set. It is commonly used to check data integrity. Message-digest (***MD5***) [13] algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. It has been utilized in a wide variety of security applications.

In this paper, a new security protocol using hybrid cryptography algorithms is proposed. It is designed to provide data security and users authenticity. It includes two phases at the same time. Firstly, it takes the advantages of the combination of both Symmetric and Asymmetric cryptographic techniques using both ***AES*** and ***ECC*** algorithms. Secondly, it takes the advantages of the combination of both anther Symmetric and Asymmetric cryptographic techniques using both ***Blowfish*** and ***RSA*** algorithms.In addition, Hashing is also used for data integrity using ***MD5*** to be ensured that the original text is not being altered in the communication medium. The proposed protocol has high operation speed, high security performance and strong usability.

The organization of this paper is as follows: Brief overviews of the existing protocols are presented in Section 2. The proposed Hybrid Encryption Protocol is introduced in Section 3. Sections 4 present the numerical results and the simulation results; respectively. Finally, the main conclusion is presented in Section 5.

2. RELATED WORK

2.1 (Subasree) Security Protocol Architecture [14]

This protocol is shown in Fig. 2. The given plain text can be encrypted with the help of ECC and the derived cipher text can be communicated to the destination through any secured channel. Simultaneously, the Hash value is calculated through MD5 for the same plain text, which already has been converted into the cipher text by ECC. This Hash value has been encrypted with DUAL RSA and the encrypted message of this Hash value also sent to the destination.

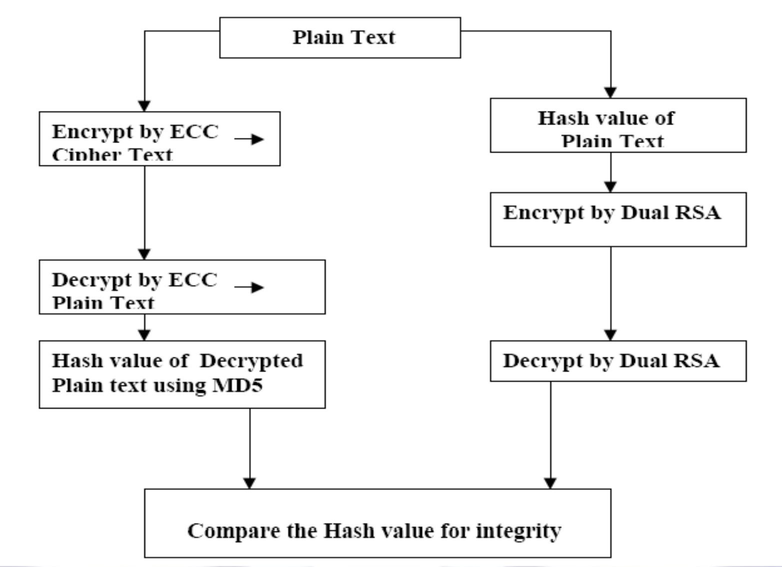
Plain Text
Encrypt by ECC → Cipher Text
Hash value of Plain Text
Encrypt by Dual RSA
Decrypt by ECC → Plain Text
Hash value of Decrypted Plain text using MD5
Decrypt by Dual RSA
Compare the Hash value for integrity

Fig. 2: (Subasree) Security Protocol Architecture [14]

there are two disadvantages. First, the message is encrypted by Asymmetric Encryption Algorithms (ECC and DUAL RSA Public key encryptions) that are slow compared to symmetric encryption. Second,if an attacker determines a person's private key, his or her entire messages can be read.

2.2 (Kumar) Security Protocol Architecture [15]

The protocol architecture is shown in Fig. 3. The given plain text is encrypted first with AES algorithm and then with ECC algorithm. The Hash value of this encrypted cipher text is taken through the MD5 algorithm. On the other side, the Hash value is first evaluated and integrated. Thereafter, the decryption of cipher text is done by AES and ECC decryption algorithms. Hence, the plaintext can be derived.

The (Kumar) Security Protocol is a combination of both the Symmetric and Asymmetric Cryptographic Techniques. However, the execution time of this protocol is long because the plaintext is encrypted sequentially by both AES and ECC

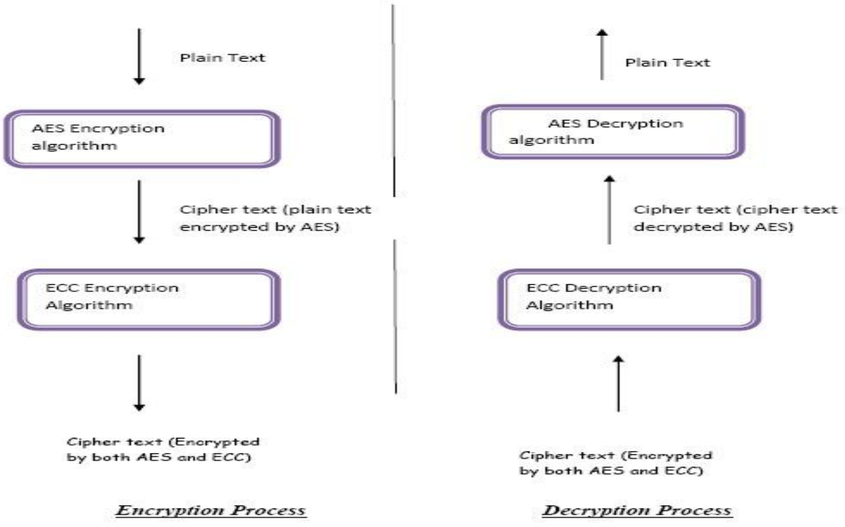
Plain Text
AES Encryption algorithm
Cipher text (plain text encrypted by AES)
ECC Encryption Algorithm
Cipher text (Encrypted by both AES and ECC)
Encryption Process
Plain Text
AES Decryption algorithm
Cipher text (cipher text decrypted by AES)
ECC Decryption Algorithm
Cipher text (Encrypted by both AES and ECC)
Decryption Process

Fig. 3: (Kumar) Hybrid Protocol Architecture [15]

2.3 (Kady) Security Protocol Architecture [16]

The protocol architecture is shown in Fig. 4. The plaintext is divided into n blocks Bi. Each block consists of 128 bits. Then, it is divided into two parts p1 blocks, and P2 blocks. The first n/2 blocks are encrypted using (AES and ECC) . In parallel, the remaining n/2 blocks are encrypted using XOR-DUAL RSA algorithm. Then hashing each two half using MD5.

In the Decryption Phase:The decryption phase the cipher text is divided into n blocks each block consists of 128 bits, Then it will divided into two parts ci blocks and Ci blocks.Hashing is used to identify whether the source node receive the same cipher text or not. In the case of the hash values are the same at the source and sink nodes, the first n/2 blocks are decrypted using AES and ECC algorithms .The remaining n/2 blocks are decrypted using XNOR-DUAL RSA algorithm

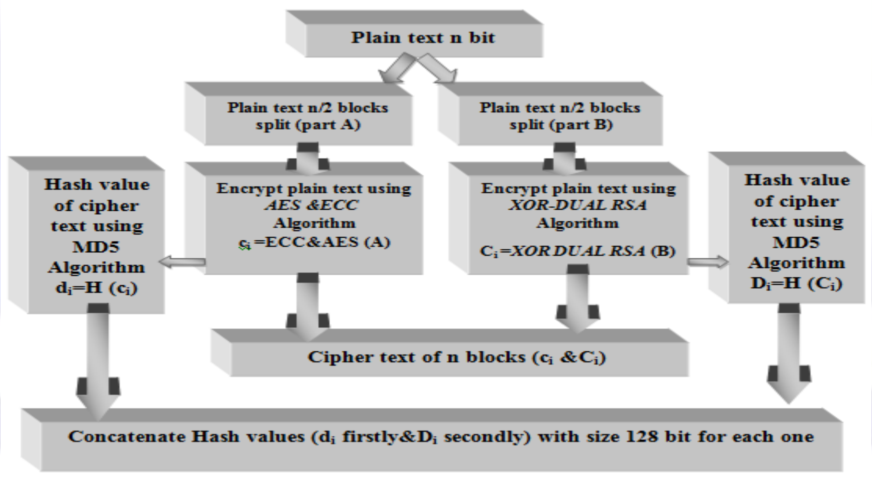
Plain text n bit
Plain text n/2 blocks split (part A)
Plain text n/2 blocks split (part B)
Hash value of cipher text using MD5 Algorithm d_i=H (c_i)
Encrypt plain text using AES &ECC Algorithm c_i =ECC&AES (A)
Encrypt plain text using XOR-DUAL RSA Algorithm C_i=XOR DUAL RSA (B)
Hash value of cipher text using MD5 Algorithm D_i=H (C_i)
Cipher text of n blocks (c_i &C_i)
Concatenate Hash values (d_i firstly&D_i secondly) with size 128 bit for each one

Fig. 4: (Elkady) Hybrid Protocol Architecture [16]

2.4 (Zhu) Security Protocol Architecture [17]

This protocol is shown in the Fig. 5. The plaintext is encrypted with Symmetric cipher algorithm, and the key and digital signature belonged to the Symmetric encryption algorithm are encrypted with Asymmetric key algorithm. The sender encrypts the plaintext P with the key KAES belonged to the AES algorithm. To ensure the security of the cipher algorithm and simplify the key management, the sender uses the key KAES only once. The receiver obtains the original information P after signature verification. The main disadvantage of this protocol, this protocol suffers from low security level since that the message is encrypted in a single phase which leads to less complexity.

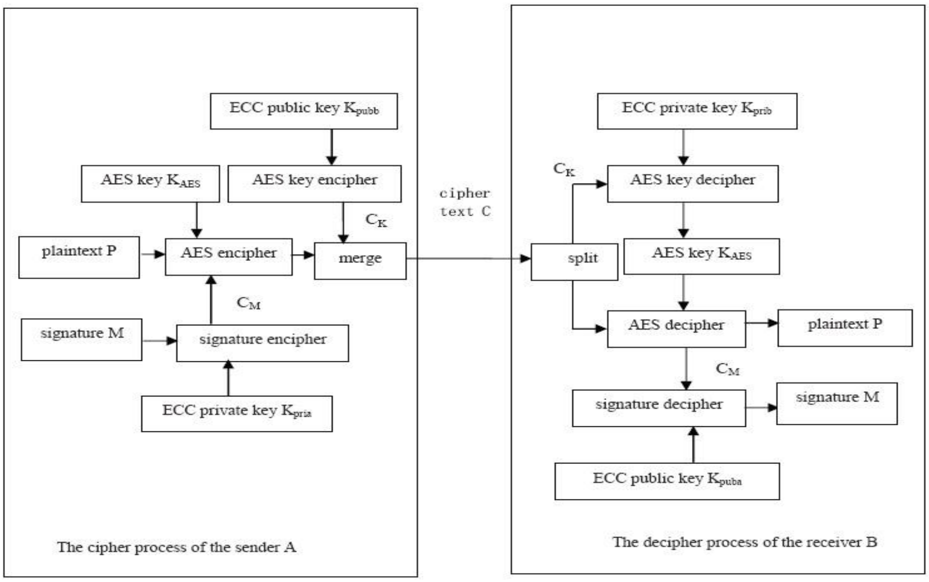

Fig. 5: (Zhu) Hybrid Protocol Architecture [17]

3. THE NEW HYBRID ENCRYPTION PROTOCOL (NHEP)

In this section, the proposed hybrid cryptography protocol (NHEP) is presented.

3.1 Encryption phase steps

The encryption phase as shown in Fig.6. The plaintext is divided into n blocks Bi. Each block consists of 128 bits. Then, it is divided into two parts **P1 (0: n/2-1) blocks, and P2 (n/2: n-1) blocks.**

If n is not integer number and has a fraction. **NHEP** protocol use padding with null for the last block to be 128 bits

The first n/2 blocks are encrypted using (**AES and ECC**) hybrid encryption algorithm. **ECC** algorithm is used for protecting secret key which is highest secure public key algorithm. Moreover, according to the mathematical problem on which **ECC** can be solved by fully exponential rather than sub-exponential for other public key systems, **ECC** needs smaller key size than other algorithms and that refers to less memory size[9]. It allows the communication nodes to handle a larger number of requests with the smallest number of dropped packet. Since that **ECC** consumes more power than symmetric algorithm, using **AES** algorithm reduces the power consumption and raises the system performance [18]. When using **AES** with **ECC**, we are able to save power, and achieve speed up to 25% for encryption and nearly 20% for decryption [19].

The first n/2 blocks are encrypted as the following:

P1 will be **encrypted** using **AES** by the key k_i which is the secret key of **AES** encryption algorithm with size 128 bits.k_i is encrypted by E

$$M = \sum_{i=0}^{i=n/2-1}(Bi) \qquad 0 < i \leq n/2-1 \qquad (1)$$

$$K_j = ECC_{enc}\ (TC_{PK},\ k\ _{i-1}) \qquad 0 < j \leq L-1 \qquad (2)$$

Where ECC_{enc} is Elliptic Curve encryption function. It ciphers the input with trust center public key (TC_{PK}) which is used as a function to authenticate the key.

$$c_i = AES\ _{enc}(K_j\ ,B_i) \qquad \textbf{(3)}$$

Where AES $_{enc}$ is the AES encryption function.

In parallel, the remaining n/2 blocks are encrypted as the following:

P2 will be encrypted using Blowfish by the key k_i which is the secret key of RSA encryption algorithm with size 128 bits.k_i is encrypted by RSA to produce K_j with L length.

Choose two very large prime numbers; denote these numbers as p and q. Set x = p × q, Z = (p-1) × (q-1). Choose a number relatively prime to Z and call it d. Find e such that e × d = 1 mod f(x), Public key (e, x) used for encryption

$$M = \sum_{i=n/2}^{i=n-1}(Bi) \qquad n/2 \leq i \leq n-1 \qquad \textbf{(4)}$$

$$KJ = RSA_{enc}\ (e,x,\ k_i\ ) \qquad (5)$$

Where RSA_{enc} is RSA encryption function. It ciphers the input

Key with public key (e,x) which is used as a function to authenticate the key.

$$C_i= BlowFish_{enc}(K_j ,B_i) \qquad (6)$$

where $BlowFish_{enc}$ is the BlowFish encryption function.

MD5 is applied to the cipher texts ci and C_i. It is the best performance of hashing function security [26].

$$d_i = MD5 (c_i) \qquad (7)$$

$$D_i = MD5 (C_i) \qquad (8)$$

At the final stage of the encryption process, the two n/2 blocks are integrated to generate cipher text of n blocks and it is sent to the sink node. The corresponding Hash values (d_i and D_i) with size 128 bits for each one are concatenated and sent to the sink node at the same time.

$$C = c_i+ C_i \qquad (9)$$

$$D= d_i + D_i \qquad (10)$$

3.1.1 Proposed Encryption Algorithm

Input: M (Plain text), k(secret key of AES encryption), s(128 bit size of block);

Output: C (Cipher text), ci (encrypted text using AES with ECC), Ci (encrypted text using BloeFish with RSA), D (Hashing value of cipher text);

```
n =M/s ;
le t i=0;
    do{
        $m = \sum_{i=0}^{i=\frac{n}{2}-1}(Bi)$ first part of plain text; what is    m and where it is used, what is $B_i$
        for(j=0;j<= n-1;j++)
            {
            $K_j = ECC_{enc} (TC_{PK}, k_{i-1})$ ;
            }
        $c_i= E_{AES}(K_j ,B_i)$;
        $d_i = MD5 (c_i)$;
        i++;
        }
        while(i<n);
i=(n/2)
do{
Let p and q two large prime numbers
x= p*q
z = (p-1) × (q-1)
Let d a relatively prime number to z
e × d = 1 mod z
Let (e, x) public key of  RSA.
        do{
        $M = \sum_{i=n/2}^{i=n}(Bi)$ second part of plain text which encrypted simultaneously with the first part;
for(j=0;j<= n-1;j++)
            {
            $K_j = RSA_{enc} (e,n, k_{i-1})$ ;
            }
        $C_i$= BlowFish $_{enc}$($K_j$ ,$B_i$);
        $D_i$ = MD5 ($c_i$);
        i++;
        }
        while(i< n);
C = $c_i$ + $C_{i\,;}$
D = $d_i$+ $D_i$ ;
```

*Where **n** is number of blocks, i is a counting number, (e, x) is Public key of RSA for encryption process and **MD5** is a hashing function.*

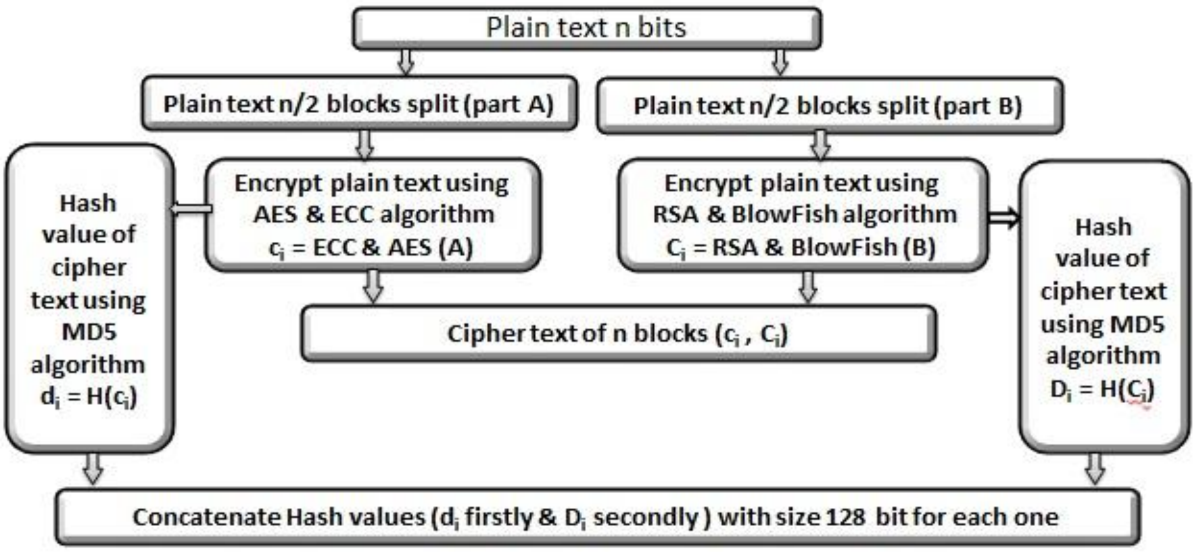
Plain text n bits
Plain text n/2 blocks split (part A)
Plain text n/2 blocks split (part B)
Hash value of cipher text using MD5 algorithm $d_i = H(c_i)$
Encrypt plain text using AES & ECC algorithm c_i = ECC & AES (A)
Encrypt plain text using RSA & BlowFish algorithm C_i = RSA & BlowFish (B)
Hash value of cipher text using MD5 algorithm $D_i = H(C_i)$
Cipher text of n blocks (c_i , C_i)
Concatenate Hash values (d_i firstly & D_i secondly) with size 128 bit for each one

Fig. 6: Encryption Steps of NHEP

3.2 Deccryption phase steps

The cipher text is divided into n blocks each block consists of 128 bits, Then it will divided into two parts c_i (0: n/2-1) blocks and C_i (n/2: n-1) blocks.

Hashing is used in order to identify whether the sink node re-ceive the same cipher text or not. In **NHEP**, if the Hash values in both phases are compared. If they are the same, then the protocol will proceed the decryption phase. Else, it will discard the message.

In the case of the hash values are the same at the source and sink nodes, the first n/2 blocks are decrypted using **AES** and **ECC** algorithms as the following

: ***Input:*** *C (Cipher text), D (Hashing value of cipher text), s (128 bit size of block), L (key length), d_i, D_i, K (encrypted key using ECC, RSA);*

Output: *M (Plain text);*

```
n = C/s;
let i=0;
        do{
```

```
        $c_i = \sum_{i=0}^{i=\frac{n}{2}-1}(Bi)$ first part of Cipher text;
        $d_i'' = MD5(c_i)$;
        $D_i'' = MD5 (C_i)$;
        if $(d_{i=} d_i'')\&( D_i= D_i'')$
                {
                 for(j=0;j<= L-1;j++)
                        {
                        $k_i = ECC_{dec} (TC_{PK}, K_{j-1})$ ;
                        }
                 $m_i = D_{AES}(K_j , c_i)$;
                i++;
                }
        }
        while(i<n/2);
i=n/2;
Give (d, p, q);
        Do
                for(j=0;j<= L-1;j++)
                        {
                        $k_i = RSA_{dec} (d_{PK}, K_{i-1})$ ;
                        }
                 $M_i = D_{BlowFish}(K_i , C_i)$;
                i++;
                }
        while(i<n);
        $M = m_i + M_i$;
```

*Where **n** is number of blocks, **i** is a counting number, **(d,p,q)** is Private key of RSA for decryption process and **MD5** is a hashing function.*

3.3 Strength of NHEP

The strength of any cryptographic algorithm is based on the computational methods and the key used in the process. In normal cryptographic approach the intruders may be able to identify cipher text patterns that are transmitted to the destination side. By analyzing the sequence of bit patterns; it is possible for the intruder to identify which type of encryption algorithm is used or they will identify the key used for encryption/decryption process.

In **NHEP**, splitting the plain text improves the strength of the proposed protocol. The intruder will be not able to identify which type of specific algorithm is applied to generate the cipher text. Thus, it is impossible to decrypt the cipher text. When mixing ***AES*** with ***ECC***, the encryption process is done by Symmetric scheme (***AES***) which is faster than Asymmetric scheme. The secret key of ***AES*** is encrypted by ***ECC*** which is more complicated than others. Also when mixing ***BlowFish*** with ***RSA***, the encryption process is done by Symmetric scheme (***BlowFish***) which is faster than Asymmetric scheme. The secret key of ***BlowFish*** is encrypted by ***RSA*** which is more complicated than others. So that we obtain time reduction and power saving which is the advantage of Symmetric encryption scheme .also we obtain the complexity of Asymmetric encryption scheme which is the advantage of Asymmetric encryption scheme.

4. NUMERICAL RESULTS

4.1 The Size of the Cipher Text

Table I describes the output of the encryption process. It shows the size of the cipher text in bytes. It is shown that (Kumar) Protocol is the worst.

TABLE 1. Size of Cipher Text (bytes)

Size of plain text (bytes)	Subasree Protocol	Kumar Protocol	Zhu Protocol	Kady Protocol	NHEP
1726	1726	1766	1726	1746	1726
2512	2512	2556	2512	2519	2512
8014	8014	8914	8014	8026	8014
8992	8992	8998	8992	8996	8992
12297	12297	12351	12297	12298	12297

4.2 Time of Encryption and Decryption Processes

The encryption time is is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time which can consider as a good indicator for power consumption .

Table 2, and **Fig.7**. shows the time of encryption process for different sizes of plain text. It is shown that, **NHEP** achieve the least time for encryption.

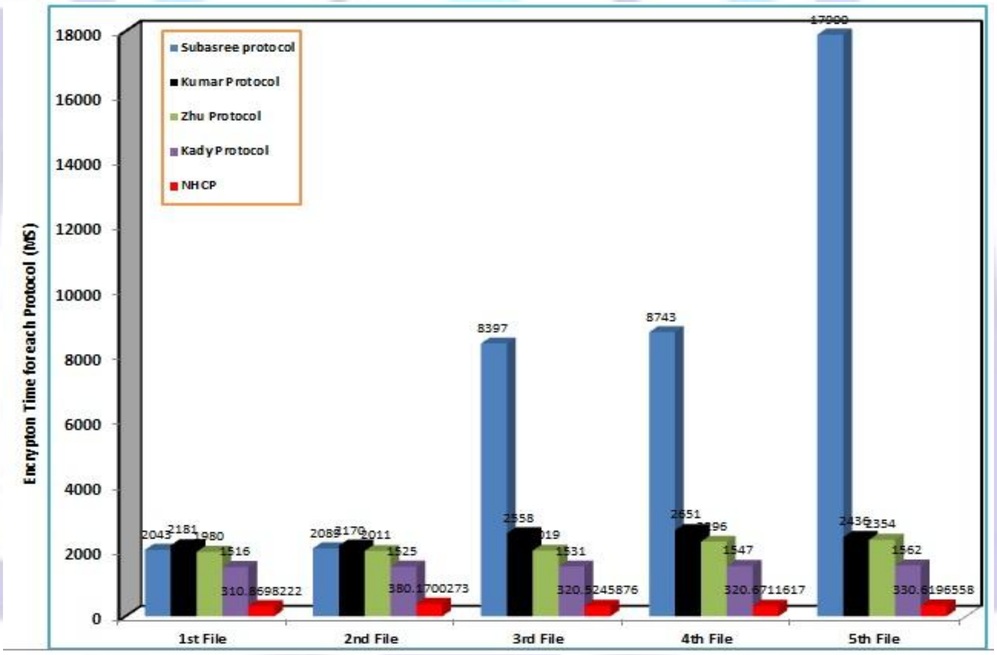

Fig. 7: Time of Encryption for each encryption protocol (ms).

As the Encryption time value is decreased, the power consumption of this encryption technique is decreased.

TABLE 2.Time of Encryption (ms)

Size of plain text (bytes)	Subasree Protocol	Kumar Protocol	Zhu Protocol	Kady Protocol	NHEP
1726	2043	2181	1980	1516	310.86982
2512	2089	2170	2011	1525	380.17003
8014	8397	2558	2019	1531	320.52459
8992	8743	2651	2296	1547	320.67116
12297	17900	2436	2354	1562	330.61966

The decryption time is the time that an decryption algorithm takes to produce a plaintext from a cipher text.**Table 3 , Fig.8** shows the time of decryption process for different sizes of plain text. As in the encryption, it is clear that (Zhu) protocol and the proposed hybrid protocol have the same results and the least time for decryption.

Table 3. Time of Decryption (ms)

Size of plain text (bytes)	Subasree Protocol	Kumar Protocol	Zhu Protocol	Kady Protocol	NHEP
1726	1119	1085	1000	950	101.850
2512	1161	1120	1016	956	106.840
8014	1196	1114	1261	965	194.614
8992	1277	1167	1328	976	125.242
12297	1283	1210	1426	983	156.665

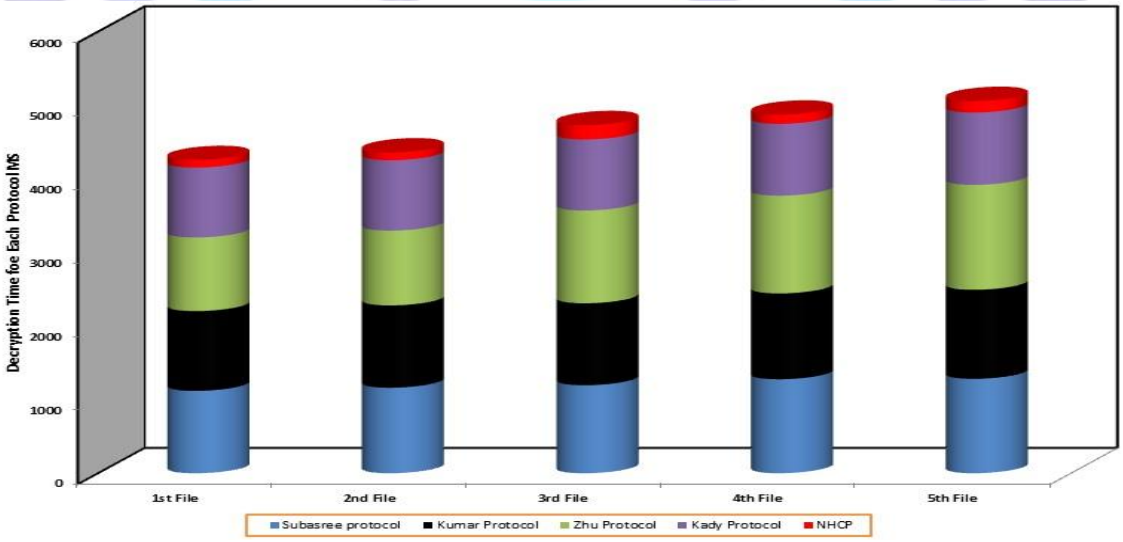

Fig 8: Time of Decryption (ms)

The results show the superiority of **NHEP** algorithm over other algorithms in terms of the encryption and decryption time, processing time, and throughput (when we encrypt the same data by using different five protocols, we found that **NHEP** requires approximately 25% of the time which is consumed for the least of other five protocols). Another point can be noticed here that **ELKADY** has an advantage over other four in terms of time consumption, and throughput. Finally, it is found that **Kumar** has low performance and low throughput when compared with other five algorithms

4.3 Throughput

Enryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as:

Throughput of encryption = T_p (Bytes) / E_t (Sec) (11)

where T_p is the total plain text (bytes) and E_t is the encryption time (second).As the throughput value is increased, the power consumption of this encryption technique is decreased. **Fig.9** shows the throughput of **NHEP** compared with the existing protocols for different sizes of plain text. It is shown that **NHEP** have the same results and they achieve the largest values

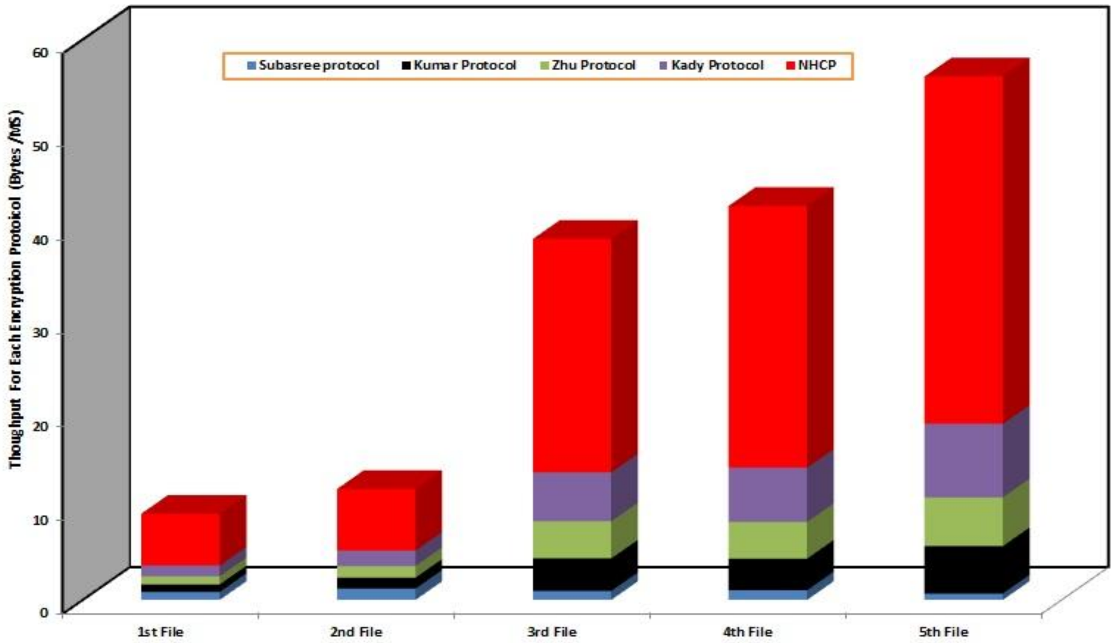

Fig 9: Throughput for each protocol

4.4 Measuring Energy Consumption in WSN

The energy consumption rate for sensors in a WSN vary greatly depending on the protocols the sensors use for communication. A basic assumption is that sensors employ batteries as a power source,which are difficult to change or recharge when there are hundreds of sensors that compose the network. Because of the power source limitation, all processes, communication protocols and systems regarding sensor networks must minimize power consumption so that sensor lifetime may be maximized.

Zigbee is a well known sensor network. It consumes 0.035706 (W) when transferring 24 bytes of data [20]. Then:

- Bits per second = 24 × 8 = 192 bits.
- Power per bit = 0.035706/192 = 185.9 uW/bit =1487.75 uW/byte.
- Energy = p × t = 0.035706 w × t (Joules) (12)

Table 4. Energy Consumed for Encryption for eachprotocol (joules)

Size of plain text (bytes)	Subasree Protocol	Kumar Protocol	Zhu Protocol	Kady Protocol	NHEP
1726	5.24613083	5.730286337	5.08435587	3.937979034	0.807519025
2512	7.807069292	8.25183513	7.515565508	5.715154431	1.424741256
8014	100.1159909	33.92369335	24.07219074	18.28118338	3.827282013
8992	116.9625251	35.4883392	30.71553901	20.70473705	4.291798373
12297	327.4780253	44.76198781	43.06610456	28.57889792	6.049132774

Table 4 , Fig 10, shows the power consumption of Zigbee sensor network for encryption respectively, and makes a comparison between the proposed protocol and the existing protocols at different sizes of plain text. The results show the superiority of **NHEP** algorithm over other algorithms in terms of the encryption and decryption power processing (when we encrypt the same data by using different five protocols, we found that **NHEP** requires approximately 20 % of the power which is consumed for the least of other five protocols). It is clear that (**Kumar**) protocol consumes the largest amount of power.

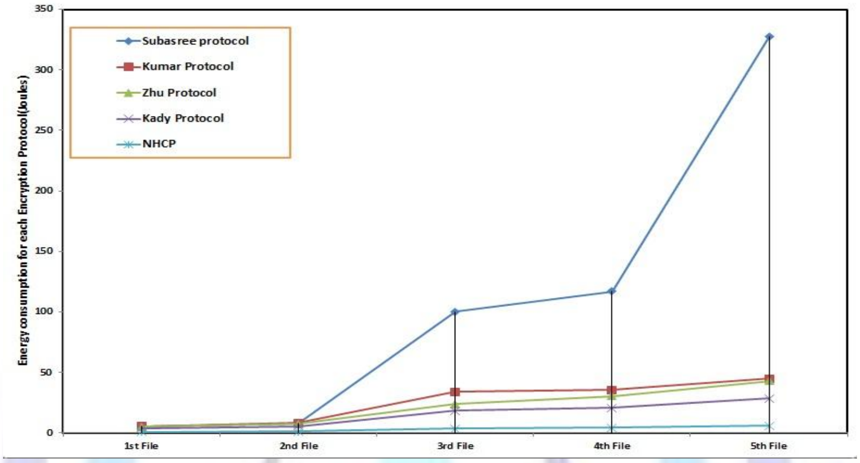

Fig 10: Power Consumption per bytes for encryption Zigbee (Joules)

Table 5 , Fig 11 shows the power consumption of Zigbee sensor network for decryption respectively

Table 5. Energy Consumed for Encryption for eachprotocol (joules)

Size of plain text (bytes)	Subasree Protocol	Kumar Protocol	Zhu Protocol	Kady Protocol	NHEP
1726	2.873431424	2.850692653	2.5678565	2.467730925	0.264567095
2512	4.338921708	4.25901168	3.797023648	3.582745991	0.400400009
8014	14.25970289	14.7736491	15.03468674	11.52275765	2.323824148
8992	17.0835119	15.62236584	17.76578214	13.06258782	1.676223658
12297	23.47230763	22.2339923	26.08847286	17.98531156	2.86641278

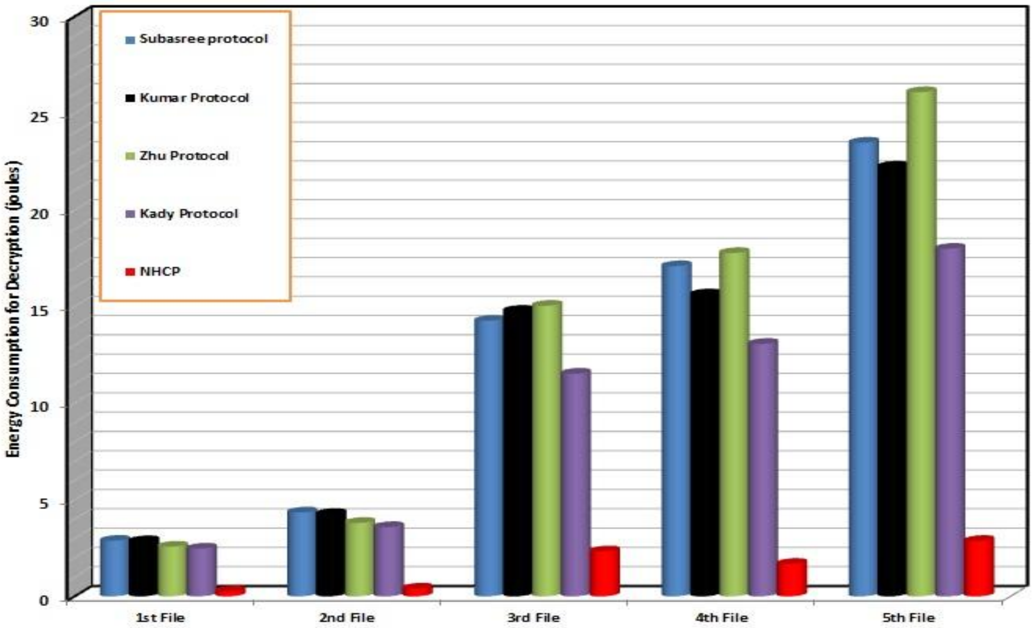

Fig 11. Power Consumption per bytes for decryption Zigbee (Joules)

5. CONCLUSION

This paper presents a performance evaluation of new hybrid encryption algorithms with four existing hybrid protocols.

In this paper, ahybrid security protocol for WSNs is proposed. It is designed in order to solve several problems as practical implementation, short response time, efficient computation and the strength of cryptosystem. ***NHEP*** tries to trap the intruder by splitting the plain text and then applies two different techniques. First, it takes the advantages of the combination of both Symmetric and Asymmetric cryptographic techniques using both ***AES*** and ***ECC*** algorithms for the first part of the data and using both ***BlowFish*** and ***RSA*** algorithms for the second part of the data. In addition, Hashing is also used for data integrity using ***MD5*** to be ensured that the original text is not being altered in the communication medium. The attractiveness of ***HCP***,

The selected algorithms are **Subaree protocol, Kumar protocol, Zhu protocol, Kady Protocol.** Several points can be concluded from the Experimental results. **NHEP** offer better security for a shorter encryption and decryption time, and smallest cipher text size. There by, reducing processing overhead and achieving lower memory consumption that is appropriate for all WSN applications.

Finally we suggest three approaches to reduce the energy consumption of security protocols: replacement of standard security protocol primitives that consume high energy while maintaining the same security level, modification of standard security protocols appropriately, and a totally new design of security protocol where energy efficiency is the main focus.

ACKNOWLEDGMENTS

This study was supported by Faculty of Computers and Informatics (Menofyia University, Banha University), Egypt

REFERENCES

[1] Faye ,S., and Myoupo, J. F. 2013. Secure and energy-efficient geocast protocols for wireless sensor networks based on a hierarchical clustered structure. International Journal of Network Security, vol. 15, no.1, pp. 121-130

[2] Bin ,T., Yi-Xian ,Y., Dong ,L., Qi, L., and Yang ,X. 2010.A security framework for wireless sensor networks.The Journal of China Universities of Posts and Telecommunications, vol. 17, pp.118-122.

[3] Abdu.Ellminaam ,D. S., Abdul kader ,H. M., Hadhoud ,M. M. 2008.Performance Evaluation of Symmetric Encryption Algorithms. IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12 pp: 280- 286

[4] Abdul_Elminaam ,D. S., Abdul_ kader ,H. M., Hadhoud ,M. M. 2009 .Evaluating The Effects of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices. IJICIS International Journal of Intelligent Computing and Information Sciences, Vol.9 No.2 ,pp:143-159.

[5] Abdul.Elminaam ,D. S., Abdul kader, H. M., Hadhoud ,M. M. 2011. Studying the Effects of Most Common Encryption Algorithms .International Arab Journal of e-Technology (IAJeT),VOL.2,No.1,PP:1-10, January

[6] Abdul.Elminaam ,D. S. , Abdul kader ,H. M., Hadhoud, M. M. 2010. Evaluating the Effects of Cryptography Algorithms on Power Consumption for Different Data Types .International Journal of Network Security (IJNS),VOL.11 No.2, pp: 91- 100.

[7] D. S. Abdul.Elminaam, H. M. Abdul kader, M. M. Hadhoud." Evaluating the Performance of Symmetric Encryption Algorithms ".International Journal of Network Security (IJNS), VOL.10 No.3, pp: 216- 222, May 2010.

[8] Abdul.Elminaam ,D. S., Abdul kader ,H. M., Hadhoud ,M. M. 2009. Tradeoffs between Energy Consumption and Security of Symmetric Encryption Algorithms. International Journal of Computer Theory and Engineering (IJCTE) ,VOL.1 No.3, pp: 342- 350.

[9] Kodali ,R. and Sarma ,N. 2013 .Energy efficient ECC encryption using ECDH. Springer-Verlag, vol. 248, pp. 471-478.

[10] Balitanas ,M. 2009. Wi Fi protected access-pre-shared key hybrid algorithm.International Journal of Advanced Science and Technolog, vol. 12.

[11] Johnson ,D., Menezes ,A., and Vanstone ,S. 2001. The Elliptic Curve Digital Signature Algorithm (ECDSA). International Journal of Information Security, vol. 1, no. 1, pp. 36-63.

[12] Frunza ,M. and Asachi ,Gh. 2007.Improved RSA encryption algorithm for increased security of wireless networks. ISSCS International Symposium, vol. 2.

[13] Hossain ,A., Islam ,K., Das ,S. K. and Nashiry ,A. 2012. Cryptanalyzing of message digest algorithms MD4 and MD5.International Journal on Cryptography and Information Security (IJCIS), vol. 2, no.1.

[14] Subasree ,S. and Sakthivel ,N. K. 2010. Design of a new security protocol using hybrid cryptography algorithms.IJRRAS, vol. 2, no. 2, pp. 95-103.

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

[16] Ren ,W. , and Miao, Z. 2013. A new security protocol using hybrid cryptography.In Proceedings of the 9th International Conference Computer Engineering Conference (ICENCO), 9th International, pp. 109-115

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

[18] Lenstra ,A. 2001 .Unbelievable security matching AES security using public key systems. Advances in Cryptology — ASIACRYPT, vol. 2248, pp. 67-86.

[19] Tillich ,S., Großschädl ,J. 2005.Accelerating AES using instruction set extensions for Elliptic Curve cryptography.Computational Science and Its Applications – ICCSA, vol. 3481, pp. 665-675,.

[20] Al-alak ,S., Ahmed ,Z., Abdullah ,A. and Subramiam ,S. 2011.AES and ECC Mixed for ZigBee Wireless Sensor Security.World Academy of Science, Engineering and Technology ,.

Professor Mohiy Mohamed Hadhoud, Former vice president of Menoufia university for education and student affairs and former dean of Faculty of Computers and Information, University, Shebin Elkom, Egypt. Currently, he is the dean of Canadian International College (CIC) in New Cairo. He is a member of National Promotion committee for professors, he is a member of National Computers and Informatics Sector Planning committee, and is the University training supervisor. Prof Hadhoud graduated from the department of Electronics and Computer Science, Southampton University, UK,1987. Since 2001 he worked as a Professor of Multimedia, Signals and image processing and Head of the department of Information Technology (IT), He was a member of the university council. He is the recipient of the university supremacy award for the year 2007. He, among others are the recipient of the Most cited paper award form the Digital signal processing journal, Vol.18, No. 4, July 2008, pp 677-678, ELSEVIER Publisher. Prof. Hadhoud has published more than 160 papers in international journals, international conferences, local journals and local conferences. His fields of Interest: Digital Signal Processing, 2-D Adaptive filtering, Digital Image Processing, Digital communications, Multimedia applications, Information security and data hiding.

Professor.Salah M. Elsayed, Dean, Faculty of Computers and Information, head of Scientific Computing Department, Benha University, Benha, Egypt. His PhD degree ,in Numerical Analysis from the department of Numerical,Theory and Algorithms of Numerical Linear Algebra ,and numerical methods of ordinary and partial differential equations (multi-integral and finite difference methods ,A domain decomposition method and chebychev pseudo spec trail methods. Prof Salah obtain Egyptian incentive prize of science in mathematics 2002,and Scopus prize of Best Author have higher citation and

H-Index in Scopus 2008 in the last ten years. Prof. Salah has published more than 100 papers in international journals, international conferences, local journals and local conferences. His fields of Interest: Numerical Analysis, numerical methods of ordinary and partial differential equations, and Information security and data hiding.

Professor. Hatem. M. Abdul-kader obtained his BSC. And M.SC. (by research) both in Electrical Engineering from the Alexandria University, Faculty of Engineering, Egypt in 1990 and 1995 respectively. He obtained his Ph.D. degree in Electrical Engineering also from Alexandria University, Faculty of Engineering, and Egypt in 2001 specializing in neural networks and applications. He is currently a Lecturer in Information systems department, Faculty of Computers and Information, Menoufya University, Egypt since 2004. He has worked on a number of research topics and consulted for a number of organizations.

Diaa Salama Abdul-Minaam was born on November 23, 1982 in KafrSakr, Sharkia, Egypt. He received the B.S from Faculty of Computers &Informatics, Zagazig University, Egypt in 2004 with grade very good with honor, and obtains master degree in information system from faculty of computers and information, menufia university, Egypt in 2009 and submitted for PhD from October 2009. He is working in Benha University,Egypt as teaching assistance at Faculty of Computer and informatics .Diaa has contributed more than 18+ technical papers in the areas of wireless networks , wireless network security, Information security and Internet applications in international journals, international conferences, local journals and local conferences. He majors in Cryptography and Network Security.(Mobile:+20166104747 E-mail: ds_desert@yahoo.com)