A New Security Protocol Using Hybrid Cryptography Algorithms

[1]**SATYA PRAKASH DAS,** Gandhi Institute of Excellent Technocrats, Bhubaneswar

[2]**SISIR MALLIK,** Gopal Krishna College of Engineering and Technology, Koraput, Odisha, India

Abstract-

A group of sensor nodes deployed in particular environment constitutes a wireless sensor network (WSN). At times the WSN can be even deployed in a very sensitive area where the security becomes a great problem. 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. A hybrid encryption method that combines both symmetric and asymmetric key can provide high security with minimized key maintenance. In this paper, a new security protocol using combination of both symmetric and asymmetric cryptographic techniques is proposed. 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. XORDUAL RSA algorithm is considered for authentication and (MDS) 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.

Index Terms-Advanced Encryption Standard, Cryptography, Elliptic Curve, Message Digest-5, WSN, XOR-Dual RSA.

I. INTRODUCTION

Security has become a challenge in Wireless Sensor Networks (WSNs) [1]. Various cryptographic algorithms have been proposed 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.

Two main 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].

Encryption is the process of encoding information in such a way that eavesdroppers or hackers cannot read it. There are two types of encryption techniques: Symmetric and Asymmetric.Symmetric cryptography, also called private-key cryptography, is one of the oldest encryption methods. It uses only one key for encryption and decryption. Common symmetric encryption algorithms include Data Encryption Standard (DES) [3] and Advanced Encryption Standard (AES) [4].Asymmetric key cryptography, also called public-key cryptography. It requires special keys to encrypt and decrypt messages. Common asymmetric encryption algorithms include RSA and Elliptic Curve Cryptography (ECC) [5]. ECDSAElliptic Curve Digital Signature Algorithm [6] is used for authenticating a device or a message sent by the device. ECDH - Elliptic Curve Diffie Hellman [7] 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 (MDS) [9] algorithm is a widely used cryptographic hash function that produces a 128-bit (16byte) 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, XOR-DUAL RSA is used since it is more robust and cannot be easily attacked like the other 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 organization of this paper is as follows: Brief overviews of the existing protocols are presented in Section II. The proposed Hybrid Encryption Protocol is introduced in Section III. Sections IV and V present the numerical results and the simulation results; respectively. Finally, the main conclusion is presented in Section VI.

II. RELATED WORK

A. (Subasree) Security Protocol Architecture [IO}

As shown in Fig. 1, the plain text is encrypted with the help of ECC and the derived cipher text is 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. In this protocol, it is difficult to extract the plain text from the cipher text, because the Hash value is encrypted with DUAL RSA and the plain text is encrypted with ECC. The Hash value is calculated with MD5. However, there are two disadvantages. First, the message is encrypted by Asymmetric 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.

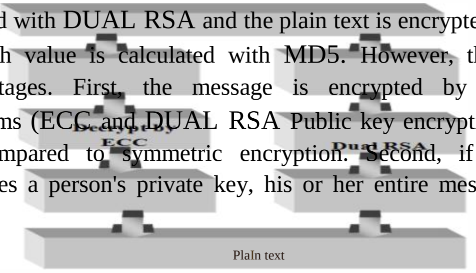

Decrypt by
ECC
Dual RSA
Plaln text
Encrypt by
ECC
Hash value of
plain text
Encrypt by
Hashing value Decrypt by usIng MD5 DualRSA
Compare tbe basb value for integrity

Fig. 1 (Subasree) Security Protocol Architecture [10]

B. (Dubal) Security Protocol Architecture [Ii}

As shown in the Fig. 2, the given plain text is encrypted with the help of key that is generated by ECDH. The encryption algorithm used is DUAL RSA, which takes as the original information and the key. The derived cipher text is appended with the digital signature for more authentications, generated by the ECDSA algorithm. Simultaneously, the Hash value of this encrypted cipher text is taken through the MD5 algorithm. Then, the generated cipher text and the signature is communicated to the destination through any secured channel. On the other side, i.e., on decryption end, the Hash value is fust evaluated and integrated. Thereafter, the decryption of cipher text is done by DUAL RSA [12]. Hence, the plaintext can be derived. In this protocol, the intruder may be trapped by both the encryption by the DUAL RSA with the key generated by ECDH algorithm and the appended signature. However, the used Asymmetric Encryption Algorithms (DUAL RSA and ECDH) are slow compared to symmetric encryption. In addition, the attacker may read the messages if he/she can determine the private key.

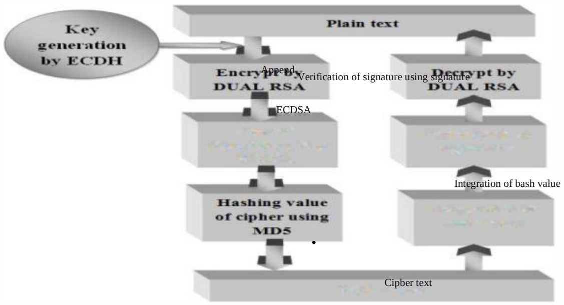

Key generation by ECDH
Plain text
Encrypt by DUAL RSA
Append
Verification of signature using signature
Decrypt by DUAL RSA
ECDSA
Integration of bash value
Hashing value of cipher using MD5
Cipber text

Fig. 2 (Dubal) Security Protocol Architecture [II]

C. (Kumar) Security Protocol Architecture [i3}

The protocol architecture is shown in Fig. 3. The given plain text is encrypted fust 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 fust evaluated and integrated. Thereafter, the decryption of cipher text is done by AES and ECC decryption algorithms. Hence, the plaintext can be derived. This 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.

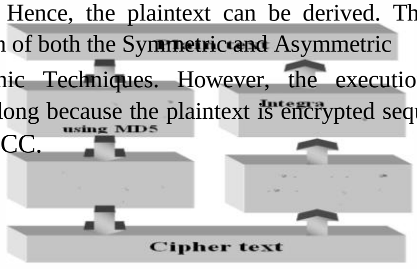

Plain text
using MD5
Integra
Cipher text
Hash.ing value IIlt.egn—tioll of of Plah. txt hasl. value
Ellcl")l.l. phlbl DecrYI.t ci,.ller t_E"xt tlsbag AES text llsing AES wI.IoECC
will. ECC

Fig. 3 (Kumar) Hybrid Protocol Architecture [13]

D. (Ren) Security Protocol Architecture [I4}

The protocol architecture is shown in Fig. 4. DES is used for data transmission because of its higher efficiency in block

$C_i = (E_{AES}h_j(8a$ (3) where E_{AES} is the AES encryption function.

In parallel, the remaining nl2 blocks are encrypted using XOR-DUAL RSA algorithm. DUAL RSA allows for extremely fast encryption and decryption that is at most four times faster than standard RSA .The XOR Encryption algorithm is an example of a symmetric encryption algorithm. This means that the same key is used for both encryption and decryption. In order to develop a stronger algorithm, XOR-DUAL RSA algorithm is presented as the following:

$M = {}^{i}{=}n/2$ L i=n-1 (8i) nj2 ‹i 5 n-l (4)

Choose two very large prime numbers; denote these numbers as p and q. Set n ◦p x q, <1>(n) ◦(P-l) x (q-l). Choose a number relatively prime to <1> and call it d. Find e such that e x d ◦1 mod <1>(n), Public key (e, n) used for encryption

$R_i = (8a\ e \bmod n$ (5)

Get ASCII for (Bi), convert ASCII to binary

L i=ASCII (8i) (6)

Where Li is a function used to convert message block to ASCII. Rj is a ciphered text using DUAL RSA.

Ci = (Ri) XOR(Li) (7)

MD5 is applied to the cipher texts Cj and Cj. It is the best performance of hashing function security [17].

di = MD5(ci) (8) Di = MD5 (Ci) (9)

At the final stage of the encryption process, the two nl2 blocks are integrated to generate cipher text of n blocks and it is sent to the sink node. The corresponding Hash values (dj and Dj) with size 128 bits for each one are concatenated and sent to the sink node at the same time.

C = Ci+ Ci (10) D = di + Di (11)

B. Decryption Phase

The decryption phase is shown in Fig. 7. The cipher text is divided into n blocks each block consists of 128 bits, Then it will divided into two parts Cj (0: nI2-1) blocks and Cj (nI2: n-l) blocks.

Hashing is used in order to identify whether the sink node receive the same cipher text or not. In the proposed protocol, 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 nl2 blocks are decrypted using AES and ECC algorithms as the following:

$C = {}^{i}{=}n/2$ L i=l (8i) 0 ‹i 5 nj2-1 (12) k i = ECCdec (TCPK, Kj-1) 0 ‹j 5 nj2-1 (13)

Kj is decrypted by ECC to produce kj which is used to decrypt the cipher text using AES decryption scheme by DAES (AES decryption function).

H ..... v.Jue or cipher Cipher tut c:; Cipher tut Ci H.ashvalae or

cipher tut asi:ag ..A ..A 'ex'' asi:ag

AIDS blow blod'',

AIDS

AJ:orithm .-\lgorithm d;''=H (<0 I>;''=H (CJ

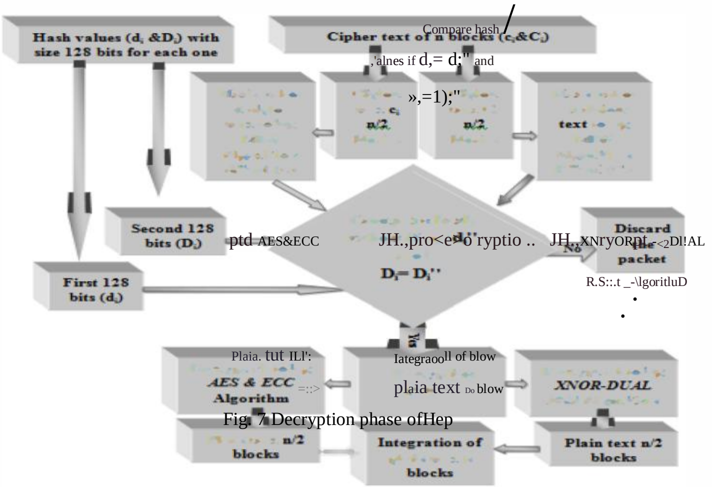


Fig. 7 Decryption phase ofHep

$m_i = (D_{AES}h_j(C_i)$ (14) mj is PI, the first part of plain text.

The remaining nl2 blocks are decrypted using XNOR-DUAL RSA algorithm as the following:

$C = {}^{i}{=}n/2$ L i=n-1(8 i) nj2 ‹i 5 n-l (15

Private Key (d, p, q) used for decryption. To make decryption, first compute some parameters dp ◦d mod (p - 1), dq ◦d mod (q - 1), Rpj ◦Rj dp mod p, Rqj ◦Rj dq mod q,

So = (Rqi - Cpi), p-1 mod q (16) Si = Rpi + So, p (17)

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

W j=ASCII (C;) (18) where Li is a function used to convert block of cipher text to ASCII.

M; =S; XNOR W; (19) Mj is P2, the second part of plain text.

At the final stage of the decryption process, the two nl2 blocks are integrated to produce plain text of n blocks.

M = mi+ Mi (20)

C. Strength of HCP Protocol

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 the proposed protocol, 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. So that we obtain time reduction and power saving which is the advantage of Symmetric encryption scheme. And also we obtain the complexity of Asymmetric encryption scheme which is the advantage of Asymmetric encryption scheme.

IV. NUMERICAL RESULTS

A. 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.

B. Time of Encryption and Decryption Processes

The encryption time is the time that an encryption algorithm takes to produce a cipher text from a plaintext. The decryption time is the time that an decryption algorithm takes to produce a plaintext from a cipher text. Table II shows the time of encryption process for different sizes of plain text. It is shown that, (Zhu) protocol and the proposed hybrid protocol achieve the least time for encryption. Table III 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.

C. 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: $\text{Throughput of encryption} = \text{Tp (Bytes)} / \text{Et (Second)}$ (21) where Tp is the total plain text (bytes) and Et is the encryption time (second). Table IV shows the throughput of the proposed hybrid protocol compared with the existing protocols for different sizes of plain text. It is shown that both (Zhu) protocol and the proposed protocol have the same results and they achieve the largest values.

D. 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 mmumze power consumption so that sensor lifetime may be maximized.

TABLE I. SIZE OF CIPHER TEXT (BYTES)

Size of plain text (bytes)	Subasree Protocol	Protocol Dubal	Protocol Kumar	Protocol Ren	Protocol Zhu	HCP
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
184[redacted]	1[redacted]	1[redacted]2	[redacted]	1[redacted]3	18[redacted]	1[redacted]

TABLE II. TIME OF ENCRY PTTON (MS)

Size of plain text (bytes)	Subasree Protocol	Protocol Dubal	Protocol Kumar	Protocol Ren	Protocol Zhu	HCP
609	2063	2032	1500	1432	998	998
[redacted]	3683	6305 [redacted]	1518	1490	1022 [redacted]	1022
35080	5651	15643	1526	1468	1059	1059
61386	15351	120608	4219	3019	3143	3143
184162	105889	198700	5752	4970	3814	3814

TABLE IIITIME OF DECRYPTION (MS)

Size of plain text (bytes)	Subasree Protocol	Protocol Dubal	Protocol Kumar	Protocol Ren	Protocol Zhu	HCP
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
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
plain	[redacted]	[redacted]	[redacted]			
184162	2087	18578	1099	1075	907	907

TABLE IV THROUGHPUT

Size of plain text (bytes)	Subasree Protocol	Protocol Dubal	Protocol Kumar	Protocol Ren	Protocol Zhu	HCP
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

Zigbee is a well known sensor network. It consumes 0.035706 (W) when transferring 24 bytes of data [19]. Then:

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

Table V shows the power consumption of Zigbee sensor network after implementing the proposed protocol and the existing protocols at different sizes of plain text. It is clear that (Kumar) protocol consumes the largest amount of power.

TABLE V. POWER CONSUMPTION PER BYTES FOR ZIGBEE (W)

Size of plain text (bytes)	Subasree Protocol	Dubal Protocol	Kumar Protocol	Ren Protocol	Zhu Protocol	HCP
609	0.906039	1.0012557	1.258636	0.895625	0.9060397	0.953647
25615	38.10872	38.153346	52.28251	38.10127	38.10872	38.136324
35080	52.19027	52.20812	71.74823	52.17539	52.19027	52.237878
61386	91.32702	91.47579	125.47683	91.3017	91.32702	91.374628
184162	273.9870	274.13578	376.41265	273.9587	273.98702	274.0346

V. SIMULATION RESULTS OF WSN

In order to prove the numerical results of the proposed protocol, it is tested as the security protocol in WSN. The simulation is done using the network simulator ns2. The topology of the WSN is shown in Fig. 8. It consists of twenty nodes. The nodes are located randomly in the network. In the assumed scenario, Node “0” wants to transmit the data to Node “18”.

Each node must have the information about the other nodes present in the WSN. This information will be first transmitted in the form of small packet. This packet contains the information about the source address. If any intermediate node receives a packet, it forwards this packet to the next neighboring node. When this packet reaches the final node it checks all the address present in this packet and then transmits reply back to the source node. The size of these packet increases gradually from small to big as the intermediated nodes adds their address to the packet. After this transmission of the packet every sensor node will have the idea of the location of every other sensor node in the network. Therefore the communication can be done from one node to the other node.

In some situations, the links present between the sensors nodes can fail or the sensor nodes can move from their actual location and there by resulting in breakage of the link. In some other cases, improper packets may be propagated over the link between any two nodes.

The hybrid algorithm (***AES*** and ***ECC***) with (***XOR-DUAL-RSA***) is used to delete some packets because of delay of execution time (time out) as shown in Fig. 9. When such insecure packets are dropped, the link will not be used for a certain time. As a result the network will then use an alternate path as the nodes are having the information about the other nodes in this network for authentication.

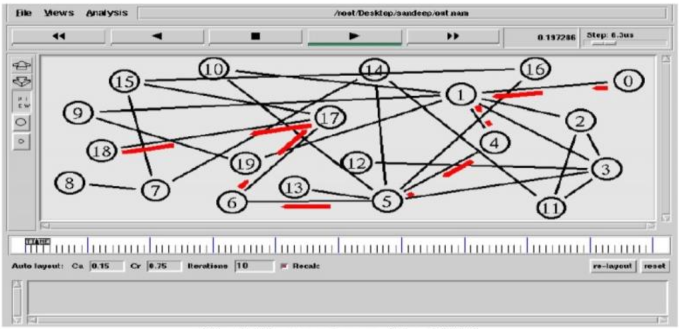
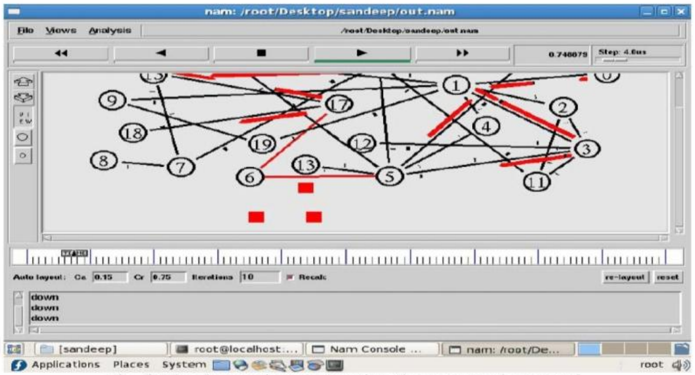


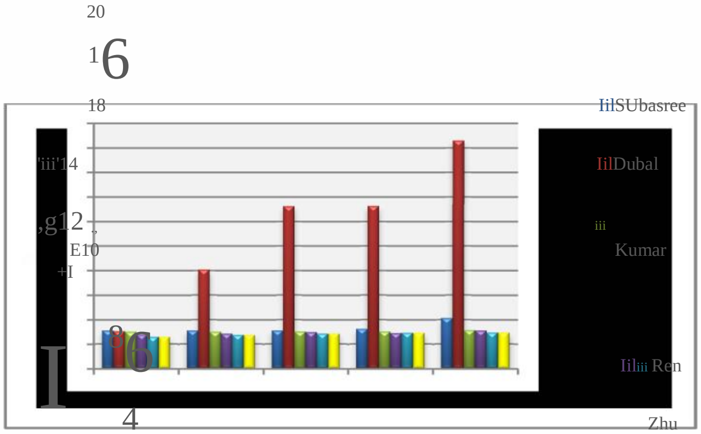
Fig. 8 The topology of the WSN



```
down
down
down
```

Fig. 9 The dropped packets using the proposed protocol

Fig. 10 shows the execution time of the proposed hybrid protocol compared to the other protocols. It is shown that the proposed protocol achieves the least execution time. When the execution time increases, it leads to increase of dropped packets. Fig. 11 shows the rate of dropped packets. It is shown that the proposed hybrid protocol achieves the least rate of packet dropping compared to the other protocols.



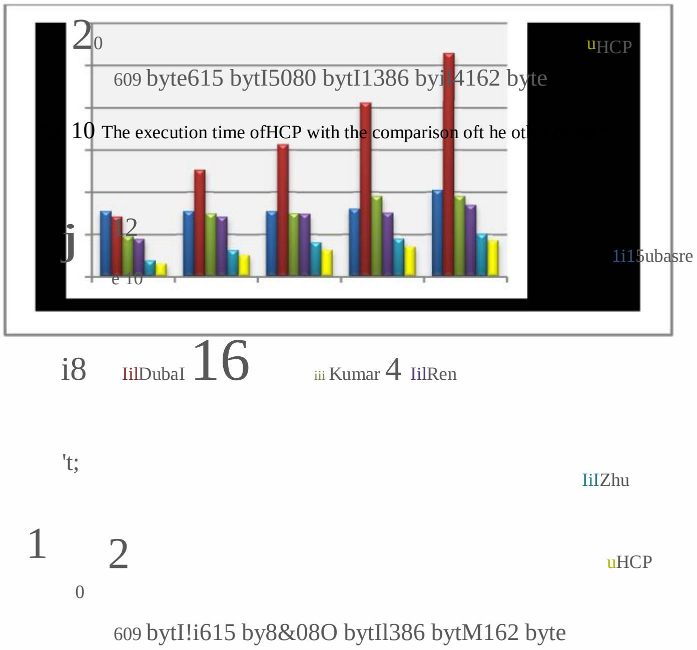


Fig. II The rate of dropped packets of HCP and the existing protocols

VI. CONCLUSION

In this paper, a robust hybrid 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. The proposed hybrid protocol 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. Second, XOR-DUAL RSA is used since it is more robust and cannot be easily attacked. 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 the proposed protocol, compared to other existing security protocols, is that it appears to 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.

REFERENCES

[I] 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.

1 15

[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 (IJCIS), vol. 2, no. I, March 2012.

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

[II] 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. 13391349, 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.