International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 3926 -3931

A Novel Hybrid Approach on Secure Data Transmission in Wireless Sensor Networks

R. Kowsalya[1], Dr. B. Rosiline Jeetha[2]
[1]*Assistant Professor, Department of Computer Science (PG), PSGR Krishnammal College For Women, India*
E-mail: [1]2017ngpphd@gmail.com
[2]*Professor, Department of Computer Science, Dr.N.G.P Arts and Science College, India*
E-mail:[2]drrosilinejeetha@drngpasc.ac.in

Abstract

In recent year wireless sensor network plays an important role in day to day life, to achieve the security, cryptography techniques are used. As wireless sensor has the limited memory space and energy consumption to provide security is vital problem. The main aim of this research work is to analysing different cryptographic techniques such as symmetric key cryptography and asymmetric key cryptography and comparing AES, DES, 3DES, RC5 and IDEA encryption techniques. In this paper, a new security symmetric algorithm was proposed to provide high security. It provides cryptographic primary key integrity, confidentiality and authentication. The results show that the proposed hybrid algorithm HSR19 gives efficient performance for communication devices with the parameters in computation time with different file sizes, encryption and decryption speed and energy

Keywords*: wireless sensor networks, symmetric algorithm, security, energy consumption*

1. INTRODUCTION

The security of the data plays a vital role. There are various encryption algorithm was available for information security. Encryption algorithm was categorized into symmetric (shared key) and asymmetric key encryption (two keys), the keys should be exchanged between the sender and receiver before the transmitting the data. DES standard recommended by NIST (National Institute of Standards and Technology). It uses 64 bits key size with 64 bits block size it has more vulnerable which shows that it is an insecure block cipher [1][2]. 3DES uses 192-bit keys it is same as DES but the encryption process time is more when compared to the simple DES. AES and RC5 uses various key bit size AES use 128 bits, 192, 256-bit keys [3-5]. RC5 uses 0 to 255 bytes key sizes and the block size of 16, 32 and 64 bits of block or word uses XOR method and easy to encrypt the data [6]. Idea uses 64-bit blocks with 128-bit keys for encrypting the data. Proposed novel algorithm HSR 19 uses key size of 128 and 192 bits.

As Energy consumption problem was increased slowly in wireless sensor network which causes a “battery gap” [7]. In this paper the performance of the different symmetric algorithm such as AES, DES, 3DES, IDEA, RC5 was evaluated and new algorithm HSR19 was proposed. The performance of the algorithm was measured in terms of energy consumption, various data types such as text and documents, using different packet sizes and key sizes.

ISSN: 2233 -7857 IJFGCN

This paper is organized as follows: Literature Review is described in Section 2, Section 3 – Proposed methodology; Section 4 includes Simulation results and Conclusion in Section 4 respectively.
literature with a brief consolidation of the survey. The detailed description of the proposed Secure Service Discovery Based on Probe Packet Mechanism (SSDPPM) is depicted in section 3. The algorithm of the proposed Probe Packet Mechanism (SSDPPM) for service discovery is presented in section 4. The Simulations setup and the simulation results are presented and studied in section 5 and 6. Section 7 concludes the paper.

2. LITERATURE REVIEW

(D. E. Burgner and L. A. Wahsheh [8]) discussed on various security issues in wireless sensor networks that affects the context and design middle ware applications such as confidentiality, integrity and authenticity when transferring the data between base station and sensor node. In which the sensor node gathers the information and send the data to the relative cluster head or to the base station.

(Ju Ren et al. [9]) discussed on the aware- reputation systems to detect the selective forwarding attack in wireless sensor networks, It evaluates the data forwarding behavior of sensor nodes, examining the packet loss.(M.Dong [10]) analysed on the detecting the clone , the storage requirement compared with LSM and RED, clone energy efficient to increases lifetime of the network in wireless sensor networks.

Hirani Sohail A [11] proved that the implementation of AES-128 consumes very less energy and encrypt the data in the fewer time. (F. Alfaleh, H. Alfehaid, M. Alanzy and S. Elkhediri [12]) stated that security of the smaller key sizes is provides high security and speed. Chip should be designed with very small size and the limitation of computation power, memory and battery life which could be suitable for IoT.

Rizk, R., &Alkady, Y [13] discussedthe issues on the practical implementations of wireless sensor networks, low response time, efficiency in computation and strength of crypt. They use the combination of symmetric and asymmetric techniques using AES and ECC algorithms for image encryption. It also traps the intruders by splitting the plain text and then applies the hybrid techniques, which secure the data while transferring between sender and the receiver and reduces the response time and computation.

3. PROPOSEDSOLUTION

The hybrid secure data transmission 19 is executed in clustering frame work to secure the data transmission through the network and enhance the time of the wireless sensor network. In the network model formation sensor nodes are located within the simulation area, the cluster head is selected according to the hyper round and the residual energy with the inter and intra cluster group of communication. To secure the data between the cluster heads and cluster the proposed algorithm was developed.

Algorithm: Hybrid secure data transmission (HSR19)
Initialize : Number of sensor nodes, current residual energy, distance and hyper round
Step1 : Deploy the nodes(n)
Step 2 : select the cluster head (ch) based on the residual energy (e)

Step 3: connect the nodes through the genetic algorithm to get the path between node i

Step 4: To exchange the data in network

Step 5 : if the data transfer between cluster head(ch) then

a. Generate the shared key value(k_i) according the cluster head (ch_i, ch_{i+1}) where Ch_{i+1} equal to the routing table r_i go to step 6

Else go to step 8

Step 6: for each data process the below function until the data gets encrypted

a. Select the data to be transfer(d_i) for each data transmission
b. Encryption (E_i)= (k_i * d_i) and transfer the data
c. Send the encrypted data to the Cluster head (ch_{i+1})

Step 7 : for each encrypted data process the below function until all the data received

a. For each data Received, Decryption (D_i)=(E_i *multiplicative inverse of (k_i)) go to step 9

Step 8: Data transmission within Cluster leaf node (clf_i) Generate the shared key value(k_i) according the cluster head (clf_i, clf_{i+1}) where Clf_{i+1} equal to the routing table r_i and the neighbour node go to step 6

Step 9 : End

4. SIMULATION RESULTS

The performances of the algorithms are evaluated with the different constraints using NS2.34 framework using Fedora operating system and all the experiments are processed. The parameter surroundings of wireless sensor network were shown in Table 1.

Parameters	**Values**
Number of Sensor nodes	2-50 in steps of 10
Simulation Area	1000 * 1000 m
Number of Clusters	100
Minimum Number of Nodes in single Cluster	30
Maximum Number of Nodes in single Cluster	50
Initial Energy	100 J
Node energy	100 J
Number of Packets	400
Listening Time	1s
Sleep time	3s
Active time	20s
Routing Protocol	Genetic Algorithm

Table 1: Simulation and Parameters

ISSN: 2233 -7857 IJFGCN

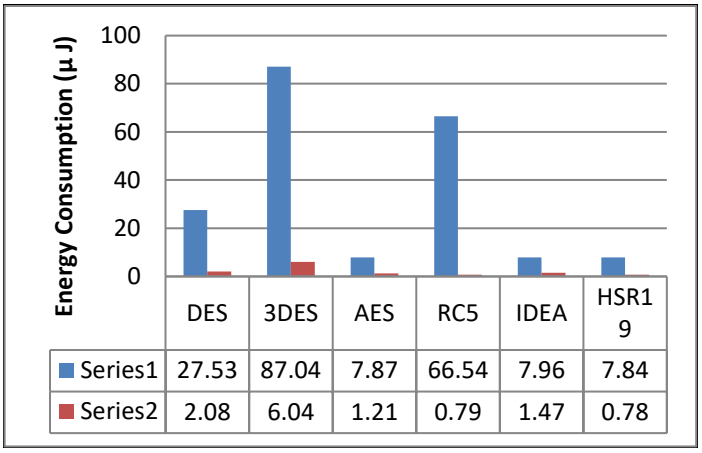

Fig. 1 Energy Consumption

The comparison of the energy consumption during processing is given using fig 1. In this figure, the proposed algorithm HSR19 algorithm key setup and the energy-per-byte numbers for encryption and decryption is very less when compared to the DES,3DES, AES, RC5, IDEA .

Parameters (Series)	**DES**	**3DES**	**AES**	**RC5**	**IDEA**	**HSR19**
Key Setup	27.53	87.04	7.87	66.54	7.96	7.84
energy-per-byte numbers for encryption and decryption phases	2.08	6.04	1.21	0.79	1.47	0.78

Table 2. Energy Consumption

Fig 2. Time taken for processing of different file size

The fig.2 represents the performance of algorithm with known plain text for a different file size in transferring the data of the wireless sensor networks. It shows that HSR15 takes less time when compared to the DES, 3DES, AES, IDEA, RC5 and HSR19.

File Size	DES	3DES	AES	IDEA	HSR19	RC5
23 KB	3.84	3.56	3.01	3.3	2.5	2.6
32 KB	3.59	5	3.08	3.76	2.85	2.9
4 MB	15.03	13.67	10.12	12.17	7.23	8.06
6 MB	16.43	24.31	15.01	13.3	12	12.05

Table 3. Performance analysis of algorithms

5. CONCLUSION

In wireless sensor network to secure the data while transmitting between the intra nodes and the cluster head internodes transmission transferring data is processed and determined the performance by measuring the parameters such that execution time and energy consumption. The evaluation and the performances of AES, DES, IDEA and HSR19 are measured and concluded that HSR19 uses less energy and secure than other algorithm to transmit the data between sensor nodes. Symmetric key is very fast in each operations but the sender and receiver needs to share the same key so the challenging is to providing a security key.

REFERENCES

[1] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall , 2005,PP. 58-309.
[2] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength Against Attacks."I BM Journal of Research and Development, May 1994,pp. 243 - 250.
[3] Ruangchaijatupon, P. Krishnamurthy, "Encryption and Power Consumption in Wireless LANs-N,'' The Third IEEE Workshop on Wireless LANs – September 27-28, 2001- Newton, Massachusetts.
[4] Hardjono, "Security In Wireless LANS And MANS," Artech House Publishers 2005.
[5] W.Stallings, "Cryptography and Network Security4th Ed," Prentice Hall , 2005,PP. 58-309
[6] Ronald L Rivest , "The RC Encryption Algorithm"MIT Laboratory for Computer Science Technology Square Cambridge Mass, March 1997.
[7] K. McKay, "Trade-offs Between Energy and Security in Wireless Networks Thesis," Worcester Polytechnic Institute, April 2005.
[8] D. E. Burgner and L. A. Wahsheh, "Security of Wireless Sensor Networks," 2011 Eighth International Conference on Information Technology: New Generations, Las Vegas, NV, 2011, pp. 315-320, doi: 10.1109/ITNG.2011.62.
[9] Ju Ren, "Adaptive and Channel -Aware detection of Selective Forwarding Attacks in Wireless Sensor Networks, IEEE Transactions on Information Forensics and Security,vol.15,no.5 ,May,2016
[10] M.Dong, "LSCD:A Low storage Clone Detection Protocol for Cyber Physical Systems, IEEE Transactions on Computer aided Design of Integrated Circuits and Systems,vol.35, no.5,May 2016.
[11] Hirani, Sohail A. "Energy consumption of encryption schemes in wireless devices. Diss.

ISSN: 2233 -7857 IJFGCN

University of Pittsburgh", 2003

[12] F. Alfaleh, H. Alfehaid, M. Alanzy and S. Elkhediri, "Wireless Sensor Networks Security: Case study," *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2019, pp. 1-4, doi: 10.1109/CAIS.2019.8769510.

[13] Rizk, R., &Alkady, Y. (2015). *Two-phase hybrid cryptography algorithm for wireless sensor networks. Journal of Electrical Systems and Information Technology, 2(3), 296–313*. doi:10.1016/j.jesit.2015.11.005