Indonesian Journal of Electrical Engineering and Computer Science
Vol. 22, No. 1, April 2021, pp. 361~368
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v22.i1.pp361-368

Adaptive security approach for wireless sensor network using RSA algorithm

Maha Salah Asaad, Muayad Sadik Croock
Control and Systems Engineering Department, University of Technology, Baghdad, Iraq

Article Info

Article history:

Received Oct 16, 2020
Revised Dec 14, 2020
Accepted Jan 17, 2021

Keywords:

AODV protocol
Encryption
RSA algorithm
Security
WSN

ABSTRACT

A type of distributed and self-regulating network is the wireless sensor network (WSN). The sensor nodes have limited computing capabilities, memory, battery power are needed to ensure a strong security design. In this paper, an adaptive cryptographic scheme for WSN that is operating on routing ad hoc on-demand vector routing (AODV) protocol. The adaptive term refers to the adopted mechanism between heavy and light asymmetric cryptography techniques of RSA. The heavy technique adopts the complete version of RSA algorithm, while the light one considers a reduced complexity version. This is to control the security operation over the included nodes even with low power ratio. In various case studies, the proposed scheme is checked and the result obtained shows the high efficiency of results in terms of protection guarantee.

Corresponding Author:

Maha Salah Assad
Department of Computer Engineering
University of Technology
Baghdad, Iraq
Email: 120632@student.uotechnology.edu.iq

1. INTRODUCTION

One of the biggest challenges regarding securing WSN's resource restrictions that are related to power, computational capabilities, and memory is cryptographic RSA algorithm. This algorithm uses public-key to produce data integrity. Data source use the receiver's public key to encrypt data and send them over it. The nodes have to use the receiver key to decrypt the data, and so, just a private key to decrypt the data [1]. Wireless communication topologies are considered in WSN, as the facilities are presented as: reducing infrastructure costs, allowing sensor networks to be deployed in prohibited areas as well [2]. This challenge involves cryptography because it promotes anonymity, confidentiality and identity which, when combining together, provide the foundations of reliable e-commerce and safe communications. In various WSN systems, the AODV protocol has been implemented to demonstrate its accuracy and effectiveness [3]. The AODV network is flexible in nature. It can take various forms and has highly changeable mobile characteristics such as power and transmission conditions. Moreover, encryption algorithms are used to prevent attacks [4].

In this paper, an adaptive encryption approach is proposed for WSN. The proposed approach adopts the residual power ration for source and destination nodes to select he suitable light or heavy RSA algorithm for encrypting the data. This is to guarantee the continuous information sending under satisfied security level. The obtained results from numerous experiments show the efficiency of the proposed approach in terms of accuracy and availability.

2. RELATED WORK

Different researchers have tackled the issues in the security of WSN. In [5], the authors proposed a fast and enforced encryption for WSN using the encryption system of chaos based on the associated map lattice. The main goal was to provide a better lightweight encryption system based on both the genetic operations and the chaotic map. The authors in [6] provided a new approach to encryption by converting the numbers. The algorithm addressed the weaknesses from current public key encryption algorithms, in particular RSA, analyzes the performance of the BB84 quantum encryption algorithm. In [7], a new era of double layer encryption cryptography key was proposed to make a more secure and trusted cloud model worthy of being done a lot of working. In [8], the low-weight and efficient RSA hybrid messaging system (SHRSA) was performed and analyzed with a four-layer authentication stack. The chart solved the problem of very low-level man speed to decrypt RSA, , by using any password, digital certificates that is external, and authentication of a third party using its four important techniques. In [9], the authors tried to improve security by suggesting a common way of a key-sharing algorithm with RSA encryption technology algorithm to encrypt data in cloud computing between the user and the cloud. In [10], current quantum computing algorithms were presented based on (symmetric and asymmetric) encryption schemes, discrepancies between quantum and traditional computing. In [11] cryptography used in wireless sensor networks (WSNs) was suggested in starting with a symmetric key encryption theme and a Diffie-Hellman key agreement protocol for exchanging secret keys. In [12], application of ECC was applied a midwife encryption technology on the famous WSN operating system. Using the TinyECC library, the functional implementation of ECC operations was completed. In [13], an algorithm to reduces the public/private key pairs for each request was proposed. It aimed to reduce the power consumption of the mass head. In [14], safe data transfer is a critical issue, thus, data transfer and security issues were suggested in CWSNs. Two stable and efficient data transfer protocols were introduced by the authors, for different methods. An efficient and robust authentication approach, based on elliptic curve encryption and the ElGamal signature scheme, was introduced in [15]. It could be applied to any messages to provide the authenticity of the hop-by-hop message content without double the built-in threshold of the chart based on the many boundaries. In [16], few positive results was shown to secure from the attacks like DOS attacks, part attack, grey hole attack altogether the results of this paper have positive over the normal secure system like a watchdog. In [17], discussing the art of researching sensor networks that deal with security-related problems was proposed. Protocols such as LEACH, which are data transfer protocols based on clusters, face a number of security issues. Adding security to these protocols was a little difficult because it arbitrarily rearranges network groups and data links, sometimes and aggressively. In [18], the intermediate nodes could use remote node IDs and message encryption. In traditional public key infrastructure schemes, these strategies may not have been feasible in conventional public-key infrastructure systems, as the middle malicious node would never send the public-key certificates of its neighbors. In [19], a cross-layer design plan should be considered for key allocation to facilitate secure key exchange. In [20], the proposed RSA scheme for defending the network against DoS attacks has been discussed in detail. Simulation results showed that RSA was very stable against DoS attacks to reduce the energy consumed and increase the network lifetime. In [21], this paper was proposed that the performance of security based on RSA algorithm with AODV for prohibiting bogus information or false data injectable attack in wireless sensor network.A new concept of using different base points of an elliptical curve (i.e., shared key) to create different pseudorandom bit sequences for two connecting nodes was proposed by the authors in [22, 23]. In [24, 25], authors presented a modified hash function in a modified academic that includes a WSN hash sponge. In [26-28], the charts were not secure in RSA when the encryption ace is small.

3. THE PROPOSED APPROACH

As mentioned above, an asymmetric cryptography technology, applied in AODV based WSN, is proposed. It aims to provide how to better achieve WSN security design with extensive knowledge of cryptography. This section can be divided into two subdivisions to facilitate reading flow.

3.1. Proposed method architecture

The proposed method uses RSA algorithms to produce a distinct option that can mange the exchange the encryption in the WSN. The design of the proposed method is presented in three stages:

a) Key generation stages: The cryptography is simulated between the nodes, included in WSN, where the key size is 256-bit. In this method of cryptography, the source of information is constructed, securely shared easily. One of them is the private key, while the other is public, which is the one which exchanged, as shown in Figure 1.
b) Encryption/Decryption stages: One of cryptography's principles is encryption, where the sender employes the public key in encrypting the information when the information is submitted. The private key is utilized

in order to decrypt the information in a way of readable format until the receiver has access to encrypted information, as shown in Figure 2.

c) Adaptive cryptography stages: The proposed method considers the power battery of the source and destinations. In case that the minimum power is lower than 60%, the method adopts the light algorithm. Otherwise, if source and distenation have apower of 60% and more, the method uses heavy algorithm as explained in Figure 3.

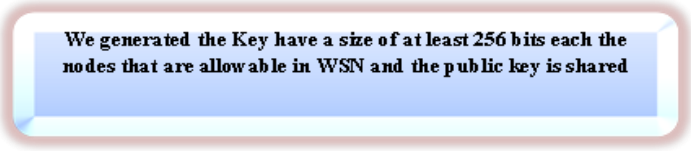

Figure 1. Key generation stages

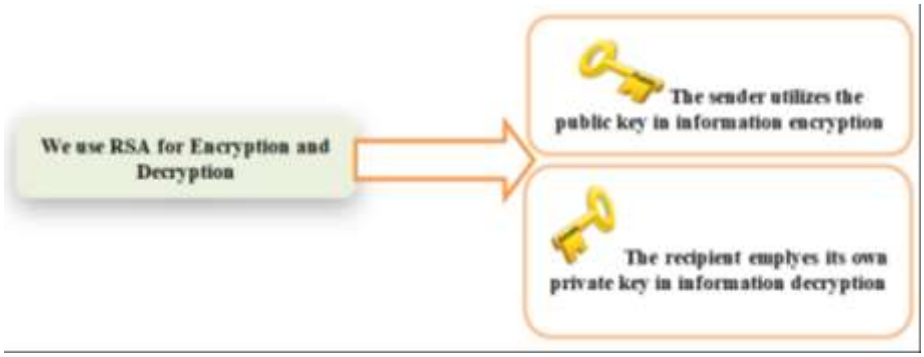

Figure 2. Encryption/Decryption

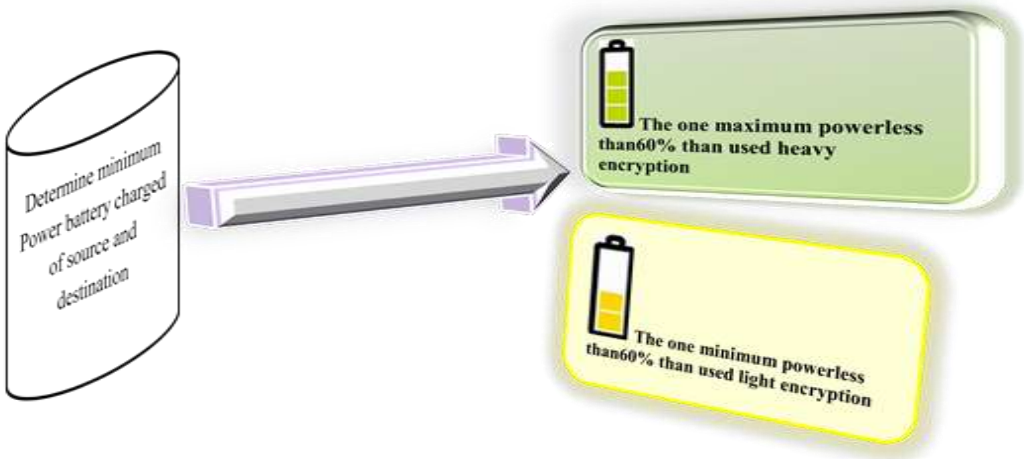

Figure 3. Adaptive cryptography stages

3.2. Proposed Method Algorithm

The proposed method is presented in flowchart, shown in Figure 4. MATLAB is employed in establishing the adopted WSN to simulate the required environment. It can be explained in numerous steps:

a) The sensor nodes are randomly allocated in the established environment.
b) A symmetric key with a size of 256-bit is generated inside the involved nodes that are employed the RSA.
c) AODV protocol finds possible paths between the source and destination and selecting the shortest path as optimal choose.

d) Transfeering time of data as well as the size of it are computed. In addion, the battery power level is evaluated.
e) Both source and destinations nodes compute their own power. In case that one of them has power less than 60%, the choosing of light algorithm is performed. Otherwise, the selection is heavy version.
f) Data encryption process (source node side) is started to encrypt the information by applying the public key. Then, at the time the recipient has access to encrypted information; the recipient's secret key is applied to decrypt the information to be in a readable format.

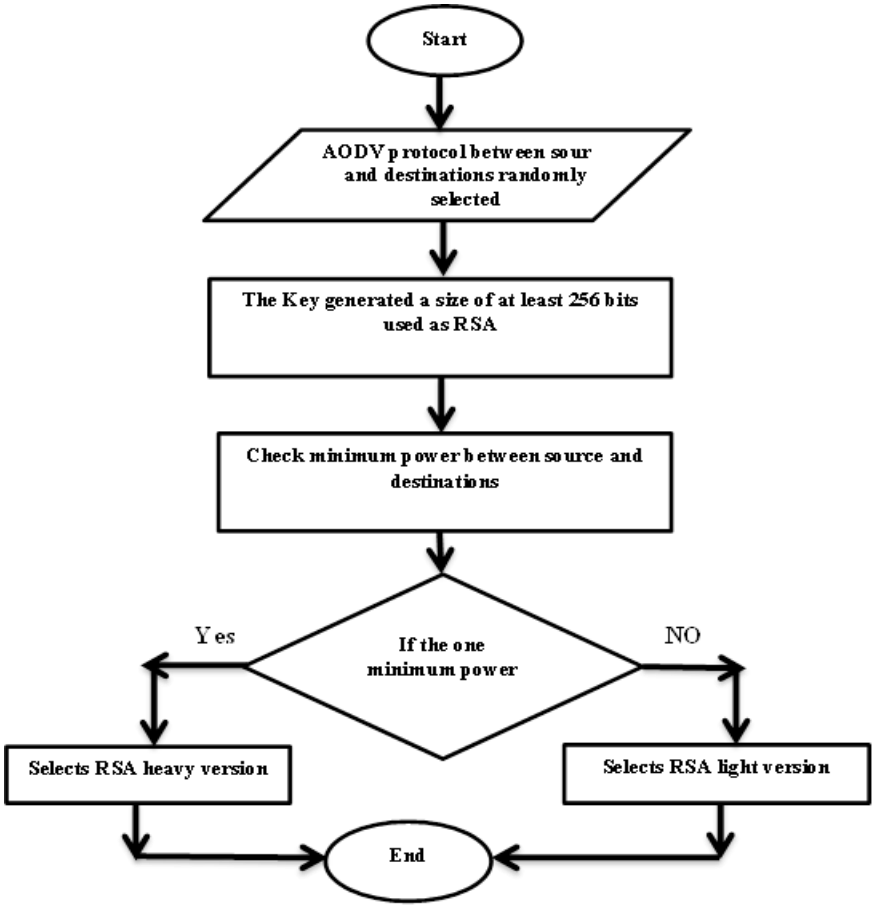

Figure 4. Proposed cryptography algorithm

4. RESULTS

As mentioned earlier, MATLAB and AODV as well as RSA method are employed in testing the proposed approach. The following steps are adopted in simulation:

a) The creation of WSN: It includes a number of sensor nodes that is generated by entring different parameters as shown in Figure 5. These parameters and the involved data are considered in this step for realizing the proposed environment.
b) The public key is generated and distributed over the included nodes as illustrated in Figure 6. These nodes have a unique key of 256-bit size, used for performing the proposed method.
c) The data is now encrypted in each node with a public key of 256-bit. It also decrypted employing the allocated private key. Figure 7 explains the requested messages, where the proposed method evaluates the required size of data and needed transmission time and battery power.
d) The proposed method computes the power of source and destinations to implement the selection of light and heavy versions of algorithm as illustraited in Figures 8 and 9.
e) Figure 10 shows the implementation of light RSA version, while Figure 11 explains the use of heavy RSA version.

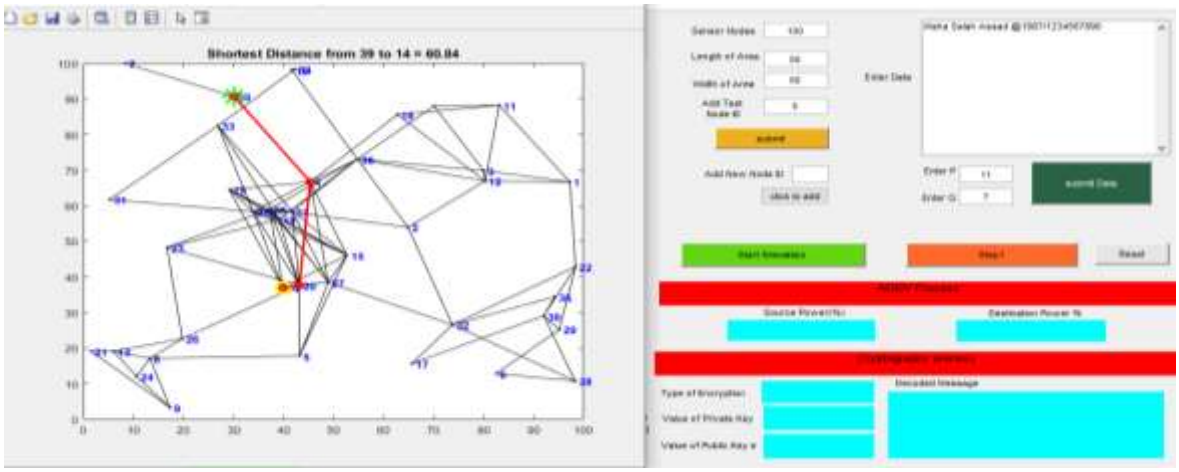

Figure 5. The creation of the adopted WSN

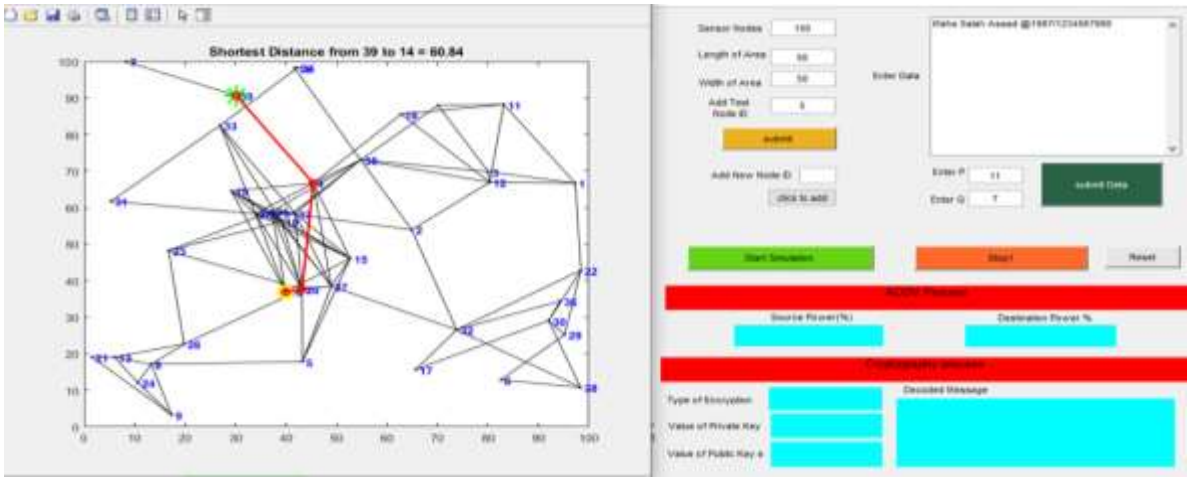

Figure 6. Adding a random key of 256-bit

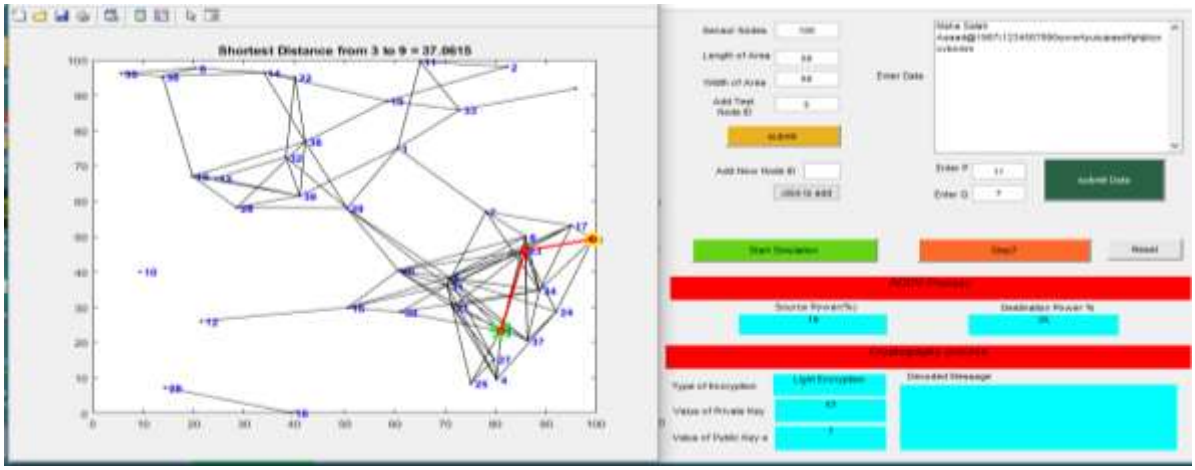

Figure 7. The requested messages to be transferred

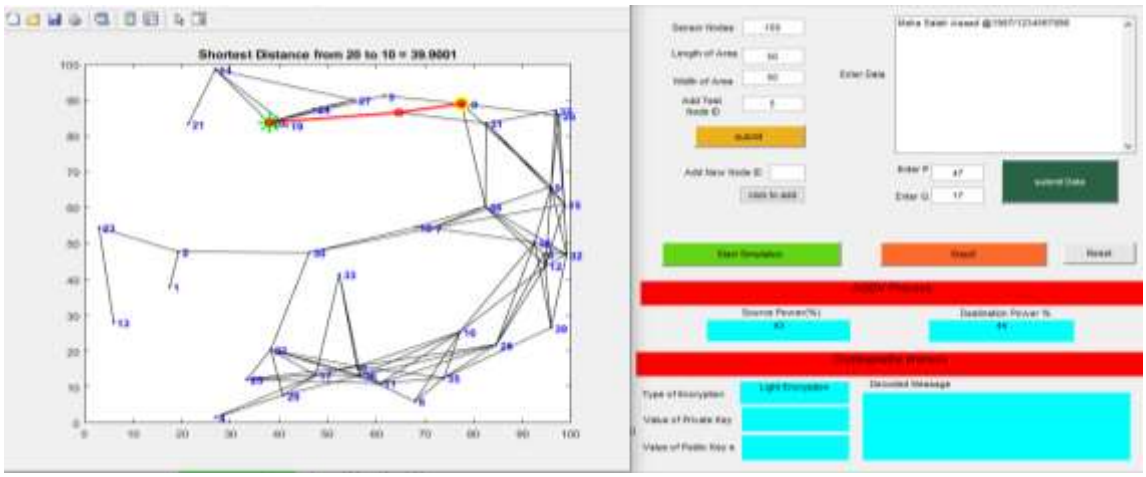

Figure 8. The selection of light version

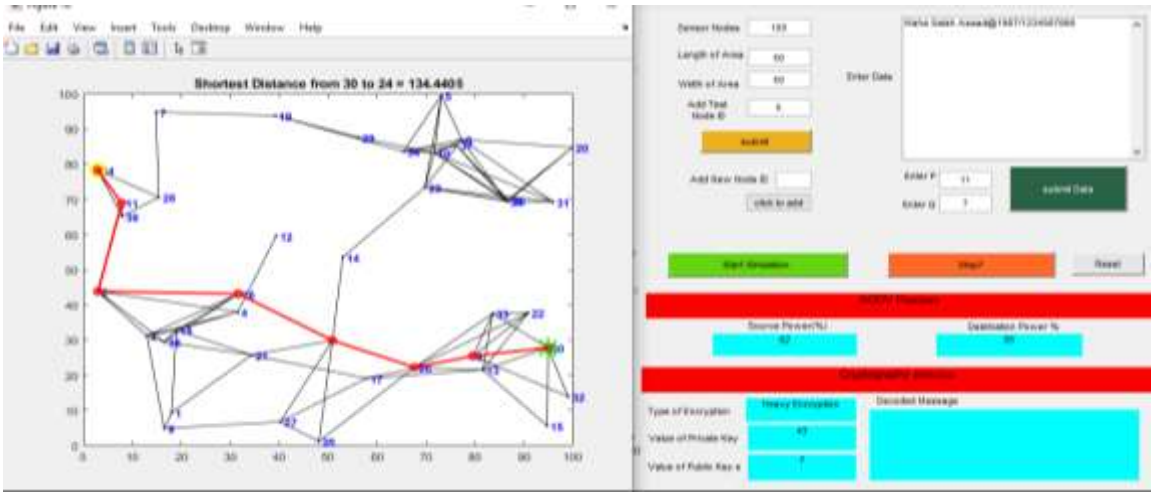

Figure 9. The selection of heavy version

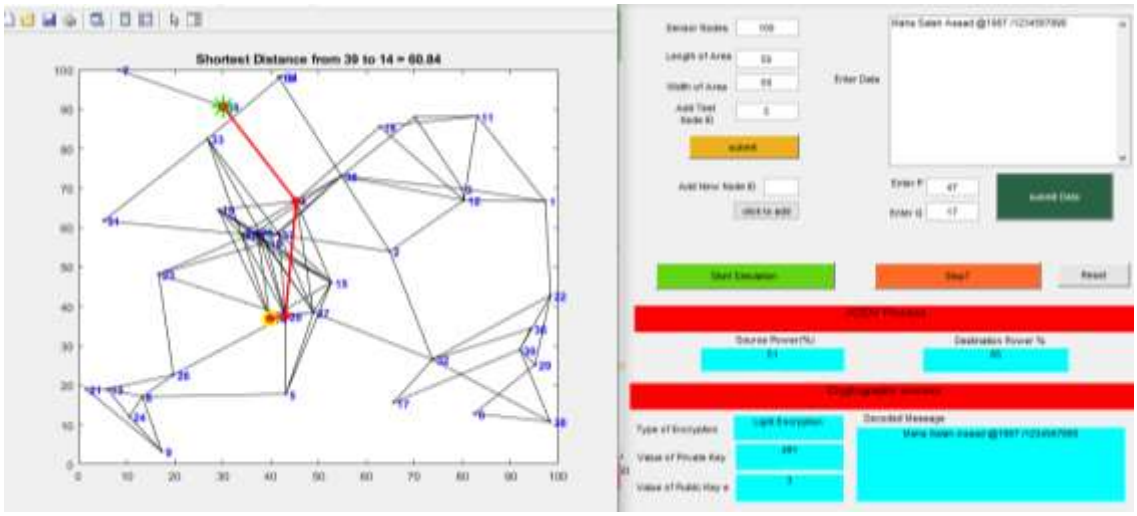

Figure 10. The encryption and Decryption process

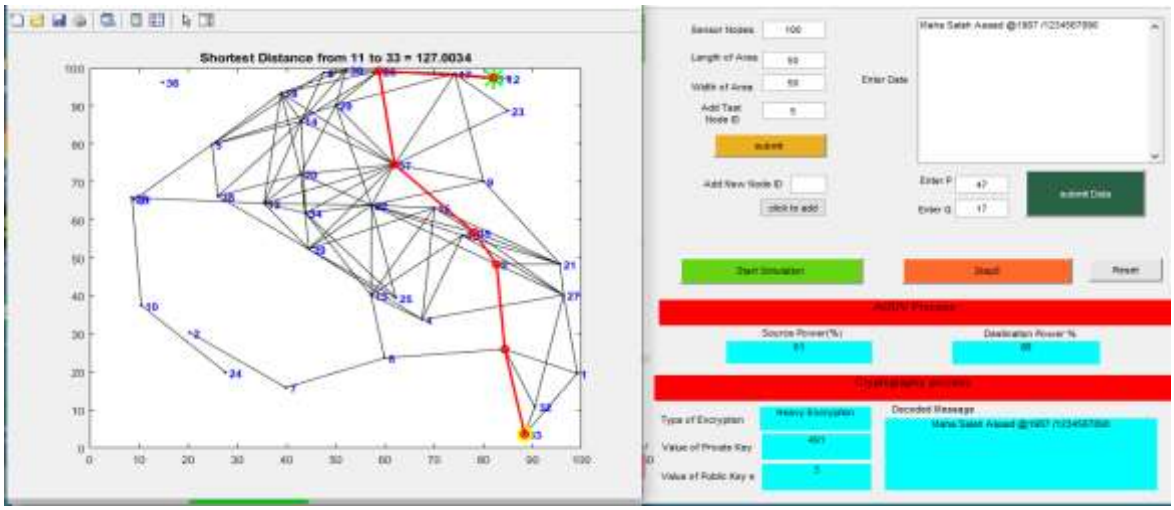

Figure 11. The encryption and Decryption process

5. CONCLUSIONS

An adaptive security approach has been proposed for WSN based on heavy and light versions of RSA algorithm. The selection of one version provided the system with high adaptively toward managing the encryption of data in which the continuous is guaranteed. A simulator was proposed for performing the WSN with the presented security method. It was built using MATLAB environment with the property of graphical user interface (GUI). The proposed approach has been tested over all the processing steps of the encryption and decryption and the efficient performance of the proposed system was presented by the results obtained.

REFERENCES

[1] J. Chen and J. Wu, "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks", Florida Atlantic University, 2019.
[2] M. Reena, S. Satpute, M. Tech, and C. S. E. 3rd, "Survey on Security in Wireless Sensor Networks Using Elliptical Curves Cryptography; Survey on Security in Wireless Sensor Networks Using Elliptical Curves Cryptography," *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 10, 2013.
[3] K. Spurthi1 and T. Narayan Shankar," A Survey of Intrusion Detection System in Manets using Security Algorithms", *International Journal of Applied Engineering Research*, vol. 12, no. 24, 2017.
[4] Dr. Indumathi .J1 , Anish A2 "Secure Data Transmission through Trusted Node in Mantes using AODV Routing Algorithm: SATEM" *International Conference on Cryptography and Security, ICC*, 2014.
[5] Aakash Dutta, 2K. Naveen Kumar, 3N. Sai and 4Radhika Rani Chintala," An Efficient Light Weight Cryptography Algorithm Scheme for WSN Devices using Chaotic Map and GE," *International Journal of Pure and Applied Mathematics*, vol. 118, no. 20, 2018.
[6] Astrid Rivera Partida, Diego Villatoro Geronimo, "A New Age Beyond of Classical Encryption", *Applied Mathematics Tecnologico de Monterrey School of Engineering and Science*, vol. 6, 2019.
[7] D.Usha, M.Subbbulakshmi, "Double Layer Encryption Algorithm Key Cryptography for Secure Data Sharing in Cloud," *International Journal of Scientific & Engineering Research*, vol. 9, no. 5, 2018.
[8] Aniruddha Bhattacharjy, Xiaofeng Zhong, and Xing Li, "A Lightweight and Efficient Secure Hybrid RSA (SHRSA) Messaging Scheme With Four-Layered Authentication Stack," *Beijing National Research Center for Information Science and Technology*, 2019. doi: 10.1109/ACCESS.2019.2900300
[9] Md Equebal Hussain, Mohammad Rashid Hussain, "Securing Cloud Data using RSA Algorithm," Suresh Gyan Vihar University, 2018.
[10] Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang, "The Impact of Quantum Computing on Present Cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018. doi: 10.14569/IJACSA.2018.090354
[11] Thomas M. ChenThomas M. ChenJorge BlascoHarsh Kupwade PatilHarsh Kupwade Patil., "Mission-Oriented Sensor Networks and Systems:Cryptography in WSNs," 2019.
[12] N. Saqib and S. Singh Shekhawat, "Securing Wireless Sensor Networks Using Elliptic Curve Cryptography," *Int. J. Eng. Trends Technol., International Journal of Engineering Trends and Technology (IJETT)*, vol. 56, no 1, 2018. doi: 10.1109/ICCNIT.2011.6020911
[13] S. Singh Gaur, A. K. Mohapatra, and R. Roges, "An Efficient Certificateless Authentication Encryption for WSN Based on Clustering Algorithm," *International Journal of Applied Engineering*, vol. 12, no. 14, pp. 4184-4190, 2017.

[14] Ms. Gauri P.Heda, Prof. Imran R. Shaikh, ”An Overview on Digital Signature Based Secure Data Transmission for Cluster WSN,” vol. 1, no. 4, July 2016,
[15] M. Manjusha, A. Prof, M. Laxmi, B. Rananavare, and A. Prof, “A Robust Message Authentication Scheme In Multihop WSN Using Elliptical Curve Cryptography And Elgamal Signature,” *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no 7, 2013.
[16] K. Spurthi1, and T. Narayan Shankar2, ”A Survey of Intrusion Detection System in Manets using Security Algorithms,” *International Journal of Applied Engineering Research*, vol. 12, no. 24, 2017.
[17] M. Reena, S. Satpute, M. Tech, and C. S. E, “Survey on Security in Wireless Sensor Networks Using Elliptical Curves Cryptography; Survey on Security in Wireless Sensor Networks Using Elliptical Curves Cryptography,” *International Journal of Computer Science Engineering (IJCSE)*, vol. 3, no. 06, 2014.
[18] H. Kupwade Patil, J. Camp, and S. A. Szygenda, "Identity based authentication using a Cross Layer Design approach in Wireless Sensor Networks," in *World Multiconference on Systemics, Cybernetics and Informatics (WMSCI 2011)*, 2011.
[19] H. Kupwade Patil and S. A. Szygenda, "Identity based key distribution schemes using a Cross Layer Design approach in Wireless Sensor Networks," in *Proc. of Intellectbase International Consortium*, vol. 15, pp. 109-118, 2011.
[20] Reza Fotohi1, Somayyeh Firoozi Bari2, Mehdi Yusefi3, ”Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol,” Faculty of Computer Science and Engineering, Shahid Beheshti University, Tehran, Iran, 2018. doi: 10.1002/dac.4234
[21] Vishwaraj1 and Bharath.S, ”Securing WSN From False Injection Data Attack Using RSA Based Security System,” *College of Engineering*, India, vol. 6, no.3, pp. 2319-6629, 2017.
[22] Kamanashis Biswas, Vallipuram Muthukkumarasamy, Elankayer Sithirasenan, and Kalvinder Singh, ”A Simple Lightweight Encryption Scheme for Wireless Sensor Networks,” Australia Development Lab and Griffith University Gold Coast, 2015.
[23] M Lavanya and V Natarajan, Lwdsa, “light-weight digital signature algorithm for wireless sensor networks,” *Sadhana*, vol. 42, no. 10, pp. 1629-1643, 2017. doi: 10.1007/s12046-017-0718-5
[24] Santanu Sarkar and Subhamoy Maitra, ”More on Correcting Errors in RSA Private Keys: Breaking CRT-RSA with Low Weight Decryption Exponents,” *Applied Statistics Unit*, Indian, 2019.
[25] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, ”Cryptography Engineering Design Principles and Practical Applications,” Wiley Publishing, Inc., 2010.
[26] Muhammed Enes Bayrakdar, ”Cooperative communication based access technique for sensor networks,” *International Journal of Electronics*, vol.107 , no.2, pp. 212-225, 2020. doi: 10.1080/00207217.2019.1636313
[27] Muhammed Enes Bayrakdar, ”Exploiting cognitive wireless nodes for priority-based data communication in terrestrial sensor networks,” *ETRI Journal*, vol. 42, no. 1, pp. 36-45, 2020. doi: 10.4218/etrij.2019-0296
[28] Muhammed Enes Bayrakdar, “Rule Based Collector Station Selection Scheme for Lossless Data Transmission in Underground Sensor Networks,” *China Communications*, vol. 16, no. 12, pp. 72-83, 2019. doi: 10.23919/JCC.2019.12.005