DOI: https://doi.org/10.33103/uot.ijccce.20.4.5

Developed Authentication Method for Wireless Sensor Networks Based on Lightweight Protocol

Maha Salah Asaad[1], Muayad Sadik Croock[2]
[1,2] *Computer Engineering Department, University of Technology, Baghdad, Iraq*
120632@student.uotechnology.edu.iq , Muayad.S.Croock@uotechnology.edu.iq

Abstract*—Wireless Sensor Networks (WSNs) can be the most important solution for several problems, particularly in emergency cases. Software engineering security for WSN can confirm four goals including confidentiality, integrity, authentication, and availability. In this paper, an authentication method for WSN is proposed based on lightweight authentication and key management protocol as well as concepts of software engineering. Moreover, the interleaving process is added to the adopted protocol to improve the security side. The proposed method uses a Kath hashing in addition to salt and hash: the MD5 algorithm. This is to provide an allowance for the authentication of the added node to join the network. The proposed method is tested over different case studies and the obtained results show the superior performance for it in terms of processing the added nodes.*

Index Terms*— Security WSN,Authentication Method,lightweight authentication and key management protocol*

I. INTRODUCTION

The dynamic network topology most likely came from the transient feature of wireless media and nodes' mobility aspects. Hence, the security of the moving sensor must be integrated with the WSNs. The security of key occupies an important place in the communication of WSN [1]. In Ad-Hoc WSN networks, nodes can change positions quite frequently. Thus, WSN is more vulnerable to attack than wired networks [2]. The security needs in WSNs have been addressed in spite of t the proposed several authentication techniques. [3].Research on routing protocols has been raised recently along with the security technologies development in WSNs. Especially, the master key-based management protocols that include Localized Combinatorial Keying (LOCK), and enhanced security protocols of sensor networks. Such as, SPINS, and BROSK which can be considered as the most recent ad hoc key management protocol when it compared to SPINS. [4]-[5]. In this area, these protocols have been widely debated [6]. According to In [7], an IoT displays the LAKD authentication protocol for the M2 M link. The idea is that the low computational cost could be sufficient for resource-constrained IoT devices. Besides this, the lightweight XOR, add, deduct, and the hash feature is used. The security protocol protection was evaluated using AVISPA tool and BAN logic, which verified the aim of mutual authentication. Its resistance to replay and MITM attacks. The new scheme was used in [8] to resolve weaknesses and obstacles to the new scheme, offering shared authentication and master agreement, and presents secure access to cloud servers. The main aim of node authentication is to effectively protect the nodes from attacks that caused by malicious nodes. A network structure consisting of the base station, cluster head and group of nodes was suggested by the author of [9]. A unique fingerprint for each sensor node was created [10] before actual deployment occurs for each of the nodes in the network. The authors in [11] speculated that there is a successful, lightweight health monitoring scheme planned for the purpose of IoT and Radio Frequency Identification (RFID) tags. This technique was applied for dual-

Received 5 June 2020; Accepted 9 July 2020

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

band RFID protocols. Which are high-frequency factor of 13.56MHz and are useful for scan individuals .there is also 2.45 GHz microwave bands that applied to monitor corporal data. In addition to that, the authors remarked, that a hyper-elliptic curve-base, regarding secure IoT node that is integrated RFID mobile health care system, could be utilized to ensure security besides the server and doctors According to the team in [12], there is a novel approach of light authentication protocol based on a password, smart card and biometric recognition. This method accomplishing mutual authentication that is required among User, GWN and sensor nodes. A biometric definition may acquire non-disclaimer aspects due to gaining protection following the analysis of the security. Then, the authors proposed three factors of user authentication protocol to understand information regarding IoT. The proposed protocol cans provide an authentication method that is quick and with no need to biometric models. In [13] the light version was used by authors to resolve the security weakness of symmetric key-based authentication techniques to provide a new, effective broadcast authentication. This was based on the data structure of the Bloom filter in order to minimize contraction overload, to minimize hash function collision by getting benefits of collision resolution for the values stored and very high resistance against collision attacks. In [14], the proposed scheme was performed depending on the ratio of 50% of dead nodes among the total ones to be triggered. To maintain the WSN in high performance to work, a simulation was adopted to emulate the protocols adopted and the blueprint provided without the need for traditional ones of NS2 and NS3. In [15] the zero-knowledge protocol was used to provide an authentication mechanism for a sensor node in WSNs. By using this technique, the keys are hidden from the attacker during the authentication. Thus, the attacker would be unaware of the keys, the purposed method is using a rekeying system with a node authentication scheme that applies dynamic keys. A suggested technique may also minimize the numerous attacks occurring on WSNs. The results have shown that this technique is very effective. In [16], the authors suggested techniques that involve principles that provide complete Mobile Ad-Hoc Networks (MANETs) cryptography services. The policy that suggested is the Stable Light Weight Encryption Protocol for MANET. Where an algorithm is executing to present availability with Do's elasticity in order to avoid TCP SYN flood attacks in the network and so the authentication code and the hash function is created. In [17] this job was organized with a new node authentication using a hashing mechanism. The parameters of software comparison produced a high throughput (minimum delay). Both the gate equivalents (GE) and power consumption were at their minimum rate. Cryptographic principles were combined using two scenarios. As claimed by authors in [18], the work was defined by PAuthKey protocol and authentication protocols development. This work provides a discussion of two groups of keys that are related to the secure group connection protocols of IoT sensor networks.at last, a collaborative method of HIP protocol is presented and named the CHIP besides an efficient key creation method. In [19], many research papers, regarding trust and authorization issues in the distributed environment are addressed. The principle of key design that is involved in the distributed authorization service development is also outlined. Further, the introduced system is presenting the described architecture of distributed authorization related to web services, and it showed implementation using. NET framework. In [20], the authors stated that there is an approach which could be used to be applied in different kind of networks. Notably, it could be used to design and create security associations at the application layer. A simulation study of ad-hoc networks, with TCP being the transport protocol, was presented in [21]. Employing four different mobility models, the authors identified some counterintuitive results, which they justify by measuring the interdependence at the physical, network, and transport layers. This paper provides a basic integration method to present complete WSN authentication services. The proposed approach tackles the problem of authentication in WSN based on software engineering methodology using a lightweight protocol authentication and key management [22]. The new nodes send requests for the closer nodes for joining the WSN and the proposed method processes the requests for being sure from the authenticated new nodes. The proposed approach is tested using numerous case studies. The results prove the claim of the proposal in terms of authentication.

Received 5 June 2020; Accepted 9 July 2020

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

III. PROPOSED SYSTEM

As mentioned above, the proposed system presents an authentication method that aims to provide mutual authentication between sensor nodes and the added nodes. This section can be divided into two sub-sections for easing the reading flow.

A. SYSTEM STRUCTURE

The proposed method adopts a lightweight protocol for mutual authentication and key management for secure communication between sensor nodes and the added nodes in the WSN. The architecture of the proposed method is divided into three phases as follows.

- **Network Initialization phase**: In this phase, the authentication was simulated between the nodes that are allowable in WSN (i.e. there is a network with (40 nodes) as shown in FIG. 1. If there is a new node with an ID of 8bit try to enter into the network, it then sent a request to close node that is a part of the network. The new node encrypts its ID number which is 8-bit by (salt and hash: you can use the MD5 algorithm) and generates the 128bit hash value then sends the hash value to the neighbor node, requesting the authentication to access the network.

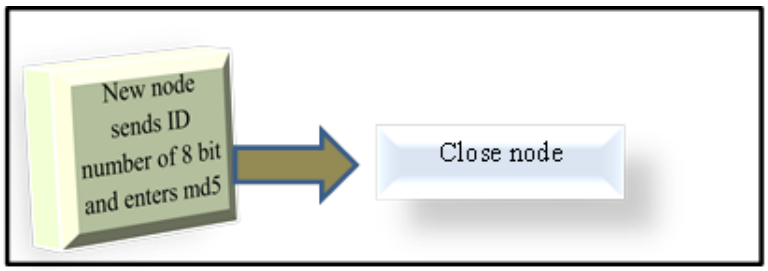

FIG. 1 NETWORK INITIALIZATION PHASE.

- **Key Establishment and Management phases**: In this phase, the closest node checks the received ID if it is included in the authenticated list as shown in FIG.2. Then, it generates a 128-bit salted hash to be combined the received ID (128-bit key hash) with generated 128-bit hash using (interleaving method) to generate new (256-bit key hash). It then sends this new key again to the new node.

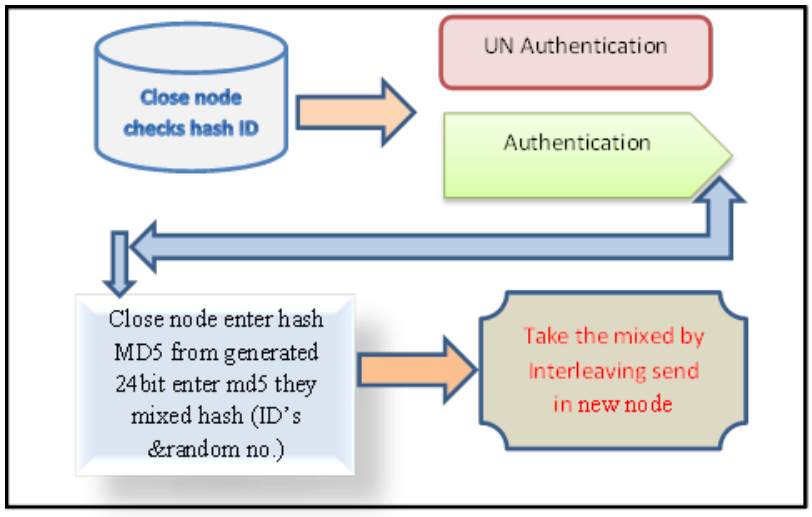

FIG.2. KEY ESTABLISHMENT AND MANAGEMENT PHASES

Received 5 June 2020; Accepted 9 July 2020

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

- **Authentication phases**: In this phase, the close node receives the 256-bit key from a new node to start the de-interleaving process for returning the 128-bit salted hash of the neighbor node and sent it again to the neighbor node to be checked with the original one for providing the authentication. FIG.3. explains this phase

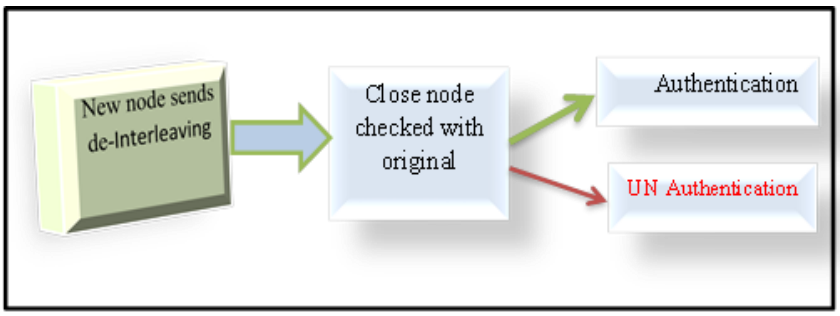

FIG.3.AUTHENTICATION PHASES

B. PROPOSED FAULT TOLERANCE ALGORITH.

The proposed algorithm of the authentication method is explained as a flowchart in FIG.4. This method can be classified into the following steps:

1. The new node sends a request message with its own ID number of 8-bits tries to enter the network to the closest node of the underlying WSN. The sent message is hashed using the Kath hashing function.

2. The close node receives the sent message to check the ID of the new node if it is included in the acceptance list. This list is initiated by the adopted company. If the ID is not included, then the new node is rejected and authenticated. IN case that the ID is included in the list (allowable ID), if the node ID in the list, then it will generate a 128-bit salted hash, and then combined the received ID (128-bit key hash) with the generated 128-bit hash by using (interleaving method) to generate new (256-bit key hash), them sending this new key again to the new node.

3. After a new node received the 256-bit key it starts the de-interleaving process to return the 128-bit salted hash of the neighbor node and sent it again to the close node.

4. The close node checks the received 128-bit with the original key for double-checking. In case there is no match, the new node is rejected and unauthenticated. While if there is a match, the new node is authenticated and joined the WSN.

Received 5 June 2020; Accepted 9 July 2020

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

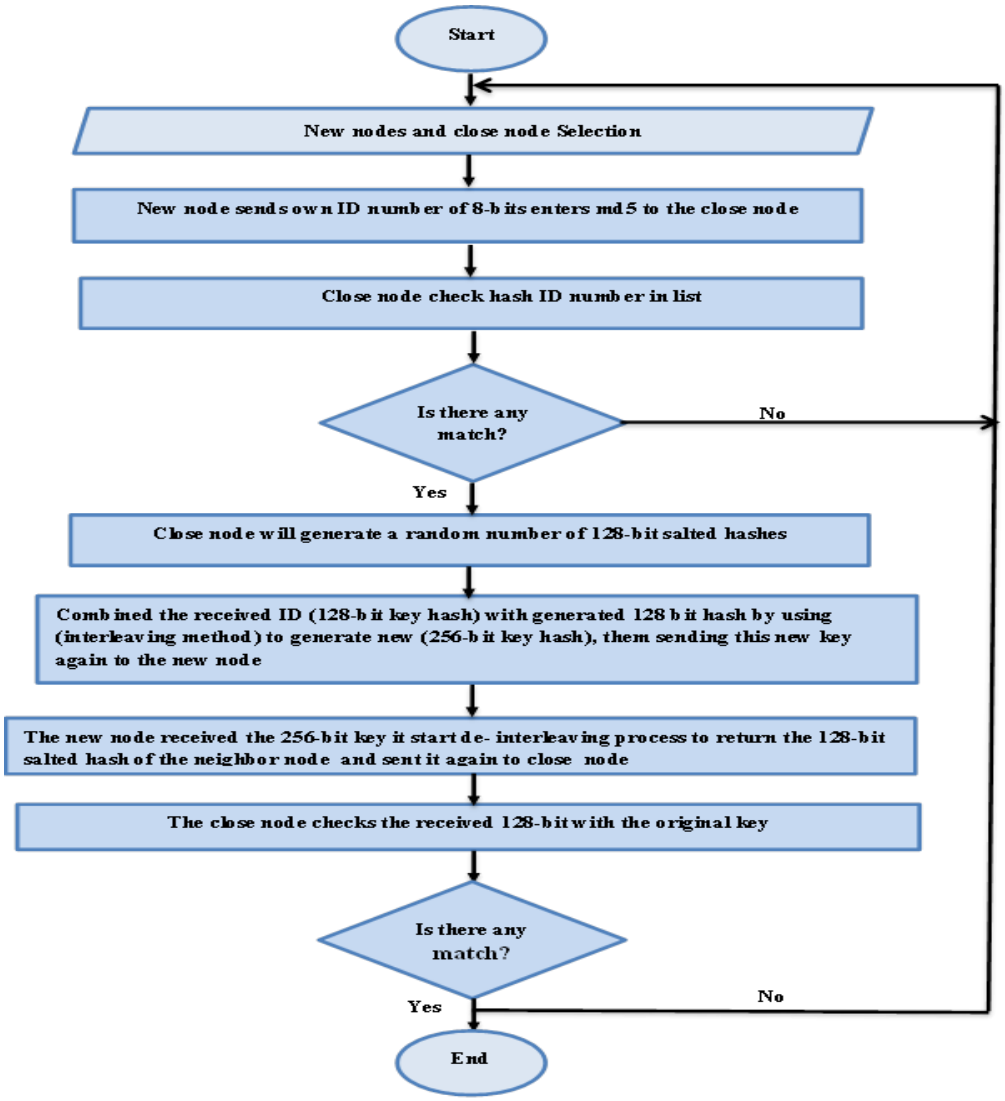

FIG.4 AUTHENTICATION ALGORTHIM

IV. SIMULATION RESULTS

In order to test the proposed authentication method, the MATLAB environment was adopted to produce a simulator based on Ad hoc On-Demand Distance Vector (AODV) as a routing protocol and lightweight protocol for authentication and key management. The simulator performs the following steps:

1. WSN design includes a range of sensor nodes. At the first stage, the number of sensor nodes is entered. Then, the proposed simulator performs the creation of the WSN with mobility to apply the AODV as shown in FIG.5.

Received 5 June 2020; Accepted 9 July 2020

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

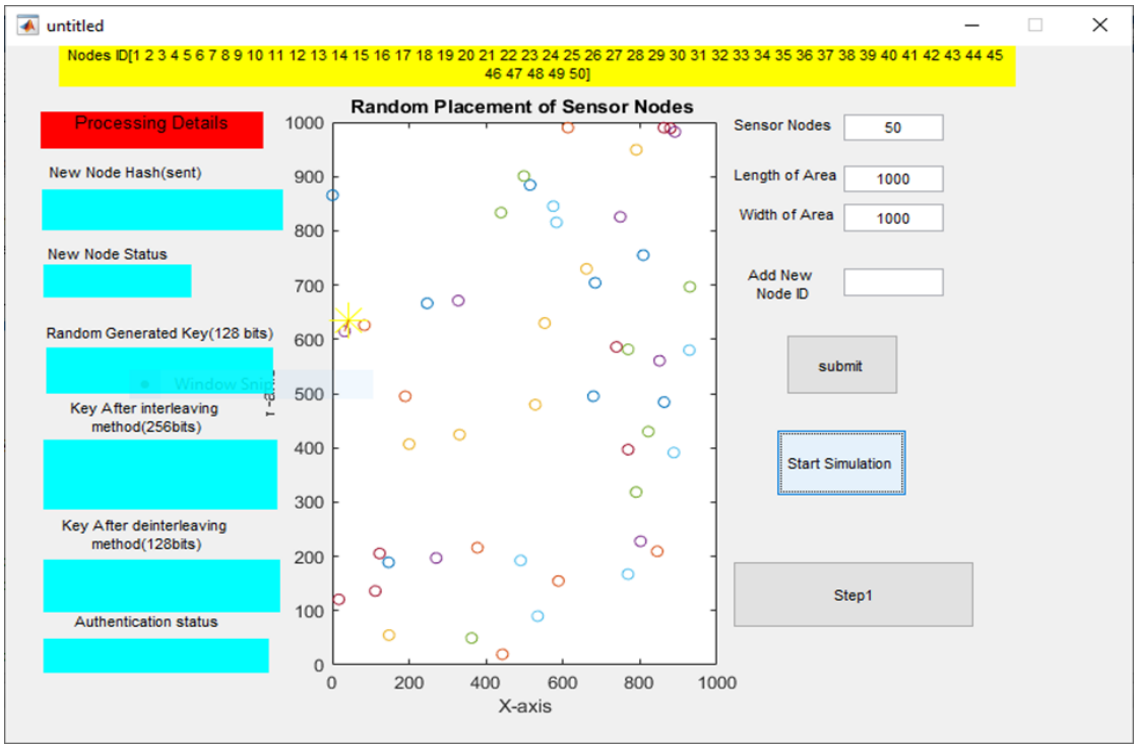

FIG.5. THE CREATION OF THE ADOPTED WSN.

2. The simulator adds new nodes as new nodes that can be seen in FIG.6. Each node has its own ID of 8-bit and can perform its part of the proposed algorithm explained before.

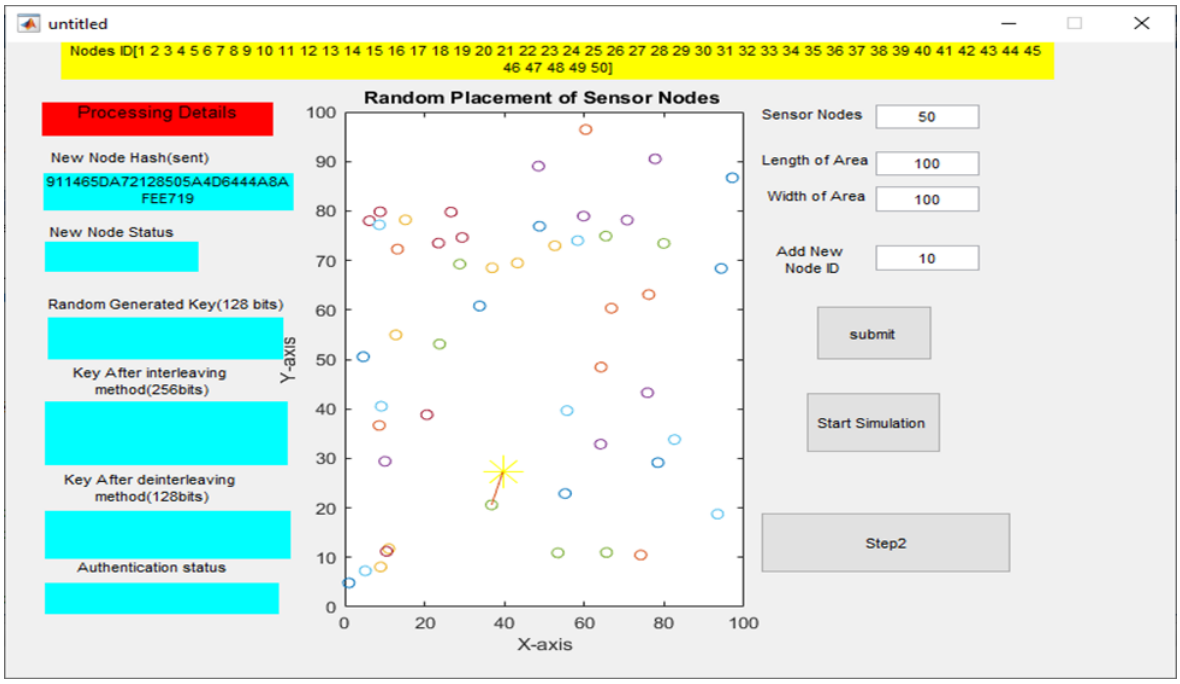

FIG.6. THE ADDED NEW NODE IN YELLOW COLOR.

3. Following the proposed authentication algorithm, the new node sends an ID number of 8-bit try to enter to network, it then sent a request to the closest node that is a part of the network, thus the closest node should request authentication. The new node encrypts its ID

Received 5 June 2020; Accepted 9 July 2020

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

number which is 8-bit by (salt and hash: the MD5 algorithm was used) and generate the 128bit hash value then sends the hash value to the closest node, requesting the authentication to join the WSN. FIG.7. shows the requested messages.

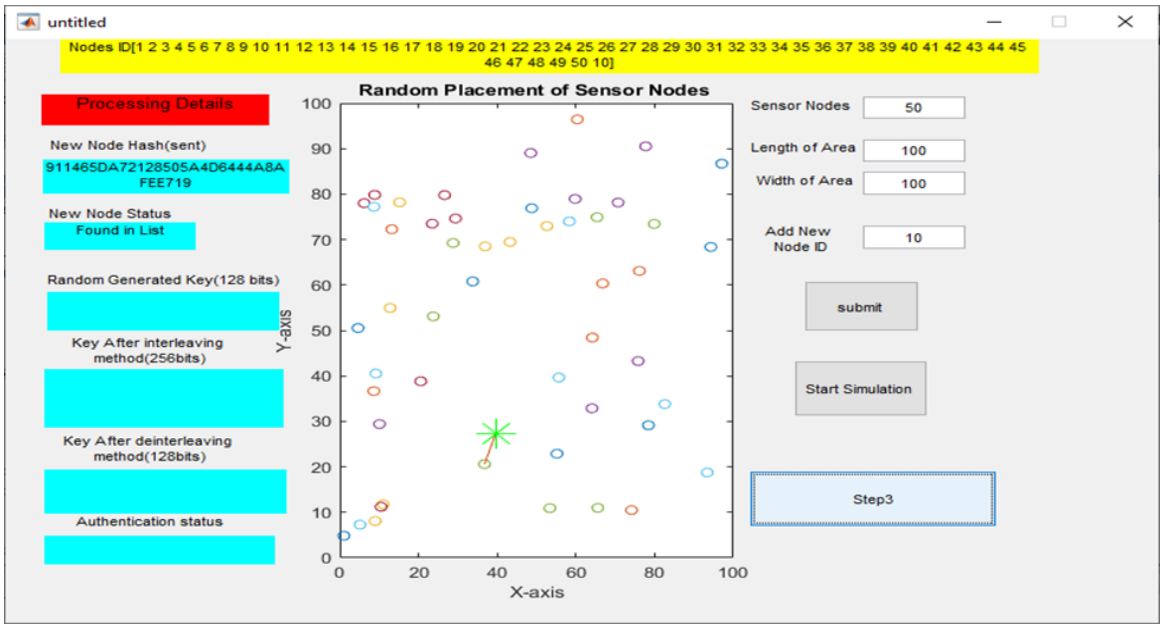

FIG.7. THE REQUESTED MESSAGES

4. The neighbor node should have the same hashing algorithm to compare the hash with the node ID list (allowable ID), if the node ID in the list, then it will generate a 128-bits salted hash. The combined the received ID (128-bits key hash) with generated 128 bit is hashed using (interleaving method) to generate new (256-bits key hash), then it sends this new key again to the new node as shown in FIG.8.

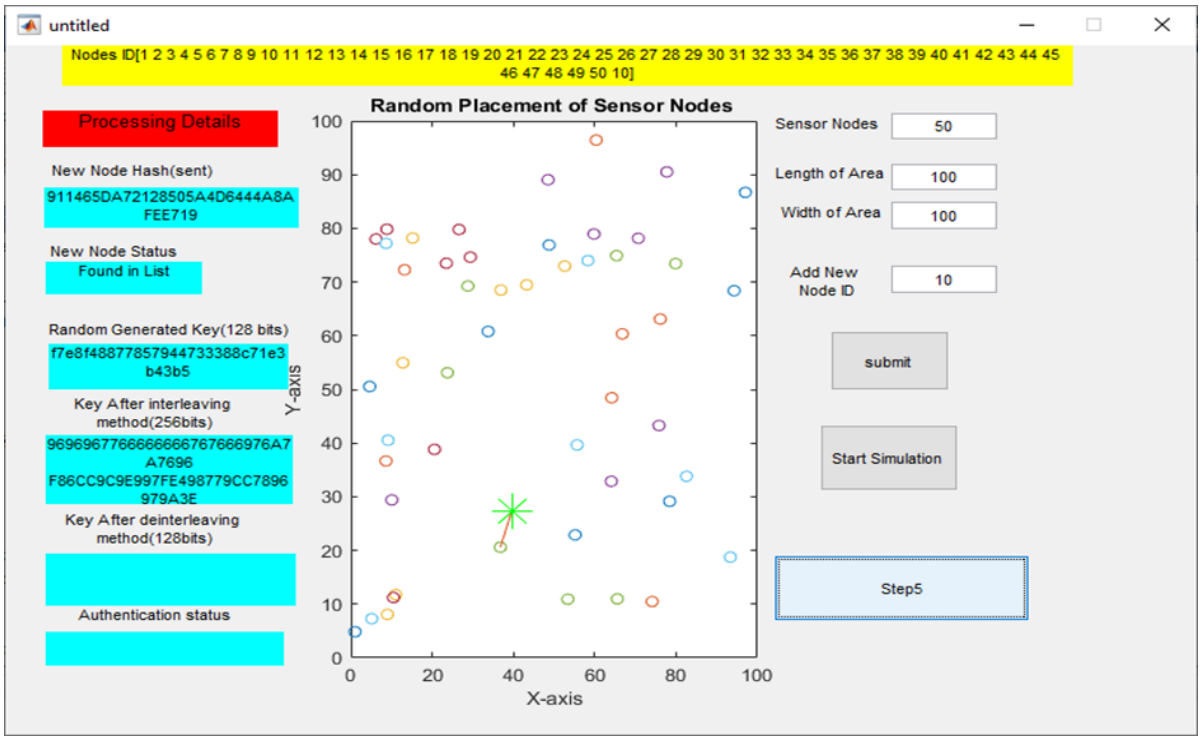

FIG.8. THE INTERLEAVING METHOD

Received 5 June 2020; Accepted 9 July 2020

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

5- After the new node received the 256-bit key it starts the de-interleaving process to return the 128-bit salted hash of the neighbor node and sent it again to the neighbor node (B) to verify it is the same then accept access if it is passed or prevent connection if it is a field. As shown in FIG.9.

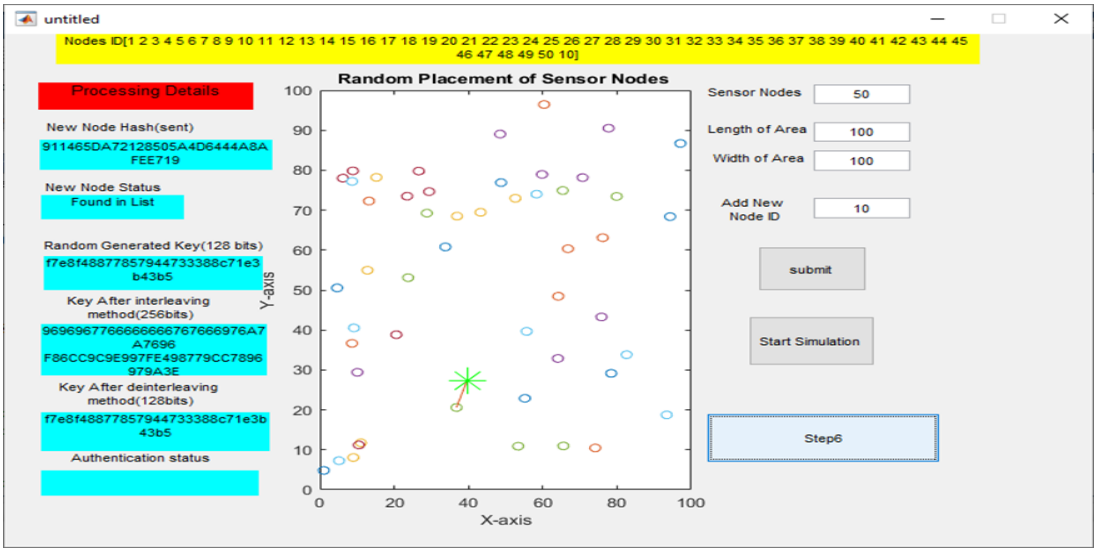

FIG.9. THE DE-INTERLEAVING METHOD

5. The close node checks the 128-bit key to give authentication as shown in FIG.10. In this figure, the new node is connected to the WSN as it has authenticated and accepted as a new node in the network. Otherwise, the proposed method rejects the new node and provides the authentication decision as shown in FIG.11.

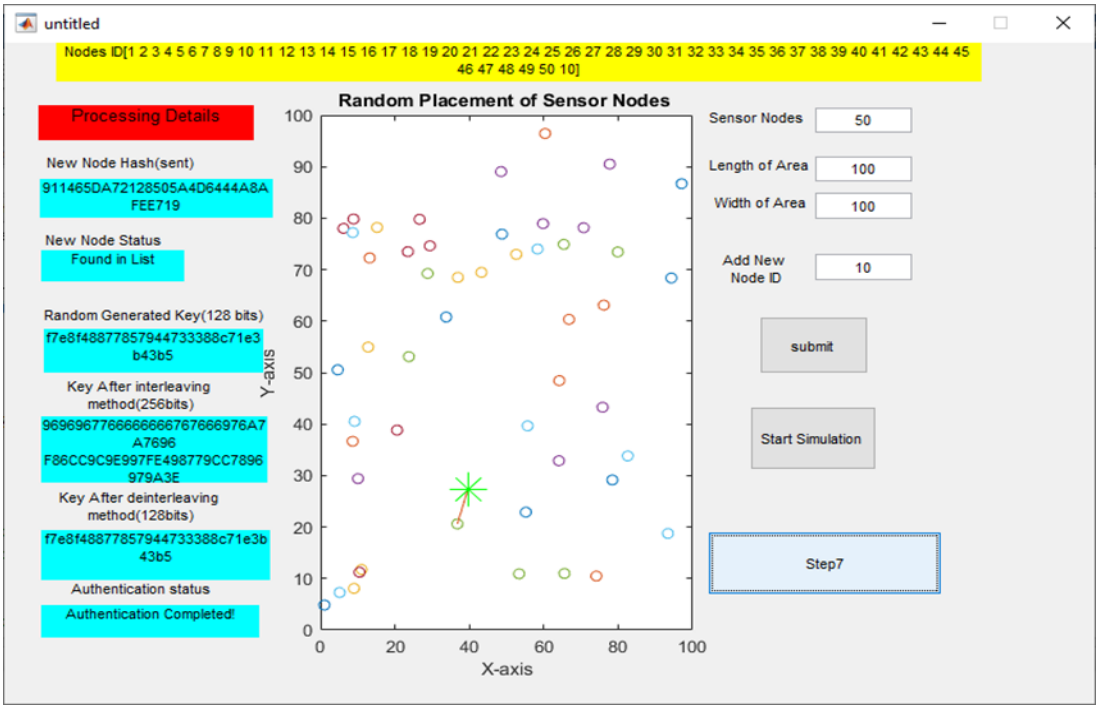

FIG.10. ADDED NODE IS AUTHENTICATED.

Received 5 June 2020; Accepted 9 July 2020

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

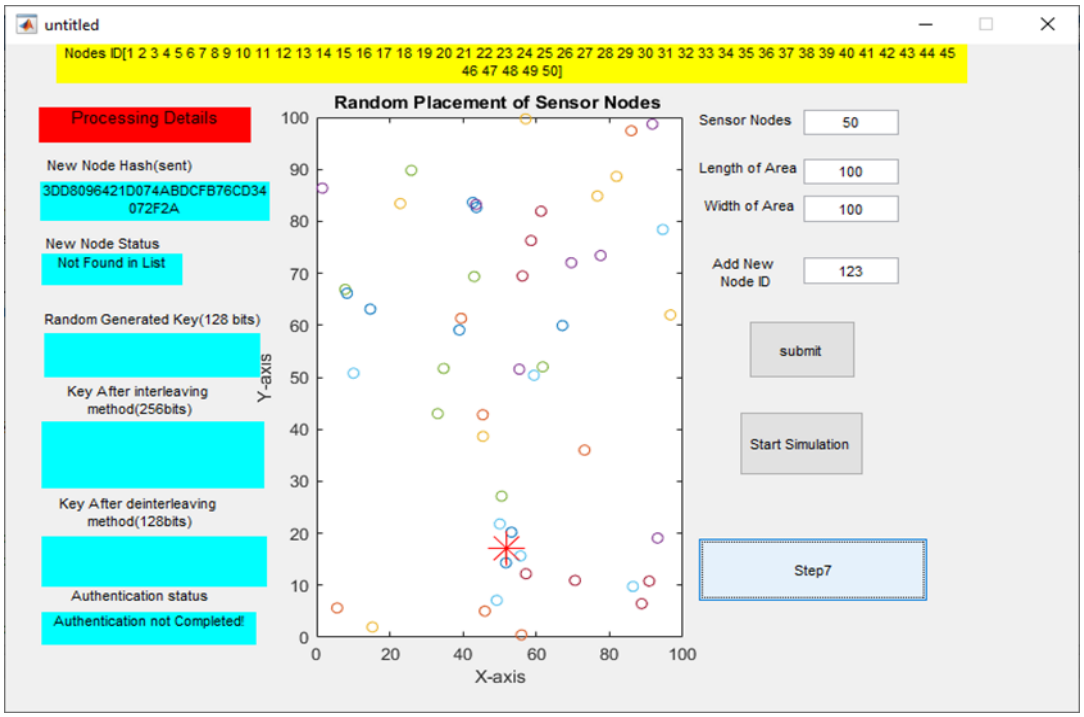

FIG. 11. THE INTRUDER NODE IS REJECTED (UNAUTHENTICATED) AND COLORED BY RED.

V. CONCLUSION

A software engineering authentication method was proposed to cover the security of Ad hoc WSN. The proposed method included different phases of key exchanging to come up with an authentication decision. These phases were proposed to ensure the identification of the new nodes that would like to join the WSN. The challenges were the generation of keys, combing them, and cyphering them using a Kath hashing function. The MATLAB was adopted to propose a network simulator for WSN based on the AODV routing protocol. The obtained simulator results showed the efficiency of the proposed method in detecting the normal and intruder nodes.

REFERENCES

[1] Yanhua Zheng, "A Research on Key Management in Wireless Sensor Networks", Zhejiang International Maritime College Zhoushan, Zhejiang, Applied Mechanics and Materials, Trans Tech Publications, Switzerland, Vols. 303-306 (2013) pp 247-250, 2013.

[2] J.A.D.C. Anuradha Jayakody, Rohan Samarasinghe and Saluka R. Kodituwakku "SecAODV: lightweight Authentication for AODV Protocol", International Journal of Computer Applications (0975 – 8887), Vol 137, No.13, March 2016.

[3] Shaymaa Mahmood Naser, Muayad Sadik Croock," Proposed Simulator Based on Developed lightweight Authentication and Key Management Protocol for Wireless Sensor Network", International Journal of Computing and Digital Systems, Vol. 7, No 4, P.P 251-260, 2018.

[4] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks", IEEE Communications Magazine, vol. 44, no. 4, pp. 122–130, 2006.

[5] B. C. Lai, D. D. Hwang, S. P. Kim, and I. Verbauwhede,"Reducing radio energy consumption of key management protocols for wireless sensor networks," ACM International Symposium on Low Power Electronics and Design (ISLPED), P.P. 351–356, 2004.

[6] Danyang Qin, Shuang Jia, Songxiang Yang, ErfuWang, and Qun Ding, "A lightweight Authentication and Key Management Scheme forWireless Sensor Networks", Hindawi Publishing Corporation Journal of Sensors, 2016.

[7] Evangelina Lara *, Leocundo Aguilar, Mauricio A. Sanchez and Jesús A. García," Lightweight Authentication Protocol for M2M Communications of Resource-Constrained Devices in Industrial Internet of Things", Facultad de Ciencias Químicas e Ingeniería, Universidad Autónoma de Baja California, Tijuana BC 22390, www.mdpi.com/journal/sensors,Sensors 2020, 20, 501; doi:10.3390/s20020501, Published: 16 January 2020.

[8] Rafael Martínez-Peláez, Homero Toral-Cruz, Jorge R. Parra-Michel, Vicente García, Luis J. Mena, Vanessa G. Félix and Alberto Ochoa-Brust," An Enhanced Lightweight IoT-based Authentication Scheme in Cloud Computing Circumstances", Facultad de Tecnologías de Información, Universidad De La Salle Bajío, 2019.

Received 5 June 2020; Accepted 9 July 2020

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

[9] Manish P. Gangawane," Implementation Of Zero Knowledge Protocol In Wireless Sensor Network for prevention Of Various Attacks," International Journal of Emerging Technology and Advanced Engineering , Volume 2, No. 8, 2012.
[10] Swapna Naik , Dr. Narendra Shekokar and Rupali Yavale" A Novel Authentication approach in Wireless sensor Network", International Journal of Scientific & Engineering Research, Val 5, No. 3, 2014.
[11] Vankamamidi S. Naresh ,1 Sivaranjani Reddi,2 and Nistala V. E. S. Murthy3Hindawi "Secure lightweight IoT Integrated RFID Mobile Healthcare System", Wireless Communications and Mobile Computing ,2020.
[12] Liang Kou1, Yiqi Shi2, Liguo Zhang1, Duo Liu1, * and Qing Yang3,"A lightweight Three-Factor User Authentication Protocol for the Information Perception of IoT" Copyright © 2019 Tech Science Press CMC, vol.58, no.2, P.P.545-565, 2019.
[13] Bacem Mbareka, Are f Meddebb,Wa f a Ben Jaballahcand Mohamed Mosbahd," An effective and lightweight Authentication and KeyManagement Scheme (AKMS) is proposed", The 8th International Conference on Ambient Systems, Networks and Technologies (ANT), 2017.
[14] Shaymaa Mahmood Naser, Muayad Sadik Croock," Developed New node Authentication and Key Management Protocol for Wireless Sensor Network", International Journal of Advanced Research in Science, Engineering and Technology, Vol 5, No 8, P.P 6606-6619, August 2018.
[15] Sagar D. Dhawale Dr. B. G. Hogade Dr. S. B .Patil, "Design and Implementation of a Dynamic Key Management Scheme for Node Authentication Security in Wireless Sensor Networks" , International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 4, April 2015.
[16] Banoth Rajkumar1* Gugulothu Narsimha2 "Secure Light Weight Encryption Protocol for MANET ",1Jawaharlal Nehru Technological University, India ,2Jawaharlal Nehru Technological University College of Engineering, Nachupally, Karimnagar, Journal of Intelligent Engineering and Systems, DOI: 10.22266/ijies2017.0630.07, Vol.10, No.3, 2017.
[17] Adarsh Kumar and Alok Aggarwal, "Light Weight Cryptographic Primitives for Mobile Ad Hoc Networks" Computer Science Engineering and Information Technology Department, Jaypee Institute of Information Technology, Noida, India {adarsh.kumar,alok.aggarwal}@jiit.ac.inS.M. Thampi et al. (Eds.): SNDS 2012, CCIS 335, pp. 240–251, 2012.
[18] Vijay Varadharajan, "Authorization and Trust Enhanced Security for Distributed Applications", ICISS 2005, LNCS 3803, pp. 1– 20, 2005.
[19] Pawani Porambage," LIGHTWEIGHT AUTHENTICATION AND KEY MANAGEMENT OF WIRELESS SENSOR NETWORKS FOR INTERNET OF THINGS", UNIVERSITY OF OULU GRADUATE SCHOOL; UNIVERSITY OF OULU, FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING; CENTRE FOR WIRELESS COMMUNICATIONS; INFOTECH OULU, Copyright © 2018Acta Univ. Oul. C 671, 2018.
[20] Srdjan Capkun, Jean-Pierre Hubaux, and Levente Buttyan, "Mobility Helps Security in Ad Hoc Networks", MobiHoc'03, June 1–3, 2003, Annapolis, Maryland, USA, ACM 2003.
[21] "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography", Sensors (Basel). 2011; Vol. 11, No. 5, P.P. 4767–4779, 2011.
[22] Banoth Rajkumar and Gugulothu Narsimha2" Secure Light Weight Encryption Protocol for MANET", International Journal of Intelligent Engineering &system, 2016.

Received 5 June 2020; Accepted 9 July 2020

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352