



# Proposed Simulator Based on Developed Lightweight Authentication and Key Management Protocol for Wireless Sensor Network

Shaymaa Mahmood Naser<sup>1</sup> and Muayad Sadik Croock<sup>2</sup>

<sup>1</sup>Information Institute for Postgraduate Studies, Baghdad, Iraq

<sup>2</sup>University of Technology, Computer Engineering Department, Baghdad, Iraq

Received 10 Mar. 2018, Revised 5 May 2018, Accepted 14 Jun. 2018, Published 1 July 2018

**Abstract:** Recently, wireless sensor networks is considered as an important part of the life. It becomes wide spread in different applications, such as military, medical and environment. In this paper, a modified lightweight authentication and key management protocol for wireless sensor network is introduced, employing the technique of Elliptic Curve Cryptography with Diffie-Hellman. In addition, A designed simulator that simulate the phases of authentication starting from base station tell the last sensor node. This simulator is produced to tackle the problem of lightweight protocol absence in the well-known simulators, such as NS2 and NS3. The modified protocol and the presented simulator are tested over different scenarios and the obtained results show the superior performance of them. Moreover, the results illustrate the high accuracy of the simulator and benefits of the modification on the lightweight protocol.

**Keywords:** Wireless Sensor Network, Lightweight Authentication And Key Management Protocol.

## 1. INTRODUCTION

The wireless sensor network consists of small pieces called nodes which are spread in wide area for sensing the event that occurring in this area. These sensing data is either treated in the same node or transmitted directly to other node or base station for more advanced processing. It is well-known that security side is the most important part for protecting this type of network because WSN is exposing for different type of attacks on : node , key and data.[1].

Security is a critical issue in the ad hoc network. The main two issues in ad hoc network are the authentication and key management [2]. Authentication is the determination and declaration of someone or something need to be involved in different types of matters. At the other hand, the verification of the sender and receiver is required as well. The node authentication and key management processes in the sensor network are considered in this research. Normally, the traditional authentication manners are not sufficient and efficient for wireless sensor network, therefore different research works have been introduced to propose new techniques. S. Raja Rajeswaril and V. Seenivasagam in [3] compared

many authentication and key management protocols that concentrated on security in wireless sensor network (WSN). They produced a satisfactory comparison that filled the hunger of researchers. After these comparison, the authors of [4] solved the problem of malicious nodes in WSN network using light weight authentication and key management protocol by symmetric cryptographic primitives with (HMAC).

At the side, key management issue is also considered significantly influence in the scale of security of homogenous WSNs [5]. Based on this principles , the technique manage the generation of keys form adversary, while adversary and authentication have not had any information about the clef by using zero knowledge protocol, presented in [1],and [6]. In this protocol, the nodes observed the neighborhood nodes, then they collected their closets neighbored to obtain the network operation in normal mode. The authors of [9] followed the same procedure, presented in [6], in addition to gathering the statistical information of nodes and sent to base station sporadically. In [8], the authors improved user authentication protocol based on ECC for hierarchical WSN, They showed how ECC is suitable for this structure.

In this paper, we introduce a development to the adopted lightweight authentication and key management

protocol by addressing the methods of Elliptic Curve Cryptography with Diffie-Helman. This is to improve the ability of securing and speed up the process. In addition, a specific simulator has been proposed to adapt with the requirements of lightweight protocol that are hard to address in NS2 and NS3 simulator. This simulator passes through three main phases for authentication of nodes and base-stations and the key management in terms of generation and verification. .

## 2. INTRODUCED SYSTEM

As mentioned above, this research work produced a simulator system that addresses the events of employing the lightweight protocol. This section can be divided into different sub-sections for easing the reading follow.

### 2.1 BLOCK DIAGRAM

The presented system can be introduced as a block diagram as shown in “Fig. 1”. The block diagram divides the introduced system into the following:

#### A. Base Station Layer:

It contains the base stations and their considered fixed points for gathering and controlling the information grouped form cluster head. This layer plays different roles of monitoring, recording, and managing of the wireless sensor network. Base station can be connected with fixed or mobile sensors.

#### B. Cluster Head Layer:

This layer includes many numbers of cluster heads that are connected with the related base station from side and with sensors from other side. It represents the communication gateway between the included sensors within the cluster. Each cluster head is selected from the sensor node depending on some criteria such as energy or distance.

#### C. Sensor Node:

Each sensor node is constructed with memory unit, microcontroller, and battery, used for measuring the parameters of the surrounding environment; there are numerous types of sensors with distinct saving capability, energy consumption and so on.

#### D. Authentications:

Each sensor node must authenticate itself to network through cluster head in the beginning of initialization of network or through other sensor nodes if after that. Also cluster authentication is generated in the initial network.

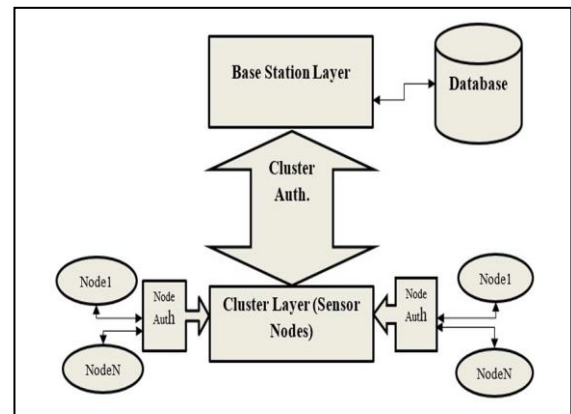


Figure 1. Diagram of the presented system

### 2.2 DEVELOPED ALGORITHM

The introduced algorithm of the presented system has been developed. The adopted algorithm is operated under the standards of Lightweight authentication and key management protocol (AKMS). The (AKMS) nominates Hash message authentication code (HMAC) algorithm and Elliptic Curve cryptography Diffie-Helman to authenticate the sensor nodes inside the network [4], “Fig. 2” shows the developed algorithm as a flowchart.

ECC can be implemented on sensor nodes because it necessitates low power, bandwidth, memory, when matching with cryptosystems remains. ECC with Diffie-Helman employs smaller keys with security similarity and compute their performance on WSN. It is used for steer connection through passing the information via public network, developed grown PUBLIC-KEY cryptosystem in mid of 1980s [7]. Through the networking stage, inside every node is initial authenticator that initialed before installed, three stages is created:

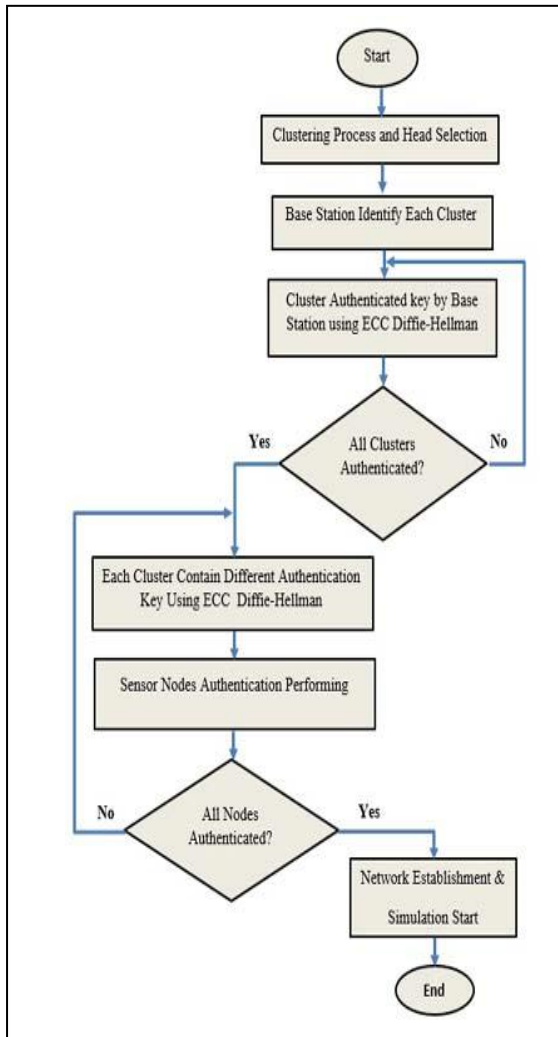


Figure 2. Flowchart of developed algorithm

**Key Redistribution stage:** in this stage the master key of 128 bits is generated, the length of key used in ECC Diffie-Helman is more enough to resist the attacks. In this stage, the master key is distributed for all nodes in the network beginning. The base station is generated the keys for clusters and the clusters generated the keys for sensor nodes that each cluster has special scope different other cluster.

**Network Initialization stage:** in this stage, each node recognizes its neighbors during the communication rang employing its random number and encryption key. While each node broadcasts random number for every node in the network, the encryption key is generated using hashing the master key and random number for such node.

**Authentication Protocol stage:** This stage is activated when new node requires entering in the network. This

protocol is very complicated for authenticate the new node to make sure of new node authentication [4].

### 2.3 DATA OF SYSTEM

SQL server is adopted in this research work to build the database of the system. The benefits of the utilized database are storing the simulated WSN including all the actions and activities in addition to the related dataset. The built database is represented in “Fig. 3” as an ER-diagram.

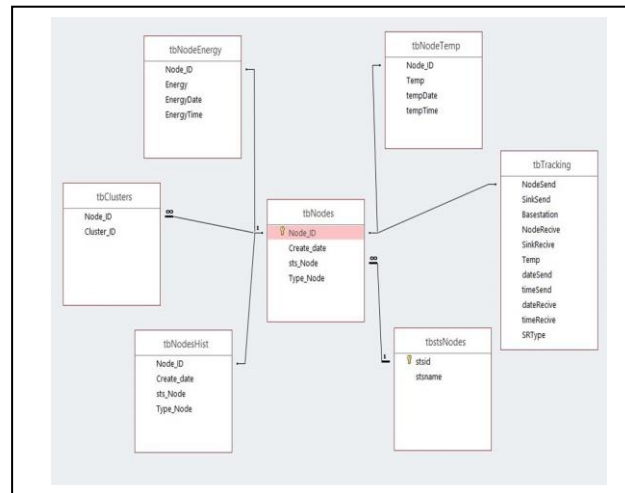


FIGURE 3. ER-DIAGRAM OF THE BUILT DATABASE

The considered database is built following the methodology of life-cycle model as explained in the block diagram, shown in “Fig. 4”, and explained below:

#### A. Requirement:

In this phase, the requirements of the system and users are collected including energy consumption of nodes, authentication information, sending and receiving messages between nodes in the network, number of cluster heads, time and date for recording temperature and status of nodes (active, sleep, died).

#### B. Design

Each table in the ER-diagram has it field’s name and description field type as follows:

- **TbNodes table:** this is the main table in the structure, it contains primary key field, called Node\_ID node identification. Create\_date records the creation date of nodes, while sts\_Node records the status of current node (active, sleep, died). Type\_Node for

specifying the node is authenticated or not, the table contains the last case of all nodes.

- *TbNodesHist table*: it includes the same as tb\_nodes table fields (Node\_ID, Create\_date, sts\_Node, Type\_Node) used for recording all movement of nodes.
- *TbNodeTemp table*: this table saves all temperature reading of nodes as the considered sensors in this work is temperature. Node\_ID field contains node identification, Temp field records the reading of nodes, and tempDate holds the date of reading temperature also tempTime hold the time of it.
- *TbNodeEnergy table*: there are four fields inside the structure of this table. Node\_ID saves the node identification, Energy field holds the energy of each node that gradually decreased, EnergyDate saves the date of recording energy and EnergyTime includes the time of recoding.
- *TbTracking table*: it is the largest table size in structure of database because of including the traffic of the messages between nodes, cluster heads and base station. NodeSend field contains the identification of node which sending request, SinkSend includes the identification of sink that supervisor of node sending request. In addition, Basestation field records 0 if request found and record -1 if not (notification message). NodeRecive field contains the identification of node which receiving the request, also SinkRecive is the same as sink\_send field work. Temp field records the information needed, dateSend implicates the date of sending request, and timeSend has the time of sending request. Moreover, dateRecive has the date of receiving request also timeRecive contains the time of it and SRType field records the type of movement (send or receive).
- *TbClusters table*: this table classifies each node and the cluster head follow it. Node\_ID is the same as node\_id in another tables, Cluster\_ID contains the number of cluster.
- *TbstsNodes table*: stsid has the number of symbol (1,2,3,...), stsname field has the status of node (active,sleep,died,...).

### C. . Implementation

In this phase, the built tables, views, procedures and relations using SQL management Studio2012 are implemented based on the designed ER-diagram explained above.

### D. Testing

This phase tests the activities of the built database by performing the insert, update, and delete actions on the database.

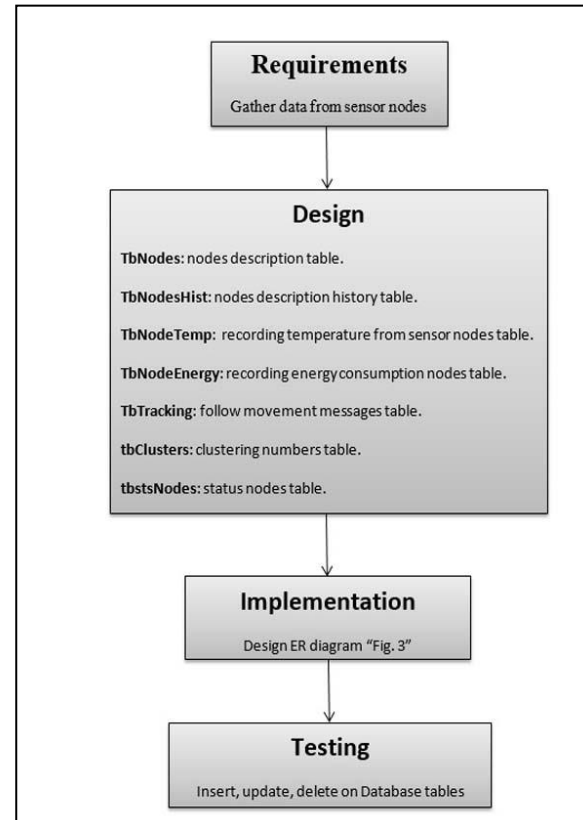


Figure 4. Built database block diagram

## 2.4 DESIGNED GUI

As mentioned earlier, the simulator, presented in this work, can simulate the actions of authentication and key management of lightweight protocol for WSN. The simulator includes different Graphical User Interfaces (GUI) pages. These pages perform the activities of the proposed simulator throughout the phases of the authentication and key management of the underlying protocol.

“Fig. 5” shows the main interface of the proposed simulator. Throughout this interface the first setting of the WSN is performed by entering the number of sensors, clusters and so on. In addition of the information of data sending intervals as well as the time for putting the nodes in sleep mode. There are also different buttons that simulate the authentication phases, such as Phase One, Phase Two and Phase Three. The first phase tackles the authentication between the base station and related cluster heads. While the second phase generates the authentication key for sensor verification. The third phase performing the nodes authentication regarding the addressed cluster head. The last button, called Strat, represents the starting of network performance over transmission and information replacement.

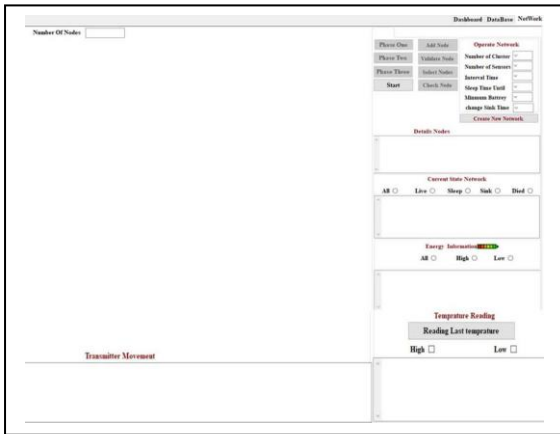


Figure 5. Home page form

All information regarding the key generation and data transmission of the included nodes at the designed WSN is shown in the square text at the interface. This includes the working nodes as active, sleep or even dead. In energy information tab, the details of energy for each node in network are appeared. Temperature Reading tab exist the High and Low reading in nodes, this depend on threshold for high and low degree. In transmitter movement appears the behavior of request between nodes.

In Database tab, shown in “Fig. 5”, the existed tables as well as information about the nodes, cluster heads, base station and recording the data are shown as in “Fig. 6”.

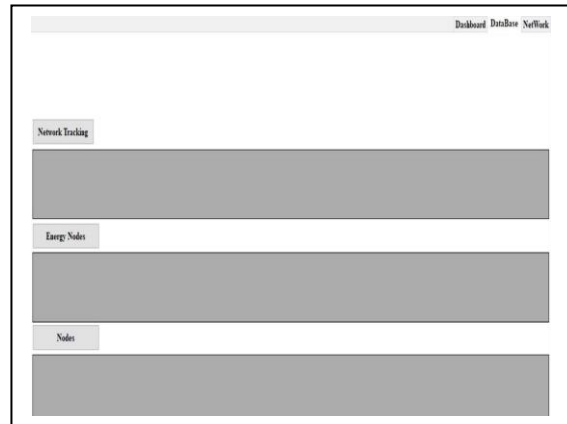


Figure 6. Database tab

In dashboard tab, explained the number of node statuses as in “Fig. 5”, the 3d clustered column chart that explains the levels of active and sleep nodes is shown in “Fig. 7”. At the beginning, the active nodes are full but gradually the percentage is decreased or increased as show this in “Fig. 8”, and “Fig. 9”.

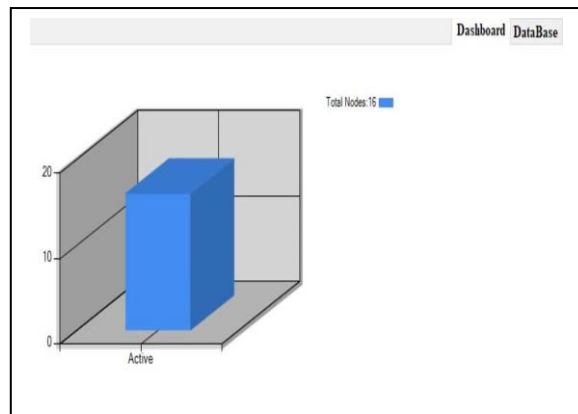


Figure 7. Dashboard normal case

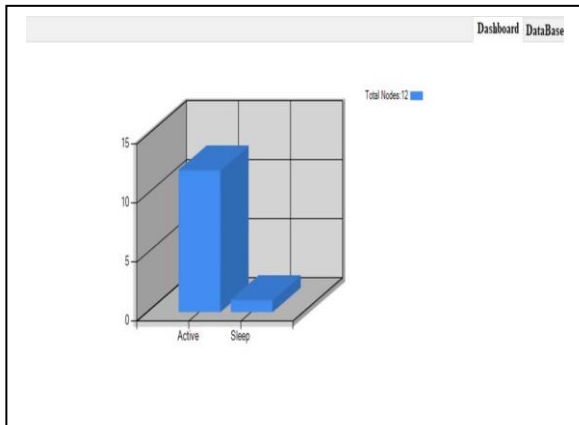


Figure 8. DASHBOARD INCREASING CASE

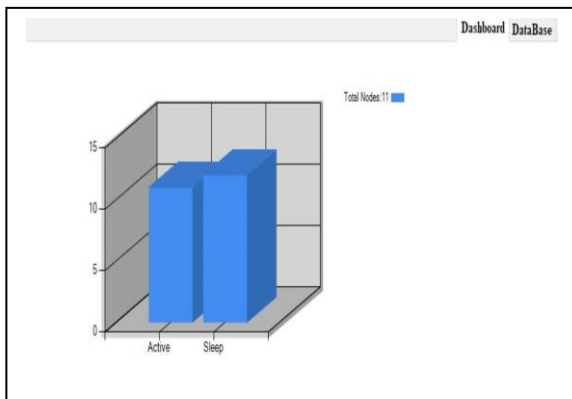


Figure 9. DASHBOARD DECREASING CASE USING THE TEMPLATE

### 3. RESULT

The proposed simulator is tested in the computer with microprocessor of i7, RAM of 4GB with the SQL server 2012 for building the database and Microsoft Visual C# for designing and performing the GUI pages and forms. The testing of the proposed simulator based on the developed lightweight protocol can verify the efficiency of the developed algorithm and such simulator.

In order to cover the most of simulator sides, different case studies are considered. These case studies show the superior of the proposed simulator and the developed algorithm to work with lightweight protocol as follows.

### 3.1 CASE STUDY1

In this case study, the normal performance of the proposed WSN is simulated. At the first time, we must enter some information such as: number of cluster, number of sensor, interval time and minimum battery rate, as shown in “Fig. 10” and the WSN is drawn as shown in “Fig. 11”.

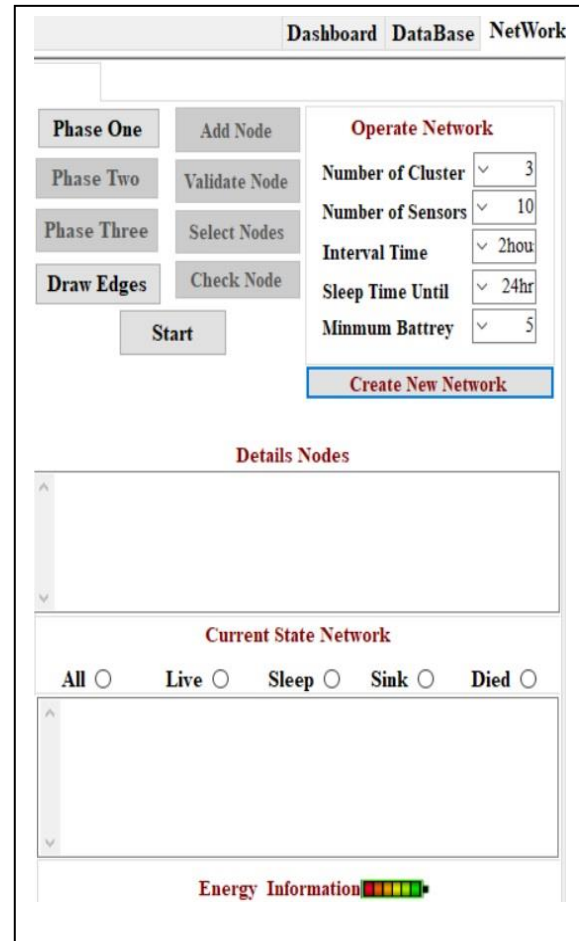


Figure 10. Setting the designed WSN

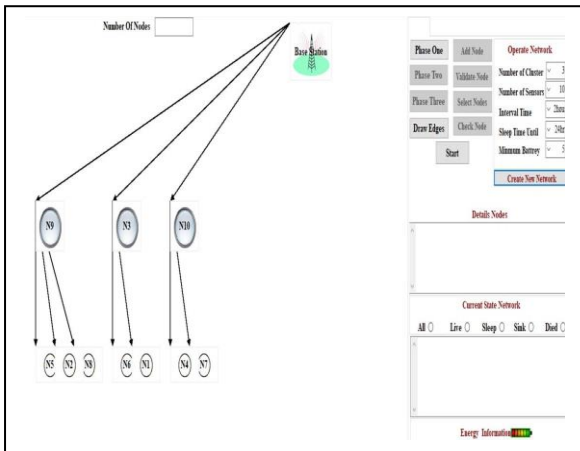


Figure 11. Operate network

At the pressing on phase one as the next step, the master key is generated for each node including the selected cluster head and the color of base station is changed with information message appearance as shown in “Fig. 12”.

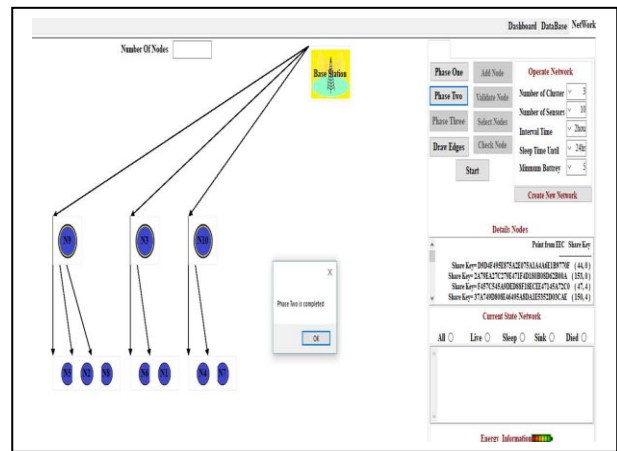


Figure13. Phase two performing

By pressing the phase three button, the color of nodes is changed to green as shown in “Fig. 14” to indicate that the included sensor nodes are authenticated successfully.

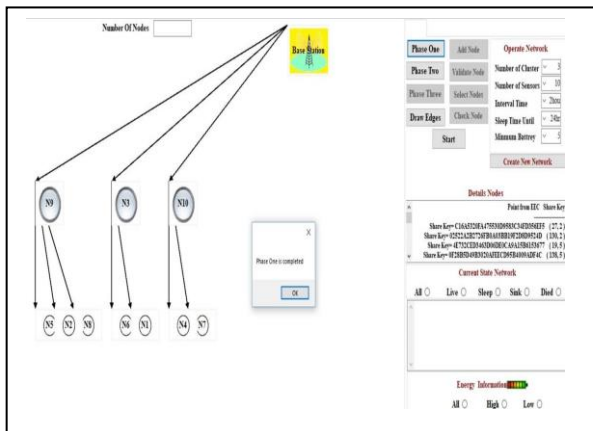


Figure 12. Phase one performing

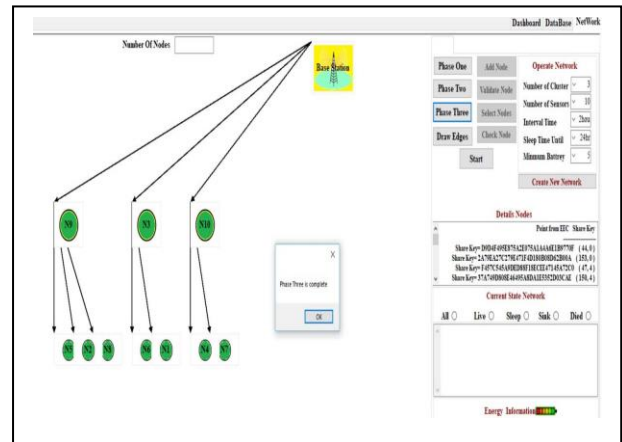


Figure 14. Phase three

After that, the button of phase two is selected and clicked to perform the neighbors recognizing of each node with others as well as distributing the encryption key. It can be shown in “Fig. 13” that the colors of nodes are changed to blue as indicator of performing the second phase.

Now the network is operated by clicking the button of Start. We can see that form reading view pallet, current status pallet and battery information pallet are appeared as shown in “Fig. 15”.

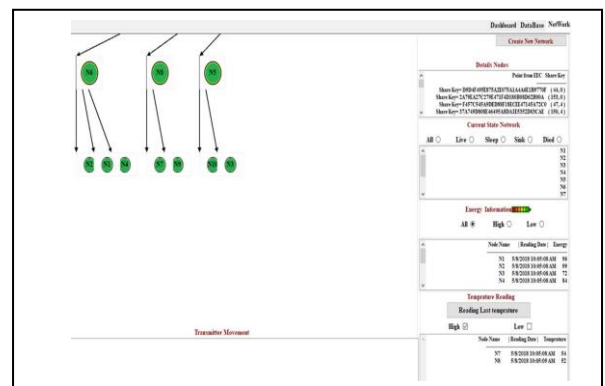


Figure (15): Status Network

### 3.2 CASE STUDY 2

This case considers the adding of a node to the network built in case study one. If a new node wants to join to network, “add node” button is pressed as shown in “Fig. 16”. The node sends random number and as a default (have initial authenticator of network) it sends it to the closest node, then cluster head then to the related base station. The recipient node is interacting with this situation by applying authentication protocol.

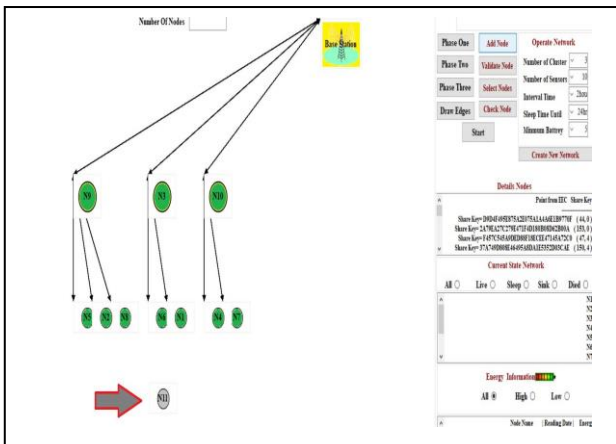


Figure 16. Additional node joins to network

If the node is authenticated, the color of it is changed to green as shown in “Fig. 17” and being a part of the specific cluster as shown in “Fig. 18”.

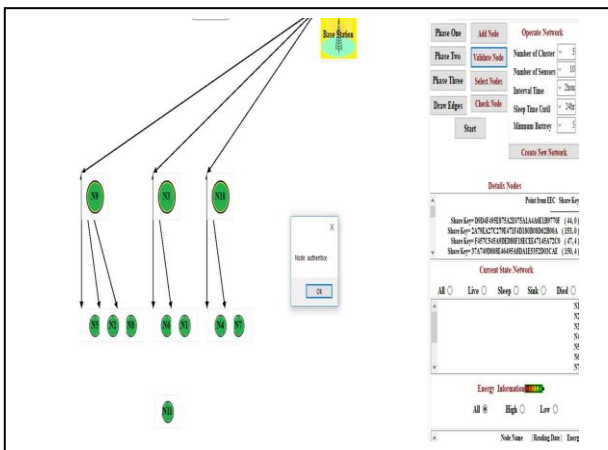


Figure 17. Successful Authentication of Added Node

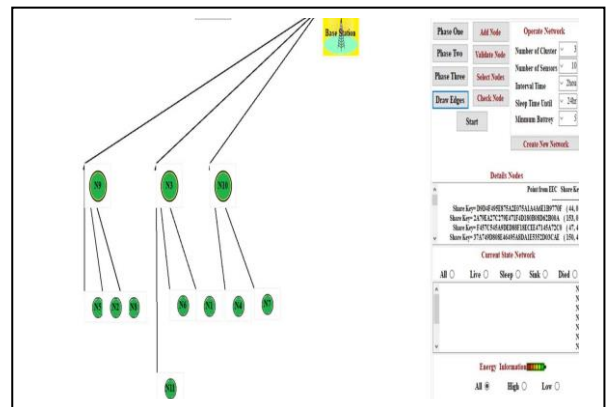


Figure 18. Successful joining node

Otherwise, if stranger node does not have initial authentication, then the network reject it and indicated with red color as shown in “Fig. 19” and “Fig. 20”.

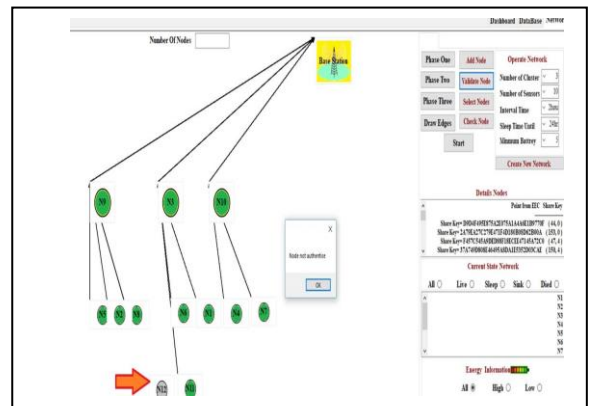


Figure 19. Added node is not authenticated

Then the color of node is changed and do not join to the network.

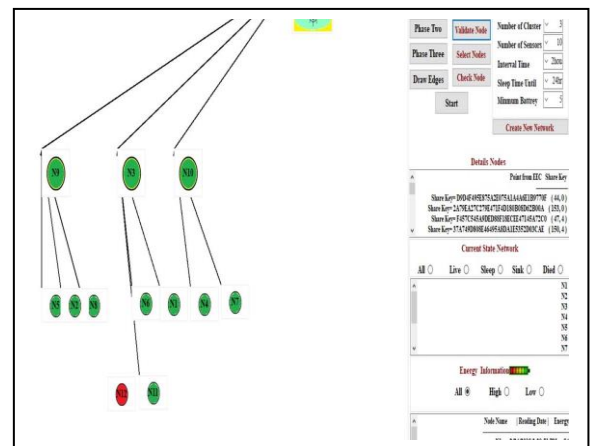


Figure 20. Added node is rejected and colored to red



### 3.3 CASE STUDY3

In order to simulate the transmission of a messages or request between nodes, we can select the source and destination nodes to be colored in different color for each of them as shown in “Fig. 21” and “Fig. 22”. It is important to note that the blue node is node source, while the purple node is the destination. In addition to prove that the simulator works in real-time performance. The “check node” button is clicked to test if the request is authenticated and successfully performed.

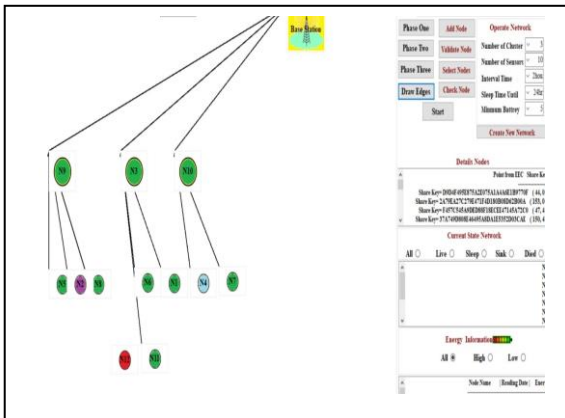


Figure (21): Selecting the source and destination nodes

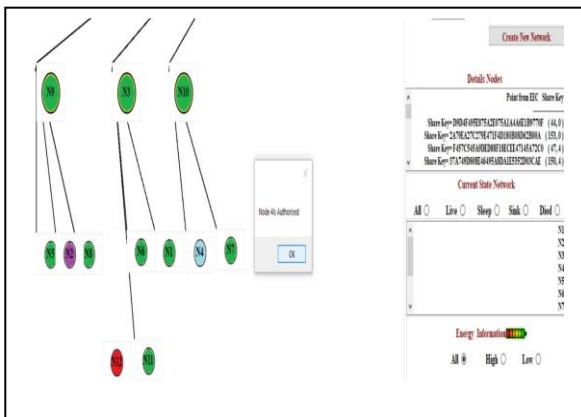


Figure 22. Request authentication and performing

“Fig. 23” shows at the bottom of page the paths of transmission between the source and destination as well as the destination to source. These paths show that the message is transmitted from node 4 at first cluster to the cluster head (sink 10) to be transmitted to the related base station. Then the base station sent the message to objective cluster head (sink 9) for delivering the message to node 2.

In the same back the message is fed back to node 4 via the same opposite sequence path. It is shown that the message is transmitted over two different clusters within the same WSN. Therefore, the transmission can be done at the same cluster or even over different clusters within the same base station as well as over different base stations and clusters. This flexibility provides the simulator with high ability to simulate the real cases of network activities.

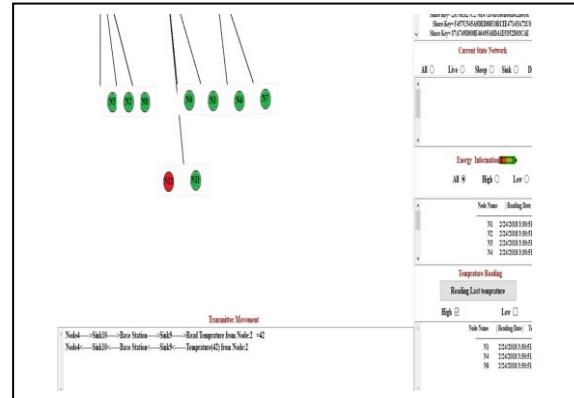


Figure 23. Transmission of a message from node 4 to node 2

### 4. CONCLUSION

A modified lightweight protocol for ad hoc WSN was presented. This modification was the results of applying the modified algorithm that uses the Elliptic Curve Cryptography with Diffie-Helman methods. In addition, an efficient WSN based on lightweight protocol simulator was proposed to avoid and compatibility issues of using the common simulators, such as NS2 and NS3. The modified algorithm improved the security side as well as speeded up the required processing time. Moreover the proposed simulator performed the activities and actions of the designed WSN in efficient way regardless the number of nodes and base stations. This simulator was designed for lightweight protocol for ad hoc WSN and it is adapted to different case studies in real-time performance. Database system is built in this simulator for storing the activities of the designed WSN and readings of sensors for future reporting and processing. Different tables were built in the database based on relational relationship. The SQL server 2012 and Visual C# environments were adopted to build the proposed simulator and database for numerous reasons, such as easiness and efficiency. Distinct case studies were considered to test the ability and efficiency of the propose simulator and developed algorithm. The results proved the superior performance of the proposed simulator and developed algorithm in normal performance and authentication of adding nodes as well as message sending tracking and performing.

**REFERENCES**

- [1] 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.
- [2] Lidong Zhou and Zygmunt J. Haas, "Securing Ad Hoc Networks", *IEEE network*, special issue on network security, P.P. 24-30, December, 1999.
- [3] S. Raja Rajeswari and V. Seenivasagam, "Comparative Study on Various Authentication Protocols in Wireless Sensor Networks", *The Scientific World Journal*, 2016.
- [4] Danyang Qin, Shuang Jia, Songxiang Yang, Erfu Wang, and Qun Ding, "A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks", *Journal of Sensors*, 2016.
- [5] Filippo Gandino, Cesare Celozzi and Maurizio Rebaudengo, "A Key Management Scheme for Mobile Wireless Sensor Networks", *Journal of Applied Sciences*, Vol 7, 2017.
- [6] Krontiris Ioannis and Tassos Dimitriou, "Towards Intrusion Detection in Wireless Sensor Networks", <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.4197&rep=rep1&type=pdf>, 2007, December 2017.
- [7] Ram Ratan Ahirwal, Manoj Ahke "Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information on Wide Area Network" (*IJCSIT*) *International Journal of Computer Science and Information Technologies*, Vol. 4, No. 2, P.P. 363 – 368, 2013.
- [8] Rakesh Maharana, Pabitra Mohan Khilar "An Improved Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC" *International Journal of Computer Applications*, Vol. 67, No. 22, April 2013.
- [9] Nasser-Eddine Rikli and Aljawharah Alnasser, "Light-Weight Trust Model for the Detection of Concealed Malicious Nodes in Sparse Wireless Ad-hoc Networks", *International Journal of Distributed Sensor Networks*, 2016.



**Shaymaa Mahmood Naser** is a Programmer and DBA in BOSA (Iraq) Received a B.Sc. from ALmustansiriyah University 2002 in computer science. She designed multi program in multi fields that serve the society. She is a lecturer in training center of BOSA, technical experience in analyzing and designing a new and rebuild Database Schemas in Oracle and SQL Server, technical. She got skills in different

programming languages, such as visualBasic/.NET, Java, SQL/Server /PL/Oracle, C#. She has a strong background in project management and customer needs.



**Muayad Sadik Crook** is assistant professor in Computer Engineering at University of Technology, Baghdad, Iraq. He obtained his B.Sc, M.Sc from University of Technology in 1998 and 2003 respectively. He got his PhD from Newcastle University in UK at 2012. His research field includes Computer Engineering, Sensor Networks and Embedded Systems.