Surviving Network Plan in Lightweight Protocol for Wireless Sensor Network

Shaymaa Mahmood Naser[1], Muayad Sadik Croock[2]
[1]Information Institute for Postgraduate Studies, Baghdad, Iraq
[2]University of Technology, Computer Engineering Department, Baghdad, Iraq

Abstract— **Recently, the Wireless Sensor Network (WSN) has been considered in managing and monitoring different fields of life, such as health, environmental, agricultural. In this paper, a WSN surviving plan based on lightweight authentication and key management protocol is proposed. The proposed surviving plan for WSN is adopted in case of increasing the dead nodes, in which the performance of such network can be efficiently affected. This is performed by monitoring the number of life nodes to be more than half of total number. In addition, a designed simulator that simulates the three phases of protocol's form base station to sensor nodes is presented following our previous work of [1]. The simulation solves the problem of lightweight protocol absence in the common use network simulators, such as NS2 and NS3. The results show the efficient performance of the proposed surviving network plan in terms of maintenance and continuity.**

Index Terms— **WSN, lightweight protocol, surviving plan, life nodes.**

I. Introduction

The Wireless Sensor Network (WSN) consists of a number sensor nodes, which are distributed in large size areas for sensing environment around each node. The received sensor readings can be analyzed and processed either in the same node or the related base station for different purposes. It is well known that the security side has the most important part in the WSN in protecting the data from hacking and the entire network from attacks. Therefore, the security in WSN can be classified as a critical problem that must be solved. [2], [3].

Different research works have been introduced to tackle the facing problem in maintenance the WSN network. In [4], a distributed framework for low energy connectivity and coverage maintenance in WSNs has been proposed. Each sensor manages self-scheduling to separately control the states of transmission and sensing units following the dynamic coordinated reconstruction mechanism. In [5], a network construction and routing method has been proposed using three duties for sensor nodes: node, cluster heads, and cluster members, by applying a hierarchical structure over all duties. This method introduced an efficient way to guarantee the top coverage, to recover the lost data with the mobility, and to reduce overall energy consumption. In [6], maintenance strategies were proposed based on a simple energy consumption analytical model to compute the required times of the happened sensor failures in the network. The addressed failures have been exchanged with the available robots before they happen.

In this paper, we propose a surviving plan that maintains the efficiency of the WSN by compensating the dead nodes with additional ones. Moreover, a specific simulator has been introduced following our previous work of [1] to adapt with the requirements of lightweight protocol that are hard to address in NS2 and NS3 simulator. This simulator includes through three main phases for authentication of nodes, cluster heads and base-stations.

II. The Proposed System

As previously mentioned, the proposed simulator uses the lightweight protocol principles. This simulator performs the contributions of this paper, such as surviving plan as well as the other phases of the protocols.

A. *Simulator Block Diagram*

The block diagram, shown in Figure (1), introduces the introduced simulator [1]. This diagram is divides into Base Station Layer, Cluster Head Layer, Sensor Node Layer and Node Authentications.

B. *Simulator Imitation*

Different actions are performed in the initiation of the introduced network simulator as follows:

Network Initialization stage: In this stage, the neighbors of nodes are perceived others by broadcasting random number for each node and generate encryption key via Hashing master key and random number. Moreover, the selection of cluster head amongst the nodes within each cluster. Each cluster head is connected with a base station.

Key Generation: In this stage the master key is generated with 128 bits length. This key is distributed amongst the cluster heads. Later on, each cluster head generates the keys for sensor nodes without repeating keys.

Authentication Protocol stage: In this stage, the authentication action is performed between the base station and cluster heads, while each cluster head is authenticated with related cluster nodes. This stage is also activated when new node requires entering in the network. This protocol performs the authentication of the new node to make sure that it is legally added [7].

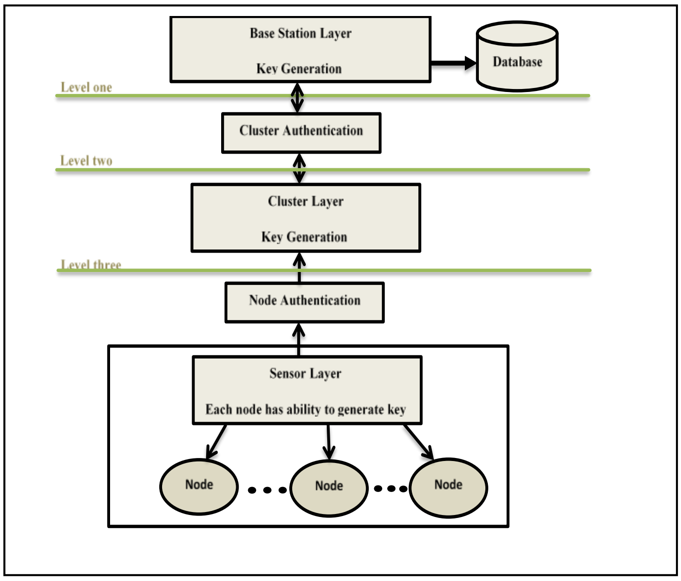


Fig. 1. Simulator block diagram

C. Proposed Surviving Plan The Network

The surviving plan for maintaining the considered sensor network is proposed to keep the efficiency of the network at high levels. There are some assumptions should be mentioned as:

1. **Sleeping operation**: When there is no request for information from the nodes for a period of time (24 hour), then the node enter sleeping mode except cluster head due to its job of gathering information to be passed to the base station.
2. **Energy consumption**: All nodes consumes the same energy at the creation of the network, where the power dissipation is running in ration of 5% per hour.
3. **Maintain Network**: After the network works normally, the energy of nodes starts to degrade which in lead can affect the performance of the network.

Figure (2) explains the proposed surviving plan algorithm as a flowchart. When the number of dead nodes in the network reaches 50% of all nodes in the network, the system is aware of the shortage and a warning message is appeared to the monitor to explain that the network needs maintenance. In addition to the warning message, a solution message is shown to select the number of added new nodes for compensating the dead ones. The system administrator must enter less or equal number of dead nodes in the network. If the administrator refuse to compensate the dead nodes, the network continues to work until the number of life nodes in the network reaches 35% and the warning message is appear from again as a last chance to survive the network following the same procedure.

If added nodes are less than the number of dead nodes in the network, the network continues to work until the percentage of dead nodes reaches 50% or 35% again. The system does not allow the selection of more compensating node than the required because it can reconstruct the network.

Generally, the added nodes must be authenticated following the explained algorithm.

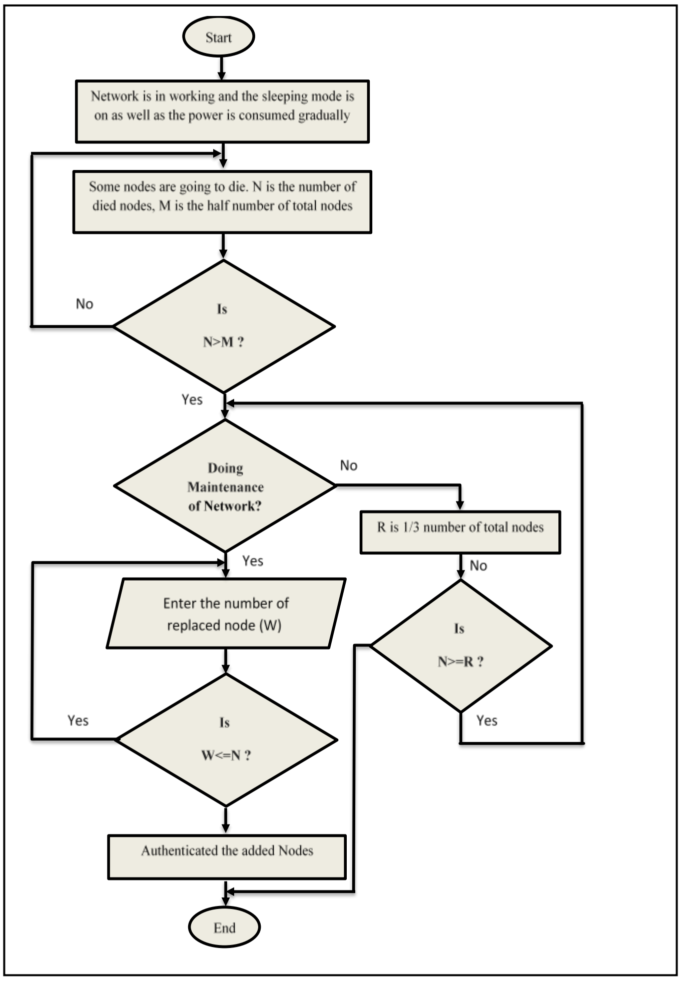

Start
Network is in working and the sleeping mode is on as well as the power is consumed gradually
Some nodes are going to die. N is the number of died nodes, M is the half number of total nodes
No
Is N>M ?
Yes
Doing Maintenance of Network?
No
R is 1/3 number of total nodes
Yes
No
Enter the number of replaced node (W)
Is N>=R ?
Yes
Yes
Is W<=N ?
Authenticated the added Nodes
End

Fig. 2. Proposed surviving plan of the Network

III. GUI DESIGN

The simulator that implements the behaviors of authentication and key management of adopted lightweight protocol in addition to surviving plan of WSN. The simulator offers monitoring screens for administrators. The Graphical User Interfaces (GUI) of aforesaid simulator can be explained as follows.

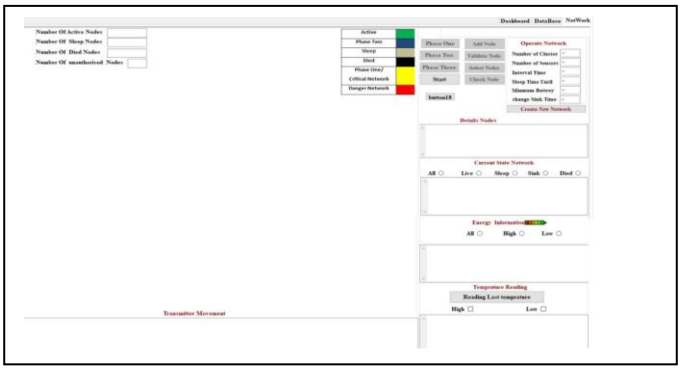


Fig. 3. Home page form

In Figure (3), the main GUI page is shown to explain the three phases of protocol and the main setting of simulation by entering the number of sensors, clusters ,time interval, sleeping time, battery and sink time. These parameters are used to create new network and the three phases is applied one by one to see the performance of it. Phase one represents the key redistribution phase by treatment the authenticated between main base station and each cluster head. In addition, the second phase performs the network initialization that activates the authentication between sensors. The last phase runs the authentication protocol for neighbored. After applying the three phases, the information of detailed node, current state network, energy information and temperature readings are appeared and stored in the database as shown in Figure (4).

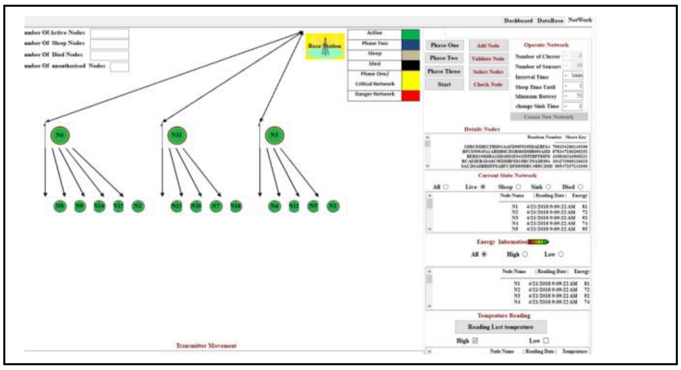


Fig. 4. Network Operation

The statistical percentages of the nodes statuses are varied depending on the number of active, sleep and died nodes as show in Figures (5) and (6).

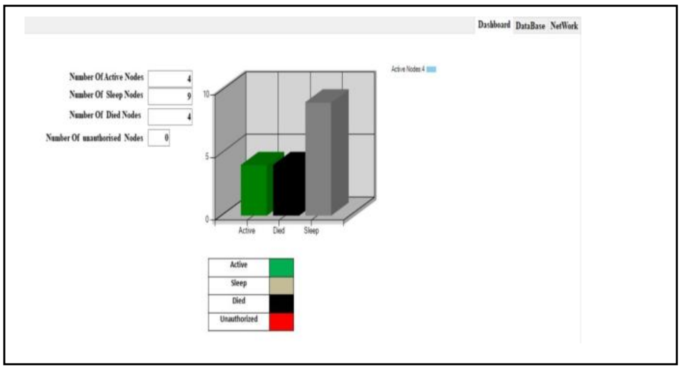

Number Of Active Nodes: 4
Number Of Sleep Nodes: 9
Number Of Died Nodes: 4
Number Of unauthorised Nodes: 0

FIG. 5. DASHBOARD PERCENTAGE

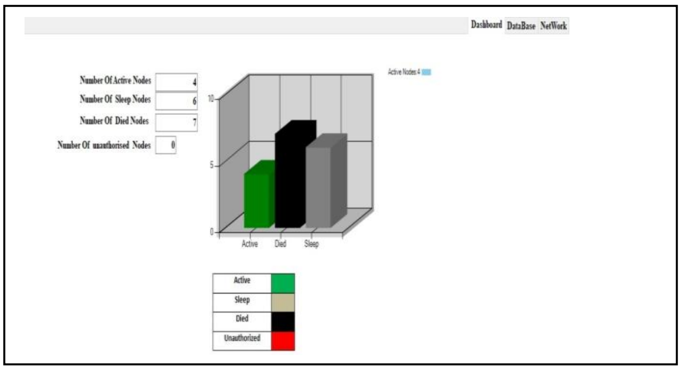

Number Of Active Nodes: 4
Number Of Sleep Nodes: 6
Number Of Died Nodes: 7
Number Of unauthorised Nodes: 0

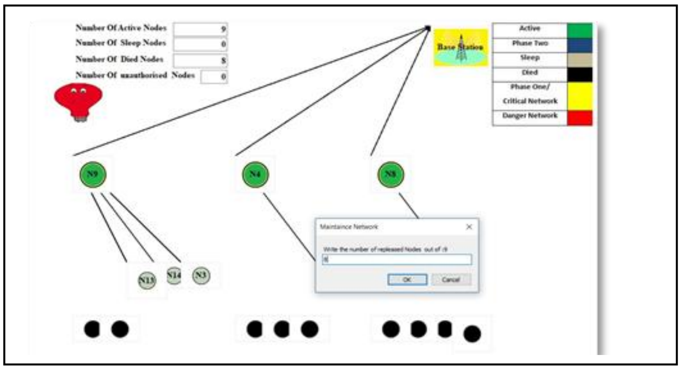
Fig. 6. Changing in dashboard percentage

IV. SIMULATION RESULT

In order to test the proposed network surviving plan, different case studies are considered. These case studies covers the possible cases that can be faces. The number of dead nodes being more than the half number of nodes in the network, the simulator applies the proposed surviving plan in two case studies as follows.

Case study1:

The number of dead nodes reaches the ratio of 50% of total nodes in the network. Figure (7) shows the appeared massage of requesting the number of compensating nodes. After selecting the compensating node number, the authentication procedure is applied and in this case, all the added nodes are authenticated as shown in Figure (8). The network is continue to working until reaching 50% of system behavior or 35% according to explained surviving plan algorithm.


Number Of Active Nodes: 9
Number Of Sleep Nodes: 0
Number Of Died Nodes: 8
Number Of unauthorised Nodes: 0

Maintaince Network

Write the number of replaased Nodes out of :8

8

Fig. 7. Maintenance Network Message

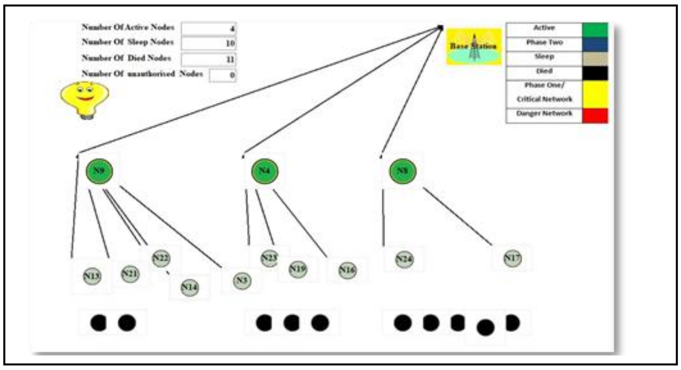
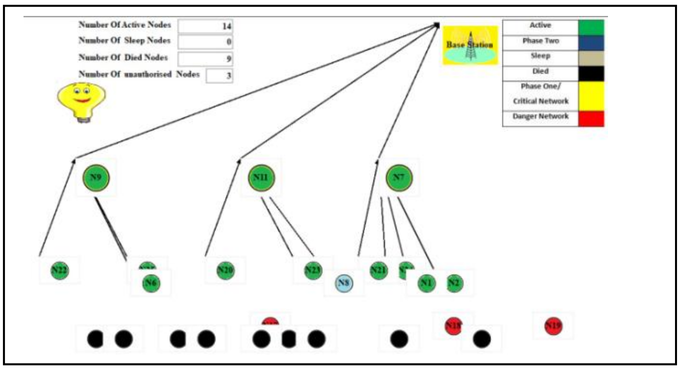

Number Of Active Nodes: 4
Number Of Sleep Nodes: 10
Number Of Died Nodes: 11
Number Of unauthorised Nodes: 0

Fig. 8. All compensated nodes added are Authenticated

Case study2:

In this case, the message of required compensating nodes of Figure (7) answered. Here, the authentication algorithm applied to the added nodes. Three of them are not authenticated, colored by red, due to missing in the initial key of such nodes as shown in Figure (9).

In abnormal case when added nodes not all of them is authenticated because does not have initial authentication network, the Figure (7) show this case , notes the red nodes is the node not authenticated but the green nodes are authorize.



Number Of Active Nodes 14
Number Of Sleep Nodes 0
Number Of Died Nodes 9
Number Of unauthorised Nodes 3

Fig. 9. Three added nodes are authenticated

V. Conclusion

A network surviving plan for the WSN has been proposed. The proposed plan was performed by adopting the ration of 50% of dead nodes among the total ones to be run. The reason behind the surviving procedure was to keep the WSN in high efficiency of working. At the other hand, a simulator was proposed to simulate the adopted protocols and the introduced system without the need for conventional one of NS2 and NS3. The conventional simulators were not supporting the lightweight protocols. The obtained results showed over two case studies and the obtained results showed the accepted performance to keep the efficiency of the considered WSN.

REFERENCES

[1] Shaymaa Mahmood Naser and 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, 2018.

[2] 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), Vol 4, No 4, 2015.

[3] Lidong Zhou and Zygmunt J. Haas, “Securing Ad Hoc Networks”, IEEE network, special issue on network security, P.P. 24-30, 1999.

[4] Yuanyuan Zeng, Cormac J. Sreenan, Naixue Xiong, Laurence T. Yang and Jong Hyuk Park, “Connectivity and coverage maintenance in wireless sensor networks”, Springer Science and Business Media, 2009.

[5] A. S. M. Sanwar Hosen, Seung-Hae Kim, and Gi-Hwan Cho, “An Energy Efficient Cluster Formation and Maintenance Scheme for Wireless Sensor Networks”, Journal of Information and Communication Convergence Engineering, Vol 10, No. 3, P.P. 276-283, 2012.

[6] Skander Azzaz and Leila Azouz Saidane “Maintenance strategies for wireless sensor networks: from a reactive to a proactive approach”, Transaction on Emerging Telecommunication Technologies, 2013.

[7] Danyang Qin, Shuang Jia, Songxiang Yang, ErfuWang, and Qun Ding, “A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks”, Journal of Sensors, 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 Croock 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.