International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Authenticated Node and Replicated Node in Wireless Sensor Networks Based on Location and Distance Information

Dr. Jamal Mohammed Kadhim[1], Enas Faris Yahya[2]
[1]Department of Computer Science, College of Science, AL-Nahrain University, Baghdad, Iraq
[2]Department of Computer Science, College of Science, AL-Nahrain University, Baghdad, Iraq
Email address: drj amal.cs@gmail.com, enasfaris2007@gmail.com

Abstract— *Sensor networks support the collection and transmission of large volume of data from different deployed environments, each sensor captured data from a monitored field and send it to the base station. Node authentication is an important security challenge in wireless sensor network (WSN) and it is the main requirement to check the node authentication of the received data at BS. Authentication process of the node was insured in each sensor node by stored the location information for the neighboring nodes. To ensure the authentication process for all attached node, firstly the BS employ redundant messages to require the location information about each attached node and store it in the database. Each sensor node embeds a unique location information and can use it to verify the node authentication and detect replication attack In this paper, there is three types of devices have been used in building a system that detected any replication node, these devices are an Ultrasonic sensor, Arduino Uno, NodeMCU esp2866.*

Keywords— *Node authentication, Replication node, Sensor node, Replication attack.*

I. INTRODUCTION

WSN shares some sensitive data, the perceived data are vulnerable to external or internal attacks in the transmission. The attacker can easy falsify data and send unauthorized data in the transmission[1]. Many researcher and companies had been attracted to the invention of wireless sensor networks (WSNs) and developed it to help us gathering information from surrounding environments. WSNs usually consist of a large number of wireless sensor nodes spread over a large field. The sensor node has the ability to contact with each other over wireless channels, able to perform a signal processing and routing of data. WSNs are standard solution for collecting data and transmitting in a variety of environments. The following figure 1 shows what a typical wireless sensor node looks like[2].

Fig. 1. Sensor node (sensor developed by Genetlab Company)

WSNs nodes can sense the environment, and communicate with neighboring nodes. Detection and monitoring process can be used in a variety of physical parameters through the sensors. WSNs have been deployed in many applications. The variety of possible application of WSNs are practically unlimited. They include Forest Fire Detection, Air Pollution Monitoring, Military Application, Medicine and health care, Traffic Monitoring, Environment Monitoring, Temperature, Tracking, Smart Home Environment Monitoring, Temperature, Tracking, Smart Home[3].

The security requirement is to reject any message has been altered by malicious node this is called verification process. The authentication process is useful in showing that no tampering has occurred during transmission and the message received from authorized source[4]. The most-critical issue of sensor network applications denote that any replicate data due to a malicious attack that can cause significant damage to the network. We classify sensor network attacks into three main categories; routing attacks, network attacks, identity attacks[5], and as shown in figure 2.

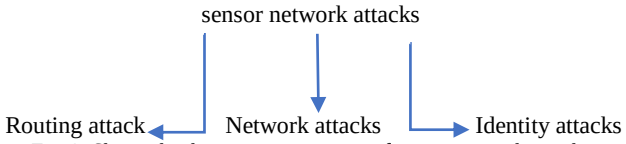

Fig. 2. Shows the three main categories of sensor network attacks

Routing attack which happening in the routing path between source to the base station. This kind of attack is attempt to tamper with data or discard data packets. Network attacks means any unauthorized access to a system by the attacker. Identity attacks intend to theft the identities of legitimate nodes in the sensor networks. The replication attack is kind of identity attack. In replication attack, the attacker attempt to add one or more nodes to the network that use the same ID. In this article, we explain the identity attack as called replication attack. The detection of node replication attacks in WSN is important problem. In sensor network system, any adversary node can capture the data, code stored in it. In this case, the attacker easily replicates a large number of clone's node and deploy them on the network. The detection method of replication attacks was introduced by any cloned node attempts to communication with the other sensor node can be detected by protecting the establish pair-wise keys[5]. The sensor network monitors the parameters or values and report

Dr. Jamal Mohammed Kadhim and Enas Faris Yahya, "Authenticated Node and Replicated Node in Wireless Sensor Networks Based on Location and Distance Information," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 4, pp. 133-137, 2019.

to the sink node about the values. Attacker can monitor the traffic and add the wrong information between the sensor network with the base station[6].The sensor nodes are limited in power, processing capacity, and storage, the lightweight techniques are needed to fulfil these requirements[7]

II. Literature Review

- V. Manjula et al., in 2011[5] introduced distributed detection in which any sensor node stores the location information for its neighbors. Each node employs the redundant messages or authenticated acknowledgment to try the process of node authentication between each sensor node that connected to the network. Each node finds the sensor node location and ID that stored in each sensor node and produced a report to the base station if it finds the same ID in the different location to detect the replicas. The simulation results achieve 100% detection of all duplicate node ID.
- Wen Tao Zhu et al., in 2012[8] introduced brood casting and multicasting approach in which every node collects all its neighbors its and their location and check the collected information about neigh boring node with the message that received from broadcast messages from the base station each node stores the location information and nod ID for its neighbors and use it to cheek the authentication each location broadcast messages and generally in every node in the WSN, the total communication cost was biggest. The simulation results achieve 100% detection to find all replicated node.
- Chakib Bekara et al., in 2012[9] introduced protocol for detection of node replication based on using of symmetric polynomial. In this protocol, the idea is tie each deployed node to the unique generation through the use of symmetric any so that cloned node are created, the cloned also run the same generation as an authenticated node. The idea of this protocol is only newly node are able to establish pair-wise keys with the neighbors, if this process fail, then the cloned node cannot succeed to populate the network. The simulation results achieve less memory, computation and transmission overheat.
- Al-Sakib Khan Pathan et al., in 2006[6] introduced a holistic approach to improving the performance of WSNS also with respect to security. This approach aims to involving all the layers for ensuring overall security in the network. If the security is not ensured in one layer despite there are some efficient security in the other layers then the security considered is not ensured for all the layers.
- Djallel Eddine Boubiche et al., in 2015[10] introduced a lightweight hash function as called a fragile watermark to detected any alteration by the attacker in the rounding path between the sensor node and the base station. The node authentication process was ensured between the sensor node and the base station. The watermark is generated and integrated into each packet. The simulation results introduced very low energy consumption over the network and a good level of security.

III. Proposed Hardware Building Of Sensor Node

Arduino Uno, NodeMCU, Ultrasonic sensor, liquid crystal display has been linked together to design the proposed sensor node. Arduino Uno used to read the signals from Ultrasonic sensor, processing the signals and report as a distance value between each sensor node by operating the equation of the distance as shown below:

Distance = Speed × Time/ 2 (1)

The product of speed was divided by 2 because the total time it took when the waves arrive to the target and return back to the echo pin. The Ultrasonic sensor connected to the Arduino Uno board at pins (4,5) the trig pin is configured as a pin 4 in the Arduino board and the echo pin is configured as pin 5 in the Arduino board, Vcc pin connected to 5V in Arduino board and G pin connected with ground pin in Arduino board.

The Arduino Uno is connected with the NodeMCU ESP 8266 to transmitting the message to the base station through the wireless device. Arduino Uno is connected with NodeMCU by these pins (5,6) (7,8). Pins (6,7) from the Arduino side and pins (7,8) from the NodeMCU side. These pins are configured as a software serial between them. Liquid crystal display connect to the Arduino Uno at the pins (A4, A5), used the liquid crystal as a display to illustrate the distance value, and as shown in figure 3.

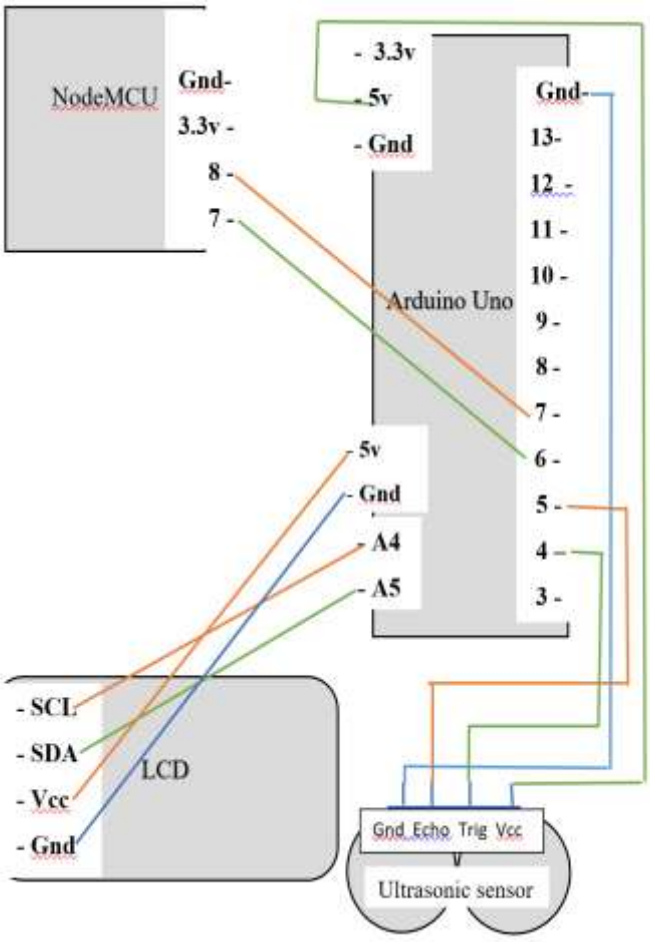

Fig. 3. Building hardware components of the sensor node

Dr. Jamal Mohammed Kadhim and Enas Faris Yahya, "Authenticated Node and Replicated Node in Wireless Sensor Networks Based on Location and Distance Information," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 4, pp. 133-137, 2019.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

IV. Proposed Software Building Of Sensor Node And Sink Node

The overall architecture of our system is represented by the block diagram. The system splits into two parts; sensor node and sink node, and as shown in Figure 4.

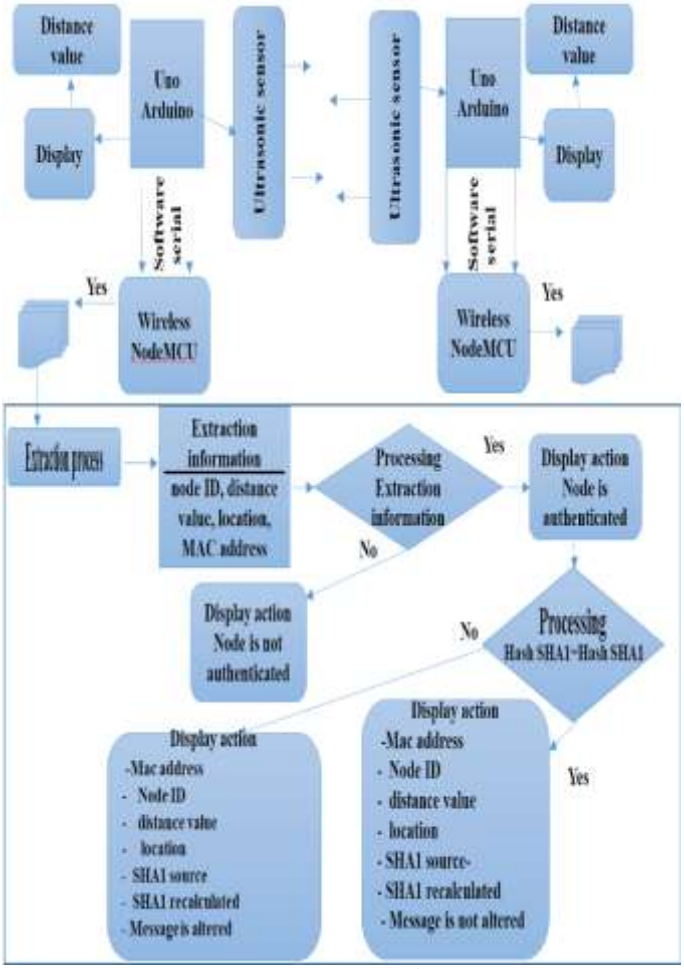

Fig. 4. General architecture of the system

In the building mechanism, the sensor node applied an XOR function to combine the data that collected from sensor, MAC address, node ID, distance value, location and one-way hash function. A one-way hash function applied to get 160 bits fixed size digest which represents the generated watermark.

A. The Sensor Nodes Level

A.1 Transmitting message

When the object moved in front of the sensor, the sensor sent the signal to the Arduino Uno and calculating the distance value, after that the Arduino Uno sent the distance value to the NodeMCU. The Arduino Uno listen to the WiFi status for the NodeMCU, if the NodeMCU connected to the WiFi network. If the NodeMCU connected to the WiFi network, then it calculated the hash function by SHA1 and then make the final data packet by adding the node name, MAC address, location distance value and SHA1 and then sent it to the sink node by NodeMCU ESP8266, and as shown in figure 5.

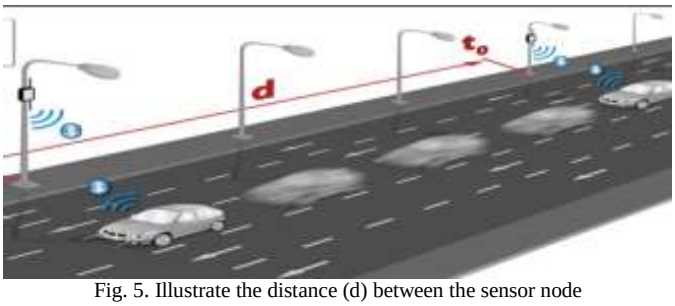

Fig. 5. Illustrate the distance (d) between the sensor node

A.2 Receiving message

The sensor node received the broadcasting message in the first time when the sensor network was building. The broadcasting message contain the node ID, location for all node, Mac address, distance value between all node and then stored in each node.

B. The Sink Node Level

B.1 Receiving message

When the data packet received from the sensor node, the sink node extracted the node ID, distance value, location and Mac address and then compare it with the information that stored in the database that related with the node ID. If all information that related to the node are equal, then the action is: the node is authenticated. After that the sink node extracted the hash function from received data packet and recalculated the hash function for the received data packet and then compare between two hash function, if the two hash are equal then data packet is not altered and the sink node extracted the information from the data packet and display it in the software window, but if the two hash function are not equal then the data packet is altered. But if the location and distance value are not equal then the action is the node is not authenticated and reported as that the node is cloned.

B.2 Transmitting message

When the system was building, each node attached to the network must be assigned and defined by adding the information about node ID, location, Mac address and calculating the distance value between each two sensor node and stored it in the data base. The system was sharing this information that stored it to all the sensor node by broadcasting message. Each sensor node stored this received broadcast message to verifying the authentication node.

V. Hardware And Software Experiment Results

This section covers a reviewed and presented of the experiment results for the proposed system of WSNs. Different scenarios are implemented to review and illustrate the experiment results about node authentication, data integrity between two nodes for our proposed scheme in our system.

A. Rate Test Results for Our Sensor Node

A.1 Generating the distance value

In the sender node, each sensor execution some specific task. In our scheme, calculating the distance value and the time that take to calculating the distance value between two sensor node. This process needs to verified an authenticated

Dr. Jamal Mohammed Kadhim and Enas Faris Yahya, "Authenticated Node and Replicated Node in Wireless Sensor Networks Based on Location and Distance Information," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 4, pp. 133-137, 2019.

node, Table 1 shows the distance value and time in our proposed procedure.

TABLE 1. Shows the distance value and time in our proposed procedure.

No.	Details	Distance in (cm)	Time in (microseconds)
Case 1	Node 1 – node2	100	5928
Case 2	Node 1 – node2	200	11768
Case 3	Node 1 – node2	300	19039
Case 4	Node 1 – node2	350	20450

A.2 Insert the location for each node

In our proposed procedure, location information and MAC address for each node should be stored in the database to identified the node that attached into the system. The figure 6 shows the details about location information and MAC address for our nodes.

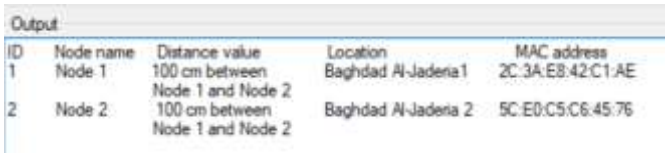

Fig. 6. Shows the location information and MAC address for our nodes.

A.3 Generating hash algorithm

The NodeMCU combined the node ID, data that collected from environment, location, distance value and string MAC address through XOR function to obtain a final message. NodeMCU calculating the SHA1 hash function for message and sent the final data packet to the sink node, and as shown in the algorithm1.

```
Algorithm 1
Input: Node ID, String MAC address, location, distance value, data
Output: Generated final message through hash SHA1
Begin:
Step 1: If data received from Arduino Uno then
        Get MAC address
Step 2: Prepare message to hash (Node ID, string MAC address,
location, distance value, data)
Step 3: Generating hash SHA1
        Let X=0              initial value for hash counter
        Let i=0              initial value for loop counter
        Let i=20             Upper limit for loop counter
        For i= 0 to 20
        Return X
        Return X+1
        X+2
        End For
Step 4: XOR function to obtain a final message
          Final message = Node ID + MAC address + data +
              location + distance value + hash SHA1
        Send final message to the sink node
        else
        Still listening to Arduino Uno
        End IF
End.
```

B. Rate Test Results for Our Sink Node

B.1 Extraction message and check the node is authenticated

The data packet received from the sensor node, the sink node extracts the received node ID, location information, distance value, MAC address and compare it with information stored in the database to verified the node authentication, and as shown in algorithm 2. The two case below explain the action in the sink node.

In the first case, if all the information is identical then the sink node extracted the hash function from received data packet and recalculated the new hash function and compare between two hash function to verified the data integrity and gives a report that the data is changed or not. The sink node reported us all information about the message received and take action, and as shown in figure 7.

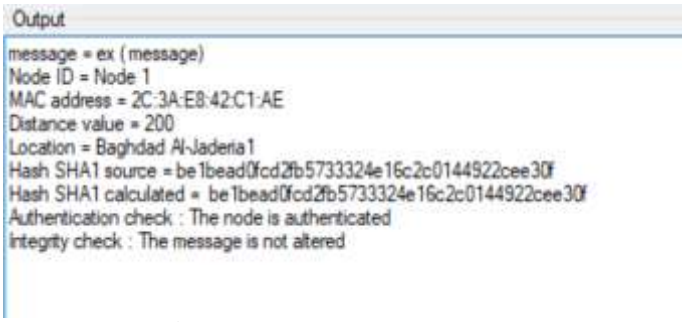

Fig. 7. Shows all information about the message and action about the message

In the second case, if the node is authenticated but the information is altered, then the action of the sink node is reported us that the message is altered, and as shown in figure 8.

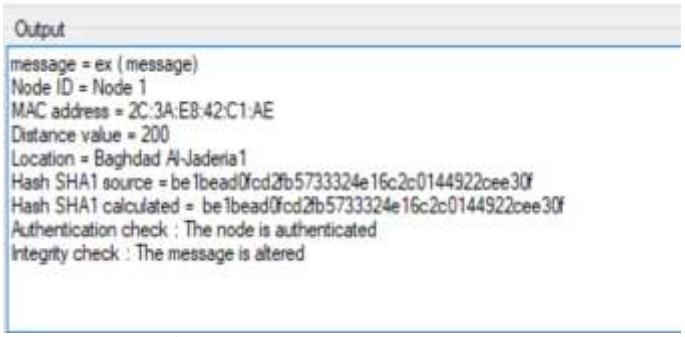

Fig. 8. shows all information about the message and action about the message

```
Algorithm 2
Input: Node name" Node 1"
Output: Authentication status ("Node is authenticated", " Node is not
authenticated")
Begin:
Step 1: If sink node received message from sensor node then
Step 2: Sink node extracted Node ID
        If Node ID = Node ID stored in the database, then
        Extracted total information from message
        Reported "Node is authenticated"
        else
        Reported "Node is not authenticated"
        End If
        End If
End.
```


Dr. Jamal Mohammed Kadhim and Enas Faris Yahya, "Authenticated Node and Replicated Node in Wireless Sensor Networks Based on Location and Distance Information," *International Research Journal of Advanced Engineering and Science*, Volume 4, Issue 4, pp. 133-137, 2019.

B.2 Extraction message and check the node is not authenticated

The sink node extracted the information that received from sensor node and compare it with information that stored in the database. If one of these information is not identical, then the sink node know that the message received from this node is not authenticated, if the node is not authenticated the sink node reject the message, and shown in figure 9.

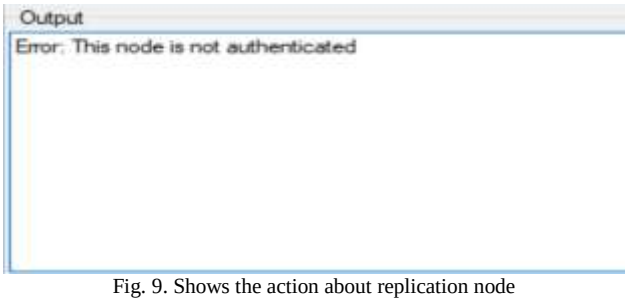

Fig. 9. Shows the action about replication node

B.3 Regenerated hash function

If the sink node verified the node authentication, the sink node extracted the Node ID, MAC address, distance value, location and received SHA1. The sink node generated a new hash SHA1 and compare between two hash, and as shown in algorithm 3.

```
Algorithm 3
Input: Node ID, String MAC address, location, distance value
Output: Generated new hash SHA1
Begin:
Step 1: If Node is authenticated then
Step 2: Prepare message to hash (Node ID, string MAC address,
location, distance value)
Step 3: Generating new hash SHA1
        Let X=0          initial value for hash counter
        Let i=0          initial value for loop counter
        Let i=20         Upper limit for loop counter
        For i= 0 to 20
        Return X
        Return X+1
        X+2
       End For
Step 4: If received hash = new hash then
      Reported "Integrity check, the message is not altered "
        else
        Reported "ERROR: The message is altered"
        End If
        End If
End.
```

VI. Conclusion

In this work, specifications were introduced to preserve node authentication in WSNs. A set of requirements has been described to make data transfer process safe and was implemented using lightweight methods to provide speed and good protection to the sensor node. Location and distance value was used to improve the performance against nodes replication. The use of XOR function was successful in our system. This mechanism was successful to detect the replication node in the network.

Acknowledgment

I special thanks to my supervisor Dr. Jamal Mohammed Kadhim who gave me all the supporting, assistance for giving me the major steps to go on to explore the subject. Grateful thanks are due to the Head of Computer Science Department and the staff of the Department at College of Sciences of AL-Nahrain University for their kind attention.

References

[1] Sun, B.W.-J.S.-Y.Z.-B.W.-J.S.-Q.D.-X.: 'A Copyright Protection Method for Wireless Sensor Networks Based on Digital Watermarking', International Journal of Hybrid Information Technology, Vol. 8, no. 6, 2015.
[2] Tranter, W.: 'Node Localizationin Wireless Sensor Networks',2017
[3] Yang, P.S.-H.: 'Wireless Sensor Networks_ Principles, Design and Applications-',2014
[4] Al-Jaber, R.S.A.-A.: 'AFragile Watermarking algorithm for content authentication ', International Journal of Computering and information sciences 2004.
[5] Chellappan, V.M.a.C.: 'The Replication Attack in Wireless Sensor Networks: Analysis and Defenses', Springer, 2011.
[6] Al-Sakib Khan Pathan, H.-W.L., Choong Seon Hong: 'Security in Wireless Sensor Networks: Issues and Challenges', 2006
[7] Jennifer Yick, B.M., Dipak Ghosal *: 'Wireless sensor network survey', Elsevier 2008
[8] Zhu, W.T., , J.Z., , R.H.D., and , F.B.: 'Detecting node replication attacks in wireless sensor networks: A survey', 2012
[9] Laurent-Maknavicius, C.B.a.M.: 'Defending Against Nodes Replication Attacks on Wireless Sensor Networks', 2012
[10] Athmani, D.E.B.-S.B.-H.T.-C.-A.-S.K.P.-A.B.-S.: 'SDAW: secure data aggregation watermarking-based scheme in homogeneous WSNs', Telecommunication Systems, 2015, 62, (2), pp. 277-288