International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 9 (2019) pp. 2084-2088
© Research India Publications. http://www.ripublication.com

# Cluster-Based Hierarchical Message Authentication Code to Secure Data Dissemination in Wireless Sensor Network (CHiMAC)

**Hind A. Alrubaish**
*Department of Computer Science*
*College of Computer Science and Information Technology*
*Imam Abdulrahman Bin Faisal University*
*P.O. Box 1982, Dammam 31441, Saudi Arabia.*

**Rachid Zagrouba**
*Department of Computer Information System*
*College of Computer Science and Information Technology*
*Imam Abdulrahman Bin Faisal University*
*P.O. Box 1982, Dammam 31441, Saudi Arabia.*

## Abstract

Wireless Sensor Networks (WSN) attract the researcher's attention over the last years. As the number of WSN applications in different areas is increasing, the need for a robust, reliable scheme is necessary. WSN suffer from the various limitation that makes the network vulnerable to numerous attacks; hence this paper proposed an improved scheme using Hierarchical Message Authentication Code and identity-based cryptography to secure data dissemination in cluster WSN. The scheme should prevent interception attack by dividing the message into two encrypted blocks; another encrypted block is added that contains IDs of source and destination nodes in addition to heads' IDs based on the communication level (WSN, Zone, Cluster). The scheme also prevents tampering and replay attacks by adding a timestamp, signing and encrypting the block at each trusted intermediate node. The cryptography load distributed among the trusted neighborhoods.

**Keywords:** Hierarchical, Message Authentication, Wireless Sensor Networks, Information Security, Encryption.

## I. INTRODUCTION

Wireless Sensor Networks (WSN) comprise of hundreds or thousands of tiny devices called nodes (sensors), that intended to perform a collaborative measurement process to accomplish critical objectives. As WSN nodes deployed in a large remote geographical area, the physical security not a realistic option which leaves nodes unattended and vulnerable to various attacks, hence robust security mechanism should be applied. Several studies have tried to address the security from various aspects; some tried to enhance the confidentiality or the integrity or the availability.

This paper introduced Hierarchical Cluster Message Authentication Code (CHiMAC) to Secure Data Dissemination in Cluster Wireless Sensor Network which is an improved scheme of [1]. The aim is to ensure the security requirements using the cluster structure of WSN and Message Authentication Code (MAC), where the message is delivered securely.

The rest of the paper organized as follows; Section II presents an overview of the cluster structure in WSN. Section III addresses the state of the art in WSN's security. Section IV introduces the proposed scheme. Finally, section V concludes the paper and provide future work.

### A. Cluster Structure in WSN

Each WSN has a Base Station (BS) that report collected data to end users, the process of collecting data from all nodes cause overhead to the network and consume a lot of energy [2]. To reduce these drawbacks, collections of nodes can be grouped to form zones or/and clusters. WSN divided into zones and each zone divided into clusters, each zone has Zone Head (ZH), and each cluster has Cluster Head (CH). Each head represents and manages its region, coordinates and communicates with other heads and aggregate the data of its region to be forwarded in a hierarchal structure as shown in figure (1). The selection of the head node achieved through various mechanisms such as; a node with the highest weight or a node that more extensive capabilities than the other members. [3].

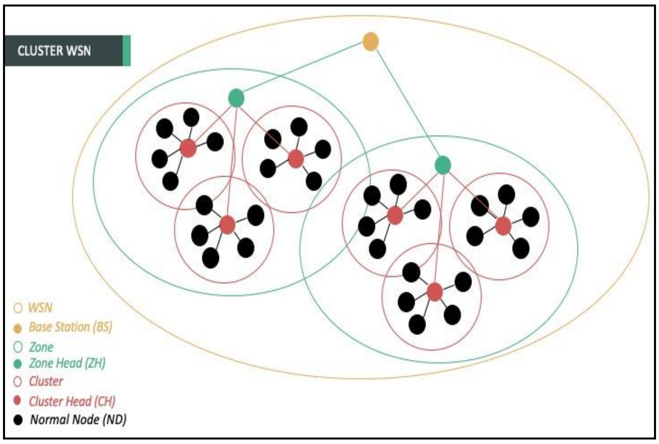


**Figure 1:** Cluster WSN

### B. Main Security Requirements in WSN

For any WSN there are main requirements should be considered to ensure the network's security:

***Confidentiality:*** The assurance that the message hidden from attackers during transmission.

***Integrity:*** The assurance that the message is complete and accurate and has not been altered or tampered, as well as the message's route.

***Availability:*** The assurance that the message has been delivered successfully to its destination.

***Authentication:*** the assurance that each node is who claims to be.

### C. *Message Authentication Code (MAC)*

There are various techniques to authenticate the message such as; $\mu$TESLA, SNEP, LEAP, fast authenticated key establishment protocols for self-organizing sensor networks, user authentication and Message Authentication Code (MAC). MAC is enclosed within the packet where the sender node combines the message and the key to generate MAC using the hash function MAC = H {M ‖ K}. The receiver generates the MAC using the message and the shared key. If MAC = MAC then the message is authenticated, and the sender is legitimate, as shown in figure (2) [4].

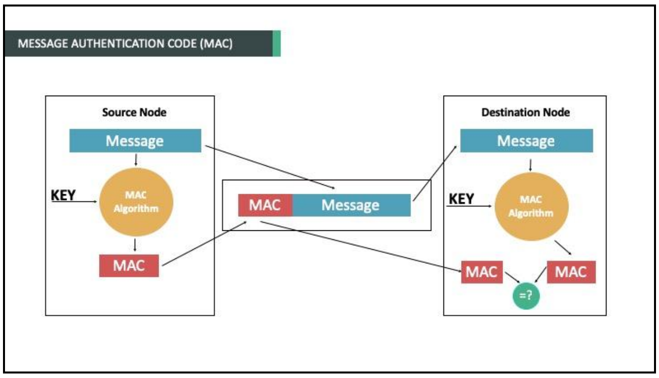


**Figure 2:** Message Authentication Code (MAC)

## II. LITERATURE REVIEW

Bohge and Trappe [5] uses a sensor network that consists of three tiers of devices. Each level has different computational capabilities; the lowest tier cannot be involved in the public key cryptography. They proposed a new certificate called TESLA which can be used by low powered nodes to authenticate incoming nodes during the handoff scheme and to provide data origin data authentication for sensor's data. The authentication process assigned to the nodes according to their capabilities.

Wu [6] proposed a simple authentication protocol for WSN based on a centralized trust model, hierarchical clustering structure and the asymmetric cryptographic algorithms, where the head of the cluster selected in a decentralized way. During the network's operation, cluster heads can aggregate data from sensor nodes and transmit it to the base station using the shared session key securely. The workflow in the proposed approach flows from the control center through the base station to the cluster head and finally to the sensor node. Authentication achieved through the asymmetric cryptography and the data transmission is protected using hash algorithms.

Trevathan *et al.* [7] presented a framework to perform an efficient authentication process in a hierarchal WSN where the messages are verified as batches. If a sensor node cannot perform the verification, it can sign the batch and pass it to up to another node to start the verification process. The proposed approach allows a fake signature to be discovered easily.

Othman and Yousif [8] proposed a scheme to achieve authentication, confidentially and integrity to secure the aggregated data in WSN. Their approach uses homomorphic encryption and message authentication code.

Abduvalive *et al.* [9] presented simple hash-based message authentication and integrity code algorithms for WSN where the scheme uses a pre-shared secret key that obtained from Elliptic Curve Diffie Hellmann (ECDH) key exchange algorithm and based on the modified SHA-1 (mSHA-a) function to compute the message authentication code.

Chowdhury and DasBit [10] proposed a lightweight function to compute message authentication code which is customized for WSN. The approach based on lightweight hash function LOCHA. Also, they use operations like XOR, premutation box in the computations to reduce the overhead.

Mershad *et al.* [1] presented a trust-based mechanism in hierarchal message authentication code to secure data dissemination in WSN. Their mechanism prevents attackers from tampering data packet or modifying their hop count by signing and encrypting the packet at each node. They added a new parameter "trust" to the routing table and each node's neighborhoods. The values of this parameter are; malicious, ambiguous, potentially trusted and trusted. The purpose of this parameter is to identify the trustworthiness of each incoming node based on their identity not their behavior during the time.

Also, they proposed a hierarchical security protocol for message authentication and encryption (HiMAC). Where each packet contains two blocks; payload block which includes the message ($M_S$), timestamp value ($T_s$) and the signature generated using MAC algorithm ($M_{algo}$) while the other block contains a list ($ID_L$) of traversed nodes IDs between the source and destination nodes, each block encrypted separately. Each node between the source and destination is repeated the same process and add its ID to the second block; the scheme illustrated figure (3).

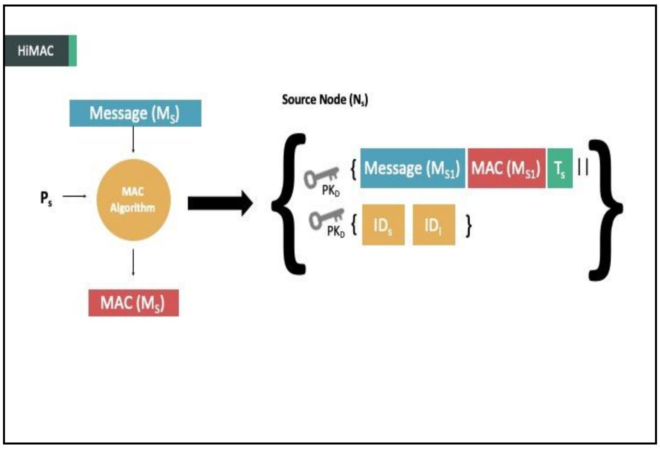


**Figure 3:** HiMAC scheme

## III. PROPOSED SCHEME

Many researchers tried to propose and implement various solutions to build a robust and high trusted mechanism, this paper we adopt scheme used in [1] with some modifications to enhance the WSN's security and to be accommodated in cluster WSN.

This section explains the proposed scheme, then compare the original scheme and the modified scheme.

### *A. CHiMAC Scheme Description*

After nodes deployment, each head zone and head cluster declare itself as a head by broadcasting its identity (ID) to its nodes, each member node has the ID of its head cluster and head zone in addition to the base station's ID which is kept for further authentication.

The proposed scheme works as the following; If node A wants to send a Message ($M_S$) to node E through the following nodes; B, C, D, node A divides the message into two payload blocks; each block uses node A's private key ($P_S$) to generate Message Authentication Code (MAC) using MAC algorithm ($M_{algo}$), then it combined with Timestamp ($T_s$) in addition to the part of the message into one block. After that, each block is encrypted using the destination's public key ($PK_D$).

Another block called IDs List ($ID_L$) is added after encrypting it using the $PK_D$, $ID_L$ contains; Source ID ($ID_S$), Intermediate Node ID ($ID_I$), Cluster Head ($ID_{CH}$) – based on the level of the communication more IDs can be added-. Finally, the Cyphered Message ($M_{cypher}$) contains three blocks; $M_{S1}$, $M_{S2}$, $ID_L$ as shown in figure (4).

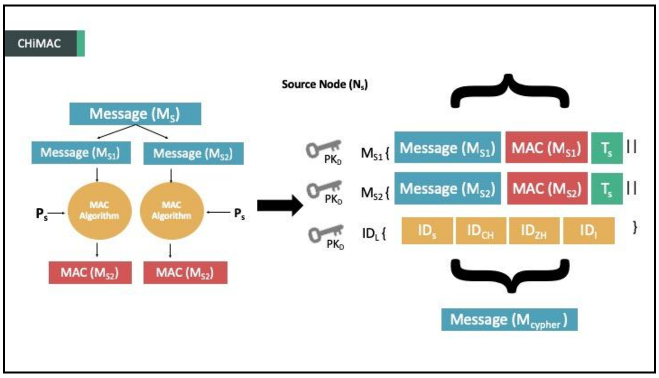


**Figure 4:** Illustrate the proposed (CHiMAC) scheme at the source node

Then node A scans the possible routes to reach node E; the selection is based on a trust model approach that has been proposed in [1]. While the message travels through nodes, each node repeats the same process explained in figure (3) except that it encrypts the $M_{cypher}$ instead of $M_S$ and add its $ID_I$ to the $ID_L$., When node E receives $M_{cypher}$ it decrypts each block using it Private Key ($P_D$) and check the received values of Cluster Head ($ID_{CH}$), Zone Head ($ID_{ZH}$) with their values that it already has it, as shown in figure (5).

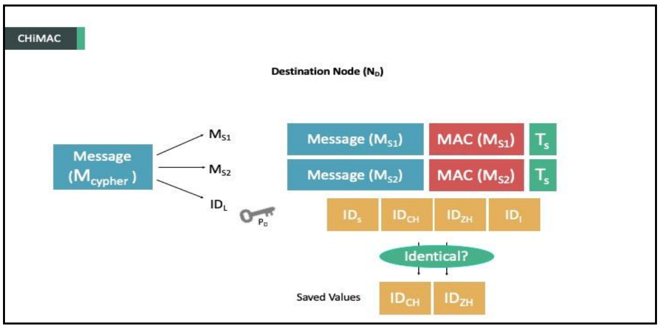


**Figure 5:** First step at the destination node using (CHiMAC): Check heads ID

If the values are not identical, the message's integrity has been breached; otherwise, it decrypts $M_{S1}$ and $M_{S2}$ using $P_D$ and extract ($M_{S1}$, MAC($M_{S1}$), $T_s$) & ($M_{S2}$, MAC($M_{S2}$), $T_s$). After that the node checks the validity of MAC ($M_{S1}$ & $M_{S2}$) by applying $M_{algo}$ ($M_{S1}$ + MAC($M_{S1}$) + $PK_I$) & $M_{algo}$ ($M_{S2}$ + MAC($M_{S2}$) + $PK_I$) to ensure the message's integrity. This process is repeated for each intermediate node -between source and the destination- in the list until $ID_L$ is empty. During each iteration, the value and the sequence of $T_s$ are checked to ensure there is no old $T_s$ or out of sequence, figure (6).

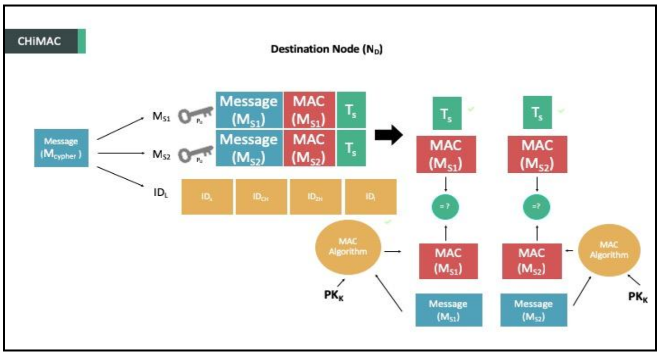


**Figure 6:** First step at the destination node using (CHiMAC): Validity of MAC and time stamp

Finally, if all the intermediate nodes are trusted and the values of the heads are matched the declared values and no $T_s$ out of sequence, this means that message is *authenticated*, figure (7).

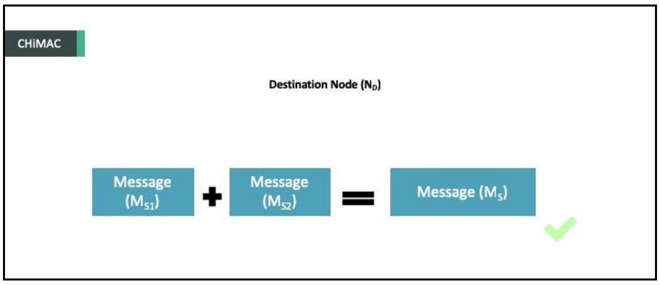
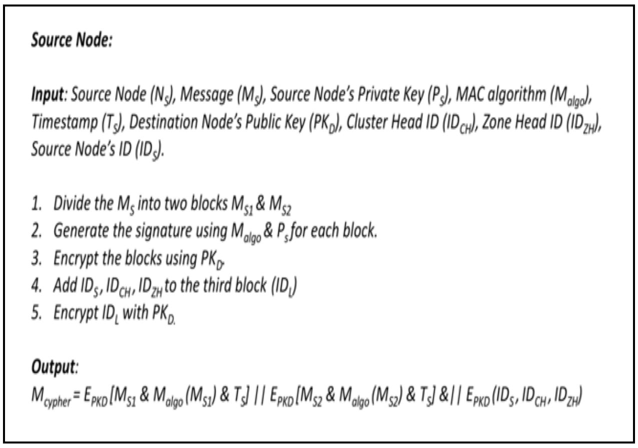


**Figure 7:** Final step at the destination node using (CHiMAC): Combine the message parts after authentication

*** Note**: *The IDs that will be added to $ID_L$ it will be based on the level of communication; (1) Nodes within one cluster:*

*(Intermediate nodes ID + $ID_{CH}$), (2) Nodes within one zone: (Intermediate nodes ID + $ID_{CH}$ + $ID_{ZH}$), (3) Nodes within one WSN: (Intermediate nodes ID + $ID_{CH}$ + $ID_{ZH}$ + $ID_{BS}$).*

The algorithm of CHiMAC at the source and destination nodes have been illustrated in Figure (8) and Figure (9).



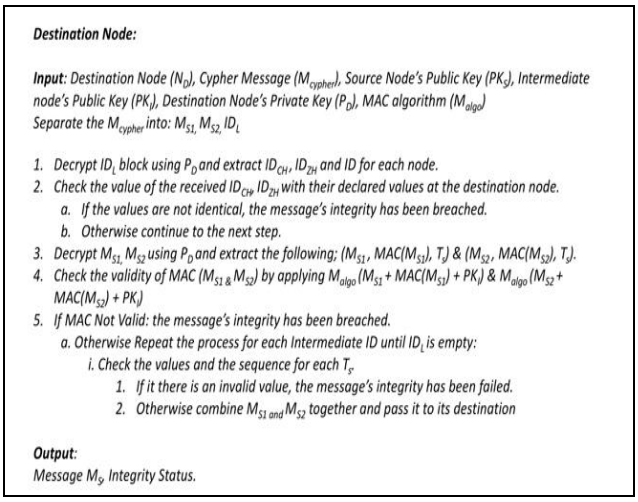
```
Source Node:

Input: Source Node ($N_S$), Message ($M_S$), Source Node's Private Key ($P_S$), MAC algorithm ($M_{algo}$),
Timestamp ($T_S$), Destination Node's Public Key ($PK_D$), Cluster Head ID ($ID_{CH}$), Zone Head ID ($ID_{ZH}$),
Source Node's ID ($ID_S$).

1. Divide the $M_S$ into two blocks $M_{S1}$ & $M_{S2}$
2. Generate the signature using $M_{algo}$ & $P_s$ for each block.
3. Encrypt the blocks using $PK_D$.
4. Add $ID_S$, $ID_{CH}$, $ID_{ZH}$ to the third block ($ID_L$)
5. Encrypt $ID_L$ with $PK_D$.

Output:
$M_{cypher} = E_{PKD}[M_{S1}$ & $M_{algo}(M_{S1})$ & $T_S] \,||\, E_{PKD}[M_{S2}$ & $M_{algo}(M_{S2})$ & $T_S]$ & $||\, E_{PKD}(ID_S, ID_{CH}, ID_{ZH})$
```

**Figure 8:** Algorithm of CHiMAC at the source node



```
Destination Node:

Input: Destination Node ($N_D$), Cypher Message ($M_{cypher}$), Source Node's Public Key ($PK_S$), Intermediate
node's Public Key ($PK_I$), Destination Node's Private Key ($P_D$), MAC algorithm ($M_{algo}$)
Separate the $M_{cypher}$ into: $M_{S1,}$ $M_{S2,}$ $ID_L$

1. Decrypt $ID_L$ block using $P_D$ and extract $ID_{CH}$, $ID_{ZH}$ and ID for each node.
2. Check the value of the received $ID_{CH}$, $ID_{ZH}$ with their declared values at the destination node.
    a. If the values are not identical, the message's integrity has been breached.
    b. Otherwise continue to the next step.
3. Decrypt $M_{S1,}$ $M_{S2}$ using $P_D$ and extract the following; ($M_{S1}$, MAC($M_{S1}$), $T_S$) & ($M_{S2}$, MAC($M_{S2}$), $T_S$).
4. Check the validity of MAC ($M_{S1}$ & $M_{S2}$) by applying $M_{algo}$ ($M_{S1}$ + MAC($M_{S1}$) + $PK_I$) & $M_{algo}$ ($M_{S2}$ +
   MAC($M_{S2}$) + $PK_I$)
5. If MAC Not Valid: the message's integrity has been breached.
    a. Otherwise Repeat the process for each Intermediate ID until $ID_L$ is empty:
        i. Check the values and the sequence for each $T_S$.
            1. If it there is an invalid value, the message's integrity has been failed.
            2. Otherwise combine $M_{S1}$ and $M_{S2}$ together and pass it to its destination

Output:
Message $M_S$, Integrity Status.
```

**Figure 9:** Algorithm of CHiMAC at the destination node

*B. CHiMAC Advantages*

The following security requirements have been achieved by CHiMAC:

***Confidentiality****:* The confidentiality of CHiMAC is enhanced by dividing the message itself into two blocks where each block is encrypted separately.

***Integrity****:* (1) The integrity of CHiMAC is ensured by the hierarchal authentication of every intermediate node and cluster head and zone head to prevent attackers from capturing or altering the message. (2) Checking the $T_s$ at the receiver side in each iteration to ensure that there are no old values or out of sequence.

***Authenticity****:* The authenticity of each node is ensured using the hierarchical message authentication code.

Table (1) summaries the added value of CHiMAC over HiMAC in clustered WSN

**Table 1:** CHiMAC Advantages

| | ***HiMAC (Mobile ad-hoc networks)*** | ***CHiMAC (Cluster WSN)*** | ***Security Requirements*** |
|---|---|---|---|
| # blocks in the message | **Two** (Message and List of IDs) | **Three** (Message Part 1, Message Part 2 and List of IDs) | Confidentiality |
| Authentication Process | ID of the sender and each node where the message will pass through | ID of the sender, each node where the message will pass through, (cluster head ID, zone head ID, base station ID) | Integrity & Authenticity |

## IV. CONCLUSION

In this paper, we presented a hierarchal authentication scheme in cluster WSN where the security of the data transmission has been enhanced. The scheme divides the message into two blocks where each block is encrypted separately. A block is added to the message contains ID of at least; source node, Intermediate nodes, and cluster head node, more IDs may be added based on the level of the communication to ensure the message and the node authenticity.

The scheme may have higher computations due to the number of encryption and decryption processes, but the communication overhead has been reduced as we used the cluster structure. The scheme is useful for critical networks that need a robust security scheme.

For future work, we will simulate and evaluate the proposed scheme and compare it with known schemes. Moreover, we will use a lightweight encryption algorithm.

## REFERENCES

[1] K. Mershad, A. Hamie, and M. Hamze, "HiMAC: Hierarchical Message Authentication Code for Secure Data Dissemination in Mobile Ad Hoc Networks," *Int. J. Commun. Netw. Syst. Sci.*, vol. 10, no. 12, pp. 299–326, 2017.

[2] S. Mahajan and P. K. Dhiman, "Clustering in Wireless Sensor Networks: A Review Shilpa," *Int. J. Adv. Res. Comput. Sci.*, vol. 7, no. 3, pp. 198–201, 2016.

[3] C. P. Systems, "Clustering in Wireless Sensor Networks 1 st part : Introduction," pp. 1–30, 2011.

[4] A. D. Dhawale, "Authentication Techniques for Wireless Sensor Network," vol. 2012, pp. 7–8, 2012.

[5] M. Bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks,"

*Proc. 2003 ACM Work. Wirel. Secur. - WiSe '03*, no. September 2003, p. 79, 2003.

[6] B. Wu, "A Hierarchical Authentication Scheme in Wireless Sensor Networks," in *2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems*, 2014, pp. 630–635.

[7] J. Trevathan, H. Ghodosi, and T. Myers, "Efficient batch authentication for hierarchical wireless sensor networks," in *2011 Seventh International Conference on Intelligent Sensors, Sensor Networks, and Information Processing*, 2011, pp. 217–222.

[8] S. Ben Othman, A. Trad, H. Youssef, and H. Alzaid, "Secure Data Aggregation with MAC Authentication in Wireless Sensor Networks," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2013, pp. 188–195.

[9] A. Abduvaliev, S. Lee, and Y.-K. Lee, "Simple hash-based message authentication scheme for wireless sensor networks," *2009 9th Int. Symp. Commun. Inf. Technol.*, pp. 982–986, 2009.

[10] A. R. Chowdhury and S. DasBit, "LMAC: A Lightweight Message Authentication Code for Wireless Sensor Network," in *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1–6.