HA^{2}CR: Hierarchical Authentication Assisted Clustered Routing for Wireless Multimedia Sensor Networks

R. Jawwharlal* and L. Nirmala Devi
Department of Electronics and Communication Engineering, Osmania University, Hyderabad, Telangana, India
Email: nirmaladevi@osmania.ac.in

Abstract² Secure data transmission is the major issue in Wireless Multimedia Sensor Networks (WMSNs). One of the most well-known strategies that are essential in solving the privacy and security issues is access control and authentication. These techniques can stop malicious nodes from joining the network. However, because to the complexity of their encryption, they place an unsustainable computational burden on the energy-constrained sensor nodes. To ensure an efficient data access, this paper proposes a simple and effective authentication and access control mechanism called as Hierarchical Authentication Assisted Clustered Routing (HA^{2}CR). Initially, HA^{2}CR clusters the entire network into different clusters and then applies authentication at two stages; one is between Base Station and Cluster Head and another is between Cluster head and Cluster Member. The Second level authentication is a mutual authentication and allows both clustered and cluster member to check the authenticity of each of them. Simulation experiments with different scenarios show the performance effectiveness of HA^{2}CR in the adversary identification and qualitative data delivery at base station. The average Malicious Detection Rate (MDR) and Packet Loss Rate (PLR) of proposed access control mechanisms observed as 92.4200%, and 6.1666 respectively. From the results the effectiveness of proposed method had proven in terms of larger MDR and lower PLR.

Index Terms² Wireless Multimedia Sensor Networks (WMSNs), hierarchical authentication, access control, clustering, packet loss, malicious detection rate

I. Introduction

In recent years, Wireless Multimedia Sensor Networks (WMSNs) have gained huge research interest due to their widespread applicability in different applications including Security, smart surveillance, smart traffic monitoring and smart health [1], [2] etc. WMSNs are specifically useful in such kind of environments where there is the human intervention is not possible. But, there are several real time problems in WMSNs including components failure, information error, wireless transmission error and security attacks due to the injection of fake data and the joining of malicious nodes into the network. Due to these problems, there is need of collaboration between multimedia sensor nodes for reliable event identification and prevention of faulty or fake reports. Security and privacy challenges are the most serious problems in WMSNs which needs to be fulfilled. Along with the multimedia sensor nodes, their data also need to be secured from different kinds of adversaries.

Access control and authentication is one of the most prominent strategies that plays a vital role in addressing the privacy and security challenges those are faced by nodes and their data in WMSNs [3]. These methods are able to prevent malicious node from entering into the network and accessing the resources in an unauthorized manner. Several method have been developed in earlier to ensure a secure and authorized communication in WMSNs. However, most of them are based on the methods like Asymmetric encryption like Elliptical Curve Cryptography (ECC) [4]. However, they create an excessive computational burden on the energy constrained sensor nodes due to their complex encryption nature. The complex operation oriented methods are not suitable for resource constrained multimedia sensor nodes. Moreover, most of the existing methods for WMSNs focus on the direct exchange of information between sensor to sensor and sensor to base station. They lack of a support of machine to machine communication which is very much required in WMSNs.

To sort out these problems, this work proposes a simple authentication and access control mechanism called as Hierarchical Authentication Assisted Clustered Routing (HA^{2}CR) for WMSNs. HA^{2}CR is a two level authentication mechanism at which the first level takes place between Cluster Head and Base Station while the second level takes place between Cluster Head and its corresponding cluster member nodes. The second phase authentication is a mutual authentication which was done between the Cluster Head and Cluster Members in a mutual fashion. Before, the proposed method clusters the entire network into different clusters.

The rest of the article is stipulated as follows. Section II explores the details of literature survey. Section III explores the details of proposed HA^{2}CR mechanism. Section IV explores the details of experimental evaluation and Section V concludes the paper.

Manuscript received July 15, 2022; revised December 12, 2022; accepted January 2, 2023.

* Corresponding author email: rjlphdou@osmania.ac.in

doi:10.12720/jcm.18.1.58-67

II. RELATED WORKS

K. Nagarathna, *et al* [5] proposed to address routing security difficulties and limitations in sensor networks. Because the behavior of these sensor nodes is dynamic, the routing must be upgraded at different points in time. When routing, two characteristics are taken into account: the trust and weight of each node in the path of routing, and the number of sensor nodes divided into separate clusters. Each node has a set of direct and indirect trust values that will be used to check the node's security. The Intelligence-Based Security Authentication technique by X. Qiu *et al*. [6] has been proposed as a new deep learning (DL)-enabled secure authentication approach that blends Blind Feature Learning (BFL) and Lightweight Physical Layer Authentication (LPLA) to overcome these challenges. In particular, at the data collection unit, an intelligent authentication mechanism is built by exploring neural networks to learn data properties.

In Trust-based distributed Topology management scheme (TRAST) is for usage in WMSNs. TRAST takes use of the control packets' received signal strength, which was then used to build the dispersed topology [7]. The application of trust in a non-secure distributed topology aids in delivering event coverage and preserving connectivity, even in the face of malicious attacks. In the case of malicious attacks, the proposed topology management scheme achieves a greater average coverage ratio and average packet delivery ratio than the Lightweight and Dependable Trust System (LDTS) and T-Must schemes. M. Usman, *et al*. [8] proposed to during the acquisition of mobile multimedia data that offer a strategy to safeguard the underlying WMSN. It is a two-layer technique that, which all MSNs are grouped into small clusters at the first layer, with a single Cluster Head representing each cluster (CH). Before sharing multimedia data, all CHs at the second layer check the identities of mobile sinks. Secure data exchange is ensured by authentication at both tiers. This technique was further tested in terms of authentication rate, data freshness, and packet delivery ratio.

An anonymous-based user authentication method was provided in the User Authentication Scheme for Secure Anonymous by Y. Kirsal Ever [9] proposal to enhance the security features, computation, and transmission overhead of wireless sensor networks. The suggested system employs improved elliptic curve encryption and is resistant to password guessing and lost/stolen smart card verifier attacks while simultaneously maintaining user anonymity. Security assessments, both formal and informal. The suggested approach offers strong security while requiring little computing and communication resources.. J. Qi, *et al*. [10] proposed a hybrid security and compressive sensing-based strategy for multimedia sensor data collection is given in this research. It has a light security mechanism, which reduces the system's complexity and energy usage. A security and compression performance analysis is done out, 8-bit integer chaotic block encryption and chaos-based message authentication codes make up the hybrid security. Its goal is to improve the security and efficiency of data collection.

To improve the correctness and trustworthiness of acquired information, to discuss data aggregation, information trust, and fault tolerance [11]. To develop a trust-based framework for data aggregation with fault tolerance based on the multilayer aggregation architecture of WMSNs, with the goal of minimizing the impact of erroneous data and providing demonstrable trustworthiness for aggregated data. This can substantially increase the quality of multimedia information and more precisely assess the reliability of acquired data. J. Ben Othman *et al*. [12] proposed QoS provisioning and network security management have become increasingly important in deciding the success of next-generation wireless communications. This special issue contains cutting-edge research on QoS and security provisioning in wireless and mobile networks.

The issues are simultaneously resolved by adopting an image communication system for IoT monitoring applications, according to the Efficient and Secure Image Communication System Based on Compressed Sensing provided by L. Li, *et al*. [13]. Low computational complexity, low energy consumption, and low storage overhead are all requirements for sensor nodes, and the suggested system can meet them. A new compressed sensing (CS) model, as well as the accompanying parallel reconstruction technique, are also presented, which aid to reduce picture encryption/decryption time. Some method focused on security based a framework for IoMT applications that is efficient, privacy-preserving, and data collecting and analysis (P2DCA) [14]. A basic wireless multimedia sensor network is partitioned into different clusters using the proposed methodology. Cluster Heads indicate each cluster (CH). Through the aggregation of data and position coordinates, the CHs are responsible for protecting the privacy of member MSNs. Later, on the cloud server, the aggregated multimedia data is evaluated with a counter-propagation artificial neural network to extract relevant information by segmentation.

D. Kundur, *et al*. [15] proposed difficulties of designing for security and privacy in distributed multimedia sensor networks are discussed. For distributed multimedia sensor networks, introduce the heterogeneous lightweight sensor nets for a trustworthy visual computing framework. The architecture's security difficulties are investigated, leading to the creation of open research questions such as secure routing in upcoming free-space optical sensor networks and distributed privacy for vision-rich sensor networking. Image transmissions with security enhancement based by H. Wang, *et al*. [16] based on the path diversities, this work provides a collaborative transmission strategy for image sensors that uses inter-sensor correlations to determine transmission and security sharing patterns. The proposed approach for secret image sharing across multiple node-disjoint pathways for image delivery achieves excellent security without requiring any key distribution or management, obviating the need for key management issues.

M. A. Jan, *et al.* [17] proposed a Seamless and Authorized Streaming (SAMS) framework for a cluster-based hierarchical in WMSNs. To create secure clusters, the SAMS leverages authentication at many levels. Only valid nodes can send data to their Cluster Heads after these clusters have been formed (CHs). Each node senses its surroundings, saves the data it captures in its buffer, and waits for its turn to transmit to its CH. Excessive packet loss and end-to-end delay for multimedia traffic may occur from this waiting. A channel allocation strategy for inter-cluster communication has been proposed to address these concerns. A member node in one cluster shifts to a neighboring CH in the event of a buffer overflow, provided that the latter has an available channel for allocation. High-Efficiency Video Coding (HEVC) is a new video code standard that allows for the efficient storage and streaming of high-resolution videos of appropriate size and quality [18]. For secure streaming of compressed HEVC streams, a unique hybrid cryptosystem incorporating DNA (Deoxyribonucleic Acid) sequences, Arnold chaotic map, and Mandelbrot sets is proposed in this study. To begin, high-resolution videos are encoded with the H.265/HEVC codec for efficient compression.

S. H. Islam, *et al.* [19] proposed a three-factor SIP (TF-SIP) for multimedia big data communications that is both strong and flexible in the face of known security flaws. In the random oracle model, it shows that our TF-SIP is proven secure. Using the M. Burrows, M. Abadi, and R. Needham (BAN) logic analysis, and it explicitly verify mutual authentication as well as the freshness of the negotiated session key between the user and the remote server. Lightweight and Privacy-Preserving Data Aggregation for Mobile Multimedia Security by S. Ma, *et al.* [20] has been proposed a lightweight and privacy-preserving data aggregation method for mobile multimedia. The suggested scheme's terminal calculation is simple, and there is no need for a trusted third party. Furthermore, building virtual aggregation zones balances multimedia large data and personal multimedia data, and batch verification improves system performance in our scheme. The presented approach can ensure the privacy, secrecy, and integrity of personal multimedia data, according to a security study.

This article discusses Amina Msolli, *et al.* [21]'s Shift-Advanced Encryption Standard (SAES), a new security method for real-time wireless multimedia sensor networks is Shift-AES. The AES algorithm is modified to make it compatible with WMSN. In this method the new approach has been shown in experiments to maintain a higher level of safety while reducing the central processing units execution time. S. Aasha Nandhini, *et al.* [22] proposed the security keys for securing the user's identity are created from the measurement matrix elements in a Compressed Sensing (CS)-based security mechanism. The security keys are used to keep the movie from being recreated by the attacker. The suggested security architecture is put to the test in real time using a WMSNs test bed, with characteristics including memory footprint, security processing overhead, communication overhead, energy usage, and packet loss is examined to show its effectiveness.

Distributed Compressive Video Sensing (DCVS) was a novel video coding system that employs Compressed Sensing (CS) independent encoding and joint decoding [23]. DCVS was well suited for resource-constrained because it overcomes the limitations of standard video coding. However, there are two key concerns with DCVS in WMSNs that must be addressed immediately; the first is balancing the encoder's storage burden and the decoder's recovery quality; the second is providing privacy protection for video coding and transmission. C. Wu, *et al.* [24] proposed a crowd-sourced approach for calculating the quality of experience of multimedia information. Use a paired comparison mechanism in framework to solve for mentioned quality problem. The following are some of the benefits of framework: 1) Reliability due to support for cheat detection; 2) A Simpler rating procedure than the commonly used but more difficult mean opinion score (MOS), which places less burden on participants; 3) economic feasibility because reliable QoE measures can be obtained with less effort than MOS; and 4) generalizability across a variety of multimedia content.

Hongxia Wang *et al* [25] proposed a robust image authentication technique based on Perceptual Hashing-Based Robust Image Authentication (PHIA), which uses a distributed processing strategy for perceptual image hashes and can provide compactness, visual fragility, perceptual robustness, and security in digital image authentication for the WMSNs. The cluster head node first generates a secure pseudorandom chaotic sequence with keys and sends it to the image capturing node; the image capturing node then divides the captured image into several overlapping rectangles using the chaotic sequence received; finally, the binary distance between the two gravity centers is calculated in each general cluster member node. The cluster head node receives the binary distance sequence from all of the general cluster member nodes and combines it to create the perceptual hashing sequence that will be delivered to the base station for image authentication. Rui Gao [26] proposed Compressed Sensing Watermarking Authentication (CSWA). Introduces a new safe data fusion technique based on (CSWA); specifically, the algorithm takes advantage of picture encryption scarcity to improve the identification of scarcity over wireless multimedia sensor networks, the method uses L-1 norm regularization, which is prevalent in compressive sensing. The resulting algorithms provide learning skills to sensor nodes, allowing them to learn the sparse structure from still image data while also utilizing the watermarking approach to provide authentication. They present the overall transmission volume as well as an energy consumption performance analysis of each node, as well as a summary of the suggested method's peak signal noise ratio values. Basavaraj Patil [27] proposed the Elliptical Curve Cryptography Digital Hashing (ECCDH) technique, which combines to give an effective authentication mechanism. ECCDH improves the authentication process for network nodes.

III. Proposed System Method

A. Overview

In this section we describe the full-fledged details of the proposed mechanism. Under the proposed mechanism, initially we cluster the entire network into various clusters. The complete clusters are two types; they are a nearby cluster and a distant cluster. The cluster formation considers energy and distance as reference matrices. After the cluster formation, the CH selection is carried out followed by mutual authentication of cluster head and cluster members. The proposed authentication is two level authentications at which the first level takes place between CH and BS while the second level takes place between CH and its corresponding cluster member nodes. The second phase authentication is a mutual authentication which was done between the CH and CMs in a mutual fashion.

B. Cluster Formation

In our proposed approach, the entire WMSN is partitioned into multiple clusters which consist of P number of cluster members, out of which only one node is selected as CH. The selection of CH is done based on the energy and distances. In each round of simulation, the cluster members exchange their information (residual energy level ($i.e., e_i$), location coordinates (x_i, y_i) and identities ($i.e., ID_i \ where \ i \in \{1,2,\ldots,N\}$)) with BS and it fetches all the required information and stores it in its database. Based on the obtained energy levels, the BS computes the where residual energy and N is a total number of nodes present in a network. The mean energy (E) signifies the network lifetime that is up to which extent the network will sustain. The mean energy is calculated as

$$E = \sum_{i=1}^{N}\left(\frac{e_i}{N}\right) \tag{1}$$

Next, the residual energy of each node is compared with mean energy (E) and determines the nodes that are having greater residual energy than the mean energy are nominated as CHs means they are eligible as cluster heads. In case if the BS found that there are more nodes with equal energy levels, then the selection process searches for minor differences in their energy levels, i.e., they will search for decimal based differences. In a second round also, if the same energy levels are found for more nodes, then a selection process goes with the nodes that are not selected as cluster heads in earlier rounds. After the finalization of CHs, the BS broadcast a message in the network field. The message composed of IDs ($i.e., j \ where \ j \in \{1,2,\ldots,J\} \& J \subset N$) and location coordinates ((x_j, y_j)) of the selected CHs. Moreover the way BS also share the information belongs to the location coordinates of cluster nodes with the selected CHs. After receiving a message from BS, the CHs retrieves and store the ID and location coordinates of cluster nodes. Further each CH respond to the message by sending an acknowledgement to the BS which denotes a successful reception of message. Next, all the CHs broadcast an advertisement to the sensor nodes by appending their energy levels. Upon receiving the advertisement, the sensor node retrieves the energy information. It is possible that a sensor node may receive and information from multiple CHs. In such condition the sensor node searches for the CH with maximum energy and minimum distance. After verification of IDs forwarded by the BS with the IDs of senor nodes, the distance is measured based on Euclidean distance as follows;

$$d = \sqrt{(x - x_i)^2 + (y - y_i)^2} \tag{2}$$

There is a possibility to more than one CHs that satisfies the maximum energy and minimum distance criteria. In such situation, the sensor node sends a joint request to all the selected CHs and selects the CH that was responded quickly. Before joining of a senor node into a cluster, they will authenticate mutually by themselves. For this purpose a mutual authentication is required between CH and sensor node to a request packet called as Joint Request Packet (JRP). The process of authentication at both levels is explained clearly in the following section.

C. Authentication

This phase provides a secured communication between sensor nodes in WMSNs. The authentication process is executed between CH and BS as well as between CH and sensor nodes. In WMSNs, whenever a node i want to join in the network it receives a 16 bit with token key (τ_i) from the BS along with this token key, they are also receive one more key called as secret key (χ_i) from the BS. The size of secret key is fixed and it is of 128 bit. The BS maintains a table of token keys of all sensor nodes and issues one for each node. With the help of τ_is and χ_is, the BS can control and manages the departure and arrival of sensor nodes into the WMSN. Here, the network authentication is done at two levels; one is at BS level another is a CH level. The former one authenticate the authenticity of CH by BS while the latter authentication is a mutual authentication that is done between CH and sensor nodes. The details are explored in the following subsections.

1) Level 1 authentication

The level 1 authentication is done between CH and BS. In each round, the BS selects an optimal number of CHs among the available sensor nodes in the network. Here the maximum limit is said to 5% of the total nodes in the network for number of CHs. For example, consider 100 sensor nodes are there in a network, and then the number of CHs is 5 *100/100= 5, i.e., among the 100 sensor nodes, only 5 are selected as CHs. Then approximately each CH will get 20 nodes as cluster members. Initially each sensor node broadcasts one control packet to BS that consists of 32 bit self-ID (ID_i), 32-bit BS-ID (ID_{BS}) and residual energy. After the receiving the control packet, the BS compute energy based on the obtained values and it will finalize the total number of CHs and the CH Nominees. The selection process of CH nominee is already discussed in section 3.2. After the completion of optimal CH selection, the BS broadcast nominee packet to the corresponding CH those were chosen as nominees. The nominee packet composed of IDs of corresponding CH (ID_i^{CH}) and also the identities of neighbour nodes of CH (ID_n). The BS initially performs an exclusive XOR operation with ID_i^{CH}, ID_{BS} and τ_{CH}^i to get the result and let it is denoted as R_{ID}. Then the R_{ID} is appended with the nominee packet and it is broadcasted to the field network. Hear the BS assigns a τ_{CH}^i for every CH and it is also with the corresponding CH. The obtained a nominee packet is decrypted successfully only with the corresponding CH. Even though any legitimate multimedia sensor node or Intruder cannot crack the nominee packet because they don't have a token key of corresponding nominee packet. If any adversary has received the nominee packets that it has to perform 2^{16} attempts to decrypt the nominee packet and then only it can get the ID_i^{CH} so the complex and lengthily encryption and decryption process restricts the malicious or adversary intruder from the selection of CH. Moreover this process ensures only the nodes to act as CH those were nominated by BS. After the reception of nominee packet, it can be decrypted by only CH that is associated with corresponding with i^{th} token key (τ_i).

$$R_{ID} = XOR(ID_i^{CH}, ID_{BS} \text{ and } \tau_{CH}^i) \qquad (3)$$

The XOR operation mentioned in the Eq. (3) is not Complex operation and it needs only few resources. Moreover it is a common operation which was generally used to perform encryption operations in security related applications and this operation generate strong cipher and also not lead to any information leakage. After the successful decryption of R_{ID}, the CH retrieve their IDs from the nominee packet and then broadcast an acknowledgement packet in response to the nominee packets. The acknowledgement contains the notification of successful decryption and it is disclosed to the XOR operation between τ_{CH}^i and ID_{BS}. As upon receiving the acknowledgment packet, the BS assumes that the nominee packet has been received to the correct and legitimate CH and establishes a secure communication link with the corresponding CH. This process ensures a secure data transmission between CH and BS. Since there is a chance to compromise the CH as accurate authentication is required before transmitting the data.

2) Level 2 authentication

Once the selection and authentication of CHs is completed, then each CH broadcast advertisement by keeping its IDs in the packet. Since there are a large number of CHs, a neighbor node may receive multiple advertising packets but the sensor node associates with the CH which has strong potential towards it. The potentiality of a CH is calculated based on the strength of signal that is received signal strength indicator (RSSI). The radio receiver of sensor node measures the RSSI of each advertising packet received and then finalizes one CH which has larger potential value. The sensor node can get joined into the cluster of potential CH if it was allowed. At this phase, the mutual authentication process occurs in which the sensor nodes check the CHs at authenticity and the CH checks the authenticity of sensor node. Algorithm 1 shows the step by step of proposed mechanism. The process of mutual authentication between CH and sensor node composed of four steps they are explained as follows.

Step 1: In this step, every sensor node broadcast request packet (REQp) that consists of a sensor node ID, ID_i^{CH} and the τ_i of sensor node. This packet is sent to the CH with strong RSSI value.

Step 2: In this step, upon receiving the REQp, the CH Extracts ID_i^{CH} , ID_i and matches with the ID_i^{CH} of potential CH_i. If they were matched, then that means the packet was received at an intended CH. Moreover, the CH also matches the ID_i with the IDs of neighbor nodes with it have. These IDs of neighbor nodes are provided by the BS. If the sensor node ID is matched with any on neighbor node ID, then the CH extracts the χ_i from neighbor table and replies back to the sensor node with an encrypted message. The encrypted messages are obtained by performing and XOR operation between a random sequence numbers (ξ_{CH}^i) with χ_i before performing this encryption it generates one session key (S_k) and performs an XOR operation with χ_i. The result is appended to ξ_{CH}^i and again it is XORed with the secret key to get the encrypted message. The final encrypted messages of size 256 bit where the ξ_{CH}^i is of 128 bit and XOR is of 128 bit. Here the ξ_{CH}^i is used only once by a sensor node in the entire communication. Next, to get the encrypted message, we employed advanced encryption standard 128 (AES-128) which is extremely secure and lightweight in manner. Moreover AES-128 consumes fewer resources to get an encrypted message.

```
Algorithm 1: Authentication
1.   Initialization
   a.   Each sensor node receives one token key $\tau_i$ from BS
   b.   Each sensor node broadcasts a packet to BS with its ID
        and it is stored at BS
   c.   BS assigns one secret key to each  SN
   d.   Inputs {$\tau_i$, $\chi_i$ , $ID_i$, $ID_{BS}$ ` • L Å « « « « « « 1
Level 1 Authentication  (BS to CH)
For i =1 to N
do
   $i$ :  % 6     ^ 6 1  % U R D G F D V W V  F R Q W U R O  S D F N H W V  W R  % 6 `
   BS select optimal cluster heads (CHs)
   BS encrypts $ID_i^{CH}$ with $\tau_{CH}^i$ to get $R_{ID}$
    % 6  : L    ^ % 6  J H Q H U D W H  Q R P L Q H H  S D F N H W V ; E \ R D G F D V W V  W R  W K H
corresponding CHs, $R_{ID}$ is appended to nominee packet }
If  $ID_i^{CH}$ matched
      Then  $CH_i$ extracts $ID_i^{CH}$ from nominee packets
end if
     $CH_i$  :  % 6  $CH_i$ broadcasts acknowledgement packet to BS}
    BS checks for $ID_{BS}$ in ACK
If  $ID_{BS}$ is matched at BS
      Then $CH_i$ is authenticated
end if
end for


Level  2 Authentication (CH-SN-CH)

$CH_i$  :  L  $CH_i$ advertises a packet which contains $ID_i^{CH}$
   I retrievers $ID_i^{CH}$
 ,  :$CH_i$ :{SNi sends one JRP that contains its ID & $ID_i^{CH}$}
$CH_i$ extract $ID_i$ and $ID_i^{CH}$
If  $ID_i$ is matched with any neighbor node ID & its $ID_i^{CH}$ also
matched
 $CH_i$ : L   $CH_i$ send an encrypted messages to i}
else
      i is declared as not authorized and its JRP is discarded
end if
       i decrypted and retransfers $\xi_{CH}^i$ and $S_k$
          L  $CH_i$: {i sends an encrypted response to $CH_i$}
$CH_i$ checks $\xi_{CH}^i$ with the $\xi_{CH}^i$ lave

If  $\xi_{CH}^i$ is  matched
     i becomes the number of CH

$CH_i$  :  L  $CH_i$ send encrypted response to i}
else
     i is declared as unauthorized
end if
      i extracts $\xi_i$ and perfect matching
if  $\xi_i$ is matched
     i become a member of CH
$CH_i$ assigns one slot to i
else
   $CH_i$ is declared as unauthorized
End if.
```

Step 3: In this step, the sensor node deciphers the encrypted message and retrieves the S_k. If the sensor node succeeded, then it will have the correct S_k because the ξ_{CH}^i and S_k are known to only CH and χ_i is known to both CH and sensor node only trustworthy sensor node. Even though an adversary receive the encrypted message it can't decipher because it would have a valid secret key of the successful decryption the node is said to be successfully authenticated. Next the sensor node needs to authenticate CH. For this purpose, sender node execute an XOR operation between ξ_{CH}^i and χ_i and the result is appended the temporary random number (ξ_i) and then encrypted with S_k to get an encrypted message. This is different from the received encrypted message and it is off 256 bit in size then the encrypted message is transmitted to the potential CH.

Step 4: In the last step, the CH decrypted the received message and check for the ξ_{CH}^i. If CH found the presence of ξ_{CH}^i then it realizes that it has been successfully authenticated. Then the CH extracts ξ_i and formulates an encrypted response with secret key. Here the S_k is appended with ξ_i and then processes for encryption. Next, this response is transmitted to sensor node after receiving the response, the sensor node extracts ξ_i and checks the presence. If it is found that ξ_i is present then it realizes that it has been authenticated successfully. Since the ξ_i is originated by sensor node it denotes that the response was received from a trustworthy CH. At this phase both sensor node and CH are said to be mutually at authenticated and are agreed to communicate with each other. With the help of a common session key, this mutual authentication is performed by sensor node those who want to join as a cluster member in any cluster. After successful authentication, the sensor node becomes a cluster member of CH and begins the data transmission.

IV. Simulation Experiments

Under simulation experiments, we conduct a vast set of experiments by varying node density as well as the position of base stations. At each sensor node, the buffer capacity is set as 100 that represents the total number of packets, a node can buffer. The performance is measured through packet loss and end-to-end delay. These metrics are measured at two different base station positions, one is the BS at center of network and another is BS at any corner. The network created with base station at center (*x=500, y=500*) of network is shown in Fig. 1 and the base station at the corner (*x=0, y=0*) of network is shown in Fig. 2.

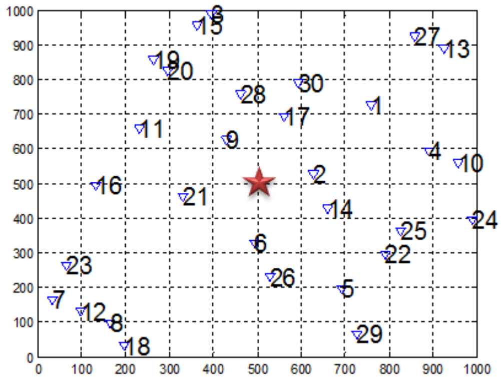


Fig. 1. Network with 30 nodes and Base station at center of network

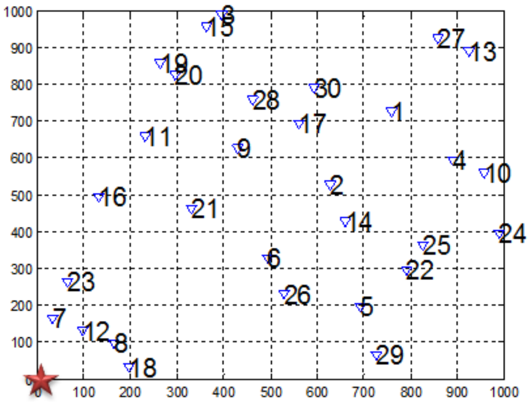
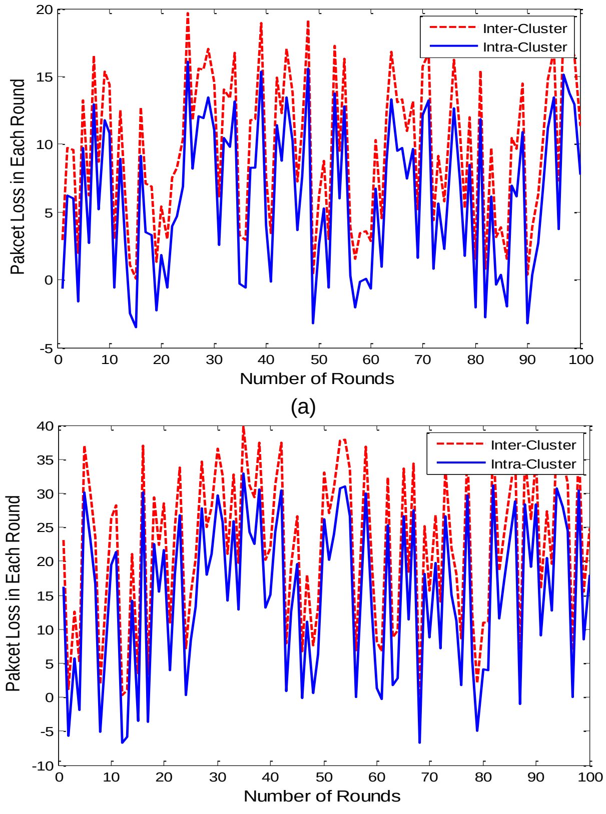


Fig. 2. Network with 30 nodes and Base station at the corner of network

The average packet loss is measured for both cases at different rounds. Fig. 3 (a) and (b) shows the packet loss in each round when the base station was located at the center of network and at the corner of network respectively. Here, we can see that the packet loss for the communication between inter clusters is more than that of the intra cluster. As the nodes of a cluster lies within the communication range of a cluster head, the transmission of packets suffers with only few loss in packets.



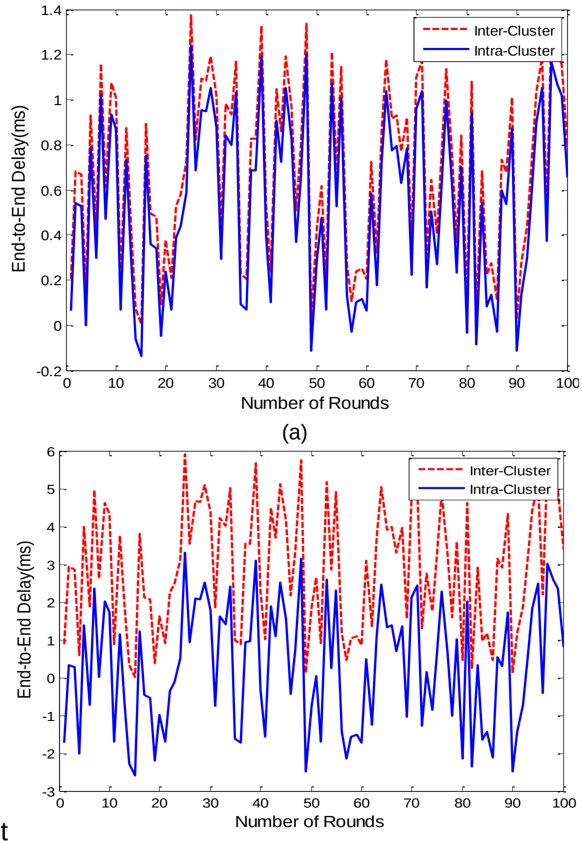
(a)

(b)

Fig. 3. Packet loss in each round when BS is at (a) center and (b) corner

On the other hand, the nodes between two different clusters need to take the help of other nodes to transmit their data to base station. At each node, there exists at least minimum loss and hence the loss at inter cluster communication is observed as more than the intra cluster. Furthermore, we can see that the packet loss is less when the base station is located at center of network than at the corner. As the distance between nodes and BS increases when it lies at the corner, the nodes at the other corner opt for multi-hop routing and it results in more packet loss. The packet loss is less when the base station is located at the center of network because it lies approximately at equal distances for the nodes in all four sides. From Fig. 3 (a), on an average, the packet loss at inter cluster communication is observed as 10.0077 While for intra cluster communication, it is observed as 6.1666. Similarly, from Fig. 3 (b), on an average, the packet loss at inter cluster communication is observed as 20.1520 while for intra cluster communication, it is observed as 13.2745.

Next, the average end-to-end delay is measured for both cases at different rounds. Fig. 4 (a) and (b) show the end-to-end delay in milliseconds in each round when the base station was located at the center of network and at the corner of network respectively. When the base station is located at uniform distances from all the nodes in the network, the time required to transmit data from each node is uniform in nature. On the other hand, if the base station lies far from some nodes, then they will take more time to forward their data to base station. Hence the end to-end delay for such kind of communication is more compared to the former case.



(a)

(b)

Fig. 4. End-to-End Delay (ms) in each round when BS is at (a) center and (b) corner

Moreover, the end-to-end delay for intra cluster communication is less than that of the inter cluster communication because the sensor nodes lies the communication range of cluster head. As the base station moves far away from few nodes, they seek multi-hop routing and in such case, the inter cluster comes into picture and increases the end-to-end delay further. From Fig. 4 (a), on an average, the end-to-end delay at inter cluster communication is observed as 0.7005 milliseconds, While for intra cluster communication, it is observed as 0.3058 milliseconds. Similarly, from Fig. 4 (b), on an average, the packet loss at inter cluster communication is observed as 3.0023 milliseconds, While for intra cluster communication, it is observed as 1.3466 milliseconds

From the Fig. 5, we can observed that the Malicious Detection Rate (MDR) is decreeing with an increasing in the percentage of malicious nodes. As malicious nodes increase in the network, the number of attacks also increases. As well as different attacks may get launched over the nodes and compromised them. In such kind of environments the detection of all malicious nodes becomes challenging and result in less MDR. For this we can also observed that even though the MDR are decreases the proposed method has better MDR compare to existing methods. Since the proposed method is developed a dynamic authentication and access control mechanism it can detect the maximum number of malicious nodes. As an average the proposed HA^{2}CR method has gained average MDR is of 92.42% while the existing methods, it is noticed as 88.61%, 87.12% and 85.48% for ECCDH, CSWA and PHIA respectively.

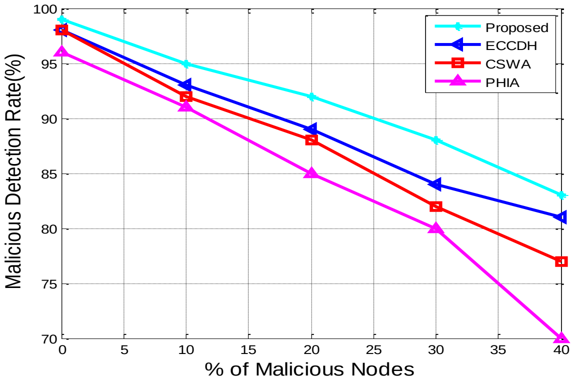


Fig. 5. MDR for varying malicious node count

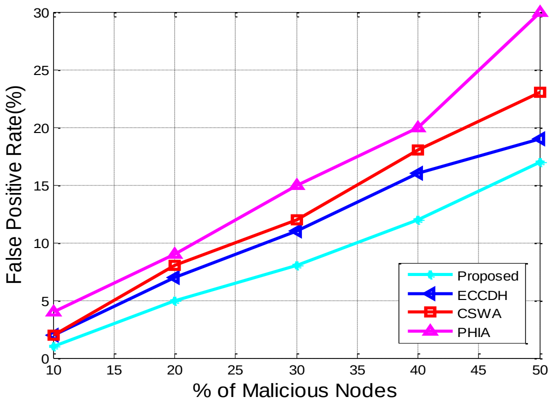


Fig. 6. FPR for varying malicious node count

Fig. 6 Explain the detail of False Positive Rate (FPR) for variation with malicious node count. From the Fig. 6, we can observed that the rising characteristics of FPR with an increasing malicious nature. However, the proposed method maintains least FPR as it proposed a hierarchal authentication between sensor node, cluster head and base station. But the FPR of proposed HA^{2}CR is observed as low compared to the existing methods ECCDH, CSWA and PHIA. As an average, the proposed HA^{2}CR method has gained average FPR is 8.23%. while the existing methods it is noticed as 11.12%, 12.39% and 15.10% for ECCDH, CSWA and PHIA respectively

The PDR can be defined as the ratio of actually received data packets at the receiver end to those which were actually sent by sender. From the Fig. 7, we observed that the packet delivery ratio variation with malicious node. As the malicious node increases it can be noticed that the PDR is decreases. But the PDR of proposed HA^{2}CR is observed as high compared to the conventional methods whith ECCDH, PHIA and CSWA.

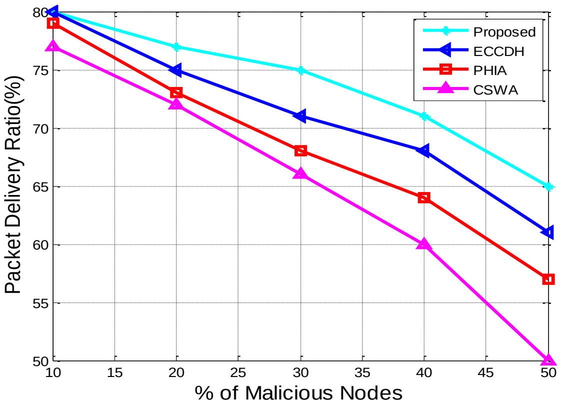


Fig. 7. PDR for varying malicious node count

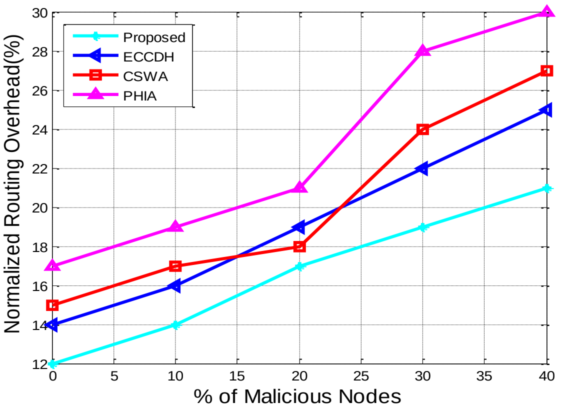


Fig. 8. NRO for varying malicious node count

Since the proposed method has two levels security mechanism, the sender node (cluster member or cluster head) checks the authenticity of receiver node, the packets drop is very less. As an average, the proposed HA^{2}CR method has gained average packet delivery ratio is 75.26% while the existing methods its noticed as 71.34%, 67.67% and 65.12% for ECCDH, PHIA and CSWA respectively.

As shown in Fig. 8, normalized routing overheads varying with malicious node. We can observed the NRO from the Fig. 8 is less for proposed method HA^{2}CR when compare with existing methods. The routing overhead is more when the additional packets are used for either routing discover or routing maintain. In this situation when it is number malicious nodes. To reduce this overhead, an efficient security check mechanism must be deployed and it was done in the proposed method. As an average, the proposed HA^{2}CR, method has gained average normalized routing overhead which is 17.26% while the existing methods its noticed as 18.34%, 19.67% and 22.12% for ECCDH, PHIA and CSWA respectively.

V. CONCLUTSION

This paper aims at the secure data transmission and proposes a new authentication and access control mechanism called as HA^{2}CR. HA^{2}CR is a two level authentication mechanism at which the first level takes place between Cluster Head and Base Station while the second level takes place between Cluster Head and its corresponding cluster member nodes. The second phase authentication is a mutual authentication which was done between the Cluster Head and Cluster Members in a mutual fashion. Before, the proposed method clusters the entire network into different clusters. Due to the 2-level authentication process, the proposed method has prevented the multimedia senor nodes from several security threats. The performance is analyzed through Packet loss, MDR, FPR and NRO. On an average, the packet loss occurred at intra cluster communication is 10.0077 while for intra cluster communication, it is observed as 6.1666 for center aligned base station. On an average, the proposed method gained and improvement in the MDR of 3.81%, 5.3% and 6.49% from ECCDH, CSWA, PHIA respectively. On an average the proposed method gained and improvement in reduction of NRO as 1.08%, 2.41% 4.87%. ECCDH, CSWA, PHIA respectively.

Even though our method provides sufficient resilience towards several issues in WMSNs, it observed that it required slightly more resources for two level authentications. Hence in the future it is suggested to model trust aware security ensuring mechanisms. These kinds of mechanisms less resources

CONFLICT OF INTEREST

The authors declare no conflict of interest

AUTHORS CONTRIBUTIONS

R. Jawwharlal: Contributed towards the design and development of proposed method, further contributed towards the implementation and analysis of proposed mechanism.

L. Nirmala Devi: Contributed towards the design of proposed method and suggested to identify a problem from literature review further, she also contributed towards the quality analysis and formatting of paper.

REFERENCES

[1] I. F. Akyildiz, T. Melodia, and K.5 &KRZGKXU\ Wireless ³ multimedia sensor networks: A survey´ *IEEE Wireless Comm*, vol. 14, no. 6, pp. 1339-1352, Dec. 2007.

[2] + 0D DQG ' 7DR ³0XOWLPHGLD sensor network and its research progresses´ *J. Software*, vol. 17, no. 9, pp. 2013-2028, Dec. 2006.

[3] - /LX < ;LDR DQG & / 3 &KHQ ³$XWKHQWLFDWLRQ DQG access control in the internet of things´ LQ *Proc. 32nd Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, 2012, pp. 588±592.

[4] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, and H. W. Wei ³$ VHFXUHG authentication protocol for wireless sensor networks using elliptic curves FU\SWRJUDSK\´ *Sensors*, vol. 11, no. 5, pp. 4767±4779, 2011.

[5] K. Nagarathna, Y. B. Kiran, J. D. Mallapur, and S. Hiremath, ³Trust based secured routing in wireless multimedia sensor networks´, in *Proc. Fourth International Conference on Computational Intelligence, Communication Systems and Networks*, 2012, pp. 53-58.

[6] X. Qiu, Z. Du DQG ; 6XQ ³Artificial intelligence based security authentication: applications in wireless multimedia networks,´ *IEEE Access*, vol. 7, pp. 172004-172011, 2019.

[7] * 0DOL DQG 6 0LVUD ³TRAST: Trust-based distributed topology management for wireless multimedia sensor networks,´ *IEEE Transactions on Computers*, vol. 65, no. 6, pp. 1978-1991, 1 June 2016

[8] M. Usman, M. A. Jan, X. He, and J. Chen, ³A mobile multimedia data collection scheme for secured wireless multimedia sensor networks´, *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 274-284, 1 Jan-Mar. 2020.

[9] < . (YHUH ³Secure anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks´, *IEEE Systems Journal*, vol. 13, no. 1, pp. 456-467, March 2019.

[10] J. Qi, X. Hu, Y. Ma, and Y. Sun, ³A hybrid security and compressive sensing-based sensor data gathering scheme,´ *IEEE Access*, vol. 3, pp. 718-724, 2015

[11] Y. Sun, H. Luo, and S. K. Das, ³A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks,´ *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 785-797, Nov.-Dec. 2012

[12] - % 2WKPDQ DQG 0 $\DG ³Special issue on last advances on QoS and security in wireless networks´, *Journal of Communications and Networks*, vol. 16, no. 4, pp. 358-362, Aug. 2014.

[13] L. Li, G. Wen, Z. Wang, and Y. Yang, ³Efficient and secure image communication system based on compressed sensing for IoT monitoring applications´ *IEEE Transactions on Multimedia*, vol. 22, no. 1, pp. 82-95, Jan. 2020.

[14] M. Usman, M. A. Jan, X. He, and J. Chen, ³P2DCA: A privacy-preserving-based data collection and analysis framework for IoMT applications,´ *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 6, pp. 1222-1230, June 2019.

[15] D. Kundur, W. Luh, U. N. Okorafor, and T. Zourntos, ³Security and privacy for distributed multimedia sensor networks,´ *Proceedings of the IEEE*, vol. 96, no. 1, pp. 112-130, Jan. 2008.

[16] H. Wang, D. Peng, W. Wang, H. Sharif, and H. Chen, ³Image transmissions with security enhancement based on region and path diversity in wireless sensor networks´, *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 757-765, Feb. 2009.

[17] M. A. Jan, M. Usman, X. He, and A. Ur Rehman, ³SAMS: A seamless and authorized multimedia streaming

framework for WMSN-Based IoMT,´ *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1576-1583, April 2019.

[18] A. Alarifi, S. Sankar, T. Altameem, K. C. Jithin, M. Amoon, and W. El-Shafai, ³A novel hybrid cryptosystem for secure streaming of high efficiency h.265 compressed videos iniot multimedia applications,´ *IEEE Access*, vol. 8, pp. 128548-128573, 2020.

[19] S. H. Islam, P. Vijayakumar, M. Z. A. Bhuiyan, R. Amin, V. 0 5DMHHY DQG %DOXVDPL\ ³A provably secure three-factor session initiation protocol for multimedia big data communications,´ *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3408-3418, Oct. 2018.

[20] S. Ma, T. Zhang, A. Wu, and X. Zhao, ³Lightweight and privacy-preserving data aggregation for mobile multimedia security,´ *IEEE Access*, vol. 7, pp. 114131-114140, 2019.

[21] A. Msolli, A. Helali, and H. Maaref, ³New security approach in real-time wireless multimedia sensor networks,´ *Computers & Electrical Engineering*, vol. 72, pp. 910-925, 2018.

[22] S. A. Nandhini and S. Radha, ³Efficient compressed sensing-based security approach for video surveillance application in wireless multimedia sensor networks,´ *Computers & Electrical Engineering*, vol. 60, pp. 175-192, 2017.

[23] D. Xiao, M. Li, M. Wang, J. Liang, and R. Liu, ³Low-cost and high-efficiency privacy-protection scheme for distributed compressive video sensing in wireless multimedia sensor networks,´ *Journal of Network and Computer Applications*, vol. 161, 2020.

[24] C. Wu, K. Chen, Y. Chang, and C. Lei, ³Crowdsourcing multimedia QoE evaluation: A trusted framework,´ *IEEE Transactions on Multimedia*, vol. 15, no. 5, pp. 1121-1137, Aug. 2013.

[25] H. Wang and B. <LQ ³3HUFHSWXDO hashing-based robust image authentication scheme for wireless multimedia sensor networks´ *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks*, p. 9, 2013.

[26] R. Gao, Y. Wen, and H. =KDR ³6HFXUH data fusion in wireless multimedia sensor networks via compressed sensing´ *Hindawi Publishing Corporation Journal of Sensors*, p. 7, 2015.

[27] B. Patila and S 5 %LUDGDU ³(QKDQFHG authentication mechanism in wireless multimedia sensor networks using (&&'+´ *Proc. 4th International Conference on Cyber Security and Privacy in Communication Networks*, 2018.

R. Jawwharlal was born in Telangana State, India, in 1978. He received the B.Tech degree from the Jawaharlal Nehru Technological University (JNTU) Hyderabad, India, in 2002 and the M.Tech Degree from the JNTU, Hyderabad, India, in 2009, both in Electronics and Communication Engineering (ECE). He is Currently Pursuing the Ph.D degree with the Department of Electronics and Communication Engineering, Osmania University, Hyderabad, India. His research interests include Wireless sensor networks, Wireless Communication and networks, Broad band wireless access, Internet of Things (IoT), UAV Communications, Machine Learning (ML) and Signal Processing.

L. Nirmala Devi received the Ph.D degree in Electronics and communication engineering from the Osmania University, Hyderabad, India, in 2014. She is currently Professor & Head Dept of ECE, Osmania University, Hyderabad. Her research interests include Machine Learning, Energy Harvesting Cooperative Networks and Digital Signal Processing. She is Member in IEEE and IET. She has published 50+ scientific papers in IEEE Journals.