Seamless and Authorized Multimedia Streaming in IoMT

Mian Ahmad Jan, *Member, IEEE,* Muhammad Usman, *Member, IEEE,* *Xiangjian He, *Senior Member, IEEE* and Ateeq Ur Rehman

***Abstract*—An Internet of Multimedia Things (IoMT) architecture aims to provide a support for real-time multimedia applications by using wireless multimedia sensor nodes that are deployed for long-term usage. These nodes are capable of capturing both multimedia and non-multimedia data, and form a network known as Wireless Multimedia Sensor Network (WMSN). In a WMSN, the underlying routing protocols need to provide an acceptable level of Quality-of-Service (QoS) support for the multimedia traffic. In this paper, we propose a seamless and authorized multimedia streaming framework (SAMS) for a cluster-based hierarchical WMSN. SAMS uses authentication at different levels to form secured clusters. The formation of these clusters allows only legitimate nodes to transmit captured data to their cluster heads. Each node senses the environment, stores captured data in its buffer, and waits for its turn to transmit to its cluster head. This waiting may result in an excessive packet loss and end-to-end delay for multimedia traffic. To address these issues, a channel allocation approach is proposed for inter-cluster communication. In case of buffer overflow, a member node in one cluster switches to a neighboring cluster head provided that the latter has an available channel for allocation. The experimental results show that SAMS provides an acceptable level of QoS and enhances the security of the underlying network.**

***Index Terms*—IoMT, WMSN, QoS, authentication, channel allocation, Inter/Intra cluster communication.**

I. Introduction

Internet of Things (IoT) incorporates a set of devices with sensing and actuating capabilities, and are able to connect with networking and web technologies [1]–[3]. However, discussion on the requirements and challenges posed by the multimedia contents is still missing in these studies. Research and discussions on multimedia contents, such as audio, videos and images, are encouraging the development of new architectures and protocols in the IoT paradigm to support the processing and transmission of multimedia contents [4]–[6]. Such developments require to revise the existing architecture of IoT by transforming it into a new concept, known as Internet of Multimedia Things (IoMT) to support real-time multimedia services and applications.

Due to the involvement of Wireless Multimedia Sensor Networks (WMSNs) in various sensitive IoMT applications, such as smart health, smart traffic monitoring, and smart surveillance and security, it is important to secure the end-to-end data streaming in such applications. Security and privacy are challenging aspects that need to be fulfilled for an interconnected system of real-world physical objects [7]. Not only the objects but also their multimedia streams need to be secured from adversary attacks. Authentication and access control techniques have a pivotal role in addressing the security and privacy challenges, faced by objects and their data in a WMSN paradigm [8]. These techniques have the ability to prevent malicious users from gaining access to network resources and prevent legitimate users from accessing resources in an unauthorized fashion. The existing studies on authentication and secured communication are mostly based on the use of asymmetric encryption techniques, such as Elliptic Curve Cryptography (ECC) [25] [26]. However, asymmetric encryption contains cipher suites that require computationally complex operations. Such requirements may not suit the resource-constrained nature of existing multimedia sensors embedded in an IoMT paradigm. Furthermore, almost all of the existing schemes for WSN/IoT emphasize on the exchange of messages directly between the end-users and sensor nodes. They lack the support for Machine-to-Machine (M2M) communication, a desirable feature in any IoT/IoMT environment.

To address these challenges, we use symmetric encryption [10] for seamless and authorized multimedia streaming (SAMS) in a cluster-based hierarchical WMSN. Using Advanced Encryption Standard, four lightweight handshake messages are exchanged to secure the communication. For seamless delivery of multimedia traffic in an end-to-end communication, a novel channel allocation scheme is proposed. The contributions of SAMS are two-fold.

1) A lightweight AES-based authentication technique to secure end-to-end multimedia streaming is proposed. Authentication is provided at two different levels within the network. Initially, an exchange of control packets is initiated to secure the communication between the base station and elected cluster heads. Next, secured clusters are formed to prevent adversaries from maliciously manipulating data streams.
2) After successful authentication, a novel channel allocation approach is adopted to maintain an acceptable level of QoS in WMSNs. The proposed scheme enables authorized multimedia sensor nodes in one cluster to

Manuscript is submitted on February 01, 2018 and asterisks indicate the corresponding authors.

Muhammad Usman is with Department of Computer Science and Software Engineering, Swinburne University of Technology, Australia. (E-mail: musman@swin.edu.au.

Xiangjian He is with Global Big Data Technologies Center (GBDTC), School of Electrical and Data Engineering, University of Technology Sydney, Australia. (E-mail: xiangjian.he@uts.edu.au.

Mian Ahmad Jan and Ateeq Ur Rehman are with Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan (E-mail: mianjan@awkum.edu.pk, ateeqhere@awkum.edu.pk)

utilize the timeslots/channels of a neighboring cluster. A member node of one cluster initiates a channel switching request to a neighboring cluster head if its buffer overflows and the node has to wait longer for its turn to transmit the data to its own cluster head.

The rest of the paper is organized as follows. In Section II, related work from the literature is provided. In Section III, we explain the network and attack model followed by detailed discussion of SAMS in Section IV. In Section V, we provide the experimental results for our scheme. Finally, the paper is concluded with future research directions in Section VI.

II. Related Work

Various surveys on secured routing and node authentication in an IoT environment were presented in [21], [22]. In these surveys, security issues and challenges along with proposed solutions were discussed. In [23], the authors proposed an authentication protocol for WSNs that uses a single hash function. The proposed work provides a very weak solution and as such, cannot combat various attacks such as sinkhole, Sybil, tampering, insider, and password guessing. Besides, the proposed work does not provide any mutual authentication among the nodes. A two-factor mutual authentication protocol was proposed in [24]. It is a key establishment protocol that incurs less computational overhead for the gateway and sensor nodes. Despite being a mutual authentication scheme, [24] does not provide any defense mechanism against replay, sinkhole, Sybil, DoS and password guessing attacks. An ECC-based user authentication protocol for WSNs was proposed in [25]. However, the proposed work violates the secrecy of the session key and user anonymity. An improved ECC-based mutual authentication scheme was proposed in [26] for WSNs. This work is more efficient than [25] and is capable to provide enhanced security features. However, it is vulnerable to key share attack and stolen smart card attacks.

In [27], a user authenticated key management protocol was proposed for generic IoT networks. In [28], a three-factor user authentication and key agreement protocol was proposed for a multi-gateway WSN-enabled IoT. In [29], a key agreement protocol using a hash function for QoS enhancement was proposed. In [30], the authors extended [29] by suggesting numerous solutions for mitigating the malicious attacks. The existing works of [27]–[30] are designed for simple sensing devices with limited security features and are not feasible for complex WMSN-based IoMT architectures. All these schemes provide direct communication between the user and sensor nodes. However, this is not the case with most of the IoMT applications.

III. Network and Attack Model

In this section, first we discuss our proposed network model in Section III-A followed by the attack model in Section III-B.

A. Network Model

In SAMS, the multimedia nodes are randomly deployed within a 100×100 m^2 area. The base station is located at 120×50 m^2 for data collection. SAMS operates in two phases, i.e., set-up and steady-state. In the set-up phase, authentication is provided at two different levels to secure the network from malicious adversaries. Upon successful authentication, the nodes are organized into clusters in which each member node associates itself with a cluster head. The steady-state phase deals with seamless transmission within the cluster, i.e., intra-cluster communication, and among the neighboring clusters, i.e., inter-cluster communication. Each member node transmits its multimedia data to its respective cluster head. The member nodes are capable to capture images and video data. Each video is a set of individual frames that are processed back-to-back as a Group of Pictures (GoP). The size of a GoP is fixed, i.e., 10 video frames per GoP, and are processed as consecutive samples. After six GoPs (i.e., 60 samples), buffer threshold for each node reaches. At this point, each node either **a)** drops the data **b)** initiates a channel allocation request to the neighboring cluster head. Each member node transmits its data to the base station via its own cluster head or its neighboring cluster head. In the latter case, a member node initiates a channel allocation request. The network model of SAMS is shown in Fig. 1.

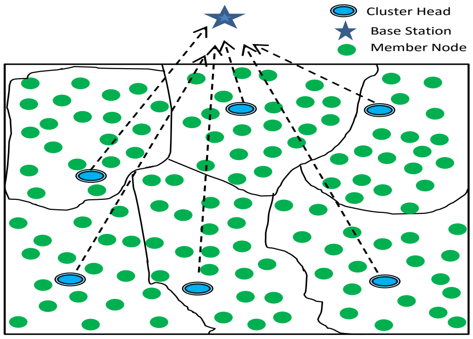


Fig. 1. Network Model

B. Attack Model

Unlike wired networks, WMSNs are deployed in extreme environments that are prone to various threats and attacks. The energy-constrained nature of these networks limits the support for computationally complex and resource-consuming security schemes. To analyze the security of SAMS, we investigate the attack models in WSNs/WMSNs by examining various malicious activities that threaten its operational mechanism. The experimental results in Section V provide various solutions to combat these threats.

1) Packet Replay: An adversary repeatedly broadcasts previously-transmitted packets to affect data freshness by causing network congestion and energy wastage.
2) DoS: An adversary attempts to make network resources unavailable to the legitimate nodes by disrupting the services provided by a given cluster head. DoS is typically accomplished by flooding the cluster heads with excessive requests.
3) Sybil: An adversary forges multiple identities to the nearby nodes in order to influence the network resources in an unauthorized manner.

4) Eavesdropping: An adversary intercepts real-time communication among the legitimate nodes by stealing information in transit.

IV. SAMS: Seamless and Authorized Multimedia Streaming

In this section, we discuss the detailed operations involved during the set-up and steady-state phases of SAMS. In our scheme, two-level authentication is performed during the set-up phase and seamless data transmission is achieved during the steady-state phase. In Table I, the notations along with their description are provided.

Notation	Description
ID_{BS}	Base Station Identity
ID_{CH_i}	Cluster Head Identity
ID_i	Multimedia Node Identity
ID_{NB}	Neighboring Nodes Identities
CH_{opt}	Optimal Percentage of CHs
E_i	Residual Energy
E_{avg}	Average Energy Threshold
τ_i	Assigned Token
λ_i	Secret Key
η	Pseudo-random Nonce
S_{key}	Session Key
M	Cipher-text Message
T_{slot}	Timeslot
n_m	Buffer occupancy at present
n_t	Buffer occupancy threshold

TABLE I. Notations and their description

A. Set-up Phase

This phase provides authentication at two different levels.

1) Between the base station and elected cluster heads.
2) During the cluster formation.

Each multimedia node i acquires a 16-bit τ_i from the base station (BS) upon joining the network, that is used for authentication at different levels. Besides τ_i, each i is provided with a 128-bit λ_i. BS maintains a table of τ_i and issues them to each i. In our scheme, BS controls and manages the authenticity of each node that wishes to join the network.

In each round, BS elects CH_{opt} among i. Here, CH_{opt} is restricted to only 5% of i. Each i broadcasts a ctr_i to BS that contains a 16-bit ID_i, E_i, and a 16-bit ID_{BS}. Upon reception, BS extracts ID_i and E_i, and computes E_{avg}, using Eq. 1.

$$E_{avg} = \sum_{i=1}^{N} \frac{E_i}{N}. \tag{1}$$

Here, N represents the total number of MSNs, $\forall i \in N$.

Any i having E_i equal or greater than E_{avg} is eligible for cluster head (CH) selection. It is highly probable that in any given round, the number of nodes eligible for CH selection is higher than CH_{opt}. In that case, all such nodes are nominees for CHs. BS uses the following criteria for CH_{opt} election among the nominees.

- E_i of a nominee i must be equal or greater than E_{avg}.
- i is not elected as a CH over the past $\frac{1}{CH_{opt}}$ rounds.
- Multiple nominees in the same geographical location are evaluated in the current round based on their previous history of election over the past $\frac{1}{CH_{opt}}$ rounds.

Once CH_{opt} are elected, BS generates the nomination packets pk_{nom}, and broadcasts them to $ID_{CH_{opt}}$. Each pk_{nom} contains ID_{CH_i} and ID_{NB}, where $ID_{CH_i} \in \{ID_{CH_1}, ID_{CH_2}, ...ID_{CH_{opt}}\}$. With each identity within ID_{NB}, there is an associated λ_i and are stored in an array $A[i][j]$. BS performs a $\oplus$ operation on ID_{CH_i}, ID_{BS} and τ_{ch_i} to generate a resultant rst_{ID} for each CH_i, as shown in Eq. 2. The rst_{ID} is then appended to the payload of pk_{nom} and broadcasts to the sensor field. Here, τ_{ch_i} is the token associated with each CH_i. The total number of generated pk_{nom} depends on the total number of elected CH_i. Any non-cluster head node, no matter if it is a legitimate multimedia node or an intruder, may intercept pk_{nom} but is unable to crack it due to the non-availability of a τ_{ch_i}. Only CH_i are capable to decrypt an rst_{ID} to retrieve ID_{CH_i}. An intruder would require 2^{16} attempts to decrypt an rst_{ID} in order to retrieve ID_{CH_i}. The encryption and decryption of an rst_{ID} restricts one or more intruders from cluster head selection. Besides, this procedure ensures that only those nodes can act as CH_i that are nominated by BS. In the deployed sensor field, each i has a τ_i but only a given CH_i can decrypt the payload of pk_{nom}.

$$rst_{ID} = M\ [\tau_{ch_i} \oplus ID_{CH_i} \oplus ID_{BS}]. \tag{2}$$

In Eq. 2, $\oplus$ is an Exclusive-OR cryptographic operation that is cost-effective in terms of resource consumption and computation. Besides, it is an extremely common component in complex ciphers and does not leak any valuable information about an original plain text. Applying it twice enables the original plain text to be retrieved. Here, M indicates that rst_{ID} is a cipher-text message.

Upon decrypting rst_{ID}, each CH_i retrieves its ID_{CH_i} from pk_{nom}. Next, each CH_i generates and broadcasts ACK control packet to acknowledge pk_{nom}. This packet contains the resultant of $\tau_{ch_i} \oplus ID_{BS}$. Each ACK informs the BS that only the legitimate CHs have assumed the roles of CH_i. At this stage, a secured authentication connection has been established between each CH_i and BS. Next, secured connections need to be established within the sensor field, i.e., at the cluster level.

Each CH_i advertises itself by generating an advertisement packet pk_{adv} that contains its identity ID_{CH_i}. A neighboring node may receive multiple pk_{adv}, however, it associates itself with a potential CH_i based on its Received Signal Strength Indicator (RSSI). The radio of a node i calculates RSSI of each pk_{adv}. Based on this calculation, i targets a potential CH_i with the highest value. Cluster formation takes place if the potential CH_i allows an i to join it. Cluster formation is not a straight forward process in SAMS. Each i needs to authenticate itself prior to the formation of a cluster. Moreover, each i needs to ensure that the targeted CH_i is a legitimate node. As a result, both i and CH_i need to be mutually authenticated.

The mutual authentication between i and any CH_i consists of four simple steps. During the first step, each i creates a join-request control packet $JReq_i$ and broadcasts to a CH_i having the strongest RSSI value. Each $JReq_i$ contains ID_i, ID_{CH_i} and τ_i, and can be expressed by Eq. 3.

$$JReq_i = M\ [ID_i, ID_{CH_i}, \tau_i]. \tag{3}$$

During the second step, each CH_i retrieves ID_{CH_i} and ID_i from $JReq_i$. If ID_{CH_i} matches with the ID_{CH_i} of a potential CH_i, it means that $JReq_i$ was indeed intended for it. For any further communication between an i and a CH_i, ID_i must also match with an identity within ID_{NB}, provided to a given CH_i by BS. If a match is found, i.e., $ID_i \in ID_{\text{NB}}$, CH_i retrieves λ_i from its table and responds back with an encrypted challenge by generating η_{CH_i} and S_{key} of 128-bit each. An $\oplus$ operation is performed on λ_i and S_{key} to generate a 128-bit cipher that is appended to η_{CH_i}, and encrypted with λ_i to generate a 256-bit encrypted challenge $\gamma_{challenge}$, using Eq. 4.

$$\gamma_{challenge} = M\ [\{\lambda_i, (\lambda_i \oplus S_{key} | \eta_{CH_i})\}\mathit{AES128}]. \tag{4}$$

In Eq. 4, η_{CH_i} is a temporary pseudo-random nonce that is used only once by a node in the entire cryptographic communication. Each CH_i transmits $\gamma_{challenge}$ to i as a challenge. We used an Advanced Encryption Standard (AES) having a key length of 128 bits in Cipher Block Chaining (CBC) mode to generate $\gamma_{challenge}$ [31]. AES-128 is extremely lightweight for resource-constrained sensor nodes.

During the third step, i needs to decipher $\gamma_{challenge}$ to retrieve S_{key}. If i is successful to do so, it will have the correct η_{CH_i} and S_{key}. Both η_{CH_i} and S_{key} are known only to CH_i, and each λ_i belongs to a specific i. Only a legitimate i can decipher $\gamma_{challenge}$. An adversary can eavesdrop only on η_{CH_i} and S_{key}, but not on λ_i in accordance with the Internet Threat model [32]. Here, i uses its λ_i to decipher $\gamma_{challenge}$. Upon successful decryption, i has successfully authenticated itself. As mutual authentication requires both i and CH_i to be verified, the latter also needs to authenticate itself. At this stage, i performs $\oplus$ operation on η_{CH_i} and λ_i and the resultant is appended to η_i and encrypted with S_{key} to generate a 256-bit encrypted challenge $\beta_{challenge}$, as shown in Eq. 5.

$$\beta_{challenge} = M\ [\{S_{key}, (\eta_{CH_i} \oplus \lambda_i | \eta_i)\}\mathit{AES128}]. \tag{5}$$

Here, η_i is a temporary nonce generated by an i to verify the authenticity of CH_i. The challenge is transmitted by i to the potential CH_i.

During the final step, CH_i decrypts $\beta_{challenge}$ to observe η_{CH_i} in it. If present, CH_i realizes that i has successfully authenticated itself. CH_i retrieves η_i, and creates an encrypted response of its own by appending η_i to S_{key} and encrypts with λ_i, as shown in Eq. 6. Next, $\gamma_{response}$ is transmitted in response to the node i's challenge.

$$\gamma_{response} = M\ [\{\lambda_i, (\eta_i | S_{key})\}\mathit{AES128}]. \tag{6}$$

Upon reception, i checks η_i in $\gamma_{response}$. The presence of η_i indicates that CH_i has also successfully authenticated itself. As η_i was generated by i, it means that the response was received from a legitimate CH_i. At this point, both i and CH_i are mutually authenticated and have agreed upon a common session key S_{key} for data transmission. This process of mutual authentication takes place for each i that wishes to join a potential CH_i. Upon successful authentication, each i becomes a member node of its CH_i that results in a secured cluster formation. At this stage, the steady-state phase initiates and each i transmits the captured data to its CH_i, by encrypting it with its respective S_{key}. The detailed operational mechanism of our two-level authentication is summarized in Algorithm 1.

Algorithm 1 Two-level Authentication

```
Initialization:
    1) Base station ($BS$) assigns $\tau_i$ to each incoming $i$.
    2) $BS$ stores $ID_i$ of each $i$ in a table.
    3) $BS$ assigns $\lambda_i$ to each $i$.
    4) Input: $\{ID_{NB}, ID_i, \lambda_i, \tau_i\}$
                                   ▷ $\forall\ i \in \{1, 2, \cdots, N\} \wedge ID_{NB} \in ID_i$
A. Authentication: Base Station-Cluster Head
for $i = 1 : N$ do                 ▷ Nested For Loop generates a Two-column Table
    for $j = 1 : 2$ do
        input $A[i][j]$
                                   ▷ $ID_{NB}$ and $\lambda_i$ are stored in $A[i][j]$
        $i \rightarrow BS : \{ctr_i$: control packets broadcast by each $i\}$
        $BS$ elects $CH_{opt}$
        $BS$ encrypts $ID_{CH_i}$ with $\tau_{ch_i}$ to generate $rst_{ID}$.
        $BS \rightarrow i : \{pk_{nom}$: contains $A[i][j]$ entries and $ID_{CH_i}\}$.
                                   ▷ The $rst_{ID}$ is appended to $pk_{nom}$ and broadcast.
        if $ID_{CH_i}$ matches then                         ▷ A match is found
            $CH_i$ retrieve $ID_{CH_i}$ and $A[i][j]$.
        end if
        $CH_i \rightarrow BS : \{ACK$: control packet broadcast by each $CH_i\}$
        BS checks for $ID_{BS}$ in $ACK$.
        if $ID_{BS}$ matches then                           ▷ A match is found
            $CH_i$ authenticated.
        end if
    end for
end for
B. Authentication: Within the Cluster
$CH_i \rightarrow i : \{pk_{adv}$: advertisement control packet containing $ID_{CH_i}\}$
$i$ retrieves $ID_{CH_i}$.
$i \rightarrow CH_i : \{JReq_i$: join-request control packet containing $ID_i$ and $ID_{CH_i}\}$
$CH_i$ retrieves $ID_i$ and $ID_{CH_i}$.
if $ID_i$ == $A[i][0]$ and $ID_{CH_i}$ matches then
    $CH_i \rightarrow i : \{\gamma_{challenge}$: encrypted challenge of $CH_i$.$\}$
                                   ▷ $\gamma_{challenge}$ is used to check the authenticity of $i$
else
    $i$ is unauthorized and $JReq_i$ is discarded.
end if
$i$ deciphers $\gamma_{challenge}$ and retrieves $\eta_{CH_i}$and $S_{key}$.
$i \rightarrow CH_i : \{\beta_{challenge}$: encrypted challenge of $i$.$\}$
                                   ▷ $\beta_{challenge}$ is used to check the authenticity of $CH_i$.
$CH_i$ checks $\eta_{CH_i}$ in $\beta_{challenge}$.   ▷ $CH_i$ compares it with its own $\eta_{CH_i}$
if Both matches then
    $i$ becomes a member node of $CH_i$.            ▷ Authentic Cluster Formation.
    $CH_i \rightarrow i : \{\gamma_{response}$: encrypted response of $CH_i$.$\}$
    $CH_i$ broadcasts $\gamma_{response}$ containing $\eta_i$
else
    $i$ is unauthorized and barred from communication to form cluster.
end if
$i$ retrieves $\eta_i$ from $\gamma_{response}$ and compare with its own.
if Both matches then
    $i$ becomes a member node of $CH_i$
    $CH_i$ allocates TDMA slots to $i$
else
    $CH_i$ is unauthorized
end if
```

B. Steady-state Phase

Upon mutual authentication, each member node i within a cluster continuously senses the environment and stores any captured data D_{capt} in its buffer that is bounded by a predefined threshold n_t. Each i waits for its turn to transmit D_{capt} using its allocated T_{slot} that are assigned by its respective CH_i. If the current buffer occupancy n_m is lower, i.e., $n_m < n_t$, and T_{slot} is ready for transmission, then i broadcasts its D_{capt} to its respective CH_i. At this point, intra-cluster communication takes place. When $n_m \geq n_t$ and T_{slot} has not arrived, it means i has to wait longer for its turn to transmit D_{capt}. In this case, i initiates a request for channel allocation to a neighboring cluster head CH_{NB}, where $CH_{NB} \in \{CH_1, CH_2, ...CH_{opt}\}$. In other words, i switches to CH_{NB} by acquiring a spare channel from it. It is important to mention here that CH_{NB} must be a neighboring CH with the next highest RSSI value after CH_i. Another reason for switching to CH_{NB} is that i drops more data packets while waiting for its turn to transmit them to its own CH_i. The dropped data packets may contain sensitive images or highly-prioritized video frames that need to be transmitted immediately. If a multimedia node keeps waiting for its turn to transmit sensitive images or GoP frames, D_{capt} may be of no use by the time it reaches BS. Each CH_i assigns a fixed number of T_{slots} to its member nodes. The duration of T_{slots} may not be sufficient in the case of video packets, i.e., GoP. A request for spare channel allocation to a CH_{NB} is initiated by an i, only if all the channels within a cluster are assigned by a CH_i, and there is no extra channel available to facilitate all or the remaining multimedia packets.

The channel allocation request is forwarded by a CH_i of an i to CH_{NB}, as shown in Fig. 2. If there is an available spare channel, CH_{NB} broadcasts a response to the requesting CH_i. To evaluate the possibility of a spare channel allocation, we analyze the amount of information, i.e., $\sum D_{capt}$, received by each CH_i in Section IV-B1.

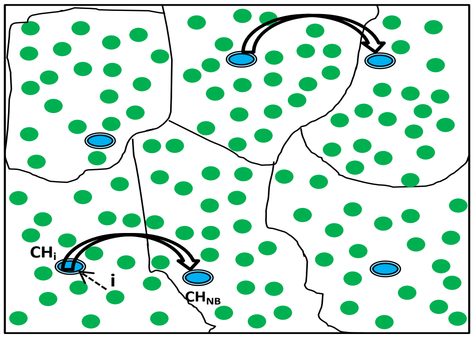


Fig. 2. Request Initiation for Channel Allocation

1) Channel Allocation Request Initiation: In intra-cluster communication, each i transmits D_{capt} to its own CH_i. This is the case when the capturing rate D_{capt} of i is higher than its transmission rate D_{trans} to a CH_i. At the time of network deployment and cluster formation, the buffer of each i remains empty because they are yet to sense the environment. In this case, $D_{capt} = D_{trans} \approx 0$. With the passage of time, each i senses the environment and stores any D_{capt} in its buffer. The consumption of n_m depends on the amount of D_{capt} over a period of time, as shown in Eq. 7.

$$\frac{d}{dt}D_{capt} \rightarrow \begin{cases} 0, & if\ t == 0, \\ n_m, & if\ t > 0. \end{cases} \tag{7}$$

Typically, each i transmits D_{capt} to its own CH_i, when its $n_m < n_t$. On the other hand, if $n_m \geq n_t$, then D_{capt} is transmitted to a CH_{NB}, as shown in Eq. 8.

$$\sum D_{capt} \rightarrow \begin{cases} CH_i, & if\ n_m < n_t, \\ CH_{NB}, & otherwise. \end{cases} \tag{8}$$

BS receives D_{capt} transmitted by each cluster head, as shown in Eq. 9. This equation represents the sum of captured data by all cluster heads.

$$\sum_{i=1}^{CH_{opt}} \sum_{j=1}^{X} CHi \frac{d}{dt} D_{capt}\left(n_{ij}\right) = \sum_{j=1}^{X} \frac{d}{dt} D_{trans}\left(n_{iX}\right),\ if\ n_m < n_t. \tag{9}$$

In Eq. 9, n_{ij} is the total number of member nodes (i.e., j) associated with a given CH_i, and n_{iX} represents all member nodes associated with the total number of cluster heads, i.e., CH_{opt}. In other words, n_{iX} represents all member nodes distributed in various clusters. It is important to mention here that CH_i is the CH of each j within its own cluster. In this equation, each member node has an allocated T_{slot} and the amount of D_{capt} in n_m does not exceed n_t, i.e., $n_m < n_t$.

When $n_m \geq n_t$, a member node i needs to react immediately to avoid the loss of D_{capt}. Instead of waiting for its allocated T_{slot} assigned by its CH_i, each member node needs to switch to a channel available with CH_{NB}. In this case, the amount of information received by a CH_{NB} is represented by Eq. 10.

$$\sum_{i=1}^{CH_{opt}-1} \sum_{j=1}^{X} CH_{NB} \frac{d}{dt} D_{capt}\left(n_{ij}\right) = \sum_{j=1}^{q} \frac{d}{dt} D_{trans}\left(n_{ij}\right),\ \forall q < X. \tag{10}$$

Here, q is the number of member nodes for whom $n_m \geq n_t$. Next, we calculate the remaining member nodes $(q+1)$ that transmit their D_{capt} to their own CH_i, using Eq. 11.

$$\sum_{i=1}^{CH_{opt}} \sum_{j=q+1}^{X} CHi \frac{d}{dt} D_{capt}\left(n_{ij}\right) = \sum_{j=q+1}^{X} \frac{d}{dt} D_{trans}\left(n_{ij}\right). \tag{11}$$

In Eq. 9, we calculated D_{capt} of all the cluster heads CH_{opt}, that is inclusive of both CH_i and CH_{NB}. It is important to mention here that a cluster head in one cluster is a CH_i for all the member nodes in that particular cluster. However, the same cluster head is a CH_{NB} for the member nodes of another cluster, as shown in Fig. 2. In Eq. 10, we calculated D_{capt}

for those member nodes that initiate a request for channel allocation to a CH_{NB}. Finally, in Eq. 11, we calculated D_{capt} only for those member nodes that transmit their D_{capt} to their own CH_i. The complete procedure for channel allocation request is shown in Algorithm 2.

Algorithm 2 : Multimedia Streaming in WMSN

```
Initialization:
    1) Each cluster head assigns TDMA slots $T_{slots}$ to its member nodes.
    2) Each member node senses the environment for capturing data $D_{capt}$.
    3) Each member node monitors its buffer occupancy level $n_m$.
    4) Input: $\{n_m, n_t, D_{capt}, T_{slots}\}$
    Steady-State Phase:
$i$ senses the environment.
                                        ▷ $i$ buffers $D_{capt}$ in its $n_m$
if ($n_m < n_t$) $\wedge T_{slot}$ is True then
    $i \rightarrow CH_i$: $\{D_{capt}$, Intra-cluster communication initiates$\}$.
else
    $i \rightarrow CH_{NB}$ : $\{C_{Req}$, Spare channel allocation request$\}$.
    $i$ sets a timer $t_w$ for a response.
    $CH_{NB}$ checks for any available $T_{slots}$
    if True then
        $CH_{NB} \rightarrow i$ : $\{C_{Res}\}$.
                                        ▷ $CH_{NB}$ sends a positive response to $i$.
    else
        $i$ waits for its own $T_{slot}$.
    end if
    if ($t_{C_{Res}} \leq t_w$) then                ▷ Channel allocated successfully.
        $i \rightarrow CH_{NB}$ : $\{D_{capt}$, Inter-cluster communication initiates$\}$.
    else
        $i$ checks the availability of its own $T_{slot}$
        if True then
            $i \rightarrow CH_i$ : $\{D_{capt}\}$.
        end if
    end if
end if
```

V. Performance Evaluations

In SAMS, each node is equipped with a single half-duplex radio transceiver that support a single-radio multi-channel communication. Our network topology is based on IEEE 802.11e standard. We executed the experiments five times with different node density and BS positions to guarantee better randomness and statistical convergence. The buffer size is set to 60, a scalar integer that represents the maximum number of consecutive samples from each input channel, that can be buffered by a node. We compare SAMS against the existing ones in terms of various performance metrics such as, communication overhead, energy cost, resilience against attacks, cluster size, packet loss and end-to-end delay.

In Table II, a comparison of our proposed two-level authentication scheme is made in terms of communication overhead. This comparison is based on the total number of transmitted messages and the total number of bits required to transmit such messages. The two-level authentication of SAMS requires 8 messages to authenticate various entities in the network. Based on our discussion in Section IV-A, ctr_i is 40-bit, and pk_{nom} and ACK are 16-bit, each. In the cluster authentication, pk_{adv} is 16-bit and $JReq_i$ is 48-bit. $JReq_i$ consists of ID_i, ID_{CH_i} and τ_i. However, τ_i was provided to each i at the time of joining the network. Hence, the remaining content of 32-bit, i.e., $JReq_i$ =$<ID_i, ID_{CH_i}>$, is communicated to each CH_i. The remaining three messages, i.e., $\gamma_{challenge}$, $\beta_{challenge}$ and $\gamma_{response}$, are of 256-bit, each. As an example, $\gamma_{challenge}$=$<\lambda_i, \lambda_i \oplus S_{key}|\eta_{CH_i}>$, and is calculated as M $(\frac{128,128|128}{128}) \times 128$. Using AES-128, the symmetric encryption/decryption requires 128 bits for a 128-bit block size [31]. Based on this discussion, SAMS incurs a communication overhead of only 72 bits for authenticating a connection between BS and each CH_i. On the other hand, it requires only 816 bits to form authenticated clusters. In comparison, the existing schemes of Table II incur excessive communication overheads. In this table, case 1 and case 2 represent the two-level authentication scheme of SAMS.

TABLE II. Communication Overhead Comparison

Schemes	Number of Messages	Number of Bits
Das [28]	3	1696 (Case 1)
	6	3168 (Case 2)
Amin-Biswas [30]	4	2016 (Case 1)
	8	3616 (Case 2)
Turkanovic [29]	4	2432
SAMS	3	72 (Level 1)
	5	816 (Level 2)

In Table III, we compare our two-level authentication against the existing schemes in terms of energy cost, incurred during the authentication. This parameter is calculated in terms of total transmission energy, consumed during in-network authentication. A single bit consumes 4.602μJ during the transmission and 2.34μJ during the reception [33]. SAMS consumes only 0.331mJ for CH-BS authentication (level 1) and 3.76mJ for secured cluster formation (level 2). The existing schemes of Table III incur much higher energy costs.

TABLE III. Energy Cost Comparison

Schemes	Total Transmission Energy (mJ)
Das [28]	7.805 (Case 1)
	14.579 (Case 2)
Amin-Biswas [30]	9.278 (Case 1)
	16.641 (Case 2)
Turkanovic [29]	9.130
SAMS	0.331 (Level 1)
	3.76 (Level 2)

In Table IV, resilience of our two-level authentication is compared against the existing schemes. In our scheme, η_i and η_{CH_i} are generated by a pseudo-random number R_i and appended to a timer T_i. This combination of T_i and R_i assures that an intruder finds it extremely difficult to replay packets. In comparison, the approaches in [30] and [29] are prone to both active and passive replay attacks. In our scheme, a different set of cluster heads are elected in each round. This election restricts an intruder from launching DoS attacks. The use of λ_i and τ_i restricts the malicious insiders from participation during the authentication. In comparison, the approach in [30] is susceptible to malicious insider attacks because they do not have a provisioning for the distribution of security primitives, prior to authentication. BS allows only those nodes that possess a valid λ_i and τ_i to communicate with itself. Each CH_i is authenticated by BS prior to cluster formation. This restricts the nodes, in the role of cluster heads, to launch Sybil attacks. In our scheme, an intruder can eavesdrop only on η_{CH_i} and S_{key}, but not on λ_i. As a result, an intruder is restricted from eavesdropping attacks. The existing schemes, on the other hand, can protect against neither Sybil nor eavesdropping attacks.

TABLE IV. Resilience against various Attacks

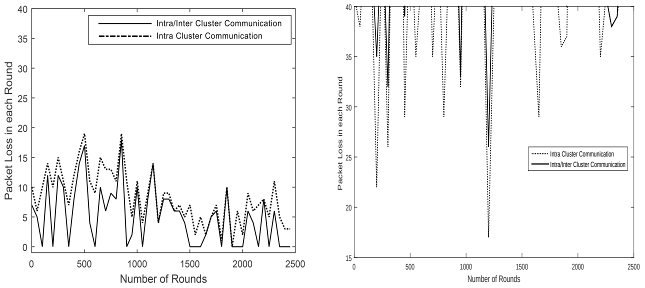
Attacks	**Das** [28]	**Amin-Biswas** [30]	**Turkanovic** [29]	**SAMS**
Replay	Yes	No	No	Yes
DoS	Yes	Yes	Yes	Yes
Insider	Yes	No	Yes	Yes
Sybil	No	No	No	Yes
Eavesdrop	No	No	No	Yes

In Table V, a performance analysis for different cluster sizes is made. For a cluster of 15 nodes, the average response time C_{Res} from a CH_{NB} is 0.2 ms. For the same cluster size, the average time required for mutual authentication $\mathrm{A}_{i \to CH_i}$ is 2.3 ms. The average time T_{Intra} taken by a packet to reach BS via its own CH_i is 0.35 ms. T_{Inter}, on the other hand, is the time taken by a packet to reach BS via a CH_{NB}. The reason for a higher T_{Inter} value is that we calculated T_{Intra} for the first node, scheduled to transmit to CH_i using its T_{slot}. For a cluster of 15 nodes, T_{Intra} is much higher for those nodes that have to wait longer for their turns to transmit to BS, upon the arrival of their T_{slots}. In comparison, for a cluster of 20 nodes, there is a slight variation among these performance metrics. However, for a cluster of 40 nodes, the variation is much higher.

TABLE V. Cluster Size: Performance Analysis

Cluster Size	$\mathbf{C}_{Res}$ $_{(ms)}$	$\mathbf{A}_{i \to CH_i}$ $_{(ms)}$	$\mathbf{T}_{Intra}$ $_{(ms)}$	$\mathbf{T}_{Inter}$ $_{(ms)}$
15	0.2	2.3	0.35	0.61
20	0.2	3.45	0.39	0.7
40	0.25	4.69	0.62	0.94

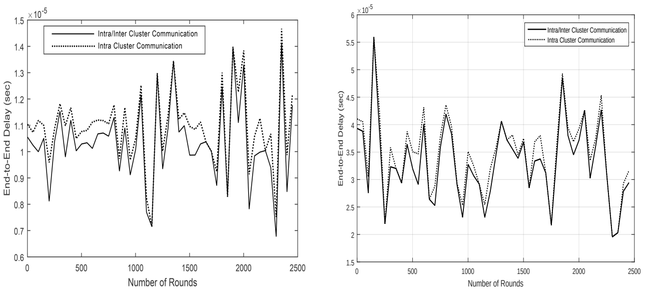
The average packet loss over a period of 2500 rounds is shown in Fig. 3. During intra-cluster communication in SAMS, each i waits for its turn to transmit D_{capt}, using its allocated T_{slot}. The average packet loss is much lower in case of inter-cluster communication due to the assignment of spare channels by CH_{NB}. SAMS follows an intra/inter cluster communication mode in which some of the nodes transmit D_{capt} to BS via CH_i, while the remaining nodes transmit D_{capt} to BS via CH_{NB}. In Fig. 3(a), the total of nodes are 100 and the BS is located outside the sensor field in a 120 × 50 m^2 area. In Fig. 3(b), the total of nodes are 500 and the BS is located outside the sensor field in a 50 × 120 m^2 area. In both these figures, the packet loss for our proposed scheme is significantly lower in comparison to intra-cluster communication mode. This is mainly because of the underlying channel allocation approach and the locations of CH_{NB} in the sensor field.



(a) N=100, BS at 120 × 50 m^2 (b) N=500, BS at 50 × 120 m^2

Fig. 3. Average Packet Loss

A comparison in terms of average end-to-end delay is shown in Fig. 4. In SAMS, each i initiates a C_{Req} to CH_{NB} that may delay the transmission of D_{capt}. However, the C_{Res} is received within the deadline t_w for most of the C_{Req} requests, that result in a much lower delay for D_{capt}. On the other hand, in an intra-cluster communication, i needs to wait longer for its turn to transmit D_{capt}, using its allocated T_{slot}. The member nodes have varying amounts of multimedia data and the transmission of D_{capt} for a node i depends on the schedule of its T_{slot}. For a varying number of nodes and different positions of BS, the average end-to-end delays are shown in Fig. 4(a) and Fig. 4(b), respectively.



(a) N=100, BS at 120 × 50 m^2 (b) N=500, BS at 50 × 120 m^2

Fig. 4. Average End-to-End Delay

VI. Conclusion

In this paper, we proposed a seamless and authorized multimedia streaming (SAMS) framework for WMSN-based IoMT. To secure the multimedia streams, a two-level authentication was provided during the set-up phase of SAMS to elect cluster heads in order to form secured clusters. The formation of these clusters allows seamless and reliable transmission of traffic from member nodes during the steady-state phase. The buffer of each member node is subject to a pre-defined threshold level. Upon exceeding this level, a member node in one cluster acquires a spare channel from a neighboring cluster head. SAMS outperforms the existing schemes in terms of various QoS metrics and provides robust defense against various threats. In future, we aim to explore the mobility of multimedia nodes to analyze its affect on streaming and to reduce communication overhead for ubiquitous data collection and transmission.

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[2] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, “A survey on internet of things from industrial market perspective,” *IEEE Access*, vol. 2, pp. 1660–1679, 2014.

[3] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security and privacy issues in internet-of-things,” *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[4] S. Rani, S. H. Ahmed, R. Talwar, J. Malhotra, and H. Song, “Iomt: A reliable cross layer protocol for internet of multimedia things,” *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 832–839, 2017.

[5] O. Said, Y. Albagory, M. Nofal, and F. Al Raddady, “Iot-rtp and iot-rtcp: Adaptive protocols for multimedia transmission over internet of things environments,” *IEEE Access*, vol. 5, pp. 16 757–16 773, 2017.

[6] G. Xu, E. C.-H. Ngai, and J. Liu, “Ubiquitous transmission of multimedia sensor data in internet-of-things,” *IEEE Internet of Things Journal*, 2017.

[7] M. A. Jan, P. Nanda, X. He, Z. Tan, and R. P. Liu, “A robust authentication scheme for observing resources in the internet of things environment,” in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on*. IEEE, 2014, pp. 205–211.

[8] J. Liu, Y. Xiao, and C. P. Chen, “Authentication and access control in the internet of things,” in *Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on*. IEEE, 2012, pp. 588–592.

[9] K. Hartke, “Practical issues with datagram transport layer security in constrained environments draft-hartke-dice-practical-issues-00,” *IETF work in progress*, 2013.

[10] F. P. Miller, A. F. Vandome, and J. McBrewster, “Advanced encryption standard,” 2009.

[11] Z. Xu, L. Chen, C. Chen, and X. Guan, “Joint clustering and routing design for reliable and efficient data collection in large-scale wireless sensor networks,” *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 520–532, 2016.

[12] P. Nayak and A. Devulapalli, “A fuzzy logic-based clustering algorithm for wsn to extend the network lifetime,” *IEEE sensors journal*, vol. 16, no. 1, pp. 137–144, 2016.

[13] M. A. Jan, P. Nanda, X. He, and R. P. Liu, “Pasccc: Priority-based application-specific congestion control clustering protocol,” *Computer Networks*, vol. 74, pp. 92–102, 2014.

[14] Y. Xiao and F. Hu, *Cognitive radio networks*. CRC press, 2008.

[15] X. Liu, “Atypical hierarchical routing protocols for wireless sensor networks: A review,” *IEEE Sensors Journal*, vol. 15, no. 10, pp. 5372–5383, 2015.

[16] J.-S. Leu, T.-H. Chiang, M.-C. Yu, and K.-W. Su, “Energy efficient clustering scheme for prolonging the lifetime of wireless sensor network with isolated nodes,” *IEEE communications letters*, vol. 19, no. 2, pp. 259–262, 2015.

[17] J.-S. Lee and T.-Y. Kao, “An improved three-layer low-energy adaptive clustering hierarchy for wireless sensor networks,” *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 951–958, 2016.

[18] Z. H. Mir and Y.-B. Ko, “Collaborative topology control for many-to-one communications in wireless sensor networks,” *IEEE Access*, vol. 5, pp. 15 927–15 941, 2017.

[19] H. K. D. Sarma, R. Mall, and A. Kar, “E 2 r 2: Energy-efficient and reliable routing for mobile wireless sensor networks,” *IEEE systems journal*, vol. 10, no. 2, pp. 604–616, 2016.

[20] L. Cheng, J. Niu, M. Di Francesco, S. K. Das, C. Luo, and Y. Gu, “Seamless streaming data delivery in cluster-based wireless sensor networks with mobile elements,” *IEEE Systems Journal*, vol. 10, no. 2, pp. 805–816, 2016.

[21] M. A. Khan and K. Salah, “Iot security: Review, blockchain solutions, and open challenges,” *Future Generation Computer Systems*, 2017.

[22] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, “Secure integration of iot and cloud computing,” *Future Generation Computer Systems*, vol. 78, pp. 964–975, 2018.

[23] M. L. Das, “Two-factor user authentication in wireless sensor networks,” *IEEE transactions on wireless communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[24] B. Vaidya, D. Makrakis, and H. Mouftah, “Two-factor mutual authentication with key agreement in wireless sensor networks,” *Security and Communication Networks*, vol. 9, no. 2, pp. 171–183, 2016.

[25] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, “A secured authentication protocol for wireless sensor networks using elliptic curves cryptography,” *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[26] W. Shi and P. Gong, “A new user authentication protocol for wireless sensor networks using elliptic curves cryptography,” *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, p. 730831, 2013.

[27] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, “Design of secure user authenticated key management protocol for generic iot networks,” *IEEE Internet of Things Journal*, 2017.

[28] A. K. Das, A. K. Sutrala, S. Kumari, V. Odelu, M. Wazid, and X. Li, “An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks,” *Security and Communication Networks*, vol. 9, no. 13, pp. 2070–2092, 2016.

[29] M. Turkanović, B. Brumen, and M. Hölbl, “A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion,” *Ad Hoc Networks*, vol. 20, pp. 96–112, 2014.

[30] R. Amin and G. Biswas, “A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks,” *Ad Hoc Networks*, vol. 36, pp. 58–80, 2016.

[31] F. P. Miller, A. F. Vandome, and J. McBrewster, “Advanced encryption standard,” 2009.

[32] E. Rescorla and B. Korver, “Guidelines for writing rfc text on security considerations,” 2003.

[33] V. Shnayder, M. Hempstead, B.-r. Chen, G. W. Allen, and M. Welsh, “Simulating the power consumption of large-scale sensor network applications,” in *Proceedings of the 2nd international conference on Embedded networked sensor systems*. ACM, 2004, pp. 188–200.