A Novel and Efficient Priority-Based Cross-Layer Contextual Unobservability Scheme Against Global Attacks for WMSNs

https://doi.org/10.3991/ijim.v15i03.18327

Islam T. Almalkawi (✉), Jafar Raed, Ayoub Alsarhan,
Alaa Eddien Abdallah, Emad E. Abdallah
Hashemite University, Zaeqa, Jordan
eslam.malkawi@hu.edu.jo

Abstract—Even though many security schemes proposed for wireless sensor networks protect transmitted data content against different attacks and fulfill most of the desired security requirements, they suffer from not addressing concealing the privacy of the contextual information. Contextual information such as event incidence, event period, and event position can be exposed to an adversary by just monitoring network packet transmission. This kind of information is very important because it can leak location information of key nodes or even detected events themselves. Therefore, proposing a contextual unobservability scheme is a challenging task in sensor networks considering many issues: the broadcast nature of the wireless channel, the different attacker models, the network resource constraints, and the overhead on system performance. Most of the existing location privacy schemes are not addressing all these issues and are either not efficient against global adversaries or degrade significantly network performance. Thus, we propose in this work an innovative and effective location contextual anonymity mechanism in Wireless Multimedia Sensor Network (WMSN) that exploits the cross-layer joint design among different layers: application, routing, and MAC layers. The proposed location unobservability scheme combines the source coding technique, probabilistic packet transmission, multipath routing, and priority-based dropping policy to enhance the efficiency level of the provided privacy service without noticeably affecting the Quality of Service (QoS) requirement for delivering multimedia content in WMSN. Performance evaluation results show that our proposed privacy mechanism outperforms other proposed location privacy techniques regarding privacy efficiency (safety period) and network performance (end-to-end delay and energy consumption).

Keywords—Wireless Multimedia Sensor Network (WMSN), Contextual Unobservability, Source / Sink Location Privacy, image processing, Global Attacks, Priority Packet Dropping, and Cross-layer Optimization

1 Introduction

Wireless Sensor Network (WSN) [1,2] usually comprises a huge number of inexpensive, small size, and resource-constrained sensor nodes that are self-organized and wirelessly communicate to interact with the surrounding environment and measure several scalar physical parameters. These sensor nodes have limited capabilities and resources with respect to storage size, processing power, communication bandwidth, and battery energy because of their reduced size and cost. The sensor nodes are usually installed in hostile and harsh situations where it is difficult to serve them with wired networks and are used in various applications, e.g., object detection and tracking, military monitoring and surveillance, and medical care applications [3,4]. Many of these applications require certain security and privacy level and raise a critical issue, especially when we know that WSN is easily vulnerable to threats compared with wired networks because of its wireless broadcast nature and limited resources, as mentioned before.

Due to the availability of inexpensive camera sensors and audio recorders, the improvement in multimedia processing techniques, and the advancement in the hardware capability of sensor nodes, Wireless Multimedia Sensor Network (WMSN) [5] has emerged. WMSN can now send multimedia content like real-time streaming, still images, video, audio, in addition to scalar data. WMSNs can also store, process multimedia data from diversified sources in real-time, correlate, and fuse them. WMSNs do not merely improve the already existing applications like tracking and monitoring, but they also open the door for new innovative fields. In these new applications, WMSNs support improving the quality of collected information, expanding the coverage range, and supporting multi-resolution views [6].

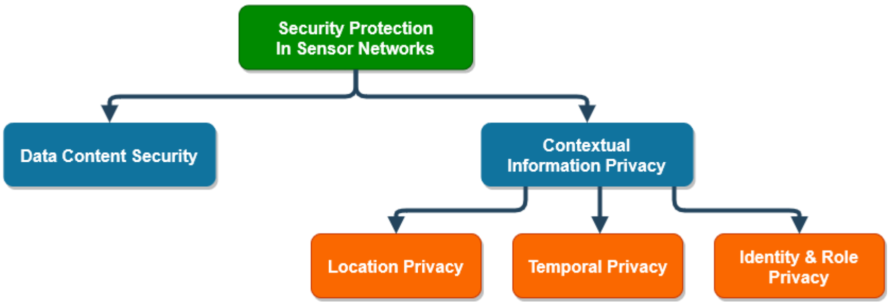

Fig. 1. Classification of Security Protection in Sensor Networks

Many security techniques proposed for WSNs targeted protecting the content of the data generated by the network against possible external or internal adversaries. In general, this can be accomplished by using different security approaches such as data encoding, packet ID verification, node violation detection, secure routing, etc. [7,8], in order to satisfy the required security goals: confidentiality, authentication, integrity, and availability. However, these techniques do not preserve the contextual information from being exposed to adversaries in WSN [9,10]. Contextual information in WSN is the collected information from generating, transmitting, and routing data packets within the network. This type of information has many aspects that may be exploited to reveal events or objects in a network system. For instance, routing packets from a data sender node to a sink node may disclose locations of detected events or important information of key nodes to network-monitoring adversaries. Also, contextual information can leak more sensitive information to attackers such as event occurrences and their happing times.

Hence, protecting the contextual content is very important as much as protecting the data content itself because they reveal vital network information such as event existence and time occurrences, event and node locations, node identities, and node rules. Figure 1 shows the classification of contextual privacy types, which are different than data content security. Consequently, preserving contextual privacy in WSN requires an additional level of security to protect the important nodes in the network or the event being monitored.

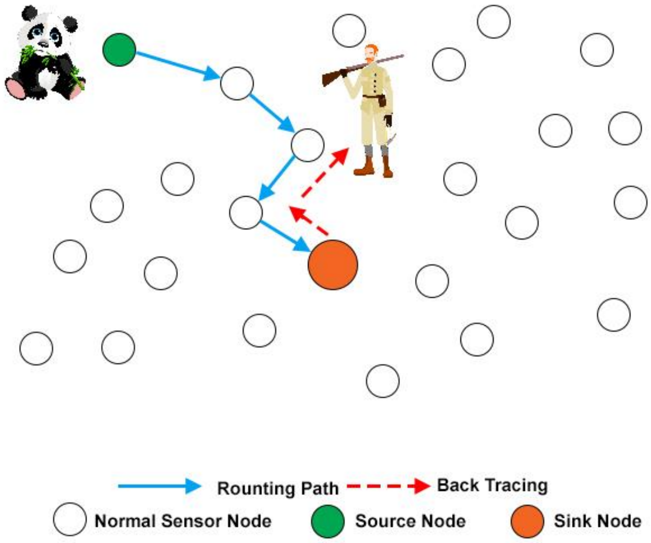

Fig. 2. Transmitted Network Packets Leak Event Location

From the different types of contextual privacy, source/sink location privacy can have critical importance for network designers in many situations [11,12]. An example of that is building a WSN for monitoring endangered species or persistent war zone conditions. In this case, if node locations are revealed, then locations of intended monitored artifacts will be exposed to malicious parties. And a worse scenario can happen if an attacker discovered the sink node location and demolished it, then -in this case- the whole network will be useless. Thus, source/sink unobservability techniques must be used in WSNs to provide location privacy of crucial locations such as data senders, storage nodes, and collecting base stations.

One of the famous models used to formalize the privacy issue is the panda-hunter scenario proposed in [13], in which the attacker (hunter) attempts to backtrack the routing path of transmitted network packets and finally catches the panda as shown in Figure 2. A lot of proposed mechanisms were introduced to resolve the location anonymity problem, like the phantom-based routing mechanism which was first proposed in [13,14]. This mechanism avoids tracking back sent packets by forwarding the packets through random walks and loops across many nodes until reaching the sink node. Using this mechanism establishes many paths between any sender node and the sink, not only one as before, thus making it hard for the attacker to recognize the original source of the sent packet. However as most of phantom-based location privacy routing, this approach is only successful against local adversaries and ineffective against global ones. Moreover, the mechanism puts an excessive overhead on the network, which leads to inappropriate delay in messages delivery, and wastes a lot of energy due to extra message transmissions. Another way of privacy technique was introduced in [15,16] targeting global attacks, which attempts to maintain a constant traffic rate across all nodes in the network by sending fake packets. For example, if a node at a certain time has no real packet, it will send a rubbish packet to keep up the constant rate of sending at all times. Although using this approach is successful against both local and global attackers, it reduces the utilization of network resources and consumes more energy, because of the big amount of fake messages sent through the network. It also increases real packet delivery delay if the transmission rate is lowered in order to decrease the number of needed network-wide fake packets.

Therefore, proposing a location privacy scheme in WMSN is a difficult mission for many issues. *First*, it should take into consideration the wireless broadcast medium used, which makes it easy for the attackers to sniff the network traffic. So, available contextual information like packet sending time and traffic rate can be used by the attacker to perform traffic analysis in order to disclose critical information about events or objects in the network. *Second*, the proposed location privacy scheme should be lightweight with respect to energy consumption, processing and storage capabilities, and communication overhead to meet the limited resources of WMSN. *Third*, the proposed privacy scheme should not noticeably affect the system performance and the intended usage of the network, especially the case of WMSN where delivering multimedia content requires crucial constraints regarding the delivery delay and energy dissipation. *Finally*, it should address the different capabilities of possible adversaries (local or global). Local attackers have limited resources and can only monitor packet transmission in a short range, while global adversaries are stronger with enough resources that can detect sent packets in any network area.

Going briefly through the literature of the proposed location privacy schemes in WSN reveals that they are either targeting only local attacks and/or introducing heavy network overhead by adopting the standard layers of the communication stack without exploiting the inter-dependencies and joint functionalities between the layers. Thus, we propose in this research work a novel event unobservability mechanism that provides an efficient source/sink location privacy against global and local adversaries without degrading system performance. Our proposed location privacy scheme addresses the above-mentioned design issues in WMSN by optimizing a cross-layer design to maintain a probabilistic priority-based network-wide traffic pattern during network operation. We maintain a certain traffic pattern that is independent of event occurrence without using network-wide dummy packets by exploiting the multimedia processing technique in the application layer in generating multiple real packets. Also, we combine the multiple packet generation with multiple-path routing used in the network layer to ensure that the generated traffic pattern throughout the network is following a probabilistic distribution that is independent of event occurrences. Moreover, we adopt a priority-based packet dropping policy in our proposed location privacy scheme to avoid traffic congestion and node buffer overflow. Network performance evaluation shows that the proposed source/sink location unobservability technique has a high level of privacy efficiency (large safety period) while maintaining a good network performance in terms of energy consumption and end-to-end delay compared with existing proposals.

The rest of the paper is organized as follows: Section II reviews briefly the theoretical background and recent work in location privacy in sensor networks. Our system parameters, attack model, and assumptions are described in Section III. Our proposed priority-based cross-layer contextual location privacy scheme is presented in Section IV. Section V shows the performance evaluation of our proposed privacy scheme through simulation results, and Section VI ends the paper with conclusions and future work.

2 Theoretical Background and Related Work

In WSN, contextual information is the data collected from generating, sending, and transferring packets through the network. This contextual information has many features that maybe exploited to uncover the privacy of objects in a communication network. For instance, forwarding data packets to the base station might disclose the positions of critical detected events or significant nodes to an attacker who may be monitor passively the network. Moreover, the adversary can reveal more important information from the network such as event occurrences and time of detecting these events. For example, an attacker (hunter) in a wild-field animal monitoring system [13] is interested not only in the location information about the wild animals but also when or whether the animals are detected by the monitoring application. In addition, the authors in [17] argue that knowing even the signal frequency used in a wireless network can expose information about the sensor's platform hardware and version of software running over them, and then this information may be used by an attacker to exploit their vulnerabilities. Figure 3 classifies in more detail the different types of contextual privacy: identity, location, role, and event existence or time occurrence.

Identity privacy: The nodes in a given communication system are distinguished by unique numbers or identities. These identities can be assigned to the nodes using the global standard Internet Protocol (IPv4 or IPv6) or the nodes are given distinctive numbers locally by the network administrator. It is very important to protect the identity of some key entities in the network like the sink node and the source node.

Location privacy: Preserving the privacy of sensitive node's locations in the network is the most common contextual unobservability investigated in the literature and it is the target of our paper. Monitoring the network data traffic and tracking packet transmission can compromise the information about the node's physical locations. As explained before, knowing the location of a source node can reveal the detected event, also knowing the location of the sink can make the entire network rendered useless. It can be seen that location privacy and identity privacy are similar, but they are different. For instance, by overhearing the transmitted packets in the network, an adversary may know from the packet fields the identity of the sender and/or the destination without being aware of their locations. Conversely, using signal localization and traffic analysis techniques can reveal the location of the sender node for example without knowing its identity.

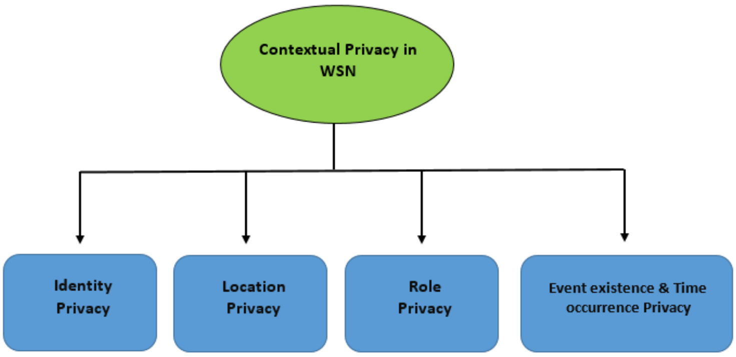
Contextual Privacy in WSN
Identity Privacy
Location Privacy
Role Privacy
Event existence & Time occurrence Privacy

Fig. 3. Taxonomy of Contextual Unobservability in WSN

Role privacy: Nodes in any network have different roles from being sources, forwarders, data storages, cluster heads, or base stations. It is very important to hide the nodes role in the network from the attackers and make them indistinguishable from each other in order not to disturb their functions and destroy the network. Node role can be revealed by monitoring network activity: the start of network traffic can leak the role of a source node, whereas a hot spot area where most of the traffic ends to expose the role of the sink node. Most of the related work combines the node role privacy with its location privacy and treats them as a one issue, e.g., concealing the role of a source node is achieved by hiding its location.

Time occurrence and event existence privacy: In many object monitoring applications and surveillance systems, it is very crucial to protect the monitored events and not to reveal their existence and time detectable occurrence to any possible eavesdropper. Event existence and time detectable occurrence information can be exposed easily to attackers no matter how resilient the used data security algorithm by just overhearing the generated transmission in the system. Recalling the panda-hunter example, data traffic will be generated when an animal passes a certain area in the network. This generated traffic by the detecting source nodes gives a clear evidence to the attacker about the animal existence and its time occurrence.

To the best of our knowledge, there is no previous work address the location privacy problem for WMSN. Our work is the first proposal for location privacy in WMSN that exploits its features to provide a novel and efficient event contextual unobservability scheme. However, there are many source/sink location unobservability schemes that were proposed to target the aforementioned privacy matters for WSNs and surveyed in [9,11], and we summarize some of them below.

A location privacy protocol was introduced in [18], which depends on giving each node a continuously changing pseudonym and on using fake messages. Many control messages will be first exchanged to distribute necessary parameters and keys (node pseudonym, broadcast pseudonym, dummy broadcast pseudonym, random numbers, and shared pair-wise keys with neighbors). Each node should change its pseudonym (ID) and select different next hop node every packet transmission. To prevent traffic rate monitoring attacks dummy packets are used that are similar to real packets. However, this scheme uses a huge amount of control information exchanged all the time in the network and the many calculations are needed every time a node wants to transmit. In addition, different next hop is selected to route the packets towards the sink which may not reside on the optimal path to the destination.

In [19], different location privacy schemes are proposed based on the use of random walk and injection of fake packets: In Forward random walk scheme (FRW), randomize the delivery path so that every node forwards the packets to a randomly selected node from its neighbors whose hop count to the sink is not larger than its own. The Bidirectional tree scheme (BTS) is working with tree topology which can improve the location privacy. In this scheme, real data packets are sent along the shortest path to the sink, and dummy packets are sent through branches to other directions to fake sinks. The zigzag bidirectional tree (ZBT) employs the proxy source and the proxy sink in which data packets are forwarded in a zigzag path. In this method, packets are collected from different sources and directed to the proxy source using branching topology. Then proxy source forwards the packets to the proxy sink using the shortest path. Finally, the proxy sink sends the real data to the sink and dummy packets to fake destinations. However, these schemes are targeting only local eavesdroppers and have a significant negative impact on the performance of the network regarding delivery delay and node energy depletion.

Another location privacy scheme proposed in [20] called Hierarchy rift protection which provides end-to-end location privacy against the local adversary. This scheme uses hierarchy routing for preserving source location in order to create trap routes along the path from sources to the sink. The proposed scheme modifies the phantom scheme by creating more diversionary routes from sources than the traditional phantom routing. However, this scheme fails easily against global attacks and increases the packet delivery delay.

Path Extension Method (PEM) that was introduced in [21] relies on fake sources, which inject the network with fake (rubbish) packets. The strategy of fake sources was used before, but the new idea in PEM is the dynamicity of fake sources, where past schemes determine fake sources at the initialization stage of the network, therefore an attacker can detect these fake sources after some time. To solve that problem, PEM intended to randomize fake sources selection and change it frequently. When a source senses an event, then some other random nodes will start acting as fake sources, which transmit fake packets to the network in a higher transmission rate than real packets are sent, so the attacker will not distinguish real messages and trace it back. Moreover, this method makes use of random walk also, where real packets go through some random walk before being forwarded to the sink using the shortest paths. This method gave good privacy results in terms of both local and global attacks even if the source was close to the sink, also it provided better overhead and message delay, but it flooded the network with a lot of fake packets.

A location privacy scheme based on the concept of the Cyclic Entrapment Method (CEM) is presented in [22]. In this method, location privacy service is provided by using fake sources through transmission loops. The loops should be established before the start operation of the sensor network after node deployment, where every loop consists of a set of nodes in an ordered sequence. Then, when a routing path of real event packets is overlapped with a loop, traffic will be generated in that loop. Even though this scheme immediately injects dummy packets through these loops to hide the sent real packets from the source going through them, an adversary can easily discover the loop trap and return to the original routing path of real packets. In addition, the performance of this proposed scheme relies on the size of the deployed loops.

Another location privacy against local attacks only called BSLDPS (Base source Linear Directional Phantom Source) proposed in [23] that tries to randomize phantom source selection. The packet will be transmitted in random walks multiple hops based on nodes location coordinates until it reaches the phantom source. Then the phantom node sends the packets to the sink using the shortest path. However, the hop count is random regardless of the distance between source and sink, so even if they are nearby, the random walk may be large leading to increase latency and energy consumption.

An algorithm called EDAD (Exponential Dummy Adaptive Distribution) was introduced in [24] for location privacy against global attacks. The proposed scheme depends on the exponential distribution of event arrival to control the packet sending rate. This algorithm uses fake packet transmissions to unify the network traffic. Since every node has its own sending interval based on the exponential distribution, an attacker cannot distinguish the time of real events using time correlation attacks. The proposed scheme got better results than their previous work (DAD) that uses uniform distribution. However, this scheme still consumes the network resources resulted from fake packet injections and increases the latency of delivering real data.

An energy-efficient privacy technique was introduced in [25], called Stochastic and Diffusive Routing using multiple virtual source nodes (SDR-m). Stochastic refers to the random selection of the next hop depending on multiple factors, and diffusion means to route data through multiple paths until it reaches the virtual source (phantom source). At network initialization, the sink node sends broadcast messages to the surrounding nodes to set up the hop-count and this process repeats from the surrounding nodes to others till all nodes become aware of their depths (hop-count from the sink) and their neighbor’s depths. Then, the sink node selects different nodes to be phantom sources and exchanges this information with all other nodes. After finishing network configuration, the routing starts consisting of two phases: In the first phase, a real source sends its data to a phantom source in a stochastic diffusive manner based on the residual energy of the next-hop node in the path to the phantom source. This strategy provides more lifetime for the network and also creates more path diversity for packets. Secondly, the phantom node just forwards packets to the final base station using the minimum distance path. The safety period of this technique depends on the number of phantom sources. Also, this location privacy technique is targeting only local attackers. Moreover, it puts an extra delay because of random paths and the usage of phantom sources.

For the purpose of maximizing the number of deceptive routes to a sink node, a 2-level privacy protocol was introduced in [26], in which each packet goes through two phantom nodes in its route to the sink. The proposed protocol uses a load balancing strategy by shifting the exhaustive routing to non-hotspot nodes, where a non-hotspot area is defined at the initialization phase and all nodes in that area are considered as possible first phantom nodes. Those first phantom nodes will not send packets to sink but to second phantom nodes, which will be randomly selected each time than a specific hop-count away from the first phantom. The selection of a second phantom goes through two stages: selecting first the group area north or south, then randomly selecting the second phantom within the selected group. After that, a real source selects randomly a first phantom to forward packets, then the first phantom selects randomly the second phantom, and finally, the second phantom forwards the packets to the sink node. This method increases complexity to attackers because there are plenty of diverse paths and attackers should expose two phantom sources before exposing the real source. However, this proposed protocol adds more delay and energy consumption because of using the second level of phantom and random walking. Furthermore, this scheme targets only local attackers, not global ones.

Instead of using the usual one-sink structure of WSN, the scheme in [27] introduced a privacy scheme called DMPPR (Dynamic Multipath Privacy Protection) that exploits multi-sink WSN in creating varying paths. The proposed scheme tries to avoid exposing real sources by creating heavy packets transmission in other far nodes (phantom sources). Since these phantom nodes have a higher transmission ratio per time, they will deceive adversaries thinking those nodes are the real ones. In this scheme, a real source transmits its data to a randomly chosen far-away phantom node using greedy routing. The phantom node then divides the received packet into many equal-lengthened portions. Then these packet portions are forwarded randomly to different next-hop nodes, each one of which will select a certain sink to forward the packet portions using random routing with a fixed direction. At the end, the sink initiates a dummy packet that travels randomly through the network every time the sink receives a real packet in order to hide the sink hot-spot area. However, on the other hand, a lot of energy is consumed due to random walking and transmitting many portions instead of just one packet. Also, dividing packets and random forwarding increase delay time. However, this scheme depends on a multi-sink network that should communicate among them to reconstruct the original packet from its divergent portions. This assumption may be hard to maintain in some cases and costs more on network construction. Finally, the scheme proved an effective privacy solution only against local adversaries.

3 System Model

We briefly explain in this section the system model and the assumptions used by our proposed location privacy scheme. In the system model, we explain the used network architecture model and the connection pattern between the nodes, the attacker model assumed by our algorithm, and the model of the node energy.

3.1 Network model

In the network architecture topology, we employ a single-tier flat network architecture [28], as the one shown in Figure 2, deployed with many randomly distributed identical sensor nodes. These nodes are assumed to be homogenous of the same capabilities and functionalities and they are equipped with camera sensors capable of taking images for sensed objects.

- Every node in the system detects events from time to time, where events are expected to occur once during every time interval, and this interval is probabilistic and follows an exponential distribution.
- A node has the ability to apply some multimedia light algorithms on a sensed image before transmitting it through the network.
- Source nodes send their packets to sink node using a QoS based routing protocol introduced in [28], which sends packets over different paths in a multi-hop propagation.
- Sink node can locate anywhere in the network, and we select it to be at the center. At the time of network deployment, the sink node is presumed to be trusted. Also, it is responsible for providing keys necessary for encrypting data transmitted through the network [29].
- All connections among nodes are supposedly encrypted, as our proposed approach is committed to providing contextual information privacy, not data content security.

3.2 Attacker model

In our proposed source/sink location unobservability scheme, we target a **global** attacker model. In this model, the attacker may simultaneously use its own sensors and hardware to capture all packets transmitted throughout the network through node-by-node packet back-tracing or network traffic monitoring in order to find out the location of important nodes. So, the assumed global attacker has the capability to apply different types of attacks on sniffed packets such as time correlation analysis and traffic rate monitoring. In more details, a global adversary can lunch the following types of attack:

- Wireless eavesdropping attack: In this type of attack, the eavesdropper exploits the wireless broadcast nature of WSN and his wireless communication capability in order to receive the sent packets by the network.
- Back tracing attack: Based on the captured packets, the global attacker can apply localization algorithms such as triangulation techniques on these packets to figure

out the position of the transmitter node. This process can be repeated several times to reach the source node.

- Traffic monitoring attack: The global adversary in this kind of attack, by using his/her powerful resources, monitors the data traffic in the entire network, and analyze its behavior. Nodes with higher packet transmission rate can indicate that they are source nodes, while hot spot areas with higher traffic can lead to the sink node.
- Packet analysis attack: Sniffed packets may reveal many useful information to eavesdropper especially if it is not encrypted. The attacker can know source ID, destination ID, and information about detected events from the packet payload. Also, the attacker can analyze the size of sent packets, time of sending, content correlation, sent packets numbers to find the location of key nodes.

The adversary is supposed to be **external**, which implies that it does not previously know any node location, it does not have the ability to compromise nodes and expose their data content, and it cannot decrypt packets. The attacker is supposedly **passive**, i.e. it only monitors the network to track data flow without having the capability to send packets, induce events, block packets, or jam network connection media.

3.3 Energy model

Our energy model assumes that sending and receiving packets utilize the low-power radio communication. Equation 1 describes the consumed energy in a node to send data of *K* bits to wirelessly propagate a distance *d*, and the dissipated energy to receive data of *K* bits calculated by Equation 2.

$$E_{Tx}(K,d) = E_{Tx-Elec}(K) + E_{Tx-amp}(K,d)$$

$$= \begin{cases} K \times E_{elec} + K \times \varepsilon fs \times d^2 \quad , \ d < d_0 \\ \\ K \times E_{elec} + K \times \varepsilon amp \times d^4 \ , \ d \geq d_0 \end{cases} \tag{1}$$

$$E_{Rx}(K) = E_{Rx-elec}(K) = K \times E_{elec} \tag{2}$$

Where $E_{Tx\text{-}elec}(K)$ refers to the energy consumed by the transmission circuitry of the node, $E_{Tx\text{-}amp}$ is the energy consumed by the amplifier circuitry, and $E_{Rx\text{-}elec}(K)$ is the energy consumed by the receiving circuitry. ϵ_{fs} and ϵ_{amp} represent the energy consumed per bit by the node emitter amplifier circuit in the unit area. d_0 is a reference distance. The setting of these parameter values is shown in Table 1.

Table 1. Energy Model Settings

Parameter	Value
Reference Distance d_0 (m)	80
E_{elec} (nJ/bit)	50
ϵ_{fs} (pJ/bit/m^2)	10
ϵ_{amp} (pJ/bit/m^4)	0.0013
Initial Energy (J)	3

4 Priority-Based Cross-layer Contextual Unobservability Scheme

Our proposed contextual privacy mechanism relies on a joint cross-layer architecture among the different layers of the communication stack to utilize the cross functionalities among the layers in order to build more effective sink/source location unobservability functionality against global attackers while providing Quality of Service (QoS) assurance in WMSN. This optimization design exploits the required multimedia source coding technique in the application layer to generate multiple real messages that will be forwarded across the network following different paths established by the routing protocol in the network layer. Then based on the network's condition and node's buffer status, these multiple real packets can be filtered out based on our proposed dropping policy that is implemented in the MAC layer.

The proposed image processing mechanism manipulates the captured image format of a certain event to generate several equal-size significance-different image streams. We take into consideration the restricted node's resources, processing power, storage memory, and battery energy, in designing of the proposed image processing mechanism. Therefore, we use a slight and lightweight procedure that needs a minimum number of calculations in contrast with other existing image processing mechanisms. We simply reorder the pixel bits of the image at the capturing source node into different packets, and then at the sink node, we reconstruct the image to return it to its original format. In comparison with sending rubbish packets in providing location privacy against global attacks, our proposed design provides a better location privacy solution based on processing image data in order to produce multiple significance-different real data packets to use them in securing nodes locations. Also, as proven in [30], the transmission of 1 bit by a sensor node consumes energy as much as processing 3000 calculation instructions. Thus, transmitting fake packets is apparently a waste of network resources.

In supporting multiple data types of different bandwidth and delay requirements, providing reliable data delivery and load balancing, and ensuring a perfect traffic pattern that is independent of detected event occurrences, we employ in our proposed privacy scheme using of a probabilistic traffic transmission with multipath routing. The real-data packets will be transmitted by all nodes at a rate following an exponential distribution to break down the relationship between packet transmission and event occurrence. These transmitted real packets will be forwarded through multiple paths where the most important packets use the best route (e.g. shortest) while less important packets follow the other established paths. In this way, we ensure that every node has enough number of real packets to transmit periodically keeping the defined traffic rate during network operation time.

Finally, in order to avoid network congestion, node's buffer overwhelming, and important packet delivery time, we adopt a priority-based dropping packet scheme. In this policy, packets are prioritized based on the bit significance of the processed image by our proposed multimedia source coding technique. Then depending on the network condition and node's queue status, the proposed packet dropping policy will be applied depending on the mentioned packet priority.

Now, the following subsections illustrate in-depth the design and implementation of the proposed Priority-based cross-layer Location Unobservability scheme against Global adversaries (**PLUG**), which is an enhancement to the one we proposed in [12].

4.1 Multimedia processing technique in the application layer

Based on the image color format and resolution, each image pixel contains a specific number of bits, e.g. image pixels in greyscale consist of 8 bits supporting 256 levels from white to black, whereas in Red Green and Blue (RGB) format image's pixels consist of 24 bits; 8 bits for each color supporting 16M different colors. The bits in each pixel determine the information contained in the image (like color and brightness) where the most important bits are on the left side. If the most left (i.e., most significant) bit is only kept in each pixel, then the generated image is still can be recognized having most of the basic features and objects. Accordingly, having more bits per pixel will eventually improve the quality and resolution of the constructed image keeping all its features. Figure **4** demonstrates the proposed image processing scheme by using the Zelda test image, where the image is shown with different resolutions based on pixel bits. Based on this fact, our proposed image manipulation mechanism processes the captured image by dividing the image pixel bits based on their importance and color information contained therein. Bits of the same importance (position) in each pixel will be later collected together in one packet.

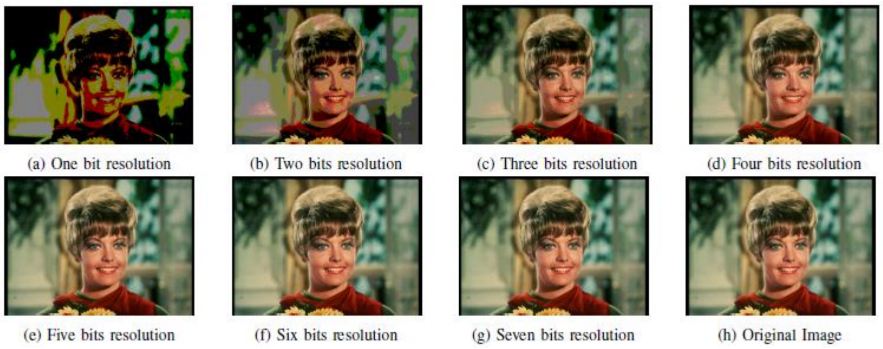
(a) One bit resolution
(b) Two bits resolution
(c) Three bits resolution
(d) Four bits resolution
(e) Five bits resolution
(f) Six bits resolution
(g) Seven bits resolution
(h) Original Image

Fig. 4. Different Image resolutions based on Number of Bits per Color per Pixel

So, following our proposed simple mechanism of image processing, we re-order the bits of the image's pixel based on bit significance and divide the original image to different resolution layers. In order to illustrate this process, we use a simple 3-pixel image and each pixel contains only 3 bits:

$$B3_{p1}B2_{p1}B1_{p1},\ B3_{p2}B2_{p2}B1_{p2},\ B3_{p3}B2_{p3}B1_{p3}$$

Where $B3_{p1}$ represents the most left (most significant) bit of pixel number 1, and $B1_{p1}$ is the least significant bit of the same pixel. After applying our processing mechanism, bits order will be like:

$$B3_{p1}B3_{p2}B3_{p3},\ B2_{p1}B2_{p2}B2_{p3},\ B1_{p1}B1_{p2}B1_{p3}$$

In the sequence of the previous example, the first part ($B3_{p1}$ $B3_{p2}$ $B3_{p3}$) is the most significant bits of the image's pixels, as discussed before, and yet represents a basic low quality (course version) image with most of the objects and features are still identified inside it. Other parts are the less significant image pixel bits and they will produce a higher quality (finer version) image with all objects and color information inside it when all parts are added together. By processing the captured image and transmitting it using the proposed format, the sink node will be able to recognize important objects by receiving only the most significant part of the sequence, which is the first part. On the contrary, if the original image is not processed by our proposed image manipulation mechanism, then receiving a part of the image pixel data will show a high (original) quality for only a part of the image. This regenerated image part might not be sufficient to recognize all the objects in the captured image.

4.2 Exponential distribution transmission with multipath routing

After processing the sensed image using our proposed scheme, image content is now converted into multiple streams (Data chunks) of different importance that can be sent over the network in many packets via a multi-path routing protocol, as the one proposed in [28]. In the multipath routing, high priority packets containing most significant pixel bits of the captured image are routed to the sink using the best-condition paths, which are usually the shortest paths. Since they have less priority, packets containing less significant bits are forwarded to sink via other found paths. Using this priority-based multipath routing strategy, we obtain several advantages: assuring high QoS requirements for different priority packets containing different significant portions of multimedia content (considering the available resources in the established routes like energy and bandwidth), load balancing since we distribute network traffic on many routes, and assisting in providing node location privacy against global attacks. If all source nodes in the WMSN apply our proposed mechanism of image processing along with using the multipath routing to continuously transmit real-data packets at a fixed rate, then global node location privacy will be achieved instead of adopting network-wide dummy packets. As a result, we utilize network resources in sending only real-data packets without needing to waste them in sending fake packets. Also, high priority packets with significant data arrive to sink node with a minimum time delay as routing them does not include any random walk.

Location privacy against global attackers is accomplished by maintaining a fixed pattern of packet traffic throughout the network regardless of the events' occurrence incident. We can attain this independency if each sensor node sends its packets at a same rate; when the packet sending rate rises, it rises all over the network, or vice versa. In our proposed packet transmission approach, the exponential distribution is used to estimate the occurrence time of the next event. The exponential distribution is simpler and easily managed compared to other types of distributions since it depends only on one factor, which is the rate of event (γ) as described in Equation 3. So, based on the selected event rate, we can now compute the required time interval in transmitting consecutive packets, leading in controlling the sending rate of the network.

$$P = e^{-\gamma \times \mathrm{T}} \tag{3}$$

$$T = \frac{lnP}{-\gamma} \tag{4}$$

P is the next event incident probability at a fixed event rate γ during a maximum time interval *T*. If we fixed the value of the event rate γ among all nodes in the network and randomly generate the value of *P* at each node, then we can use Equation 4 to calculate the time interval between two separate events. The calculated time interval will be different from one node to another since *P* is randomly generated at each node. Let us suppose that a camera sensor shoots an event with image resolution of M × N pixels where each pixel consists of *b* bits. Now, the captured image will be manipulated and split to form *n* packets, where each packet consists of *S* bits as a data payload. Consequently, every node will apply Equation 6 to transmit one of its packets each time interval *t*. As all nodes send their packets in different time intervals and packets transmission remains continuous before and after the event occurrence, then it will be a difficult job for an attacker to detect event occurrences or locations.

$$n = \frac{M \times N \times b}{S} \tag{5}$$

$$t = \frac{T}{n} \tag{6}$$

4.3 Packet priority and dropping policy

In many applications, there is no need to send all the image pixel bits to be recognized by the receiver because of its high information redundancy, as explained before. In many cases, keeping only 3 bits –for each color- per pixel can clearly show the image content with all its features as shown in Figure 3. In other words, some bits can be disposed of with no important information loss. Therefore, our proposed algorithm applies a dropping packet policy to give a larger sending priority to the packets that contain important information based on image bit significance in order to avoid network congestion, reduce node’s queueing delay, and improve important packet’s delivery time.

Our proposed packet dropping policy depends on two factors: the significant degree of the packet based on the image pixel bit importance (*PixBitId*), and the dropping rate (α) that depends on the fullness of the node's buffer (let's say above 50%). This proposed packet dropping policy is only applied when the number of received packets exceeds the half size of the node's buffer in order to ensure that the node has always packet to be sent every *t* time following the proposed exponential distribution transmission rate explained in Equation **6**. The implementation of the priority-based packet dropping policy is modeled by Equation **7**.

$$P_{Not-Drop} = \begin{cases} 1 & , \quad PixBitId \leq Q_S \\ 1 - \frac{(PixBitId - Q_S) \times \alpha}{100} & , \quad PixBitId > Q_S \end{cases} \tag{7}$$

Where $P_{Not\text{-}Drop}$ is the probability that the packet will not be dropped and (Q_S) is the pixel bit threshold. Equation **7** implies that packets containing first image pixel bits up to the threshold value (Q_S) are mandatory to be sent and will not be dropped. Thus, these packets will be labeled with high priority and should be treated rapidly in queue processing and transmission scheduling. However, the dropping probability of other packets containing remaining pixel bits depends on the degree of bit significance, where the dropping probability rate decreases by α% with each pixel bit Id larger than the value of (Q_S). The threshold value (Q_S) can be set by the source node in order to determine the required image quality level that is needed to send based on event importance, whereas the dropping rate (α) is set by the forwarder (relay) node to get rid of the unimportant packets based on buffer condition. A random number between 0 and 1 will be generated each time when a packet is ready to be sent; if it is greater than $P_{Not\text{-}Drop}$ then the packet will be dropped and all packets with subsequent pixel bits of the same image will be removed from the node queue.

Now, the pseudo-code of our proposed priority-based cross-layer contextual unobservability scheme is shown below with all operation steps.

Our proposed privacy scheme pseudocode algorithm

```
Initializer:{
 PacketPriority = PriorityList.base(PixBitId);
 N = no. packets per captured image;
 P = Probability of a new event occurrence at this node;
 γ = event rate
  }
List Filler(packet):{
     If(packet received from another sensor){
 newImgId = packet.ImgId();
oldImgId = Packets.findPreviousImgIdFromSameSensor(packet.sensorId);
if(newImgId != oldImgId) {Packets.DropBySensorId(packet.sensorId);}
Pakets.Add(packet);}
  If(new captured image Img){splittedPackets = Img.split(N);}
  }
Transmitting Packets(){
$t$ = Calculating using Equation 6;
While(Packets.ListCount != 0 ){
      Packet = Packets.popHighestPriority(PacketPriority);
      $P_{Not-Drop}$ = calculated using Equation 7;
      If($P_{Not-Drop}$ == 1){SendPacketToNextHop(t, OptimalPath)}
      If{ Queue fullness > 50%}{
          Rand = random(0,1);
          If($P_{Not-Drop}$>Rand){SendPacketToNextHop(t, OtherPath);}
          Else{Packets.DropByImgId(packet.ImgId);}
      }
      Else{ SendPacketToNextHop(t, OtherPath);}
}
  }
```

5 Performance Evaluation

We evaluate in this section the privacy and network performance of our proposed event unobservability mechanism (PLUG) to verify its privacy efficiency and its effect on network performance. We show the simulation results in comparison with other related works, CEM [22] and PEM [21].

5.1 Methodology

We ran several experiments and tests using Network Simulator 2 (NS2 simulator) version 2.35 under Windows 10 professional on Intel(R) Core(TM) i9 -8950K 2.9 GHz and 32 GB RAM machine. We conducted several simulations (over 100) in order to assess the efficiency of our proposed priority-based cross-layer contextual location privacy scheme and determine its impact on network operation performance. We simulate our proposed location privacy scheme assuming a 5000×5000 m^2 network size deployed with different node's numbers from 1000 to 5000 communicating in multi-hop and positioning in a randomized grid. The sink node is positioned in the middle of the network. The packet size is 50K bytes sent with a traffic rate that is following the exponential distribution as explained before.

Table 2 details all simulation settings and network specifications. The simulation outcomes from our proposed privacy scheme are compared with other existing proposed location privacy schemes in several measurements such as safety period, energy consumption, and end-end delay.

Table 2. Used Parameters of the Network Simulation

Network Parameter	Value
Network size	5000×5000 m^2
Node Distribution	Uniformly Distributed
IFQ length	30
Energy model	EnergyModel
Packet Size	50 KB
Node number	Up to 5000
Sink Location	Center of the Network
Radio Range	100 m range using omnidirectional antenna
Max Hop Count for High Priority Packets	64 hops, where PEM and CEM got 77.
Extra Hop Count for Low Priority Packets	Additional 7 hops

5.2 Packets delivery percentage

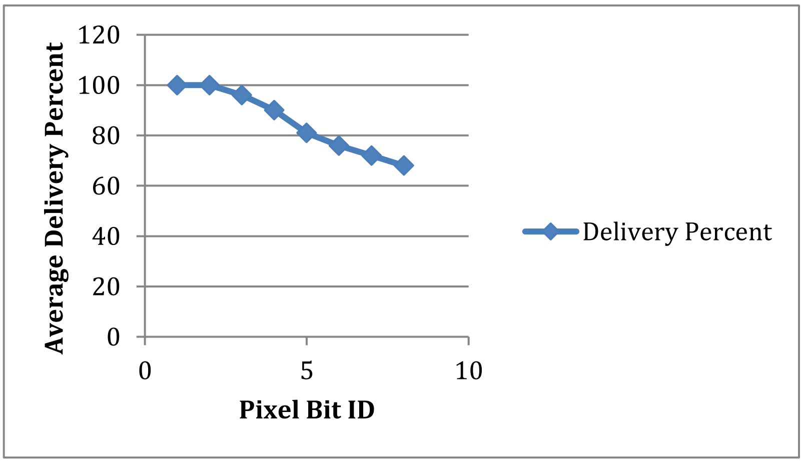

Fig. 5. Packet Delivery Percentage

Our proposed algorithm implies a packet dropping policy, in which we divide image's bits into two groups: significant bits, which are necessary to recognize the object captured by the image, and less significant bits that contribute in increasing the resolution of the image, but it can be disposed of. The significant bits group are always forwarded to the next node, while the other group will be subjected to our dropping policy as defined by Equation 7. This policy is applied only in the case the buffer is going to be full to guarantee that there will be always enough room for the new important packets and to save the energy of processing and transmission surplus packets across the WMSN. In our simulation, we considered the first two bits of each color of image pixel as significant bits, where we used an RGB image format that has 8 bits representing each pixel color. The diagram in Figure 5 shows the average percentage of delivering each bit during the lifetime of the WMSN network, starting initially at no data among the nodes. We assumed that Q_S=2 and α= 5. It is clear that greater image *PixBitId* means lower significance, then higher *PixBitId* also means higher dropping percentage.

5.3 Image reconstruction delay

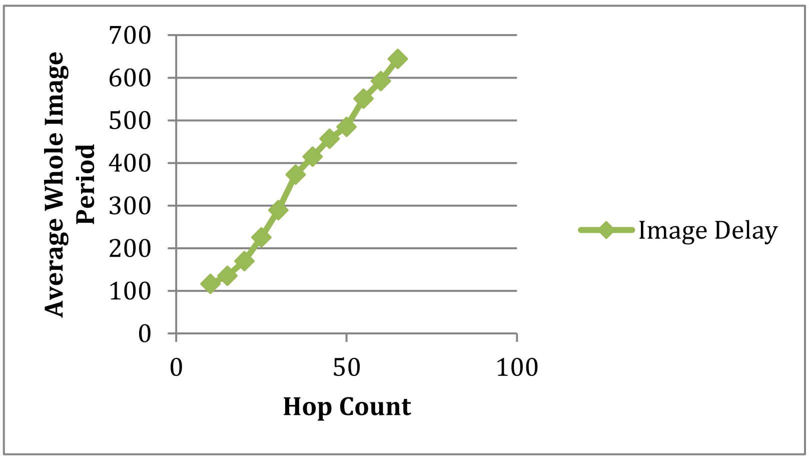

Fig. 6. Average Image Reception Delay

In our approach, we adopt a routing technique that depends on delivering significant packets using optimized (shortest) paths through the network to the sink node. Whereas other packets are forwarded through longer paths to their destination. This technique guarantees that the sink node can recognize sensed objects as fast as possible using most significant packets that contain enough information for identifying the detected objects as demonstrated before. Furthermore, sending low significant packets in different paths gives us an additional layer of unobservability. However, to keep a fixed packet transmission rate for the sake of privacy while not increasing the whole-image delivery delay, we do not use much longer paths for the less significant packets. We measure the average complete-image delivery delay to check the efficiency of our scheme, counting only the images that arrived completely to the sink node, without dropped parts. In order to measure end-end delay for a whole image with different hops distances, we used 800KB captured image size with a packet size of 50KB (i.e., 16 packets are needed to transmit the whole image). And if we assume that the first 100KB of image data are the most significant ones and they will be forwarded through the shortest paths, then the average time needed to receive the complete image is shown in Figure 6.

5.4 Safety period performance

One important measurement of the efficiency level of any proposed privacy mechanism is the safety period, which is calculated by the total number of transmitted packets by a sender before the eavesdropper locates this sender or the sink. One way to achieve efficient results in terms of safety period is injecting the network with dummy packets –along with real packets- to maintain a fixed transmission rate across the network by which the adversary will not be able to identify the occurrences of events, but this way is resource exhaustive since we waste network's energy on fake data. However, in our proposed approach, we exploited the special characteristics of multimedia content and processed it to generate multiple packets of different importance. Then, we managed to use those real packets to maintain a certain network transmission rate in order to hide event occurrences in the WMSN instead of using fake packets. Figure 7 shows that the safety period has been improved in our protocol comparing with other existing works, because of using the abovementioned probabilistic transmission rate across the whole network with the random transmission period for every source. This was achieved by using the exponential distribution that gave us an easy way to control the transmission rate across all nodes. Also, we could obtain better value for the safety period because of applying multipath routing providing different routes to further maintain the independence of the traffic rate and to support different packet priorities.

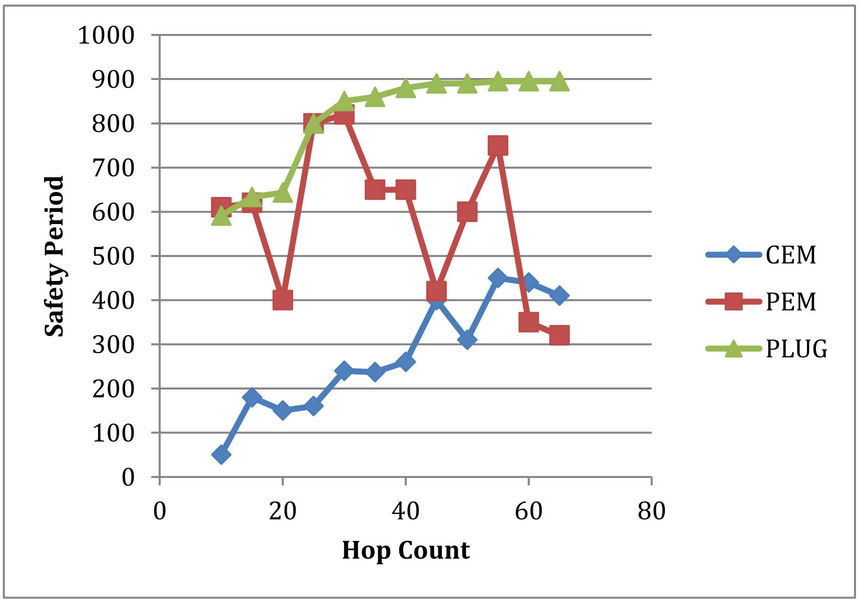

Fig. 7. Average Safety Period Performance

In comparison with PEM and CEM, PLUG made better safety period values as shown in Figure 7, where it shows a proportional relationship between the safety period and hops count. On average, PLUG has 30% higher results than PEM, and the ratio increases to 63% when hop counts becomes 65. Although PEM and PLUG have close results in low-hop-count nodes, as hop count grows, PLUG achieves better difference from PEM, where the safety period in PEM does not increase consistently with the hop-count. If we assume that a 40 hops-node sends packets every 10 seconds, then a captured object can stay at the same place for 45 minutes (10s × safety period for 40 hops node) before being exposed with CEM, and for 1.8 hours with PEM, and for 2.48 hours with PLUG. CEM relies on pre-selected fake sources that inject fake messages while delivering the real one to the sink. But since fake sources are fixed, it is an easy mission for the attacker to uncover it, and once they are uncovered, real sources can be found easily. Therefore, CEM results are the lowest regarding the safety period. PEM improves the safety period results by using randomly selected fake sources with every event, so it becomes harder for the attacker to identify real nodes. Whereas PLUG managed to maintain a unified transmission rate across the network, by which an attacker cannot detect events' occurrences.

5.5 Energy consumption performance

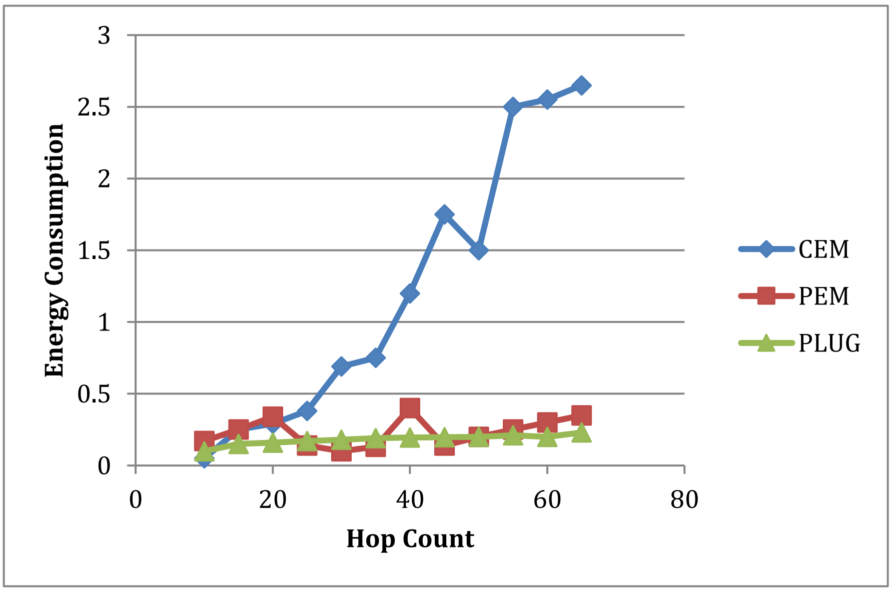

Fig. 8. Energy Consumption Performance

Figure 8 displays that average energy dissipation in our proposed location unobservability protocol got minimum energy consumption figures compared to other approaches. This was achieved because our scheme avoids using of network-wide fake (rubbish) packets in protecting node location privacy, but utilizes the processing of the multimedia content in generating many real packets to maintain the network traffic rate and enhance the quality of received images. In addition, our privacy scheme is not employing long random walks for forwarding packets but only a restricted number of extra hops to forward less important packets. Moreover, adopting the use of our proposed priority-based packet dropping policy saves the energy of processing and transmitting unwanted less significant packets by –possibly- dropping some of them according to packet significance and the status of node’s buffer as explained in Equation **7**. Those mentioned techniques gave us lower energy consumption and gave the WMSN more lifetime to send real data packets.

Our proposed scheme avoids techniques used to enhance network privacy like fake data and random walk routing that consume more nodes energy. On the other hand, CEM's main concept is to create fixed loops of dummy packets traversing across fake sources to make it harder for the attacker to distinguish real packets. Since their loops are fixed, and to avoid to be easily exposed by attackers to discover real sources, it is important for CEM to create as many as possible long fake data loops to achieve good privacy figures. And that is the reason behind the high energy consumption results for CEM. Also, PEM creates varying fake source groups, where a different fake source group is selected with every detected event, and that is how PEM could reduce the number of fake sources. But still, those are fake sources injecting dummy packets into the network and reducing the utilization of nodes energy. Moreover, PEM uses random walk routing, which reduces network lifetime. In PLUG, nodes have a unified transmission rate across the network, so fake sources are not needed, and the energy is totally utilized in transferring only real packets. Also, PLUG exploits a multipath routing with minimal possible extra hops, 7 hops only, which is less than the half number of PEM that has 15 hops random walk. In addition, we apply a packet dropping policy on less significant packets in case a node is being overwhelmed. With this dropping policy, we decrease energy consumption by reducing the number of transmitted packets without affecting recognizing detecting objects. To sum up, we manage to achieve good energy figures, as shown in Figure 8, via omitting fake sources, avoiding long random walks, and adopting the dropping policy.

5.6 End-to-end delay performance

Another important measurement of a successful proposed location unobservability scheme is the packet delivery delay. Any proposed privacy scheme should not ruin the network's intended objective or compromise its performance, especially when we need to assure high QoS for multimedia content. In our approach, nodes always send real data because it relies on the redundant and plenty structure of multimedia data, so all sources are real data sources. Also, we used multipath routing to improve the privacy of our protocol, as stated earlier in the paper, where most significant data packets are forwarded to the sink using optimal (shortest) paths in order to recognize the events in a short time. The remaining low priority packets will be forwarded through other routes, which are restricted to be longer only with extra 7 hops since it was enough to give us efficient performance regarding safety period and energy dissipation. Figure 9 shows that the average end-to-end delay of significant packets has fewer values than the ones in other approaches because it does not involve any random walks. Furthermore, less significant packets also have less delay than other approaches, because we used a lower extra number of hops for the other established routes: PEM for instance used 15 hops, whereas we used only 7.

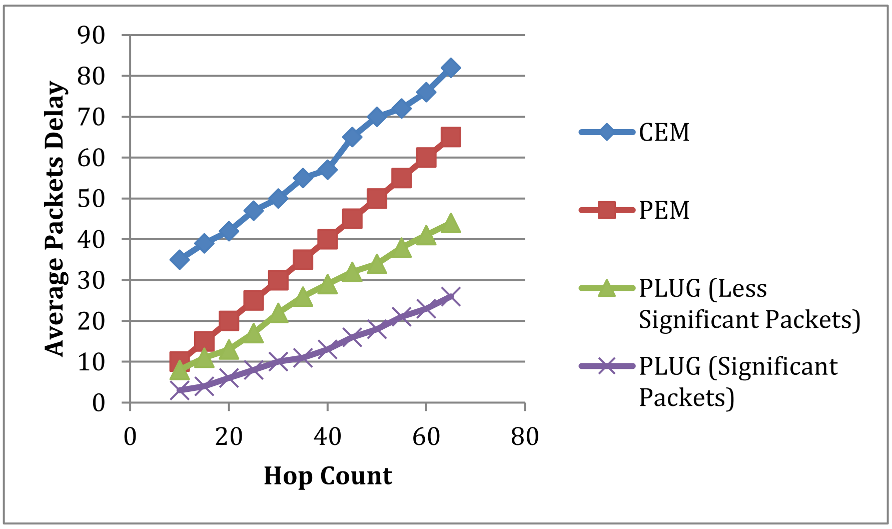

Fig. 9. Average End-to-End Delay Performance

Figure 9 demonstrates the results of average end-to-end delay for the three schemes, which is defined as the number of hops by which a packet passes through in its travel from a source node to the sink node. Since significant and less significant packets are treated differently in PLUG, then we show two different results plots for each. Taking into consideration that significant packets are routed using shortest paths, then definitely it will achieve the least delivery time, where PEM has an average ratio of 64% higher delivery time than PLUG, and CEM is 77% higher. In a matter of fact, random walk is not used in our algorithm, but we prefer to use instead of it a multipath routing with less significant packets in order to add an extra layer of privacy. PEM used a random walk of 15 hops, we were satisfied with only 7 hops since it was enough to achieve a convincing value of safety period, to minimize energy consumption, and to not increase the end-to-end delay too much. Hence, although less significant packets go through not optimal (longer) paths, it still has a better delivery time average, 30% lower average ratio of PEM, and 56% lower results than CEM.

6 Conclusion

We introduce in this paper the first effective scheme that supports Wireless Multimedia Sensor Networks (WMSNs) with unobservability service regarding source/sink nodes locations and event occurrences. Our proposed location anonymity scheme succeeds to hide the location of important network nodes and object events by efficiently exploiting the joint design among the application, routing, and MAC layers to increase privacy efficiency and network performance. The proposed priority-based cross-layer contextual unobservability scheme makes use of a multimedia processing mechanism applied to detected event images in conjunction with probabilistic (based on exponential distribution) continuous transmission, a multi-path routing protocol for different significance image parts, and a priority-based packet dropping policy for insignificant image parts to maintain a unified traffic pattern all across the network. By adopting this proposal, we protect significant contextual information from being exposed to both local and global attackers without noticeably wasting network resources or degrading system performance. This is done by avoiding using fake packets injection or long random walks/loops. So, in other words, the network is mostly utilized in delivering data packets and providing location privacy. Simulation results indicate that the proposed location anonymity protocol offers a high degree of privacy in terms of the safety period by removing the dependency of event occurrence on packet transmission. Moreover, it imposes a lower impact on network performance regarding end-to-end delay and energy consumption in comparison with other proposed approaches since we avoid using random walks/ long loops and network-wide dummy packets respectively. In future work, we plan to test the performance of our proposed scheme against different types of attack models including additional attacks such as active attackers (generating or modifying packets), insider attackers (malicious nodes), and harmful attackers (warm-hole and routing blocking). Also, we will analyze our scheme in a real-time application using wireless hardware such as Raspberry Pi 4 and Arduino Mega.

7 Acknowledgement

This paper was supported and funded by Hashemite University, Jordan.

8 References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks, vol. 38, no. 4, pp. 393– 422, 2002. https://doi.org/10.1016/s1389-1286(01)00302-4

[2] V. Potdar, A. Sharif, and E. Chang, "Wireless sensor networks: A survey," in 2009 International Conference on Advanced Information Networking and Applications Workshops, pp. 636–641, 2009. https://doi.org/10.1109/waina.2009.193

[3] P. J. Sousa, R. Tavares, P. Abreu, M. Teresa Restivo, "NSensor – Wireless Sensor Network for Environmental Monitoring," International Journal of Interactive Mobile Technologies (iJIM), vol. 11, no. 5, pp. 25–36, 2017. https://doi.org/10.3991/ijim.v11i5.7067

[4] Abubakar Adam, Adamu Abubakar, Murni Mahmud, "Sensor Enhanced Health Information Systems: Issues and Challenges," International Journal of Interactive Mobile Technologies (iJIM), vol. 13, no. 1, pp. 99–114, 2019. https://doi.org/10.3991/ijim.v13i01.7037

[5] I. T. Almalkawi, M. Guerrero Zapata, J. N. Al-Karaki, and J. Morillo-Pozo, "Wireless multimedia sensor networks: Current trends and future directions," Sensors, vol. 10, no. 7, pp. 6662–6717, 2010. https://doi.org/10.3390/s100706662

[6] R. Cucchiara, "Multimedia surveillance systems," in Proceedings of the Third ACM International Workshop on Video Surveillance &Amp; Sensor Networks. VSSN '05, 2005, pp. 3–10, 2005. https://doi.org/10.1145/1099396.1099399

[7] L Raghavendar Raju, C R K Reddy Reddy, "A Key Exchange Approach for Proficient and Secure Routing in Mobile Adhoc Networks," International Journal of Interactive Mobile Technologies (iJIM), vol. 11, no. 4, pp. 43–54, 2017. https://doi.org/10.3991/ijim.v11i4.6440

[8] Dina M. Ibrahim, Nada M. Alruhaily, "Anomaly Detection in Wireless Sensor Networks: A Proposed Framework," International Journal of Interactive Mobile Technologies (iJIM), vol. 14, no. 10, pp. 150–158, 2020. https://doi.org/10.3991/ijim.v14i10.14261

[9] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," Ad Hoc Networks, vol. 7, no. 8, pp. 1501 – 1514, 2009. https://doi.org/10.1016/j.adhoc.2009.04.009

[10] M. Conti, J.Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," IEEE Communications Surveys Tutorials, vol. 15, no. 3, pp. 1238–1280, 2013. https://doi.org/10.1109/surv.2013.011413.00118

[11] J. Jiang, G. Han, H. Wang, and M. Guizani, "A survey on location privacy protection in wireless sensor networks," Journal of Network and Computer Applications, vol. 125, pp. 93 – 114, 2019. https://doi.org/10.1016/j.jnca.2018.10.008

[12] I. T. Almalkawi, J. Raed, N. Alghaeb, and M. G. Zapata, "An efficient location privacy scheme for wireless multimedia sensor networks," in 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2019, pp. 1615–1618. https://doi.org/10.1109/etfa.2019.8869338

[13] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy constrained sensor network routing," in the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 88–93, 2004. https://doi.org/10.1145/1029102.1029117

[14] P. Kamat, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in 25th IEEE International Conference on Distributed Computing Systems, pp. 599–608, 2005. https://doi.org/10.1109/icdcs.2005.31

[15] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper," IEEE Transactions on Mobile Computing, vol. 11, no. 2, pp. 320–336, 2012. https://doi.org/10.1109/tmc.2011.32

[16] A. Bushnag, A. Abuzneid, and A. Mahmood, "Source anonymity against global adversary in wsns using dummy packet injections: A survey," Electronics, vol. 7, no. 10, 2018. https://doi.org/10.3390/electronics7100250

[17] S. Pai, S. Bermudez, S. Wicker, M. Meingast, T. Roosta, S. Sastry, and D. Mulligan, "Transactional confidentiality in sensor networks," Security Privacy, IEEE, vol. 6, no. 4, pp. 28–35, 2008. https://doi.org/10.1109/msp.2008.107

[18] A. Abuzneid, T. Sobh, and M. Faezipour, "An enhanced communication protocol for anonymity and location privacy in wsn," in IEEE Wireless Communications and Networking Conference Workshops, 2015, pp. 91–96. https://doi.org/10.1109/wcncw.2015.7122535

[19] H. Chen and W. Lou, "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," Pervasive and Mobile Computing, vol. 16, pp. 36 – 50, 2015. https://doi.org/10.1016/j.pmcj.2014.01.006

[20] S. Babu and K. Balasubadra, "Chronic privacy protection from source to sink in sensor network routing," International Journal of Applied Engineering Research, vol. 13, no. 5, pp. 2798–2808, 2018.

[21] W. Tan, K. Xu, and D. Wang, "An anti-tracking source-location privacy protection protocol in wsns based on path extension," IEEE Internet of Things Journal, vol. 1, no. 5, pp. 461–471, 2014. https://doi.org/10.1109/jiot.2014.2346813

[22] Yi Ouyang, Xhengyi Le, Guanling Chen, J. Ford, and F. Makedon, "Entrapping adversaries for source protection in sensor networks," in 2006 International Symposium on a World of

Wireless, Mobile and Multimedia Networks (WoWMoM'06), 2006, pp. 10 pp.–34. https://doi.org/10.1109/wowmom.2006.40

[23] L. Bai, G. Li, and H. Zhu, "Privacy protection algorithm based on linear directional phantom source node in wsn," in 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), 2017, pp. 851–854. https://doi.org/10.1109/icsess.2017.8343044

[24] A. Bushnag, A. Abuzneid, and A. Mahmood, "An efficient source anonymity technique based on exponential distribution against a global adversary model using fake injections," in Proceedings of the 13th ACM Symposium on QoS and Security for Wireless and Mobile Networks. Q2SWinet '17, 2017, pp. 15–21. https://doi.org/10.1145/3132114.3132120

[25] Manjula R., RajaDatta. s.l , "A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs". Pervasive and Mobile Computing, Vol. 44. pp. 1574-1192, 2018. https://doi.org/10.1016/j.pmcj.2018.01.006

[26] L. C. Mutalemwa, M. Kang and S. Shin. Fukuoka, "Controlling the Communication Overhead of Source Location Privacy Protocols in Multi-hop Communication Wireless Networks". International Conference on Artificial Intelligence in Information and Communication (ICAIIC), pp. 055-059, 2020. https://doi.org/10.1109/icaiic48513.2020.9065284

[27] G. Han, H. Wang, X. Miao, L. Liu, J. Jiang and Y. Peng, "A Dynamic Multipath Scheme for Protecting Source-Location Privacy Using Multiple Sinks in WSNs Intended for IIoT", IEEE Transactions on Industrial Informatics, Vol. 16, pp. 5527-5538, 2020. https://doi.org/10.1109/tii.2019.2953937

[28] I. T. Almalkawi, M. G. Zapata, and J. N. Al-Karaki, "A cross-layer based clustered multipath routing with QoS-aware scheduling for wireless multimedia sensor networks," International Journal of Distributed Sensor Networks, vol. 8, no. 5, pp. 392515, 2012. https://doi.org/10.1155/2012/392515

[29] I. T. Almalkawi, M. G. Zapata, and J. N. Al-Karaki, "A Secure Cluster-Based Multipath Routing Protocol for WMSNs," Sensors, vol. 11, no. 4, pp. 4401-4424, 2011. https://doi.org/10.3390/s110404401

[30] L. A. Grieco, G. Boggia, S. Sicari, and P. Colombo, "Secure wireless multimedia sensor networks: A survey," in 2009 Third International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pp. 194–201, 2009. https://doi.org/10.1109/ubicomm.2009.27

9 Authors

Islam T. Almalkawi received his Ph.D. degree in 2013 from Polytechnic University of Catalunya (UPC), the M.Sc. degree in 2008 from Carnegie Mellon University (CMU), and BSc. degree in 2004 from Hashemite University (HU). He is currently an Assistant Professor in the Computer Engineering Department at Hashemite University (HU). Dr. Almalkawi worked as Research Assistance in several European Union projects during master and Ph.D. studies. His research interests include Wireless Sensor Networks, Multimedia Networks, Wireless Network Security, Image Processing, Cognitive Radio Networks, Internet of Things Networks, and Smart and Green Wireless Systems.

Jafar Raed was a batch topper Computer Engineering Bachelor graduate from the Hashemite University in 2019. He trained as a full stack developer In Nextwo Company in 2019. He is currently working as a Consultant Engineer in Embedded Systems with SEDCO Company. He contributed to several projects in WSN in Collaboration with King Abdullah II Design and Development Bureau (KADDB) In Jordan. His research interests include Wireless Ad Hoc Networks, Routing Protocols, Simulation Optimization, Computer Security, and Embedded Systems.

Ayoub Alsarhan received the B.E. degree in computer science from the Yarmouk University, Jordan, in 1997, the M.Sc. degree in computer science from Al-Bayt University, Jordan, in 2001, and the Ph.D. degree in electrical and computer engineering from Concordia University, Canada, in 2011. He is currently an Associate Professor with the Computer Information System Department, Hashemite University, Zarqa, Jordan. His research interests include cognitive networks, parallel processing, cloud computing, machine learning, and real-time multimedia communication over the Internet.

Alla E. Abdallah is currently an associate professor in the Department of Computer Science at the Hashemite University (HU), Jordan. He received his Ph.D. in Computer Science from Concordia University in 2008, where he worked on routing algorithms for mobile ad hoc networks. He received his BS in Computer Science from Yarmouk University, Jordan, and MS in Computer Science from the University of Jordan in 2000 and 2004, respectively. Prior to joining HU, he was a network researcher at consulting private company in Montreal (2008 - 2011). His current research interests include Routing Protocols for Ad Hoc Networks, Parallel and Distributed Systems, and Multimedia Security.

Emad E. Abdallah is currently a Professor in the Department of Computer Information Systems at the Hashemite University (HU), Jordan. He received his Ph.D. in Computer Science from Concordia University in 2008, where he worked on multimedia security, pattern recognition, and 3D object recognition. He received his BS in Computer Science from Yarmouk University, Jordan, and MS in Computer Science from the University of Jordan in 2000 and 2004, respectively. Prior to joining HU, he was a Software Developer at SAP Labs Montreal. His current research interests include computer graphics, multimedia security, pattern recognition, and computer networks.

Article submitted 2020-09-08. Resubmitted 2020-11-16. Final acceptance 2020-11-17. Final version published as submitted by the authors.