Privacy-Aware Ant Routing for Wireless Multimedia Sensor Networks in Healthcare

Yasmine N. M. Saleh, Claude C. Chibelushi, Ayman A. Abdel-Hamid , and Abdel-Hamid Soliman

Abstract— **Although the importance of privacy is well-acknowledged for sensitive healthcare data, significant research efforts are still needed to develop robust privacy protection solutions for Wireless Multimedia Sensor Networks (WMSNs) used in the context of healthcare. The aim of this paper is to investigate privacy-preserving mechanisms for WMSNs for use in healthcare, to ensure privacy-aware transmission (from sensors to the base station) of multimedia data. The AntSensNet is a WMSN-based routing protocol, which combines the basics of the ant colony optimization-based routing with the hierarchal structure of the network, to provide QoS and power efficient multipath multimedia packet scheduling. In this paper, the AntSensNet routing protocol was extended by adding to it privacy-preserving mechanisms, towards achieving unlinkability, anonymity / pseudonymity and location privacy. The standard AntSensNet routing protocol is vulnerable to privacy threats. Consequently, the following privacy attacks' countermeasures were incorporated: (i) size correlation and encryption of scalar and multimedia data transmitted through a WMSN, and size correlation and encryption of ants, to achieve unlinkability and location privacy; (ii) fake traffic injection, to achieve anonymity, source location and base station location privacy, as well as unlinkability; (iii) pseudonyms, to achieve unlinkability. To assess the impact of such countermeasures, a quantitative performance analysis was conducted through simulation to gauge the overhead of the added privacy countermeasures. It can be concluded that the added privacy measures have enhanced privacy but at the expense of extra delay and multimedia jitter. The sources and the volumes of fake traffic must be carefully studied depending on the health condition of a patient to determine what vitals need to be monitored, whether video and audio monitoring is required or not versus the required level of privacy.**

Index Terms— **Wireless Multimedia Sensor Networks (WMSN) - Anonymity - Ant Routing - Location Privacy – Pseudonymity - Unlinkability**

I. Introduction

Privacy violations and security risks in healthcare systems may cause leakage of sensitive information about patients' diseases which may be embarrassing or critical; and could cause the patients to lose their jobs, or be unable to obtain insurance, and sometimes lead to risks such as an adversary (or criminal mind) finding the location of a person, with possible life-threatening consequences [1]. A key factor for the acceptance of the interchange of healthcare information in medical healthcare networks is the consistent and coordinated safeguard of patients' privacy and security [2].

Privacy in WSN-based healthcare systems is a complex issue due to the capturing of continuous medical data for potentially long periods of time. The diverse and wide range of data about the medical and the daily routines, and the health information is utilized by different information systems belonging to a wide range of beneficiaries such as insurance companies, life coaches, family, homecare providers, researchers and others [3][4]. Privacy in healthcare systems based on Wireless Multimedia Sensor Networks (WMSN) imposes even more challenges due to the nature of the multimedia data (video and audio). It is important to identify the necessary privacy services for a WMSN-based healthcare system at the design stage to avoid the challenging and the overhead in time and money due to the addition of these services after the system is developed.

"Privacy-by-design" refers to privacy protection safeguards that must be taken into consideration during the stages of the engineering process of a system [5]. In [6] a formal privacy threat analysis methodology was applied to a WMSN-based healthcare sub-system to discover the significant privacy services that must be present in a healthcare sub-system to be accepted by patients and governments in real life. Data should be delivered securely and privately from source to destination.

Ant Colony Optimization (ACO) is a swarm intelligence based algorithms inspired by the behavior of ant colonies in search for food [7]. The distributed heuristic nature of the ant-based routing protocols are suitable for WSNs due to: distributed nature of the algorithm (no single point of failure); simple operations carried at the nodes; asynchronous and autonomous algorithm interactions; self-organizing nature; adaptation to different traffic and adaptation to topological variation and traffic demand [8]. The basic idea of ant-based routing is to acquire information about the route using a collective learning process for path sampling using concurrent and independent agents (ants) to try out a path to a certain

Yasmine N. M. Saleh is with the Arab Academy for Science and Technology and Maritime Transport, Alexandria, Egypt (email: yasmine_nagi@aast.edu).

Prof. Claude C. Chibelushi was with Staffordshire University, Beaconside, Stafford ST18 0AD, U.K. He is now with Semantic 21 Ltd, 9&10 Beacon Business Park, Stafford, ST180WL, UK (email: Claude.Chibelushi@semantics21.com)

Prof. Ayman A. Abdel-Hamid is with the Arab Academy for Science and Technology and Maritime Transport, Alexandria, Egypt (email: hamid@aast.edu)

Dr Abdel-Hamid Soliman is with Staffordshire University, Mellor building, College Rd, Stoke on Trent, ST4 TDE, U.K (email: a.soliman2staffs.ac.uk).

destination [9].

The aim of this paper is to present the enhancement of the AntSensNet [8] WMSN-based routing protocol, to make it privacy and security aware (using a key management protocol called LEAP [10]). It is envisaged that the enhancement will increase the domain of deployment of this routing protocol, to include applications requiring privacy and security services. The AntSensNet routing protocol will be used as the underlying routing protocol to create a privacy-aware WMSN-based healthcare sub-system.

The rest of this paper is organized as follows. Section II reviews the AntSensNet routing protocol. Section III discusses the proposed privacy-aware AntSensNet protocol. Section IV depicts performance evaluation experiments and analysis using NS2-based simulation experiments. Finally, section V outlines conclusion and discusses future work.

II. AntSensNet Routing Protocol Review

A recent study conducted by [7], showed that many WMSN-based ant-based protocols aim to increase network lifetime by reducing energy consumption. In addition, many protocols adopt one or more QoS metrics and use multipath routing for network traffic load distribution. Among these WMSN-based ant routing protocols are: M-IAR [11], ASAR [12], ACOLBR [13], ACOWMSN [14], [15], EAQHSeN [16], AntSensNet [8] and several others.

The AntSensNet protocol combines the basics of the ant colony optimization-based routing with the hierarchal structure of the network, to provide QoS and power efficient multipath video packet scheduling. It is designed especially for WMSNs. The choice of the AntSensNet protocol as the underlying routing protocol for this research work has been justified in [6].

AntSensNet is composed of three main parts: (1) clustering the network nodes into colonies. Clustering is an important step as it allows scalability, saves network resources as resource- rich nodes are selected as cluster heads, forming a backbone of cluster heads and increasing the network lifetime by applying cluster head rotation. (2) Route discovery between the clusters, which is based on the application requirements. (3) Traffic forwarding is based on the routes discovered in (2).

In the route discovery phase, forward ants (FANTs) leave the source node to the neighboring nodes to discover the routes surrounding the node towards the base station. As the FANTs move around the network, each node constructs a routing table containing the identification of all surrounding neighborhood nodes and their corresponding pheromone level.

The data collected by ants is stored in a pheromone table containing: cluster head neighbor ID - traffic class (based on the application) - QoS parameters - Expiration time

The AntSensNet protocol is a three-phase algorithm: the forward ants (FANTs) phase, the backward ants (BANTs) phase and the routing maintenance phase. The FANTs phase is when a cluster head needs to send the data; the pheromone table is checked to find an unexpired route to use. If all paths in the table are expired or the paths are unsatisfactory, FANTs are broadcast from the cluster head to the sink to discover other routes. When a cluster head receives a FANT, it updates the ant. The cluster head adds its ID to the ant nodes stack, increments the hop count field and updates the ant's information field. In the BANTs phase, after the FANT reaches the sink, the sink evaluates the QoS parameters to decide whether these parameters are appropriate for the application requirements. If the parameters in the FANT are not appropriate, then the ant is discarded. If the parameters are appropriate, a BANT is generated and sent back in the same path that the FANT followed. During the return of the BANT, the pheromones are updated in the routing tables of the cluster heads it passes by. In the route maintenance phase, the routes are updated to deal with the congestion and lost link problems

III. Proposed Privacy-aware AntSensNet Routing Protocol

In this section, the privacy of AntSensNet routing protocol is assessed to identify the required privacy services. Next, the privacy-aware AntSensNet protocol will be discussed.

A. *Privacy Assessment of AntSensNet routing protocol*

The AntSensNet paper [8] protocol did not mention any privacy or security services supported by the proposed protocol for the protection of the data, or of the identity of the sender/receiver or the location of the sender/receiver of the data. The lack of privacy and security services can cause serious privacy threats as depicted in Table 1.

Table 1 Privacy threats and their corresponding privacy services required for the AntSensNet protocol

AntSensNet Property	Privacy Threat	Privacy Service Required
All FANTs are sent to one sink	A global adversary can monitor the overall traffic of the network moving towards base station	**Location Privacy** of the base station.
Data captured by the sensors is sent to the cluster head and then routed to the base station	A global adversary can trace the traffic and learn the origin or identity of the sender of the messages	**Location Privacy** of the sender. **Anonymity and unlinkability** can be achieved using fake messages, which hide the identity of a sensor.
Every cluster head holds a routing table of the real IDs of cluster heads	A local adversary can give away the true identity of the surrounding nodes. A global adversary can learn the true identities of all network nodes	**Pseudonymity** to hide the real identities of all the sensor nodes.
Every cluster head holds a routing table of the pheromone levels and the paths to the sink	Once a cluster head is captured, an adversary can learn about the network formation and characteristics of the paths	**Pseudonymity** and encryption of ants to hide the network information.
Ants captured during forward phase	A local or global adversary can learn the source node	**Pseudonymity** **Unlinkability** through the continuous update and re-encryption of the ants at each cluster head and the encryption of the ant.
Ants captured during backward phase	A local or global adversary can learn the source and sink node	**Pseudonymity** **Unlinkability** through the continuous update and re-encryption of the ants at each cluster head.
An ant is captured by an adversary	It gives away information about all cluster head in the path (ID, hop count, residual energy and other important parameters)	**Pseudonymity** **Unlinkability** through the continuous update and re-encryption of the ants at each cluster head.

B. *Privacy-Aware AntSensNet Protocol*

The proposed privacy-aware AntSensNet protocol is based on the integration of privacy-enhancing features together with the Localized Encryption and Authentication protocol (LEAP) key management protocol [10] into the AntSensNet protocol [8]. Basically, the operation of the AntSensNet protocol is divided into three main stages: pre-deployment stage, deployment stage and traffic forwarding stage. The privacy-enhancing features and the key management protocol are integrated into all three stages. Consequently, the work presented in this section is a combination of the AntSensNet protocol with privacy- enhancing features and with the chosen encryption key management protocol to deliver the privacy-aware AntSensNet protocol. A detailed review of all three stages is discussed in this section.

Stage 1: Pre-deployment Stage

The aim of this stage is to pre-load the (scalar and multimedia) sensors with their hash functions for generating the pseudonyms and the pseudorandom functions for generating the encryption keys, before their deployment, to achieve **pseudonymity and unlinkability**. In order to avoid the compromise of the whole network in case one or more nodes are captured by an adversary, the base station will deploy a pool of hash functions that will be randomly distributed among the sensor nodes. Only the base station will know which hash functions and in what order they belong to every sensor node.

The nodes are also pre-loaded with the pseudorandom functions for the operation of the LEAP-based key management protocol. In addition, the individual key, which is only known to the base station, is generated and pre-loaded into the sensor node. For a sensor node *u* with a unique ID, the individual key is generated using pseudorandom function as follows:

$$K_u^m = f_{K^m}(u) \qquad (1)$$

where $K_u^m$is the individual key of the sensor node named *u* generated using the master key K_u^mstored at the base station and only known to it and not to the rest of the sensor nodes [10]. This ensures the secure communication between the sensor nodes and the base station through the intermediate nodes (such as gateways and cluster heads). The base station computes $K_u^m$when communication is required with the node *u*, which does not impose much extra computational effort due to the efficiency of the pseudorandom functions. The same steps are followed for the pairwise key, where a master key is used at the base station to generate a special key K_i loaded into all the sensor nodes before deployment to generate pairwise keys between the sensor nodes. According to [10], the master key K_u is generated using

$$K_u = f_{K_I}(u) \quad (2)$$

Stage 2: Deployment and Initialization Stage

The aim of this stage is to prepare the sensor nodes for the operation stage through the creation of the: pseudonyms for all sensors, clusters of sensors, individual and pairwise encryption keys. Similar to Stage 1, Stage 2 (deployment and initialization stage) is used to achieve **pseudonymity and unlinkability.** Stage 2 is assumed to be *mostly* carried out during the safety period T_{saf}, which is the time elapsing before an adversary compromises a sensor node. This stage is subdivided into three sub-stages: generation of pseudonyms, generation of encryption keys, and the clustering process. The details of each sub-stage are outlined as follows.

Generation of pseudonyms

Every node is pre-loaded with a set of hash functions that are used to generate pseudonyms for the sensor nodes instead of using the real IDs of the sensor nodes. Every sensor node is expected to use a unique pseudonym for every transmission and then change the pseudonym after the node receives an acknowledgment that the transmission has successfully arrived at the base station. To update the pseudonym at the base station, a sensor node can randomly choose a hash function from the pool of functions that is already pre-loaded in the pre-deployment stage and send an encrypted message to the base station to indicate which hash function will be used in the next transmission. However, this will cause a huge communication overhead in the network. In this research work, the hash functions have been deployed in the same order as that stored at the base station to avoid sending messages to the base station from each cluster head to inform the base station which hash function is used to update the pseudonym. This way the base station will automatically update the pseudonym after sending an acknowledgment that the data has been successfully received. However, only during Stage 2, the sensor node will generate its first pseudonym (*p_id*$_0$) and keep it until the end of this stage.

Generation of encryption keys

Encryption of the data being communicated between the different network components is important to guarantee the protection of the data and prevent adversaries from having access to the data being transmitted. Encryption keys are used to encrypt the data at the source before sending it to the destination. Only by using correct key, the destination can decrypt the data and understand the content of the received message. Only two keys of the LEAP protocol have been adopted into this research work: the individual keys and the pairwise keys. Both the individual key and the master pairwise key are generated and pre-loaded into the sensor nodes during the pre-deployment stage (Stage 1). In Stage 2, the establishment of pairwise shared keys undergo three steps: neighbor discovery, pairwise key establishment and key erasure [10].

Neighbor discovery: According to [10], after deployment and during the T_{saf} time interval, a sensor node *u* tries to communicate with all its next one-hop neighbors using a HELLO broadcast message containing its pseudonym generated in Stage 2 (pseudonym generation). The sensor node *u* awaits the acknowledgment of the neighbors, which is authenticated using the master key K_v generated using $K_v = f_{K_1}(v)$.

Assuming v is the sender, u verifies the identity of node v using:

$$u \longrightarrow *: u$$
$$v \longrightarrow u: v, MAC(K_v, u|v) \qquad (3)$$

where MAC is the Message Authentication Code using the symmetric key *k*. In their work, [10] proposed a one-way key chain based authentication scheme. The authentication scheme is a mandatory requirement to avoid the case when an adversary can deplete the energy of a sensor node by inserting false packets into the network. This one-way key authentication is computationally lightweight. The basic idea of this scheme is that each node generates a one-way key chain and sends the first key of the chain (referred to as AUTH key), encrypted using the pairwise key, to each next hop neighbor. When a node is sending a message to another node, the next AUTH key in the chain is added to the message. A neighboring node verifies the messages using the most recent AUTH key received from the sending node.

Pairwise key establishment: Both sensor nodes u and v can now compute their pairwise keys K_{uv} using the equation:

$$K_{uv} = f_{K_v}(u) \qquad (4)$$

After the pairwise keys are generated, the authentication between sensor node u and v is no longer required because the messages will be authenticated using K_{uv}.

Key erasure: When T_{saf} elapses, the node u erases the K_I and the master keys of the neighbors that were exchanged during the pairwise key generation. However, only the master key of the node is kept.

Clustering process

Before the clustering phase starts, sensor nodes broadcast HELLO packets containing: node ID, clustering pheromone value and the node state. In order to suppress an adversary listening to the network from acquiring information about the data being communicated and the cluster head election, the node ID is replaced by the pseudonym. In addition, both the clustering pheromone and the node state are encrypted using the LEAP pairwise key established between the neighboring nodes earlier in this stage.

Stage 3: Traffic Forwarding

After Stage 2 is finished, all IDs and keys have been prepared, clusters and cluster heads have been set up and routing tables have been built. The aim of this stage is to deliver the data from the sensors to the base station both privately and securely, thus the title traffic forwarding.

In this stage, all three privacy mechanisms, anonymity/pseudonymity, unlinkability and location privacy, are ensured as explained in Stages 1 and 2. To ensure that an adversary monitoring the network would not relate the pseudonym with its related sensor nodes and threaten the source location privacy, the sensor nodes update their pseudonyms after receiving an AUTH for their transmission to the base station. However, this will create a problem of how to make the rest of the neighbor sensor nodes aware of the pseudonym update. One way to overcome this problem is to encrypt the pseudonym using the LEAP pairwise key and send it to all next hop neighbors in the routing table. However, this will cause a huge computational overhead (an encryption operation per neighbor) and communication overhead (sending the encrypted new pseudonym for each next hop neighbor on the list). Consequently, in this work, the new pseudonym is sent to the cluster head and the cluster head will be responsible for broadcasting the new pseudonym to the sensor nodes neighbors. This decreases the computational and communication overhead (compared to the previous solution) on the sensor nodes. The same idea is applied for the cluster heads where the base station is responsible for broadcasting the new pseudonym to the rest of the cluster heads in the network.

When a sensor node has to report data to the base station, this data should be sent to the cluster head so that it is later forwarded to the base station. However, to ensure the highest privacy and security, the data is encrypted using a LEAP individual key shared between this sensor node and the base station. This will ensure that the data is only accessed and comprehended by the base station and not the intermediate nodes. For multimedia data, the captured video and audio data is processed and either encrypted on-board (at the sensor level) or forwarded to the cluster head to be encrypted using the individual key shared between the cluster head and the base station

C. *Fake Packet Generation in critical scenarios*

In critical deployment scenarios, advanced fake packet generation technique may be required to make it harder for an adversary to threaten the privacy of the sub-system. The fake traffic of the whole sub-system can be based on tunable parameters at each level of the deployment starting from the gateway level until the base station level. The base station is responsible for setting these tunable parameters at each level by sending encrypted messages (using individual keys) to each cluster head instructing it to set a particular fake to real ratio of messages. At the level of the cluster heads right above the gateway level, if the number of gateways is less than two, fake messages must be generated from this cluster head to trick the adversary into thinking that there is more than one gateway connected and thus increase the anonymity level of this gateway. In case there is more than one gateway connected to the cluster head, a ratio can be used to determine the amount of the fake traffic to the amount of the real traffic.

IV. Performance Evaluation

To assess the overhead due to the introduction of the privacy measures into a WMSN-based healthcare sub-system, the NS2 simulation tool was used to simulate a sub-system configured according to a possible hospital scenario as depicted in figure 1.

First, only one scalar sensor was allowed to generate traffic under each gateway. The network, which was based on the ant routing protocol, was allowed to run for varying times ranging from 50 seconds to 500 seconds. Each time, each experiment was run 10 times to be able to calculate the mean, standard deviation, margin of error, upper bound and lower bound for a 95% confidence interval. Average end-to-end delay, percentage of packet delivery ratio, throughput, number of generated packets, number of received packets, number of dropped packets, percentage of packet loss ratio and average number of simulation clock ticks required to run the whole network was recorded. Next, the same experiment was repeated but the data generated from the scalar sensor was encrypted using LEAP protocol before sending it to the base station and the average number of clock ticks was recorded. Finally, the experiment based on ant routing and encrypted data was run and fake traffic was introduced. The fake traffic was generated with the same rate as the traffic generated by the scalar sensor (a rate of 40 kbps). The same approach was repeated for combinations of different numbers of scalar (as depicted by a *w* or *i* and multimedia sensors (as video sensor or audio sensor in per cluster head and the results were recorded.

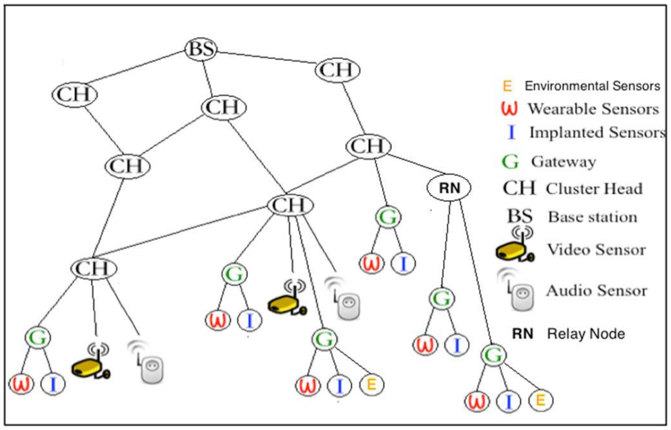

Fig. 1 A possible layout of the network components of a hospital

The data rates of the sensors deployed in these simulations depend on the type of sensors and where they are deployed (in-body deployment and/or on-body deployment) [17]. In the simulation of the experiments, the traffic generated by the gateways is consistent with the average bit rate of the in-body sensors (few Kbps to few Mbps) and on-body sensors (bps to kbps) as presented by [17]. In the simulation experiments, the average bit rate traffic generated by in-body and on-body sensors is 40Kbps.

The traffic generated by the multimedia sensors is consistent with the multimedia traffic rate in the AntSensNet routing protocol paper [8] which is Constant Bit Rate (CBR) traffic of four packets per seconds. The same rate was deployed in WMSN-based NS2 experiments in the literature such as [18], [19] and [20].

Figures 2 to 6 show the results of the experiments. In these figures, S denotes scalar sensor and M denotes multimedia sensor. It can be noticed when only security is applied, average end-to-end delay, packet delivery ratio, throughput, packet loss ratio, number of generated, received and lost packets are not altered. This is because security is applied at the level of the node and the network packets are only encrypted (no extra packets are injected into the network). However, in case of applying privacy (injecting fake traffic into the network), the number of packets are changed which affects average end-to-end delay, packet delivery ratio, throughput, packet loss ratio, number of generated, received and lost packets.

It can be concluded from the previous figures that as more sensors are introduced in the network (especially multimedia sensors) with the application of privacy and security, increased average end-to-end delay and decreased throughput are reported. In addition, it is clear from Figure 10 that the application of fake traffic or encryption to multimedia data adds a significant overhead (presented in the form of simulation clock ticks) to the overall network. The significant increase in the average number of clock ticks denotes that there is a significant increase in the total time required to enhance the privacy of multimedia data. This implies that in cases when real-time or very quick collection of healthcare data is required, multimedia data should be cut to the minimum possible, to decrease the overhead due to the processing of the multimedia data.

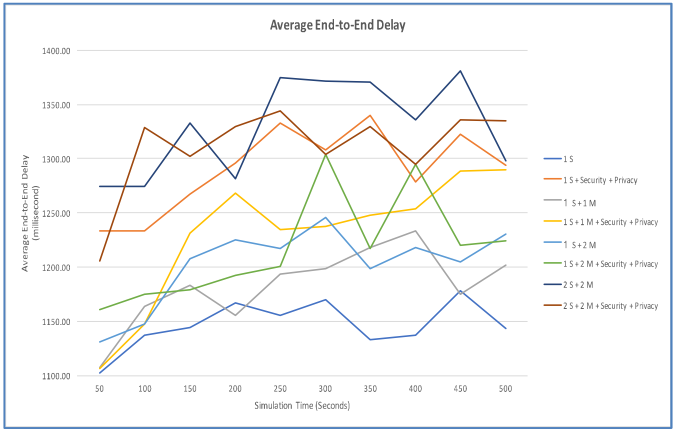

Fig. 2 Average end-to end delay for different simulation times with different types and numbers of sensors

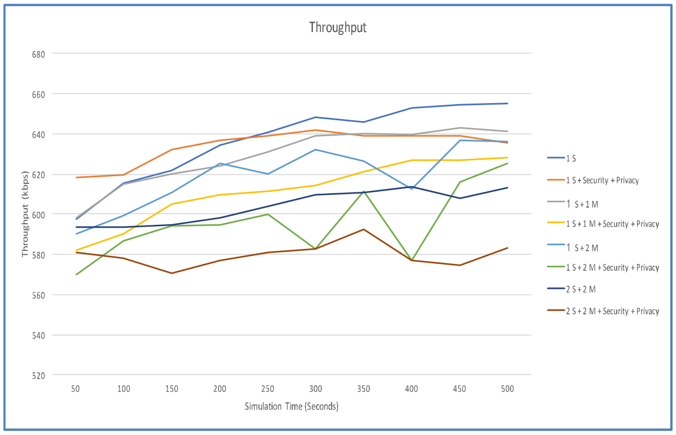

Fig. 3 Mean throughputs for different simulation times with different types and numbers of sensors

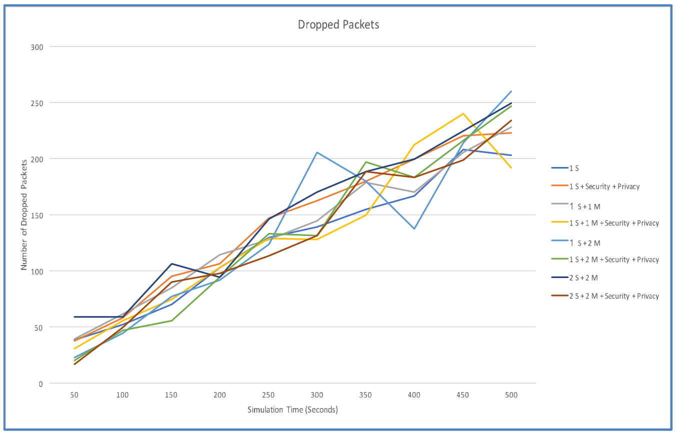

Fig. 4 Mean number of dropped packets for different simulation times with different types and numbers of sensors

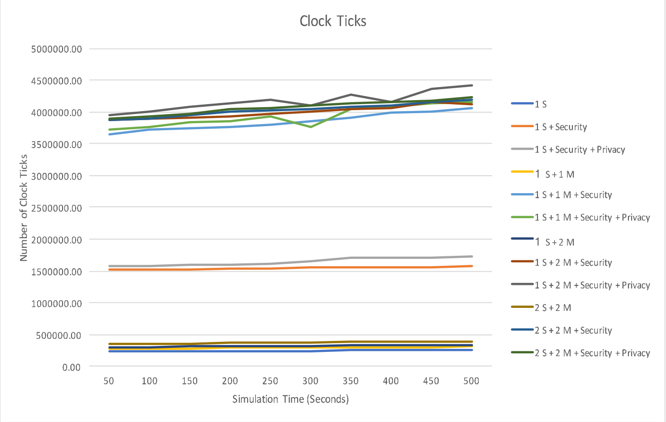

Fig. 5 Mean number of clock ticks for different simulation times with different types and numbers of sensors

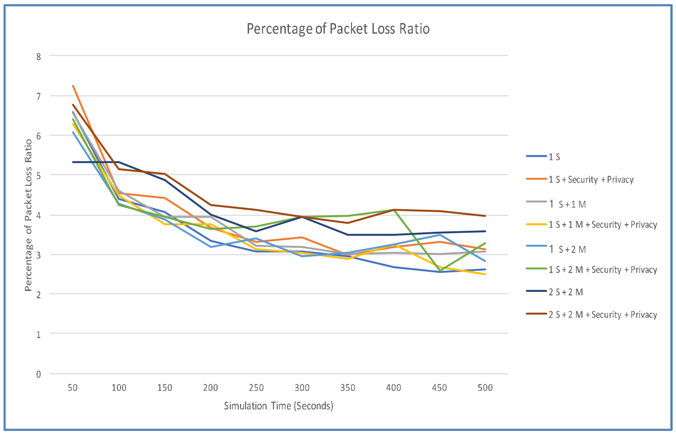

Fig. 6 Mean percentage of packet loss ratio for different simulation times with different types and numbers of sensors

V. Conclusion and Future Work

In this paper, the AntSensNet protocol was enhanced to ensure the privacy-aware transmission of data in a WMSN-based healthcare system.

The simulation showed almost seven times overhead due to the introduction of privacy measures for scalar data compared to almost fourteen times overhead due to the application of the privacy measures for multimedia data. This indicates that in critical medical cases when quick intervention of medical help is required, the communication of the multimedia data should be kept to the minimum.

Moreover, the simulation showed the overall overhead and no details of the causes of the overhead were available. Consequently, in the future, theoretical analysis is required to assess the memory, computation, and network messages overhead due to the introduction of the privacy mechanisms inside the different network nodes to be able to thoroughly present the overhead of the addition of privacy and security measures at both the network and the nodes level.

References

[1] P. Kumar and H.-J. Lee, “Security Issues in healthcare applications using wireless medical sensor networks: A survey,” *Sensors*, vol. 12, no. 1, pp. 55–91, Jan. 2011, doi: 10.3390/s120100055.

[2] US Department of Health and Human Services, “Nationwide privacy and security framework for electronic exchange of individually identifiable health information.” pp. 1–11, 2008, Accessed: Mar. 01, 2016. [Online]. Available: https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.

[3] D. Kotz, S. Avancha, and A. Baxi, “A privacy framework for mobile health and home-care systems,” in *Proceedings of the first ACM workshop on Security and privacy in medical and home-care systems*, 2009, pp. 1–12, doi: 978-1-60558-790.

[4] Y. N. Saleh, C. C. Chibelushi, A. A. Abdel-Hamid, and A.-H. Soliman, “Privacy Preservation for Wireless Sensor Networks in Healthcare: State of the Art, and Open Research Challenges,” *Prepr. arXiv 2012.12958*, 2020.

[5] G. Danezis *et al.*, “Privacy and data protection by design– from policy to engineering,” 2015.

[6] Y. N. M. Saleh, “A Study of Privacy-Preserving Mechanisms for Wireless Multimedia Sensor Networks in Healthcare,” Staffordshire University, 2018.

[7] F. L. Benmansour and N. Labraoui, “A Comprehensive Review on Swarm Intelligence-Based Routing Protocols in Wireless Multimedia Sensor Networks,” *Int. J. Wirel. Inf. Networks*, pp. 1–24, 2021.

[8] L. Cobo, A. Quintero, and S. Pierre, “Ant-based routing for wireless multimedia sensor networks using multiple QoS metrics,” *Comput. Networks*, vol. 54, no. 17, pp. 2991–3010, 2010, doi: 10.1016/j.comnet.2010.05.014.

[9] M. Saleem, G. Di Caro, and M. Farooq, “Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions,” *Inf. Sci. (Ny).*, vol. 181, no. 20, pp. 4597–4624, 2011.

[10] S. Zhu, S. Setia, and S. Jajodia, “{LEAP}: Efficient security mechanisms for large-scale distributed sensor networks,” *ACM Trans. Sens. Networks*, vol. 2, no. 4, pp. 500–528, 2006.

[11] A. Rahman, R. Ghasemaghaeil, A. El Saddikl, and W. Gueaieb, “M-IAR : Biologically inspired routing protocol for wireless multimedia sensor networks,” in *Proceedings of the IEEE International Instrumentation and Measurement Technology Conference (IMTC)*, 2008, pp. 1823–1827, doi: 10.1109/IMTC.2008.4547341.

[12] Y. Sun, H. Ma, L. Liu, and Y. Zheng, “ASAR: An ant-based service-aware routing algorithm for multimedia sensor networks,” *Front. Electr. Electron. Eng. China*, vol. 3, no. 1, pp. 25–33, 2008, doi: 10.1007/s11460-008-0013-7.

[13] J. Bi, Z. Li, and R. Wang, “An ant colony optimization-based load balancing routing algorithm for wireless multimedia sensor networks,” in *Proceeding of 12th IEEE International Conference on Communication Technology (ICCT)*, 2010, pp. 584–587.

[14] X. Yu, J. Luo, and J. Huang, “An ant colony optimization- based QoS routing algorithm for wireless multimedia sensor networks,” in *Proceedings of the 3rd International Conference on Communication Software and Networks (ICCSN)*, 2011, pp. 37–41.

[15] I. Bennis, O. Zytoune, and D. Aboutajdine, “Enhanced AntNet protocol for wireless multimedia sensor networks,” in *International Conference on Networked Systems*, 2013, pp. 316–320.

[16] K. Malik, M. Dave, S. K. Dhurandher, I. Woungang, and L. Barolli, “An ant-based QoS-aware routing protocol for heterogeneous wireless sensor networks,” *Soft Comput.*, vol. 21, no. 21, pp. 6225–6236, 2016.

[17] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, “Wireless body area networks: A survey,” *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1658–1686, 2014.

[18] M. Akhlaq and T. R. Sheltami, “Performance comparison of video compression and streaming over wireless ad hoc and sensor networks using MPEG-4 and H. 264.,” in *International Conference on Networked Digital Technologies*, 2012, pp. 368–377.

[19] D. S. B. Adhyapak and A. P. Laturkar, “Swarm Based Cross Layer Optimization Protocol for WMSN,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 10, no. 1, pp. 302–308, 2018.

[20] L. Zhang, D. Shen, X. Shan, and V. O. K. Li, “An ant-based multicasting protocol in mobile ad-hoc network,” *Int. J. Comput. Intell. Appl.*, vol. 5, no. 2, pp. 185–199, 2005.