Computer Modeling in Engineering & Sciences

Tech Science Press

Doi:10.32604/cmes.2025.072603

ARTICLE

Information Diffusion Models and Fuzzing Algorithms for a Privacy-Aware Data Transmission Scheduling in 6G Heterogeneous *ad hoc* Networks

Borja Bordel Sánchez*, Ramón Alcarria and Tomás Robles

IT Department, Universidad Politécnica de Madrid, Alan Turing Street, Madrid, 28031, Spain

*Corresponding Author: Borja Bordel Sánchez. Email: borja.bordel@upm.es

Received: 30 August 2025; Accepted: 29 December 2025; Published: 26 February 2026

ABSTRACT: In this paper, we propose a new privacy-aware transmission scheduling algorithm for 6G *ad hoc* networks. This system enables end nodes to select the optimum time and scheme to transmit private data safely. In 6G dynamic heterogeneous infrastructures, unstable links and non-uniform hardware capabilities create critical issues regarding security and privacy. Traditional protocols are often too computationally heavy to allow 6G services to achieve their expected Quality-of-Service (QoS). As the transport network is built of *ad hoc* nodes, there is no guarantee about their trustworthiness or behavior, and transversal functionalities are delegated to the extreme nodes. However, while security can be guaranteed in extreme-to-extreme solutions, privacy cannot, as all intermediate nodes still have to handle the data packets they are transporting. Besides, traditional schemes for private anonymous *ad hoc* communications are vulnerable against modern intelligent attacks based on learning models. The proposed scheme fulfills this gap. Findings show the probability of a successful intelligent attack reduces by up to 65% compared to *ad hoc* networks with no privacy protection strategy when used the proposed technology. While congestion probability can remain below 0.001%, as required in 6G services.

KEYWORDS: 6G networks; *ad hoc* networks; privacy; scheduling algorithms; diffusion models; fuzzing algorithms

1 Introduction

6G mobile technologies are envisioned to enable a large new collection of innovative services with an enhanced extreme Quality-of-Service (QoS). These range from remote control of critical infrastructure (supported by extreme Ultra-Reliable Low Latency Communications or eURLLC with congestion probabilities below 0.001%) to immersive experiences based on enhanced Mobile Broadband Communications (eMBBC). But, among all these emerging services, those that require an overlay infrastructure are the most challenging.

Paradigms such as Industry 5.0 and Vehicular *Ad-hoc* Networks (VANET) rely on complex, heterogeneous infrastructures supported by underlying 6G links. In these new paradigms, dynamic adaptation and massive customization are key elements. Thus, 6G-powered mobile nodes, with an extremely varying catalog of hardware capabilities, are wirelessly interconnected in an ephemeral manner; and the architecture of the infrastructure can evolve and dynamically change according to the needs and the required customization. However, this approach introduces new open problems. On the one hand, a changing network topology must be managed with specific protocols and algorithms (such as choreographed self-configuration schemes) which may introduce additional overheads and redundancies. So, the extreme QoS expected from 6G deployments and communications might not be achieved at the final application level. On the other hand, transversal issues such as privacy, security, or reliability are very hard to guaranty when trustworthy paths

at transport level cannot be analyzed and preserved in the long term. For some of these issues, extreme-to-extreme solutions are a valid response. For example, security schemes for abnormal data filtering can be implemented through Artificial Intelligence models in extreme nodes, and additional authentication planes can be included in base stations [1]. But this approach is not valid for privacy preservation.

In fact, in 6G heterogeneous *ad hoc* networks, intermediate nodes are not trustworthy, but all of them must handle the data packets for which they provide routing functionalities. This exposure allows attackers to capture private information in a transparent way. Malicious nodes can enter *ad hoc* networks long enough to deploy intelligent attacks, where learning algorithms extract patterns from even small packets. Some authors have proposed privacy preserving solutions for 6G *ad hoc* networks, such as anonymous message authentication and key exchange mechanisms [2], Blockchain-enabled data sharing [3], Blockchain-enabled trust computation [4], semantic-aware communications [5], or traffic densers against black hole attacks [6]. But they are computationally costly, with processing times between 200 and 500 ms [7] and almost 30% of CPU overload [8], and they greatly penalize the final Quality-of-Service at the overlay-network level. Actually, 6G eURLLC standards cannot be met when those existing privacy-preserving solutions are implemented. Therefore, new privacy-preserving technologies for 6G heterogeneous *ad hoc* networks are required; so, the expected 6G QoS is still feasible while modern intelligent attackers are mitigated.

Specifically, as current approaches require large processing and computational delays, the following research gaps are still uncovered:

- Privacy-preserving communication scheduling algorithms for 6G *ad hoc* networks, compatible with extreme QoS
- Protection schemes against illegitimate data capture and learning adapted to dynamic 6G *ad hoc* networks with ultra-reliable low-latency and lightweight computational cost

To fulfill these gaps, in this paper, we propose a privacy-aware data transmission scheduling algorithm which allows 6G *ad hoc* nodes to find the optimum balance between Quality-of-Service and privacy protection. So, 6G requirements are compatible with protection against intelligent attacks and illegitimate data capture. The algorithm is executed at the network level, so extreme nodes can calculate the optimum time slot and transmission frame for private data. The proposed algorithm uses fuzzing algorithms to generate false data packets, whose purpose is to confuse potential intelligent attackers operating within the *ad hoc* network. To analyze the level of learning and/or confusion of intelligent attackers, a probabilistic dynamical system is used. In this system, information diffusion models and network statistics are employed to estimate the amount of private information captured. Although this approach has no impact on network latency, false data packets can penalize effective network bandwidth. To avoid congestion situation, the teletraffic theory is employed to propose a combined model where queue models and network statistics are used to understand the behavior, lifecycle, and performance of *ad hoc* nodes when false data are injected. So, the final probabilistic model represents the balance between privacy and performance. Particle Swarm Optimization techniques can be used to find the optimum balance and transmission schedule.

The remainder of the manuscript is organized as follows. Section 2 introduces the state of the art in privacy-preserving solutions for 6G-enabled *ad hoc* networks. Section 3 presents the proposed contribution, the scheduling algorithm and the teletraffic model and the probabilistic information diffusion model. Section 4 describes the experimental methodology and experiments. Section 5 discusses the experimental results and Section 6 concludes the paper.

2 State of the Art

In general terms, privacy-preserving technologies in 6G networks can be classified into two big groups: intelligent mechanisms [9] and Blockchain-enabled solutions [10]. Next subsections discuss the limitations and research opportunities related to both alternatives. Section 2.1 analyzes Blockchain-enabled solutions, while Section 2.2 describes the previous intelligent and computational approaches.

2.1 Blockchain-Enabled Solutions for Privacy Preservation in 6G

Intelligent mechanisms include a federated learning scheme to preserve differential privacy [11] or semantic analyzers to remove sensible messages [11]. Blockchain-enabled solutions deploy overlay authentication layers [1], store transparent and immutable records of nodes' reputation [12], and apply information theory techniques [13], information packet comparisons [4] or network virtual representations (digital twin) [14] to identify those nodes that are potentially collecting private data, in order to remove them from the infrastructure [15]. However, all these proposals require a long-term stable network configuration, so permanent and unique identifiers can be distributed, the intelligent algorithms can converge, and/or the virtual or reputational representations are stable enough to run the decision-making algorithms. But, in *ad hoc* networks, connections are ephemeral or, even, opportunistic. Also, the general network architecture is constantly evolving, preventing any analyzing algorithm or framework from converging or staying stable long-term. Then, different approaches are needed to preserve privacy.

In fact, some authors have investigated how Blockchain-enabled techniques could be adapted to *ad hoc* networks [16]. Certificateless authentications [17] or new protocols such as Cooperative Sensing Smart Contract [18] are described. Most of these schemes are designed to be lightweight (low computational latency), so the response time may be below the evolution rhythm in the *ad hoc* infrastructure. Delays of around 100 ms have been reported [18], but these values are above the expected performance in 6G *ad hoc* networks. Some other authors describe alternative network architectures, in which Blockchain networks act as orchestrators [19]. But this scheme is only valid for some specific applications and for very homogeneous networks [20], while future infrastructures are expected to be very heterogeneous.

Table 1 summarizes the relevant state of the art.

The technology proposed in this paper is not tailored for any specific application and can be used in any type of *ad hoc* network. Its main focus (thanks to numerical models and optimization algorithms) is to find the optimum balance between privacy-preservation and network performance so that 6G extreme QoS is met.

2.2 Intelligent and Computational Mechanisms for Privacy Preservation in 6G

Intelligent techniques for *ad hoc* networks may be found as well. Most of them focused on intrusion detection. From deep learning algorithms to detect illegitimate data capturers [21], to predictive techniques for the detection of abnormal private data handlers [22] and federated strategies to detect misbehaviors [23]. However, although the authors claim these techniques are fitted to match the requirements of *ad hoc* networks, convergence times in the range of thousands of seconds are still reported [23]. For many *ad hoc* network application scenarios (such as vehicular networks), this is not acceptable [24].

Lightweight intelligent schemes for privacy preservation in *ad hoc* networks have been investigated in the last years. Some intelligent schemes have proven to be successful in optimizing QoS in communications [25], but privacy considerations are usually not integrated into these models. Some centralized security threat detection models are compatible with differential privacy by design [26], however, no particular instrument against illegitimate learning is integrated. On some occasions, anonymization and privacy are

implemented; but they are commonly tailored for some particular applications or hardware capabilities (e.g., cameras) [27].

On the other hand, in the context of 6G Internet-of-Things (IoT), industrial IoT, or edge computing, authentication schemes are commonly proposed for privacy preservation [28]. Specifically, low-latency authentication algorithms [29] are studied, including strategies defined in other contexts such as certificateless authentication [30], two-factor [31], or three-factor authentication [32]. However, despite reported efforts, computational delays above 500 ms are still required [7]. And this delay is far above the expected latency in 6G networks (100 microseconds [33]). Some other authors propose traffic filters and classifiers to "sanitize" data and ensure that private information is not handled [34]. Although preliminary evaluations with offline datasets show good precision, their performance in real-time data exchange processes (especially in terms of computational delays) is still unknown.

Finally, some authors propose alternatives taking advantage of the mobility of the nodes. Algorithms to calculate privacy-preserving trajectories for data dissemination [35] have been reported, as well as technologies to group the transport nodes that are allowed to handle private data [36]. These schemes do not require a long-term network structure, and computational delays are acceptable. However, they assume that *ad hoc* nodes can freely choose the path for their data packets, which is not true for most scenarios (especially in opportunistic networks).

In this paper we propose a privacy-aware data transmission scheduler, where extreme nodes can calculate the optimum communication scheme to preserve their private data against intelligent attackers. We use probabilistic models, which can be employed by extreme nodes with no global knowledge about the *ad hoc* network. Besides, since we use probabilistic models, the network architecture may change dynamically without impact. Data packets and transmission protocols are not extended, and no additional overhead is introduced, so eURLLC is preserved by fulfilling the existing research gaps in the state of the art.

Table 1: Summary of the state of the art

References	Description	Limitations
[4,12,13]	Immutable records describing communications and nodes' behavior	Require long-term stable network configurations
[14]	Virtual representations of *ad hoc* networks	Require long-term stable network configurations
[17,18]	Authentication and certification Blockchain-enabled protocols	Heavy computational delays not compatible with 6G QoS
[19,20]	Central orchestrators	Tailored and compatible only with some specific applications
[21–23]	Intelligent intrusion detection mechanism	Heavy computational delays not compatible with 6G QoS
[25–27]	Lightweight intelligent solutions	No particular protection against illegitimate learning is provided
[28–32]	Data and network sanitation	No evidence of performance in real-time scenarios
[35,36]	Privacy-aware routing protocols	Require long-term stable network configurations and large calculation delays

3 A Privacy-Aware Data Transmission Scheduling Algorithm

This section introduces the proposed framework to find the optimum data transmission schedule in terms of network performance (Quality-of-Service) and privacy preservation. A Particle Swarm Optimization strategy analyzes all possible schedules, their impact on network congestion and latency using teletraffic theory, and the potential learning achieved by intelligent attackers through probabilistic and information diffusion models. Section 3.1 introduces the general data transmission framework, the network and traffic models, and the fuzzing algorithm employed to propagate false information among the nodes. Section 3.2 introduces the probabilistic models used to describe information propagation in *ad hoc* networks and the potential learning of intelligent attackers. Finally, Section 3.3 combines both visions and proposes the global data transmission scheduling scheme. Fig. 1 shows a general description of the proposed technology.

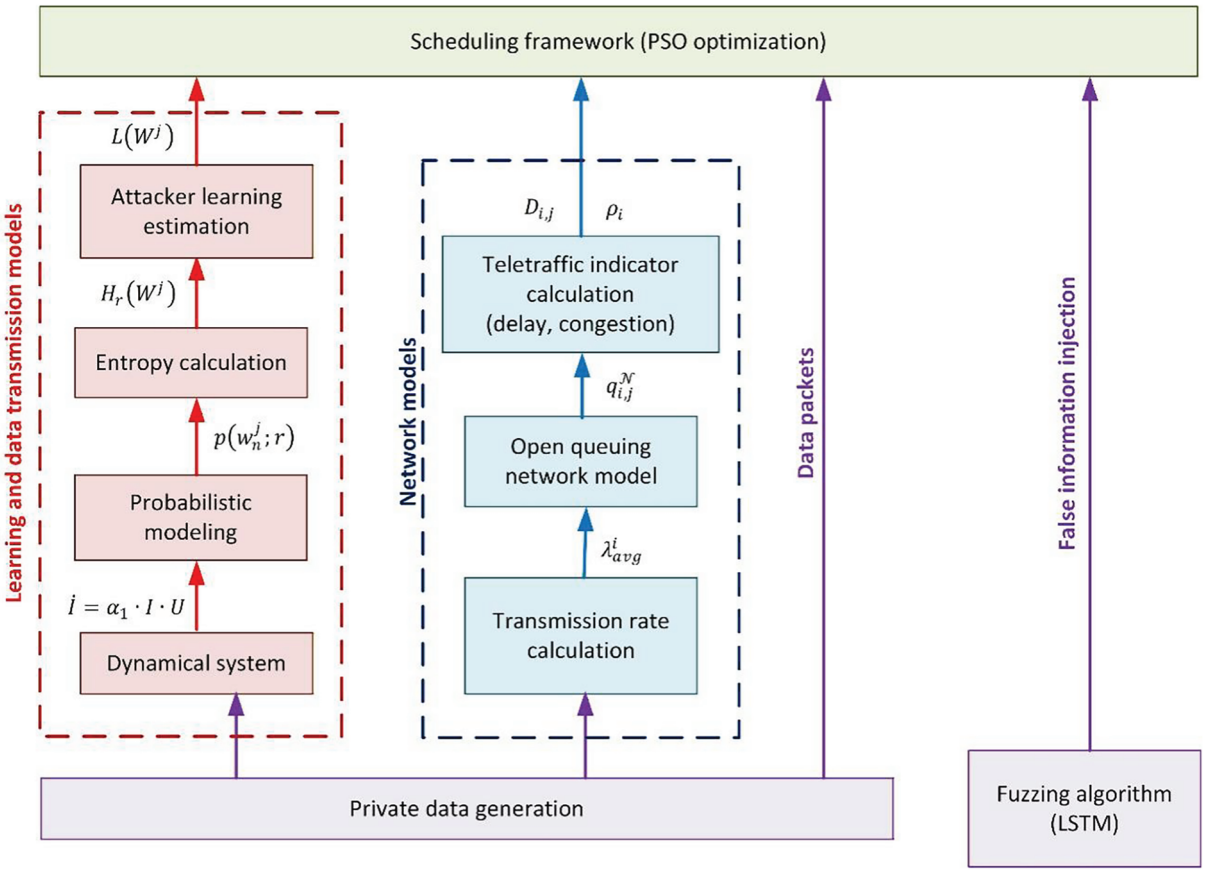

Figure 1: General overview of the proposed technology

3.1 Network Models and Fuzzing Algorithms

An *ad hoc* network can be described as a graph $\mathcal{N}$, where the M_a vertex a_i represent the network nodes, and the edges $e_{i,j}$ represent opportunistic and ephemeral wireless links between nodes a_i and a_j. As communication links are ephemeral, the network graph evolves with time (1).

$$\begin{aligned} &\mathcal{N}(t) = (A, E(t)) \\ &A = \{a_i \, i = 1, \ldots, M_a\} \\ &E(t) = \{e_{i,j}(t) \quad i, j = 1, \ldots, M_a\} \end{aligned} \tag{1}$$

Graph $\mathcal{N}$ is edge-labeled, where each edge $e_{i,j}$ is labeled with a probability $p_{i,j}^{\mathcal{N}}$ representing the probability of wireless link $e_{i,j}$ to be actually stablished at a given time instant. Non-established links at a given time instant t_0 are noted as $e_{i,j}(t_0) = \varnothing$.

Each node a_i divides time in frames with a duration of T_{frame} seconds (see Fig. 2). Each time frame, besides, can be broken down in K time slots T_k with a duration of T_{slot} seconds (2). So, in each time slot T_k only one data unit x_k^i can be transmitted. Each data unit can be a byte, packet, message... depending on the application. Time slots T_k can be dummy too, when no data is transmitted. For those dummy time slots T_k, we are assuming $x_k^i = \varnothing$.

$$T_{frame} = K \cdot T_{slot} \tag{2}$$

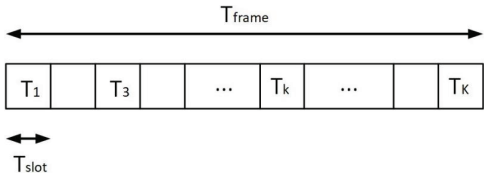

Figure 2: Structure of any time frame

Then, the instant transmission rate λ_r^i can be easily obtained (3), where r is the discrete time instant (4). And the average transmission rate λ_{avg}^i can be calculated as well (5), where R is the maximum number of past time frames to be considered (so past events do not affect future behaviors excessively). On the other hand, 6G wireless links are expected to provide a certain bitrate B_{6G} by configuration or standard, which can be easily expressed in terms of the selected data unit (bytes, packets, etc.). Then, the average service time μ_{6G} can be obtained (6) for all links, if the propagation delays are considered negligible (as distances among nodes are typically short in *ad hoc* networks).

$$\lambda_r^i = \frac{x_{total}}{T_{frame}}$$

$$x_{total} = \sum_{\substack{k=1 \\ \forall k \,:\, x_k^i \neq \varnothing}}^{K} 1 \tag{3}$$

$$t = r \cdot T_{frame} \tag{4}$$

$$\lambda_{avg}^i = \frac{1}{R} \sum_{r=0}^{R-1} \lambda_{-r}^i \tag{5}$$

$$\mu_{6G} = \frac{1}{B_{6G}} \tag{6}$$

With these parameters, any graph $\mathcal{N}$ can be understood as an open queuing network (see Fig. 3), where routing probabilities $q_{i,j}^{\mathcal{N}}$ are dependent on probabilities $p_{i,j}^{\mathcal{N}}$ (7). We are assuming an opportunistic routing strategy [37]. Specifically, probabilities $q_{i,j}^{\mathcal{N}}$ are calculated to ensure graph $\mathcal{N}$ is a Jackson's queueing

network (arrivals follow Poisson distribution and flows conserve), so further results about network latency and congestion can be extracted.

$$q_{i,j}^{\mathcal{N}} = \frac{p_{i,j}^{\mathcal{N}}}{\sum_{j=1}^{M_a} p_{i,j}^{\mathcal{N}}} \tag{7}$$

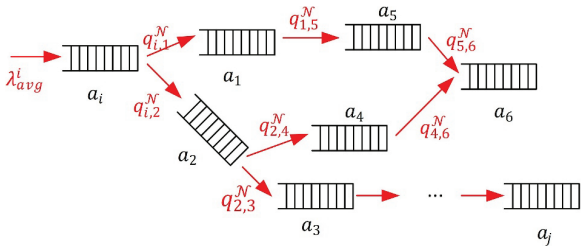

Figure 3: *Ad hoc* network as an open queuing network

Probabilities $p_{i,j}^{\mathcal{N}}$ can be estimated through the Laplace definition for probability and considering the existence of every edge (communication link) $e_{i,j}$ is evaluated once in each time frame (8).

$$p_{i,j}^{\mathcal{N}} = \frac{p_{i,j}^{sum}}{R}$$
$$p_{i,j}^{sum} = \sum_{\substack{r=0 \\ \forall e_{i,j}(-r \cdot T_{frame}) \neq \varnothing}}^{R-1} 1 \tag{8}$$

Under these conditions, the punctual network congestion ρ_i at node a_i (9) and the network delay $D_{i,j}$ for a data unit transmitted by node a_i to node a_j (10) can be extracted by solving two systems of M_a linear equations. As nodes a_i are independent and have no information about other nodes a_j within the *ad hoc* network, delay $D_{i,j}$ and congestion ρ_i are calculated using the Montecarlo algorithm and considering λ_{avg}^{i} is always positive and has an upper bound (11).

$$\rho_i = \frac{\lambda_{avg}^{i} + \sum_{j=1}^{M_a} q_{i,j}^{\mathcal{N}} \cdot \lambda_n^j}{\mu_{6G}}$$
$$\left\{ \lambda_n^j = \lambda_{avg}^{j} + \sum_{i=1}^{M_a} q_{j,i}^{\mathcal{N}} \cdot \lambda_n^i \quad j = 1, \ldots, M_a \right\} \tag{9}$$
$$\left\{ D_{i,j} = D_i + \sum_{m=1}^{M_a} q_{i,m}^{\mathcal{N}} \cdot D_{m,j} \quad i = 1, \ldots, M_a \right\}$$

$$D_i = \frac{1}{\mu_{6G} - \lambda_n^i} \tag{10}$$

$$0 \leq \lambda_{avg}^{i} \leq \frac{K}{T_{frame}} \tag{11}$$

Two restrictions on any potential data transmission scheme can be extracted now:

- Delay $D_{i,j}$ must be below the expected latency for 6G services D_{6G}.

- The punctual network congestion ρ_i at every node a_i must be always below a given threshold $\rho_{th} < 1$.

To meet those restrictions, the number of dummy time slots T_k in each time frame must find an equilibrium. Typically, *ad hoc* networks require a low bitrate and private data to be transmitted are sparse. But synthetic false information must be injected to ensure intelligent attackers are confused and do not consolidate any knowledge about nodes a_i (see Section 3.2).

Although many different strategies to create false information have been reported (recently, for example, algorithms based on generative Artificial Intelligence are very common [38]), *ad hoc* networks require a solution computationally lightweight enough to be executed by nodes. We propose a fuzzing algorithm based on Long Short-Term Memory (LSTM), which still needs a training phase but does not require complex models to generate large populations of different data. Although simpler strategies could be used, current learning models are powerful enough to ignore entries with low entropy (information). So, injected fuzzed packets must replicate the information level of real data as precisely as possible.

LSTM has the ability of removing, keeping, and/or updating some specific parts of a given data input, but preserving at long-term the desired pieces of information using the memory unit. Fig. 4 shows the proposed fuzzing algorithm.

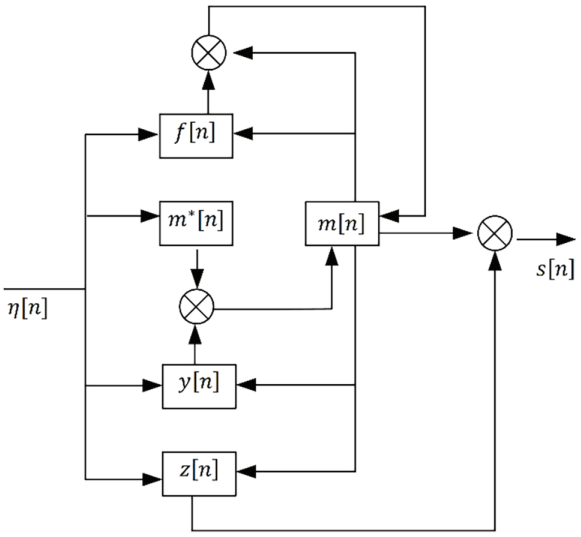

Figure 4: Block diagram for the LTSM-based fuzzing algorithm

The fuzzing algorithm includes tree basic blocks: the input block described by function $y[r \cdot K + k]$ (12), the forgot block described by function $f[r \cdot K + k]$ (13), and the output block described by function $z[r \cdot K + k]$ (14). Two additional intermediate functions are needed as well: the memory function $m[r \cdot K + k]$ (15) and the state function $s[r \cdot K + k]$ (16). The state function is also the general output from the LSTM. Where $\xi_{\{1,\ldots,11\}}$ are hyperparameters to be determined through a training process, r indicates the time frame and k the time slot within the time frame. And $\eta[n]$ is the original private data to be fuzzed.

$$y[r \cdot K + k] = y[n] = sig(\xi_1 \cdot \eta[n] + \xi_2 \cdot m[n-1] + \xi_3)$$
$$sig(w) = \frac{1}{1 + e^{-w}} \tag{12}$$
$$f[r \cdot K + k] = f[n] = sig(\xi_4 \cdot \eta[n] + \xi_5 \cdot m[n-1] + \xi_6) \tag{13}$$
$$z[r \cdot K + k] = z[n] = sig(\xi_7 \cdot \eta[n] + \xi_8 \cdot m[n-1] + \xi_9) \tag{14}$$

$$m\left[r \cdot K + k\right] = m\left[n\right] = f\left[n\right] \bigotimes m\left[n-1\right] + y\left[n\right] \bigotimes m^{*}\left[n\right]$$
$$m^{*}\left[n\right] = tanh\left(\xi_{10} \cdot \eta\left[n\right] + \xi_{11}\right) \quad (15)$$
$$s\left[r \cdot K + k\right] = s\left[n\right] = z\left[n\right] \bigotimes m\left[n\right] \quad (16)$$

In this work, hyperparameters are calculated using a backpropagation through time (BPTT) technique, and a dataset including private data units and examples of fuzzed data units where the sensible information has been removed and/or randomized. BPTT is selected as its complexity and scalability is linear, ensuring the training delays do not grow uncontrollably when large *ad hoc* networks with dynamic heterogenous behaviors are modeled. Besides, BPTT can be trained with relatively small datasets (some thousands of entries) and get high precision models.

The final question is to determine which information units x_k^i are original private data $\eta[n]$ and which ones are fuzzed false information $s\left[n\right]$. The objective is to reduce as much as possible the learning of potential intelligent attackers.

3.2 Probabilistic Models for Data Transmission and Learning Level in Intelligent Attacks

While an elevated number of dummy time slots T_k facilitates to meet the expected QoS in 6G-enabled networks, a flooding of false fuzzed data units would ensure no intelligent attacker is able to learn from private data. In order to find the optimum equilibrium, we propose a model to estimate the learning level of attackers, depending on the transmitted data (private or fuzzed).

For an intelligent attacker running illegitimate data capture at node a_j, the learning level $L\left(W^j\right)$ follows an exponential law (17) depending on the entropy $H_r\left(W^j\right)$ of the set of received data units W^j. Where L_{speed} is a configuration parameter which controls de evolution speed of the learning level. The real set W^j is unknown by source node a_i and it must be estimated from the set of transmitted data units X^i.

$$L\left(W^j\right) = 1 - e^{-\frac{H_r\left(W^j\right)}{L_{speed}}}$$
$$L_{speed} > 0 \quad (17)$$

First, entropy $H_r\left(W^j\right)$ is calculated as a function (18) of the instantaneous entropy $H_r\left(W^j; r\right)$ for each time frame (19). Function β may take different forms, such as the statistical mean β_{mean} (20), the maximum value β_{min} (21) or the maximum value β_{max} (22). The selected function depends on the scenario we are assuming (worst scenario, best scenario or average scenario). Typically, β_{mean} will be employed.

$$H_r\left(W^j\right) = \beta\left(\left\{H_r\left(W^j; -r\right) r = 0, \ldots, R-1\right\}\right) \quad (18)$$
$$H_r\left(W^j; r\right) = -\sum_{\forall w_n^j} p\left(w_n^j; r\right) \cdot log\left(p\left(w_n^j; r\right)\right) \quad (19)$$
$$H_r\left(W^j\right) = \beta_{mean}\left(H_r\left(W^j; r\right)\right) = \frac{1}{R}\sum_{R=0}^{R-1} H_r\left(W^j; -r\right) \quad (20)$$
$$H_r\left(W^j\right) = \beta_{min}\left(H_r\left(W^j; r\right)\right) = \underset{r \in [0, r-1]}{\operatorname{argmin}} \left\{H_r\left(W^j; -r\right)\right\} \quad (21)$$
$$H_r\left(W^j\right) = \beta_{max}\left(H_r\left(W^j; r\right)\right) = \underset{r \in [0, r-1]}{\operatorname{argmax}} \left\{H_r\left(W^j; -r\right)\right\} \quad (22)$$

Second, probability $p\left(w_n^j;r\right)$ of the n-th data unit w_n^j in set W^j in the r-th time frame can be estimated by combining two different probabilities (23). On the one hand, probability $p\left(x_n^i;r\right)$ represents the probability of the n-th data unit x_n^i in set X^i in the r-th time frame, understood as Laplace's definition (24). Where $card\left\{\cdot\right\}$ is the cardinality operator. On the other hand, probability $p\left(x_n^i \to w_n^j\right)$represents the probability of transmitted data unit x_n^i to be received by node a_j and be integrated as received data unit w_n^j.

$$p\left(w_n^j;r\right) = p\left(x_n^i;r\right)\cdot p\left(x_n^i \to w_n^j;r\right) \tag{23}$$

$$p\left(x_n^i;r\right) = \frac{card\left\{\widetilde{X_n^i}\left[r\right]\right\}}{card\left\{X^i\left[r\right]\right\}}$$

$$\widetilde{X_n^i}\left[r\right] = \left\{x_c^i \in X^i\left[r\right] \vdots x_c^i = x_n^i\right\} \tag{24}$$

Probability $p\left(x_n^i \to w_n^j\right)$ is, moreover, composed of two different variables (25). Probability $p_{x_n^i}^{re}$ represents the relevance of data unit x_n^i. It evolves and reduces exponentially with discrete time r, where r_0 indicates the discrete time instant when the data was transmitted (26) and v is the decreasing ratio (a configuration parameter). As data relevance reduces, it is less probable that any potential attacker will extract any knowledge from it. Finally, probability $p_{x_n^i}^{tx}$ is the probability of data unit x_n^i to successfully travel from node a_i to node a_j. To estimate probability $p_{x_n^i}^{tx}$ we are using an information diffusion model.

$$p\left(x_n^i \to w_n^j;r\right) = p_{x_n^i}^{re}\cdot p_{x_n^i}^{tx} \tag{25}$$

$$p_{x_n^i}^{re}\left[r\right] = \left(\frac{1}{v}\right)^{|r-r_0|}$$

$$v > 1 \tag{26}$$

Probability $p_{x_n^i}^{tx}$ will increase in a polynomial form with the number of nodes a_j which can potentially receive the data unit x_n^i (27), known as "informed" nodes. Where h is a configuration parameter controlling the growing speed. This number of "informed" nodes $I[r]$ is estimated through a dynamical system (28). Additionally, any node may be on other three states. Nodes a_i may also be "uninformed", and potentially open to receive data unit x_n^i. Variable $U[r]$ represents the number of nodes in this state. Besides, nodes a_i may be "cancelled", if they receive a later or contradictory data unit, so x_n^i data unit is not processed but it is routed. Variable $C[r]$ represents the number of nodes in this state. Finally, nodes a_i may be in the status "unavailable" if they cannot accept the data unit x_n^i so it gets totally discarded. Variable $V[r]$ represents the number of nodes in this state. Parameters $\alpha_{\{1,\ldots,3\}}$ are variables representing the speed at which nodes may change their status.

$$p_{x_n^i}^{tx}[r] = \left(\frac{I}{M_a}\right)^h \tag{27}$$

$$\dot{U} = -\alpha_1\cdot I\cdot U - \alpha_2\cdot C\cdot U + \alpha_3\cdot V$$

$$\dot{I} = \alpha_1\cdot I\cdot U$$

$$\dot{C} = \alpha_2\cdot C\cdot U$$

$$\dot{V} = -\alpha_3\cdot V \tag{28}$$

This dynamical system can be numerically solved, using, for example, Runge-Kutta methods, and variable $I[r]$ is then easily obtained.

Finally, the parameters $\alpha_{\{1,\ldots,3\}}$ are obtained from the characteristics and architecture of the *ad hoc* network under consideration. Parameter α_1 represents the speed at which data units propagate in the *ad hoc* network. So, it can be obtained basically by analyzing the network connectivity. In particular, the mean number of interconnections among nodes is employed (29). Where b_3 is a configuration parameter to be freely selected.

$$\alpha_1 = \frac{b_3}{M_a} \sum_{k=1}^{M_a} \left(\frac{1}{\binom{M_a - 1}{k}} \sum_{\substack{\forall c_1, \ldots, c_k \in [1, M_a] \\ c_1, \ldots, c_k \neq k}} p^{\mathcal{N}}_{k,c_1} \cdot \ldots \cdot p^{\mathcal{N}}_{k,c_k} \right) \tag{29}$$

Parameter α_2 describes the network consistency, so data units are received as they were transmitted. The volatility of ephemeral network links among nodes are used to calculate this parameter (30). We are using the Tsallis' entropy to measure this volatility, as *ad hoc* networks are not in long-term equilibrium and this indicator facilitates measuring the system's diversity under these conditions. Where $b_{\{1,2\}}$ are configuration parameters to be freely selected.

$$\alpha_2 = \frac{b_2}{b_1 - 1} \left(1 - \sum_{\forall i,j} \left(p^{\mathcal{N}}_{i,j} \right)^{b_1} \right)$$
$$b_1 \geq 0 \; b_1 \neq 1 \tag{30}$$

Finally, parameter α_3 describes how fast unavailable nodes may recover and receive new information once again. Unavailability may be caused by congestion or ephemeral connections. Anyway, network recovery is directly related to the mean number of active communication links. Algorithm 1 describes the proposed calculation method.

Then, one additional restriction for any data transmission schedule can be extracted, ensuring privacy preservation: learning level $L\left(W^j\right)$ cannot be above the maximum admissible threshold L_{th} (31). The optimum transmission schedule is the one reducing as much as possible the learning level of intelligent attackers, while ensuring 6G QoS is still achieved. An optimization algorithm is used to find such scheme (see Section 3.3).

$$L\left(W^j\right) < L_{th} \tag{31}$$

Algorithm 1: Calculation procedure for $\boldsymbol{\alpha_1}$ parameter.

Input Probabilities $p^{\mathcal{N}}_{i,j} \forall\, i, j \in (1, M_a)$ and parameter K_{max}
Output Parameter α_1
Create $e_{gobal} = 0$
for $i \in [1, M_a]$ **do**
for $j \in [1, M_a]$ **and** $j > i$ **do**
for $k \in [1, K_{max}]$ **do**
Calculate the set $Comb$ of combinations of k elements without repetition from set $[1, M_a] - \{i, j\}$

(Continued)

Algorithm 1 (continued)

for each $c \in Comb$ **do**
$p = p^{\mathcal{N}}_{i,c(1)}$
for $n \in [2, k]$ **do**
$p = p \cdot p^{\mathcal{N}}_{c(n-1),c(n)}$
end for
$p = p \cdot p^{\mathcal{N}}_{c(n),j}$
$e_{global} = p \cdot (k+1) + e_{global}$
end for
end for
$e_{global} = p^{\mathcal{N}}_{i,j} + e_{global}$
end for
end for
$\alpha_1 = e_{global}$

3.3 Scheduling Framework

Any candidate to be the optimum privacy-aware data transmission schedule must minimize an objective function F_i, where restrictions deducted from the network congestion model and restrictions coming from the attackers' learning model are combined (32). In this function parameters $\gamma_{\{1,..,3\}}$ control how variations in the optimization variables affect the global function, while parameters $\varepsilon_{\{1,..,3\}}$ determine the relative importance and contribution of each variable.

$$F_i = \left(exp\left\{ \frac{D_{i,j} - D_{6G}}{\gamma_1} \right\} \right)^{\varepsilon_1} \cdot \left(exp\left\{ \frac{\rho_i - \rho_{th}}{\gamma_2} \right\} \right)^{\varepsilon_2} \cdot \left(exp\left\{ \frac{L\left(W^j\right) - L_{th}}{\gamma_3} \right\} \right)^{\varepsilon_3} \tag{32}$$

But scheduling must be also efficient in computational terms, so a maximum of O_{total} optimization iterations are considered in the proposed scheme. To find the optimum data transmission schedule in terms of privacy and performance, we are defining the "state" θ_k of each time slot T_k in every time frame. State θ_k may take three different values: "0" if time slot is dummy and no data is transmitted, "1" if a private data unit from the transmission queue is routed and "2" is a false synthetic fuzzed data unit is transmitted.

The final purpose is to find the state θ_k to be assigned to every time slot T_k, so function $F_i(\cdot)$ is minimum. We are using the Particle Swarm Optimization (PSO) algorithm to achieve this purpose (33). PSO algorithm iterates O_{total} rounds, calculating the updated state θ^o_k for every o-th iteration.

$$\begin{aligned}
&\theta^o_k = \theta^{o-1}_k + \omega^o_k \\
&\omega^o_k = \begin{cases} \lfloor g^o_k \rfloor \; if \; \psi^3_{(0,1)} \\ \lceil g^o_k \rceil \; otherwise \end{cases} \\
&g^o_k = \varphi_1 \cdot \psi^1_{(0,1)} \cdot \left(\theta^{best}_k - \theta^{o-1}_k \right) + \varphi_2 \cdot \psi^2_{(0,1)} \cdot \left(\theta^{best}_{global} - \theta^{o-1}_k \right) + \sigma_o \cdot \omega^{o-1}_k \\
&\sigma_o = \sigma_{max} - \frac{\left(\sigma_{max} - \sigma_{min}\right) \cdot o}{O_{total}}
\end{aligned} \tag{33}$$

In this PSO algorithm, o the current iteration and θ^{best}_k the best state of the k-th particle (time slot) according to function $F_i(\cdot)$ and θ^{best}_{global} the best particle's position ever created according to function $F_i(\cdot)$.

Parameters $\psi_{(0,1)}^{\{1,\ldots,3\}}$ are random numbers following a uniform distribution in the range $[0,1]$ and parameters $\varphi_{1,2}$ are configuration values, as well as parameters σ_{max} and σ_{min}.

Finally, the states $\left\{\theta_k^{best}\right\}$ minimizing function F_i the most, after O_{total} iterations, are finally employed as transmission schedule.

4 Experimental Methodology and Validation

In order to evaluate the performance and utility of the proposed scheduling algorithm, an experimental validation is carried out. The experiments are based on simulation scenarios and tools, representing different configurations to exhaustively analyze the behavior of the proposed technology.

All simulations were designed and executed using MATLAB R2022a software, with standard precision. Contrary to other suites, MATLAB allows deep control of calculation precision and computational cost, so the specific configurations of small *ad hoc* nodes can be replicated with fidelity, and scalability experiments can be carried out with a reduced experimental error. Anyway, if *ad hoc* nodes with very reduced numerical precision are employed, results could be sightly different.

Each simulation was repeated twelve times to ensure that exogenous numerical effects do not impact the final results. In order to minimize errors, the consolidated results are calculated as the average value of all individual simulations. The random parameters required to run the simulations were randomly selected by the default MATLAB libraries, in order to remove any possible bias introduced by human intervention. Any possible exogenous effect should be mitigated by repeating simulations ten times.

As hardware platform, we employed a Linux architecture (Ubuntu 20.04 LTS) with the following hardware characteristics: Dell R540 Rack 2U, 96 GB RAM, two processors Intel Xeon Silver 4114 2.2G, HD 2 TB SATA 7.2K rpm.

Two different experiments were developed. In the first experiment, the congestion probability, QoS-compliance probability, and the probability of a successful intelligent attack are monitored in an *ad hoc* network implementing the proposed solution. Networks with different sizes (number of nodes, M_a), as well as different model configurations (i.e., different alternatives for the β function), were considered. The same experiment was repeated too for different values of the size of time frames (in time slots), K. Results from this first experiment were compared to the performance of *ad hoc* networks with a regular opportunistic data transmission scheme [42]. In the second experiment, the computational cost (delay) of running the proposed optimization framework was studied. The experiment was repeated for *ad hoc* networks with different sizes, and different sizes of time frames. In order to make results comparable, data were normalized considering the computational cost of standard opportunistic routing protocols.

All experiments simulated an *ad hoc* network in a smart lab. Different nodes with sensing capabilities had to route small data pieces towards a gateway, so later the information can be sent to a cloud infrastructure based on FIWARE components where it is stored. Nodes could include sensors for temperature, humidity, and carbon dioxide. To represent the heterogeneity of real *ad hoc* networks, nodes implemented totally or partially these sensing capabilities in a random basis. New information was produced every three minutes. As the proposed solution was local, the final results were calculated as the average from all individual nodes. To ensure some coherent information can be extracted from that data, they replicated real measures. Measures from the same dataset were used to train the fuzzing algorithm offline, and the final trained model was integrated into the simulation.

The real data for the training process and the simulated data generation were produced with real DTH-11 sensors (for humidity and temperature measurements) and CCS811 sensors for carbon dioxide measurements. Fuzzing algorithm was trained using Jupyter notebook technologies.

In all simulations, an intelligent attacker randomly placed within the *ad hoc* network developed an illegitimate data capture. This attack was based on a multi-layer perceptron [39], as this intelligent model has proved to carry out successful attacks learning from network data packets [40]. Although other intelligent models could be used as well [41], depending on the target application and focus.

To analyze the computational cost, internal functions and mechanisms from MATLAB were employed. On the other hand, congestion and latency at every network node were calculated numerically using teletraffic theory. The success probability of intelligent attackers was later estimated, by testing the trained model during simulations with new real data not employed before. To facilitate comparisons, percentages were used. For all simulations, congestion, excessive latency, or successful attacks were detected when the proposed thresholds, i.e., ρ_{th}, D_{6G} and L_{th}, were achieved.

Finally, for all simulations in the experimental phase, the system was configured with the parameters indicated in Table 2.

Table 2: Configuration and simulation parameters

Parameter	Value	Comments	Parameter	Value	Comments
$\varepsilon_1, \varepsilon_2, \varepsilon_3$	2	Homogenous weights	$\gamma_1, \gamma_2, \gamma_3$	10%	Standard value to consider any error or deviation relevant
φ_1, φ_2	0.5	Homogenous weights	h, v	2	Geometric progression
ρ_{th}	0.7	Standard value in teletraffic theory	L_{speed}	10	Medium size of an IP data packet
L_{th}	0.75	Regular value for algorithms trained with medium-quality datasets	R	25	Value high enough to reduce the impact of errors
O_{total}	50	Usual default configuration	b_2, b_3	M_a	To preserve all data evolves in range [0, 1]
D_{6G}	100	Common value in future 6G networks	b_1	2	Typical value in computational applications
Repetitions for each simulation	12	Values over 10 ensures a relevant error reduction	Simulated time	72 h	Long periods guarantee rare behaviors are observed

5 Results and Discussion

Fig. 5 shows the congestion probability, in terms of the number of network nodes M_a, calculated during the first experiment. As can be seen, the standard opportunistic routing strategies [42] evolve linearly with the number of nodes M_a. This is consistent with a fixed input stream for each individual node, where the traffic load increases homogeneously with each new node incorporated into the *ad hoc* network. Besides, congestion probability is always below 0.001%, which is coherent with eURLLC in 6G communications.

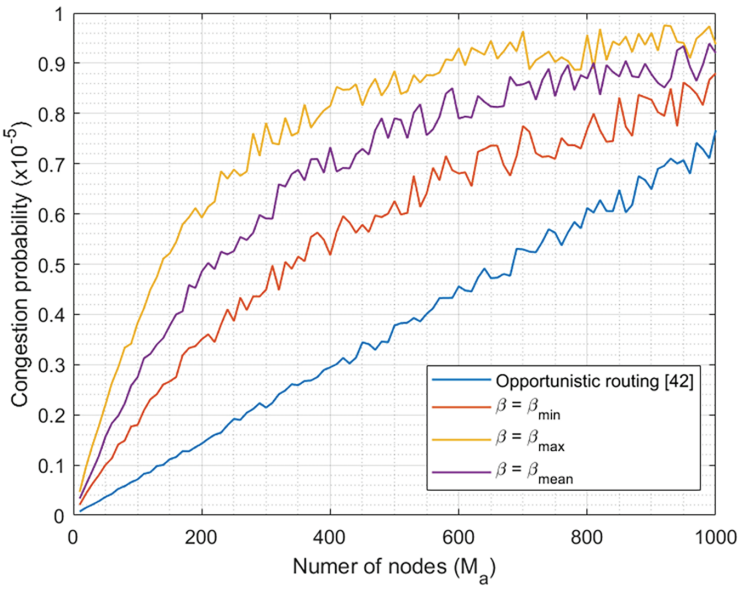

Figure 5: Congestion probability depending on $\boldsymbol{M_a}$, always below 0.001% (6G QoS)

In *ad hoc* networks implementing the proposed scheduling solution, expected 6G QoS is also met, as congestion never exceeds 0.001%. But in this case, evolution is exponential and congestion probability higher.

In fact, the proposed solution increases the data input streams, as they do not only include private data but also false fuzzed information. Due to this increase, the congestion probability also goes up with the number of nodes. An exponential evolution is also coherent, as traffic follows a Poisson distribution and β function affects the exponent in the learning model, causing yellow, purple and orange lines to evolve similarly but with different growing speeds. As the entropy considered increases, the growing speed does it as well. This exponential increase is not unlimited, as it stops when the probability gets closer to the defined thresholds. Because of the proposed definition for function F_i. So, although the behavior may be worse in terms of QoS, it is still fully compatible with 6G standards. Additionally, this deterioration facilitates a much higher improvement in privacy preservation (see Figs. 6 and 7).

For *ad hoc* networks larger than $\boldsymbol{M_a}$ = 1000 devices, the asymptotic evolution towards the congestion threshold (D_{6G}) will continue. So 6G requirements are always fulfilled. Eventually, no optimum transmission schedule being able to meet the 6G QoS requirements could be found. But, in that case, algorithm configuration should be updated to facilitate convergence.

Fig. 6 shows the congestion probability, calculated during the first experiment, for different values of K parameter (number of time slots in each time frame). As can be seen, for standard opportunistic routing strategies [42], parameter K has no impact as packets are transmitted in an opportunistic manner. The congestion probability is clearly below 0.001%, expected in 6G applications. On the other hand, the proposed scheduling algorithm shows a behavior as a "saddle". This is typical in PSO algorithms, when the number of particles varies. For a small number of time slots, it is very difficult to find a transmission schedule meeting all proposed restrictions. So, the congestion probability increases. As the number of particles (time slots) goes up, the optimization error reduces, and the congestion probability does the same. But, when the number of particles goes above 40 time slots, numerical errors are relevant again and the congestion probability increases (although much slows this time). Then, the optimum number of timeslots in each time frame is in the range between 25 and 40 (approximately).

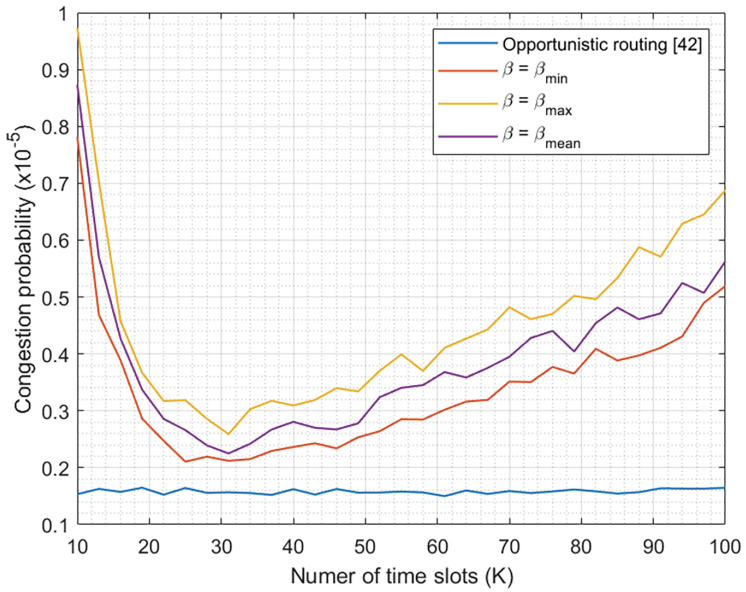

Figure 6: Congestion probability depending on $\boldsymbol{K}$, always below 0.001% (6G QoS)

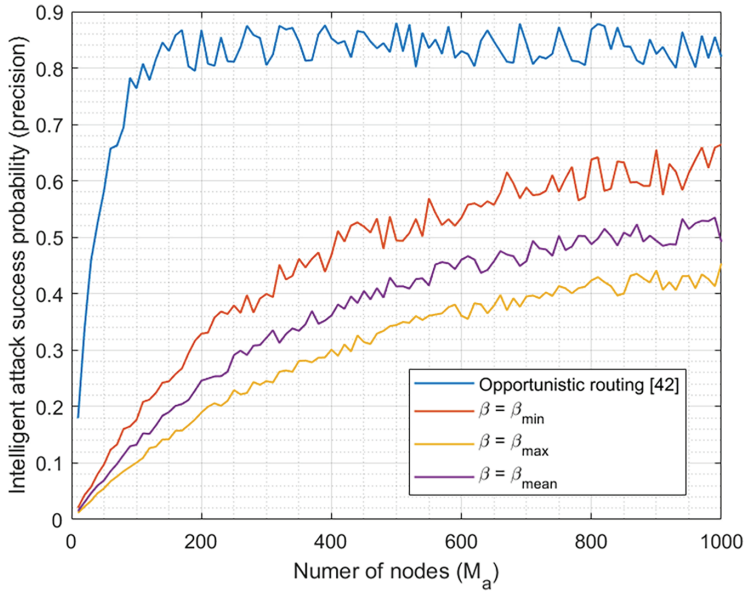

Figure 7: Probability of successful intelligent attack depending on $\boldsymbol{M_a}$, reducing up to 65% when using the proposed mechanism

As in Fig. 5, the differences between different β functions can be explained by the different values in the exponent in the learning model (the growing speed is higher as this exponent increases, see yellow line). Again, congestion probability for the proposed scheduling scheme is higher, as fuzzed information is transmitted to protect private data. Figs. 6 and 7 show the great improvement in privacy preservation we achieve thanks to this increase in the network congestion probability. But, always, the congestion probability is below 0.001% (the threshold defined in the optimization algorithm and the expected 6G QoS).

So, in conclusion, the proposed solution is acceptable in terms of network performance and fully compatible with 6G standards.

Fig. 7 shows the probability of a successful intelligent attack, depending on the number of nodes M_a in the *ad hoc* network. For all possible solutions, the evolution is exponential. In fact, since more nodes are part of the *ad hoc* network, more information is available, learning is stronger, and successful attacks are much more probable. But the main difference is the growth speed. In traditional routing strategies, success probability is above 80% for all network configurations, as no privacy protection instrument is considered. While, when the proposed scheduling solution is implemented, this probability reduces drastically. Being always below the results for traditional approaches. In the worst case (when β_{min} function is used), the success probability of intelligent attacks reduces up to 65% (for M_a = 200). But can be achieve up to 75% in the best situation (when β_{max} function is used). In the most critical region, reduction of success probability is more conservative and is between 25% (for β_{min} function) and 50% (for β_{max} function).

This reduction is more extreme for small networks, where data diffusion is faster and straightforward. For larger networks, when data may get lost, queued, or delayed, the discrepancies between reality and the proposed information diffusion model increases, and the probability does the same. In this case, implementations of β function overestimating the information entropy captured by attackers offer better results (contrary to results in Figs. 5 and 6). So, in balance, β_{mean} seems to offer the best mix between privacy and performance. For β_{mean} function, network performance (congestion probability) duplicates, although in absolute terms the values are below 6G requirements. But, as counterpart, intelligent attack success probability is reduced by half, going below 40%.

To conclude the first experiment, Fig. 8 shows the probability of a successful intelligent attack, depending on the number of time slots K in each time frame. Again, as can be seen, traditional opportunistic routing strategies are independent of this parameter, while the proposed scheduling algorithm shows behavior as a "saddle". The differences between the implementations of β function are equivalent to those explained before (Fig. 5). Reduction in success probability, in this case, achieves "only" 50% under the best circumstances. Again, the "saddle" form is typical of PSO algorithms were the number of particles changes, as the global optimization error evolves similarly and that causes an increase in the success probability. Tradeoff between privacy protection and network performance is equivalent to the previous discussion. If we take β_{mean} function as reference, network performance (congestion probability) duplicates, while intelligent attack success probability reduces below 50%. Congestion in absolute terms the values is always below 6G requirements, and privacy protection suffers a very significant improvement.

In conclusion, the proposed algorithm provides successful privacy-aware scheduling for data transmission in 6G-enabled *ad hoc* networks.

Finally, Fig. 9 shows the results of the second experiment. As can be seen, for the optimum values of K (as said before K = 20), the computational cost is five times higher than the standard opportunistic routing technologies. This increase includes the solving process of all linear equations and the optimization procedure. The evolution with the number of nodes M_a has a complexity of n^3, which is typical of solving algorithms for linear equations (the main element in the proposed congestion and teletraffic model).

This increase in computational cost is inevitable, as new functions are included. But even in the worst scenario, the increase is below one magnitude order.

Regarding the changes with K parameter, evolution is slightly more complex than linearity but still does not achieve n^2 complexity. This behavior is common in PSO algorithm.

In conclusion, the proposed algorithm matches the best computational behavior currently reported in the state of the art, and any increase does not achieve one additional magnitude order. So, the proposed solution is admissible, in computational terms, to be deployed in *ad hoc* networks.

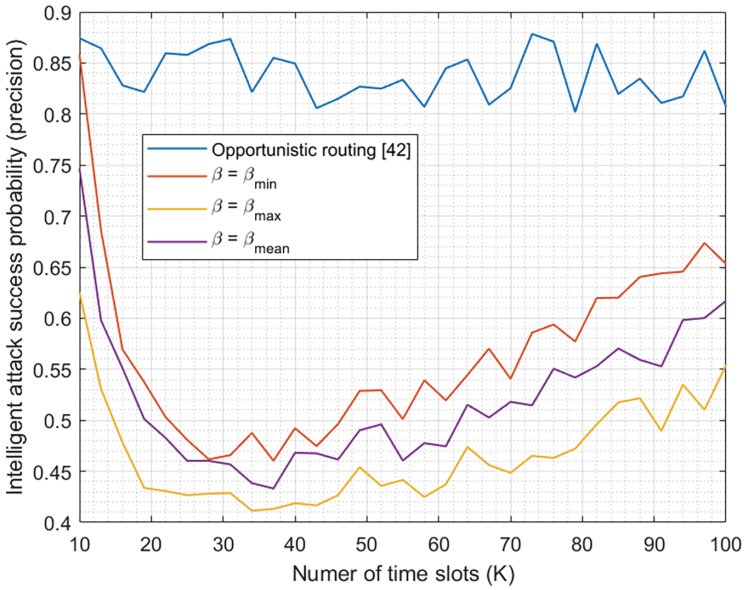

Figure 8: Probability of successful intelligent attack depending on K, reducing up to 50% when using the proposed mechanism

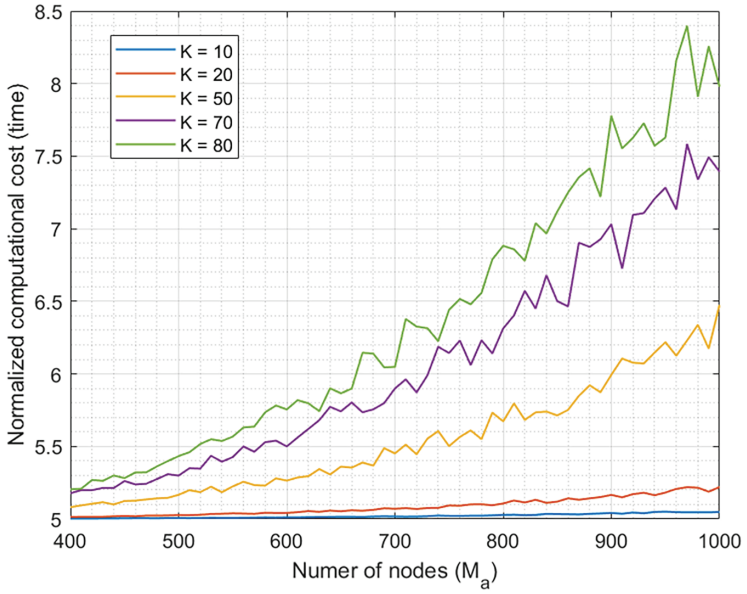

Figure 9: Normalized computational cost, showing a polynomial scalability

6 Conclusions

In this paper, we propose a scheduling algorithm, so that extreme nodes can choose the optimum time and scheme to transmit private data and keep them safe, making compatible network performance and 6G extreme QoS. The scheduler uses a probabilistic function in which teletraffic theory and information diffusion models are combined to find the optimum balance between privacy and Quality-of-Service. Real private data are optimally mixed with false information generated by fuzzing algorithms, so the learning level in intelligent attackers is reduced but network performance is preserved. A probabilistic dynamical system

is employed to represent and control the potential learning of intelligent attackers. While queue models and networks statistics are used to understand the behavior, lifecycle, and performance of *ad hoc* nodes.

An experimental validation based on simulation scenarios is provided. Results show that the probability of a successful intelligent attack reduces to 65% compared to *ad hoc* networks with no privacy protection strategy. Besides, an increase in the congestion probability is observed, caused by the additional fuzzed information injected by the proposed solution. But, in any case, the performance achieved is compatible with the expected 6G Quality-of-Service.

In practical scenarios, the proposed solution could enable critical real-time applications that handle private and sensitive data, such as Industry 5.0 services in essential infrastructures (e.g., power plants) or remote healthcare support in emergency situations. Future work should investigate its behavior in real environments, particularly in resource-constrained elements such as unattended fungible nodes. The use of real 6G testbeds will also be considered in future work.

Acknowledgement: None.

Funding Statement: This work has received funding from the European Commission by the Ruralities project (grant agreement no. 101060876).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Borja Bordel Sánchez; data collection: Ramón Alcarria, Borja Bordel Sánchez; analysis and interpretation of results: Ramón Alcarria, Tomás Robles; draft manuscript preparation: Borja Bordel Sánchez, Tomás Robles. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors confirm that the data supporting the findings of this study are available within the article.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Xu H, Zhou Z, Zhang L, Sun Y, Chih-Lin I. BE-RAN: blockchain-enabled open RAN for 6G with DID and privacy-preserving communication. In: Proceedings of the 2024 IEEE Globecom Workshops (GC Wkshps); 2024 Dec 8–12; Cape Town, South Africa. p. 1015–21. doi:10.1109/gcwkshp64532.2024.11100619.
2. Vijayakumar P, Azees M, Kozlov SA, Rodrigues JJPC. An anonymous batch authentication and key exchange protocols for 6G enabled VANETs. IEEE Trans Intell Transport Syst. 2022;23(2):1630–8. doi:10.1109/tits.2021.3099488.
3. Wang Z, Xu Y, Liu J, Li Z, Li Z, Jia H, et al. An efficient data sharing scheme for privacy protection based on blockchain and edge intelligence in 6G-VANET. Wirel Commun Mob Comput. 2022;2022(1):5031112. doi:10.1155/2022/5031112.
4. Singh Rawat G, Singh K, Shariq M, Das AK, Ashraf Chaudhry S, Lorenz P. BTC2PA: a blockchain-assisted trust computation with conditional privacy-preserving authentication for connected vehicles. IEEE Trans Intell Transport Syst. 2025;26(1):1134–48. doi:10.1109/tits.2024.3488184.
5. Guo S, Zhang A, Wang Y, Feng C, Quek TQS. Semantic-enabled 6G communication: a task-oriented and privacy-preserving perspective. IEEE Netw. 2025;1:3547760. doi:10.1109/mnet.2025.3547760.
6. Soni G, Chandravanshi K. A novel privacy-preserving and denser traffic management system in 6G-VANET routing against black hole attack. In: Sustainable communication networks and application. Singapore: Springer Nature; 2022. p. 649–63. doi:10.1007/978-981-16-6605-6_49.

7. Liao L, Zhao J, Hu H, Sun X. Secure and efficient message authentication scheme for 6G-enabled VANETs. Electronics. 2022;11(15):2385. doi:10.3390/electronics11152385.
8. Xu T, Wang N, Pang Q, Zhao X. Security and privacy of 6G wireless communication using fog computing and multi-access edge computing. Scalable Comput Pract Exp. 2024;25(2):770–81. doi:10.12694/scpe.v25i2.2629.
9. Xu Q, Su Z, Li R. Security and privacy in artificial intelligence-enabled 6G. IEEE Netw. 2022;36(5):188–96. doi:10.1109/mnet.117.2100730.
10. Nguyen T, Tran N, Loven L, Partala J, Kechadi MT, Pirttikangas S. Privacy-aware blockchain innovation for 6G: challenges and opportunities. In: Proceedings of the 2020 2nd 6G Wireless Summit (6G SUMMIT); 2020 Mar 17–20; Levi, Finland. p. 1–5. doi:10.1109/6gsummit49458.2020.9083832.
11. Wang X, Lyu J, Peter JD, Kim BG. Privacy-preserving AI framework for 6G-enabled consumer electronics. IEEE Trans Consumer Electron. 2024;70(1):3940–50. doi:10.1109/tce.2024.3371928.
12. Velliangiri S, Manoharan R, Ramachandran S, Rajasekar V. Blockchain based privacy preserving framework for emerging 6G wireless communications. IEEE Trans Ind Inf. 2022;18(7):4868–74. doi:10.1109/tii.2021.3107556.
13. Bordel B, Alcarria R, Robles T. A blockchain ledger for securing isolated ambient intelligence deployments using reputation and information theory metrics. Wirel Netw. 2024;30(6):5887–903. doi:10.1007/s11276-023-03375-9.
14. Guan Y, Lu R, Zheng Y, Zhang S, Shao J, Wei G. Toward privacy-preserving cybertwin-based spatiotemporal keyword query for ITS in 6G era. IEEE Internet Things J. 2021;8(22):16243–55. doi:10.1109/jiot.2021.3096674.
15. Sánchez BB, Alcarria R, Robles T. A probabilistic trust model and control algorithm to protect 6G networks against malicious data injection attacks in edge computing environments. Comput Model Eng Sci. 2024;141(1):631–54. doi:10.32604/cmes.2024.050349.
16. Zainuddin AA, Omar NF, Zakaria NN, Mbourou Camara NA. Privacy-preserving techniques for IoT data in 6G networks with blockchain integration: a review. Int J Perceptive Cogn Comput. 2023;9(2):80–92. doi:10.31436/ijpcc.v9i2.405.
17. Ilyas I, Din IU, Alourani A, Ashraf MU. Lightweight consortium blockchain-enabled secured Vehicular ad Hoc Network using certificateless conditional privacy-preserving authentication mechanism. PLoS One. 2024;19(10):e0310267. doi:10.1371/journal.pone.0310267.
18. Vuppula R, Pradhan HS. Blockchain-oriented location privacy preserving for cooperative spectrum sensing in 6G wireless networks. IET Blockchain. 2023;3(2):74–97. doi:10.1049/blc2.12025.
19. Alharthi A, Ni Q, Jiang R. A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET. IEEE Access. 2021;9:87299–309. doi:10.1109/access.2021.3086225.
20. Zhang J, Jiang Y, Cui J, He D, Bolodurina I, Zhong H. DBCPA: dual blockchain-assisted conditional privacy-preserving authentication framework and protocol for vehicular ad hoc networks. IEEE Trans Mob Comput. 2024;23(2):1127–41. doi:10.1109/TMC.2022.3230853.
21. Mustafa Hilal A, Alzahrani JS, Abunadi I, Nemri N, Al-Wesabi FN, Motwakel A, et al. Intelligent deep learning model for privacy preserving IIoT on 6G environment. Comput Mater Continua. 2022;72(1):333–48. doi:10.32604/cmc.2022.024794.
22. Li H, Li S, Min G. Lightweight privacy-preserving predictive maintenance in 6G enabled IIoT. J Ind Inf Integr. 2024;39(3):100548. doi:10.1016/j.jii.2023.100548.
23. Jai Vinita L, Vetriselvi V. Federated learning-based misbehaviour detection on an emergency message dissemination scenario for the 6G-enabled internet of vehicles. Ad Hoc Netw. 2023;144(3):103153. doi:10.1016/j.adhoc.2023.103153.
24. Bordel B, Alcarria R, Chung J, Kettimuthu R. Efficient and choreographed quality-of- service management in dense 6G verticals with high-speed mobility requirements. Integr Comput Aided Eng. 2024;31(2):173–95. doi:10.3233/ica-230722.
25. Inzillo V, Garompolo D, Giglio C. Enhancing smart city connectivity: a multi-metric CNN-LSTM beamforming based approach to optimize dynamic source routing in 6G networks for MANETs and VANETs. Smart Cities. 2024;7(5):3022–54. doi:10.3390/smartcities7050118.
26. Al-Rubaye RHK, Türkben AK. Using artificial intelligence to evaluating detection of cybersecurity threats in ad hoc networks. Babylon J Netw. 2024;2024:45–56. doi:10.58496/bjn/2024/006.

27. Li L, Zhu F, Eicher-Miller HA, Thomas JG, Huang Y, Sazonov E. Extra-lightweight AI-based privacy preserving framework for egocentric wearable cameras. In: Proceedings of the 2025 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 2025 Jun 11–12; Nashville, TN, USA. p. 401–10. doi:10.1109/cvprw67362.2025.00044.
28. Su H, Dong S, Zhang T. A hybrid blockchain-based privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans Veh Technol. 2024;73(11):17059–72. doi:10.1109/tvt.2024.3424786.
29. Cheng G, Huang J, Wang Y, Zhao J, Kong L, Deng S, et al. Conditional privacy-preserving multi-Doma in authentication and pseudonym management for 6G-enabled IoV. IEEE Trans Inf Forensics Secur. 2024;19(5):10206–20. doi:10.1109/tifs.2023.3314211.
30. Zhu F, Yi X, Abuadbba A, Khalil I, Huang X, Xu F. A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans Intell Transport Syst. 2023;24(10):10456–66. doi:10.1109/tits.2023.3275077.
31. Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-factor privacy-preserving protocol for efficient authentication in Internet of vehicles networks. IEEE Internet Things J. 2024;11(8):14253–66. doi:10.1109/JIOT.2023.3340259.
32. Xu T, Xu C, Xu Z. An efficient three-factor privacy-preserving authentication and key agreement protocol for vehicular ad-hoc network. China Commun. 2021;18(12):315–31. doi:10.23919/jcc.2021.12.020.
33. Banafaa M, Shayea I, Din J, Hadri Azmi M, Alashbi A, Ibrahim Daradkeh Y, et al. 6G mobile communication technology: requirements, targets, applications, challenges, advantages, and opportunities. Alex Eng J. 2023;64:245–74. doi:10.1016/j.aej.2022.08.017.
34. Lin JC, Srivastava G, Zhang Y, Djenouri Y, Aloqaily M. Privacy-preserving multiobjective sanitization model in 6G IoT environments. IEEE Internet Things J. 2021;8(7):5340–9. doi:10.1109/jiot.2020.3032896.
35. Xia Y, Wu L, Zheng X, Yu T, Jin J. Data dissemination with trajectory privacy protection for 6G-oriented vehicular networks. IEEE Internet Things J. 2022;9(21):21469–80. doi:10.1109/JIOT.2022.3183406.
36. Tamilvizhi T, Surendran R, Andres Tavera Romero C, Sadish Sendil M. Privacy preserving reliable data transmission in cluster based vehicular adhoc networks. Intell Autom Soft Comput. 2022;34(2):1265–79. doi:10.32604/iasc.2022.026331.
37. Karyakarte M, Agarkar A, Kulkarni L, Patil M, Chavhan G, Sule B. Dynamic opportunistic routing protocol for ad-hoc Internet of Vehicles (IoV). Computing. 2024;106(6):1707–28. doi:10.1007/s00607-023-01248-9.
38. Goyal M, Mahmoud QH. A systematic review of synthetic data generation techniques using generative AI. Electronics. 2024;13(17):3509. doi:10.3390/electronics13173509.
39. Kruse R, Mostaghim S, Borgelt C, Braune C, Steinbrecher M. Multi-layer perceptrons. In: Computational intelligence. Berlin/Heidelberg, Germany: Springer; 2022. p. 53–124. doi:10.1007/978-3-030-42227-1_5.
40. Ahmed S, Khan ZA, Mohsin SM, Latif S, Aslam S, Mujlid H, et al. Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron. Future Internet. 2023;15(2):76. doi:10.3390/fi15020076.
41. Khalaf BA, Mostafa SA, Mustapha A, Abed Mohammed M, Abduallah WM. Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods. IEEE Access. 2019;7:51691–713. doi:10.1109/access.2019.2908998.
42. Yamamoto R, Yamazaki T, Ohzahata S. VORTEX: network-driven opportunistic routing for ad hoc networks. Sensors. 2023;23(6):2893. doi:10.3390/s23062893.