# Designing a Security Framework Based on Hybrid Communication in the Internet of Nano Things

Aryan Rana, Sunil Prajapat, Pankaj Kumar, Deepika Gautam, Chien-Ming Chen

***Abstract*—In recent years, nanotechnology has emerged as a significant field of study with far-reaching implications. Integrating this nanoscale technology into the Internet of Things (IoT) has given rise to the Internet of Nano Things (IoNT) paradigm. This revolutionary technology significantly impacts healthcare, smart homes, and defense. This technological advancement has opened up new possibilities for enhancing the efficiency and effectiveness of these areas and has the potential to revolutionize their approach. Many research initiatives are addressing the definition of secure, scalable, and reliable network architectures at the nanoscale. However, the nano nature of this technology poses several security challenges for secure data transmission. Authentication is one of a prerequisite for secure data transmission. Our study presents a novel ECC-based authentication protocol for IoNT in this context. Since the nanoscale devices have less computational capabilities, this protocol leverages a secure hash function and XOR operations to ensure lightweight yet robust authentication. The protocol seamlessly integrates molecular and electromagnetic communication methods, thereby enhancing both security and efficiency within IoNT networks. In such a hybrid approach, parameter settings and message exchange are properly devised to achieve the aforementioned security services effectively. The security and authentication aspects of the protocol are rigorously examined using the Real-or-Random (ROR) model and Burrows-Abadi-Needham (BAN) logic, with its resilience against security threats tested via the AVISPA tool. We also analyze communication costs, computational overhead, and real-world feasibility. Finally, by employing the Nano-sim and N3Sim tools, we simulate and demonstrate the Internet of Nano-Things environment (i.e., expressed in terms of the packet loss ratio and the average amount of time required for propagation of authentication messages through molecular communications). This research stands as a pivotal contribution, fortifying the foundations of IoNT through heightened security and enhanced reliability.**

***Index Terms*—Internet of Nano Things (IoNT), Authentication, Molecular-based Communication, Electromagnetic Communication, AVISPA.**

Aryan Rana is with Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, India (e-mail: ishu.aryan113@gmail.com).

Sunil Prajapat is with Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, India (e-mail: sunilprajapat645@gmail.com).

Pankaj Kumar is with Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, India (e-mail: pkumar240183@gmail.com).

Deepika Gautam is with Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, India (e-mail: gautamdeepika1999@gmail.com).

Chien-Ming is with School of Artificial Intelligence, Nanjing University of Information Science and Technology, Nanjing, China (e-mail: chienmingchen@ieee.org).

## I. Introduction

The Internet of Things (IoT) is a network of physical devices, automobiles, buildings, and other entities that are integrated with sensors, software, and network connectivity and can gather and share data [1]. This technology has revolutionized the way we live and work by enabling new levels of efficiency, automation, and convenience. This sector has grown in various domains, including agriculture, industries, homes, the military, and healthcare [2]. As this technology advanced, a new paradigm, the Internet of Nano Things (IoNT), emerged [3]. The Internet of Nano Things (IoNT) refers to the integration of nanotechnology with the IoT to create a network of interconnected nano-scale devices [4]. At its core, the primary objective of IoNT is to amass and interchange data, akin to the IoT; however, what sets it apart lies in the scale, the sensor capabilities, the type of communication it employs, and the power utilization, all of which culminate in a distinctive approach to data exchange. The nano-devices used in IoNT are very small and operate on a nano-scale. The nano network consists of nanosensors that perform simple computations and tasks, nano routers that are integrated with other nano-devices, and a nano-micro interface device (NMID) that acts as an aggregator [4], [5]. The data shared among these devices is communicated from the NMID to the smart gadget for further use.

IoNT is being employed in various disciplines [5], [6] such as Fig. 1 clearly shows the employment of IoNT in the healthcare domain. One may wonder how IoNT would differ from the Medical Internet of Things (MIoT) after looking at Fig. 1. IoNT and MIoT are concerned with incorporating technology and gadgets into the healthcare industry. However, the size of the devices and the kind of data they gather are different. Medical IoT devices tend to appear in larger, more traditional shapes, including wearables and medical equipment, and they use wireless technology to collect and transfer data. These devices can enable remote patient monitoring, individualized treatment regimens, and data-driven illness management. In addition, they can monitor various patient health indicators, such as heart rate, blood pressure, and glucose levels. IoNT, on the other hand, makes use of nanoscale devices and sensors that can gather and send information at the molecular level. Nanoscale devices, for instance, might be used to target cancer cells more precisely or to monitor and detect illnesses early.

In the context of the IoNT, two preferred communication techniques are employed: nano-electromagnetic communication and molecular communication [7]. The use of electromagnetic waves, such as radio waves, at the nano-

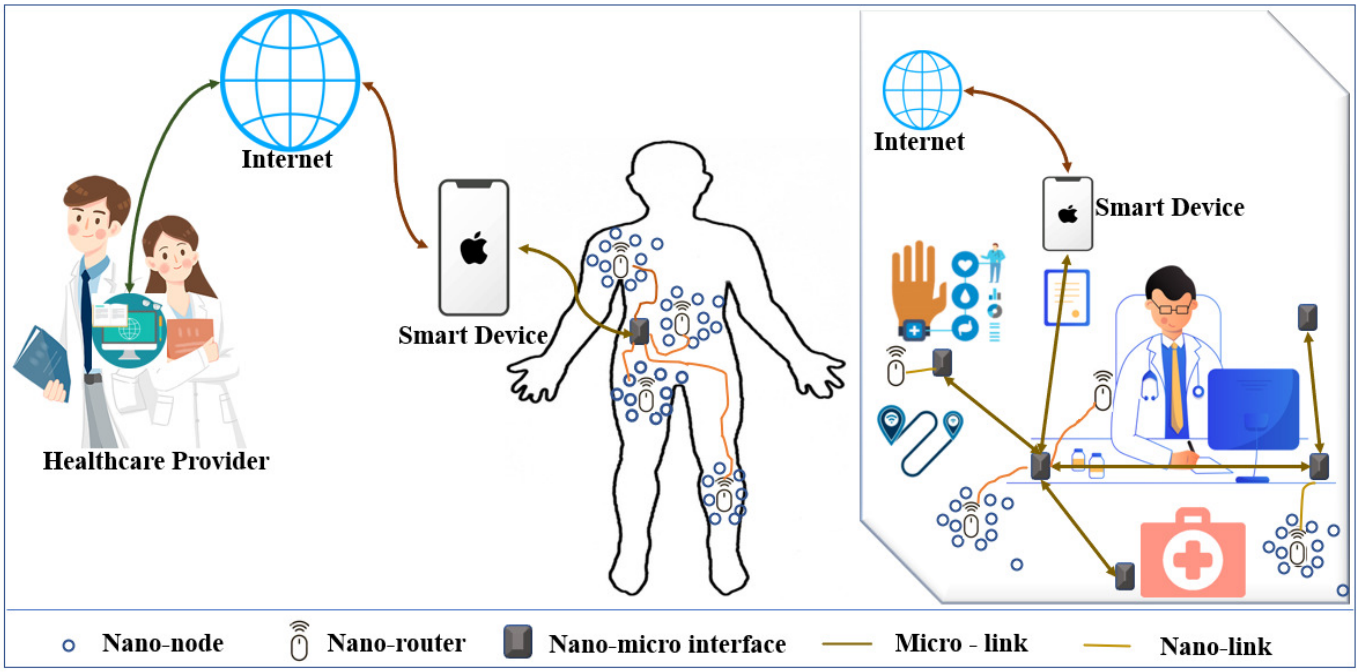



Fig. 1. The Employment of the Internet of Nano Things.

scale level for communication is called nano-electromagnetic communication. The small size and limited power of nano-scale devices make them more challenging to implement. RFID technology is one example of how electromagnetic wave communication is employed in IoNT [7]. RedTacton is an even better communication technology that can be utilized for communication between nano-scale technologies and the human body [8]. RedTacton operates at a higher frequency than RFID, allowing a faster data throughput and more stable connection, thus making it more advantageous [8]. Terahertz (THz) communication is a comparatively recent technology that transmits data by using electromagnetic waves in the terahertz frequency spectrum (0.1 - 10 THz) [9]–[11]. THz communication between nano-scale devices and between nano-scale devices and gateways can be used. Because of their great penetration and data rate, THz waves can establish communication with devices located behind barriers or inside confined areas [9], [11]. This can include using nano-scale devices, such as nano-particles or nano-robots, to transmit and receive information [4], [7].

Moreover, molecular communication in IoNT is a field of research that aims to develop communication systems using molecules as the carrier of information at the nano-scale level. One approach to facilitate molecular communication between devices in a network is by utilizing chemical or biological molecules to transmit and receive data [12], [13]. Since molecules are precisely engineered to engage with certain receptors or enzymes, molecular communication can be exceedingly concentrated and localized [12]. This makes it ideal to be employed in IoNT, where devices are relatively small and are positioned in difficult-to-reach locations. Molecular communication is the most promising approach for IoNT communication in areas such as the human body, animals, plants, etc. [13]. A hybrid of nano electromagnetic and molecular communication in IoNT helps improve communication performance in nano-scale networks [4]. Molecular communication allows sending information in noisy surroundings where nano-electromagnetic communication may be inhibited, while nano-electromagnetic communication allows sending information across great distances where molecular communication may be constrained [14]. Electromagnetic waves offer fast and reliable information transmission, while molecular communication is energy-efficient for nanoscale devices [4]. This hybrid approach hence improves effectiveness by optimizing communication methods. It also enhances network dependability by providing redundancy through multiple communication channels. If one method faces limitations or disruptions, the other acts as a backup, ensuring uninterrupted communication. Indeed, the considered hybrid framework greatly enhances the capability of IoNT networks.

As sensitive data is sent during the action, security and associated considerations for the IoNT become paramount [15]. We cannot risk having this information leaked or stolen since it might have devastating results because the content is even more sensitive than that of IoT [4]. Although some studies examine the security and difficulties associated with this technology, considerable material still needs to be added. [16], [17] explores a number of concerns and issues relating to security and privacy in the context of molecular communication. Concerns have been raised pertaining to the security of sensitive information transferred over the IoNT due to the possibility of unwanted access and eavesdropping in molecular communication. Islam et al. [18] showcased the use of a Diffie-Hellman algorithm to establish a secure channel in molecular communication. Sicari et al. [4] also developed a mechanism that outlines the architecture and functionality

required to secure the IoNT environment. This technique lays the groundwork for creating a secure protocol in this domain, giving it the potential to unlock new opportunities for the field while ensuring the protection of sensitive information.

Authentication is a key security mechanism provided by cryptography. Many authentication systems have been presented in the field of IoT to date. However, since the IoNT technology is new and still developing, no such authentication algorithm is proposed to ensure its security. Furthermore, authentication in IoNT is challenging since it is difficult to provide each device with a unique name and address [4]. This difficulty may be solved by assigning the same name and address to nano-devices at the same distance from the nano router [7]. Consequently, minimizing the time and effort required to assign a unique identifier to the devices. Employing this concept, an authentication method may be built using existing symmetric or asymmetric key mechanisms. Authentication is a critical aspect of securing the IoNT network. It would help eliminate numerous security concerns in this field and enable further research in this area. Furthermore, with authentication protocols in place, malicious activities can be prevented, and the overall security of the IoNT can be improved. By verifying the identities of devices before granting them access to the network, the risk of unauthorized access and data breaches can be minimized. In addition, this would enable researchers to explore the full potential of the IoNT without compromising the security of the sensitive information.

Building upon the foundational work by Akyildiz [3], our proposed study aims to realize the aforementioned security service within the IoNT network architecture. Our contribution lies in introducing a novel methodology for implementing authentication at the nanoscale level. The IoNT network architecture involves communication among nanoscale devices, microdevices, and generic IoT devices, leading to two distinct communication phases. In the initial phase, generic IoT devices communicate with microdevices; in the subsequent phase, microdevices communicate with nanoscale devices. This division is necessary due to the diverse nature of network components utilized in IoNT. The resulting network architecture combines a hybrid communication bus, catering to the specific communication requirements of different devices. To ensure resilience against remote or proximity attacks, nanodevices utilize diffusion-based molecular communication. On the other hand, electromagnetic communication is employed by other nanoscale, microscale, and generic IoT devices.

Furthermore, our objective is to incorporate authentication throughout the communication process. However, there is a notable lack of literature providing explicit results regarding the time required to complete cryptographic operations. Currently, a concrete cryptosystem in this particular field has yet to be established. However, aligning with studies [4], [19], [20], which have presented time estimates for basic security tasks executed by electronic devices of nanometric scale, our study seeks to provide a state-of-the-art advancement in authentication methods among nanoscale devices. Additionally, the proposed methodology is inherently adaptable and has the capacity to integrate any cryptographic algorithm available in existing literature or those defined in the foreseeable future.

The introduction of security functionalities brings about evident computational and communication overheads. These, in turn, affect the overall performance of the network architecture. However, due to the intricate nature of experimental test beds at the nano-scale, accurately quantifying the security implications becomes challenging. To address this limitation, an initial study is conducted to explore how security functionalities impact the performance of a representative IoNT scenario. Assumptions and parameters align closely with those outlined in [4], [19]. The reference values, as suggested by previous research, for both electromagnetic communication and molecular communication feasible within the bloodstream, are adopted based on studies such as [4], [21] and [4], [22] respectively. Additionally, the time required to complete cryptographic operations has been appropriately configured, following the guidelines provided in [4], [19].

Considering the previously mentioned discourse, a nano network involving a varying number of nanodevices is conceptualized, employing the subsequent tools: Nano-Sim [19], [23] for simulating electromagnetic-based communication on the nano-scale, and N3 Sim [24] for simulating molecular diffusion. The parameter configurations are extracted from [4], [20]. To delve deeper, the simulations specifically evaluate the packet loss ratio and the average time necessary for the dissemination of authentication messages through molecular communications. Furthermore, the primary contributions of the paper are outlined in the following subsection.

### A. Motivation and Contributions

Many different authentication and key agreement techniques have been put out in the context of IoT over the years [25], [26]. The IoT industry has undergone a transformation because of this new technology, and the focus has now been directed to IoNT after IoT saw significant growth. However, new technology brings with it new opportunities and challenges [5], [7]. Furthermore, [4] proposed a secure architecture that serves as a foundation for further developing this novel technology. Taking all this into consideration, we observed a gap in the IoNT's network that no authentication scheme had been put forward in this area (as per our best knowledge). The following highlights some of the research's significant contributions:

- We propose a secure, lightweight authentication and key agreement scheme for the IoNT, considering the capability of nano-scale devices. This scheme is divided into two phases. The first phase is between the gateway device and NMID. Whereas the second authentication phase is given for NMID, nano routers, and nano devices Since there is no concrete evidence in the literature of how authentication can be done in IoNT, we use an approach where the distance between the device plays a key role in the authentication. As there is a lot of scope for improvement in this sector, the second phase can be considered a hypothesis that can lay the groundwork for future work.
- Additionally, the ROR model-based formal security analysis, BAN logic analysis [27], and informal security analysis of the proposed authentication technique are

described. To confirm that our system is immune to various threats, we also simulate Automatic Validation of Internet Security Protocols and Applications (AVISPA). The results demonstrate that the suggested scheme is secure against a number of attacks in addition to ensuring mutual authentication and key agreement.

- Through the proposed scheme, we also exploit the potentiality of the hybrid communication technique instead of considering the traditional approach. We also use, Nano-sim [19], [23] and N3Sim [24] tools designed for simulating communication and diffusion at the nano-scale. The simulation is based on a case study of nano-device diffusion into the blood in an artery arm. The parameters are set according to a previous study [4], [19]. The simulations evaluate the packet loss ratio and the average time required for nano devices to construct the authentication messages. In simpler terms, the use of simulation tools is to evaluate the performance of a nano-network as well as the impact of security operations on the mentioned factors.

### B. Structure of the paper

The remainder of the paper's structure is as follows: The related research in this study area is covered in section II. The working model, which is further split into four subsections, is described in Section III. These subsections provide us with a clear understanding of the IoNT system model, how communication works in IoNT, and what security standards we need to meet to guard against potential attacks. The mathematical foundations that the suggested method employs are covered in Section IV. In section V, the proposed algorithm is outlined. The informal and formal security analyses are provided in Section VI. The security and efficiency of our scheme are included in Section VII. Finally, the proposed work is concluded in Section VIII.

## II. Related Work

With the increasing miniaturization of electronics and the growing demand for more connected devices, the field of IoNT is expected to grow in the coming years. The section discusses IoNT-related existing works. The preliminary work by Akyildiz *et al.* [3] presented a preliminary architecture for the IoNT network that comprised components such as nano-devices, nano routers, nano-micro interface device, and the gateway. Taking note of the nano electromagnetic communication, Perwej *et al.* [8] gave a review where the human body was used as a communication medium using RedTacton, who also highlighted the advantages of RedTacton. According to Agarwal *et al.* [28], with the growth in internet users, there is a demand for greater bandwidth. This problem can be addressed by employing a frequency band known as Terahertz. Its large channel capacity makes huge bandwidth accessible for relatively short ranges $(> 1m)$. Ali *et al.* [29] described the various IoNT network models and the architectural requirements for deployment. Further, terahertz communication is discussed in [9]–[11]. Also, they addressed that THz frequencies are located between the microwave and infrared regions of the electromagnetic spectrum, which provides a great amount of accessible bandwidth. This is particularly useful for IoNT applications where high data rates and large amounts of data need to be transmitted. Atakan *et al.* [12] described molecular communication in nanomedicine and also highlighted improvements in Body Area Networks (BAN). In [30], an examination of the obstacles associated with linking in-body nano-communication with Body Area Networks (BAN) is presented. Ali *et al.* [29] described the various IoNT network models and the architectural requirements for its deployment. Manojkumar *et al.* [31] emphasized the security and application of IoNT soon.

Akhtar *et al.* [7] provided a full overview of the IoNT, its present predicament, and future scenarios. Several applications and challenges have also been presented in [7]. [16], [17] also touch on this cutting-edge technology's security features. In these publications, molecular communication is the main focus. An architecture for secure communication in the IoNT network is given by Sicari *et al.* [4]. Their work also focuses on a hybrid communication technique, including molecular and nano-electromagnetic communication. Additionally, [18] provides an algorithm for a secured molecular system and a secret key exchange that is also efficient in terms of energy consumption. As mentioned in [4], [7], authentication is one of the most important cryptographic mechanisms to ensure secure communication. Many ECC-based authentication systems have been introduced for the IoT context. A secure two-factor mutual authentication approach for the TMIS (Telecare Medical Information System) was described by Radhakrishnan *et al.* [25] employing elliptic curve cryptography. Cho *et al.* [26] have introduced another safe IoT-enabled smart home authentication-focused technique that makes use of PUF technology. The summary of the main contributions of the researchers and the novelty of their research is provided in Table I.

There is still more to be done in the field of IoNT, as was evident from the examination of the current state of knowledge. Therefore, to improve the security and privacy of the data being exchanged in the system and address security-related problems, this study intends to introduce authentication into the IoNT network.

## III. Work model

This section is divided into four subsections: the architecture of the nano-device, which shows the components used in a nano-device; the system model, which represents the IoNT environment's design, the communication model, which describes the communication process between the devices engaged in the IoNT environment and lastly the security model or the security requirements which we aim to achieve by our proposed authentication protocol.

### A. Architecture of Nano Device:

Nano Device Schema: Nano-devices generally consist of three primary parts in the IoNT:

- Sensing and Actuation: These components enable the nano-device to perceive its surroundings and react appropriately. Examples include actuators for movement

TABLE I
SUMMARY OF MAIN CONTRIBUTIONS OF AUTHORS.

| Literature | Year | Scope of Study | Main Contribution |
|---|---|---|---|
| Akyildiz *et al.* [3] | 2010 | IoNT and Nano electromagnetic communication | Analysis of electromagnetic communication among nanoscale devices and identification research obstacles in channel modeling, information encoding, and protocols for nanonetworks and the IoNT. |
| Loscri *et al.* [16] | 2014 | Security and Privacy In Molecular Communications | Discuses security and privacy in molecular communication, proposes research directions, and highlights the need for tailored security solutions. Compares molecular communication with traditional communication and outlines potential approaches to safeguard system reliability. |
| Sicari *et al.* [4] | 2019 | Secure architecture for IoNT | Introduces a new method to improve the safety and reliability of nanonetworks. Combines molecular diffusion and electromagnetic communication. Evaluation of the security protocols' impact on performance using Nano-Sim and N3Sim tools is also provided. |
| Nikhat *et al.* [7] | 2020 | IoNT existing state and future prospects | Architecture, key applications in healthcare, transportation, and defense, security concerns, and market trends of IoNT. Emphasis on potential avenues for future research and opportunities. |
| Yin *et al.* [11] | 2022 | Terahertz nano-communication | Highlight the significance of Terahertz (THz)-band communications (0.1 10 THz) as a pivotal technology for future 6G wireless systems tailored for healthcare applications. Emphasize the potential of nano-scale devices in medical diagnostics and treatment. Address challenges like biological safety and spectrum scarcity through advanced channel modeling. |
| Radhakrishnan *et al.* [25] | 2022 | Two-Factor Mutual Authentication Scheme Using ECC for IoT-Based Telecare Medical Information System | Combines smart cards with ECC for secure and efficient two-factor authentication, maintaining user privacy during password change. |
| Cho *et al.* [26] | 2022 | Anonymous user authentication scheme for IoT-enabled smart home environments using PUF | A new method for secure communication in smart homes using PUF technology to enhance a two-factor authentication scheme is proposed. Offers protection against attacks and guarantees user anonymity and forward secrecy. |
| Alabdulatif *et al.* [32] | 2023 | IoNT survey | An extensive overview of IoNT, including its applications and advantages. Weaknesses in the IoNT design and solutions for privacy and security problems are pointed out. A summary of current field-wide research is provided to set the study apart from previous research. |

or other physical changes and sensors for temperature, humidity, pressure, chemical composition, etc.

- Processing and Communication: These parts enable the nano-device to process sensor data and exchange information with other devices. Microcontrollers or microprocessors are a few examples and communication modules for wired or wireless communication.
- Power and Energy Management: These elements enable nanotechnology to function independently and effectively. Examples include energy storage mechanisms like batteries or power management circuits that help to maximize energy efficiency.

Together, these three components (as seen from Fig. 2) allow the nano-device to function as part of the larger IoNT ecosystem, sensing its environment, processing and communicating information, and managing its power usage. It's also worth noting that security and privacy are critical aspects of the IoNT, as these tiny devices are vulnerable to hacking, spoofing, and other malicious activities.

### *B. System model:*

As we see from [3], [4], [7], many architectures have been proposed for the IoNT environment, which is almost similar. [4] introduces nano controllers, a nano-device capable of ensuring the security in the nano network, whereas [3], [7] discusses the basic architecture for the IoNT. We propose a similar architecture for the IoNT, depicted ahead.

- Nano Devices: These are the smallest component of the nano network, equipped with nano-scale components. Also known as nanomachines, nano-devices can perform

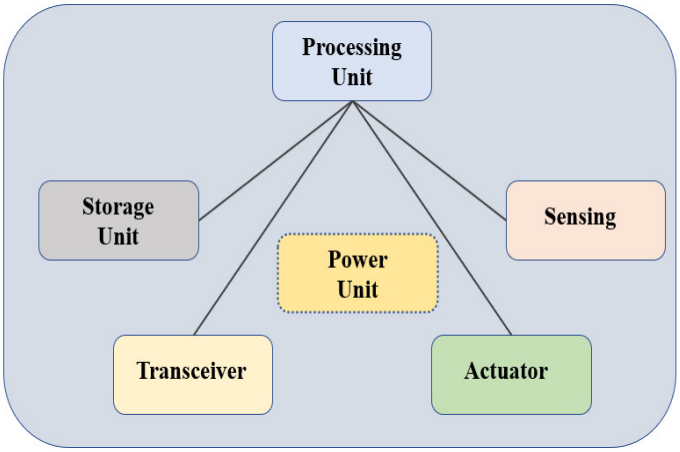



Fig. 2. Block Diagram of Nano-Device

simple tasks such as sensing, actuation, or responding to commands received by the nano routers. A number of nano-devices are connected with one nano router to gather the information. These nano-devices use molecular communication to transmit and receive information with the corresponding nano routers.

- Nano Routers: Nano routers are less abundant than nano-devices; for a given environment, there is only one nano router to which numerous nano-devices are linked. These nanomachines are more powerful because they have greater computation capability and relatively high power and storage capacities. Information is received from nano-devices and sent to nano micro interface devices using nano routers. Nano routers merely receive and send data; they do not perform any sensing functions. The nano routers communicate with nano-devices using molecular communication, whereas they communicate with nano micro-interface devices using nano electromagnetic communication.
- Nano-Micro Interface Device (NMID): NMID is a hybrid device that can communicate in both macro and nano paradigms. This device collects the data and information obtained from the nano routers. Further, the received data is sent to the gateway outside the nano network. The interface device can carry out more complicated activities and is more powerful than nano routers. The data transport from the nano network to the gateway device is handled by a single device, i.e., the interface device, which acts as an aggregator [7]. This device communicates to the other devices using nano electromagnetic waves.
- Gateway: The gateway device serves as the controller of the entire system that gathers all the aggregated data from the interface device. Additionally, this information can be accessed from anywhere with an internet connection [7]. For example, with e-healthcare systems, information can be provided to healthcare professionals for monitoring a person's health. Any smart device, such as a smartphone, smartwatch, or other wearable technology, can serve as a gateway.

In conclusion, molecular communication is used by the nano-devices and nano routers to communicate, and these nano routers then aggregate the data gathered by all the nano-devices and transfer it to the interface device through nano electromagnetic communication. Likewise, the interface device gathers the data and sends it to the gateway device linked to the internet. To sum up, a nano router, a nano device, and a nano micro interface device make up the nano network. A hybrid approach is adopted for communication similar to that in [4]. The system model can be best understood from Fig. 3.

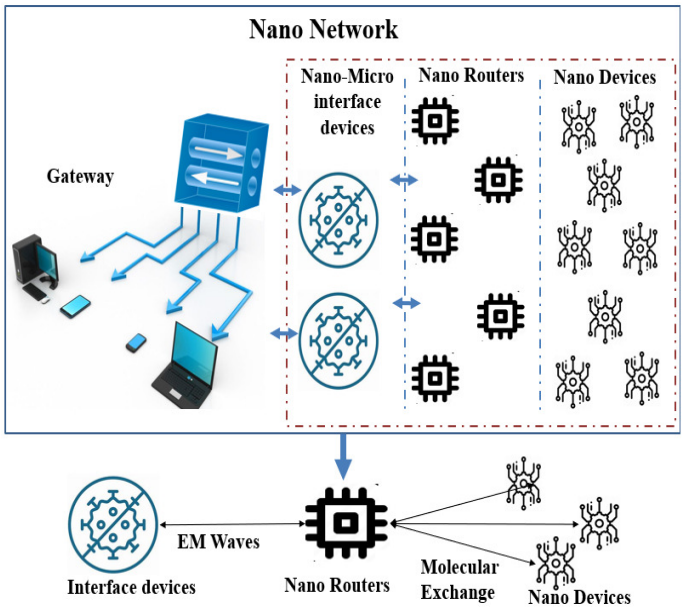



Fig. 3. The IoNT communication model.

### C. Communication Model:

Fig. 3 clearly explains the type of communications between the devices in the IoNT network. In this subsection, we briefly discuss molecular communication and nano-electromagnetic communication in the terahertz band.

1) Molecular communication: The most practicable method for nano-robot communication is thought to be molecular communication. In contrast to electromagnetic waves used in electromagnetic communications (even at the nano-scale), light waves used in optical communications, or sound waves used in acoustic communications, encoded molecules are considered information carriers in molecular communication [16]. Additionally, the information encoding can vary depending on several factors, such as the configuration, concentration, sequence of macro-molecules [33], or the presence or absence of a certain type of molecule (which is used to digitally encode messages) [34]. Complex proteins are information carriers in molecular communications, and a digital symbol transformation is not always necessary. Short-range molecular communication depends on passive transport utilizing calcium signaling or diffusion, whereas long-range molecular communication makes

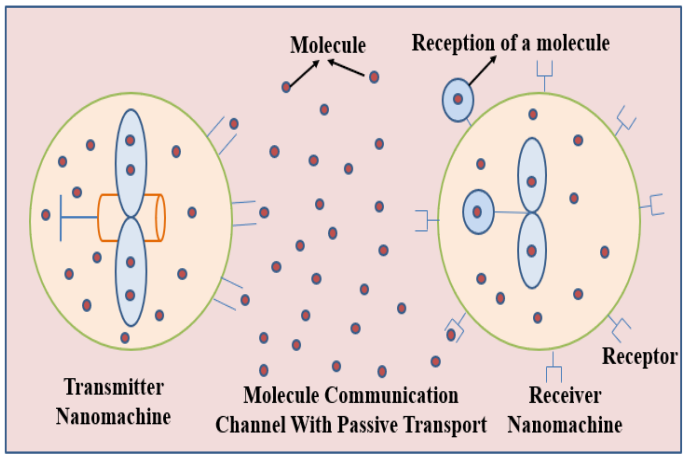



Fig. 4. Molecular interaction channel of passive transportation.

use of pheromones [16]. Medium-range molecular communication uses active transport using molecular motors in fluidic medium [16].

The molecular communication channel depicted in Fig. 4 is primarily a binary channel with bits 0 and 1. In the binary channel technique, at the beginning of the fixed-duration time slot, a transmitter (TN) transmits one or more molecules to provide bit 1. The receiver (RN) can appropriately receive bit 1 if the molecule or a threshold concentration reaches it during the slot period. If not, the receiver will erroneously get a bit of 0. To deliver 0, the transmitter transfers no molecules over a slot period. However, when bit 0 is delivered, the molecules released in the earlier slot intervals could eventually reach the receiver. This might lead to a delivery error of 0 [12]. By prolonging the propagation of a single bit over two slot durations, the binary channel technique is also adjusted to avoid such problems. In order to transfer bits 0 and 1, precisely, 00, 01, 10, and 11 are sent. The above discussion is shown in Fig. 4.

2) Nano electromagnetic communication (terahertz band): Terahertz (THz) band communication, sometimes called T-wave communication, is a form of wireless communication that operates in the THz frequency band, which is situated between microwave and infrared frequencies [9]. Because there is a lot of unutilized bandwidth in this frequency range, it is a viable technology for the Internet of Nano Things (IoNT). For applications like high-definition video streaming, virtual reality, and real-time control in the IoNT, THz band communication can offer high data speeds and minimal latency. Compared to other wireless technologies, it also consumes much less power [9]. THz waves also pass through various non-metallic items, including clothes and walls, making them suitable for internal communication and sensing. In-vivo nanonetworks, or networks of linked devices tiny enough to be implanted in the human body, have the ability to utilize Terahertz (THz) communication [11]. THz waves are a potential technique for in-vivo communication and sense since they can pass through biological tissue. The devices must be positioned near the skin's surface to effectively communicate since THz waves' ability to penetrate deep into biological tissue is constrained [11].

### D. Security Requirement

Security is crucial when it comes to handling sensitive data. It is essential to have robust measures to protect such data from unauthorized access, theft, or compromise. This section outlines the fundamental security requirements for the IoNT environment.

- Key Management: Given that they may be used for both encryption and decryption, keys are crucial to the security of the data. In the IoNT context, keys can either be distributed prior to network deployment or must be produced when communication is taking place [7]. Furthermore, it becomes crucial to keep the keys secure from the adversary.
- Confidentiality, Integrity and Availability: The "Confidentiality, Integrity, and Availability" (CIA) triad is a widely recognized model for information security that revolves around protecting sensitive information from unauthorized disclosure to maintain the privacy of the data. The exchange of communications between a sender and a receiver has to be protected from alterations by outsiders without the participant's consent. A malicious client shouldn't be capable of interfering with or negatively affecting the type of administration provided by nano-devices or nanosystems [32].
- Authentication and Access Control: To ensure the goal of secrecy, authentication is necessary. All messages intended for nano communication systems must pass via a gateway and undergo authentication. Typically, classical symmetric or asymmetric cryptography is used to provide authentication. Even access control should be ensured.
- Proximity to certain attacks: Terahertz communications render remote attacks viable since they don't require a physical attack to succeed [4]. Due to the adversary's closeness to the nano network, they may be able to enter the network without authorization and cause harm. As the opponent may block the transmission or saturate the communication channel with a high number of molecules, a denial of service (DoS) attack is also conceivable [7]. Attacks like eavesdropping and spoofing are also feasible [4], [16], in which the two nano devices' communication can be monitored and, if possible, changed to disrupt transmission. It is also crucial to address potential threats like replay attacks, DDoS attacks, and man-in-the-middle attacks in order to guarantee the comprehensive security of the IONT paradigm.

## IV. Preliminaries

In this section, we discuss the mathematical terminologies and the notations used in this paper.

- Biometric and Fuzzy Extractor: Fuzzy extractors are a tool for incorporating biometric data into cryptographic security requirements. The fuzzy extractor can be represented as $(\mathcal{M}, \mathcal{F}, \mathcal{H})$ where $\mathcal{H}$ is the bio-metric input of

TABLE II
NOTATIONS OF THE DEVISED SCHEME.

| Symbols | Description |
|---|---|
| $E_q(.)$ | Elliptic curve over a real prime finite field |
| $e$ | Basepoint on $G$ |
| $q$ | Large prime |
| $h(.)$ | One-way secure hash function |
| $s$ | Private key of the server |
| $ID_k$ | Identity of the $k^{th}$ user |
| $PW_k$ | Password of the $k^{th}$ user |
| $UID$ | Identity of the nano micro interface device |
| $VID_j$ | Identity of the $j^{th}$ nano router |
| $XID_i$ | Identity of the $i^{th}$ nano device |
| $x_{iv}$ | $v^{th}$ distance of the $i^{th}$ nano device |
| $z$ | Shared secret key between the nano router and interface device |
| $P_{pub}$ | Public key of the server |
| $\|\|$ | Concatenation operation |
| $\oplus$ | Bitwise XOR operation |
| $\delta T$ | Valid time delay in message transmission |

data of metric space of finite dimension and $\mathcal{M}$ is the bit length of the output string. These fuzzy extractors are described as a pair of functions, one of which generates uniform random bits from pre-specified input values and the other of which retrieves the string closest to the legitimate input data within the predetermined approach from the input value [25]. The two processes by which the fuzzy extractor is specified are

- Gen (.): is a probabilistic method that takes biometric input $B_k \in \mathcal{H}$ and gives $\sigma_k \in \{0,1\}^t$ as output which is secret data, and $\tau_k$ as a public value (also known as reproduction variable) for the biometric input data. Here $Gen(B_k) = \sigma_k, \tau_k$.
- Rep(.): is a deterministic approach, when given a biometric input $B_k \in \mathcal{H}$, $\mathcal{F}$ and $\tau_k$ then replicate the biometric key $\sigma_k$, i.e., $Rep(\tau_k, B_k^*) = \sigma_k$, where $d(B_k, B_k^*) \leq \mathcal{F}$.

- Elliptic Curve Cryptography (ECC): Based on [35] we define ECC: Let $E_q(c,d) : y^2 = x^3 + cx + d \mod q$, be a non-singular elliptic curve with a prime finite field $F_q$, where $c, d \in F_q$ with $4c^3 + 27d^2 \mod q \neq 0$ and $G = \{(x,y) : x, y \in F_q, (x,y) \in E\} \cup \{\theta\}$ forms and abelian group, under addition, where $\theta$ is the identity of the group $G$.
- Elliptic curve discrete logarithm problem (ECDLP): Let $G$ be a cyclic group formed by base point $e$ of a prime order elliptic curve $q$. Calculating $a \in Z_q^*$ is computationally hard by any polynomial constraint approach for given $e$ and $a.e$ where $e \in G$ and $a \in Z_q^*$.
- Elliptic curve Diffie-Hellman problem:(ECDHP): This problem is as follows, for points $f.e, h.e \in G, \forall (f,h) \in Z_q^*$, it is hard to calculate $fh.e$.

## V. PROPOSED SCHEME

In this section, we discuss the possible authentication, firstly among the gateway and the nano micro interface device and then among the devices involved in the nano-network. We propose a lightweight methodology since the nano-scale devices can perform very few computations compared to the available IoT devices. The proposed framework is as follows:

1) *Initialization phase:* In this phase, the server performs the following steps to initialize the system parameters as below:
   - Server selects $q$, a non-singular elliptic curve $E_q(c,d)$ : $y^2 = x^3 + cx + d \mod q$ with base point $e \in G$, where $c, d \in Z_q^*$ with $4c^3 + 27d^2 \mod q \neq 0$ and $G$ is a group generated by $e$ of order $q$.
   - During the registration and login phase, $Gen(.)$ and $Rep(.)$ are used to perform biometric using the fuzzy extractor.
   - The server selects it's $h(.)$, generates $s \in Z_q^*$ as private key and $P_{pub} = s.e$ as public key.
   - Due to the limited storage and processing capability of nano-scale devices, they cannot perform highly difficult processes. Therefore, we assume that the server stores a small number of values in nano-devices, nano routers, and interface devices before network deployment, reducing the computational overhead. So, the following values are stored in each device by the server:
     - Server selects $UID$ (identity of the interface device), $z \in Z_q^*$ (shared secret key between the interface device and all the nano routers) and list of $x_{iv}$'s ($v^{th}$ distance of the $i^{th}$ nano device from the nano router). Since it is difficult to provide each nano-device a unique name and address, the same identity for nano-devices located at the same distance from nano routers is given out.
     - Server stores $UID, VID_j$ (identity of the $j^{th}$ nano router), list of $x_{iv}$'s and, $z \in Z_q^*$ (shared secret key between the interface device and all the nano routers) in the nano routers.
     - Server stores $VID_j, x_{iv}$ ($v^{th}$ distance of the $i^{th}$ nano device from the nano router) and $XID_{iv}$ (the identity of the $i^{th}$ nano device at a distance of the v) in the nano-devices.

   Finally, the server publishes $\{E_q(c,d), q, e, P_{pub}, h(.), Gen(.), Rep(.)\}$ and keeps s secretly.
2) *User registration phase:* In this phase, the user registers on the server, and all the messages are sent via a secure channel. The detailed steps are shown in Fig. 5.
   - Step 1: User inputs $ID_k, PW_k$ and $B_k$ in the gateway (i.e., a smart device or smart wearable), then gateway selects $r_k \in Z_q^*$ and computes $(\sigma_k, \tau_k) = Gen(B_k)$, $F_k = h(ID_k)$ and $P_k = h(ID_k||\sigma_k||r_k)$ and sends $F_k$, $P_k$ to the server.
   - Step 2: The server first checks that if $F_k$ is new or existing one. If it is new, the server moves forward or rejects the request. Then the server computes, $\alpha_k = h(F_k||s||P_k)$ and then stores $F_k$, $P_k$ and $\alpha_k$ in the database. Further, the server sends $e, UID, z$ to the gateway.
   - Step 3: After receiving $e$, $UID$ and $z$ form the server the gateway computes, $\beta_k =$

| User/Gateway | | Server |
|---|---|---|
| User input $ID_k$, $PW_k$ and $B_k$ in the Gateway | | |
| Gateway Selects $r_k \in Z_q^*$ | | |
| Gateway then Computes ($\sigma_k$,$\tau_k$)=Gen $B_k$ | | |
| $P_k$=h($ID_k$ \|\| $\sigma_k$ \|\| $r_k$), $F_k = h(ID_k)$ | | |
| | $\xrightarrow{F_k, P_k}$ | |
| | | Check if $F_k$ is new or existing one |
| | | Computes $\alpha_k$=h($F_k$ \|\|$s$\|\|$P_k$) |
| | | Stores $F_k$, $P_k$, $\alpha_k$ |
| | $\xleftarrow{e, UID, z}$ | |
| Computes $\beta_k$=h($ID_k$\|\|$PW_k$\|\|$\sigma_k$) $\oplus r_k$ | | |
| $Q_k$=h($PW_k$\|\|$\sigma_k$\|\|$r_k$) | | |
| $\gamma_k = h(PW_k \| \sigma_k) \oplus z$ | | |
| Stores $(\beta_k, Q_k, \gamma_k, UID, e, P_k, \tau_k)$ | | |

Fig. 5. User registration phase between gateway and server.

$h(ID_k||PW_k||\sigma_k) \oplus r_k$ , $Q_k = h(PW_k||\sigma_k||r_k)$, $\gamma_k = h(PW_k||\sigma_k) \oplus z$. Then the gateway stores $(\beta_k, Q_k, \gamma_k, UID, e, P_k, \tau_k)$ in the database.

3) *Login, authentication, and key agreement phase:* This phase is divided into two phases: the first between the gateway and the NMID, and the second between the NMID, nano routers, and nano-devices. The detailed steps are shown in Fig. 6 and Fig.7.

*Authentication and key agreement between the gateway and the nano micro interface device:*

- Step 1: User inputs $ID_k^*, PW_k^*$ and $B_k^*$ in the gateway. Then the gateway computes $\sigma_k^* = Rep(B_k^*, \tau_k^*)$ and gets $\sigma_k^*$. Further the gateway computes $r_k^* = h(ID_k^*||$
$PW_k^*||\sigma_k^*) \oplus \beta_k$, $Q_k^* = h(PW_k^*||\sigma_k^*||r_k^*)$ and checks if $Q_k^* \stackrel{?}{=} Q_k$ or not. If yes then the gateway verifies the user. Next, gateway computes $z = h(PW_k||\sigma_k) \oplus \gamma_k$ and gets $z$. Then computes the following:
$$A = ID_k \oplus h(UID||z)$$
$$B = h(ID_k||z) \oplus P_{pub}$$
$$C = h(ID_k||UID||z||T_1)$$
and sends $\{A, B, C, T_1\}$ to the nano micro interface device.
- Step 2: After receiving the message from the gateway, the interface device first checks $T_2 - T_1 \leq \delta T$; if yes, then proceeds further. Then the device computes $ID_k^{**} = A \oplus h(UID||z)$ and $C^* = h(ID_k^{**}||UID||$
$z||T_1)$ and checks if $C^* \stackrel{?}{=} C$ or not. If yes, the gateway is authenticated. Further, it computes $P_{pub} = B \oplus h(ID_k||z)$. The interface device generates a random nonce $m \in Z_q^*$ and computes the following
$$D = m \oplus h(UID||z||T_3)$$
$$E = h(ID_k||UID||z||m)$$
$$SK_{ID1} = h(ID_k||UID||z.P_{pub}||m)$$
and sends $D, E, T_3$ to the gateway.
- Step 3: After receiving this message, the gateway device first computes $T_4 - T_3 \leq \delta T$. If yes, then proceeds further and computes $m^* = D \oplus h(UID||z||$
$T_3)$ and $E^* = h(ID_k||UID||z||m^*)$.Checks if $E^* \stackrel{?}{=} E$ or not. If yes, then the nano micro interface device is mutually authenticated. Further, the gateway computes the session key $SK_G = h(ID_k||UID||z.$
$P_{pub}||m)$. Now, $SK = SK_G = SK_{ID1}$ which shows that session key agreement is successful.
The nano network becomes active after this authentication among the gateway and the nano micro interface device. Then, a subsequent authentication occurs among the nano-devices, nano routers, and the nano micro interface device.

*Authentication and key agreement phase between nano-devices, nano routers, and nano micro interface device:*

- Step 1: Once the nano network becomes active, the interface device selects $x_{iv}$ from the list, selects $u \in Z_q^*$ and computes the messages
$$M_1 = h(UID||z||u||T_5)$$
$$M_2 = z \oplus u$$
$$M_3 = z \oplus x_{iv}$$
and sends $\{M_1, M_2, M_3, T_5\}$ to the nano router it wants to authenticate.
- Step 2: On receiving this message the $j^{th}$ router checks if $T_6 - T_5 \leq \delta T$ or not. If yes, the nano router proceeds and computes $x_{iv} = z \oplus M_3$ and checks $x_{iv}$ in the list. Then proceeds to compute $u^* = z \oplus M_2$ and $M_1^* = h(UID||z||u^*||T_5)$. Checks if $M_1^* \stackrel{?}{=} M_1$. If yes, the authentication is successful. Then the nano router computes
$$M_4 = h(VID_j||u^*)$$
$$M_5 = u^* \oplus x_{iv}$$
and sends $M_4, M_5$ to the $i^{th}$ nano device present at the $v^{th}$ distance.
- Step 3: After receiving the message from the $j^{th}$ nano router, the nano device first computes $u^{**} = M_5 \oplus x_{iv}$ and $M_4^* = h(VID_j||u^{**})$. Checks if $M_4^* \stackrel{?}{=} M_4$ or not. If yes, then the nano router is authenticated; further, the nano-device computes
$$M_6 = XID_i \oplus x_{iv}$$
$$M_7 = h(XID_i||u^{**})$$
and sends $\{M_6, M_7\}$ to the nano router.
- Step 4: Further, this message reaches the nano router, and the nano router computes $XID_i^* = M_6 \oplus x_{iv}$ and $M_7^* = h(XID_i^*||u^*)$, then checks if $M_7^* \stackrel{?}{=} M_7$. If yes, then the nano-device is authenticated. Then the $j^{th}$ nano router computes $M_8 = h(VID_j||z||T_7)$, $M_9 = VID_j \oplus x_{iv}$ and the session key $SK_{NR} = h(z||UID||VID_j||T_7)$. Then nano router sends $\{M_8,$
$M_9, T_7\}$ to the interface device.
- Step 5: Lastly, the interface device checks if $T_8 - T_7 \leq \delta T$. If yes then computes $VID_j^* = M_9 \oplus x_{iv}$, $M_8^* = h(VID_j^*||z||T_7)$ and checks if $M_8^* \stackrel{?}{=} M_8$. If yes the computes, $SK_{ID2} = h(z||UID||$
$VID_j||T_7)$. Now, $SK = SK_{NR} = SK_{ID2}$ shows that session key agreement and mutual authentication are successful. To put it succinctly, this archi-

| User/Gateway | | NMID |
|---|---|---|
| User input $ID_k^*, PW_k^*, B_k^*$ | | |
| Compute $\sigma_k^* = Rep(B_k^*, \tau_k^*)$, gets $\sigma_k^*$ | | |
| Compute $r_k^* = h(ID_k^*\|\|PW_k^*\|\|\sigma_k^*) \oplus \beta_k$ | | |
| $Q_k^* = h(PW_k^*\|\|\sigma_k^*\|\|r_k^*)$ | | |
| Checks $Q_k^* \stackrel{?}{=} Q_k$ | | |
| Then computes $z = h(PW_k\|\|\sigma_k) \oplus r_k$ | | |
| Gets $z$, further computes | | |
| $A = ID_k \oplus h(UID\|\|z)$ | | |
| $B = h(ID_k\|\|z) \oplus P_{pub}$ | | |
| $C = h(ID_k\|\|UID\|\|z\|\|T_1)$ | | |
| | $\xrightarrow{\{A,B,C,T_1\}}$ | |
| | | Checks $T_2 - T_1 \leq \delta T$ |
| | | Computes $ID_k^{**} = A \oplus h(UID\|\|z)$ |
| | | $C^* = h(ID_k^{**}\|\|UID\|\|z\|\|T_1)$ |
| | | checks $C^* \stackrel{?}{=} C$ |
| | | Further computes |
| | | $P_{pub} = h(ID_k^{**}\|\|z) \oplus B$ |
| | | Select $m \in Z_q^*$ (random nonce) |
| | | Computes $D = m \oplus h(UID\|\|z\|\|T_3)$ |
| | | $E = h(ID_k\|\|UID\|\|z\|\|m)$ |
| | | $SK_G = h(ID_k\|\|UID\|\|z.P_{pub}\|\|m)$ |
| | $\xleftarrow{\{D,E,T_3\}}$ | |
| Checks $T_4 - T_3 \leq \delta T$ | | |
| ,if yes then computes | | |
| $m^* = D \oplus h(UID\|\|z)$ | | |
| $E^* = h(ID_k\|\|UID\|\|z\|\|m^*)$ | | |
| checks $E^* \stackrel{?}{=} E$ | | |
| $SK_G = h(ID_k\|\|UID\|\|z.P_{pub}\|\|m)$ | | |

Fig. 6. Authentication and key agreement between the gateway and the nano micro interface device.

tecture describes how authentication may be built using current technology and methods. According to the studies [1,3], nano routers and micro interface devices can perform more calculations than nano-devices, which is exploited in the proposed algorithm above.

## VI. Security

This section shows that the proposed scheme satisfies the basic security requirements and is resistant to various attacks.

### A. Informal security analysis

- *Mutual authentication:* The provision of authentication in the IoNT network was the primary goal of this scheme's development. The discussion above makes it quite evident that mutual authentication occurs. Step 2 of the authentication process between the interface device and the gateway involves the interface device determining if $C^* \stackrel{?}{=} C$ authenticates the interface device. Moreover, the interface device is mutually authenticated in step three when the gateway determines if $E^* \stackrel{?}{=} E$. Similarly, in the authentication process involving interface devices, nano routers, and nano-devices, step 2 involves authenticating the interface device where the nano router verifies if $M_1^* \stackrel{?}{=} M_1$, and step 3 involves authentication of the nano router where the nano-devices check if $M_4^* \stackrel{?}{=} M_4$. All nano-devices that are present at the $v^{th}$ distance are authenticated in step 4, where the corresponding nano router checks if $M_7^* \stackrel{?}{=} M_7$. Finally, the nano router is mutually authenticated by NMID in step 5, where NMID computes $M_8^* \stackrel{?}{=} M_8$.
- *Session key agreement:* To ensure a secure connection, another crucial step is the creation of session keys. It can be seen that session keys have been created, and a session has been formed in both the key agreement steps. In step 3 of the first authentication phase, we see that $SK = SK_G = SK_{ID1}$ establishes a secure session between the gateway and the interface device. Furthermore, step 5 of the second authentication phase $SK = SK_{NR} = SK_{ID2}$ shows session key agreement.
- *Eavesdropping:* An attacker can intercept messages delivered across the communication channel. The one-way secure hash function and random nonce protect the messages conveyed in the communication channel, demon-

| NMID | NR | Nano-Devices |
|---|---|---|
| Select $x_{iv}$ from list and $u \in Z_q^*$<br>Computes<br>$M_1 = h(UID\|\|z\|\|u\|\|T_5)$,<br>$M_2 = z \oplus u$, $M_3 = z \oplus x_{iv}$<br>Send $\{M_1, M_2, M_3, T_5\}$ | | |
| $\xrightarrow{\{M_1, M_2, M_3, T_5\}}$ | | |
| | Checks $T_6 - T_5 \leq \delta T$<br>$x_{iv} = z \oplus M_3$<br>Checks $x_{iv}$ in list<br>Computes $u^* = z \oplus M_2$<br>$M_1^* = h(UID\|\|z\|\|u^*\|\|T_5)$<br>$M_1^* \stackrel{?}{=} M_1$<br>Computes<br>$M_4 = h(VID_j\|\|u^*)$,<br>$M_5 = u^* \oplus x_{iv}$ | |
| | $\xrightarrow{M_4, M_5}$ | |
| | | Computes<br>$u^{**} = H_5 \oplus x_{iv}$<br>$M_4^* = h(VID_j\|\|u^{**})$,<br>$M_4^* \stackrel{?}{=} M_4$<br>Computes<br>$M_6 = XID_i \oplus x_{iv}$,<br>$M_7 = h(XID_i\|\|u^{**})$<br>Send $\{M_6, M_7\}$ |
| | $\xleftarrow{M_6, M_7}$ | |
| | Computes<br>$XID_i^* = M_6 \oplus x_{iv}$,<br>$M_7^* = h(XID^*\|\|u^*)$<br>Checks $M_7^* \stackrel{?}{=} M_7$<br>Computes<br>$M_8 = h(VID_j\|\|z\|\|T_7)$,<br>$M_9 = VID_j \oplus x_{iv}$<br>$SK_{NR} = h(z\|\|UID\|\|VID_j\|\|T_7)$ | |
| $\xleftarrow{M_8, M_9, T_7}$ | | |
| Checks $T_8 - T_7 \leq \delta T$<br>Computes<br>$VID_j^* = M_9 \oplus x_{iv}$,<br>$M_8^* = h(VID_j^*\|\|z\|\|T_7)$<br>Checks $M_8^* \stackrel{?}{=} M_8$<br>$SK_{ID2} = h(z\|\|UID\|\|VID_j\|\|T_7)$ | | |

Fig. 7. Authentication and key agreement phase between nano-devices, nano routers, and the nano micro interface device.

strating the proposed scheme's resistance to eavesdropping. The introduction of an eavesdropping nano-device is hard if the attacker is unaware of the random nonce. Eavesdroppers won't be able to snoop on the conversation because all the nano-devices have been authenticated. Consequently, the proposed schemes are not prone to eavesdropping attacks.

- *Spoofing:* Another method an attacker can use to disrupt communication is spoofing nano-devices. An attacker can try to alter or replay the obtained data by spoofing. In the first authentication phase, we use random nonce $r_k$ and a one-way hash function that prevents spoofing of the gateway device or the nano micro interface device. Since mutual authentication occurs, all the devices involved in the communication are valid. Similarly, for spoofing the nano-devices or the nano routers in the second authentication phase, the attacker must know the random nonce u used to construct the messages and the value

of the distance's $x_{iv}$'s stored in the nano-devices must be known. Without prior knowledge of these values, it is very hard for the attacker to get hold of the confidential messages and spoof the devices. Ultimately, the proposed protocols are safe from spoofing attacks.

- *Known Session-Specific Temporary Information (KKSTI) Attack:* The attacker in this attack already knows the session's random numbers; thus, we can check whether or not our suggested protocols are secure. Since it is extremely difficult for an attacker to calculate $z.P_{pub}$ during the authentication phase between the gateway and NMID, the attacker won't be able to compute the session key even if the random number m is known. As a result, KSSTI attacks cannot be used against the suggested protocols.
- *Privileged insider attack:* An attacker may be a privileged server insider. As a result, the attacker can access the secret values needed to register the gateway. It is obvious that using a biometric and not sending $PW_k$ to the server in the registration phase prevents an attacker from obtaining the required data. Therefore, the suggested protocol is secure from privileged insider attacks.
- *Smart Device (Gateway) Stolen attack:* If the attacker steals the smart device, i.e., the gateway, all the information inside the smart device can be accessed by them. The values $(\beta_k, Q_k, \gamma_k, UID, e, P_k, \tau_k)$ will be obtained by the attacker. However, these encrypted values do not let the attacker penetrate the user's privacy and confidential details as a one-way hash function and random nonce $r_k$ are used. Also, we use biometrics whose secret value is also not known. Hence, meaningful information about the gateway or the user is inaccessible to the attacker.
- *DoS and DDoS Attack:* An attacker could attempt to inundate the IoNT network with malicious nodes, resulting in a denial-of-service attack. DDoS attacks would also result from simultaneous attacks from a significant number of devices. For example, suppose the attacker sends a lot of messages to NMID requesting authentication. In that case, NMID won't accept them since the attacker will not know the parameter $z$ and the requests will be denied when $C^* \stackrel{?}{=} C$. Hence in the first authentication phase, these attacks are not possible. Again, if an attacker successfully inserts malicious nodes into the nano network, the security parameter $z$ would prevent the malicious nodes from establishing authentication, preventing these attacks in the second authentication phase.
- *Replay Attack:* Fresh timestamps $T_1$ and $T_3$ are used in the first authentication phase by both the Gateway and NMID, respectively, and the NMID generates a random nonce $m \in Z_q^*$. In the proposed scheme, each time an entity gets a message, it verifies the validity of the timestamps and random nonce. As a result, the adversary will be unable to execute a replay attack. In the same way, the use of a random nonce, $u$, and fresh timestamps, $T_5$ and $T_7$, prevents an adversary from conducting a replay attack on the second authentication scheme. Hence, the proposed scheme is resistant to replay attacks.

TABLE III
NOTATION OF BAN LOGIC.

| Symbols | Description |
|---|---|
| $q_1, q_2$ | Two principals |
| $w_1, w_2$ | Two statements |
| $SK$ | The session key |
| $q_1 \mid \equiv w_1$ | $q_1$ believes $w_1$ |
| $q_1 \mid \backsim w_1$ | $q_1$ once said $w_1$ |
| $q_1 \Rightarrow w_1$ | $q_1$ controls $w_1$ |
| $q_1 \lhd w_1$ | $q_1$ receives $w_1$ |
| $\#w_1$ | $w_1$ is fresh |
| $(w_1)_K$ | $w_1$ is encrypted with $K$ |
| $q_1 \stackrel{SK}{\longleftrightarrow} q_2$ | $q_1$ and $q_2$ have a shared key $SK$ |

## B. BAN Logic Analysis

This section gives BAN logic [27] of the proposed authentication protocol (i.e., the first authentication protocol between the gateway and the nano micro interface device). It is a type of formal analysis that assists in confirming the accuracy of an authentication procedure. The notations used in the proof are included in the following Table III, along with their definitions.

1) LOGICAL POSTULATES:
   - Message meaning rule (MMR): $\frac{q_1 \mid \equiv q_1 \leftrightarrow q_2, q_1 \lhd (w_1)_K}{q_1 \mid \equiv q_2 \mid w_1}$
   - Nonce verification rule (NVR): $\frac{q_1 \mid \equiv \#(w_1), q_1 \mid \equiv q_2 \mid \backsim w_1}{q_1 \mid \equiv q_2 \mid \equiv w_1}$
   - Jurisdiction rule (JR): $\frac{q_1 \mid \equiv q_2 \Rightarrow w_1, q_1 \mid \equiv q_2 \mid \equiv w_1}{q_1 \mid \equiv w_1}$
   - Belief rule (BR): $\frac{q_1 \mid \equiv (w_1, w_2)}{q_1 \mid \equiv w_1}$
   - Freshness rule (FR): $\frac{q_1 \mid \equiv \# w_1}{q_1 \mid \equiv \#(w_1, w_2)}$
2) OBJECTIVE: The following objectives have been identified to establish the effectiveness of our protocol:
   a) Goal 1: G $\mid \equiv (G \stackrel{SK}{\longleftrightarrow} NMID)$
   b) Goal 2: G $\mid \equiv NMID \mid \equiv (G \stackrel{SK}{\longleftrightarrow} NMID)$
   c) Goal 3: NMID $\mid \equiv (G \stackrel{SK}{\longleftrightarrow} NMID)$
   d) Goal 4: NMID $\mid \equiv G \mid \equiv (G \stackrel{SK}{\longleftrightarrow} NMID)$
3) ASSUMPTIONS: Our BAN Logic protocol relies on the following assumptions:
   - $A_1 : NMID \mid \equiv \#(T_1)$
   - $A_2 : G \mid \equiv \#(T_3)$
   - $A_3 : G \mid \equiv NMID \Rightarrow (G \stackrel{SK}{\longleftrightarrow} NMID)$
   - $A_4 : NMID \mid \equiv G \Rightarrow (G \stackrel{SK}{\longleftrightarrow} NMID)$
   - $A_5 : G \mid \equiv G \stackrel{z}{\leftrightarrow} NMID$
   - $A_6 : NMID \mid \equiv G \stackrel{z}{\leftrightarrow} NMID$
4) IDEALIZED FORMS: Based on BAN logic, the idealized forms of our protocol can be described as follows:
$$M_1 : G \rightarrow NMID : (ID_k, P_{pub}, T_1)_z$$
$$M_2 : NMID \rightarrow G : (UID, m, T_3)_z$$
5) BAN LOGIC PROOF: We implement the BAN logic analysis of our protocol as follows:
   - Step 1: NMID receives $M_1$
$$S_1 : NMID \lhd (ID_k, P_{pub}, T_1)_z$$
   - Step 2: Applying MMR rule using $S_1$ and $A_6$
$$S_2 : NMID \mid \equiv G \mid \backsim (ID_k, P_{pub}, T_1)$$

TABLE IV
DESCRIPTIONS OF QUERIES USED IN THE ROR MODEL

| Query | Description |
|---|---|
| $Execute(R_{N_m}^{t1}, R_{G_n}^{t2})$ | This query enables the adversary to interfere with the messages transmitted between the nodes $R_{N_m}^{t1}$ and $R_{G_n}^{t2}$ through the public channel. |
| $Reveal(R^t)$ | This query enables the adversary to obtain the current session key $SK_{mn}$. |
| $CorruptD_n$ $(R_{G_n}^{t2})$ | The adversary can use this query to access $D_n$ of $R_{O_n}^{t2}$ to extract any stored information. |
| $Test(R^t)$ | This query involves flipping a coin say $b$. After executing the $Test$ query $(R^t)$, $(R^t)$ receives a random number when $b = 0$ and a session key $SK_{mn}$ when $b = 1$, or null () otherwise. If the adversary cannot differentiate between the random number and the session key, we can ensure that our scheme protects the session key. |
| $Send(R^t, message)$ | The adversary can use this query to send a request message to other participants and receive the response message. |

- Step 3: Applying FR using $M_1$ and $A_1$
$$S_3 : NMID| \equiv \#(ID_k, P_{pub}, T_1)$$
- Step 4: Applying NVR using $S_2$ and $S_3$
$$S_4 : NMID| \equiv G| \equiv (ID_k, P_{pub}, T_1)$$
- Step 5: Applying BR using $S_4$
$$S_5 : NMID| \equiv (ID_k, P_{pub})$$
- Step 6: NMID can calculate the session key $SK = h(ID_k$ $||UID||z.P_{pub}||m)$
$$S_6 : NMID| \equiv G| \equiv (G \overset{SK}{\longleftrightarrow} NMID)$$ (Goal 4)
- Step 7: Applying JR using $A_4$ and $S_6$
$$S_7 : NMID| \equiv (G \overset{SK}{\longleftrightarrow} NMID)$$ (Goal 3)
- Step 8: G receives $M_2$
$$S_8 : G \lhd (UID, m, T_3)_z$$
- Step 9: Applying MMR rule using $S_8$ and $A_5$
$$S_9 : G| \equiv NMID| \backsim (UID, m, T_3)$$
- Step 10: Applying FR using $M_2$ and $A_2$
$$S_{10} : G| \equiv \#(UID, m, T_3)$$
- Step 11: Applying NVR using $S_9$ and $S_{10}$
$$S_{11} : G| \equiv NMID| \equiv (UID, m, T_3)$$
- Step 12: Applying BR using $S_{11}$
$$S_{12} : NMID| \equiv (m, UID)$$
- Step 13: G can calculate session key $SK = h(ID_k||$ $UID||z.P_{pub}||m)$
$$S_{13} : G| \equiv NMID| \equiv (G \overset{SK}{\longleftrightarrow} NMID)$$ (Goal 2)
- Step 14: Applying JR using $A_3$ and $S_{13}$
$$S_{14} : G| \equiv (G \overset{SK}{\longleftrightarrow} NMID)$$ (Goal 1)

### C. Formal security proof using ROR model

As demonstrated in various recent studies [26], [36], [37], the ROR model is a popular method demonstrating the security of various authentication protocols. This section will use the ROR model to assess the proposed framework's session key security. We see that in the proposed scheme $N_{D_m}^{t_1}$ and $G_{w_n}^{t_2}$ are participants acting as $m^{th}$ NMID and $n^{th}$ Gateway. Here, $t_i$ represents the NMID instance. Under the ROR model, an attacker can execute different security attacks using queries such as $Execute$, $Test$, $Send$, and $Corrupt\mathscr{D}_s$. These queries enable the attacker to carry out a range of malicious activities. Table IV provides a detailed description of the various queries.

*1) Security Proof:*

**Theorem VI.1.** *$Adv_s(t)$ denotes the probability of successfully breaking the session key security of the proposed scheme within polynomial time $t$. The resulting expression is:*

$$Adv_s(t) \leq \frac{q_{hash}^2}{|Hash|} + \frac{q_s}{2^{l-1}|D_p|} + 2Adv_s^{ECDHP}(t)$$

*Here, $q_s$ and $q_{hash}$ are the numbers of send and hash queries, respectively, $|Hash|$ represents the range space of the hash function, $D_p$ denotes the size of the password dictionary, $l$ represents the number of bits of biometric information, and $Adv_s^{ECDHP}(t)$ is the adversary's advantage to break ECDHP.*

*Proof.* We divided the formal proof into five games, denoted by $G_j$, where $j = 1, 2, 3, 4, 5$. We will use $S_{cadv,j}$ to represent the probability of the adversary winning game $G_j$, and $Probs[S_{cadv,j}]$ to denote the advantage of $S_{cadv,j}$. The proof proceeds by defining the specific steps of each game as follows.

- $\mathcal{G}_1$: Game $\mathcal{G}_1$ simulates an attack scenario in which the protocol is running under real conditions. The adversary is not allowed to conduct any queries and has no access to any information. Thus, the adversary randomly selects a bit $b$. The security of $SK$ is guaranteed by our protocol's ability to achieve semantic security through random bit guessing.

$$Adv_s(t) = |2Prob_s[Sc_1^{adv}] - 1| \quad (1)$$

- $\mathcal{G}_2$ : In game $\mathcal{G}2$, the adversary performs an eavesdropping attack by first executing the $Execute(RU_r{}^{t1}, R_{G_n}^{t2})$ query and then intercepting the transmitted messages $A, B, C, T_1$ and $N_n, G_n, T_2$. The adversary then uses the $Test(R^t)$ query to determine whether the returned result is $SK_{mn}$ or not. Computing $SK_{mn}$ requires the secret values $N_{mn}$ and $N_{mn}$, as well as the computed values $UID_m$, $UID_n$ and $T_2$. Since the adversary is unable to access the required values to compute $SK_{mn}$, their probability of winning in-game $\mathcal{G}2$ is the same as in-game $\mathcal{G}1$. This means that the security of $SK_{mn}$ is maintained even under an eavesdropping attack. In other words, the fact that the adversary cannot obtain the secret values necessary to compute $SK_{mn}$ ensures that their success probability in $\mathcal{G}2$ is no different than their probability of winning in

$\mathcal{G}1$. So,

$$Prob_s[Sc_1^{adv}] = Prob_s[Sc_2^{adv}] \tag{2}$$

- $\mathcal{G}_3$ : The adversary can compute $SK_{mn}$ by using both $Hash$ and $Send$ queries, as well as the transmitted messages $A, B, C, T_1$. However, since these messages are protected by random numbers $N_m$, $N_m$, and hash functions, the adversary must find a hash collision to calculate $SK_{mn}$. This can be achieved using the birthday paradox.

$$|Prob_s[Sc_3^{adv}] - Prob_s[Sc_2^{adv}]| \leq \frac{Q_{hash}^2}{2|Hash|} \tag{3}$$

- $\mathcal{G}_4$ : In $\mathcal{G}4$, the adversary uses a $Corruptdn(R_{G_n}^{t2})$ query to try to obtain $Sk_{rs}$. By employing a power analysis attack, the adversary can extract the secret credentials $D, G, T_1$ from the SC memory in $\mathcal{G}4$. Here, $C^* = h(ID^{**}k||UID||z||T_1)$, and $P_{pub} = h(ID^{**}k||z) \oplus B$. To compute $SKmn$, the adversary needs $ID_n$, $PW_n$, $B_n$, and random numbers. Using the password dictionary and bio-metric information of $n$ bits, the adversary can attempt to guess the values used to compute $Sk_{mn}$. Therefore, we can conclude that the adversary's ability to guess correctly determines their probability of winning in $\mathcal{G}_4$. Hence, we have

$$|Prob_s[Sc_4^{adv}] - Prob_s[Sc_3^{adv}]| \leq \frac{Q_s}{2^l|d_p|} \tag{4}$$

- $G_5$ :The adversary can use $D, G, T_3$ messages and $N_m$ to compute $SK_{mn}$, but they cannot compute $N_{mn}$ as both parameters' security is based on ECDHP. As a result, we can conclude that:

$$|Prob_s[Sc_5^{adv}] - Prob_s[Sc_4^{adv}]| \leq Adv_s^{ECDHP}(t). \tag{5}$$

Through the usage of the $Test(R^t)$ query, the adversary tries to identify the appropriate bit $b$ that would lead to their victory in the game. Consequently, we obtain the following result:

$$Prob_s[Sc_5^{adv}] = \frac{1}{2} \tag{6}$$

By merging equations (1), (2), and (6), we arrive at the following result:

$$\begin{aligned} \frac{1}{2}Adv_s(t) &= |Prob_s[Sc_1^{adv}] - \frac{1}{2}| \\ &= |Prob_s[Sc_2^{adv}] - \frac{1}{2}| \\ &= |Prob_s[Sc_2^{adv}] - Prob_s[Sc_5^{adv}]| \end{aligned} \tag{7}$$

Additionally, by applying the triangular inequality, we can convert equations (3), (4), (5), and (7) into the following form:

$$\begin{aligned} |Prob_s[Sc_2^{adv}] - Prob_s[Sc_5^{adv}]| &\leq |Prob_s[Sc_2^{adv}] \\ -Prob_s[Sc_4^{adv}]| + |Prob_s[Sc_4^{adv}] &- Prob_s[Sc_5^{adv}]| \\ \leq |Prob_s[Sc_2^{adv}] - Prob_s[Sc_3^{adv}]| &+ |Prob_s[Sc_3^{adv}] \\ -Prob_s[Sc_4^{adv}]| + |Prob_s[Sc_4^{adv}] &- Prob_s[Sc_5^{adv}]| \\ \leq \frac{q_{hash}^2}{2|Hash|} + \frac{q_s}{2^l|D_p|} &+ Adv_s^{ECDHP}(t). \end{aligned} \tag{8}$$

Thus, by merging equations (7) and (8), we get the following result:

$$Adv_s(t) \leq \frac{q_{hash}^2}{|Hash|} + \frac{q_s}{2^{l-1}|D_p|} + 2Adv_s^{ECDHP}(t) \tag{9}$$

□

### D. Formal Security Analysis Using AVISPA

AVISPA [38] is a tool for formally designing, evaluating and validating the security features of networking protocols. It has four distinct test backends that enable the use of various protocol analysis techniques [39].

- Control-Logic-based Attack Searcher (CL-AtSe)
  This backend tool employs a constraint logic programming method to find security issues in the protocol. CL-AtSe examines the protocol as a collection of constraints for inconsistencies or breaches of security standards [40].
- SAT-based Model-Checker (SATMC)
  This backend tool employs a symbolic model-checking approach to verify the validity of the protocol. SATMC develops logical formulae representing the protocol, which it then solves to check for errors or vulnerabilities.
- On-the-Fly Model-Checker (OFMC)
  The OFMC backend tool verifies the protocol's correctness using a finite model checking approach, and it leverages numerous coding strategies to illustrate the work for detecting protocol falsification and verification for an unlimited number of sessions as needed [41].
- Tree Automata-based Protocol Analyzer (TA4SP)
  For infinite sessions, TA4SP measures intrusion knowledge using popular tree languages to validate the security features.

In this paper, we used an OFMC backend, which provides the XOR operation, to simulate the proposed system using AVISPA. The suggested technique can thwart replay and MITM attacks if the SUMMARY portion of OF is SAFE.

*1) HLPSL Codes of The Proposed Scheme:* We use the HLPSL programming language in this section to implement the suggested protocol for the core Gateway and NMID operations. Fig. 8 provides an illustration of how the environment and the session work. Kindly note that the session's role includes declarations for all essential roles and channels. Next, given the context of the environment, we define the invader knowledge, secrecy goals, and authentication goals. Last, we list every constant and variable used in the programs.

TABLE V
SIMUATION PARAMETERS.

| General Parameters | Value |
|---|---|
| Simulation Time | 5s |
| Number of seeds | 5 |
| Artery size | 30 mm $\times$ 1 mm $\times$ 1 mm |
| Number of Nano Devices | $[4, 8, 12, 16, 20]$ |
| Number of Nano Routers | $[2, 4, 6, 8]$ |
| Number of Nano-Micro Interface Devices | 1 |
| Details related to electromagnetic-based communication channel | |
| Packet Size | 128 Bytes |
| Nano Routers communication range | 4.5 mm, 4 mm, 3.6 mm,3.17 mm, 2.52 mm |
| Nano-Micro Interface Device communication range | 4.5 mm |
| Physical transmission range | 10 bps, 10 kbps, 10 Mbps, 10 Gbps, and 10 Tbps |
| Time required to perform cryptographic operations | $10^3, 10^4$ $ns$ |
| Pulse Energy | 100 pJ |
| Pulse Duration | 100 fs |
| Packet Generation time interval | 0.1 s |
| Modulation Scheme | TS-OOK |
| Details related to the molecular communication channel | |
| Modulation scheme | OOK |
| Nano-devices communication range | 0.02 nm |
| Diffusion coefficient | 1.0 $nm^2/ns$ |
| Packet generation time interval in the molecular channel | 0.5s |
| Brownian motion factor | 0.5 |
| Inertia factor | 0.5 |

```
%%%% Role Session %%%%
role session (Gateway,NMID:agent,z,Ppub:symmetric_key,H,ADD,MUL:hash func)
def=
local TN1, TN2,SV1,SV2:channel(dy)
composition
Gateway(Gateway,NMID,z,Ppub,H,ADD,MUL,TN1,SV1)
/\NMID(ateway,NMID,z,Ppub,H,ADD,MULTN2,SV2)
end role

%%%% Role environment %%%%
role environment()
def=
const Gateway,NMID:agent,z,Ppub,:symmetric_key,H,ADD,MUL:hash func IDk,PWk,Bk,ok,rk,Qk,A,B,C,Tk,T1,T2,T3,T4,mk,m1,m2,E,:text,

Sp1,Sp2,Sp3,Sp4,Gateway_NMID_m1,Gateway_NMID_m2:protocal id

intruder knowledge (Gateway,NMID,ok,rk,Qk,m,T1,T3,h,add mul)
composition
session(Gateway,NMID,z,Ppub,H,ADD,MUL)
/\session(k,NMID,z,Ppub,H,ADD,MUL)
/\session(Gateway,k,z,Ppub,H,ADD,MUL)
end role

%%%% goal %%%%
goal
secrecy of Sp1,Sp2,Sp3,Sp4
authentication on Gateway_NMID_m1,
authentication on Gateway_NMID_m2,
end goal
environment()
```

Fig. 8. Role of Session, Environment, and Goal.

```
% OFMC
% Version of 2016/04/13
SUMMARY
 SAFE

DETAILS
BOUND_NUMBER_OF_SESSIONS

PROTOCOL
/home/span/span/testsuite/results/OUTER(IONT).if

GOAL
as specified BACKEND

BACKEND
 OFMC
COMMENTS
STATISTICS
parseTime: 0.005
searchTime: 1.80s
visitedNodes: 128 nodes depth: Splies
depth:4 piles
```

Fig. 9. Simulation results.

*2) AVISPA Simulation Results:* Fig. 9 displays the OF for the suggested design produced after using the OFMC backend. The suggested scheme can prevent replay and MITM attacks because the Summarized parts are SAFE.

## VII. PERFORMANCE ANALYSIS

Assessing the efficacy of any system or application requires a critical component: performance evaluation. Therefore, in this section, we comprehensively evaluate the proposed method's performance, analyzing its efficiency and effectiveness. Hence, the computational and communication, as well as obtained results, have been discussed. Furthermore, a comparative analysis between our scheme and other schemes within the IoT environment has been provided. It is important to highlight that our authentication scheme is pioneering within the IoNT paradigm. Consequently, there is no existing scheme (to the best of our knowledge) within this field that can be directly compared regarding computation and communication costs. Nevertheless, as IoNT is an extension of the IoT concept, we have included a comparative analysis to enhance comprehension. Considering the foundational relationship between IoNT and IoT, the included comparative analysis aims to provide a broader perspective on computation and communication costs. Lastly, we examine the consequences of our findings about the viability and efficacy of our suggested approach.

### A. Computational cost analysis

The computational cost analysis for the login, authentication, and key agreement phases is described here. The remaining phases should be taken into account for the study

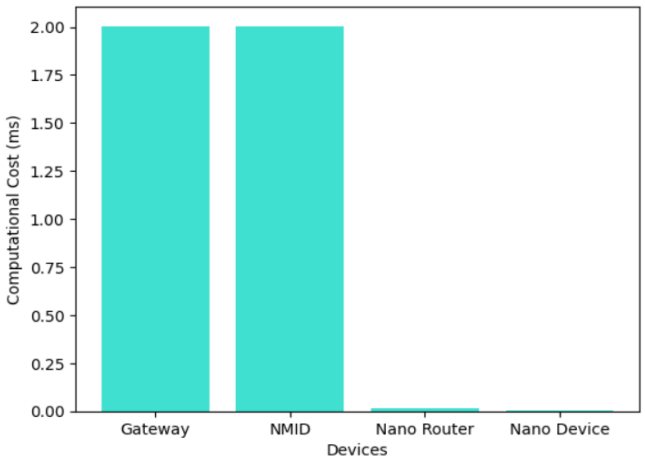



Fig. 10. Comparison of Computational Costs of Devices.

because they are only executed once and not often. Considering that there are two authentication phases for various devices, the computational cost for each is shown individually. The consumption time of the one-way hash function, symmetric key encryption/decryption, fuzzy extractor, and elliptic curve scalar multiplication operation are denoted as $T_H$, $T_{e/d}$, $T_F$, and $T_{ECCM}$, respectively. Further according to [26], each time is defined as $T_H = 0.0026ms$, $T_{e/d} = 8.7ms$, $T_F = 1.989ms$ and $T_{ECCM} = 1.989ms$. In the first authentication phase, the login of the gateway consumes $T_F + 6T_H$, and the authentication consumes $3T_H + 1T_{ECCM}$. The total computational operations consumed by the entire phase is $T_F + T_{ECCM} + 9T_H$ , approximately $4.0014ms$. Further, in the second authentication phase, NMID consumes $3T_H$, NR consumes $5T_H$, and the nano-devices consume $2T_H$. The total computational operations consumed by the entire phase is $10T_H$, approximately $0.026ms$ to carry out this phase. Consequently, the entire login, authentication, and key agreement phase consumes $T_F + T_{ECCM} + 19T_H$ approximately $4.0274ms$.

Fig. 10 shows the comparison between the computational cost of each entity of the proposed IoNT network. As stated in section III-B, the gateway and NMID have a greater computational capability than that of nano routers and devices. After analyzing the computational costs of each device independently, Fig. 10 clearly demonstrates that the gateway and NMID consume the same amount of time, while nano-routers consume significantly less time, and nano-devices consume the least amount of time to complete cryptographic operations.

The computational costs of the methods discussed in [42]–[47], as well as our proposed scheme, have been summarized in Table VI. The computational cost of our proposed scheme is determined by the cumulative costs incurred in two distinct phases. As illustrated in Figure 11, it is evident that despite involving costs from two phases, our scheme's computational cost remains lower compared to the other schemes under consideration. Our approach is computationally efficient and maintains comprehensive security measures without compromising our steadfast commitment to safety. This observation is noteworthy and highlights the effectiveness of our method.

TABLE VI
COMPARISON TABLE OF COMPUTATIONAL COST

| Protocols | First Phase $(ms)$ | Second Phase $(ms)$ |
|---|---|---|
| [42] | $8T_{e/d} + 20T_H \approx 71.012$ | - |
| [43] | $2T_{e/d} + 20T_H \approx 17.792$ | - |
| [44] | $10T_{e/d} + 18T_H \approx 88.7468$ | - |
| [45] | $9T_{e/d} + 7T_H \approx 62.1134$ | - |
| [46] | $17T_{ECCM} + 18T_H \approx 13.9698$ | - |
| [47] | $15T_{ECCM} + 18T_H \approx 29.8818$ | - |
| Proposed | $T_F + T_{ECCM} + 9T_H \approx 4.0014$ | $10T_H \approx 0.026$ |

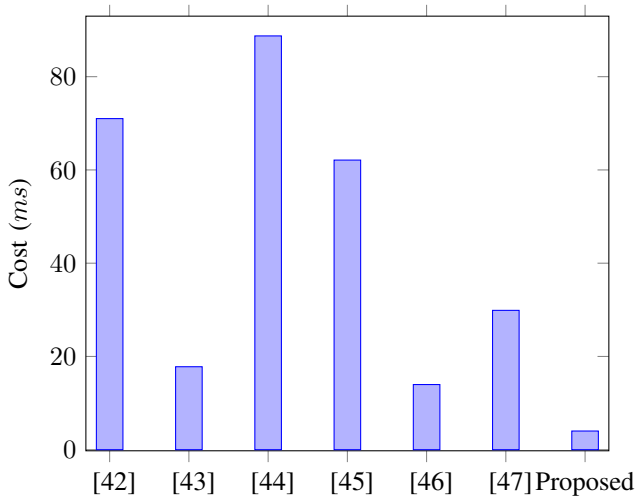



Fig. 11. Comparison based on Computational costs (in $ms$).

### B. Communication cost analysis

This section evaluates the communication cost for the different components or entities in the system and assesses the resources required for this communication. Referring to [25], [47], the length of identity is considered to be 128 bits. Further, 256 bits is the length of the elliptic curve point, and the one-way hash output, random nonce, encryption/decryption and timestamp lengths are considered to be 256, 256, 128 and 32 bits, respectively. So, in the proposed scheme, the messages exchanged in the public channel are $\{A, B, C, T_1\}$, $\{D, E, T_3\}$, $\{M_1, M_2, M_3, T_5\}$, $\{M_4, M_5\}$, $\{M_6, M_7\}$ and $\{M_8, M_9, T_7\}$. Hence corresponding to these messages, the communication costs are $[ID_k \approx 128$, $B \approx 256$, $C \approx 256$, $T_1 \approx 32]$ = 128+256+256+32, $[m \approx 256$, $E \approx 128$, $T_3 \approx 32]$ =256+128+32, $[UID \approx 128$, $M_2 \approx 256$, $M_3 \approx 256$, $T_5 \approx 32]$ = 128+256+256+32, $[VID_j \approx 128$, $M_5 \approx 256]$ = 128+256, $[XID \approx 128$, $M_7 \approx 256]$ = 128+256 and $[M_8 \approx 256$, $VID_j \approx 128$, $T_7 \approx 32]$ = 256+128+32, i.e., for the messages $\{A, B, C, T_1\}$ the cost is 672 bits, $\{D, E, T_3\}$ is 416 bits, $\{M_1, M_2, M_3, T_5\}$ is 672 bits,$\{M_4, M_5\}$ is 384 bits $\{M_6, M_7\}$ is 384 bits and $\{M_8, M_9, T_7\}$ is 416 bits.

The communication costs of the schemes [42]–[47] and the proposed scheme are summarized in Table VII. Furthermore, it is evident from Figure 12 that the communication costs of the proposed scheme, encompassing two components, are lower than those of the schemes [46], [47], and higher than those of the schemes [42]–[45]. However, it's worth noting that the scheme [42] is vulnerable to desynchronization attacks, [43]

TABLE VII
COMPARISON TABLE OF COMMUNICATION COST

| Protocols | First Phase (in bits) | Second Phase (in bits) |
|---|---|---|
| [42] | 640 + 1280 + 512 = 2432 | - |
| [43] | 1088 + 576 + 416 = 2080 | - |
| [44] | 320 + 160 + 288 = 768 | - |
| [45] | 160 + 160 + 288 = 608 | - |
| [46] | 1536 + 800 + 800 = 3168 | - |
| [47] | 1600 + 800 + 1056 = 3456 | - |
| Proposed | 672 + 416 = 1088 | 672 + 384 + 384 + 416 = 1856 |

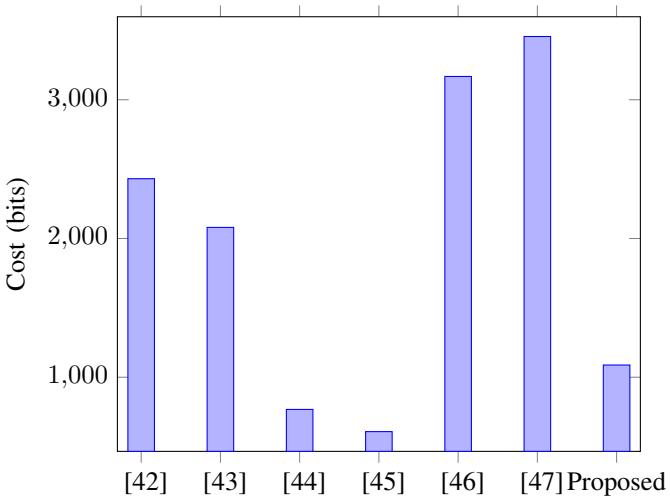



Fig. 12. Comparison based on communication cost (in bits).

is susceptible to MITM and perfect forward and backward secrecy attacks, [44] is prone to replay attacks, and [45] is exposed to offline guessing and node capture attacks. Thus, even though these schemes exhibit lower communication costs, they lack the requisite security measures. Consequently, our proposed scheme offers improved security alongside manageable communication overheads.

### C. Performance analysis of Nano network

This section contains a study of the performance of a nano-network. As stated in section III-B, nano routers and NMID execute more tasks as compared to nano-devices. To authenticate all these devices, secure messages are constructed which involve cryptographic operations. Thus, the entire authentication process leads to computation and communication overheads. Without adopting a security mechanism, in [19], the packet size is set to 128 bytes. Since this packet size is the sensing data that has to be communicated. As the proposed scheme aims to authenticate the devices after which this data has to be sent, there is no exchange of this data during authentication. From the above section, it can be seen that the byte size of the messages constructed is comparable with the available literature. Hence the packet size is set to 128 bytes.

We employ a hybrid strategy for communication in the nano network, as was indicated in section III. *Nano-Sim* [19], [23] tool, integrated with NS-3 simulation framework, is used to model electromagnetic wave communications generated in the terahertz band. Also, *N3Sim* [24] is used to simulate molecular communications.

Despite recent developments in IoNT, evaluating the behavior of this network is difficult. The scheme presented here strives to examine the behavior of the nano-network in accordance with existing scientific literature.

*1) Implemented scenario and parameter settings:* In line with [4], [19], the proposed IoNT network is applicable in the medical environment. So we have considered the IoNT network placed in the artery of the arm where the network contains a substantial number of nano-devices, nano routers, and one nano micro-interface device. We consider 30 mm long arteries with a diameter of 1 mm as in [4]. Nano routers are evenly dispersed in the constrained environment corresponding to respective nano-devices. These routers transmit data to NMID, which then employs IEEE 802.11 wireless technology to transmit the sensitive data to the Gateway device.

*Nano-Sim* is used to model the communications among the nano routers and NMID based on the exchange of electromagnetic waves in the terahertz band. The simulation settings shown in Table V are considered based on available literature. As suggested in [4], the values used have no negative effects on the human body and allow the transmission of signals through the blood. We employ data speeds of 10 bps, 10 kbps, 10 Mbps, 10 Gbps, and 10 Tbps, which are permissible by nano-scale communications based on the interchange of electromagnetic waves. Then, for each of the predicted data rates, a specified maximum communication range is considered: 4.5 mm, 4 mm, 3.6 mm, 3.17 mm, and 2.52 mm. This is done by considering the propagation models presented in [22] and the propagation of electromagnetic waves in the blood. The time required to perform the cryptographic operations is set as $[10^3, 10^4]$ $ns$ because the computation cost computed above lies around these values.

Further, the protocol suite used for electromagnetic-based communication includes two main protocols:

Transparent MAC for the data-link protocol and selective flooding for the routing protocol. These protocols have already been implemented in Nano-Sim. Transparent MAC assumes that packets sent from the network layer to the physical interface are transmitted without additional control at the data-link level, such as channel sensing. This means packets are sent directly to the physical layer without checking whether the channel is free. On the other hand, selective flooding assumes that packets are sent to all devices within the communication range of the sender. In other words, the packets are broadcasted to all devices but only the targeted device will accept and process the packet and the others will ignore them.

N3Sim is the simulation tool used to study the propagation of information between nano-devices and nano-routers using molecular communication within the human body. The simulation considers collisions between emitted particles and an inertia factor of 0.5, which is relevant for the human body. The packet generation time interval for nano-routers is set to 0.5 seconds, which is longer than the packet generation time interval for nano-devices. The diffusion coefficient is set to 1.0 $nm^2/ns$ or similar to the value calculated for ionic calcium in the cytoplasm. The motion of the nano-devices is

also considered, modeled by Brownian motion, which allows us to observe the effect of molecule interactions. The factor for Brownian motion is set to 1, not exceeding 25% of the distance between the emitter and receiver. Finally, N3Sim uses On-Off Keying (OOK) pulses, which provide a larger range in broadcast communication than other methods. A summary of these parameter settings can be found in Table V.

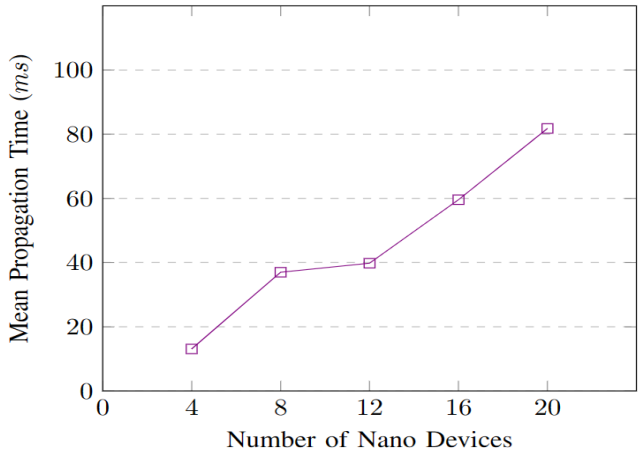



Fig. 13. Mean Propagation Time in Molecular Communications.

### D. Obtained Results

The packet loss ratio is measured, which shows the performance of the electromagnetic-based communication paradigm. The percentage of packets that are not received by NMID and, consequently, by the smart device is indicated by the packet loss ratio. Since the nano-devices communicate through molecular communications, their performance is evaluated in terms of the time required to propagate the constructed authentication messages.

*1) Packet Loss Ratio:* The packet loss ratio is shown in Fig. 14. However, almost similar findings to [4] were achieved. The graphs demonstrate that the packet loss percentage falls as the transmission rate lowers. As a result, the nano router's communication range increases. This results in the formation of multi-hop pathways between nano-routers and NMID, improving the likelihood of efficiently transferring data generated by the nano routers to NMID. The amount of time consumed in conducting cryptographic operations and the density of nano routers have no substantial effect on the packet loss ratio. Thus, molecular communication does not affect the packet loss ratio.

*2) Average amount of time required for propagation of authentication messages through molecular communications: N3Sim* simulates instances with a variable number of transmitters and receivers. This allows simulations to be performed in which molecular information is transmitted from a single transmitter to a large number of receivers. Fig. 13 depicts the average time required to exchange messages through the molecular-based communication channel. The behavior of nano-devices is observed when the parameter settings are put in accordance with Table V. Since communication latencies are not discovered in Section VI-C, we do not make any comparisons with the delay caused by molecular communication due to diffusion. There are still a lot of simulation results to be obtained in this state of work which would provide concrete evidence for an efficient work model in the IoNT environment.

## VIII. Conclusion

This paper proposed an authentication and key agreement scheme for the IoNT network. The authentication procedure is partitioned into two halves, one designed with lightweight methods and the other with a different approach than conventional ones. In addition, a hybrid method was employed to facilitate communication across the IoNT network's components, utilizing the various IoNT communication protocols available in the literature. The proposed approach resolves and safeguards the IoNT network's security challenges by implementing a secure authentication and key agreement mechanism between the devices. The formal and informal security analyses assess the security strength of the suggested protocol. The BAN logic and the ROR model validate the correctness of the proposed mechanism. The AVISPA simulation also demonstrates the practicality and dependability of the suggested authentication mechanism in improving system security. Furthermore, the comparative analysis illustrates that the scheme incurs minimal communication and computation overheads, all while ensuring robust security measures. Results from simulations using the Nano-Sim and N3-Sim tools provided useful information for assessing the efficacy of the proposed work in the context of the IoNT. As the IoNT grows, there will be an increasing need for secure authentication and signatures to protect the network from unauthorized access. One potential future scope for authentication in the IoNT is the development of biometric authentication methods that can be integrated into tiny devices. Also, the future of authentication in the IoNT will likely involve advanced security measures to ensure the integrity and security of the network. Future directions that could be investigated to ensure the safe and secure operation of the IoNT while preserving people's right to privacy include advancements in quantum and post-quantum-based cryptography, blockchain-based solutions, edge and fog computing, artificial intelligence-based security, and interdisciplinary research (such as biochemical cryptography).

## References

[1] Y. Perwej, M. K. Omer, O. E. Sheta, H. A. M. Harb, and M. S. Adrees, "The future of internet of things (iot) and its empowering technology," *International Journal of Engineering Science*, vol. 20192, 2019.
[2] Y. Perwej, K. Haq, F. Parwej, M. Mumdouh, and M. Hassan, "The internet of things (iot) and its application domains," *International Journal of Computer Applications*, vol. 975, no. 8887, p. 182, 2019.
[3] I. F. Akyildiz and J. M. Jornet, "The internet of nano-things," *IEEE Wireless Communications*, vol. 17, no. 6, pp. 58–63, 2010.
[4] S. Sicari, A. Rizzardi, G. Piro, A. Coen-Porisini, and L. A. Grieco, "Beyond the smart things: Towards the definition and the performance assessment of a secure architecture for the internet of nano-things," *Computer Networks*, vol. 162, p. 106856, 2019.
[5] M. M. Shetty and D. Manjaiah, "Challenges, issues and applications of internet of things," in *Internet of Things: Novel Advances and Envisioned Applications*. Springer, 2017, pp. 231–243.
[6] S. Malik, K. Muhammad, and Y. Waheed, "Nanotechnology: A revolution in modern industry," *Molecules*, vol. 28, no. 2, p. 661, 2023.
[7] A. Nikhat and P. Yusuf, "The internet of nano things (iont) existing state and future prospects," *GSC Advanced Research and Reviews*, vol. 5, no. 2, pp. 131–150, 2020.

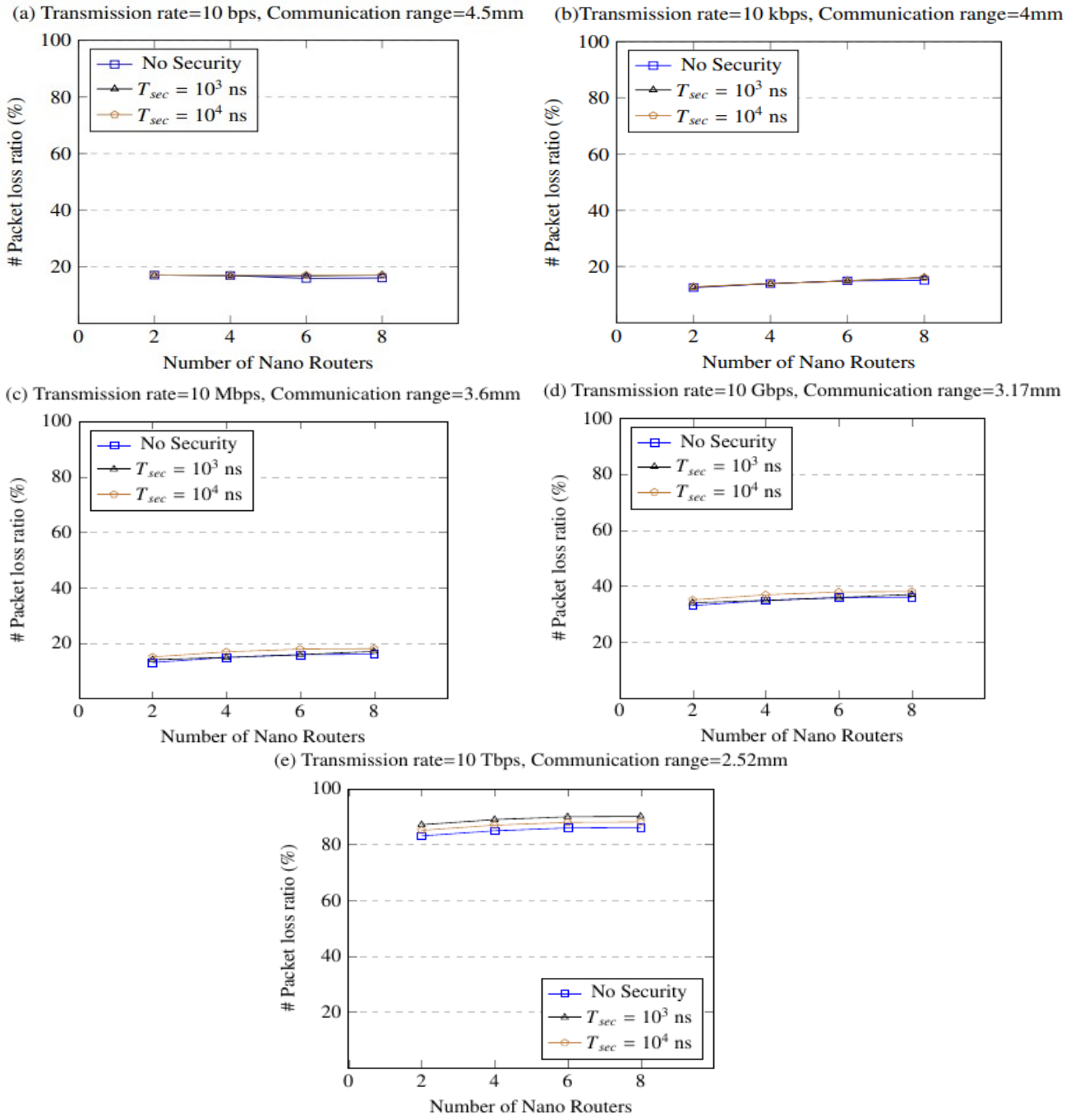



Fig. 14. Packet Loss Ratio.

[8] Y. Perwej, "A literature review of the human body as a communication medium using redtacton," *Communications on Applied Electronics (CAE), ISSN*, pp. 2394–4714, 2016.

[9] S. Kiran, M. R. Babu, B. Kiranmai, and K. Gurucharan, "Advanced wireless communications for future technologies-6g and beyond 6g," in *Wireless Communication with Artificial Intelligence*. CRC Press, 2023, pp. 1–26.

[10] R. Zhang, K. Yang, A. Alomainy, Q. H. Abbasi, K. Qaraqe, and R. M. Shubair, "Modelling of the terahertz communication channel for in-vivo nano-networks in the presence of noise," in *2016 16th Mediterranean Microwave Symposium (MMS)*. IEEE, 2016, pp. 1–4.

[11] X.-X. Yin, A. Baghai-Wadji, and Y. Zhang, "A biomedical perspective in terahertz nano-communications—a review," *IEEE Sensors Journal*, 2022.

[12] B. Atakan, O. B. Akan, and S. Balasubramaniam, "Body area nanonetworks with molecular communications in nanomedicine," *IEEE Communications Magazine*, vol. 50, no. 1, pp. 28–34, 2012.

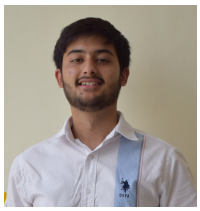
[13] M. Pierobon and I. F. Akyildiz, "A physical end-to-end model for molecular communication in nanonetworks," *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 4, pp. 602–611, 2010.

[14] W. Guo, C. Mias, N. Farsad, and J.-L. Wu, "Molecular versus electromagnetic wave propagation loss in macro-scale environments," *IEEE Transactions on Molecular, Biological and Multi-Scale Communications*, vol. 1, no. 1, pp. 18–25, 2015.

[15] A. D. Maynard, "Nanotechnology: assessing the risks," *Nano today*, vol. 1, no. 2, pp. 22–33, 2006.

[16] V. Loscri, C. Marchal, N. Mitton, G. Fortino, and A. V. Vasilakos, "Security and privacy in molecular communication and networking: Opportunities and challenges," *IEEE transactions on nanobioscience*, vol. 13, no. 3, pp. 198–207, 2014.

[17] F. Dressler and F. Kargl, "Security in nano communication: Challenges and open research issues," in *2012 IEEE International Conference on Communications (ICC)*. IEEE, 2012, pp. 6183–6187.
[18] S. R. Islam, F. Ali, H. Moon, and K.-S. Kwak, "Secure channel for molecular communications," in *2017 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2017, pp. 1–4.
[19] G. Piro, L. A. Grieco, G. Boggia, and P. Camarda, "Nano-sim: simulating electromagnetic-based nanonetworks in the network simulator 3." in *SimuTools*, 2013, pp. 203–210.
[20] M. Masoumi, W. Shi, and L. Xu, "Nanoscale cryptography: opportunities and challenges," *Nano convergence*, vol. 2, no. 1, pp. 1–15, 2015.
[21] J. M. Jornet and I. F. Akyildiz, "Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3211–3221, 2011.
[22] C. Funck, F. B. Laun, and A. Wetscherek, "Characterization of the diffusion coefficient of blood," *Magnetic resonance in medicine*, vol. 79, no. 5, pp. 2752–2758, 2018.
[23] G. Piro, L. Grieco, G. Boggia, and P. Camarda, "Simulating wireless nano sensor networks in the ns-3 platform," in *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, 2013, pp. 67–74.
[24] I. Llatser, D. Demiray, A. Cabellos-Aparicio, D. T. Altilar, and E. Alarcón, "N3sim: Simulation framework for diffusion-based molecular communication nanonetworks," *Simulation Modelling Practice and Theory*, vol. 42, pp. 210–222, 2014.
[25] N. Radhakrishnan and A. P. Muniyandi, "Dependable and provable secure two-factor mutual authentication scheme using ecc for iot-based telecare medical information system," *Journal of Healthcare Engineering*, vol. 2022, 2022.
[26] Y. Cho, J. Oh, D. Kwon, S. Son, J. Lee, and Y. Park, "A secure and anonymous user authentication scheme for iot-enabled smart home environments using puf," *IEEE Access*, vol. 10, pp. 101 330–101 346, 2022.
[27] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems (TOCS)*, vol. 8, no. 1, pp. 18–36, 1990.
[28] K. Agarwal, K. Agarwal, and S. Agarwal, "Evolution of internet of nano things (iont)," *Int. J. Eng. Technol. Sci. Res*, vol. 4, no. 7, pp. 274–277, 2017.
[29] N. A. Ali, W. Aleyadeh, and M. AbuElkhair, "Internet of nano-things network models and medical applications," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2016, pp. 211–215.
[30] F. Dressler and S. Fischer, "Connecting in-body nano communication with body area networks: Challenges and opportunities of the internet of nano things," *Nano Communication Networks*, vol. 6, no. 2, pp. 29–38, 2015.
[31] M. Kumar, J. Aggarwal, A. Rani, T. Stephan, A. Shankar, and S. Mirjalili, "Secure video communication using firefly optimization and visual cryptography," *Artificial Intelligence Review*, pp. 1–21, 2022.
[32] A. Alabdulatif, N. N. Thilakarathne, Z. K. Lawal, K. E. Fahim, and R. Y. Zakari, "Internet of nano-things (iont): A comprehensive review from architecture to security and privacy challenges," *Sensors*, vol. 23, no. 5, p. 2807, 2023.
[33] N. M. Luscombe, D. Greenbaum, and M. Gerstein, "What is bioinformatics? an introduction and overview," *Yearbook of medical informatics*, vol. 10, no. 01, pp. 83–100, 2001.
[34] T. Breithaupt, "Fan organs of crayfish enhance chemical information flow," *The Biological Bulletin*, vol. 200, no. 2, pp. 150–154, 2001.
[35] A. A. Khan, V. Kumar, J. Srinivas, S. Kumari, and M. K. Gupta, "Raks: robust authentication and key agreement scheme for satellite infrastructure," *Telecommunication Systems*, vol. 81, no. 1, pp. 83–98, 2022.
[36] G. Thakur, P. Kumar, S. Jangirala, A. K. Das, Y. Park *et al.*, "An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment," *IEEE Access*, 2023.
[37] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park, "Design of secure mutual authentication scheme for metaverse environments using blockchain," *Ieee Access*, vol. 10, pp. 98 944–98 958, 2022.
[38] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani *et al.*, "The avispa tool for the automated validation of internet security protocols and applications," in *Computer Aided Verification: 17th International Conference, CAV 2005, Edinburgh, Scotland, UK, July 6-10, 2005. Proceedings 17*. Springer, 2005, pp. 281–285.
[39] S. Banerjee, A. K. Das, S. Chattopadhyay, S. S. Jamal, J. J. Rodrigues, and Y. Park, "Lightweight failover authentication mechanism for iot-based fog computing environment," *Electronics*, vol. 10, no. 12, p. 1417, 2021.
[40] I. Ullah, N. U. Amin, J. Khan, M. Rehan, M. Naeem, H. Khattak, S. J. Khattak, and H. Ali, "A novel provable secured signcryption scheme a hyper-elliptic curve-based approach," *Mathematics*, vol. 7, no. 8, p. 686, 2019.
[41] S. S. Ullah, S. Hussain, A. Gumaei, and H. AlSalman, "A secure ndn framework for internet of things enabled healthcare," *Computers, Materials & Continua*, vol. 67, no. 1, pp. 223–240, 2021.
[42] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks," *Multimedia Systems*, vol. 23, pp. 195–205, 2017.
[43] M. K. Khan and S. Kumari, "An improved user authentication protocol for healthcare services via wireless medical sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 4, p. 347169, 2014.
[44] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, "A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity," *Security and Communication Networks*, vol. 9, no. 15, pp. 2643–2655, 2016.
[45] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks," *Multimedia Systems*, vol. 21, pp. 49–60, 2015.
[46] V. Sureshkumar, R. Amin, V. Vijaykumar, and S. R. Sekar, "Robust secure communication protocol for smart healthcare system with fpga implementation," *Future Generation Computer Systems*, vol. 100, pp. 938–951, 2019.
[47] M. R. Servati and M. Safkhani, "Eccbas: An ecc based authentication scheme for healthcare iot systems," *Pervasive and Mobile Computing*, vol. 90, p. 101753, 2023.



**Aryan Rana** "received his graduation from Panjab University, Chandigarh and Master degree from the Central University of Himachal Pradesh, Dharamshala, India. His research interests include authentication, IoNT, and Blockchain technology."

**Sunil Prajapat** "Sunil Prajapat received his M.Sc. degree in mathematics from the Central University of Himachal Pradesh, Dharamshala (HP), 176215, India. He is working on his Ph.D. dissertation in the Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Dharamshala (HP), 176215, India, and is a CSIR Fellow. His research interests are post-quantum cryptography, coding theory, blockchain, and various applications of cryptographic primitives in the real world."

**Pankaj Kumar** "received the M.Sc. from CCS University Meerut India and Ph.D. degrees from Galgotias University in 2005 and 2020, respectively. He has been an assistant professor at Srinivasa Ramanujan Department of Mathematics in the Central University of Himachal Pradesh, Dharamshala H.P. He has published over 40 academic research papers on information security and privacy preservation. His current research interests include cryptography, Blockchain, wireless network security, information theory, and network coding."

**Deepika Gautam** received the "M.Sc. degree in Mathematics from Central University Of Himachal Pradesh, Dharamshala(HP), 176215 India. She is currently pursuing a Ph.D. Degree from Central University of Himachal Pradesh, Dharamshala. Her research interests include digital signature, authentication, and Blockchain technology. "

**Chien-Ming Chen** (Senior Member, IEEE) received the Ph.D. degree from the National Tsing Hua University, Taiwan. He is currently an Associate Professor at the Shandong University of Science and Technology, China. His current research interests include network security, the mobile internet, the IoT, and cryptography. He also serves as an Associate Editor for IEEE Access and an Executive Editor for the International Journal of Information and Computer Security.