

Secured Data Transmission in Network Using Nano Technology

Dr. M. P. Vani¹, S. Kumudini², Siva Prakash³, Tanishadas⁴, Aditya Mittal⁵

¹Associate Professor, Vellore Institute of Technology, Vellore, India

^{2,3}Scholar, Vellore Institute of Technology, Vellore, India

^{4,5}Student, Vellore Institute of Technology, Vellore, India

Abstract

A Nanonetwork is mutually joined or related nanomachines used in communication system and helps to estimate uncomplicated tasks, making them simple to understand which are able to execute a very easy and uncomplicated tasks and is therefore easy to understand, such as computing, data storing, sensing. Nanonetworks consists of range of operation by permitting them to coordinate, share and combine information. Nanonetworks enables new application of Nanotechnology in biomedical field. The foremost concept behind nanotechnology and nanoscience was to control and manipulate atoms and molecules. The term “nanotechnology” was coined by professor Norio Taniguchi over a decade later. A Nanotechnology was in a position to develop small devices small . A Nanonetwork comprises of nanoscale computing devices and sensors that helps in communication at the nanoscale. Applications in networking consists of wireless technology, IOT, wireless and mobile nano devices. Based on the application requirement nanonetworks classifies the nanomachines to various application requirements like nano transmitters, Nano receiver, Nano Robot, Nano controller. Communication security is taken care from unauthorized access. Security composes of physical security, emission security, encryption security, transmission security. Some of the best tools used for secure business communication are perception point, Mail fence, rocket chat.

Keywords: Nanonetwork, nanoscience, emission, encryption, security, nano receiver ,nano controller, Mail fence, rocket chat

Introduction

A Nanonetwork is a mutually joined or related nanomachines which are able to execute a very easy and uncomplicated tasks and is therefore simple to understand such as computing, data storing, sensing and actuation.[1][2]Nanonetworks are range of operation by allowing them to coordinate, share and fuse formation. Nanonetworks enable new application of Nanotechnology in biomedical field.

The first idea behind nanotechnology and nanoscience was presented in 1959. Richard Feynman, a known theoretical physicist, gave a talk “There’s plenty of Room at the bottom” at an American Physical Society meeting. Here, Feynman described how scientists would be able to control and manipulate atoms and molecules. The term “nanotechnology” was coined by professor Norio Taniguchi over a decade later.

Thanks to nanotechnology, we were able to develop small devices with only, one to a few hundred nanometers. It is expected that networks of nanodevices will be a crucial component of every field of the

human society. A nanonetwork is composed of nanoscale communicating devices and sensors that facilitate communication at the nanoscale.

Applications in Networking:

Wireless Technology

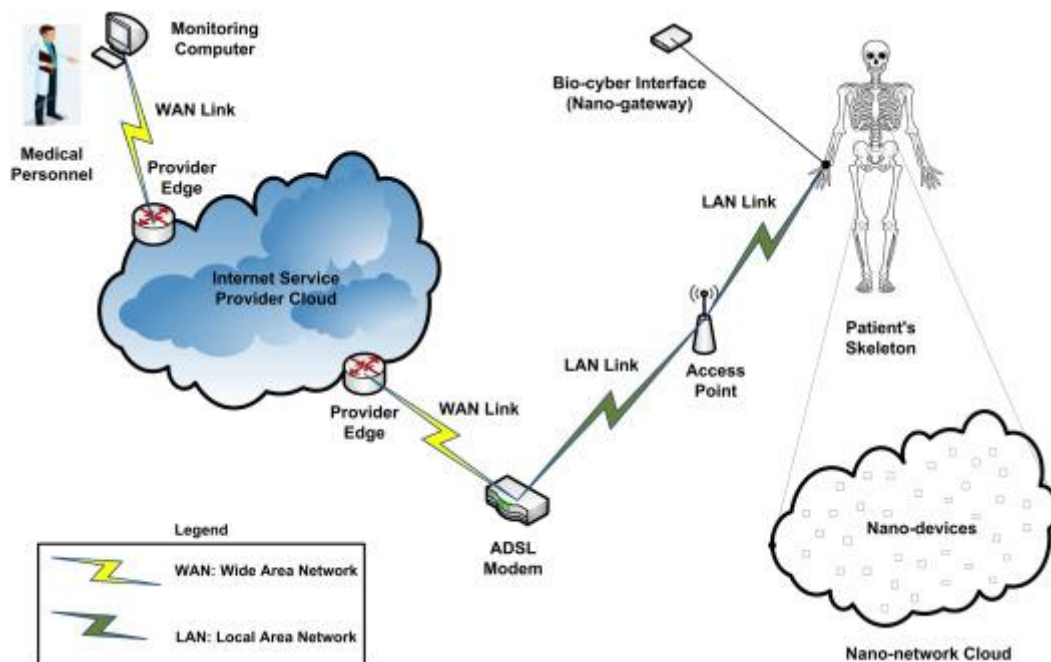
Nanotechnology will radically change the telecommunication enterprise. When compared to previous traditional technologies, nanotechnology will have a more significant effect due to the perfection in security, and operation of both core and cellular network. The Nanotechnology concept may be implemented in mobile device development to assist in embedding the nanodevices inside human environments (public places, home, and workplace) to create a new platform for computing, sensing, and communicating.

IoT (Internet of Things)

Internet of Things is the arrangement of things that include equipment, network system, sensors, and programming, enabling data exchange between the executive and other related objects. Nano biochips can be used to pass the information or data to the general population, to the machines, or among themselves. They are self-learning and upgrade themselves each time they play out their mission. Nano Intelligent Things can interact with devices or people in an efficient manner, can connect with the Internet and other Nano applications and systems, and can be controlled from a distance.

Wireless and Mobile Nanodevices

Portable devices for sensing and calculation are already a significant dream of remote businesses. It’s a way for it to surround itself with non-stop available knowledge. These devices can be attached to the office, home, and open spots. Devices need to be implanted into physical objects and be adjusted to the surrounding, to become a part of the system of encompassing Nanodevices (an organic framework.) Nanosensors and devices that can communicate with these organic frameworks can be created along with the development of nanotechnology.



Nano-networks communication architecture

Nano-Networks and Communication

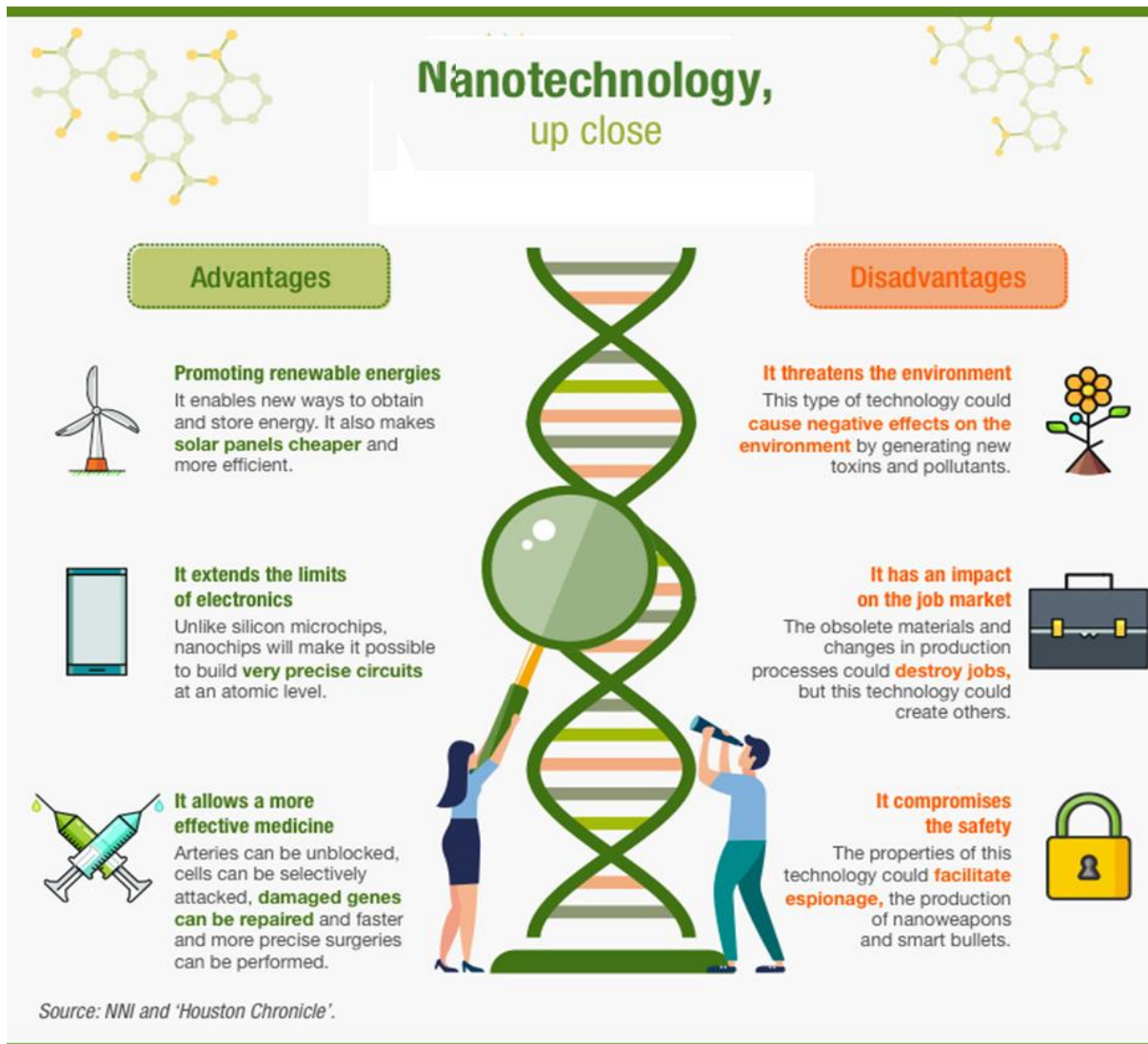
Nanomachines rely on nanometer-scale parts that can convey, process information, detect, or activate another system. The most basic way to interconnect these devices is through electromagnetic waves that propagate low loss wirelessly. Nanomachines need to have Nanoantenna's for high frequencies. Another type of communication between them is called Molecular Communication – the transmission and reception of data encoded in molecules.

Nanotechnology is believed to be the next industrial revolution which may give a sea of possibilities that exceed our current expectations in many science fields. In networking, nanotechnology could provide solutions for human-machine interaction, memory enlargement, sensing, and power-efficient computing. Titanium Cobra Engineers are always in line with the current Networking and Nanotechnology tech trends and successfully apply those best practices onto each of our clients' solutions.

Ascending: You start with a nanometric structure a molecule, for example and through mounting or self-assembly process create a larger mechanism than the one you started with


Dry Nanotechnology: It is used to manufacture structures in coal, silicon, inorganic materials, metals and semiconductors that do not work with humidity


Wet Nanotechnology: It is based on biological systems present in the aqueous environment including genetic materials, membranes, enzymes and other cellular components




Nanotechnology, up close

Advantages


- 


Promoting renewable energies
It enables new ways to obtain and store energy. It also makes **solar panels cheaper** and more efficient.
- 


It extends the limits of electronics
Unlike silicon microchips, nanochips will make it possible to build **very precise circuits** at an atomic level.
- 

It allows a more effective medicine
Arteries can be unblocked, cells can be selectively attacked, **damaged genes can be repaired** and faster and more precise surgeries can be performed.

Disadvantages

- 

It threatens the environment
This type of technology could **cause negative effects on the environment** by generating new toxins and pollutants.
- 

It has an impact on the job market
The obsolete materials and changes in production processes could **destroy jobs**, but this technology could create others.
- 

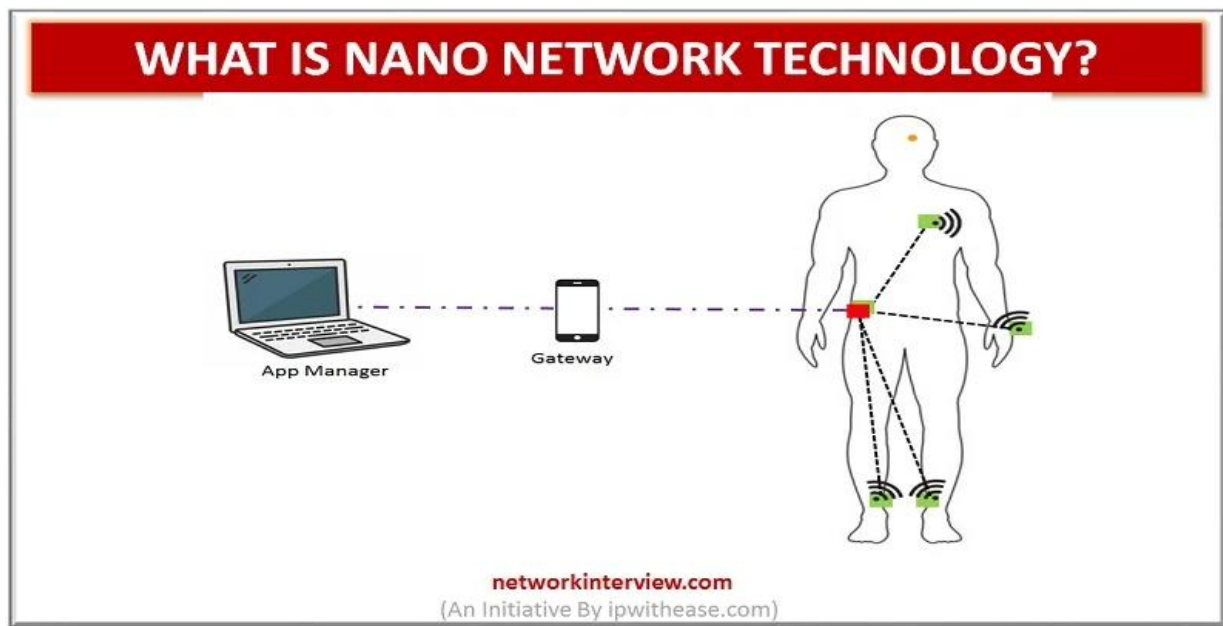
It compromises the safety
The properties of this technology could **facilitate espionage**, the production of nanoweapons and smart bullets.

Source: NNI and 'Houston Chronicle'.

Communication approaches:

Electromagnetic communication:

This is defined as the transmission and reception of electromagnetic radiation from components based on novel nanomaterials. Electronic nanoscale components such as nanobatteries[4], nano scale energy harvesting systems,[5] nano-memories,[6] logical circuitry in the nano scale and even nano antennas from communication point of view .the idiosyncratic property observed in nanomaterials will decide on the specific bandwidth, for the emission of electromagnetic radiation, the time lag of the emission, or the magnitude of the emitted power for a given input energy, amongst others.



A nanonetwork is a set of interconnected nanomachines. They are able to perform only very simple tasks such as computing, data storing, sensing and actuation. ^{[1][2]}

Nanonetworks are expected to expand the capabilities of single nanomachines both in terms of complexity and range of operation by allowing them to coordinate, share and fuse information. Nanonetworks are expected to expand the capabilities of single nanomachines both in terms of complexity and range of operation by allowing them to coordinate, share and fuse information. Nanonetworks enable new applications of nanotechnology in the biomedical field, environmental research, military technology and industrial and consumer goods applications.

Communication approaches:

Classical communication paradigms need to be revised for the nanoscale. The two main alternatives for communication in the nanoscale are based either on electromagnetic communication or on molecular communication.

Electromagnetic:

This is defined as the transmission and reception of electromagnetic radiation from components based on novel nanomaterials ^[3]. Recent advancements in carbon and molecular electronics have opened the door to a new generation of electronic nanoscale components such as nanobatteries, ^[4] Nanoscale energy harvesting systems, nano-memories, logical circuitry in the nanoscale and even Nano-antennas. Similarly, wind power generation is dependent on strong wind conditions and faces geographical limitations as it is only feasible in high-altitude or offshore areas. Furthermore, the generation process emits low-frequency noise, which can affect human physiological functions such as the circulatory and respiratory systems. Moreover, the power output is proportional to the square of the blade size, necessitating large-scale installations ^[5]. Recent trends in energy-harvesting studies have focused on technologies that harvest energy from the surrounding environment with fewer spatial, temporal, and size constraints. Notable examples include piezoelectric/friction electricity ^[6,7], photovoltaic devices ^[8], and evaporation-driven power generation. From a communication perspective, the unique properties observed in nanomaterials will decide on the specific bandwidth for emission of electromagnetic radiation, the time lag of the emission. Or the magnitude of the emitted power for a given input energy, amongst others. For the time being, two main alternatives for electromagnetic communication in the nanoscale have been envisioned. First, it has been experimentally demonstrated that it is possible to receive and demodulate an electromagnetic wave by means of a nanoradio, i.e., an electromechanically resonating carbon nanotube which is able to decode an amplitude or frequency

modulated wave^[9] Second, graphene-based nano-antennas have been analyzed as potential electromagnetic radiators in the terahertz band^[10]

Molecular:

Molecular communication is defined as the transmission and reception of information by means of molecules.^[11] The different molecular communication techniques can be classified according to the type of molecule propagation in walkaway-based, flow-based or diffusion-based communication.

In walk-way based molecular communication, the molecules propagate through predefined pathways by using carrier substances, such as molecular motors.^[12] This type of molecular communication can also be achieved by using *E.coli* bacteria as chemotaxis.^[13]

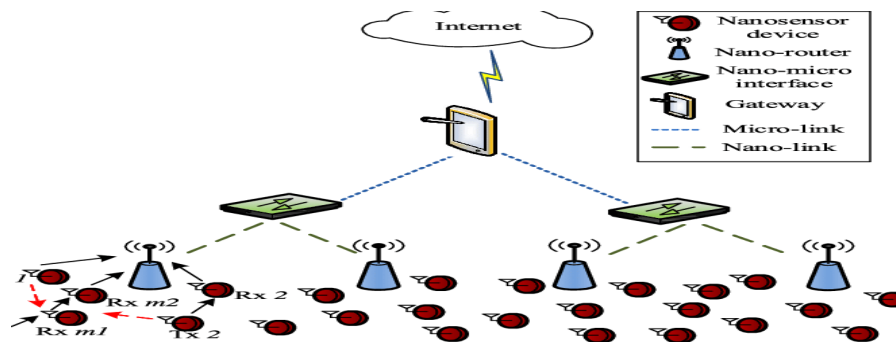
In flow-based molecular communication, the molecules propagate through diffusion in a fluidic medium whose flow and turbulence are guided and predictable. The hormonal communication through blood streams inside the human body is an example of this type of propagation. The flow-based propagation can also be realized by using carrier entities whose motion can be constrained on the average along specific paths, despite showing a random component. A good example of this case is given by pheromonal long range molecular communications.^[14]

In diffusion-based molecular communication, the molecules propagate through spontaneous diffusion in a fluidic medium. In this case, the molecules can be subject solely to the laws of diffusion or can also be affected by non-predictable turbulence present in fluidic medium. Pheromonal communication, when pheromones are released into a fluid medium, such as air or water, is an example of diffusion-based architecture. Other examples of this kind of transport include calcium signalling among cells,^[15] as well as quorum sensing among bacteria.^[16]

Based on the macroscopic theory^[17] of ideal (free) diffusion the impulse response of a unicast molecular communication channel was reported in a paper^[18] that identified that the impulse response of the ideal diffusion based molecular communication channel experiences temporal spreading. Such temporal spreading has a deep impact in the performance of the system, for example in creating the intersymbol interference (ISI) at the receiving nanomachine.^[19] In order to detect the concentration-encoded molecular signal two detection methods named sampling-based detection (SD) and energy-based detection (ED) have been proposed.^[20] while the SD approach is based on the concentration amplitude of only one sample taken at a suitable time instant during the symbol duration, the ED approach is based on the total accumulated number of molecules received during the entire symbol duration in order to reduce the impact of ISI a controlled pulse-width based molecular communication scheme has been analysed.^[21] The work presented in^[22] showed that it is possible to realize multilevel amplitude modulation based on ideal diffusion. A comprehensive study of pulse-based binary^[23] and sinus based,^{[24][25][26][27]} concentration-encoded molecular communication system have also been investigated.

The IEEE P 1906.1- Recommended practice for Nanoscale and Molecular communication framework^[11] is a standards working group sponsored by the IEEE Communications society Standards Development Board whose goal is to develop a common frame work for nano scale and molecular communication.^[2] because this is an emerging technology. The standard is designed to encourage innovation by reaching consensus on a common definition, terminology, framework, goals, metrics, and use-cases that encourage innovation and enable the technology to advance at a faster rate.

ARCHITECTURE OF NANONETWORKS



Nano network is comprised of several nano-scale devices such as nano transmitter, nano receiver, nano router, and other specialized nanodevices to perform exclusive tasks like sensing, actuation, monitoring, and control.

Network Architecture for the Internet of Nano-Things

The composition of nanonetworks depends upon the prospective application requirements. For example, a biomedical application like nano surgeries might need specialized nanodevices like nanorobots along with essential components of the nano network.

Nano transmitters, nano receivers, and nano routers are the essential components of nanonetwork, however, a nanonetwork might not necessarily contain all of the below-mentioned nanodevices.

Following is a detailed classification of nanomachines that can be part of nanonetworks according to application requirements.

Nano Transmitters:

Nano Transmitters are specialized nanomachines that are competent of sending encoded messages molecules into the nano network domain information molecules can be sent into the domain by two types of nano transmitters, and generic nano transmitters. Pre-encoded nano transmitters have encoded molecules stored in their compartment at the time of fabrication. Nanosystems that can be used as pre-encoded nano transmitters are artificially synthesized cells, genetically engineered biological cells, or artificial cells.

For example, lipid-based liposomes (i.e., molecule carrying enclosure) and polymer-based nanospheres and nanocapsules can be used as nano transmitters. Generic nano transmitters mimic natural cells such as bacteriophage, viruses, etc.

Unlike pre-encoded nano transmitters, the message molecule is synthesized inside the nano transmitter according to the trigger signal

Nano Receiver

A nano receiver detects the transmitted signal from the environment, further processes it, and produces an output signal in response. Same as nano transmitters, nano receivers take up the molecule from the environment, process it via a predefined biochemical algorithm that decodes the signal.

The decoded signal is then used to initiate an appropriate response in the environment e-g, stopping, initiating drug delivery sessions, synthesize or release some molecules, internal reconfiguration, or other biochemical reactions.

Nano Sensor

A nano sensor is a simple nanodevice that senses the environment to detect the presence of biological components or changes in environmental conditions like light, pH level, temperature.

Nano sensors can coordinate the changes in the environment with other nanodevices, which may work as a trigger signal to initiate an appropriate response.

Nano Robot

Nanorobots are nanodevices that have actuation capabilities in addition to the sensing ability. Nanorobot consists of sensors, actuators, information processing unit, memory unit, and power unit that make nanorobots a powerful device.

Nanorobots can manipulate the surrounding environment by performing actuation functionalities like precise delivery of therapeutic molecules to diseased cells.

Nano controller

Nano controllers are specialized nanodevices that are used to monitor and control other devices in the nano network. Their tasks may include monitoring the drug release process to make sure that a controlled amount of drug is released or to initiate/stop a process in the nano network.

Nano Router

Nano routers are more sophisticated nanodevices in terms of power, storage, and computation capacity. They are in charge of aggregating and processing information coming from various nanodevices in the network.

Nano segmentation operation

Nano segmentation manages security policies at the most granulated level possible within a network.

the three types of communication security are-

Communications security includes cryptosecurity [i.e., encryption or decryption], transmission security, emission security [i.e., intercept and analysis of emanations from equipment], and physical security of COMSEC material.

Example of communication security include encryption in transit, multi-factor authentication, secure network architecture, and on-premise deployment of the communication system.

Communication security means prevention of unwanted and unauthorized access to telecommunications. It includes four major disciplines:

- physical security
- emission security
- encryption security
- transmission security.

Organizations that want to secure their communication and protect their customer data must pay attention to all four areas.

In this article, we discuss eight approaches that can **help organizations secure their communication** and cover all four areas of communication security. communication security:

Also referred to as COMSEC, **communication security is the prevention of unauthorized access to communications** traffic. In essence, COMSEC as a discipline tries to protect any piece of information or data transferred over email, chat, phone, and other means.

Today, as communication means are developing and becoming more digital, the call for security is greater than ever.

8 communication security strategies for organizations

Here's a list of the best secure communication strategies used for organizations wanting to safeguard the data:

1. Physical security

The network operator is responsible for protecting data against any damage and ensuring smooth connectivity.

Ideally, servers should be located in a closed facility with limited access. Organizations concerned about communication security **often choose on-premise deployment of any service to ensure maximum safety**. In addition, having an efficient alarm system to notify authorities to respond swiftly and control the damage can aid secure communication. When companies choose cloud providers, data security becomes a shared responsibility between the company and the cloud provider.

2. Network and architecture of the communication system

The reliability of any communication network largely depends on a continuous and secure flow. To ensure this, **the network must consist of autonomous units that can work independently** to ensure smooth communication.

In addition, **the hardware (including base stations and servers) should always have an uninterrupted power supply (UPS) to act as a backup**. The density of these hardware units in the network ensures its ability to serve its users.

In extreme cases, networks can be air-gapped to prevent the slightest possibility of external access.

3. Preventing unauthorized access

Strong access controls must be implemented within a communication system **to ensure** communication security and stay compliant with data sovereignty. Sensitive information, including the user's name and personal details, should not be accessible even to employees below a certain security clearance level.

4. Multi-factor authentication

It is one way to enable secure communication between people without anyone eaves dropping, stealing data, or spreading misinformation. Sometimes unauthenticated users may need to join meetings for which a service that allows users to identify and accept or block their requests is required.

5. Data encryption in transit

Data traveling through an untrusted network, like the internet, is most vulnerable during transit. Therefore, it is crucial to put a protective mechanism, like end-to-end (E2E) encryption, in place.

It lets data travel safely between two parties, preventing any tampering from unauthorized third-party users. The cryptographic key decrypts the communication when it reaches the receiver. It is also important to secure **the management of these cryptographic keys** for communication security.

Not every employee in your organization will need access to every piece of information. Admin controls play an important role in readily managing this aspect. When personnel join the company, change departments, or leave the organization, their login credentials and access limits are altered or removed by the admin.

Even so, **a large organization requires periodic inspection of employee access and admit controls to avoid any data leaks or misinformation spreads**. This helps prevent compliance mishaps with laws like) and Health Insurance Portability and Accountability Act (HIPAA).

6. Regular audits

When an insider performs regular audits, they may not produce accurate results if the auditor is biased or has ulterior motives. Besides, **if an audit is used to spread malware, misuse information, or launch phishing attacks, it can result in an adverse outcome.**

Outsourcing security audits to a reliable and compliant third party can be beneficial in ensuring communication security. The authorized auditor should launch a surprise audit if the security system picks up multiple failed-login attempts or any unusual activity in the communication.

7. Internal training

Safety protocols may not work if people don't follow standard secure communication practices. Conducting regular training sessions for your staff on standard procedures while communicating can strengthen the communication network's security. **Internal training can help employees verify the information and avoid cyberattacks.**

Internal training is especially important to bolster cybersecurity.

8. Careful third-party use

Communication services require metadata for every communication to operate properly. Details about the communication, including the who, when, where, and how, may be collected and stored. The service provider needs to share the purpose of each collected piece of information.

An open source messaging solution is appropriate for your organization as it has essential transparency to ensure only the necessary metadata is collected and used.

Best tools for secure business communication

Any accidental or unintentional misuse of data can cause significant damage to a business. Thus, they place greater emphasis on communication security. Some of the most secure communication platforms available today are:

1. Perception Point

Perception Point comes equipped with dynamic engines and unique security technology to prevent threats, including malicious files and URLs, and enables secure business communication. This **platform can detect attacks across emails, web browsers, and online platforms** and deals with them independently.

2. Mailfence

A browser-based communication platform, Mailfence allows you to conduct your business with total control and freedom over emails. Whenever you send an email, it carries your digital signature (which only you can do), leaving no room for impersonation. All communication is encrypted, and two-factor authentication ensures added security.

3. Pexip

Used by security centric organization like military institutions,

Pexip is a collaborative platform that connects people over video conferences. Features like self-hosting and API support make it a secure communication platform. In addition, Pexip's integration with Rocket.Chat lets people access chat, voice calls, and file sharing through a single platform.

4. Rocket.Chat

An open-source communication platform, Rocket.Chat offers **transparent data management and multi-factor authentication** that is ideal for highly regulated industries. It also offers on premise deployment and end-to-end encryption. You can add another layer of security for sensitive data—an approval process—that prevents data loss.

A secure communication platform for your business

With an **open-source platform** like Rocket.Chat that can be **hosted on-premise**, you have the required transparency to monitor everything related to your team's communication. Additionally, it is a highly secure platform that is ISO 27001 certified and compliant with some of the most strict data sovereignty laws, including GDPR, HIPAA, and the California Consumer Privacy Act (CCPA).

Rocket.Chat is a preferred choice for **organizations operating in highly regulated industries** such as Finance, Government and Defense, Healthcare, and Education.

Conclusion:

To conclude it mutually deals with uncomplicated tasks, with various operations, Nanonetwork consists of new application of nano technology in biomedical field .It deals with wireless technology, nano transmission and nano security. It makes use of best tools for secure business communication.

References

1. J. M. Jornet and M. Pierobon (November 2011). "Nanonetworks: A New Frontier in Communications". *Communications of the ACM*. **54** (11): 84–89. doi:[10.1145/2018396.2018417](https://doi.org/10.1145/2018396.2018417). S2CID [240230920](https://doi.org/10.26434/chemrxiv-2018-240230920).
2. Bush, S. F. (2010). *Nanoscale Communication Networks*. Artech House. ISBN [9781608070039](https://doi.org/10.1002/9781118070039).
3. Rutherglen, C.; Burke, P. J. (2009). "Nano-Electromagnetics: Circuit and Electromagnetic Properties of Carbon Nanotubes". *Small*. **5** (8): 884–906. doi:[10.1002/smll.200800527](https://doi.org/10.1002/smll.200800527). PMID [19358165](https://pubmed.ncbi.nlm.nih.gov/19358165/).
4. Curtright, A. E.; Bouwman, P. J.; Wartane, R. C.; Swider-Lyons, K. E. (2004). "Power Sources for Nanotechnology". *International Journal of Nanotechnology*. **1**: 226–239. Bibcode:2004IJNT...1..226C. doi:[10.1504/IJNT.2004.003726](https://doi.org/10.1504/IJNT.2004.003726).
5. Wang, Z. L. (2008). "Towards Self-Powered Nanosystems: From Nanogenerators to Nanopiezotronics". *Advanced Functional Materials*. **18** (22): 3553–3567. doi:[10.1002/adfm.200800541](https://doi.org/10.1002/adfm.200800541). S2CID [43937604](https://doi.org/10.26434/chemrxiv-2018-43937604).
6. Bennewitz, R.; Crain, J. N.; Kirakosian, A.; Lin, J.L.; McChesney, J. L.; Petrovykh, D. Y.; Himpfel, F. J. (2002). "Atomic scale memory at a silicon surface". *Nanotechnology*. **13** (4): 499–502. arXiv:[cond-mat/0204251](https://arxiv.org/abs/cond-mat/0204251). Bibcode:2002Nanot..13..499B. doi:[10.1088/0957-4484/13/4/312](https://doi.org/10.1088/0957-4484/13/4/312). S2CID [15150349](https://doi.org/10.26434/chemrxiv-2018-15150349).
7. Burke, Peter J.; Li, Shengdong; Yu, Zhen (2006). "Quantitative theory of nanowire and nanotube antenna performance". *IEEE Transactions on Nanotechnology*. **5** (4): 314–334. arXiv:[cond-mat/0408418](https://arxiv.org/abs/cond-mat/0408418). Bibcode:2006ITNan...5..314B. doi:[10.1109/TNANO.2006.877430](https://doi.org/10.1109/TNANO.2006.877430). S2CID [2764025](https://doi.org/10.26434/chemrxiv-2018-2764025).
8. Burke, Peter J.; Rutherglen, Chris; Yu, Zhen (2006). "Carbon Nanotube Antennas" (PDF). In Lakhtakia, Akhlesh; Maksimenko, Sergey A (eds.). *Nanomodeling II*. Vol. 6328. p. 632806. doi:[10.1117/12.678970](https://doi.org/10.1117/12.678970). S2CID [59322398](https://doi.org/10.26434/chemrxiv-2018-59322398). Archived (PDF) from the original on 10 June 2021. Retrieved 10 June 2021.
9. Atakan, B.; Akan, O. (June 2010). "Carbon nanotube-based nanoscale ad hoc networks". *IEEE Communications Magazine*. **48** (6): 129–135. doi:[10.1109/MCOM.2010.5473874](https://doi.org/10.1109/MCOM.2010.5473874). S2CID [20768350](https://doi.org/10.26434/chemrxiv-2018-20768350).
10. Jornet, J. M.; Akyildiz, Ian F. (April 2010). "Graphene-based Nano-antennas for Electromagnetic Nanocommunications in the Terahertz Band". *Proc. Of EUCAP 2010, Fourth European Conference on Antennas and Propagation, Barcelona, Spain*: 1–5. ISSN [2164-3342](https://doi.org/10.26434/chemrxiv-2018-2164-3342). Archived from the original on 19 January 2018. Retrieved 10 June 2021.

11. T. Nakano; A. Eckford; T. Haraguchi (2013). Molecular Communication. Cambridge University Press. ISBN 978-1107023086.
12. Moore, M.; Enomoto, A.; Nakano, T.; Egashira, R.; Suda, T.; Kayasuga, A.; Kojima, H.; Sakakibara, H.; Oiwa, K. (March 2006). "A Design of a Molecular Communication System for Nanomachines Using Molecular Motors". Proc. Fourth Annual IEEE Conference on Pervasive Computing and Communications and Workshops.
13. Gregori, M.; Akyildiz, Ian F. (May 2010). "A New NanoNetwork Architecture using Flagellated Bacteria and Catalytic Nanomotors". IEEE Journal on Selected Areas in Communications. **28** (4): 612–619. doi:10.1109/JSAC.2010.100510. S2CID 15166214.
14. Parcerisa, L.; Akyildiz, Ian F. (November 2009). "Molecular Communication Options for Long Range Nanonetworks". Computer Networks. **53** (16): 2753–2766. doi:10.1016/j.comnet.2009.08.001. hdl:2099.1/8361.
15. Barros, M. T. (2017). "Ca²⁺-signaling-based molecular communication systems: design and future research directions". Nano Communication Networks. **11**: 103–113. doi:10.1016/j.nancom.2017.02.001. Archived from the original on 23 April 2024. Retrieved 16 August 2017.
16. "The challenge of molecular communication". Technology Review (Physics ArXiv Blog). 28 June 2010. Archived from the original on 20 January 2021. Retrieved 10 June 2021.
17. Berg, H.C. (1993). Random Walks in Biology. Princeton University Press. ISBN 9780691000640.
18. Mahfuz, M.U.; Makrakis, D.; Mouftah, H. (20–23 January 2010). "Characterization of Molecular Communication Channel for Nanoscale Networks" (PDF). Proc. 3rd International Conference on Bio-inspired Systems and Signal Processing (BIOSIGNALS-2010). Valencia, Spain: 327–332. Archived from the original (PDF) on 20 September 2015. Retrieved 10 June 2021.
19. Mahfuz, M.U.; Makrakis, D.; Mouftah, H.T. (2010). "On the characterization of binary concentration-encoded molecular communication in nanonetworks". Nano Communication Networks. **1** (4): 289–300. doi:10.1016/j.nancom.2011.01.001. Archived from the original on 24 September 2015. Retrieved 6 May 2012.
20. Mahfuz, M.U.; Makrakis, D.; Mouftah, H.T. (26–29 January 2011). "On the Detection of Binary Concentration-Encoded Unicast Molecular Communication in Nanonetworks" (PDF). Proc. 4th International Conference on Bio-inspired Systems and Signal Processing (BIOSIGNALS-2011). Rome, Italy: 446–449. Archived from the original (PDF) on 10 June 2021. Retrieved 10 June 2021.
21. Mahfuz, M.U.; Makrakis, D.; Mouftah, H.T. (8–11 May 2011). "Characterization of intersymbol interference in concentration-encoded unicast molecular communication". 2011 24th Canadian Conference on Electrical and Computer Engineering (CCECE). Niagara Falls, ON. pp. 000164–000168. doi:10.1109/CCECE.2011.6030431. ISBN 978-1-4244-9788-1. S2CID 18387617.
22. Mahfuz, M.U.; Makrakis, D.; Mouftah, H.T. (8–11 May 2011). "On the characteristics of concentration-encoded multi-level amplitude modulated unicast molecular communication". 2011 24th Canadian Conference on Electrical and Computer Engineering (CCECE). Niagara Falls, ON. pp. 000312–000316. doi:10.1109/CCECE.2011.6030462. ISBN 978-1-4244-9788-1. S2CID 1646397.
23. Mahfuz, M.U.; Makrakis, D.; Mouftah, H.T. (15–18 August 2011). "A comprehensive study of concentration-encoded unicast molecular communication with binary pulse transmission". 2011 11th

- IEEE International Conference on Nanotechnology. Portland, Oregon, USA. pp. 227–232. [doi:10.1109/NANO.2011.6144554](https://doi.org/10.1109/NANO.2011.6144554). ISBN 978-1-4577-1516-7. S2CID 23577179.
24. Mahfuz, M.U.; Makrakis, D.; Mouftah, H.T. (26–29 October 2011). "Transient characterization of concentration-encoded molecular communication with sinusoidal stimulation". Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies. Barcelona, Spain. pp. 1–6. [doi:10.1145/2093698.2093712](https://doi.org/10.1145/2093698.2093712). ISBN 9781450309134. S2CID 3490172.
25. Akyildiz, Ian F.; Brunetti, F.; Blazquez, C. (June 2008). "Nanonetworks: A New Communication Paradigm". *Computer Networks*. **52** (12): 2260–2279. [doi:10.1016/j.comnet.2008.04.001](https://doi.org/10.1016/j.comnet.2008.04.001).
26. Akyildiz, Ian F.; Jornet, J. M. (June 2010). "Electromagnetic Wireless Nanosensor Networks". *Nano Communication Networks*. **1** (1): 3–19. [doi:10.1016/j.nancom.2010.04.001](https://doi.org/10.1016/j.nancom.2010.04.001).
27. Akyildiz, Ian F.; Jornet, J. M. (December 2010). "The Internet of Nano-Things". *IEEE Wireless Communications*. **17** (6): 58–63. [doi:10.1109/MWC.2010.5675779](https://doi.org/10.1109/MWC.2010.5675779). S2CID 6919416.