DEFENCE APPLICATIONS OF QUANTUM COMPUTING

Saasha Joshi
Panjab University, Chandigarh, India

A Space-based Quantum Internet would require a constellation of 400 satellites in the mid-Earth orbit, at an altitude of 3,000 kilometers [2].
The fact that the property of Quantum Entanglement is highly fragile, requires high number of satellites to be used to ensure no loss of quantum information.

QUANTUM SATELLITES

Quantum Satellites in space can provide a method for long-range satellite-to-ground and inter-satellite secure quantum communication for the military advantage. These communication methods make use of the quantum phenomena such as SUPERPOSITION and ENTANGLEMENT.
In quantum entanglement, two photonic particles must interact physically and together exist in a single quantum state. This physical interaction and co-existence can be achieved by shooting a laser through a photon. This laser splits the photon into two entangled particles which even at a large distance, remain entangled to one another and exist in a single quantum state [1].

Quantum satellites with the help of established mobile ground stations, unmanned vehicles or missile defence systems, can perform quantum key distribution in which these entangled photons can be transmitted between different channels for an effective teleportation of information.

QUANTUM KEY DISTRIBUTION (QKD) FOR SECURE MILITARY COMMUNICATION

The process of QUANTUM KEY DISTRIBUTION involves transmission of information in the form of polarized light particles or PHOTONS from one entity to another. Each of these transmitted photons have a random quantum state which can be measured with the help of beam splitters, horizontal, vertical and diagonal. However, the sequence of beam splitters which can correctly decrypt the message remains unknown to the receiver. This necessitates the receiver to select a random sequence of basis to decrypt the message. The receiver then communicates with the sender to measure the state of the transmitted qubits in order to establish if both have the same key. This process is known as KEY SIFTING [3]. The photons read using the wrong beam splitter are discarded and the resulting sequence is regarded as the key.

TRUSTED NODES FOR QKD (FUTURE SCOPE)

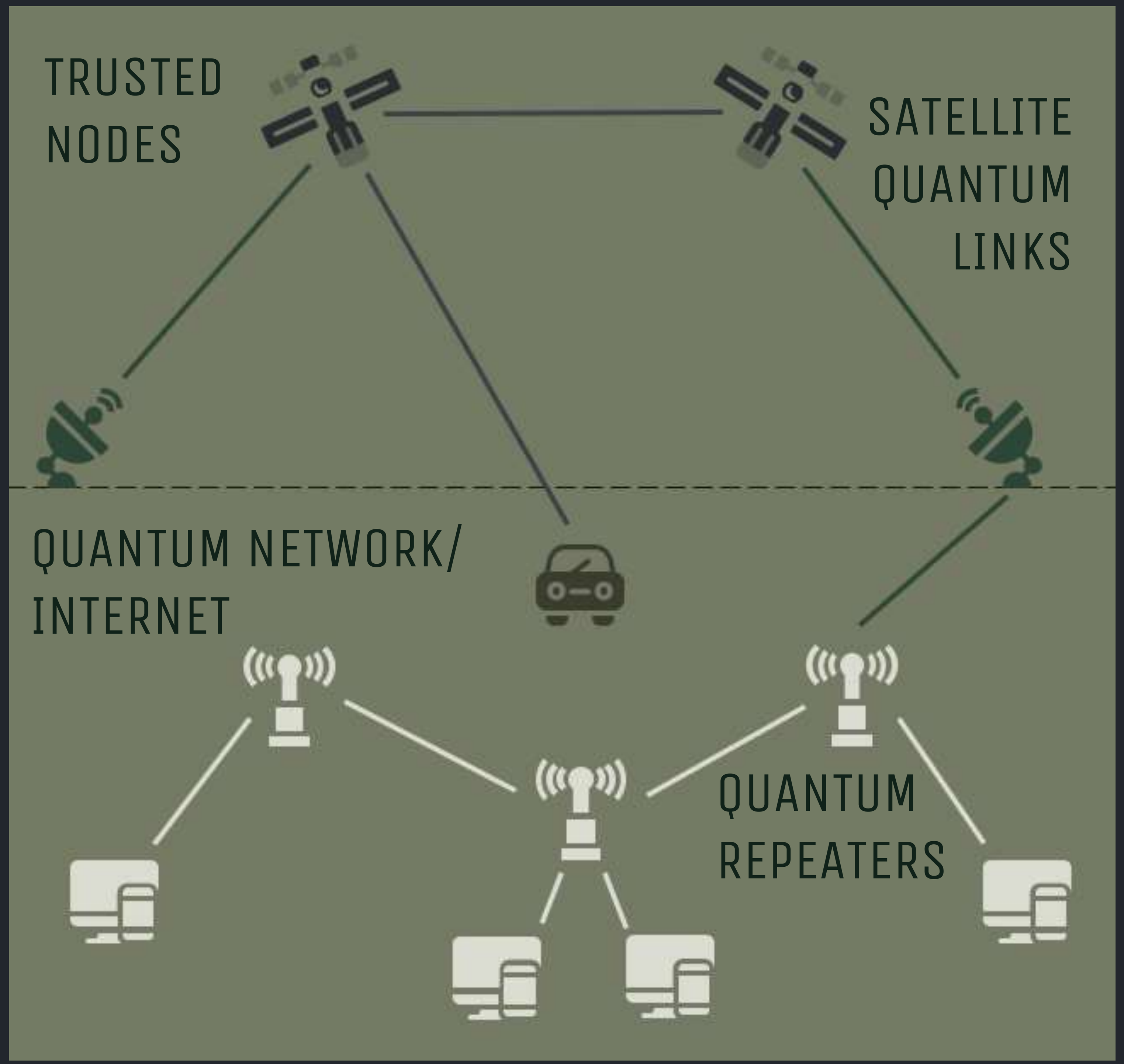
Satellite-based technology in a quantum enabled constellation of satellites, can be used to build an effective and logically coherent system for a SPACE-BASED QUANTUM INTERNET [2].
Satellites as simplified trusted nodes can enable long distance QUANTUM KEY DISTRIBUTION which can make military communications more secure by using quantum encryption techniques to prevent any cyber attacks. In presence of any eavesdropper, the QKD process alerts the sender and the receiver of the intrusion. This intrusion is detected by the alteration of the state of photons which the eavesdropper causes by measuring the quantum photons.

Therefore, these quantum satellites or trusted nodes can perform a key hopping process, where a key generated at the starting node is transferred securely to the end node by jumping over various intermediate nodes.

$$A \xrightarrow{Key\ AB} B \quad \Rightarrow \quad A \xrightarrow{Key\ AN} N \xrightarrow{Key\ NB} B$$

This key distribution between two nodes A and B occurs with the help of a trusted node N. In order to transfer the $Key\ AB$ from A to B, A sends N an encrypted $Key\ AN$. N decrypts the key received from A and re-encrypts the original $Key\ AB$ to $Key\ NB$ to send it to B.

A's Bit Sequence	1 0 1 1 0 0 1 1 0 0 1 1 1 0
B's Beam Splitter Sequence	+ / + + / / + + / + / / + +
B's Measurement	1 0 0 1 0 0 1 1 0 0 0 1 0 0
Sifted Key	1 – – 1 0 0 – 1 0 0 – 1 – 0



QUANTUM REPEATER NETWORK

The materials in communication cables can absorb photons, thus, making it difficult to transfer information for more than few kilometers [4]. To overcome this issue in quantum information transfer, a network of repeater devices can be established to amplify the signal of the incoming photons. Such a network can measure and transfer the quantum properties of incoming photons to another set of new photons [2]. These networks preserve the property of quantum entanglement while allowing end-to-end transmission of photons from one repeater to another.
GROUND-BASED QUANTUM INTERNET can use this technology to transmit quantum information over long distances.

1. Magnuson, Stew, 'Quantum 101: Understanding the Spooky" National Defense (Vol. 103 No. 784) March 2019. https://www.questia.com/magazine/1G1-581311990/quantum-101-understanding-the-spooky.
2. Khatri S, Brady AJ, Desporte RA, Bart MP, Dowling JP. Spooky Action at a Global Distance $-$ Resource-Rate Analysis of a Space-Based Entanglement-Distribution Network for the Quantum Internet. arXiv preprint arXiv:1912.06678. 2019 Dec 13.
3. Quantum XChange, https://quantumxc.com/quantum-cryptography-explained/, 2019.
4. Martin Giles, "Explainer: What is quantum communication?", MIT Technology Review, February 14, 2019, https://www.technologyreview.com/s/612964/what-is-quantum-communications/ .
5. Figure from [3] and ITU Workshop on Quantum Information Technology (QIT) for Networks.