Impact of Quantum Computing on IoT Security

Many IoT systems deployed today will remain operational for many years. With advances in quantum computers, it is possible that large-scale quantum computers will be available in the future to perform cryptanalysis on existing cryptographic algorithms and cipher suites. Such scenario will have two consequences. First, key exchange, public-key encryption, and signatures would no longer be secure due to Shor's algorithm. Second, the security level of symmetric algorithms will decrease, for example, the security of a block cipher with a key size of n bits will only offer $n/2$ bits of security due to Grover's algorithm.

The above scenario becomes critical when we consider the "harvest and decrypt" attack in which an attacker can begin to harvest (store) encrypted data today, before a quantum computer is available, and then decrypt years later, once a quantum computer is available. It may also become difficult to update IoT devices securely. This situation would force us to switch to quantum-resistant alternatives, especially for key exchange, public-key encryption, and signatures. As IoT devices are vulnerable to hacking, it becomes important to use quantum-safe cryptography to protect the data transmitted between IoT devices and the internet.

Quantum computing has the potential to greatly impact IoT systems in many ways including:

Negative impact:

1. Breaking encryption: quantum computers can perform computations much faster than classical computers, which means they could potentially break encryption algorithms that are currently used to secure IoT devices and networks.
2. AI methods can be empowered by quantum computers to automate various attacks such as hacking, phishing, ransomware, and malware propagation at large scales.
3. DDoS Attack: Quantum computers can also be used to launch devastating Distributed Denial of Service (DDoS) attacks, as they can generate large amounts of traffic to overload servers.

Positive impact:

1. Quantum Cryptography: quantum computing can be used to develop new, more secure encryption methods that would be much more difficult to break. Quantum Key Distribution (QKD) is an example of a quantum cryptography technique that can be used to secure IoT communications.
2. Vulnerability identification and management: quantum computing can be used to simulate and analyze complex systems to identify potential vulnerabilities in IoT networks and devices. This could help improve overall security.
3. Secure key exchange: quantum properties such as entanglement can be used to safely exchange private keys.

This lecture describes how quantum computers can impact IoT security, both positively and negatively, and what steps are needed to transition to cryptographic algorithms that provide security in the presence of quantum computers.