Assignment #5

Mohammed Shahzad

444105788@student.ksu.edu.sa

The survey research titled "Reliability in Internet of Things: Current Status and Future Perspectives" by Liudong Xing touches all perceivable dimensions of the important issue of reliability in Internet Of Things.

The paper begins with an apt introduction to reliability as one of the crucial requirements for adoption of the IoT in critical applications. There may include, for example: Malfunctions of supporting IoT devices (e.g., wearable medical devices), failing to capture critical data, any network outage, data corruption, or loss during transmission or storage which may cause catastrophic effects, such as mission failure, financial loss, and harm to people and environments.

The paper then analyses reliability aspect and address issues arising from each suggested solution right from the perception layer, communication layer, support layer to end-user in Application Layer. Then we are presented with architectural challenges in reliability for IoT. These constitute reliability issues in Physical Layer. Due to limited, IoT devices especially those operating in harsh and unattended environments are prone to failures. They often communicate through wireless links that are also error prone due to noises, signal attenuations, or channel fading.

The researcher also notes that, advances in various IoT enabling technologies are making the IoT systems more powerful and intelligent. On the other hand, the cooperation and interaction among the system components become more complicated, creating new and unknown dependencies.

During different phases, the system may need to perform different tasks or functions involving different subsets of system resources or components. These components may undergo different environment conditions and stress levels, thus have different failure rates or mechanisms during different phases. For example, in a smart home, due to the changing brightness of the sun, the solar panels function with different production performance with time. During some time (e.g., afternoon), energy from the solar panels is sufficient to supply the electrical panel of the smart home but during other time, electricity stored and/or from the public grid may have to be used to supply the smart home.

Another example made the point mentioned very clear. During the night phase, only the physiological information is measured by biosensors; during the daytime phase, both the physiological and motion data are monitored by biosensors and motion sensors, respectively. In both examples during different phases, different subsets of system components contribute to

the system function, requiring a distinct reliability model to describe the system failure behaviour at each phase.

Then we see how reliability parameters at other levels in IoT service model. So, the research paper then moves to the next layer, that is Communication layer (CL) that is most responsible and crucial for routing data and its security. The CL is also responsible for providing a ubiquitous access and networking environment for the PL. As we know, In the case of a failure of a node or a link on the selected path, a reliable routing protocol is responsible for detecting the occurrence of the failure and finding an alternative path to accomplish the desired information transmission.

For failure resilient WSNs, multipath routing protocols have been designed, they achieve high reliability and use multiple paths to link disjoint, node disjoint, or overlapped/correlated. They may be used in parallel, or in a standby style. Reliability-Aware Single-Path Routing also exist and works on designing reliability into the single-path routing algorithms. Similarly, based on the ARQ protocol, the retransmission-based mechanism uses ACK and timeout to provide reliable data transmissions if a condition like, say, the number of retransmissions exceeds a predetermined maximum value.

In the next section of the paper, support layer reliability is discussed. We know that in Wireless sensor networks, data is diverse and countless. For this we use support layer (SL) technologies like cloud computing. The discussed issues include:

1) Retrying: a failed service task is retried on the same resource;
2) Alternate Resource: a failed service task is retried on another resource;
3) Replication
4) Checkpointing

The researcher then mentions how cloud cyberattacks may affect reliability. Multiple VMs configured alike on the same cloud present a challenge to the security of cloud. In particular, the CRA may be launched by malicious attackers, where VMs running the malware are co-located with a target user's VMs and a side channel can then be established to enable the data theft or corruption.

Cloud-RAID Reliability with its seven may provide some relief in terms of reliability SANs reliability, which is a high-speed FC fabric capable of connecting any server and any storage element, allowing multiple storage resources to be accessed by multiple hosts simultaneously, is also studied.

Then we look at relatively newer technologies like edge computing and their relation to reliability in IoT. The researcher rightly points out that, as variants and extensions of the conventional cloud computing, edge computing and fog computing are gaining popularity for IoT applications due to their advantages in improving the response time and saving bandwidth. Their reliability is not extensively studied but equally important.

The author then concludes the research paper with her insights on future developmental issues that are currently research worthy. These include cross-domain, cross-layer reliability research, and cascading failures- Driven by factors such as dynamic changes in network workloads caused by a component failure, a chain reaction or domino effect taking place causing extensive damage and even outage of the entire network.

The paper suggests that despite the rich and fast-growing body of works on IoT, the reliability research is still in its early stage. As IoT systems and applications evolve, additional new aspects of system complexity and dynamics may arise, making the existing reliability models and solutions inadequate or inaccurate. New and efficient reliability models and tools are expected for capturing the new features and behaviours, leading to more effective and accurate IoT system reliability analysis, optimization, and design. The ultimate goal is to transform our society towards being industry revolution ready.

***