September 10, 2019

DISASTER MANAGEMENT SYSTEM USING NETWORK SNAPSHOT IN LOW POWER AND LOSSY NETWORKS (LLNS)

Lele Zhang

Chuanwei Li

Xiang Fang

Xiaopu Zhang

DISASTER MANAGEMENT SYSTEM USING NETWORK SNAPSHOT IN LOW POWER AND LOSSY NETWORKS (LLNS)

AUTHORS:

Lele Zhang
Chuanwei Li
Xiang Fang
Xiaopu Zhang

ABSTRACT

Presented herein are techniques to introduce snapshot technology into wireless networks. In particular, the remote side of the network (e.g., edge devices, border routers, cloud, *etc*.) collect status information from all nodes of a network, such as a personal area network (PAN), while at the same time collecting and storing one or more snapshot(s) of the network. If the wireless network crashes, the remote side is configured to restore the entire network from the existing saved snapshot(s).

DETAILED DESCRIPTION

Currently, the Disaster Management System (DMS) is required by many information technology industries, such as banks, document centers, data centers, and so on. Internet of Things (IoT) networks also need DMS to handle different kinds of potential threatens, such as:

1. Hacker attacks,
2. Hardware failure,
3. File damage,
4. Incorrect human operations (e.g., wrong firmware upgrading),
5. Disasters (e.g., earthquake, fire, *etc*.)
6. Unexpected power outages,
7. *Etc*.

The Connected Grid Mesh (CG-Mesh), which has been developed for industrial customers to manage Advanced Metering Infrastructure (AMI) and Distributed Automation (DA) equipment, also needs DMS. CG-Mesh could support millions of nodes in the field, thus fast recovery of all nodes is a critical requirement for CG-Mesh customers.

However, due to using low data rate links (e.g., IEEE802.154.4g and P1901.2), CG-Mesh is easily affected by environmental conditions that change over time. Some examples include temporal changes in interference (e.g., other wireless networks or electrical appliances), physical obstructions (e.g., doors opening/closing or seasonal changes in foliage density of trees), and propagation characteristics of the physical media (e.g. temperature or humidity changes). The time scales of such temporal changes can range between milliseconds (e.g. transmissions from other transceivers) to months (e.g. seasonal changes of outdoor environment).

In addition, Low-cost and low-power designs limit the capabilities of the transceiver. In particular, Low power and Lossy Network (LLN) transceivers typically provide low throughput. Furthermore, LLN transceivers typically support limited link margin, making the effects of interference and environmental changes visible to link and network protocols. Interference may be external (non-network devices generating electromagnetic interference) or internal (other network devices communicating within the same frequency band).

For the above reasons, the topology of CG-Mesh changes quite frequently and the entire network needs a long period of time to achieve stability. Therefore, if the whole network is devastated by a major event (e.g., power outage), the customers will want to recover everything as soon as possible. The techniques presented herein provide a solution for quick recovery following a major event.

A common traditional/conventional solution for network recovery is to save all key information into local nodes when a major event occurs. For example, if an unexpected power outage occurs, nodes have a large bulk capacitor to extend operation for a few seconds. During this time, the nodes store some critical information into their non-volatile memory and send Power Out Notification (PON) messages to the router. When next powered up, these nodes will fast recover by using saved parameters and will send PRN Power Restore Notification (PRN) messages to inform the router that they are back online. This mechanism is currently used in CG-Mesh, but experiences two problems.

A first problem with this conventional solution for network recovery is that the terminal node is often limited with memory resources, while the critical information grows quickly. At the same time, the application information also saved in memory grows quickly. As such, the limited memory resources will be insufficient in the near future. If the memory capacity is increased (e.g., add a new peripheral memory), it will increase the cost of the hardware. A second problem is that saving information into memory consumes energy, which as noted is supplied by a big bulk capacitor. However, this capacitor is also used to send the PON. As such, some nodes may be powered-off before they have successfully written the critical information, which will lead to the unsuccessful recovery of nodes when power is restored. Providing a larger capacitor will increase the increase the cost of the hardware.

Another prior art solution proposes to save critical information periodically on remote battery-backed edge devices, such as the border router. This method avoids local storage problems but has new problems, which include:

1. Every node has its own period to send updates regarding network topology to the edge device (e.g., border router). Using RPL DAO message, each node has different DAO schedules, e.g., node A updated 10 minutes ago, node B updated 5 minutes ago, node C updated 30 minutes ago, and so on. Therefore, if a crash occurs, and the border router pushes the latest updates to the respective node, the topology may be wrong.
2. Sometimes customers want to roll back firmware upgrades. For example, a new firmware version 2.0.1 is available and used to upgrade all nodes currently running version 2.0.0. A few days later, the customer determines that the previous version provides better performance is better, thus they ask to roll back to the older version. These prior art solution cannot address this issue because it does not have integrated backup topology information.

Presented herein are new network recovery techniques based on snapshot technology. In computer systems, a snapshot is the state of a system at a particular point in time, which

is often adopted in File System Recovery. With the development of virtual machine technology, this method is often used for VM fast restoration on cloud computing. The techniques presented herein use snapshot technology to improve DMS in LLNs.

In DMS theory, two key indicators are important:

1. Recovery Time Objective (RTO), which is the targeted duration of time and service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable breaks in business continuity. For a CG-Mesh, the sooner the better.
2. Recovery Point Objective (RPO), which is the maximum targeted period in which data (transactions) may be lost from an IT service due to a major incident. For example, in CG-Mesh, RPO could be a topology of 1 hour ago, 3 days ago, *etc*.

The techniques presented herein have two primary parts. In Part One, the use of periodic snapshots is proposed with reference to the entire network topology, rather than with reference to only a single node. In Part Two, these snapshots are used for restoring the entire network.

Part One:

In CG-Mesh, difference kinds of Type-length-values (TLVs), based on Constrained Application Protocol (CoAP), are used to manage nodes. In the techniques presented herein, a new TLV command is added to enable nodes to save required information at the same time as information is sent, for example, to the router/fog/cloud (e.g., the router sends multicast command TLV to all nodes, which tells them to save required topology information at 3:00 pm, and then send the updates to router).

The topology information may include, but is not limited, to:

1. neighbor entry information table (including link quality, e.g., ETX)
2. parent list
3. IP address
4. Self routing rank
5. frame counter
6. firmware version
7. *etc*.

Once the router/fog/cloud receives all of this information, it will generate a snapshot file with timestamps. These files could be saved in the edge device, such as the router or cloud device in a data center.

Figure 1, below, illustrates are two different typologies for the same CG-Mesh instance. So, for DMS, they are two snapshots, T0 and T1. Both of them could be saved remotely, if needed.

Part Two:

As noted above, in Part Two of the techniques presented herein, the stored snapshots can be used to restore the entire network. The restoration of networks contains two type:

1. **Automated restoration.** If the cloud/fog/router detects that a disaster occurs, it will automatically recover using a snapshot (usually the latest snapshot). In this model, every node needs to rejoin the network and the router could push the routing information directly before a node sends an RPL DAO message, as long as the node has its link-local address. This could significantly shorten reformation time.

2. **Mutual restoration.** The customers use this to roll back the network to a specific snapshot version (e.g., usually not latest version, but perhaps a snapshot from 1 week ago, 1 month ago, *etc*.). In this model, every node is already on-line and the router pushes the desired configurations to all terminals and sets an effective time (e.g., initiate configuration at 4 p.m. tomorrow, which could make all nodes to use the same baseline configurations at the same time).

As noted, the techniques herein propose the use of snapshot technology for recovery of LLNs. The nodes capture snapshots, which can be stored at the remote side (e.g., edge device/border router/cloud). Therefore, if the network crashes, the remote side can restore the entire network from existing saved snapshot(s).

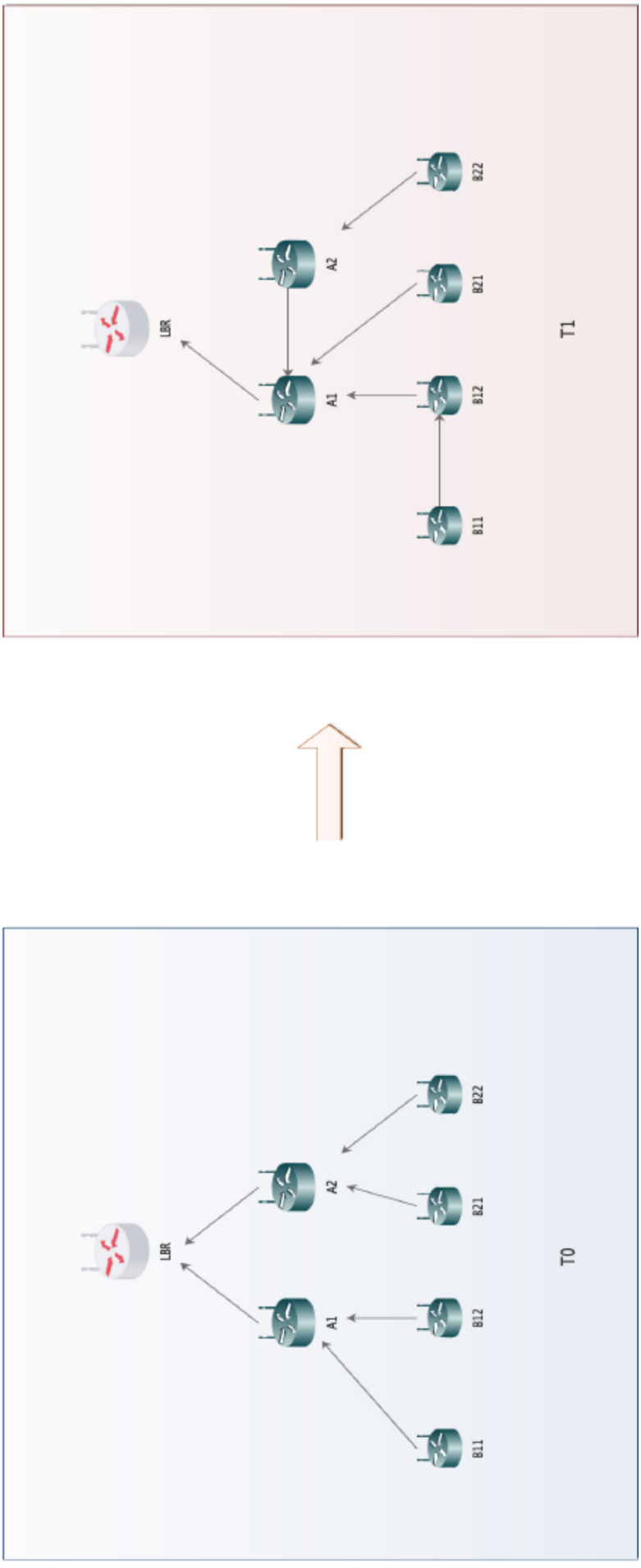

Figure 1