SWIFT NODE MIGRATION MECHANISMS FOR LOW POWER AND LOSSY NETWORKS

Dapeng Zhu
Xiaopu Zhang
Yuping Wang
Caijun Jiang

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
Zhu, Dapeng; Zhang, Xiaopu; Wang, Yuping; and Jiang, Caijun, "SWIFT NODE MIGRATION MECHANISMS FOR LOW POWER AND LOSSY NETWORKS", Technical Disclosure Commons, (August 26, 2019)
https://www.tdcommons.org/dpubs_series/2423

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.
SWIFT NODE MIGRATION MECHANISMS FOR LOW POWER AND LOSSY NETWORKS

AUTHORS:
Dapeng Zhu
Xiaopu Zhang
Yuping Wang
Caijun Jiang

ABSTRACT

Techniques are described herein to refine Personal Area Network (PAN) migration processes and shorten offline duration using various mechanisms, including: 1) performing a re-authentication and key exchange with a target PAN's Field Area Router (FAR) over a current PAN's FAR while performing migration between the two PANs; 2) eliminating a re-authentication process by sharing the same pairwise master key (PMK) for one node between all FARs in one service set; 3) synchronizing with a target PAN over current PAN's FAR, which can be quicker than synchronization over the air; and 4) eliminating Dynamic Host Configuration Protocol (DHCP) version 6 (DHCPv6) processes, keep a global Internet Protocol version 6 (IPv6) address unchanged, and creating a downward route adaptively while performing migration between the two PANs. Using these mechanisms, a node will be able to migrate between various PANs more quickly and the service interruption gap will be much shorter.

DETAILED DESCRIPTION

Field Area Routers (FARs) are routers in a Smart Grid network that are installed in the field at locations such as electricity poles. On the southbound, FARs connect Low power and Lossy Network (LLN) domains that may include a large number of devices such as sensors and actuators, also referred to as smart objects or Minimalist Connected Objects (MCOs) in some architectures using low power Radio Frequency (RF) and Power Line Communication (PLC) links. FARs usually act as directed acyclic graph (DAG) roots through which all of the traffic from the LLNs to a control center is transiting and, thus, play a critical role in the infrastructure. On the northbound, these routers communicate with the Utility Control Center using various wireless backhaul technologies such as 2nd
Generation (2G) cellular, 3rd Generation (3G) cellular, 4th Generation/Long Term Evolution (4G/LTE) cellular, and/or WiMax.

In a typical smart grid network configured for an Advanced Metering Infrastructure (AMI) application, a FAR can communicate to thousands of end-points (nodes) on the downlink (access network) using an IP-based mesh network. This mesh network is typically secured using group-based encryption keys in which these keys are initially handed over to the mesh nodes via initial authentication processes.

The nodes can connect to one or more FARs depending on various factors such as their proximity, available signal strength, interference, availability of suitable neighbors, etc. In some areas, these factors change very often, and what has been observed in deployed networks is that as many as 35% of the nodes roam or migrate to adjoining FARs on a daily basis.

The process of node migration between different PANs is quite expensive given the low mesh network bandwidth, and the load on various servers such as Authentication, Authorization, and Accounting (AAA), DHCP, and Field Network Director (FND) servers. This can be a major issue considering that the (re)joining time is a critical Service Level Agreement (SLA) component for utilities. Therefore, it is highly desirable to refine node migration process.

A goal of this proposal is to provide a swift node migration mechanism that allows nodes to switch between various PANs very quickly with awareness on service quality, reliability, and availability. A node migration process and corresponding state for current connected grid mesh (cg-mesh) implementations is shown in Figure 1, below.

![Node migration process](image)

**Figure 1**

Typically, a node remains in an offline state during migration besides the phase of discovering the new PAN. If the node has a service traffic exchange with a head-end system or other servers such as for providing a firmware upgrade while performing a migration, the service will interrupt. This process is quite expensive given the low bandwidth of the
mesh network and the load on the AAA servers. Techniques for refining node migration processes are a focus of this proposal.

It has been observed that authentication is the most significant component of PAN migration time. The existing re-authentication and key exchange for current cg-mesh systems is shown in Figure 2, below.

Consider an example involving migrating a node, referred to herein as node-A, from Pan-1 to PAN 2. For migrating to PAN-2, node-A needs to first leave PAN-1 and then re-authenticate with FAR-2. Once node-A leaves PAN-1, node A will enter an offline state; therefore, all services for node-A will interrupt. Maintaining service reliability can involve either eliminating re-authentication or remaining in online state during re-authentication.

A first component of the proposal provided herein includes a mechanism to perform re-authentication and key exchange with a new FAR over an old RAR while a node is migrating to a new PAN. Consider the example, as shown in Figure 3, in which node-A re-authenticates with FAR-2 over FAR-1.

Figure 2

Consider an example involving migrating a node, referred to herein as node-A, from Pan-1 to PAN 2. For migrating to PAN-2, node-A needs to first leave PAN-1 and then re-authenticate with FAR-2. Once node-A leaves PAN-1, node A will enter an offline state; therefore, all services for node-A will interrupt. Maintaining service reliability can involve either eliminating re-authentication or remaining in online state during re-authentication.

A first component of the proposal provided herein includes a mechanism to perform re-authentication and key exchange with a new FAR over an old RAR while a node is migrating to a new PAN. Consider the example, as shown in Figure 3, in which node-A re-authenticates with FAR-2 over FAR-1.
Using the mechanism illustrated in Figure 3, the offline period for node-A can be shortened, as shown in Figure 4, below.

At least one advantage of the mechanism illustrated in Figure 3 is that node-A stays in online state and all service traffic exchange with head-end system and/or other servers doesn't interrupt while re-authenticating and exchanging key with FAR-2.

A second component of the proposal provided herein includes a mechanism to eliminate the re-authentication process by sharing the same PMK for one node between all FARs in one service set.

In current cg-mesh implementations, when joining a PAN (e.g., PAN-1 or PAN-2), such as PAN-1, for the first time, node-A first performs a full authentication, then both FAR-1 and node-A obtain a PMK and a subsequent 4-way handshake is performed based on the PMK. While migrating to PAN-2, node-A needs to re-authenticate with FAR-2.
This proposal provides an enhancement to the existing mechanism in which, once node-A finishes the 4-way handshake, FAR-1 can distribute the PMK to all other FARs, such as FAR-2, in the same service set as shown in Figure 5, below.

![Figure 5](image)

At least one advantage of the mechanism illustrated in Figure 5 is that node-A will be able to skip the re-authentication process and go straight to the 4-way handshake, namely key exchange, as shown in Figure 6, below. This mechanism can highly reduce migration time and help a node recover a previous service with higher speed.

![Figure 6](image)

In some previous solutions, a node would need to go through the authentication process when migrating to another FAR for the first time. Using the PMK distribution mechanism as provided by the present proposal, a node can skip the authentication process while migrating as long as it has undergone a full 802.1x authentication with any FAR in the same service set.
A third component of the proposal provided herein includes a mechanism to synchronize with a new PAN over an old FAR while migrating to the new PAN. It has been observed that synchronization is the second significant component of PAN migration time.

Consider the example involving node-A. Because a sync beacon is typically transmitted in a non-deterministic way instead of Time Slot Channel Hopping (TSCH), it is possible that node-A may have to spend a large amount of time waiting for a sync beacon from PAN-2.

Based on the first component, as discussed above, this proposal further provides that once node-A finishes its key exchange, FAR-2 sends broadcast schedule information to node-A via FAR-1, as shown in Figure 7.

Sending the broadcast schedule to node-A over FAR-1 may have at least two advantages: 1) it can help node-A get synchronized with PAN-2 more quickly; and 2) node-A can remain in online state as shown in Figure 8, below, to maintain service reliability with PAN-1.
Finally, a fourth component of the proposal provided herein includes a mechanism to eliminate the DHCPv6 global address configuration process and keep the global address unchanged while migrating to a new PAN.

Typically, the Routing Protocol for LLN (RPL) protocol uses a Destination Advertisement Object (DAO) message to build a downward route table (e.g., as shown in Figure 2). FAR-2 can still build a valid download route to node-A even if it keeps the global IPv6 address unchanged while migrating from PAN-1 to PAN-2. However, there is an issue that downward traffic from the head-end system to node-A will still be forwarded to FAR-1, but FAR-1 cannot reach node-A, so this traffic will be dropped.

By leveraging the above components, FAR-2 can know node-A migrates from PAN-1, so once FAR-2 receives a DAO message from node-A, it can notify FAR-1 to update the route to node-A: (Destination: node-A, Next-hop: FAR-2), so all downward traffic to node-A will be communicated using the path shown in Figure 9, below.
Keeping the global IPv6 address unchanged may have several advantages including, but not limited to: 1) avoiding re-registration processed with the FND and head-end system (e.g., in current cg-mesh systems, if a node changes its global IPv6 address, it needs to re-register with the FND and head-end system); and 2) skipping the DHCPv6-based IPv6 address configuration process. Accordingly, the node migration process can be refined as illustrated in Figure 10, below.

![Node migration process](image)

**Figure 10**

Thus, the node migration process and offline duration can be refined as shown in Figure 10 using the above four components. Accordingly, a node can migrate between various PANs more swiftly and the service interruption gap will be much shorter using techniques as provided by this propose.

In summary, techniques are described herein to refine PAN migration processes and shorten offline duration using various mechanisms, including: 1) performing a re-authentication and key exchange with a target PAN's FAR over a current PAN's FAR while performing migration between the two PANs; 2) eliminating a re-authentication process by sharing the same PMK for one node between all FARs in one service set; 3) synchronizing with a target PAN over current PAN's FAR, which can be quicker than synchronization over the air; and 4) eliminating DHCPv6 processes, keeping the global IPv6 address unchanged, and creating a downward route adaptively while performing migration between the two PANs. Using these mechanisms, a node will be able to migrate between various PANs more quickly and the service interruption gap will be much shorter.