December 2020

NOVEL SECURED INTER-PERSONAL AREA NETWORK GROUP MANAGEMENT IN LOW-POWER AND LOSSY NETWORKS

Nan Yi

Wenjia Wu

Huimin She

Lele Zhang

NOVEL SECURED INTER-PERSONAL AREA NETWORK GROUP MANAGEMENT IN LOW-POWER AND LOSSY NETWORKS

AUTHORS:
Nan Yi
Wenjia Wu
Huimin She
Lele Zhang

ABSTRACT

Low-power and Lossy Network (LLN) environments may comprise, possibly among other things, different personal area networks (PANs) resulting in, for example, node communication challenges across or between PANs. To address these types of challenges, techniques are presented herein that support a novel secure group management method to self-solve the inter-PAN problem that is both low-cost and customer-friendly. Aspects of the techniques presented herein encompass establishing a secure node-to-node (N2N) communication link between involved inter-PAN nodes, automatically looking for the relay neighbors between different PANs (as the inter-PAN node can help with forwarding the local the Routing Protocol for LLN (RPL) messages), automatically propagating the group information and maintaining the local RPL tree between the inter-PAN nodes, etc. Aspects of the techniques presented herein employ, among other things, spreading PAN advertisement (PA) messages with group and hop information to identify a feasible routing path, using the Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) protocol to establish a secure transport tunnel, automatically unicasting a destination-oriented directed acyclic graph (DODAG) Information Solicitation (DIS) message to join the group tree, etc. Under aspects of the techniques presented herein an application server need not know the topology of a network.

DETAILED DESCRIPTION

The Wireless Smart Utility Network (Wi-SUN) alliance promotes the Institute of Electrical and Electronics Engineers (IEEE) technical standard 802.15.4g standards-based interoperability for the Internet of Things (IoT) in LLNs such as, for example, a distribution

automation (DA) application. In a Wi-SUN field area network (FAN) the RPL (see Request for Comments (RFC) 6550) is the routing protocol and the EAP-TLS (see RFC 5216) is the authentication protocol. These elements play significant roles in LLNs.

In a customer's deployment, border routers with a different PAN identifier (ID) may be employed in the customer's applications. Nodes will join different PANs and register to the same application center. Due to latency and reliability requirements the application will determine an area of involved nodes as a group to build an additional local RPL tree. The root (e.g., application server) could collect and process information from the involved nodes. For example, as depicted in Figure 1, below, there is a PAN A where Node R is the application server that may collect information from the other red nodes. The red nodes will form a local RPL tree towards Node R with a specified RPL instance ID.

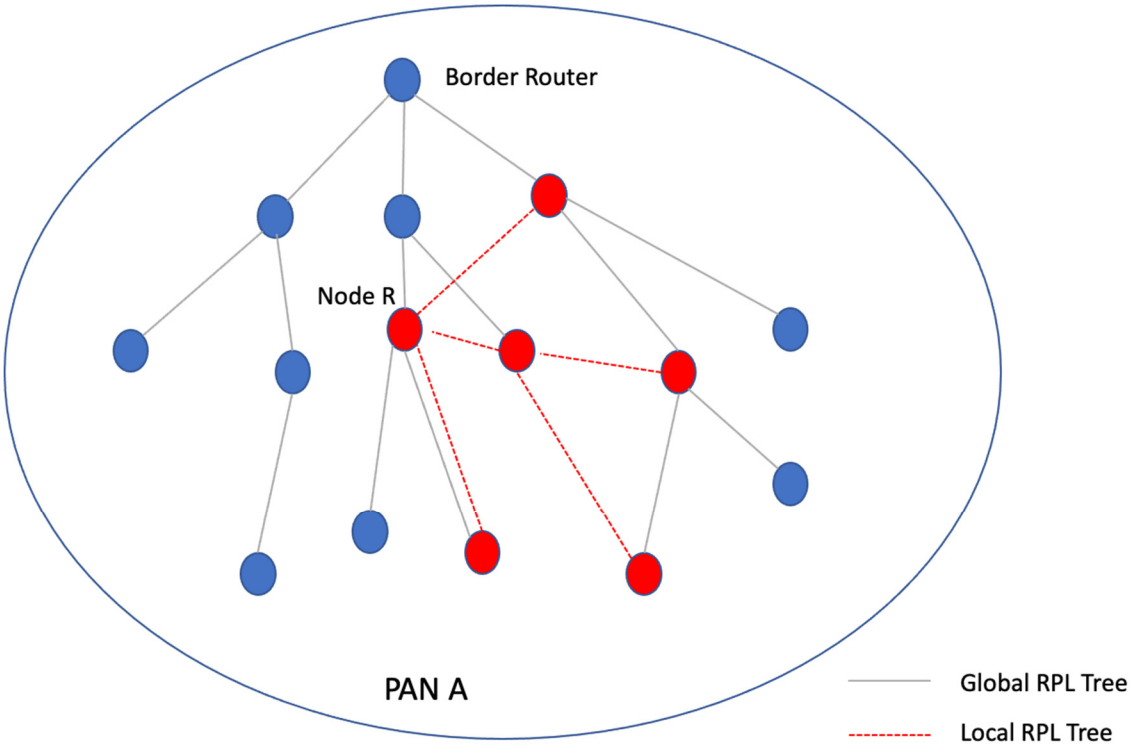

Figure 1: Illustrative PAN

However, applications do not necessarily know the topology of the involved nodes. The inter-PAN disconnection problem must be solved if the involved nodes belong to

different PANs. The nodes in the same application group are not able to join the same local RPL tree since they belong to different PANs. For example:

- In Figure 1, above, the red nodes belong to a group and they will form a local RPL tree.
- In Figure 2A, below, Node B has joined PAN B. It does not know PAN A's broadcast information and is unable to decrypt any encrypted messages from PAN A.
- In Figure 2B, below, the red nodes belong to a group and they will build up a local RPL tree. Node B has joined PAN B, but it is unable to hear any messages from the same group.

Consequently, Node R is unable to communicate with node B through the local RPL tree.

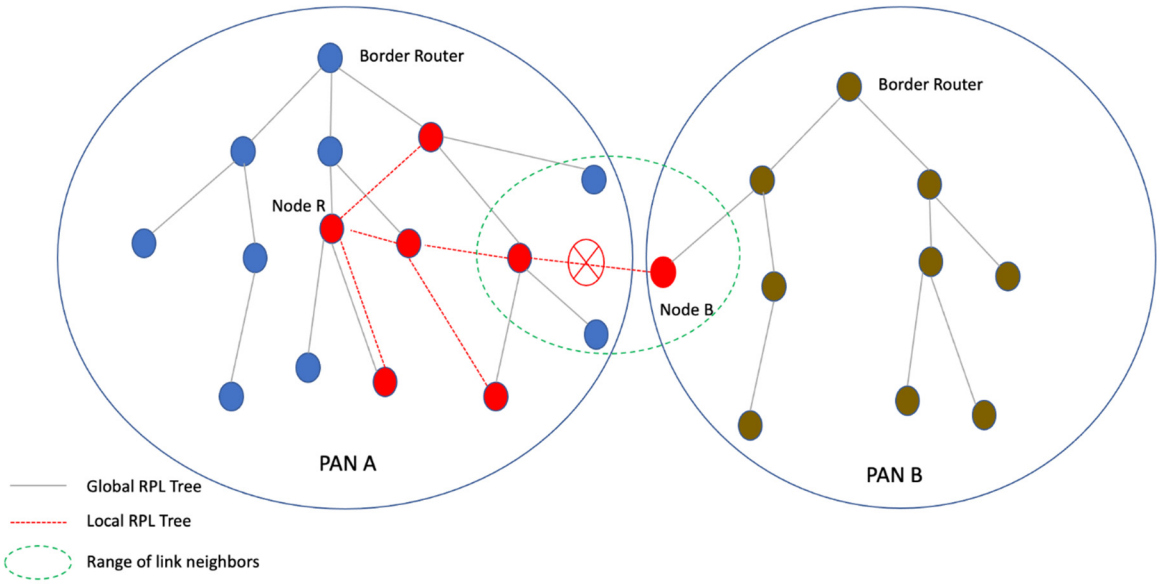

Figure 2A: Node B Joining PAN B

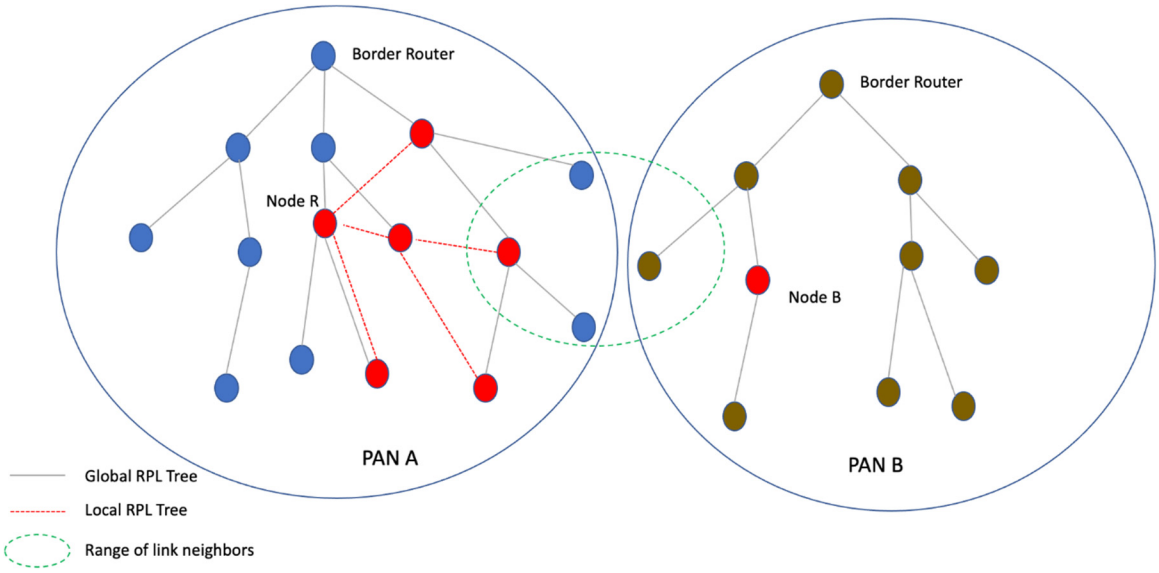

Figure 2B: Node B Unable to Receive Messages

To address the types of challenges that were described above, techniques are presented herein that support a novel secure group management method to self-solve the inter-PAN problem. Aspects of the method include, for example:

- Establishing a secure node-to-node (N2N) communication link between involved inter-PAN nodes.
- Automatically looking for the relay neighbors between different PANs, as the inter-PAN node can help with forwarding the local RPL messages.
- Automatically propagating the group information and maintaining the local RPL tree between the inter-PAN nodes.

For example, as illustrated in Figure 3, below, Node B is not able to receive any packets from the same group. But it can activate Node D as a group inter-PAN node, establish a secure link with Node C, and help forward local RPL messages inter-PAN and make Node B join this local RPL tree.

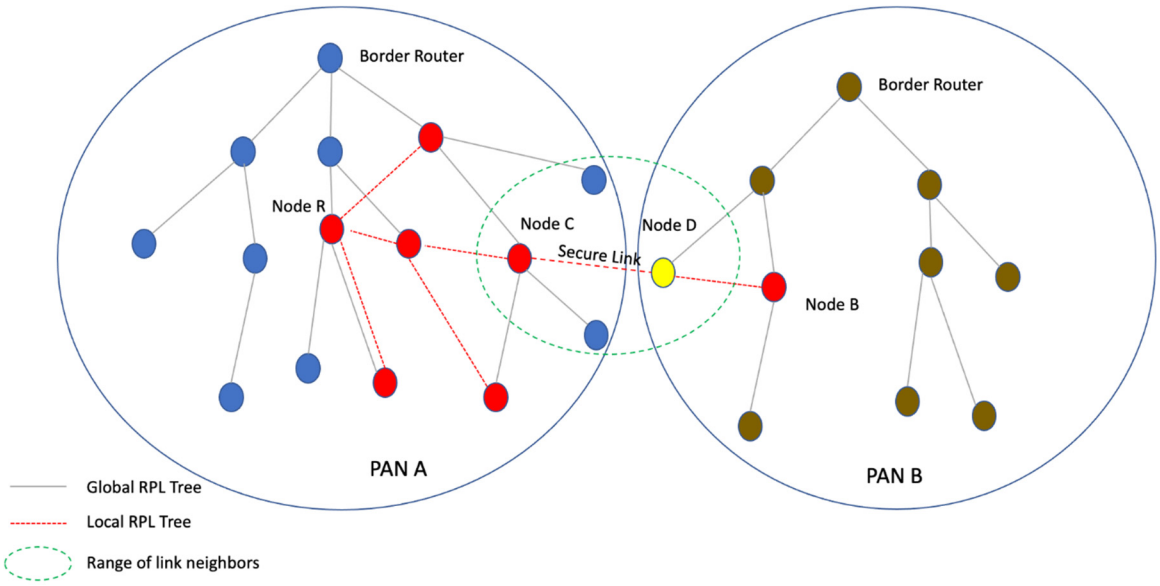

Figure 3: Illustrative Group Inter-PAN Node

As noted previously, techniques are presented herein that support a novel secure group management method to self-solve the inter-PAN problem within the involved nodes in LLNs.

In LLNs, considering the customers' deployments and the variable network topology, the involved nodes in a same group may belong to different PANs. When the nodes need to self-construct the group management, the inter-PAM problem arises. For example, in some customer instances the application server may not know the topology of the LLNs. Some specified nodes may have been selected in the LLNs as a group to form a local RPL tree, for managing and aggregating information more efficiently. The root node will broadcast a DODAG information object (DIO) with a specified RPL instance ID and the involved nodes in the same PAN will join the local RPL tree through the RPL protocol. Therefore, the involved nodes in the same PAN need to join the local RPL Tree.

However, the nodes in another PAN (i.e., other-PAN nodes) cannot join the local RPL tree due to the inter-PAN problem. For example, as depicted in Figure 4, below, Node B and Node G do not know the broadcast schedule about PAN A and cannot decrypt the DIO messages from PAN A, which will cause its failure to join the local RPL tree.

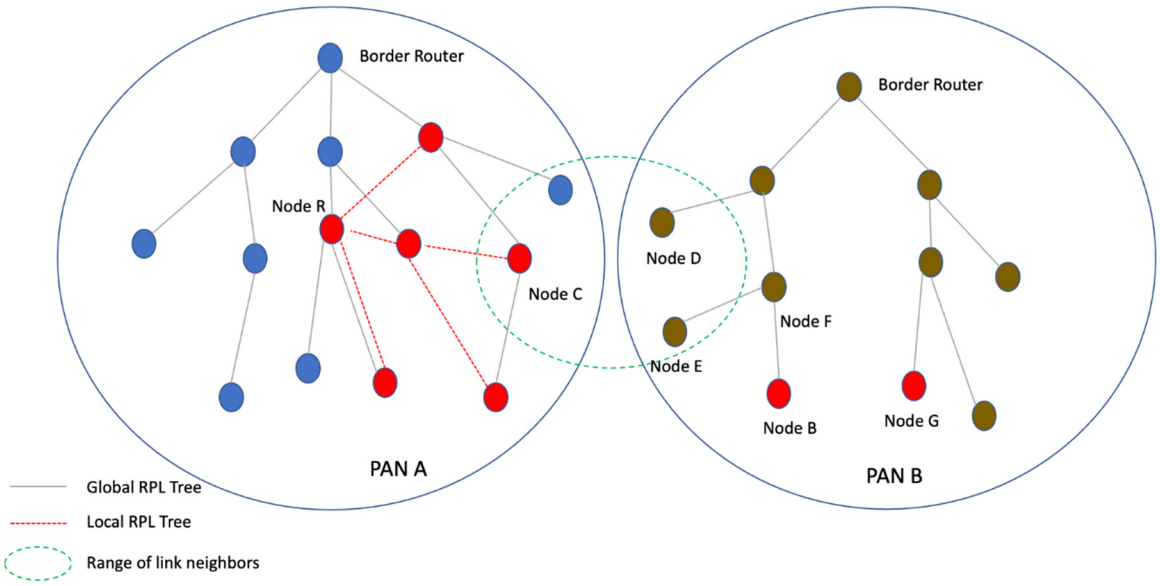

Figure 4: Nodes B and G Unable to Join Local RPL Tree

Aspects of the techniques presented herein include a number of unique elements, various of which are briefly described below.

A first element of the techniques presented herein comprises propagating group and predicted hop information by the unencrypted asynchronous discovery messages, such as a PA. A node may help its neighbors to propagate this information using its own discovery message if the predicted hop is less than the limited maximum hop.

Under aspects of the techniques presented herein, when nodes have joined the group management the nodes will broadcast their RPL information and propagate the discovery message with its group and hop information. Additionally, their neighbors will help to spread the group and predicted hop information through their own discovery messages. In order to reduce message flooding the predicted hop shall be less than the limited maximum hop in a local RPL tree. For example, as depicted in Figure 5, below, after Node C joins the local RPL tree it will broadcast its local RPL DIO and send out a PA with its group and hop information in this local RPL tree.

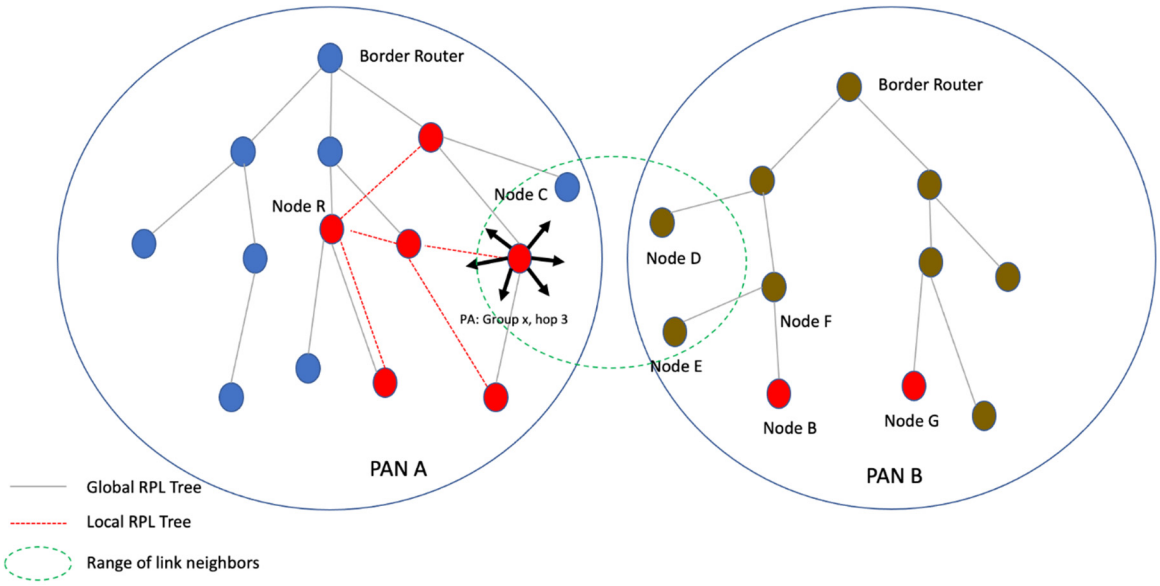

Figure 5: Node C Joins Local RPL Tree

Once Node D and Node E receive the PA messages with the group and hop information, they will process the messages, predict their own hop (such as the minimum of the original-hop plus one) in the tree, and propagate the group and hop information in the PA. See Figure 6, below.

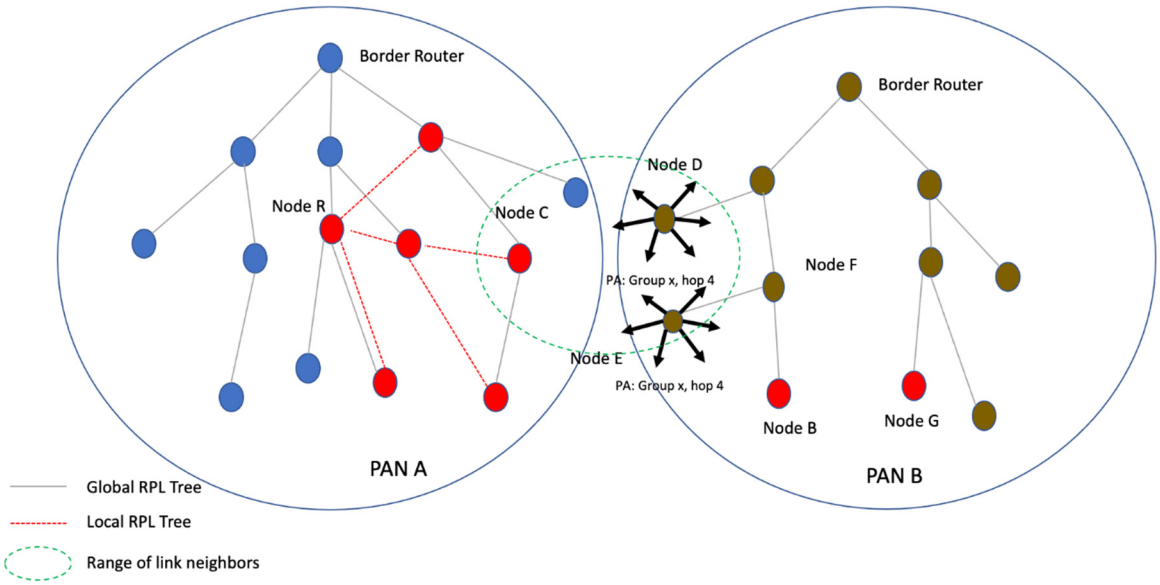

Figure 6: Nodes D and E Respond to Received PA Messages

As depicted in Figure 7, below, Node F will receive the PA messages from Node E and Node D, choose a better node as proxy, and send the information out in its PA. Finally, the red Node B will receive this information

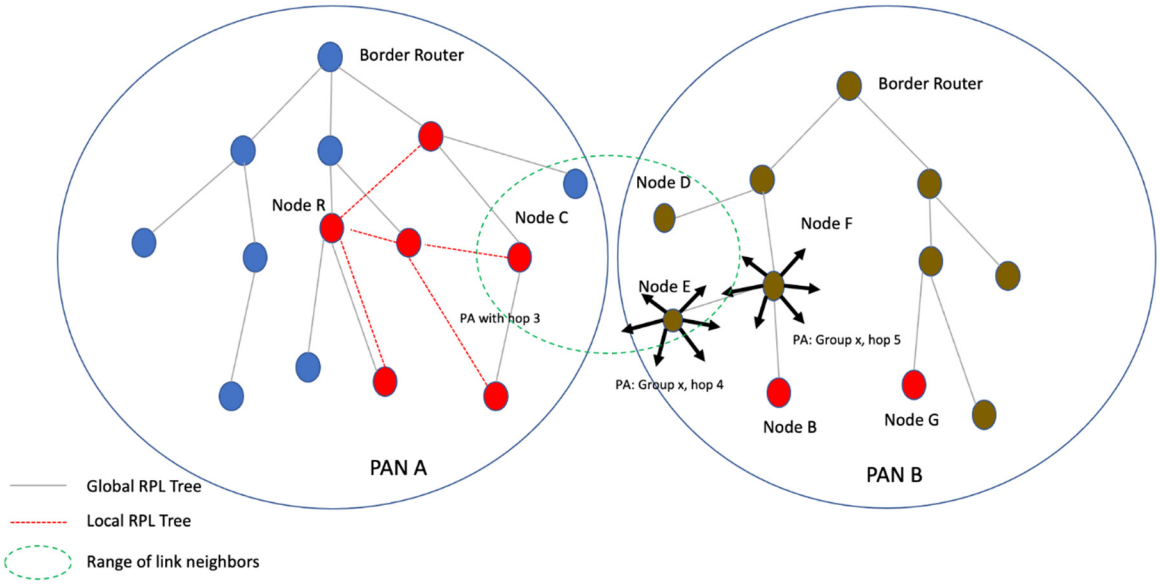

Figure 7: Node F Responds to Received PA Message

A second element of the techniques presented herein comprises the other-PAN nodes selecting the best proxy and triggering the inter-PAN node establishing a secure N2N link with the inter-PAN peer.

As illustrated in Figure 8, below, Node B will receive PAs with group and hop information from its neighbors and it will select the best predicted hop neighbor as a proxy. Node E will be Node B's best proxy. Then Node B will unicast a EAP-TTLS start with group information to its proxy Node E.

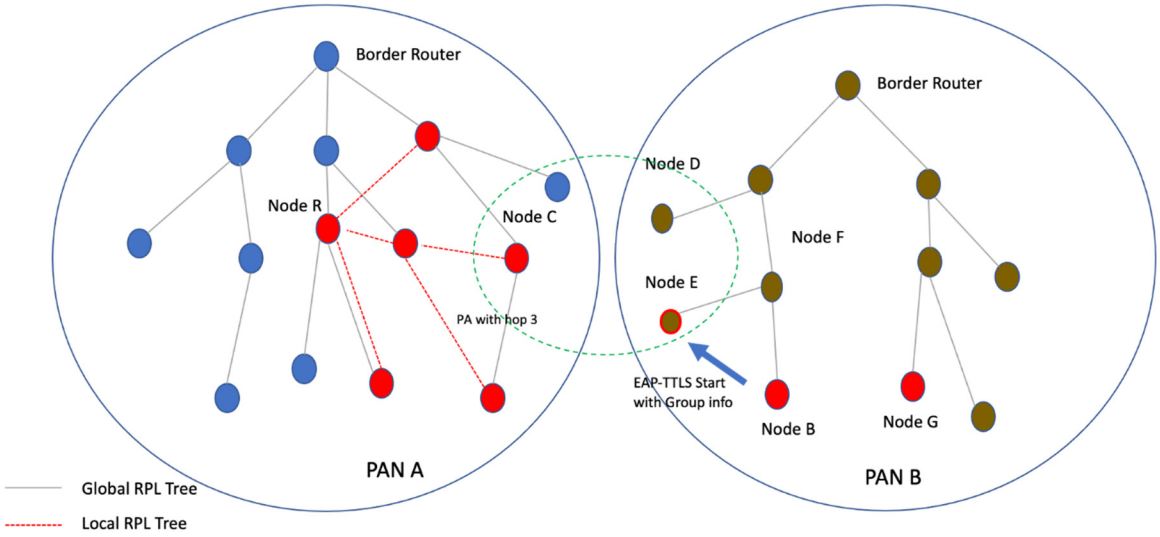

Figure 8: Node B Responds to Received PA Message

As depicted in Figure 9, below, once Node E receives the EAP-TTLS start message, Node E will trigger an EAP-TTLS start to its best proxy Node C.

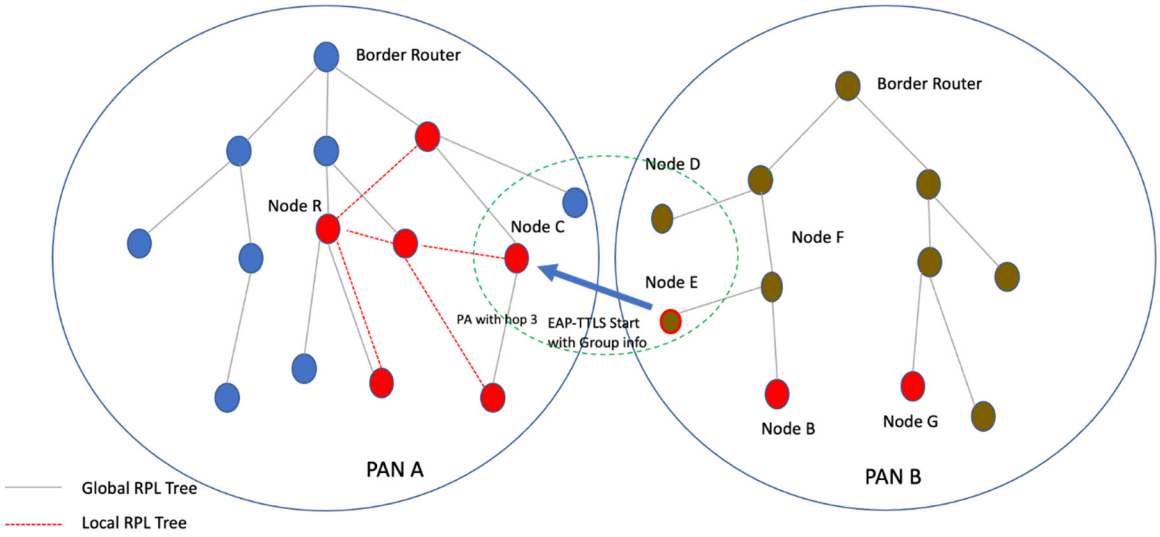

Figure 9: Node E Responds to EAP-TTLS Message

As depicted in Figures 10 and 11, below, Node C as the authenticator will accept the EAP-TTLS start message, complete a handshake and create a tunnel (employing EAP-TTLS according to RFC 5281) with Node E. Node E is then able to join the group.

Through the tunnel, the inter-PAN nodes Node C and Node E may safely communicate with each other.

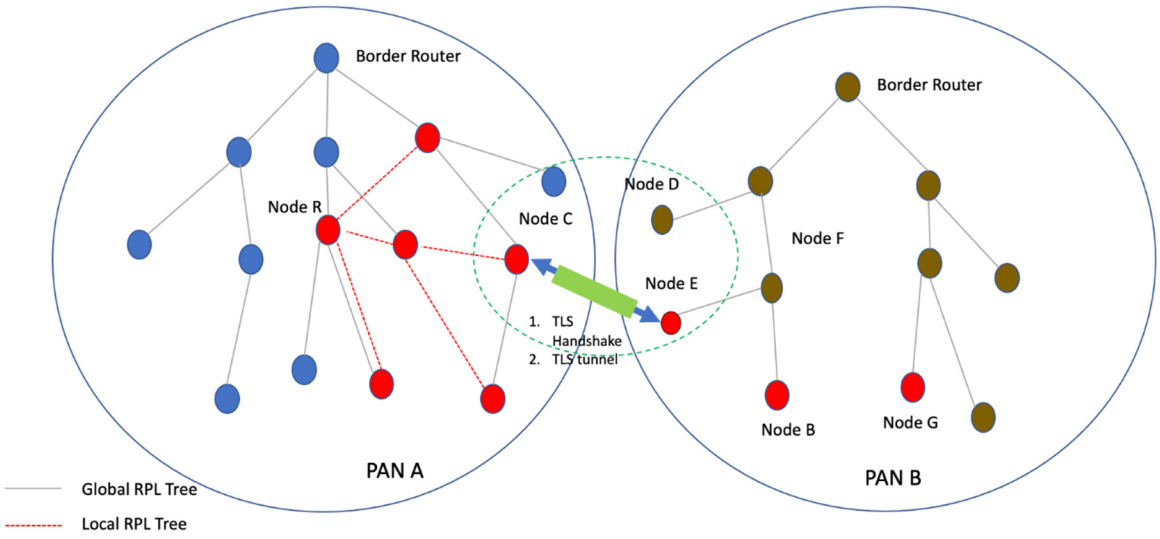

Figure 10: Node C Responds to EAP-TTLS Start Message

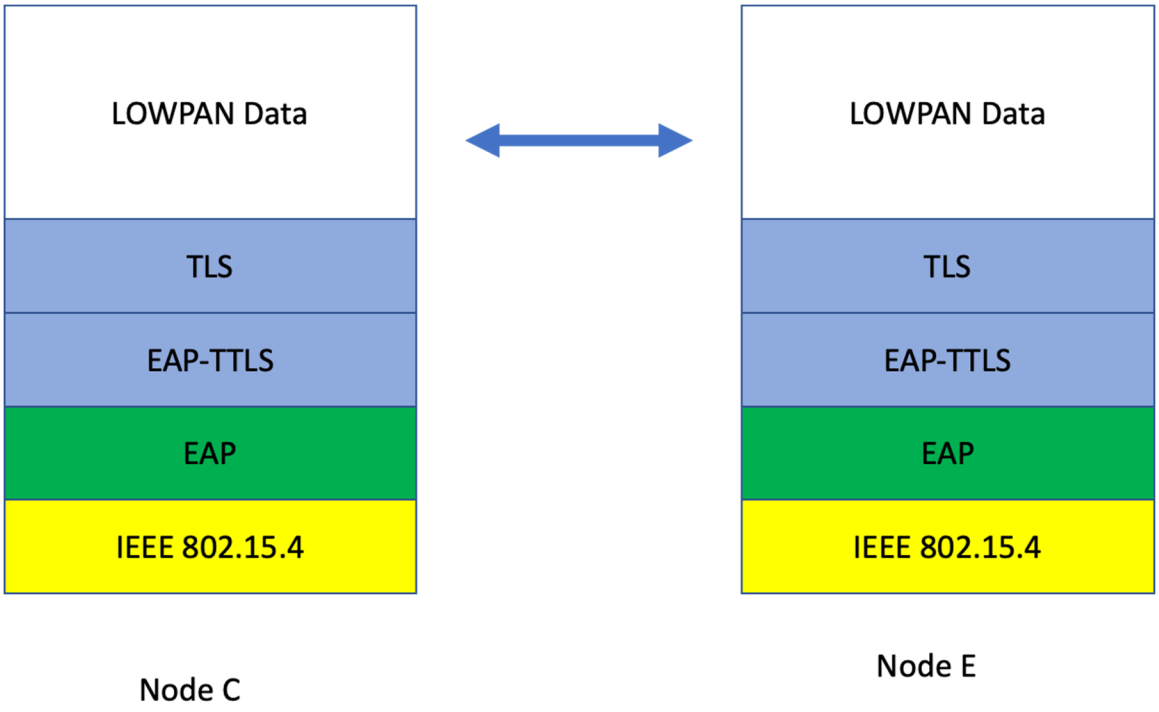

Figure 11: Illustrative Protocol Stack

A third element of the techniques presented herein comprises the inter-PAN nodes automatically requesting RPL information (e.g., a DIO), joining the group tree, and propagating RPL information in its PAN.

As illustrated in Figure 12, once Node E joins the group, it will automatically unicast a DIS message to Node C on the secure tunnel to get the local RPL DIO and join the local RPL tree. Then Node E will broadcast the local RPL DIO in its PAN, and Nodes B and G will join the local RPL Tree.

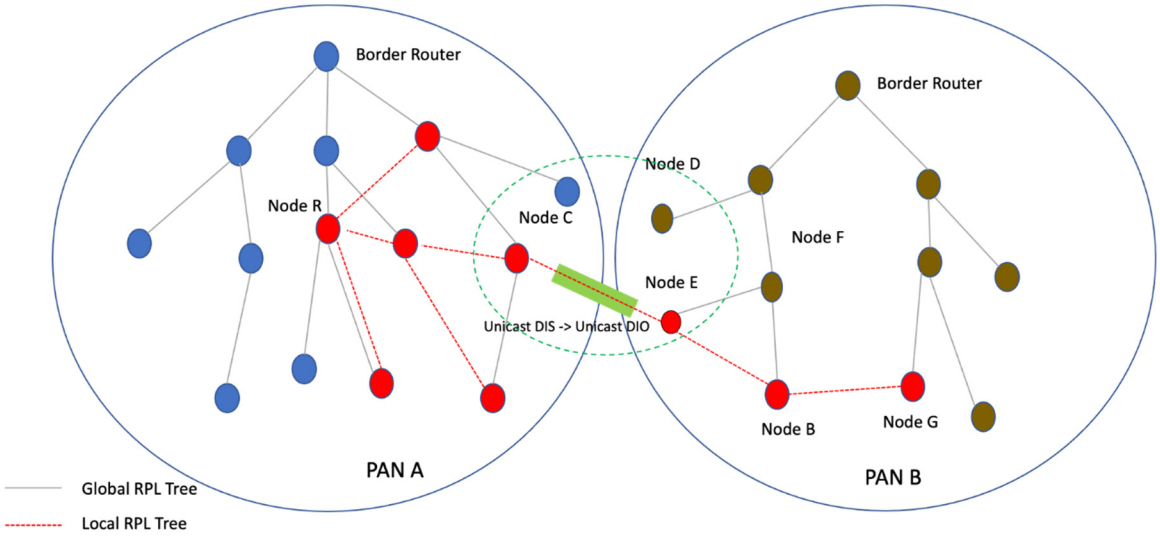

Figure 12: Node E Joins the Local RPL Tree

In summary, techniques have been presented that support a novel secure group management method to self-solve the inter-PAN problem that is both low-cost and customer-friendly. Aspects of the techniques presented herein encompass establishing a secure N2N communication link between involved inter-PAN nodes, automatically looking for the relay neighbors between different PANs (as the inter-PAN node can help with forwarding the local RPL messages), automatically propagating the group information and maintaining the local RPL tree between the inter-PAN nodes, etc. Aspects of the techniques presented herein employ, among other things, spreading PA messages with group and hop information to identify a feasible routing path, use of the EAP-TTLS protocol to establish a secure transport tunnel, automatically unicasting a DIS message to

join the group tree, etc. Under aspects of the techniques presented herein an application server need not know the topology of a network.