October 2020

ZERO TRUST: DISTRIBUTED AND LIGHT-WEIGHT AUTHENTICATION FOR WORMHOLE ATTACKS IN LOW-POWER AND LOSSY NETWORKS

Ling Wei

Huimin She

Chuanwei Li

Lele Zhang

ZERO TRUST: DISTRIBUTED AND LIGHT-WEIGHT AUTHENTICATION FOR WORMHOLE ATTACKS IN LOW-POWER AND LOSSY NETWORKS

AUTHORS:
Ling Wei
Huimin She
Chuanwei Li
Lele Zhang

ABSTRACT

Anomaly detection in a Low-Power and Lossy Network (LLN) is important in light of threats such as a wormhole attack. However, such detection is challenging given node constraints such as, for example, limited power and memory. Techniques are presented herein that address those challenges thus benefiting the stability, reliability, and security of LLNs. The presented techniques include, among other things, a distributed and light-weight authentication method (where identification of a suspicious node is done locally, between two nodes, thus obviating heavy traffic upward to a root node) and a node rating credit rank mechanism (through which, for example, a node may detect whether there is a wormhole attack).

DETAILED DESCRIPTION

The Wireless Smart Utility Network (Wi-SUN) alliance promotes Institute of Electrical and Electronics Engineers (IEEE) 802.15.4g standards-based interoperability for the Internet of Things (IoT) in a LLN. Such a network typically contains thousands of nodes, with each node having limited resources such as, for example, memory, energy, computing capability, etc. Due to high quality of service (QoS) requirements in terms of low latency, low routing cost, low packet loss, etc., these constrained nodes attempt to select a preferred parent node as a default upward router. Thus, if an attacker compromises two legitimate nodes and claims it offers better conditions to be a parent, many other nodes will be deceived and will select a malicious node as their parent node. Then, the whole network may suffer from various kinds of wormhole attacks by the malicious nodes.

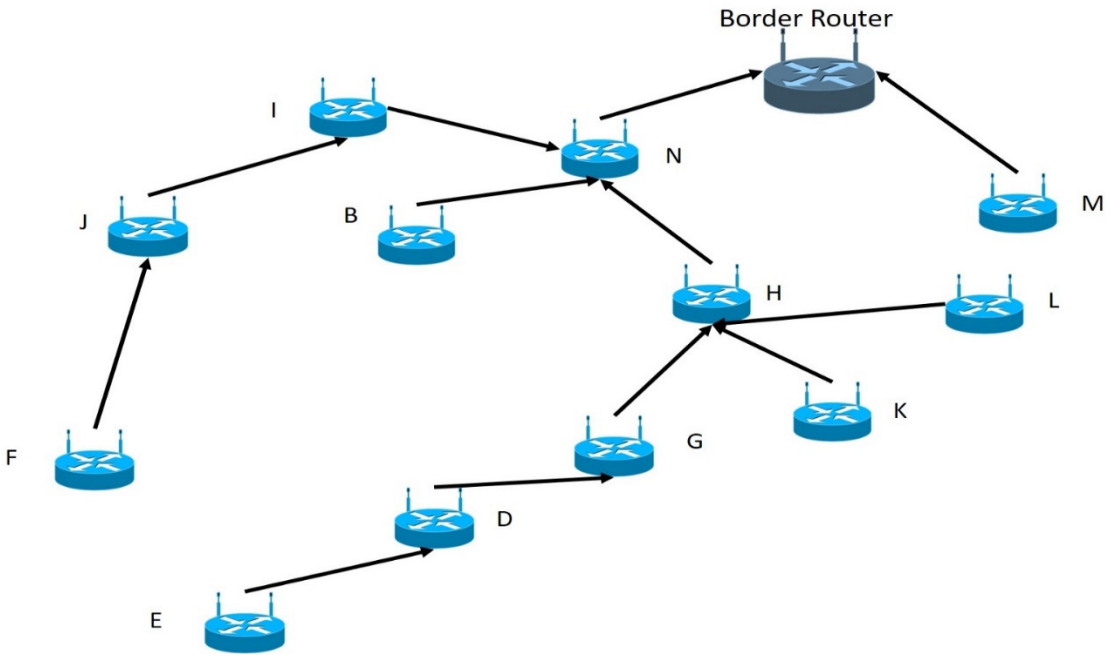

Figure 1: Illustrative LLN Network Topology

Figure 1, above, illustrates an initial LLN network topology. Two malicious nodes, node A and node C, then compromise the network, as shown in Figure 2, below. Node C will periodically broadcast false routing information in the neighborhood, thus deceiving the innocent nodes (i.e., D, E, F, G, J) into attaching to it. Even though a security mechanism is used to protect the network, that is not secure enough for LLNs. For Wi-SUN, a group key (e.g., GTK) is used to encrypt/decrypt media access control (MAC) frames. If the key is revealed or cracked by an attacker, any malicious node can easily become a wormhole node. Unfortunately, these kinds of attacks are very difficult to detect and prevent within the thousands of nodes in a LLN.

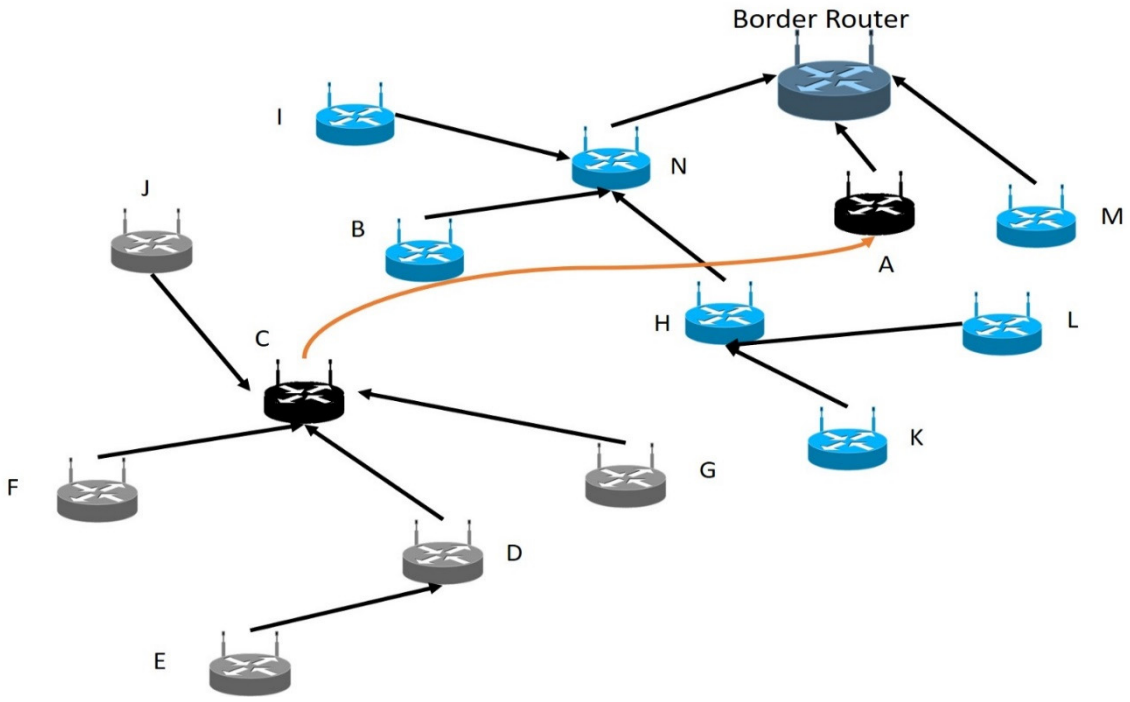

Figure 2: Compromised LLN Network Topology

Techniques are presented herein that support a novel distributed light-weight authentication mechanism between two nodes to detect and prevent a wormhole attack in LLNs.

As noted previously, a wormhole attack is very difficult to detect in LLNs. For example, according to the Routing Protocol for LLN (RPL), a child node will not change its parent node as long as the link quality or condition between them is good enough even though the upper layer's traffic may always fail due to a wormhole attack. In addition, the wormhole node will broadcast its false routing conditions to deceive its neighbor nodes to attach to it, such as, for example, a fake rank value and a fake hop count.

To address these problems, along the lines of a zero trust network, aspects of the techniques presented herein make use of a distributed and tiny certification authentication to verify the suspicious L2 link security between two nodes. Elements of particular interest and note within the techniques that are presented herein are discussed below.

A first element includes a light-weight authentication method that leverages the existing certification between two connected nodes. For example, in Wi-SUN the public key infrastructure is based on IEEE 802.1x and Extensible Authentication Protocol (EAP)-

Transport Layer Security (TLS) using Initial Device Identifier (IDevID) concepts to provide secure device identity. Therefore, every node must have a root certificate that is signed by a Wi-SUN approved manufacturer certificate authority (CA). Each node has its embedded node certification which is signed by a CA private key that is used to send to a server to verify its legal identity. In addition, within a personal area network (PAN) or a field area network (FAN) every node has the same CA public key to verify the legal identity of a server. Therefore, aspects of the techniques presented herein can make use of the existing node certification to verify the node legality between any two connected nodes when a node joins a FAN. For example, as shown in Figure 3, below, if Node A wants to check to see if Node B is a wormhole node it may send the node authentication request message to Node B. The two nodes may then exchange respective certifications and verify each other. As an additional layer of security, because the certification includes the identity information such as the owner's public key, the suspicious node could send a specific message signed by its private key after the node authentication process and the other node will use the public key in the adverse certification to decrypt the specific message. If it fails, it proves that the suspicious node stole the other node's certification and it is a malicious node.

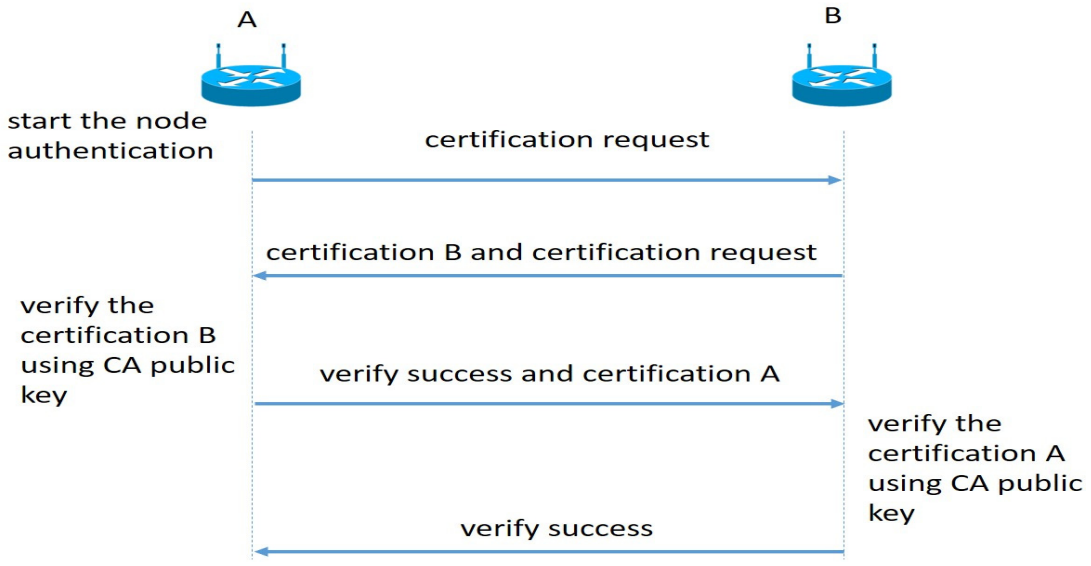

Figure 3: Light-weight Authentication Method

A second element within the techniques that are presented herein comprises a rating credit rank mechanism for a node to determine the certification request initiation (e.g., when should a node start a certification request for its neighbor node?).

In the beginning, a node considers that all of its neighbor nodes are reliable and grants them a fair credit rank value. If any exceptional network phenomena arise – such as, for example, the dropping of numerous application packets, suddenly explosive traffic, strange topology changes, unexpected packet transmission, etc. – the credit rank value of a target node will be decreased accordingly. A specific timer may be employed to calculate this value periodically. If the credit rank value is lower than a fixed value, a node will trigger the timer event to start the node authentication request (as described above). If such an authentication fails it may report the information to the root node, and the root node will double check and take the appropriate next step.

For example, as illustrated in Figure 4, below, Node E finds that most of its application packets are dropped but the L2 link is very good. It may then start the node authentication mechanism with node D. But it is not sure whether node D is a wormhole because any node in the upward path could be a malicious node. However, the node could detect the network attack and identify the suspicious upward path.

A third element within the techniques that are presented herein comprises upward path verification – e.g., once a node detects a potential wormhole attack in the suspicious upward path, it requests its parent node complete certification authentication as described in the first element summary above.

For example, as illustrated in Figure 4, below, after Node E finds that there is a wormhole attack in its upward path it will ask its parent node (Node D) for node authentication. If that authentication succeeds then Node D will ask its parent node (Node C) for node authentication. Finally, the wormhole node doesn't have the correct node certification and will be discovered by its child node.

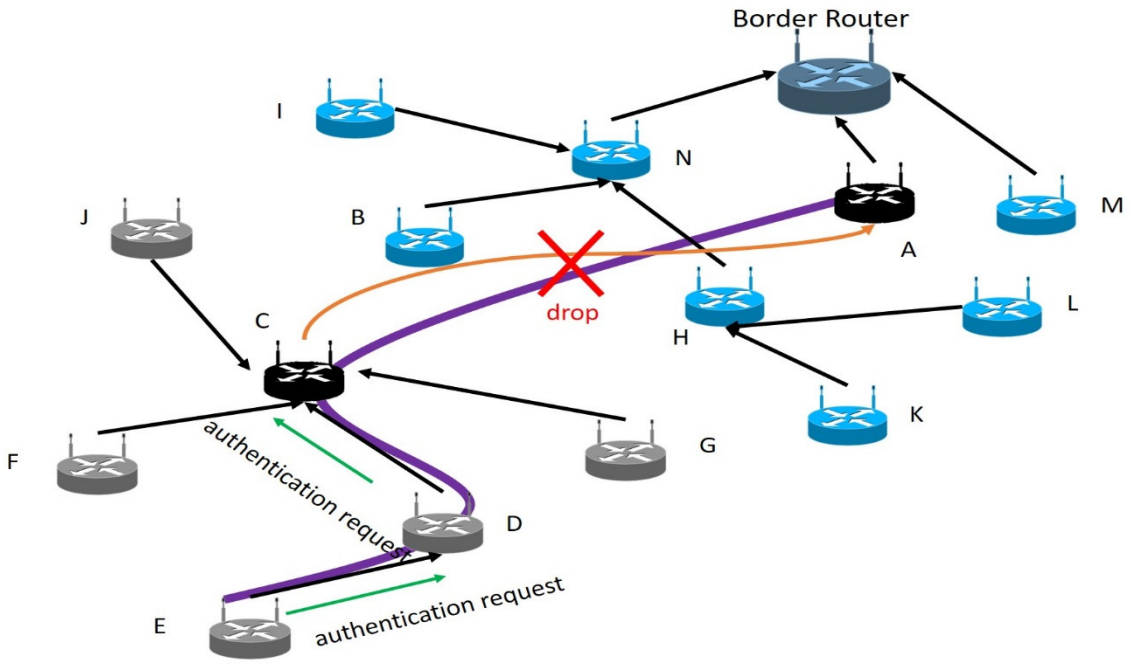

Figure 4: Illustrative Node Authentication

A fourth element within the techniques that are presented herein comprises distributed authentication. A border router supervises the global network status, including the network topology, network traffic, and network congestion. When it finds a suspicious node it will request that the node start the node authentication process with its neighbor nodes to verify its legality.

This authentication process may happen anywhere, and may reduce network congestion and save network traffic. At the same time, based on zero trust network concepts, the wormhole nodes could be detected quickly in LLNs, which is not a time-sensitive network. For example, as illustrated in Figure 5, below, the border router discovers that the Node C and Node L suddenly become many nodes' parent nodes and the network topology as such has changed. It then requests that their neighbor nodes (e.g., Node B and Node J, respectively) begin the node authentication request with Node C and Node L. If any node cannot provide the effective node certification for its neighbor node, it will be regarded as a malicious node. The authentication process takes place locally, which has limited influence on the global network performance.

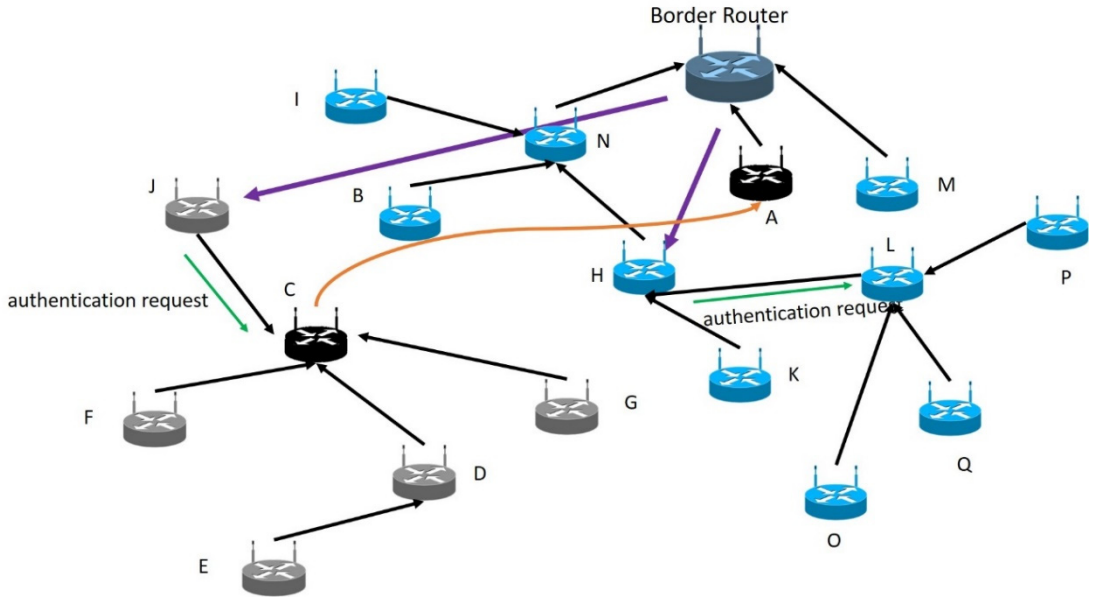

Figure 5: Distributed Authentication

A fifth element within the techniques that are presented herein comprises reporting. After a node discovers a malicious node around it, it will report the suspicious situation to the border router. The border router has to double check if the suspicious node is really a malicious node or not. If it is, the border router must refresh the group key process in LLNs to prevent the continuous wormhole attack.

In summary, techniques herein provide a new light-weighted authentication mechanism that may complement security methods for anomaly detection in LLNs. Anomaly detection can be facilitated through a preliminary judgement locally by a node itself and validation of the identity legality of a suspicious node can be performed between two nodes, which provides a traffic savings to the root node. If the validation fails, the failure can then be reported to the root node to take a next step. Thus, the presented techniques leverage the existing certification between two connected nodes (allowing identification of a suspicious node to be done locally, between two nodes, thus obviating heavy traffic upward to a root node), employ a rating credit rank mechanism, support upward path verification, and employ distributed authentication.