Journal of Network and Computer Applications ■ (■■■■) ■■■–■■■

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Puppet attack: A denial of service attack in advanced metering infrastructure network

Ping Yi [a,*], Ting Zhu [b], Qingquan Zhang [b], Yue Wu [a], Li Pan [a]

[a] National Engineering Laboratory for Information Content Analysis Technology, School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

[b] Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, MD 21250, USA

ARTICLE INFO

Keywords:
Security
Denial of service
Puppet attack
Advanced metering infrastructure

ABSTRACT

Advanced Metering Infrastructure (AMI) is the core component in a smart grid that exhibits a highly complex network configuration. AMI shares information about consumption, outages, and electricity rates reliably and efficiently by bidirectional communication between smart meters and utilities. However, the numerous smart meters being connected through mesh networks open new opportunities for attackers to interfere with communications and compromise utilities assets or steal customers private information.

In this paper, we present a new DoS attack, called puppet attack, which can result in denial of service in AMI network. The intruder can select any normal node as a puppet node and send attack packets to this puppet node. When the puppet node receives these attack packets, this node will be controlled by the attacker and flood more packets so as to exhaust the network communication bandwidth and node energy. Simulation results show that puppet attack is a serious and packet deliver rate goes down to 20–10%. After analyzing the puppet attack, we propose the detection and prevention mechanism. Simulations show that puppet attack causes the same damage as a flooding attack and the proposed method can prevent the puppet attack efficiently.

1. Introduction

Smart grid delivers electricity between suppliers and consumers using two-way digital technology to control intelligent appliances at consumers home or building to save energy, reduce cost and increase reliability, efficiency and transparency (Grillo et al., 2014). Advanced Metering Infrastructure (AMI) is one of the major advancement for collecting data on energy consumption more frequently and accurately. The role of an AMI is to enable communication between utility companies and electricity meters, including remote electricity usage readings (on-demand and periodic), sending of updated price information to the meters, transmission of alerts about outages, and upgrades of meter firmware, among other communications. Some messages require real-time delivery, while others can be buffered and delayed without negative consequences (Short, 2013).

Advanced Metering Infrastructure (AMI) refers to systems that collect, measure and analyze energy usage, from networks that connected to next-generation electricity meters, or, smart meters. AMI includes software, hardware, communication networks, customer-associated systems and meter data management software. Wireless mesh network is one key technology in AMI network (Kulkarni et al., 2012). The smart meters form a mesh network and multi-hop communication is possible through several meters until the concentrator is reached. Wireless mesh network is able to handle smart metering communication traffic with a high reliability, and the potential coverage gaps are properly filled with repeater nodes (Gharavi and Xu, 2011; Grochocki et al., 2012a).

The addition of a communication infrastructure and the new computational capabilities of smart grid devices add a significant attack surface to traditional energy delivery systems. For example, cyber intrusions that would previously have required physical access to the utility network may now be possible through a remote exploit. In the context of AMIs, the fact that smart meters are not only connected to the utility network but also directly accessible by customers enables new attack vectors. Indeed, field area networks in which meters are deployed appear to be an attractive target for adversaries, because they consist of large numbers of physically accessible devices and have limited or no security monitoring capabilities. Security threats grow exponentially, from inside and outside of the AMI network system (Grochocki et al., 2012b).

In this paper, we present a new attack called a puppet attack, which results in denial of service in AMI network. In this attack,

* Corresponding author.

http://dx.doi.org/10.1016/j.jnca.2015.04.015
1084-8045/

the attacker first selects one or more normal nodes as puppets. Then the attacker sends out data packets, which contain specific attack information to these puppet nodes. When the puppet nodes receive these attack packets, they generate a high volume of route packets. There is limited communication bandwidth in mesh network and route packets are top priority in all packets. Excess route packets will exhaust limited communication bandwidth and result in network congest. As a result, puppet attack causes a denial of service attack in AMI network.

The contributions of this paper are as follows.

- We identify and present a new and severe denial of service attack (i.e., puppet attack) in AMI network.
- This work is the first in-depth work to investigate the impact of a puppet attack in AMI. We analyze the mechanism of puppet attack and compare it with the other attack.
- We present a distributed and adaptive method to detect the puppet attack. Then an isolation mechanism is designed to prevent the puppet attack. In this mechanism, the direct neighbors of the attacker cut off the links to the attacker and do not receive the packets from the attacker any more.

The remainder of this paper is structured as follows. Section 2 introduces the puppet attack in AMI network. Section 3 describes the approach to detect and prevent the puppet attack. In Section 4, we present simulation experiments. Section 5 briefly discusses related work, and Section 6 concludes the paper.

2. The model of the puppet attack

2.1. Overview of Advanced Metering Infrastructure (AMI)

In smart grid, electricity suppliers can monitor, predicate, and control energy generation consumption in real time. Users can know the current price of electrical energy and obtain energy management information from smart meters. It helps users reduce homes energy use. AMI network is the core component to help energy information to transfer and access.

Advanced metering infrastructure (AMI) is an architecture for automated, two-way communication between a smart utility meter with communication network and a utility company. The goal of an AMI is to provide utility companies with real-time data about power consumption and allow customers to make informed choices about energy usage based on the price at the time of use. AMI is an important part of any smart grid initiative.

Wireless mesh network technology is uniquely suited for use in AMI applications due to its ability to dynamically form ad hoc network links between neighboring network nodes. Furthermore communication range can be increased by performing multiple hops from one node to the next until the final destination is reached. Thus wireless mesh networks are able to overcome variable propagation conditions by finding alternative paths through the mesh in the event that one path is blocked by an obstruction, e.g. a lorry parked outside a house.

Dynamic Source Routing (DSR) is one of classic route protocols in wireless mesh network. It is used to form mesh network and forward packets. We introduce Dynamic Source Routing protocol and a denial of service attack against the source routing protocol in the following section.

2.2. Dynamic Source Routing (DSR) protocol

DSR is an on-demand routing protocol using in wireless mesh network, composed of two parts: route discovery and route maintenance. In DSR, whenever a node need to send a packet to a destination and cannot find a route to that destination in its route cache, the node initiates route discovery. The initiator broadcasts a route request packet (RREQ) to its neighbors, specifying the destination and a unique sequence number from the initiator. A node receives the RREQ, if it has recently received the same request identifier from the initiator, it discards the RREQ. Otherwise, it adds its own node address to the list in the RREQ and rebroadcasts the packet. When the RREQ reaches the destination, the destination sends a route reply packet (RREP), including a list of intermediate node's addresses based on the RREQ. When the RREP reaches the initiator of the RREQ, the initiator caches the new route in its route cache. Intermediate nodes also can send RREPs, if they have routes to the destination.

Route maintenance starts when a node sending a packet along a specified route to the destination discovers that the route is broken. If a node on the route cannot receive the confirmation from its next-hop node after a limited number of retransmissions of the packet, it returns a route error packet (RRER) to the source of the packet, identifying the path from itself to the next-hop node as broken. The source then removes this broken link from its route cache. For successive packets to the destination, the source may select another route to that destination from its cache, or it may initiate a new route discovery for that destination if no route exists.

Route salvage is a function of Route Maintenance. Suppose that an intermediate node forwards a packet, and detects that the route to the next-hop node for that packet is broken. The node will start to salvage the packet. To salvage a packet, the node first searches for a replacement route to the destination in his cache. If the node finds a route, it replaces the initial route on the packet with the path from its route cache. The node then sends the packet to the next-hop node along this route. If there exists no route in its cache, the node broadcasts an RREQ to find a new route for the destination. When the node receives RREPs, it replaces the initial route for the packet with the new route. In a word, if a node can forward the packets to its next-hop node, it can salvage the packet by replacing the initial route in the packet with this new route, rather than discarding the packet. This salvage mechanism is not secure and is vulnerable to a puppet attack.

2.3. Puppet attack

In this section, we describe our newly discovered attack, called puppet attack, which is a denial of service attack in AMI network. We first describe the effect of puppet attack. We begin with the normal process of a route discovery in Fig. 1 and then discuss the puppet attack using an example in Fig. 2.

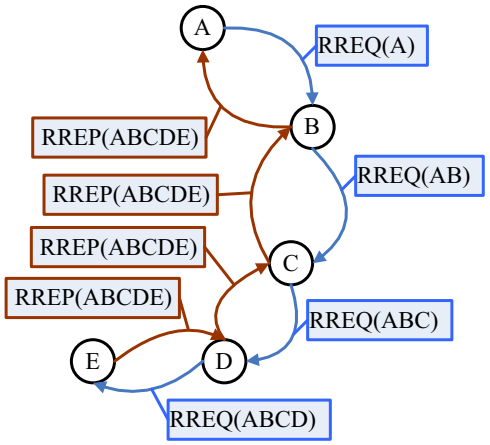

Fig. 1. The address list of packet when forwarding RREQ and replying RREP.

Please cite this article as: Yi P, et al. Puppet attack: A denial of service attack in advanced metering infrastructure network. Journal of Network and Computer Applications (2015), http://dx.doi.org/10.1016/j.jnca.2015.04.015