Denial of Service Mitigation Approach for IPv6-enabled Smart Object Networks

Luís M. L. Oliveira[1], Joel J. P. C. Rodrigues[2], Amaro F. de Sousa[3],
and Jaime Lloret[4]

[1]Instituto de Telecomunicações, Portugal
Department of Informatics, University of Beira Interior, Covilhã, Portugal
Polytechnic Institute of Tomar, Portugal
email: loliveira@ipt.pt

[2]Instituto de Telecomunicações, Portugal
Department of Informatics, University of Beira Interior, Covilhã, Portugal
email: joeljr@ieee.org

[3]Instituto de Telecomunicações, Portugal
Department of Electronics, Telecommunications and Informatics, University of Aveiro, Portugal
email: asou@ua.pt

[4]Integrated Management Coastal Research Institute, Universidad Politécnica de Valencia, Spain
email: jlloret@dcom.upv.es

Abstract. Denial of service attacks (DoS) can be defined as any event that reduces or eliminates a network's capacity to perform its expected function. DoS is a common attack type because in most of time it only uses regular equipment and does not require high knowledge skills. In fact, there are several standard techniques used in traditional computing to mitigate the effects of some of the more common denial of service techniques, although this is still an open problem to the network security community. The denial of service attacks is more expressive in smart object networks. First, because wireless sensor networks devices cannot support the computational overhead necessary to implement many of the typical defensive strategies. Second, small traffic rates are enough to drain node's energy that makes the network inoperable. The denial of service attacks is even more alarming if the sensor networks support highly critical and sensitive services, such as fire detection and alarm. To realize the Internet of Things vision it is necessary to integrate the smart object networks into Internet. The integration of smart object networks in the Internet is considered an exceptional opportunity for Internet growth. However, it is also considered as security threat, because more attacks can be done, such as DoS attacks initiated from anywhere. For all these reasons, DoS attack is considered as a hot topic for WSN scientific community. The aim of this paper is to provide a solution based on 6LowPAN neighbor discovery protocol to be supported only on edge routers to mitigate DoS and DDoS attack initiated from the Internet.

Keywords: Wireless Sensor Networks, Low-Power Personal Area Networks, Denial of service attacks, 6LoWPAN neighbor discovery, Internet of things.

1. Introduction

Nowadays, there is a growing tendency to embed computation and wireless communication devices on quotidian objects, transforming them in to smart objects. These objects will collect and process information from different sources to both control physical processes and to interact with human users [1]. The embedded computational and communication devices are characterized by small size, power constrains, small computing and storage resources and by reduced radio ranges and throughput [3-3]. Several connected smart objects are designated by low power over wireless personal area networks (LoWPAN).

Wireless sensor network (WSN) is a subtype of smart objects network, where the devices can interact with their environment by sensing and controlling physical parameters, such as temperature, humidity, and solar radiation. A single smart network may comprise hundreds of smart objects devices working together to accomplish a common task. Self-organization, fault-tolerance, and self-optimization are the main characteristics of smart object networks [2]. Actually, there are already many technologies that can be used to connect smart objects [3], most of them based on the standard IEEE 802.15.4 layer two protocol [4]. Although, some of these technologies are proprietary, such as the ZigBee [5] and WirelessHART [6]. Moreover, these solutions are not compatible with IP protocol and consequently complex gateways are necessary to connect these networks to the Internet. In a near future, users can access the information collected by smart objects from the Internet, using regular devices and standard protocols. However, a new paradigm is necessary to enable smart objects to be accessed from the Internet where all the devices and networks are IP-enabled, independently of their physical and MAC layers protocols [1]. Supporting IP protocol in all smart devices will also simplify the application development because tools in use on regular computing for commissioning, configuring, managing, and debugging can be used or adapted. Initially, the scientific community considered IP stack protocols too heavy to be supported by small power and resource-constrained devices. However, the scientific community and the industry started to rethink many misconceptions about the use of IP stack in all devices and now the IPv6 protocol is considered the most consensual solution to connect the smart objects to the Internet [7]. Nevertheless, IPv6 was not designed to be used in low power and resource constrained objects. The 6LoWPAN [8-9] adaptation layer was defined to be used between data link layer and network layer to permit the use of IPv6 protocol over IEEE 802.15.4 data link layer. To be used with 6LoWPAN other new protocols best fitted to low power and resource constrained devices were defined, such as routing and neighbor discovery protocols. In fact, the protocols designed to run over LoWPAN must have low overhead on data packets and on message exchange, minimal memory and computation requirements and support for sleeping nodes considering battery savings [8]. The neighbor discovery (ND) can be supported on the physical, data link or network layer; in this paper only ND network layer protocol will be considered. The neighbor discovery is one of the most important protocols, because it is used to the nodes on the same link to discover each other's presence, to determine each other's link-layer addresses, to find routers and maintain reachability information about the paths to active neighbors [10].

The IPv6 ND protocol was not designed for non-transitive wireless links. Moreover, it requires multicast transmission and the IEEE 802.15.4 only supports unicast and broadcast. As a consequence it is necessary to optimize the IPv6 ND to fits on LoWPAN. The adapted ND protocol supports sleeping hosts, eliminating multicast-based address resolution for hosts, instead of defining a registration feature that, provides multi-hop prefix and header compression context and optional multi-hop duplicate address detection [10].

Connecting smart objects networks to the Internet can be considered simultaneously an opportunity and a challenge. An opportunity, because more services can be provided. A challenge, because the smart object networks are now exposed to more security issues [11-13]. As a consequence more successful security attacks can now initiated from anywhere. The security is even more alarming if the smart objects networks are used to support critical infrastructures, such as smart grids applications and fire detection. Supporting security services on resource constrained devices is even more challenging, because of the overhead introduced. Denial of service and distributed denial of service can be done locally and remotely and is one of the most common security attack type, because usually it only requires regular and inexpensive resources and does not requires high technical skills [14]. This paper proposes a new mechanism to be supported only on edge routers, based on the neighbor discovery messages exchanged by the LoWPAN devices and the edge routers, to mitigate the denial and distributed denial of service attacks remotely initiated.

The remainder of this paper is organized as follows. Section 2 analyses the IPv6 enabled smart networks, while Section 3 focuses on security attacks for wireless sensors with IPv6 end-to-end connectivity support. The Sections 4 and 5 present a new countermeasure mechanism based on 6LoWPAN neighbor discovery to mitigate network and transport layer DoS attacks remotely initiated and discuss their application. Finally, Section 6 concludes the paper and pinpoints future research topics.

2. IPv6 Enabled Smart Networks

IEEE 802.15.4 [4] is a data link standard specified to address the low-power and low-rate wireless personal area networks requirements. Two types of devices were defined: full-function devices (FFD) and reduced-function devices (RFD). FFD devices support all network functionalities, consequently can participate in peer-to-peer topologies because multi-hop communications are supported. RFD devices support a limited set of functionalities, they are mainly used in sensing and/or actuation operations. Multi-hop communications are not supported and, thus, they can only be used in star topologies. The protocol defines a central controller device, referred to PAN coordinator, which builds a WPAN with other compliant devices. The PAN coordinator starts a new network by selecting a suitable channel according to energy detection scanning, which measures the interference of each channel. After the channel selection the PAN coordinator broadcast periodically a beacon to announce the WPAN configurations. The other nodes start to listen the beacons to search for available WPAN and to select a coordinator. Only full function devices can operate as a PAN coordinator. Two topologies are supported, the star topology network, where all communications must go through the PAN coordinator and the peer-to-peer topology, where devices can communicate with one another directly, but still the PAN coordinator must be present [15].

The IEEE 802.15.4 protocol defines the physical (PHY) and the media access control (MAC) layers. The PHY layer defines three physical operation modes, 20 kbps at 868 MHz, 40 kbps at 915 MHz, and 250 kbps at 2.4 GHz (DSSS). The MAC layer provides two operational modes, the asynchronous beaconless and the synchronous beacon-enabled mode. The beacon-enabled mode is designed to support the transmission of beacon packets between transmitter and receiver, providing synchronization among nodes. In the beacon-enabled mode, the PAN coordinator broadcasts a periodic beacon containing information about the PAN. In the beacon-enabled mode, the period between two consecutives beacons defines a superframe structure that is divided into 16 slots. Beacons always occupy the first slot, while the other slots are used for data communications. In these slots, slotted carrier sense multiple access with collision avoidance (CSMA/CA) is used for data transmission. In order to support low-latency applications, the PAN coordinator can reserve one or more slots, designated by guaranteed time slots, which are assigned to devices running such applications (in this case, these devices do not need to use contention based medium access mechanisms) [16]. In the beaconless mode, there is no superframe structure and no guaranteed time slots. As a consequence, only random access methods, such as unslotted CSMA/CA can be used to medium access. The frame length is limited to 127 bytes because unreliable and error prone wireless links are used and the devices have limited buffering capabilities.

2.1. 6LoWPAN Adaptation Layer

Currently, the IEEE 802.15.4 protocol is widely accepted as the PHY and MAC layer protocol to be used on smart object networks. However, the WPAN constrains does not permit to support IPv6 directly over IEEE 802.15.4 [8]. The maximum link-layer packet size of 127 bytes is one of the most obvious limitations because implementing standard IPv6 headers over LoWPAN would result in extremely small payloads for higher-level protocols. In the best case, the maximum size of an IP packet is 88 bytes; the IPv6 header has a minimum size of 40 bytes, which results in 48 bytes for upper-layer protocols like TCP or UDP; the length of the TCP header is another 20 bytes, which results in 28 bytes available for the application-layer protocol (in the TCP case). The IETF created the 6LoWPAN working group to define the support of IPv6 over IEEE 802.15.4 LoWPAN networks. In order to comply with the maximum transmission unit (MTU) requirements of IPv6 protocol and to minimize the overhead, 6LoWPAN [9] introduces an additional adaptation layer to be introduced between data link and network layers. This layer provides a mechanism for packet fragmentation, header compression, and support for data link layer forwarding of IP packets, also known as mesh-under routing. Although 6LoWPAN was originally designed to support IPv6 over IEEE 802.15.4, it can later be adapted for other similar link technologies.

In LoWPAN networks, packets will often have to use multiple radio hops to reach the destination. The multi-hop forwarding is motivated by the fact that the sending node may not have radio range to reach the destination node. To send a packet to another node, two main processes are involved: forwarding and routing. On the forwarding process, packets are moved from the input to the output interface and are executed at lower layers. Note that in most of time, only one physical interface is involved in the forwarding process. Routing process can be executed at layer 2 or at layer 3. Routing process usually uses a routing protocol to evaluate the best path to reach the destination. Each node maintains a routing information base that contains all the information needed to run the routing protocol. The routing information base is used to fill the forwarding information base, which is consulted when a packet needs to be forwarded. Routing in a 6LoWPAN network can be done in three different ways, link-layer mesh-under, 6LoWPAN mesh-under, and route-over [17-18]. Link-layer mesh and LoWPAN mesh-under are designated by mesh-under and are transparent to the network layer. Routing at network layer is designated by route-over.

A typical LoWPAN consists of edge routers, routers, and nodes (Figure 1). 6LoWPAN nodes usually do sensing and actuation operations, they do not forward packets destined to other nodes. Routers are intermediate nodes that can be used to forward datagram to others nodes or routers in the same LoWPAN and are present only in route-over topologies. Edge routers are used to connect the LoWPAN to others networks, for example, the Internet. Typically, only nodes and routers have energy and computational resources constrains, the edge router is main powered and has more computational resources [8].

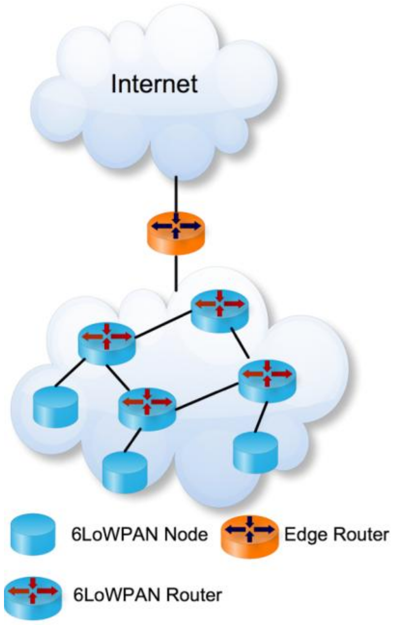

Figure 1 – Illustration of 6LoWPAN network architecture.

2.2. Neighbor Discovery Protocol for 6LoWPAN

The IPv6 neighbor discovery protocol is used by the nodes on the same link to discover each other's presence, to determine each other's layer two addresses, to search routers, to maintain reachability information about the paths to active neighbors, and to address auto configuration [10, 19].

The neighbor discovery protocol for IPv6 networks uses multicast to exchange most of the messages and it was designed considering the router and the nodes always on link. However, given the resource constraints of LoWPAN nodes, the absence of multicast support at layer two and the low duty-cycle, neighbor discovery on 6LoWPANs requires a different approach focused on the efficient use of available energy. Although the standard IPv6 neighbor discovery protocol should work on 6LoWPANs, there are convincing reasons to optimize the neighbor discovery. In fact, the IPv6 neighbor discovery protocol was not designed for non-transitive wireless links, making heavy use of multicast, which is inefficient and impractical in low-power networks, because broadcast is used in absence of multicast support. As a consequence, the rate of ND transmitted messages is limited due to energy conservation policies. Also, IPv6 ND assumes that local link nodes are always a single hop away and nodes are always listening, but in LoWPANs that is not the case.

Neighbor discovery optimizations for 6LoWPAN [10] are being proposed to address the specific needs of LoWPAN. Neighbor discovery optimization for low power and lossy networks (draft-ietf-6lowpan-nd-18) [10] is a work in progress specification proposed by IETF's 6LoWPAN Working Group. It describes optimizations to the IPv6 neighbor discovery, header compression context information dissemination, auto configuration addressing mechanisms, and duplicate address detection for low power networks. The neighbor discovery signaling was simplified by replacing the address resolution with address registration mechanism. It also eliminates the need for periodic router advertisement multicasting, by providing host-initiated request for router advertisements. Moreover, in most cases multicast messages was replaced by unicast messages. The node to host interaction is not affected by the 6LoWPAN routing approach; as a consequence the interaction between this interaction is the same both in mesh-under and route-over.

The edge router designated on draft-ietf-6lowpan-nd-18 [10] as 6LBR plays an important role in 6LoWPANs. Besides being responsible for connecting the LoWPAN to the Internet, it is also responsible for propagating the IPv6 prefix and header compression context information across the LoWPAN. The 6LBR also maintains a network-wide cache of the hosts' IPv6 addresses and EUI-64 identifiers, which makes it able to make layer two address resolution and detect and avoid duplicate addresses. Alternatively, DHCPv6 can be used to ensure unique addresses on the network. 6LoWPAN neighbor discovery assumes each IPv6 is derived from the unique EUI-64 address, so it does not require, by default, either duplicate-address detection or address resolution if the IPv6 link-local address are used [20]. There are also optional and separated mechanisms that can be used between LoWPAN routers (6LR) and 6LBR to execute multi-hop duplicate address detection and distribution. These optimizations lead to a significant drop in signaling messages in the local network, resulting in significant energy savings, extending the longevity of the network.

To achieve these goals, the new ND protocol defines three new ICMPv6 message options: the required Address Registration Option (ARO) and the optional Authoritative Border Router Option (ABRO), and 6LoWPAN Context Options (6CO).

Two new ICMPv6 message types are also defined to carry out the optional multi-hop Duplicate Address Detection: Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC).

The nodes in a LoWPAN use ND to perform address auto configuration, layer two address resolution, neighbor unreachability detection, and to find default routers.

When the interface on a node device is initialized, a link-local address is formed based on the EUI-64 identifier. Next, the device nodes send an RS message including the source link-layer address (SLLA), so that router can reply with a unicast RA message. The RA message can include the SLLA, ABRO, 6CO, and the IPv6 Prefix Option (PIO) (Figure 2). Once an address has been configured in a node, a NS with an address registration option will be sent to the edge router to register that address.

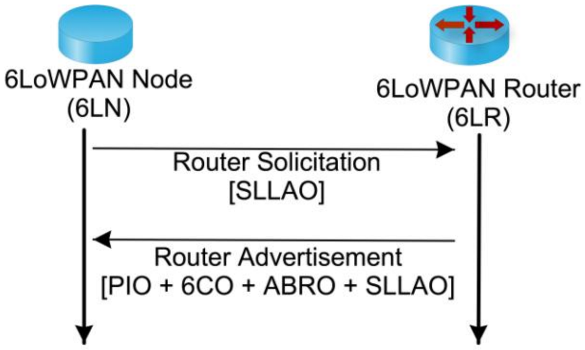

Figure 2. Host initiated router discovery.

The process of address registration (Figure 3) is necessary to avoid the layer-two address layer resolution based on multicast neighbor solicitation messages. The host sends a unicast NS message to the router, with the Address Registration option (ARO). The router replies with a unicast NA message with the ARO and the status of the registration. The status indicates either a successful registration or a failure due to a duplicated address or because the router's registration cache is full.

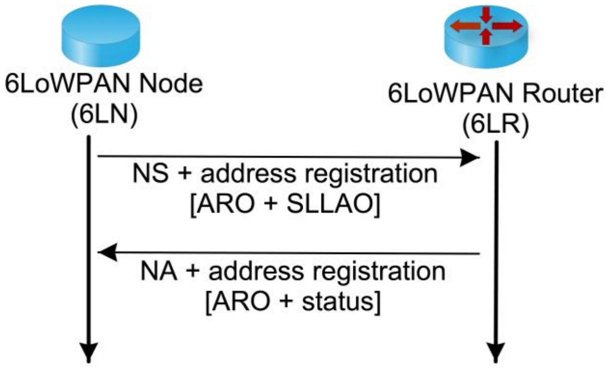

Figure 3. Node address registration.

The address registration mechanism and the SLLA router advertisement option provide enough information in routers and nodes to resolve an IPv6 address and to its associated layer two addresses. Note that all prefixes, except the link-local addresses are always assumed to be off-link, so all communications must be through the edge router. The multicast addresses are also supposed to be off-link, because multicast-based addresses resolution between neighbors is not needed. The information transported on NA messages have a lifetime associated, before the lifetime expires the node must repeat above described process. Note that nodes can receive router advertisements messages from multiple edge routers. In this situation should attempt to register with more than one of them to increase the network resilience.

The node device also uses neighbor solicitation messages to perform unreachability detection. This operation is mainly used to verify the default router reachability.

The optional multi-hop duplicate address detection process is shown in Figure 4. It can be used in route-over networks to assure address uniqueness within the 6LoWPAN for non-EUI-64 based addresses. It is similar to the standard address registration process, except that as the edge router is responsible for managing the address registration cache, the intermediate router that the host tries to register with, must first check with the

6LBR if the address is not a duplicate. This is done using the new DAR and DAC ICMPv6 messages.

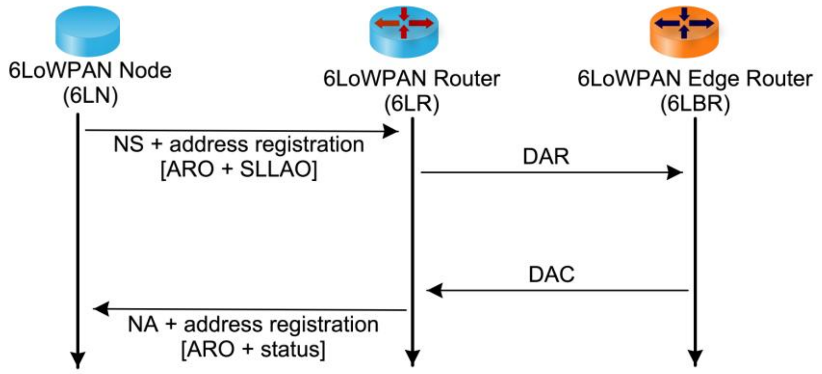

Figure 4. Host address registration with multi-hop DAD.

An edge router does not need to send unsolicited router advertisement messages, because the node devices will send router solicitation messages whenever they need updated information. Unicast neighbor advertisement messages are always used in response to neighbor solicitation messages.

2.3. Connectivity Models

Three main models can be used to connect LoWPAN to the Internet. In this first deployment model, all the LoWPAN nodes support IP stack, however, they are not connected to the Internet [21]. In fact, there are several scenarios that do not require any connectivity with the Internet, for example the smart grid applications. Smart grid networks are used to monitoring the power generation networks, the automation and control devices, smart metering, and building and home energy management. These networks can also use the IP protocol suite in all nodes but due security and privacy reasons in most of the cases are completely disconnected from the public Internet. In this case, supporting IP suite in all devices continues to be advantageous as described in the introduction, although assigning global IPv6 addresses to all devices is not desirable.

In the second model, a proxy device is used to connect the smart network to the Internet. Internet user will have access to the information provided by smart objects, such as environmental data, using the proxy device. The proxy can act as a server that collects data from the smart objects. This connectivity model can be used to connect networks without IP support, to preserve scarce resources on such networks and to increase scalability, although it does not provide end-to-connectivity. Supporting more than one point of connection between the smart object network and the Internet could not be possible if the proxy uses stateful translation mechanisms. This connectivity model is similar to the previous model. So, the support of IP suite protocol continues to represent a benefit, but assigning IP global addresses to all devices is optional. The second model can be considered an intermediate model between the first model and the smart object full integrated in the public Internet.

In the third model (Figure 1), the smart object networks are considered as an extension to the Internet. This connectivity model can be used in a near future to support services provided by smart cities, where the citizens can use the Internet to make quotidian decisions based on environmental data such as air quality, temperature, and real-time transportation information. All of these networks will make use of the IP protocol suite and one or more router could be used, for redundancy and scalability purposes, to connect these networks to the Internet. In such model, the IP end-to-end connectivity is required and, at least, one IP global address must be assigned per device.

3. Security Attacks for Wireless Sensors with IPv6 End-to-End Connectivity Support

Protecting the resources and the information transmitted over the network from attacks is the main concern of the security services [11-13]. Besides the differences between smart object networks and the other network types, both share some security requirements. Despite this, due to resources constrains and the number of nodes, in smart object networks providing security services is even more challenging when compared with regular networks. Confidentiality, integrity, availability, freshness, robustness, and survivability are the most relevant security requirements in smart objects networks [22-23, 30]. Confidentiality requirement ensure that no other than the legitimate entities have access to the data transmitted and stored in smart object network. Authenticity is a central concept to confidentiality, because it ensures that the identity of the sender is correct. Authentication is also necessary for automated node interactions. Integrity requirement is necessary to prevent that no message can be altered by any entity as it transverses from the sender to destination without being detected. The availability requirement is important to ensure that services provided by the smart object network are always available to be used by the legitimate users. Data freshness requirement is important to prevent other parties to replaying old messages. There are two types of data freshness requirements, strong and weak data freshness. In the first, it allows total order request-response pair and allows delay estimation. In the second, a partial message ordering is provided, but delay estimation is not supported. Robustness and survivability must be ensured to guarantee the network still operational even if a set of nodes are compromised due to security attack. Smart object networks are vulnerable to several types of security attacks, which can be classified, according to security requirements in three main groups [11]: attacks on secrecy and authentication, attacks on network availability, and stealthy attacks against service integrity. Eavesdropping, packet reply attacks, tampering and spoofing of packets are examples of attacks against the secrecy and authenticity. Several mechanisms can be used to prevent attacks on secrecy and authenticity, most of which based on cryptography. Device data confidentiality and integrity is harder to obtain when compared with communication confidentiality because is requires both logical and physical measures to protect against attackers. Introduce false data into the smart object network is the main goal of stealthy attacks against service integrity. Attacks on network availability are often designated as denial of service attack. This paper focus on DoS and their countermeasures, in particular to those that can be used to prevent remote initiated attacks.

A denial-of-service (DoS) attack is characterized by an explicit attempt to prevent the network to perform its expected functions [24]. During a DoS attack, the attacker attempts to reduce the network's capacity. Several events can be used to perform a DoS attack, flooding the network with junk traffic and disrupting network connections are two of the most common techniques. DoS attacks can be classified as logic attacks and resource exhaustion flooding attacks. Logic attacks exploit security vulnerabilities to cause a server or service to crash or significantly reduce performance. Resource exhaustion flooding attacks cause the network node's or network's resources to be consumed to the point where the service is no longer responding or the response is significantly reduced [11]. When a DoS is originated from several sources it is designated by distributed denial of service (DDoS). On both types the attack sources can be locally or remotely located. In fact, there are several techniques that can be used to make a DoS security attack. The techniques that can be used to perform a DoS attack can be classified according to the protocol layer that is intended to attack [11, 24]. Jamming and tampering are the most common attack against the physical layer. The jamming is intended to interfere with the normal radio communication link. The attacker uses the same spectrum that legitimate network nodes are using. Defenses against jamming involve code spreading and frequency hop techniques. The link layer is responsible for medium access control, error detection, frame construction and detection, and reliable point-to-point and point-to-multipoint connections between adjacent nodes. Introduce collisions, is the main technique to perform a DoS attack on link layer protocols. Forcing collisions can be used to achieve resource exhaustion and unfairness. Using small frames, error-correction codes and rate limitation are three of the most used mechanisms to mitigate layer two DoS attacks. In smart object networks the routing can be both performed on link layer (mesh-under approach) or at network layer (route-over approach), as consequence DoS attacks directed to routing information protocols can pointed to both layers. Create loops, attracting or repelling network traffic from the selected nodes are the main objectives of DoS attack directed to routing protocols. Adding message authentication codes to routing information messages is one of the principal countermeasure technique, because the receivers can detect the sender identity and if the messages have been tampered or spoofed [26-27]. Managing end-to-end connections is the transport layer main function, and flooding and desynchronization are two of the possible attacks in this layer [11]. In flooding attacks, several new connection requests are sent until the exhaustion of the receiver resources. To avoid this attack it is necessary to identify the legitimate requests to avoid wasting resources with bogus connections. The desynchronization attack refers to the disruption of an existing connection. This attack uses spoofed messages causing the retransmission of missing frames due to error that never really existed.

Puzzle resolution and authentication techniques are the most common countermeasures to prevent from transport layer DoS attacks [29-30]. Note that UDP protocol is most widely used in smart object networks than TCP, so apparently flooding and desynchronization attacks are not so disruptive. However, any unnecessary transmitted message has an important impact in the energy consumption and UDP is harder to control when end-to-end connections between the smart object and the Internet are supported.

DoS attack can also be directed to the application layer protocols. Application-layer DoS attacks are even more difficult to detect because the transport layer connection is valid and so are the requests. Application layer DoS attacks are even more difficult to detect because the transport layer connection is valid and so are the requests. During the attack one or more clients send a large number of requests. Legitimate request could be mixed with fake requests, which means a denying all philosophy will result in a DoS, situation that attackers are trying to force. Defending against application layer DoS attacks usually involves some sort of rate-shaping algorithm that watches clients and ensures that they request no more than a configurable number requests per time period. If the client requests more than the configurable number, the client's IP address is blacklisted for a specified time period and subsequent requests are denied until the address has been released from the blacklist. The above-described countermeasures should be implemented on edge routers. First, the edge routers have more energy and computation resources than smart object nodes. Second, it makes more sense to filter the traffic closest to the source.

In the third connectivity model presented in Section 2.3 the smart object networks truly belong to the Internet just like any other network. Any Internet user, potentially, have access to the information provided by smart objects accessing the device. This connectivity model can be used to support a myriad of new services and applications. However, the smart objects network becomes also exposed to remotely initiated security attacks, in particular to DoS and DDoS.

4. A Solution to Mitigate DoS Attacks on WSN with IPv6 End-to-End Connectivity

This section presents a new countermeasure mechanisms based on 6LoWPAN neighbor discovery to mitigate DoS and DDoS attacks remotely initiated. The new security mechanisms run only on the edge routers, not overloading the smart object nodes. Furthermore, the proposed mechanisms reuse the registration address process messages. This mechanism protects against transport and application layer DoS and DDoS attacks, filtering unsupported traffic at the edge and rate-shape the requests from the Internet to ensure that any Internet client generate no more requests than the imposed limits.

As explained in the Section 2.2, the address registration process is necessary to avoid the layer-two address layer resolution and to guarantee the node’s IP address uniqueness. According to routing approach two different procedures can be used to perform the address registration [10]. In the mesh-under, the nodes exchange the address registration with the edge router. In the route-over, the process is similar to the used on mesh-under approach, but the nodes exchange the NS and the NA messages with an 6LR and the 6LR uses the new Duplicate Address Request (DAR) and DAC ICMPv6 messages to verify the address uniqueness on the edge router.

New information must be included on the Address Registration Option (ARO) and DAR address registration messages [10] to implement the proposed mechanism. So, the following information must be included on the ARO message: *i*) the transport-layer protocol accepted, *ii*) if the node accepts connections from the Internet, and *iii*) the maximum Internet clients request rate-shape limit. Then, new three fields must be defined for being transported on first ARO reserved field. In fact, the ARO option contains two fields reserved for future use, the first with 8 bits and the second with 16 bits length. The duplicated address messages also contain an 8bit length reserved field, which can be used to transport the same information. The figure 6 represents the new ARO and DAR message formats and Table I the valid values and the description for each new field.

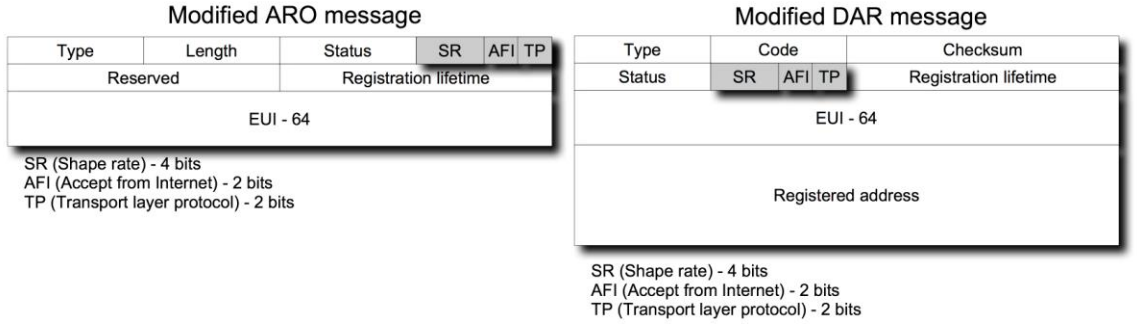

Figure 6. New address registration option (ARO) and duplicate address request (DAR) message formats.

Field	Length	Values	Description
Shape rate	4 bits	0000	Not used
		0001-1111	Rate limit value
AFI	2 bits	00	Not used
		01	Do not Accept packets from the Internet
		10	Accept packets from the Internet
		11	To be defined
TP	2 bits	00	Not used
		01	UDP
		10	TCP
		11	Accept any

Table I. Address registration option (ARO) and duplicate address request (DAR) new data fields.

Three new data structures will be created at the edge routers, the filtering database, the Internet client's address table, and the Internet client blacklist table. The filtering database will be used to filter unwanted traffic and it is constituted by the node's IP address (IP address) and registered lifetime (Lifetime). If the node accepts data from the Internet (Accept data from the Internet), the accepted transport layer protocol (Accepted transport layer protocol) and Internet client rate request limit (Rate request limit) (Figure 7). Information extracted from the new ARO and DAR messages are used to fill the filtering database, according to the correspondence defined in (Table II).

Filtering database fields	ARO message fields	DAR message fields
IP address (128 bits)	EUI-64	Registered address
Lifetime (16 bits)	Registration lifetime	Registration lifetime
Accept data from Internet (2 bits)	Accept data from Internet	Accept data from Internet
Accepted transport layer protocol (2 bits)	Accepted transport layer protocol	Accepted transport layer protocol
Rate request limit (4 bits)	Rate request limit	Rate request limit

Table II. Filtering database fields correspondence.

The Internet client's address table is used for ensure that any Internet client generate no more packets than the imposed limits. Limits per client and per node will be applied. As may be seen in Figure 8, this table is constituted by the Internet client IPv6 address (Client IP address), lifetime (Lifetime), smart object IP address (Destination address), the rate packet computed per minute (Rate request), and the rate request limit (Rate request limit) copied form the filtering database table.

IP address	Lifetime	Accept data from the Internet	Accepted transport layer protocol	Rate request limit
(128 bits)	(16 bits)	(2 bits)	(2 bits)	(4 bits)

Figure 7. Filtering database table format.

The Internet client blacklist table is used to store the Internet client's IP address that exceeds the imposed rate limits (Figure 9) and comprise the following fields: Internet client's IP address (IP address), the configurable amount of time in seconds that the IP address must remains in the blacklist (Lifetime), IP address of the destination node (IP destination address), and the number of times that this address was added to the blacklist (Counter). The Lifetime value must be increased if the same client IP address repeats several times for the same or for different destination address. So, the blacklist table entries should not be removed after the lifetime goes to zero. However, periodically the oldest entries must be flushed.

Client IP address	Lifetime	IP destination address	Rate request	Rate request limit
(128 bits)	(16 bits)	(128 bits)	(4 bits)	(4 bits)

Figure 8. Internet client address table.

Client IP address	Lifetime	IP destination address	Counter
(128 bits)	(16 bits)	(128 bits)	

Figure 9. Internet client blacklist table.

4.1. Mesh-under Networks

In the mesh-under routing approach [11] nodes register the address directly on the edge router. When a node has configured a non-link local IPv6 address it registers that address in one or more edge router, using the NS message with ARO option. Beyond the behavior defined in the 6LoWPAN neighbor discovery working progress document, the node also add to ARO information related to the new data fields (i.e., SR, AFI, and TP). If the values of the new data fields are equal to zero, the edge router handles neighbor solicitation message and the ARO option as specified in the 6LoWPAN neighbor discovery working progress document Section 6.5. If the new data fields are different from zero and in addition to the normal behavior, the new data fields' values are copied into the filtering database table according to the Table II. The edge router should ignore the new ARO fields if the new format is not supported.

4.2. Route-over Networks

In the route-over routing approach [11] the ARO can also be used to register an address in a 6LR (6LoWPAN router). In this situation, the 6LR reuses the information contained in the ARO, sent by the node, in the DAR message (Figure 4). So, in addiction to the normal operation defined in the 6LoWPAN neighbor discovery working progress document the Section 8.2, the 6LR before send the DAR message must copy the new data fields (i.e., SR, AFI, and TP) from the ARO message into the new DAR message (Figure 6). The edge router updates the filtering database table according to the correspondence defined in the Table II. The 6LR should ignore the new DAR fields if the new format is not supported.

4.3. Filtering Packets Received from the Internet

When the edge router receives a packet from the Internet destined to the smart objects network, before consulting the routing table, must verify if the destined address exists, if the destination node accepts the transport layer protocol in use, and if the packet IP source address is not present in the Internet client blacklist table with lifetime value greater than zero. The packet will be forwarded, using the regular routing mechanisms, if all the mentioned conditions are true. Otherwise, the packet will be discarded. Internet client´s address and Internet client blacklist tables will be actualized for each packet received from the Internet.

5. Discussion

Denial of service (DoS) and distributed denial of service (DDoS) can be done locally and remotely, and it is one of the most common security attack type, because usually it only requires regular and inexpensive resources, and does not requires high technical knowledge [11-13]. The frequency and sophistication of DoS and DDoS are rapidly increasing. To execute DoS and DDoS attacks several techniques are used, including direct attacks, remote controlled attacks, reflective attacks, worms, and viruses.

There are several techniques that can be used to prevent or to mitigate DoS attacks although a generic defense mechanism against to this security attacks is considered as an open issue. Furthermore, most of the proposed defense mechanisms require high computational resources making them inappropriate to be used on smart object networks. DoS security attacks are even more destructive to smart object networks when compared to the other networks. First, it is easier to exhaust resource on constrained networks. Second, a DoS can draw node's energy making them unavailable until the attack is ended and the battery is recharged.

This paper presents a solution to prevent from remotely initiated DoS network and transport layer attacks, filtering unwanted traffic originated on the Internet and destined to smart object networks nodes and it is based on address registration process defined in neighbor discovery protocol for 6LoWPAN. With this mechanism, only traffic that conforms to the following rules will be forwarded from the Internet into the smart object networks:

- The destination node address must be registered; this condition is necessary to guarantee that only traffic destined to reachable node will be forwarded.

- The nodes must manifest intention to accept data from the Internet; In fact, several nodes, for example 6LoWPAN routers, are registered but do not make sense accept data from the Internet in most of the situations.
- Information about the node's supported transport protocol should be registered on the edge router; according to this condition only traffic transported over the supported protocol will be forwarded.
- Nodes should inform the edge router about the accepted traffic rate limit; in fact, there are several slow variation in time physical processes which do not require high rate requests, for example air temperature monitoring. The traffic rate is computed for each client and for each destination address.

To implement the proposed mechanism is necessary to add more three data fields to ARO and DAR messages. This modification does not increase the length of the messages because the new fields use an existing eight-bit length reserved field. Moreover, it does not increase the overhead on the resource-constrained nodes (i.e. smart object nodes and 6LoWPAN routers) because the filtering mechanisms, all processing and storing overhead will be applied only on the edge routers, which have less resource constrains. The proposed mechanism uses stateless traffic processing, so it can runs simultaneously in different edge routers, providing more robustness to the network. In the original ARO and DAR messages the zeros are used to fill the reserved data fields, as a consequence less compression rates will be achieved on the new messages because different values will be used on the same fields [25].

The security model used in the proposed mechanism can also be used to enforce security services on the edge to provide confidentiality and authenticity based on cryptography. Internet client authenticity must be ensured to provide a more robust remote DoS attack control. Authentication and client puzzles based mechanisms [13, 28-29] can be used in the edge router to provide a more coarse traffic admission control. Add authentication, client puzzle mechanisms to the current solution and provide more application-based control will be addressed as future work.

6. Conclusions and Future Work

Smart object networks, which include wireless sensor networks, can provide support for innumerous applications. In fact, the sensors give the smart objects the capacity to sense the physical world and to control some physical processes due to actuation capabilities. There are already a number of emerging applications of smart objects in power grid monitoring and control, e-health, intelligent transport systems, environmental monitoring, and energy management. So far, the smart object networks are isolated from the Internet. First, a large number of technologies are used and some of them incompatible with IP protocol. Second, due to security reasons, most of the problems related with interconnection were already solved. However, providing security services in smart object networks is considered as an open issue. Providing security in resource-constrained network is even more challenging when compared with regular networks. So, special protocols and mechanisms have been developed for use in smart object networks. The frequency and sophistication of Denial of Service (DoS) attacks are rapidly increasing. This paper presented a security mechanism to prevent from remotely initiated transport level DoS attacks. The proposed mechanism filters at the edge router the traffic received from the Internet and destined to smart object nodes. The edge router only forwards the Internet traffic into the smart objects network if the traffic meets predefined conditions.

In the proposed solution smart nodes uses an adapted version of 6LoWPAN neighbor address registration mechanism to inform the edge router about the conditions used to filter the Internet received traffic. In this mechanism, all the required information is carried on address registration messages, the edge routers support storage and processing overhead. So, the new mechanism requires no more messages than those used to perform the address registration and also does not increase the length of the messages.
Authentication and client puzzles based mechanisms can also be supported in the edge router to provide a more granular traffic admission control. Including these mechanisms and the performance evaluation in real scenarios, the proposed DoS attack prevention mechanism is addressed as a future work.

Acknowledgements

This work has been partially supported by the *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Portugal, and by National Funding from the FCT – *Fundação para a Ciência e Tecnologia* through the Pest-OE/EEI/LA0008/2011.

References

1. Gershenfeld N, Krikorian R, Cohen D. The Internet of Things. *Scientific American 2004*; **291**(4): 76-81.
2. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: a survey. *Computer Networks*2002; **38**(4): 393–422.
3. Karl H, Willig A. *Protocols and architectures for wireless sensor networks*, Wiley, 2005.
4. IEEE Std 802.15.4-2006. *Part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)*. IEEE Std. 802.15.4-2006, 2006.
5. ZigBee Alliance, ZigBee Specification, October 2007
6. Wireless HART homepage. Available from: http://www.hartcomm.org/ [January 2012].
7. Hui J, Culler D. Extending IP to Low-Power, Wireless Personal Area Networks. *IEEE Internet Computing* 2008, **12**(4):37-45.
8. Kushalnagar N, Montenegro G, Schumacher C. *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*. Internet Engineering Task Force, Request for comments 4919, August 2007.
9. Montenegro G, Kushalnagar N, Hui J, Culler D. *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*. Internet Engineering Task Force, Request for comments 4944, September 2007.
10. Shelby Z, Thubert P, Hui J, Chakrabarti S, Bormann C, Nordmark E. *6LoWPAN Neighbor Discovery*. Internet Engineering Task Force, IETF draft draft-ietf-6lowpan-nd-18 working progress, October 2011.
11. Roman R, Lopez J. Integrating Wireless Sensor Networks and the Internet: a Security Analysis. Internet Research 2009, **19**(2): 246- 259.
12. Yong W, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. *Communications Surveys & Tutorials*, IEEE 2006, **8**(2): 2-23. doi: 10.1109/COMST.2006.315852
13. Du X, Chen H. Security in Wireless Sensor Networks, IEEE Wireless Communications 2008, **15**(4): 60-66.
14. Pelechrinis K, Iliofotou M, Krishnamurthy V. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *Communications Surveys & Tutorials*, IEEE 2011, **13**(2): 245-257. doi: 10.1109/SURV.2011.041110.00022.
15. Lin K, Chin-Feng L, Xingang L, Xin G. Energy Efficiency Routing with Node Compromised Resistance in Wireless Sensor Networks. ACM/Springer Mobile Networks and Applications 2010. DOI: 10.1007/s11036-010-0287-x

16. Hongjuan L, Lin K, Keqiu L. Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks. Computer Communications 2011. **34**(4): 591-597.
17. Oliveira L, Sousa A, Rodrigues J. Routing and mobility approaches in IPv6 over LoWPAN mesh networks. *International Journal of Communication Systems* 2011, 24: 1445–1466. doi: 10.1002/dac.1228
18. Akkaya K, Younis M. A survey of routing protocols in wireless sensor networks, *Elsevier Ad Hoc Network Journal* 2005, 33: 325– 349.
19. Narten T, Nordmark E, Simpson W, Soliman H. *Neighbor Discovery for IP version 6 (IPv6)*. Internet Engineering Task Force, Request for comments 4861, September 2007.
20. Singh H, Beebee W, Nordmark E. *IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes*. Internet Engineering Task Force, Request for comments 5942, July 2010.
21. Vasseur J, Dunkels A. Interconnecting Smart Objects with IP, Morgan Kaufmann 2010. ISBN 978-0123751652.
22. Ramen R, Lopez J, Gritzalis S. Situation awareness mechanisms for wireless sensor networks, IEEE Communication Magazine 2008, **46**(4): 102-107.
23. Sakerindr P, Ansari N. Security Services in Group Communications over Wireless infrastructure, Mobile Ad Hoc and Sensor Networks, IEEE Wireless Communications 2007, **14**(5): 8-20.
24. Peng T, Leckie C, Ramamohanarao K. Survey of network-based defense mechanisms countering the DoS and DDoS problems, ACM Computer Surveys 2007. **39**(3): 224-260. DOI: 10.1145/1216370.1216373
25. Hui J, Thubert P. *Compression Format for IPv6 Datagrams in 6LoWPAN Networks*. Internet Engineering Task Force, draft draft-ietf-6lowpan-hc-06 working progress, October 2009.
26. Tsao T, Alexander R, Dohler M, Daza V, Lozano A. *A Security Framework for Routing over Low Power and Lossy Networks*. Internet Engineering Task Force, draft draft-tsao-roll-security-framework-01, September 2009.
27. Karlof C, Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, Proceedings. First IEEE Int'l. Workshop. Sensor Network Protocols and Applications, May 2003, pp. 113–27.
28. Shi E, Perrig A. Designing Secure Sensor Networks, Wireless Communications Magazine 2004, **11**(6): 38–43.
29. Newsome J. The Sybil Attack in Sensor Networks: Analysis and Defenses, Proceedings of. IEEE Int'l. Conference of Information Processing in Sensor Networks, Apr. 2004.
30. Lopez J, Roman E, Alcaraz C. Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Network, Foundations of Security Analysis and Design, Springer, 2009, LNCS 5705, pp. 289–338.