CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE
Concurrency Computat.: Pract. Exper. 2013; **25**:129–142
Published online 12 June 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/cpe.2850

SPECIAL ISSUE PAPER

Denial of service mitigation approach for IPv6-enabled smart object networks

Luís M. L. Oliveira [1,2,3], Joel J. P. C. Rodrigues [1,2,*,†], Amaro F. de Sousa [1,4] and Jaime Lloret [5]

[1] *Instituto de Telecomunicações, Portugal*
[2] *Department of Informatics, University of Beira Interior, Covilhã, Portugal*
[3] *Polytechnic Institute of Tomar, Portugal*
[4] *Department of Electronics, Telecommunications and Informatics, University of Aveiro, Portugal*
[5] *Integrated Management Coastal Research Institute, Universidad Politécnica de Valencia, Spain*

SUMMARY

Denial of service (DoS) attacks can be defined as any third-party action aiming to reduce or eliminate a network's capability to perform its expected functions. Although there are several standard techniques in traditional computing that mitigate the impact of some of the most common DoS attacks, this still remains a very important open problem to the network security community. DoS attacks are even more troublesome in smart object networks because of two main reasons. First, these devices cannot support the computational overhead required to implement many of the typical counterattack strategies. Second, low traffic rates are enough to drain sensors' battery energy making the network inoperable in short times. To realize the Internet of Things vision, it is necessary to integrate the smart objects into the Internet. This integration is considered an exceptional opportunity for Internet growth but, also, a security threat, because more attacks, including DoS, can be conducted. For these reasons, the prevention of DoS attacks is considered a hot topic in the wireless sensor networks scientific community. In this paper, an approach based on 6LowPAN neighbor discovery protocol is proposed to mitigate DoS attacks initiated from the Internet, without adding additional overhead on the 6LoWPAN sensor devices. Copyright © 2012 John Wiley & Sons, Ltd.

Received 29 January 2012; Revised 22 March 2012; Accepted 2 April 2012

KEY WORDS: 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 into 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 constrained, small computing, and storage resources and by reduced radio ranges and throughput [2, 3]. Networks composed of several connected smart objects are designated as low power over wireless personal area networks (LoWPAN). The provisioning of reliable energy-efficient and low-delay communications in resourced constrained network has become a challenging resource issue. A layered multipath power control scheme is proposed in [4], which has high performance on reliability, energy-efficiency, and low-delay communication in underwater sensor networks. Multiple-path forward error correction approach [5] based on Hamming codes, can also be used to improve the reliability and energy efficiency.

*Correspondence to: Joel J. P. C. Rodrigues, Department of Informatics, University of Beira Interior, Covilhã, Portugal.
†E-mail: joeljr@ieee.org

Wireless sensor networks are a subtype of smart object networks, where the devices can interact with their environment by sensing and controlling physical parameters, such as temperature, humidity, and solar radiation. A single network may comprise hundreds of smart devices working together to accomplish a common task. Self-organization, fault-tolerance, and self-optimization are the main characteristics of smart object networks [2]. Currently, 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 [6] but some being proprietary, such as ZigBee [7] and WirelessHART [8]. Nevertheless, these solutions are not compatible with IP protocol and consequently require complex gateways to connect them to the Internet. The aim is that, in a near future, users can access the information collected by smart objects from the Internet, using regular devices and standard protocols. To reach this aim, a new paradigm is necessary to enable smart objects to be accessed from the Internet where all devices and networks are IP-enabled, independently of their physical and media access control (MAC) layer protocol [1]. The support of Internet protocol (IP) 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 IP protocol stack was considered too heavy to run on small power and resource constrained devices. Meanwhile, the scientific community, together with the industry, started to rethink many misconceptions about the use of IP in all devices and now the IPv6 protocol is considered the most consensual solution to connect the smart objects to the Internet [9]. Nevertheless, IPv6 was not designed to be used in low power and resource constrained objects. The 6LoWPAN [10, 11] adaptation layer was defined between the data link layer and the network layer to enable the use of IPv6 protocol over IEEE 802.15.4 data link layer. Together 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 networks must have low overhead on data packets and on message exchange, minimal memory and computation requirements and support for sleeping nodes considering battery savings [10]. Neighbor Discovery (ND) is one of the most important protocols, because it is used by the nodes to discover each other's presence on the same link, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors [12]. Concerning the ND protocol, it can be supported on the physical, data link, or network layers [13]. In this work, we only consider ND protocol on the network layer.

The original IPv6 ND protocol not only was not designed for nontransitive wireless links but also requires multicast transmission, a feature not supported by the IEEE 802.15.4 standard. As a consequence, it was necessary to optimize the IPv6 ND to fit to LoWPAN. The adapted ND protocol [12] supports sleeping hosts, eliminates the multicast-based address resolution for hosts, because it defines a registration feature that provides multihop prefix and header compression context and optional multihop duplicate address detection.

Connecting smart object networks to the Internet can be considered simultaneously an opportunity and a challenge [9, 14]. It is an opportunity because more services can be provided. It is a challenge because the smart object networks are now exposed to more security issues [15–17] because successful security attacks can now be initiated from anywhere. The security is even more alarming if the smart object networks are used to support critical infrastructures, such as smart grid applications or fire detection. Supporting security services on resource constrained devices is even more challenging because of the overhead introduced. Denial of service (DoS) and distributed denial of service (DDoS) can be done locally and remotely and are one of the most common types of security attacks, because usually they only require regular and inexpensive resources and do not require high technical skills [18]. This paper proposes a new mechanism to be supported only on edge routers, based on the ND messages exchanged by the LoWPAN devices and the edge routers, to mitigate the remotely initiated DoS and DDoS attacks.

The remainder of this paper is organized as follows. Section 2 analyses the IPv6 enabled smart object 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 remotely initiated DoS attacks and discuss its application. Finally, Section 6 concludes the paper and pinpoints future research topics.

DOI: 10.1002/cpe

2. IPV6 ENABLED SMART OBJECT NETWORKS

IEEE 802.15.4 [6] is a data link layer 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 and can support peer-to-peer topologies because of their multihop routing capabilities [19]. RFD devices support only a limited set of functionalities and are mainly used for sensing and/or actuation operations. Multihop communications are not supported by RFD and, thus, they can only be used in star topologies. The protocol defines a central controller device, referred to personal area network (PAN) coordinator, which builds a wireless PAN (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 broadcasts periodically a beacon to announce the WPAN configurations. The other nodes start listening to the beacons to search for available WPAN and to select a coordinator. Only FFD devices can operate as PAN coordinators. Two topologies are supported. In a star topology network, all communications go through the PAN coordinator (i.e., all nodes, except the PAN coordinator, can be RFD devices). In a peer-to-peer topology, devices can communicate with one another directly, but still the PAN coordinator has to exist [20].

The IEEE802.15.4 protocol defines the physical (PHY) and the MAC layers. The PHY layer defines three physical operation modes, 20 kb/s at 868 MHz, 40 kb/s at 915 MHz, and 250 kb/s 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 beacon periodically broadcasted by the PAN coordinator contains information about the PAN. In this 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 is used for data transmission. 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) [21]. In the beaconless mode, there is no superframe structure and no guaranteed time slots. As a consequence, only random access methods, such as unslotted carrier sense multiple access with collision avoidance, 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 constraints do not permit to support IPv6 directly over IEEE 802.15.4 [10]. 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-layer 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 Transmission Control Protocol (TCP) or User Datagram Protocol (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). To circumvent this problem, the Internet Engineering Task Force (IETF) created the 6LoWPAN working group with the aim of defining the support of IPv6 over IEEE 802.15.4 LoWPAN networks. To comply with the maximum transmission unit requirements of IPv6 protocol and to minimize the overhead, 6LoWPAN [11] introduces an adaptation layer 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.

DOI: 10.1002/cpe

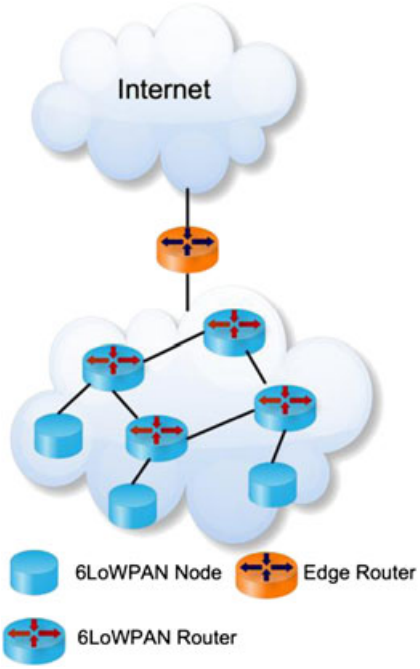

Figure 1. Illustration of 6LoWPAN network architecture.

In LoWPAN networks, packets will often have to use multiple radio hops to reach the destination. The multihop 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 many times, a single physical interface is involved in the forwarding process. The routing process 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 [21, 22]. Link-layer mesh-under 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 perform only sensing and actuation operations. They send their own datagrams to other destination nodes and receive datagrams from other destination nodes but they do not forward datagrams originated on other nodes and destined to other nodes. Routers are intermediate nodes that can be used to forward datagrams 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 other networks, for example, the Internet. Typically, nodes and routers have energy and computational resources constraints and only the edge routers are main powered with more computational resources [10].

2.2. Neighbor discovery protocol for 6LoWPAN

The IPv6 ND 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 [12, 23].

The original IPv6 ND protocol was not designed for nontransitive 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

DOI: 10.1002/cpe

limited because of energy conservation policies. Also, IPv6 ND assumes that local link nodes are always a single hop away and nodes are always listening, but in LoWPAN networks this is not the case.

Although the standard IPv6 ND protocol should work on 6LoWPANs, the resource constraints of LoWPAN nodes, their absence of multicast support at layer two and their low duty-cycle requires a different approach for the ND protocol on 6LoWPANs, focusing on the efficient use of available energy.

Neighbor discovery optimizations for 6LoWPAN [12] are being proposed to address the specific needs of LoWPAN. Neighbor discovery optimization for low power and lossy networks (draft-ietf-6lowpan-nd-18) [12] 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 process with an 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 were replaced by unicast messages. The node to router 6LoWPAN ND message exchange is not affected by the routing approach and, as a consequence, the protocol behavior is the same both in mesh-under and route-over configurations.

The edge router, designated in [12] 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 network. The 6LBR also maintains a network-wide cache of the hostsIPv6 addresses and 64-bit extended unique identifier (EUI-64), 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 addresses are used [24]. There are also optional and separated mechanisms that can be used between LoWPAN routers (6LR) and 6LBR to execute multihop 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 lifetime 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 order router option (ABRO), and 6LoWPAN Context Options (6CO).

Two new ICMPv6 message types are also defined to carry out the optional multihop duplicate address detection: duplicate address request (DAR) and duplicate address confirmation (DAC).

The nodes in a LoWPAN network 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 a router solitication message including the source link-layer address (SLLA), so that the router can reply with a unicast router advertisement message. The router advertisement message can include the SLLA, authoritative order router option, 6CO, and the IPv6 Prefix Option (Figure 2). Once an address has been configured in a node, a neighbor

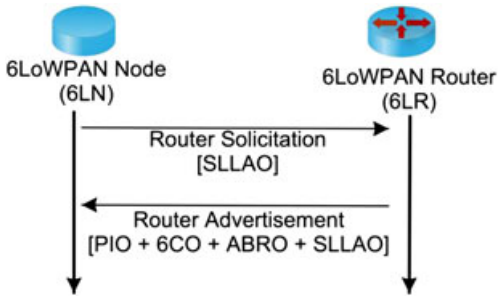

Figure 2. Host initiated router discovery.

DOI: 10.1002/cpe

solicitation (NS) message with an address registration option is sent to the edge router to register that address.

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 ARO. The router replies with a unicast neighbor advertisement (NA) message with the ARO and the status of the registration. The status indicates either a successful registration or a failure (either because of a duplicated address or because the router's registration cache is full).

The address registration mechanism and the SLLA router advertisement option provide enough information in routers and nodes to resolve an IPv6 address 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 and the node must repeat the above described process before the lifetime expires. Note that nodes can receive router advertisements messages from multiple edge routers. In this case, they should attempt to register with more than one router 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 multihop 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 because 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 duplicated. This is carried out using the new DAR and DAC ICMPv6 messages.

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.

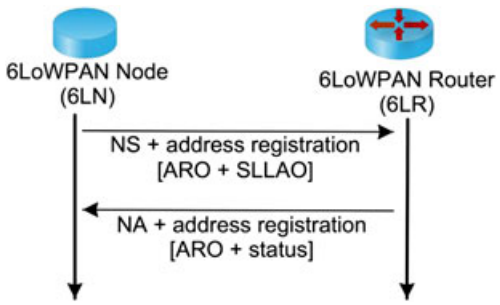

Figure 3. Node address registration.

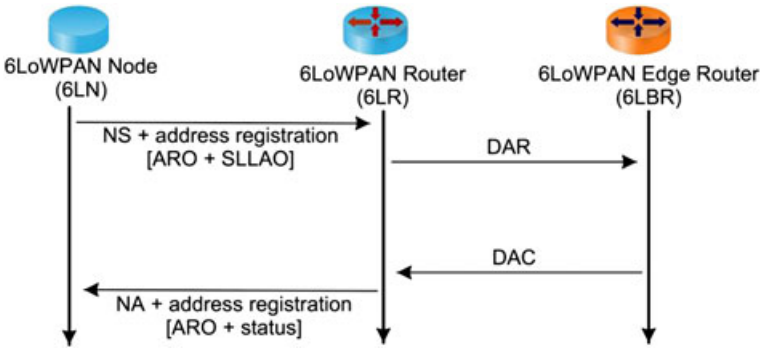

Figure 4. Host address registration with multihop Duplicate Address Discovery (DAD).

DOI: 10.1002/cpe

2.3. Connectivity models

Three main models can be considered concerning the connection of LoWPAN networks to the Internet. In the first model, all LoWPAN nodes support the IP protocol stack but they are not connected to the Internet [25]. In fact, there are several scenarios that do not require any connectivity with the Internet, as 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 because of security and privacy reasons, in most of the cases they are completely disconnected from the public Internet. In this case, the assignment of global IPv6 addresses to all devices is not desirable.

In the second model, a proxy device is used to connect the smart object network to the Internet. Internet users 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-end connectivity. Supporting more than one point of connection between the smart object network and the Internet is not possible if the proxy uses stateful translation mechanisms. This connectivity model is similar to the previous model. Therefore, the support of IP protocol stack 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 fully 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 the 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 stack and more than one router can 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 for each device.

3. SECURITY ATTACKS IN SMART OBJECT NETWORKS

Protecting the resources and the information transmitted over the network from attacks is the main concern of the security services [15–17]. Besides the differences between smart object networks and the other network types, both share some security requirements but, because of resource constraints and the number of nodes, providing security services in smart object networks is even more challenging when compared with standard networks. Confidentiality, integrity, availability, freshness, robustness, and survivability are the most relevant security requirements in smart objects networks [26–28]. Confidentiality ensures that no other than the legitimate entities have access to the data transmitted and stored in the 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 ensures that no message can be altered by any entity, without being detected, as it transverses from the sender to destination. Availability ensures that services provided by the smart object network are always available to be used by the legitimate users. Data freshness prevents other parties from replaying old messages. There are two types of data freshness requirements, strong and weak data freshness. In the first type, it guarantees data framing ordering and delay. In the second type, a partial message ordering is provided, but does not guarantee delay. Robustness and survivability is the guarantee that the network remains operational even if a set of nodes are compromised because of a 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 [15]: 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

DOI: 10.1002/cpe

which are based on cryptography. Device data confidentiality and integrity are harder to obtain when compared with communication confidentiality because they require both logical and physical measures to protect against attackers. Introducing 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 DoS attack. This paper focus on DoS and their countermeasures, in particular to those that can be used to prevent remote initiated attacks.

A DoS attack is characterized by an explicit attempt to prevent the network to perform its expected functions [29]. During a DoS attack, the attacker attempts to reduce the network's capacity. Several strategies can be used to perform a DoS attack. Flooding the network with junk traffic or 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 its performance. Resource exhaustion flooding attacks cause the network nodes or network resources to be consumed to the point where the service is no longer responding or the response is significantly reduced [15]. When a DoS is originated from several sources, it is designated as a DDoS attack. In both cases, the attack sources can be locally or remotely located. The techniques that can be used to perform a DoS attack can be classified according to the protocol layer that is to be attacked [15, 29]. Jamming and tampering are the most common strategies against the physical layer. The jamming is intended to interfere with the normal radio communication link where 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. Forcing frame collisions can be used to achieve resource exhaustion and unfairness and it is the main technique to perform a DoS attack on link layer protocols. Using small frames, error-correction codes and rate limitation are three of the most used mechanisms to mitigate link layer DoS attacks.

In smart object networks, the routing can be performed either on link layer (mesh-under approach) or at network layer (route-over approach). Therefore, DoS attacks directed to routing information protocols can point to both layers. Creating loops and attracting (or repelling) network traffic from selected nodes are the main strategies of DoS attacks directed at routing protocols. Adding message authentication to routing information messages is one of the main countermeasure techniques, because the receivers can detect if the messages have been tampered or spoofed [30, 31].

Managing end-to-end connections is the transport layer main function. Flooding and desynchronization are two of the possible attacks in this layer [15]. 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 because of errors that have never really existed. Puzzle resolution and authentication techniques are the most common countermeasures to prevent transport layer DoS attacks [28, 32]. Note that the UDP protocol is much more used in smart object networks than TCP and, therefore, flooding and desynchronization attacks are not so disruptive. However, any unnecessary transmitted message has an important impact on the energy consumption and UDP is harder to control when end-to-end connections between the smart object and the Internet are supported.

DoS attacks 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. During the attack, one or more clients send a large number of requests reducing drastically the server processing capability. Defending against application layer DoS attacks usually involves some sort of rate-shaping algorithm that monitors client's behavior and ensures that they request no more than a configurable number of requests per time period. If the client generates 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.

In smart object networks, the adequate entity to implement the previous described countermeasures is the edge router for two reasons. First, the edge routers have more energy and computation

DOI: 10.1002/cpe

resources than smart object nodes. Second, it makes more sense to filter the traffic closer to the source.

In the third connectivity model presented in Section 2.3, the smart object networks are connected 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 object network becomes also exposed to remotely initiated security attacks, in particular to DoS and DDoS.

4. MITIGATION OF DOS ATTACKS ON WIRELESS SENSOR NETOWRK WITH IPV6 END-TO-END CONNECTIVITY

This section proposes a countermeasure mechanism based on 6LoWPAN neighbor discovery to mitigate remotely initiated DoS and DDoS attacks. The proposed security mechanism runs only on the edge routers, not overloading the smart object nodes. It reuses the registration address process messages and protects the wireless sensor networks 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 generates no more requests than the imposed limits.

4.1. Proposed mechanism

As explained in 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. Depending on the routing approach, two different procedures can be used to perform the address registration [12]. In the mesh-under routing approach, the nodes exchange the NS and the NA messages with the edge router. In the route-over routing approach, the process is similar to the one for mesh-under between the nodes and the 6LRs and, additionally, the 6LR uses the new DAR and DAC messages to verify the address uniqueness on the edge router.

Note that the current ARO option contains two fields reserved for future use, the first with 8 bits and the second with 16 bits length. Moreover, the DAR messages also contain an 8-bit length reserved field. We propose the use of the 8-bit length reserved fields of both cases to implement the security mechanism. The new information to be included on these field is: (i) the transport-layer protocol switch are to be accepted, (ii) the reachability acceptance from the Internet, and (iii) the maximum Internet clients request rate-shape limit. Figure 5 presents the proposed format for the new ARO and DAR messages. Table I presents the proposed valid values and the description of each new value.

Three new data structures are created at the edge routers: the filtering database, the Internet client's address table, and the Internet client blacklist table.

Information extracted from the new ARO and DAR messages are used to fill the filtering database, according to the correspondence defined in Table II. The filtering database is used to filter unwanted traffic and it is composed of the node's IP address (IP address), the registered lifetime (Lifetime), the reachability acceptance from the Internet (Accept data from the Internet (AFI)),

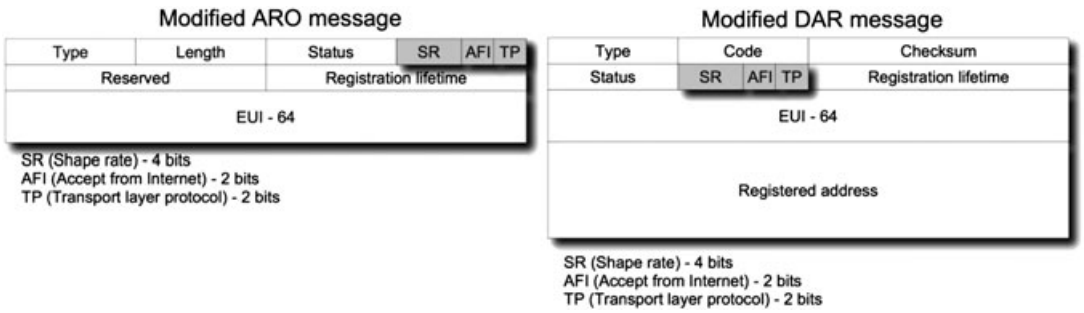

Figure 5. New ARO and DAR message formats.

DOI: 10.1002/cpe

Table I. ARO and DAR new data fields.

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

AFI, Accept from Internet; TP, Transport layer protocol.

Table II. Filtering database fields correspondence.

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

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

Figure 6. Filtering database table format.

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

Figure 7. Internet client address table.

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

Figure 8. Internet client blacklist table.

the accepted transport layer protocol (Accepted transport layer protocol (TP)) and the Internet client rate request limit (Rate request limit (SR)) (Figure 6).

The Internet client address table is used for ensuring that no Internet client generates more packets than the imposed limits. Limits per client and per node will be applied. As may be seen in Figure 7, this table is composed of 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 from the filtering database table.

The Internet client blacklist table is used to store the Internet client's IP address that exceeds the imposed rate limits (Figure 8) and comprise the following fields: Internet client's IP address (IP address), the configurable amount of time in seconds that the IP address must remain 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.

DOI: 10.1002/cpe

Therefore, the blacklist table entries should not be removed after the lifetime goes to zero. However, the oldest entries must be periodically flushed.

4.2. Mesh-under networks

In the mesh-under routing approach [15], nodes register the address directly on the edge router. When a node has configured a nonlink local IPv6 address, it registers that address in one or more edge router, using the NS message with ARO option. Besides the behavior defined in the 6LoWPAN neighbor discovery working progress document, the node also adds to ARO information related to the new fields (i.e., SR, AFI, and TP). If these values are equal to zero, the edge router handles neighbor solicitation message as specified in the 6LoWPAN neighbor discovery working progress document. If the new fields are different from zero, and in addition to the normal behavior, the new field values are copied into the filtering database table according to Table II. The edge router should ignore the new ARO fields if the new format is not supported.

4.3. Route-over networks

In the route-over routing approach [15], the ARO is used to register an address in a 6LR (6LoWPAN router). In this case, the 6LR reuses the information contained in the ARO, sent by the node, in the DAR message (Figure 4). Therefore, in addition to the normal operation defined in the 6LoWPAN neighbor discovery working progress document, the 6LR must copy the new fields (i.e., SR, AFI, and TP) from the ARO message into the new DAR message (Figure 5) before sending it to the edge router. 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.

4.4. Filtering packets received from the Internet

When the edge router receives a packet from the Internet destined to an address of the smart object network, it must first verify if the destined address exists, if the destination node accepts the transport layer protocol of the packet, and if the packet IP source address is not present in the Internet client blacklist table with lifetime value greater than zero. Then, the packet is forwarded, using the regular routing mechanisms, if the previous mentioned conditions are true or discarded, otherwise. Internet client's address and Internet client blacklist tables are updated for each packet received from the Internet.

5. DISCUSSION OF THE PROPOSED SOLUTION

Denial of service and DDoS can be carried out locally and remotely, and they are among the most common types of security attacks, because they require only regular and inexpensive resources, and do not require high technical knowledge. The frequency and sophistication of DoS and DDoS are rapidly increasing based on several techniques including direct attacks, remote controlled attacks, reflective attacks, worms, and viruses.

Although there are several techniques to prevent or to mitigate DoS attacks, a generic defense mechanism against these security attacks is considered a research open issue. Furthermore, most of the proposed defense mechanisms require high computational resources making them inappropriate to be used on smart object networks. DoS is even more destructive to smart object networks when compared with other networks. First, it is easier to exhaust resources on constrained networks. Second, sensors energy can be rapidly consumed making them unavailable until the attack is ended and the battery is recharged.

The proposed security mechanism prevents smart object networks from remotely initiated DoS (and DDoS) network and transport layer attacks. The mechanism filters unwanted traffic originated on the Internet and destined to the smart object network nodes and it is based on the address registration process defined in the ND protocol proposed for 6LoWPAN. With this mechanism, the traffic is forwarded from the Internet to the smart object networks only if it is in accordance with the following rules:

DOI: 10.1002/cpe

- The destination node address must be registered; this condition guarantees that traffic is not forward to nonexisting nodes.
- The nodes must previously declare willingness to accept data from the Internet; in this way, nodes that make no sense to be addressed from outside will not be reached as, for example, the 6LR routers.
- Information about the node's supported transport layer protocol must be previously registered on the edge router; in this way, only traffic of such protocols will be forwarded.
- Nodes should previously inform the edge router about the accepted traffic rate limit; in fact, in most sensor cases, measurements data is generated at a slow acquisition rate(for example, air temperature monitoring), which puts a limit on acceptable request rates preventing, in this way, flooding attacks.

To implement the proposed mechanism, it is only necessary to define three fields in ARO and DAR messages. These fields do not increase the length of the messages because they use already existing 8-bit length reserved fields. Moreover, the mechanism does not increase the overhead on the resource constrained nodes (i.e., smart object nodes and 6LoWPAN routers) because the filtering mechanisms and all processing (and storing) overhead run only on the edge routers, which have less resource constraints. The proposed mechanism uses stateless traffic processing, so it can run 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, the compression rates are not compromised on the new messages because different values are used on the same fields [33].

6. CONCLUSIONS AND FUTURE WORK

Smart object networks, which include wireless sensor networks, can provide support for numerous applications. In fact, the sensors give the smart objects the capacity to sense the physical world and to control some physical processes because of 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 because of two reasons. First, a large number of technologies is used and some of them are incompatible with IP protocol. Second, the security problems because of outside attacks are not an issue.

Providing security services in smart object networks connected to the Internet is considered an open issue. Providing security in resource constrained network is even more challenging when compared with standard networks. Therefore, special protocols and mechanisms have been developed for use in smart object networks. The frequency and sophistication of DoS attacks are rapidly increasing.

This paper has presented a security mechanism to prevent 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 use 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 and the edge routers are the only entities that are required to support storage and processing overhead. The proposed mechanism requires no additional messages than those used to perform the address registration and also does not increase the length of the messages.

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 [17, 28, 32, 34, 35] can be used in the edge router to provide a more coarse traffic admission control. Adding authentication, client puzzle mechanisms to the current

DOI: 10.1002/cpe

solution, providing more application-based control and conducting a performance evaluation in real scenarios will be addressed as 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*. John-Wiley: New York, 2005. ISBN 978- 0470095102.
4. Xu J, Li K, Min G, Lin K, Qu W. Energy-Efficient Tree-based Multi-path Power Control for Underwater Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems,* **99**. DOI: 10.1109/TPDS.2012.49.
5. Xu J, Li K, Min G. Reliable and Energy-Efficient Multi-path Communications in Underwater Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems,* **99**. DOI: 10.1109/TPDS.2011.266.
6. 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). 2006. IEEE Std. 802.15.4–2006.
7. ZigBee Alliance. ZigBee Specification, October 2007.
8. WirelessHARThomepage. January 2012. Available from: http://www.hartcomm.org/
9. Hui J, Culler D. Extending IP to Low-Power, Wireless Personal Area Networks. *IEEE Internet Computing* 2008; **12**(4):37–45.
10. Kushalnagar N, Montenegro G, Schumacher C. IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. August 2007. Internet Engineering Task Force Request for comments 4919.
11. Montenegro G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. September 2007. Internet Engineering Task Force Request for comments 4944.
12. Shelby Z, Thubert P, Hui J, Chakrabarti S, Bormann C, Nordmark E. 6LoWPAN Neighbor Discovery. October 2011. Internet Engineering Task Force, IETF draft draft-ietf-6lowpan-nd-18 working progress.
13. Chang M, Chao C, Chen L, Lai F. An Efficient Service Discovery system for Dual-Stack Cloud File Q14 Q15 Service. *IEEE System Journal* 2011; **99**. DOI: 10.1109/JSYST.2011.2177131.
14. Zhou BL, Chao H-C, Vasilakos A. Joint Forensics-Scheduling Strategy for Delay-Sensitive Multimedia Applications over Heterogeneous Networks. *IEEE Journal on Selected Areas in Communications* 2011; **29**(7):1358–1367.
15. Roman R, Lopez J. Integrating Wireless Sensor Networks and the Internet: a Security Analysis. *Internet Research* 2009; **19**(2):246–259.
16. 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.
17. Du X, Chen H. Security in Wireless Sensor Networks. *IEEE Wireless Communications* 2008; **15**(4):60–66.
18. 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.
19. Zhou CL, Wang X, Tu W, Mutean G, Geller B. Distributed Scheduling Scheme for Video Streaming over Multi-Channel Multi-Radio Multi-Hop Wireless Networks. *IEEE Journal on Selected Areas in Communications* 2010; **28**(3):409–419.
20. 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* 2012; **17**(1):75–89. DOI: 10.1007/s11036-010-0287-x.
21. 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.
22. 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.
23. Narten T, Nordmark E, Simpson W, Soliman H. Neighbor Discovery for IP version 6 (IPv6). September 2007. Internet Engineering Task Force Request for comments 4861.
24. Singh H, Beebee W, Nordmark E. IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes. July 2010. Internet Engineering Task Force Request for comments 5942.
25. Vasseur J, Dunkels A. *Interconnecting Smart Objects with IP*. Morgan Kaufmann: San Francisco, CA, USA, 2010. ISBN 978-0123751652.
26. Ramen R, Lopez J, Gritzalis S. Situation awareness mechanisms for wireless sensor networks. *IEEE Communication Magazine* 2008; **46**(4):102–107.

27. 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.
28. Lopez J, Roman E, Alcaraz C. *Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Network, Foundations of Security Analysis and Design*, LNCS 5705. Springer: Berlin/Heidelberg, 2009. 289–338.
29. 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.
30. Tsao T, Alexander R, Dohler M, Daza V, Lozano A. A Security Framework for Routing over Low Power and Lossy Networks. September 2009. Internet Engineering Task Force, draft draft-tsao-roll-security-framework-01.
31. Karlof C, Wagner D. Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *First IEEE International Workshop on Sensor Network Protocols and Applications*, Alaska, USA, May 2003; 113–127, DOI: 10.1109/SNPA.2003.1203362.
32. Newsome J. The Sybil Attack in Sensor Networks: Analysis and Defenses. In *3rd International Symposium on Information Processing in Sensor Networks (IPSN 2004)*. ACM: New York, NY, USA, Apr. 2004, DOI: 10.1145/984622.984660. (Availablefrom:http://doi.acm.org/10.1145/984622.984660).
33. Hui J, Thubert P. Compression Format for IPv6 Datagrams in 6LoWPAN Networks. October 2009. Internet Engineering Task Force,draft draft-ietf-6lowpan-hc-06 working progress.
34. Shi E, Perrig A. Designing Secure Sensor Networks. *Wireless Communications Magazine* 2004; **11**(6):38–43.
35. Akkaya K, Younis M. A survey of routing protocols in wireless sensor networks. *Elsevier Ad Hoc Network Journal* 2005; **33**:325–349.

DOI: 10.1002/cpe